The pfSense® Firewall/VPN/Router for Amazon AWS is a stateful firewall and VPN appliance. It is suitable for use as a VPN endpoint for mobile devices, laptops, and desktop computers to ensure that data sent over unsecured wireless networks or untrusted wired networks is encrypted using industry standard encryption algorithms. It can also be used to establish a connection between one or many sites with the internet or each other.

This AMI can be run in any region where EC2 offers service on various sizes of instance. pfSense for AWS is available in the AWS Marketplace.

**Getting Started**
In order to use a Netgate appliance instance to protect your VPC subnets, you will need the following:

- A VPC.
- One internet facing public subnet, which the Netgate appliance instance will have its primary/WAN interface connected to.
- One or more private subnets, which the Netgate appliance instance will have its secondary/LAN interface (and possibly additional optional interfaces) connected to.
- Separate routing tables for the internet-facing subnet and the private subnet(s).
- Separate security groups for the internet-facing subnet and the private subnet(s).
- An elastic IP or Public IP for the WAN interface of the appliance.

For the purposes of this guide, your VPC will contain two subnets (public and private) as well as an Internet Gateway. The end result should look like the following diagram:

If you already have all of these in place with an existing VPC, feel free to skip ahead to *Launching an Instance*. 
Custom Route Table

<table>
<thead>
<tr>
<th>Destination</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.0.0/16</td>
<td>local</td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td>igw-id</td>
</tr>
</tbody>
</table>

VPC 172.16.0.0/16

Region

Availability Zone A

Public Subnet: 172.16.0.0/24

Internet Gateway

Internet

EC2 Instances

Private Subnet: 172.16.1.0/24

Disense

Fig. 1: Architecture Diagram
There are a range of specifications to choose from and this page will help guide you through those choices.

### 2.1 Supported EC2 Instance Types

Your instance type will depend on your expected network throughput, as well as the types of services you will provide with your pfSense® appliance.

For general firewall appliances that do not require high throughput, **T2** instances are General Purpose Burstable Performance Instances that provide a baseline level of CPU performance with the ability to burst above the baseline.

If you are planning to provide advanced services like web proxying, IDS/IPS, or Server Load Balancing, you may consider an instance that provides more CPU and/or faster storage resources, such as **m4.large** or **m4.xlarge**.

The following EC2 instance types are supported by Netgate:

- t2.nano
- t2.micro
- t2.small
- t2.medium
- t2.large
- m3.medium
- m3.large
- m3.xlarge
- m4.large
- m4.xlarge
- c3.large
- c3.xlarge
- c4.large
- c4.xlarge
- r4.large
- r4.xlarge
2.2 Sizing Your EBS Volume

The pfSense appliance is only supported with EBS storage. For general purpose firewalls, your storage requirements will typically be small and the default 8GB general purpose SSD volume should be more than enough.

In situations where you may provide web proxying or caching to your users, or other advanced features, you should consider increasing the volume size to something more appropriate, for example 64GB.
NEW SERVICES provisioned in a VPC may be assigned IP addresses or other resources, but Amazon puts limits on VPC resources per Region. Before provisioning a new resource, make sure to check these limits.

The following tables list the limits for Amazon VPC resources per Region. Unless indicated otherwise, requests can be made to increase these limits using the Amazon VPC limits form. For some of these limits, the current limit applied can be viewed using the Limits page of the Amazon EC2 console.

**Note:** If a limit increase is requested that applies per resource, we increase the limit for all resources in the Region. For example, the limit for security groups per VPC applies to all VPCs in the Region.
3.1 VPC and Subnets

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default limit</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPCs per Region</td>
<td>5</td>
<td>The limit for Internet gateways per Region is directly correlated to this one. Increasing this limit increases the limit on internet gateways per Region by the same amount.</td>
</tr>
<tr>
<td>Subnets per VPC</td>
<td>200</td>
<td></td>
</tr>
<tr>
<td>IPv4 CIDR blocks per VPC</td>
<td>5</td>
<td>This limit is made up of your primary CIDR block plus 4 secondary CIDR blocks.</td>
</tr>
<tr>
<td>IPv6 CIDR blocks per VPC</td>
<td>1</td>
<td>This limit cannot be increased.</td>
</tr>
</tbody>
</table>

3.2 DNS

For more information, see DNS Limits.
### 3.3 Elastic IP Addresses (IPv4)

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default limit</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elastic IP addresses per Region</td>
<td>5</td>
<td>This is the limit for the number of Elastic IP addresses for use in EC2-VPC. For Elastic IP addresses for use in EC2-Classic, see Amazon EC2 Limits in the Amazon Web Services General Reference.</td>
</tr>
</tbody>
</table>

### 3.4 Flow Logs

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default limit</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow logs per single network interface, single subnet, or single VPC in a Region</td>
<td>2</td>
<td>This limit cannot be increased. You can effectively have 6 flow logs per network interface if you create 2 flow logs for the subnet, and 2 flow logs for the VPC in which your network interface resides.</td>
</tr>
</tbody>
</table>
### 3.5 Gateways

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default limit</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer gateways per Region</td>
<td>50</td>
<td>–</td>
</tr>
<tr>
<td>Egress-only internet gateways per Region</td>
<td>5</td>
<td>This limit is directly correlated with the limit on VPCs per Region. To increase this limit, increase the limit on VPCs per Region. You can attach only one egress-only internet gateway to a VPC at a time.</td>
</tr>
<tr>
<td>Internet gateways per Region</td>
<td>5</td>
<td>This limit is directly correlated with the limit on VPCs per Region. To increase this limit, increase the limit on VPCs per Region. Only one internet gateway can be attached to a VPC at a time.</td>
</tr>
<tr>
<td>NAT gateways per Availability Zone</td>
<td>5</td>
<td>A NAT gateway in the pending, active, or deleting state counts against your</td>
</tr>
</tbody>
</table>
CREATING AN IAM USER IN YOUR AWS ACCOUNT

pfSense® uses AWS Identity and Access Management (IAM) accounts for administration. Every AWS account includes at least one user. For security reasons, the root account should not be used for day-to-day administration. This section describes the process of creating and using an IAM user account for administering pfSense.

See also:
To find out more about AWS security and credentials read Understanding and Getting Your Security Credentials.

There are multiple methods for creating users in IAM. The recommended method is to use the AWS Management Console. The process of creating a user and enabling that user to perform work tasks consists of the following steps:

1. Create the user.
2. Create credentials for the user.
3. As a best practice, create only the credentials that the user needs. For example, for a user who requires access only through the AWS Management Console, do not create access keys.
4. Grant the appropriate permissions to the user to administer pfSense.
5. Provide the user with the necessary sign-in information.
6. (Optional) Configure multi-factor authentication (MFA) for the user.

4.1 Creating IAM Users (Console)

You can use the AWS Management Console to create IAM users. To create one or more IAM users (console):

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose Users and then choose Add user.
3. Type the user name for the new user. This is the name they will use to sign in to AWS. To add up to 10 users at once, choose Add another user for each additional user and type their user names.
4. User names can be a combination of up to 64 letters, digits, and these characters: +=,.@-  
5. Names must be unique within an account and are not case sensitive.
6. Select AWS Management Console access. This creates a password for each new user.
   - For Console password, choose one of the following:
     - Autogenerated password. Each user gets a randomly generated password that meets the account password policy in effect (if any). You can view or download the passwords when you get to the Final page.
     - Custom password. Each user is assigned the password that you type in the box.
• We recommend that you select **Require password reset** to ensure that users are forced to change their password the first time they sign in.

7. Click **Next**. On the **Set permissions** page, specify how you want to assign permissions to this new user(s). Choose one of the following three options:

   • **Add user to group.** Choose this option if you want to assign the user(s) to one or more groups that already have permissions policies. IAM displays a list of the groups in your account, along with their attached policies. You can select one or more existing groups, or choose **Create group** to create a new group.

   • **Copy permissions from existing user.** Choose this option to copy all access rights from an existing user to the new user(s).

   • **Attach existing policies to user directly.** Choose this option to see a list of the managed policies in your account. Select the policies that you want to attach to the new users or choose **Create policy** to open a new browser tab and create a new policy.

8. Choose **Next: Review** to see all of the choices you made up to this point. When you are ready to proceed, choose **Create user**.

9. To view the users’ access keys (access key IDs and secret access keys), choose **Show** next to each password and access key that you want to see. To save the access keys, choose **Download .csv** and then save the file to a safe location.

   **Important:** This is your only opportunity to view or download the secret access keys, and you must provide this information to your users before they can use the AWS API. Save the user’s new access key ID and secret access key in a safe and secure place. **You will not have access to the secret keys again after this step.**

10. On the final page you can choose **Send email** next to each user. Your local mail client opens with a draft that you can customize and send. The email template includes the following details to each user:

    • User name

    • URL to the account sign-in page. Use the following example, substituting the correct account ID number or account alias:
      
      https://AWS-account-ID or alias.signin.aws.amazon.com/console

    **Important:** The user’s password is not included in the generated email. You must provide them to the customer in a way that complies with your organization’s security guidelines.
AWS IAM Roles are used to delegate access to users, applications, or services that require controlled access to AWS resources. IAM Roles should be used to manage all pfSense® instances. This unique role can be specified when launching a new instance, or attached to an existing instance.

The AWS Management Console is the recommended method for creating roles for use with pfSense. It is also recommended to create these roles based on the principle of least privilege, also known as the principle of least authority, which is the assignment of lowest needed privileges based on necessity. The below instructions attempt to follow this principle.

5.1 Create Policy for pfSense Management IAM Role

Create a custom policy that will be associated with an IAM role allowing access to the pfSense Management GUI running on an EC2 Instance.

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane of the console, select Policies then choose Create Policy.
3. Drop down the Service menu and select EC2.
4. In the Actions dropdown check the box next to All EC2 actions (ec2:)

| Note: | If stricter policies are required for the actions that can be performed on the pfSense EC2 Instance, these can be set here. |

5. Select the Resources dropdown arrow and review resulting warnings.
6. Click the All resources bubble
7. Select Review policy.
8. Populate the Name field (e.g. pfSense_EC2_Access) and Description, if desired.

| Note: | Policy names must be unique within the AWS account, and the name of the policy cannot be changed once created. |

9. Select Create Policy.
5.2 Create IAM Role for pfSense Management

Create a role that an IAM user, or users within an IAM Group, can assume and use to connect to and manage pfSense running on an EC2 Instance.

**Note:** The administrator of the specified account can grant permission to assume this role to any IAM user in that account. To do this, the administrator attaches a policy to the user or a group that grants permission for the `sts:AssumeRole` action. That policy must specify the role’s ARN as the Resource.

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane of the console, select **Roles** then choose **Create Role**.
3. Select the **Another AWS account** role type.
4. In the **Account ID** field, type the AWS account ID that will be allowed to access the destination resource.
5. The **Require external ID** checkbox should remain cleared unless granting permissions to users from an account that you do not control. Reference AWS Documentation for External ID Roles in the event this is required.
6. It is recommended to restrict the role to users who sign in with multi-factor authentication (MFA). Select **Require MFA** to add a condition to the role’s trust policy to require MFA sign-in.
7. Select **Next: Permissions**.
8. Type the name of the previously created Custom policy in the search field. Check the box next to the correct Policy name.
9. Select **Next: Tags**

**Note:** IAM tags are key-value pairs that can be used to organize, track, or control access for this role. This is an optional step. More information can be found within AWS Documentation for Tagging IAM Entities.

10. Select **Next: Review**.
11. Populate the **Role name** field (e.g. pfSense_Admin) and Role description if desired.

**Note:** Role names must be unique within the AWS account, and the name of the role cannot be changed once created.

12. Review remaining configured settings then select **Create role**.

This role can now be assigned to an IAM User or all users in an IAM group allowing secure administrative access to the EC2 Instance(s) containing pfSense.

**Instance Usage**
LAUNCHING AN INSTANCE

Here are instructions on how to launch a new instance of the pfSense® firewall/VPN appliance from the Amazon EC2 Management Console.

1. Select the region for the instance to run in using the region tab at the upper right corner of the page.

   ![Region Selection](image)

   - US East (N. Virginia)
   - US East (Ohio)
   - US West (N. California)
   - **US West (Oregon)**
     - Asia Pacific (Mumbai)
     - Asia Pacific (Seoul)
     - Asia Pacific (Singapore)

2. Navigate to the AWS Management Console Main Page and select EC2 under the Compute section in the All services dropdown.
3. Launch a new instance by clicking on the **Launch Instance** button under the **Create Instance** section of the EC2 dashboard.

4. Select **AWS Marketplace** in the left-hand Navigation Menu. Type **Netgate pfSense** in the search box and press enter.
5. Click the **Select** button for the Netgate pfSense Firewall/VPN/Router listing in the search result.

6. Review pricing and other helpful information, then click **Continue**.
7. Choose the instance type to run by clicking the checkbox next to the desired type. Click Next: Configure Instance Details.

8. Choose the desired Network and Subnet that the instance will be deployed in. Optionally expand the Advanced Details section and set parameters as text in the User Data field. The available options are:

- **password** - setting a value via a directive like `password=abcdefg` will set the password for the administrative account to the value you specify - `abcdefg` in this example. If no value is set here, a random password will be assigned in order to keep administrative access from being exposed to the Internet with a default password.

- **mgmtnet** - setting a value via a directive like `mgmtnet=10.0.1.0/24` will restrict management access (http, https, ssh) to the network you specify - `10.0.1.0/24` in this example. This will cause the firewall rules on the instance (not on Amazon’s access lists, but on the Netgate pfSense appliance’s own firewall) to restrict management traffic for the instance to the specified source network. The default behavior is to allow management from any host.
These directives can be set by placing them on a single line in the User Data field and separating them with colons. To specify both parameters, type a statement similar to this one:

```
password=abcdefg:mgmt.net=10.0.1.0/24
```

**Note:** If a password is set using the password parameter listed above, the password is retrieved by the instance via an unencrypted HTTP request when the system is configured the first time it boots. The request is made to an Amazon Web Services-operated server on the local LAN that stores metadata about each instance running. The data for an instance is only made available to that instance, but is available to be queried from the instance without providing any authentication credentials.

It is advised to change the admin password via the pfSense web GUI after the instance comes up to avoid any security risks associated with the unencrypted request. Otherwise it is possible to choose not to set the password at all and let a random password be set.

9. Choose the desired Network and Subnet to which the Instance will be deployed. Scroll down to configure the network interface(s) with a Static or DHCP-assigned IP address.

10. Click Next: Add Tags to accept the Storage Device Configuration.
11. It is recommended to set a tag that can be used to differentiate this instance from other instances by entering a value for the **Name** tag. Click **Next: Configure Security Group** after setting any desired tags.

Press the **Add Tag** button. Input **Name** under the **Key** field and the desired **Instance Tag Name** under the **Value** field (e.g. *Netgate Firewall/Router*).

12. Select a security group to launch the instance with. The **Security group name** and **Description** can be left at the default, or replaced with the desired values. The recommended settings for a security group should allow at least the following traffic:

- **TCP port 443 from 0.0.0.0/0**
  - HTTPS - This is the port that the management web GUI listens on.
- **TCP port 22 from 0.0.0.0/0**
  - SSH - This port can be used to connect to a command prompt with an ssh client.
- **UDP port 1194 from 0.0.0.0/0**
- OpenVPN - The OpenVPN server that is configured by default is bound to this port.
- UDP port 500 from 0.0.0.0/0
- IKE for IPsec VPN.
- UDP port 4500 from 0.0.0.0/0
- IPsec/NAT-T for IPsec VPN.

**Note:** If there is an existing security group that includes this access, click Select an existing security group, then select the desired group(s) to use and click Continue. Otherwise, select Create a new security group, and add rules for this access by filling in the form for each rule and clicking the Add Rule button. When all of the rules have been added, click Review and Launch.

13. Review any AWS warnings and make note of recommendations. Scroll down to review the remaining instance details and click Launch after making any needed adjustments.
14. Select an existing key pair or create a new key pair to connect to the instance with. Click the checkbox that indicates acknowledgment of access to the selected private key file and then click **Launch Instances**.

**Important:** Do NOT select the **Proceed Without a Key Pair** option.
MANAGING THE CONFIGURATION OF THE INSTANCE

Once the instance is launched, monitor its status using the Instances page of the EC2 Management Console. The EC2 Management Console will display whether the instance is up and reachable and will also display its current public IP address and the hostname that resolves to the public IP address. Find the hostname and public IP address in the EC2 console by clicking on the Instances heading on the left, finding the instance and checking the checkbox next to it and looking at the details at the bottom of the page.

In the example above, the hostname of the instance is ec2-23-20-204-54.compute-1.amazonaws.com. The public IP address is available by putting together the 4 numbers included in the hostname - 23.30.204.54. It is also possible to obtain the IP address by using a popular DNS lookup tool such as host, dig, or nslookup to resolve the hostname to its IP address.

Note: The hostname and IP address used in this and other examples in this guide are associated at the time of writing with a test instance. This address/hostname will not be the same values used to access the instance and they will not even be associated with the same test instance by the time this guide is available to the public.

In order to manage the configuration of the instance, connect to it via https or ssh. To connect via ssh, use the key pair chosen while creating the instance to connect to the admin account. From the command line on a Unix/Linux host, use a command similar to ssh -i my_key_file admin@public_IP, where the appropriate private key file and public IP or hostname are substituted. In the example below, the key file my_ec2_key is used to connect to the IP address 23.20.204.54.

Note: The first time logging into the instance, the ssh key of the instance will not be cached locally, type yes when
asked whether to continue connecting. This should not be necessary on subsequent sessions.

A limited set of configurations is possible through the ssh interface. The preferred method for managing most of the configurations or viewing data on the status of the pfSense® instance is through the https web GUI. To connect via https, enter an https:// URL containing the public IP address or hostname of the instance into a web browser. For example, https://23.20.204.54.

It’s very likely there is a browser warning indicating that the security certificate of the site is not trusted, because the instance uses a self-signed certificate for https communication. Click on the option to proceed to the site anyway and a login screen with the Netgate logo should appear.

The username to log in with is **admin**. The password to use is either a value set in the User Data during the creation of the instance or a random password. If a specific password wasn’t set, find out that value that the random password was set to through one of two different means:

1. The first is to log in over ssh with the key pair that was selected when the instance was created and examine the contents of the file located at **/etc/motd**. Select option 8 (**Shell**) from the console menu that is presented after log in and execute `cat /etc/motd` from the shell.

2. Alternatively, view the System Log for the instance in the EC2 Management Console. After the messages that are displayed that show the status of the boot process, a message should appear that indicates what the administrative password was changed to.

The message, using either of the methods mentioned, will look like this

```
***
***
```
In this example, the password was changed to `abcdefg`.

**Note:** Be aware that the System Log output in the EC2 Management Console is not updated in real time and may take a few minutes to show up. It is preferable to explicitly set a password by passing a value in with the User Data field so the password will be known in advance. To allow a random password to be set, connect via ssh and find out what the password was changed to after the instance is up without any delay.

Once the password has been determined and entered into the login form, the pfSense Web GUI should be available.
Using the Remote Access IPsec VPN

An IPsec VPN for remote users is preconfigured on the instance when it comes up. In order to use it, you will need to configure the IPsec VPN client on your device.

See also:

A guide for manually configuring Android or iOS (iPhone/iPod/iPad) mobile clients to establish an IPsec VPN is located in the pfSense® Documentation.

For iOS clients, a profile can be downloaded and installed that will automatically configure an IPsec VPN to the instance. The profile can be downloaded by visiting the page at `/iphone_ipsec_profile.php` on the instance. If the instance IP address were 23.20.204.54, the correct URL to visit would be `https://23.20.204.54/iphone_ipsec_profile.php`. You will need to authenticate to the web interface by typing the username (admin) and password prior to being able to download the profile.

The profile should be downloaded and saved automatically upon opening the page. If the page is visited in a web browser on an iOS device, the device should automatically launch the Settings app and attempt to install the new profile. If the profile is downloaded to another non-iOS device, it can be sent via email as an attachment. If the attachment is opened in the iOS email client, the Settings app new profile installation will also open.

The name and description of the profile being installed will be displayed. Tap the `Install` button. A warning message will be displayed that indicates that the profile is unsigned. Tap on `Install Now` to continue.

Enter your passcode for the iOS device (the one you enter when you wake the device from sleep) and the password to access the IPsec VPN (the one you entered to get access to the Web GUI) when prompted and the profile will be installed. When the screen shows that the profile was installed, tap `Done`.

When the profile has been installed, the VPN can be enabled in the Settings app. There will be a heading named `VPN` under the main Settings page. If there are more than one VPN configured on the device, tap the VPN heading. The newly installed profile should be selected. It will have a check mark next to it. There will be an on/off switch at the top of the page to enable the VPN. If this is the only VPN configured, the switch to enable the VPN will be next to the VPN heading on the main Settings page. Tap the switch to enable the VPN. You should be prompted for a username and password. The username (admin) should already be filled in. Enter the password and tap `OK`. A welcome message should be displayed. Tap `OK` and you are ready to use the VPN.
An OpenVPN VPN for remote users is automatically configured the first time the instance is booted. In order to use it, you will need an OpenVPN client app installed on your device and you will need to import a configuration that specifies how to connect to the instance.

An OpenVPN configuration can be downloaded by visiting the page /openvpn_connect_profile.php on your instance. If the instance IP address were 23.30.204.54, the correct URL to visit would be https://23.20.204.54/iphone_ipsec_profile.php. You will need to authenticate to the web interface by typing the username (admin) and password prior to being allowed to download the configuration.

The profile should be downloaded and saved automatically upon opening the page. The file that it was saved in should be imported into the OpenVPN client on the device that you wish to connect with.

### 9.1 Tips for configuring OpenVPN based on platform/client

#### 9.1.1 OpenVPN Connect App on iOS (iPhone/iPad/iPod)

The iOS version of the OpenVPN Connect App allows you to import an OpenVPN profile by opening an attachment to an email message. Save the config to a file named remote-access-vpn.ovpn and send it to an email account that the iOS device is configured to retrieve mail for. Open the email message and touch the attachment to open it. You will be presented with Open in OpenVPN as one of the available options. Touch the OpenVPN icon to select that option. The OpenVPN Connect App should then open and list the profile under a heading that says **New profiles are available**…. Click on the green ball with the + sign in it to import the profile. Type in the username, admin, and password then change the On/Off switch to **On**.

#### 9.1.2 OpenVPN Connect App on Android

The Android version of the OpenVPN Connect App allows you to import an OpenVPN profile from an SD card. Save the configuration file to the SD card. Launch the OpenVPN Connect App. From the menu, select Import, then Import Profile from SD card. Browse to the location of the configuration file and select it. Enter the username, admin, and password to connect to the VPN. Press **Connect**.

#### 9.1.3 TunnelBlick on MacOS X

The TunnelBlick App for MacOS allows you to import an OpenVPN configuration file. Save the configuration to a file on your system. Click on **VPN Details**. Click on the + symbol underneath the existing configurations to add a new configuration. Click on the **I have configuration files** button. Click on the **OpenVPN Configuration(s)** button. Follow the instructions presented by TunnelBlick (copy the config into an empty folder TunnelBlick creates on the
Desktop, rename the folder, click on the folder). When the profile is imported successfully, click on its name and then click on Connect. Enter the username, admin, and password to connect to the VPN.

9.1.4 OpenVPN Connect Client on Windows

The OpenVPN Connect Client on Windows allows you to import an OpenVPN configuration file from the local disk. Save the file on your system. Click the + symbol to the right of Connection Profiles. Select Local File and click on the Import button. Find the profile you wish to import in the file browser window and click Open. A box with the name of the new profile should appear under Connection Profiles now. Click on that box and enter the username, admin, and password to connect to the VPN.
ENABLING ENHANCED NETWORKING WITH THE ELASTIC NETWORK ADAPTER (ENA)

To enable enhanced networking on AWS, pfSense® Firewall/VPN/Router must be version 2.4.1 or above. Use the update wizard in the pfSense console to perform the update if necessary and then ENA can be enabled. Enabling ENA is outlined in the steps below:

**Warning:** Updating the pfSense Firewall/VPN/Router will force it to reboot and cause a disruption in service. Be sure to perform the update during a maintenance cycle.

1. Install AWS CLI. Documentation on the installation and use of AWS CLI can be found at https://aws.amazon.com/cli/
2. Determine the Instance ID for the pfSense Instance from the EC2 Console.
3. Stop the instance using Amazon EC2 console.
4. Enable the enhanced networking attribute by executing the following AWS CLI command:
   ```bash
   aws ec2 modify-instance-attribute --instance-id i-042c16b65423b7dac --ena-support
   ```
5. Use the EC2 Console to start the pfSense Instance. Once the pfSense Instance has started, confirm that EnaSupport is enabled by executing the following AWS CLI command:
   ```bash
   aws ec2 describe-instances --instance-ids i-042c16b65423b7dac --query 'Reservations[].Instances[].EnaSupport'
   [true]
   ```
6. Change the pfSense Instance Type to one that supports Enhanced Networking using the EC2 console. After selecting an Instance Type that supports Enhanced Networking use the EC2 console to stop the pfSense Instance.
7. Once the pfSense Instance has stopped, use the EC2 Console to select the pfSense Instance and then under the Actions button select Instance Settings > Change Instance Type and select a new Instance Type.
8. In the EC2 Console the pfSense Instance should now show an Instance Type of m4.xlarge.
9. Using the EC2 console select the pfSense Instance and then under the Actions button select Instance State > Start.
Fig. 1: The selected pfSense Instance ID is i-042c16b65423b7dac.
Fig. 2: In this case m4.xlarge was selected as the new Instance Type and then Apply was selected.
11.1 Protecting a private network in VPC

An instance of the Netgate appliance can be used as a firewall for a VPC subnet. This will generally require more manual configuration than using an instance to host a remote access VPN does. See the VPC User Guide for a more detailed explanation of how to configure your VPC and your Netgate appliance instance to support this.

11.2 Connecting a local pfSense® device

In addition to connecting remote devices as clients, a device running pfSense® as a firewall/router can be connected as a peer to a pfSense appliance.

See also:
Read Configuring a Site-to-Site Static Key OpenVPN Instance in the pfSense documention to see the process of configuring this setup.

When implementing the configuration changes detailed in the document, you should use the Netgate appliance instance on AWS as the “server” end of the connection and your local pfSense device as the client “end”. You will also need to make sure that you are using a unique port. The default remote access OpenVPN server is configured to use UDP port 1194. It is suggested that if you are adding a site-to-site tunnel, you should use a port between 1195 and 2000. Whichever port you decide to use, you will need to make sure that the port is open both in the firewall rules on the Netgate appliance instance and in the Security Group in the EC2 Management Console.

If you wish to route all traffic from your home/office network through the OpenVPN tunnel to your Netgate appliance instance, you will need to add this statement to the advanced options for the OpenVPN Client on the home/office pfSense device:

```
redirect-gateway def1;
```

This will cause a default route to be set that sends all locally originated traffic on your home/office network over the OpenVPN tunnel when it is established. If you use this configuration to send all traffic from your local network through the OpenVPN tunnel, you will also need to establish a NAT on the Netgate appliance instance on AWS for traffic from the home/office network to the internet. This can be accomplished by adding the CIDR block for your home/office network to the preconfigured Alias called Networks_to_NAT. This is done by navigating to Aliases under the Firewall heading on the web GUI, then clicking on the edit icon to the right of Networks_to_NAT. Add the new network address and mask to the list of Networks and click the Save button. Then click the Apply Changes button. You will also need to add the network used for the tunnel endpoints (IPv4 Tunnel Network) to the Networks_to_NAT alias as well using the same procedure that was used to add the home/office network.
11.2.1 Connecting multiple pfSense gateways to a Netgate appliance

Multiple home/office networks can be connected to a single Netgate appliance instance. This could be used to allow clients at different office locations to communicate without requiring tunnels between each individual location. It could also be used as a way to apply policies on traffic to/from the internet in one place and have them take effect across multiple locations.

Each site would need to have the instructions above for connecting an individual device repeated to add an OpenVPN server on the Netgate appliance instance and an OpenVPN client on the local pfSense device. Each OpenVPN Server that is configured must use a unique port and a unique network for IPv4 Tunnel Network. It is recommended to use a name that uniquely identifies each location connected in this manner in the Description field when adding an OpenVPN Server for a site in the Netgate appliance.

11.3 Detect and Recover EC2 Instance Failure

You can create an Amazon CloudWatch alarm that monitors an Amazon EC2 instance and automatically recovers the instance if it becomes impaired due to an underlying issue.

For more information about instance recovery, see Recover Your Instance.
FREQUENTLY ASKED QUESTIONS

Contents

• Frequently Asked Questions
  – 1. I don’t know the password to the web GUI. How do I find out what it is?
  – 2. I don’t like the random password that was selected. How can I change it?
  – 3. How do I access my instance?
  – 4. How do I connect a VPN client to my instance?
  – 5. Why does the pfSense® Dashboard say my WAN address is 10.X.Y.Z?
  – 6. I added custom firewall rules to allow some traffic to my instance, why I am not seeing the packets arrive?
  – 7. How do I route all the traffic from my entire home network over a VPN?

12.1 1. I don’t know the password to the web GUI. How do I find out what it is?

The first time the instance boots, it looks for a user-defined password set in the User Data box when the instance was created. If you didn’t set one, it chooses one randomly so that the instance is not accessible via a default password to malicious users. You can find out the random password that was set by choosing Get System Log from the Actions Menu for the instance in the EC2 Management Console. A message should appear after the system boot messages that looks like the following:

```
***
***
*** Admin password changed to: abcdefg
***
***
```

It may take 5-10 minutes after the instance boots for this message to appear in the system log. If you would like to find out the password sooner, you can log in via SSH using the SSH key that was selected when the instance was created. The same message that will be written to the system log will be written to the file /etc/motd. Running the command cat /etc/motd will show you what the password is.
12.2 2. I don’t like the random password that was selected. How can I change it?

The password can be changed via the web GUI. Log in with the username admin and the existing password. Under the System category, click on User Manager. The admin account should appear in a list of accounts. Unless you’ve added other accounts, it should be the only account present. Click on the Edit button (the icon with the e in it) to the right of the account listing. Type your choice for a new password into the two boxes labeled Password. Click the Save button at the bottom of the screen.

12.3 3. How do I access my instance?

There are several ways that you can manage or use your instance. You should be able to connect via SSH or HTTPS in order to manage the configuration of your instance. If you connect via SSH, you will either need to know the password of the admin account and login with that account, or use the SSH key that was selected when the instance was created. Here is a sample command line to log in with an SSH key from a Unix or Linux host:

```
ssh -i ~/.ssh/my-ec2-key admin@ec2-A-B-C-D.compute-1.amazonaws.com
```

You would substitute the actual location of your SSH private key for `~/.ssh/my-ec2-key` and the real hostname, which you can retrieve from the EC2 Management Console by looking at the data for the instance, for example `ec2-A-B-C-D.compute-1.amazonaws.com`. If you know the password for the admin account, you could use a command similar to the one above, but omit the `-i ~/.ssh/my-ec2-key`.

To connect via HTTPS, you need to know the password to the instance, either by setting it explicitly in the User Data when the instance is created or by retrieving it from the instance. Once you know the password, you should be able to connect to the instance with any web browser by typing in the hostname of the instance to the URL field.

12.4 4. How do I connect a VPN client to my instance?

See the section in the user guide on Using the remote access IPsec or OpenVPN VPN.

12.5 5. Why does the pfSense® Dashboard say my WAN address is 10.X.Y.Z?

Amazon AWS instances use DHCP to assign private addresses to the public-facing interfaces of an instance. The publicly routable IP address that you use to access the instance is NATed by Amazon to the private address that you see configured on the WAN interface of your instance.

12.6 6. I added custom firewall rules to allow some traffic to my instance, why I am not seeing the packets arrive?

Amazon AWS provides packet filtering in addition to the Netgate Appliance itself being a stateful firewall. If you allowed traffic on the Netgate Appliance but have a security group configuration in the settings for the instance that is restricting traffic, you will need to also add your rules to the security group in the EC2 Management Console.

Given that the Netgate Appliance is a fully functional firewall, you may assign an AWS security group that allows all traffic and perform whatever filtering you desire with rules on the Netgate Appliance.
12.7 7. How do I route all the traffic from my entire home network over a VPN?

If your home gateway/router has support for OpenVPN, you can connect a site to site tunnel from your home network to the Netgate VPN Appliance and configure your routing so that all Internet traffic is sent over the encrypted tunnel. See the user guide section on *Connecting a local pfSense® device*.

This may provide for simpler administration at home, but your mobile devices and laptops that get used outside the home should have an OpenVPN client installed and configured anyway so that you are always receiving the benefits of sending your traffic through a VPN.
The pfSense® Certified firewall and VPN appliance from Netgate for Amazon EC2 is a stateful firewall and VPN appliance. In addition to its capabilities as a VPN gateway and firewall for users and offices, it is capable of acting as a firewall to protect instances providing services in Amazon’s Virtual Private Cloud or VPC service. This service differs from the classic EC2 service in that it allows for management of instances on private subnets.

This guide will explain how to launch, manage, and use an instance of the appliance to act as a gateway for other instances in a VPC subnet.

13.1 Preparing your VPC

In order to use a Netgate appliance instance to protect your VPC subnets, you will need the following:

- One internet-facing subnet, which the Netgate appliance instance will have its primary/WAN interface connected to.

- One or more private subnets, which the Netgate appliance instance will have its secondary/LAN interface (and possibly additional optional interfaces) connected to.

- Separate routing tables for the internet-facing subnet and the private subnet(s)

- If you already have all of these in place with an existing VPC, feel free to skip ahead to Launching an Instance.

These instructions will demonstrate how to create a single private subnet and set it up behind an instance of the pfSense® Certified firewall and VPN appliance from Netgate. In the Amazon VPC Management Console, create a new VPC, subnets, and routing table(s).

1. Go to Your VPCs view in the menu on the left side of the VPC Management Console under the Virtual Private Clouds grouping. Click the Create VPC button.
2. Enter a CIDR block to use in the box that pops up. If you will connect to hosts in your VPC using a VPN from hosts at other sites in your infrastructure, be sure to select address space that does not conflict with the private address space used elsewhere by your organization. Make sure the block you choose is large enough to contain all subnets you may want to include within it. E.g. if you plan to use a /24 for your internet-facing subnet and a /24 for your private network, the CIDR block you select here will need to be at least a /23 to hold those 2 subnets. The maximum size block you can select is a /16. For the purposes of this example, we will use 10.2.0.0/16. Leave the value of Tenancy set to Default. Click on the Yes, Create button.

3. To create the subnets required, go to the Subnets view in the menu on the left side of the VPC Management Console. Click the Create Subnet button. Select the VPC you just created and choose the availability zone you desire. Enter the subnet you wish to use for the internet-facing hosts in the CIDR Block field. This subnet will be the one that the WAN interface of the Netgate appliance instance is attached to and could include any other hosts or appliances that you wish to be available directly from the Internet and not protected behind the Netgate
The subnet you select here must be a block that is within the address space you assigned to the VPC. For this example, we will use 10.2.0.0/24. Click on the **Yes, Create** button.

4. Create the private subnet. Still in the **Subnets** view of the VPC Management Console, click the **Create Subnet** button. In the box that pops up, select the appropriate VPC and the same Availability Zone that you assigned to your public subnet. Enter the subnet you wish to use for your private network in the CIDR Block field. This network should be a subnet of the address space you assigned to the VPC and should be distinct from the subnet you assigned to the public subnet. For this example, we will use 10.2.1.0/24. Click on the **Yes, Create** button.

5. Both subnets that you created will have been created to use a default route table that was created for the VPC. The private subnet can continue to use that default table. A new route table will need to be created for the public subnet. Go to the **Route Tables** view in the menu on the left side of the VPC Management Console. The single existing route table should be displayed. Click on the **Create Route Table** button. Select the VPC and click on
6. Associate the public subnet (10.2.0.0/24 in our examples) with the routing table that was just created. Go to the Subnets view on the left hand side of the VPC Management Console. Check the checkbox next to the public subnet and scroll down to look at the Details tab for that subnet. At the top of the Details tab will be listed the CIDR block, VPC, and Availability Zone. Under those items, the Route Table will be listed and will have a link labeled replace next to it. Click on the link. Select the route table in the box that pops up and click on the Yes, Replace button.

7. In order to send traffic from the public subnet to the Internet, we will need to add a default route to an Internet Gateway. We must first create one. Go to the Internet Gateways view in the menu on the left hand side of the VPC Management Console. Click on the Create Internet Gateway button. Click the Yes, Create button on the box that pops up. Click the checkbox next to the new Internet Gateway and then click the Attach to VPC
button. Select the VPC and click on the **Yes, Attach** button.

8. The route table for the public subnet will need to be updated so that it has a default route to the Internet Gateway. Go to the **Route Tables** view on the left hand side of the VPC Management Console. Check the checkbox next to the route table for the public subnet. Under the **Routes** tab for that route table, there should only be listed a single route for the CIDR block of the VPC (10.2.0.0/16 in our example) that has a target of **local**. There is a row underneath this route with a text box in the Destination field and a pop up menu for the Target field. Enter **0.0.0.0/0** for the Destination and select the Internet Gateway (should be formatted like igw-XXXXXXX) for the target. Click on the **Add** button that appears at the right side of the row. Click the **Yes, Add** button on the box that pops up.

There are a few more VPC configuration changes that will be required later, but next you must launch a Netgate appliance instance.
13.2 Launching an Instance in a VPC

In the Amazon EC2 Management Console, launch a new instance of the pfSense® firewall and VPN appliance. This process is the same as the one for launching an EC2 (non-VPC) instance, up until step 11, which details the values to enter for the Configure Instance Details screen in order to specify the instance should be created in your VPC.

1. Select the region to run the instance in using the tab at the upper right corner of the page.

2. Launch a new instance by clicking on the Launch Instance button under the Create Instance section of the EC2 dashboard.
3. Select **AWS Marketplace** on the **Create a New Instance** menu. Type **Netgate pfSense Firewall/VPN/Router** in the search box and press enter (or click on the **Search** button next to the text box).

4. Click on the link for the **Netgate pfSense Firewall/VPN/Router** appliance in the search results.

5. Click on the **Continue** button on the info page for the Netgate pfSense Firewall/VPN/Router.
6. Click on the Launch with EC2 Console tab

7. If the license terms haven’t been accepted, click on the Accept Terms button.

8. A message should be displayed indicating that the subscription is being processed.
9. Select the version of the image to run under the popup menu labeled Select a Version. Generally the most recently issued version should be selected. Identify which region to launch the instances in and click on the Launch in EC2 Console button to the right of that region.

10. Choose the instance type to run on. Click Next: Configure Instance Details.
11. On the **Configure Instance Details** page, under the **Network** field, select the VPC that was created. For the **Subnet** field that appears right below the **Network** field, select the public subnet that was created earlier. In our examples, this is **10.2.0.0/24**.

12. Scroll down to the **Network Interfaces** heading. A single interface named **eth0** should be displayed by default. Click on the **Add Device** button underneath **eth0**. Select the private subnet that was created (**10.2.1.0/24** in our example). Pick an IP address within the range of the private subnet and enter it in the **Private IP** field. Keep in mind that the first 3 or 4 IP addresses are reserved. For this example, we will use **10.2.1.5**.
Optionally, expand the **Advanced Details** section and set parameters as text in the **User Data** field. The available options are:

- **password** Setting a value via a directive like `password=abcdefg` will set the password for the administrative account to the specified value - `abcdefg` in this example. If no value is set here, a random password will be assigned in order to keep administrative access from being exposed to the internet with a default password.

- **mgmtnet** Setting a value via a directive like `mgmtnet=10.0.1.0/24` will restrict management access (http, https, ssh) to the specified network - `10.0.1.0/24` in this example. This will cause the firewall rule on the instance (not on Amazon’s access lists, but on the Netgate appliance’s own firewall) to restrict management traffic for the instance to the specified source network. The default behavior is to allow management from any host.

These directives can be set by placing them on a single line in the **User Data** field and separating them with colons. Specify both parameters, by typing a statement similar to:

```
password=abcdefg:mgmtnet=10.0.1.0/24
```

Click **Next: Add Storage** after optionally setting these parameters.

**Note:** If setting a password using the password parameter listed above, the password is retrieved by the instance via an unencrypted HTTP request when the system is configured the first time it boots. The request is made to an Amazon Web Services-operated server on the local LAN that stores metadata about each instance running. The data for an instance is only made available to that instance, but is available to be queried from the instance without providing any authentication credentials.

It is advised to change the admin password via the pfSense webGUI after the instance comes up, or choose not to set the password at all and let a random password be set.
13. Click Next: Tag Instance to accept the Storage Device Configuration.

14. Optionally, a tag can be set on the instance to differentiate this instance from other VM’s that were started by entering a value for the Name tag. Click Next: Configure Security Group after setting any desired tags.
15. Select a security group to launch the instance with. The recommended settings for a security group should allow at least the following traffic:

- TCP port 443 from 0.0.0.0/0 - HTTPS - This is the port that the management web GUI listens on.
- TCP port 22 from 0.0.0.0/0 - SSH - This port can be used to connect to a command prompt with an ssh client.
- UDP port 1194 from 0.0.0.0/0 - OpenVPN - The OpenVPN server that is configured by default is bound to this port.
- UDP port 500 from 0.0.0.0/0 - IKE for IPsec VPN.
- UDP port 4500 from 0.0.0.0/0 - IPsec/NAT-T for IPsec VPN.
If you have an existing security group that includes this access, select **Select an existing security group**, then select the group(s) to use and click **Continue**. Otherwise, select **Create a new security group**, and add rules for this access by filling in the form for each rule and clicking the **Add Rule** button. When all of the rules have been added, click **Review and Launch**.

16. Verify the details for the instance and click **Launch**.

17. Select an existing key pair or create a new key pair to connect to the instance with. Do not select **Proceed**
Without a Key Pair. Click the checkbox that indicates you acknowledge having access to the selected private key file and then click Launch Instance.

18. In order to reach the instance from the Internet, associate an Elastic IP with the WAN interface of the instance. In the VPC Management Console, go to the Elastic IPs view by clicking on Elastic IPs on the left side of the page. Click on the Allocate New Address button. Select that you want the EIP used in VPC and click on the Yes, Allocate button in the box that pops up. After the Elastic IP address is allocated, associate the address with the WAN interface of the Netgate appliance by clicking on the Associate Address button.

A box will pop up that will either let you specify the instance and Private IP address of the interface or the Network Interface and the Private IP Address of the interface. Use one of these methods to select the correct interface and click on the Yes, Associate button. The instance should now be reachable via ssh or https.
19. In order for traffic to be allowed to be routed from the private subnet through the public interface of the instance, the Source/Dest Address Check on the private interfaces needs to be disabled. In the EC2 Management Console, go to the “Network Interfaces” view by clicking on Network Interfaces in the menu on the lefthand side of the page.

Click the checkbox to the left of the private/LAN interface on the Netgate appliance instance. Click on the Actions button at the top of the page and select Change Source/Dest Check on the popup menu. Select the radio button labeled Disabled on the box that pops up and click on the Save button.

Non-local traffic from the private subnet should now be sent through the private/LAN interface on the Netgate appliance instance.
13.3 Managing a VPC Instance

Once the instance is launched, you can connect to it via the Elastic IP that was attached to the primary interface during the provisioning phase.

In order to manage the configuration of the instance, you can connect to it via https or ssh. A limited set of configurations is possible through the SSH interface, the preferred method for managing most of the configurations or viewing data on the status of the pfSense® instance is through the https webGUI.

13.3.1 Connecting via SSH

To connect via SSH, you would use the key pair you chose while creating the instance to connect to the admin account. From the command line on a Unix/Linux host, you would use a command similar to:

```
ssh -i my_ec2_key admin@23.20.204.54
```

Where the appropriate private key file and public IP or hostname are substituted.

**Note:** The first time you log into your instance, the SSH key of the instance will not be cached on your computer and you will need to type yes when asked whether you want continue connecting. This should not be necessary on subsequent sessions.

Once logged in, you should see the console menu similar to the one below:
13.3.2 Connecting via HTTPS

To connect via https, you would enter a URL containing the public IP address or hostname of your instance into a web browser. For example, https://23.20.204.54. It’s very likely that you will receive a browser warning indicating that the security certificate of the site is not trusted. This is because the instance uses a self-signed certificate for https communication. You should click on the option to proceed to the site anyway. The pfSense login screen with the Netgate logo should appear.

The username to log in with is admin. The password to use is either a value that you set in the User Data during the creation of the instance or a random password.

Tip: It is preferable to explicitly set a password by passing a value in with the User Data field so the password will be known in advance.

If you did not set a specific password, you can find out that value that the random password was set to through one of 2 different methods.

1. The first method is to log in over SSH with the key pair that you selected when the instance was created and examine the contents of the file located at /etc/motd. You would do this by selecting option 8) Shell in the console menu that is presented when you SSH in, then run this command in the shell:

   ```
   cat /etc/motd
   ```

2. The second method is to view the System Log for the instance in the EC2 Management Console. After the messages that are displayed that show the status of the boot process, a message should appear that indicates what
the administrative password was changed to. Be aware that the System Log output in the EC2 Management Console is not updated in real time and may take a few minutes to show up.

The message you should look for using either of the methods mentioned about will look like this:

```plaintext
***
***
*** Admin password changed to: abcdefg
***
***
```

Once you’ve determined your password and entered it into the login form, the pfSense WebGUI should be available to you.

### 13.4 Forwarding traffic from VPC subnets through the instance

Some additional configuration is required within the VPC instance’s pfSense® webGUI before you are able to manage traffic from the private subnet.

1. Log into the pfSense WebGUI for the instance.
2. Click on the Interfaces heading on the left and then click the Assign link.
3. Click on the + icon to add a new Interface under the Interface assignments tab. A LAN interface should automatically be added with the next available network interface (xn1).
4. Click on the Interfaces heading on the left again and then click on LAN. Click the checkbox to enable the LAN interface. Set the IPv4 Configuration Type to Static IPv4 and enter the IP address you assigned to the 2nd interface during the provisioning phase. Click the Save button.

Now, you can create other instances attached to your private subnet and protect them with the firewall on the pfSense instance.

#### 13.4.1 Common ways to manage private hosts

**Allowing private hosts to connect to the Internet**

To allow private hosts to be able to connect to the Internet, you can allow any traffic from the LAN in your firewall rules, there should be a rule like this in place by default.

Next, set up NAT rules to cause addresses in the private subnet to be NATed to the IP address of the WAN interface:

1. Under the Firewall heading on the left, click on the NAT link.
2. On the Outbound tab click the radio button for Manual Outbound NAT rule generation (AON - Advanced Outbound NAT).
3. Click the Save button.
4. Click on the Aliases link under the Firewall heading on the left.
5. Add your private subnet to the Networks_to_NAT alias.

**Note:** There is an existing NAT rule configured by default that uses the alias Networks_to_NAT.
Allow private hosts to connect to each other

If your hosts should only contact each other and a private network segment elsewhere, you can configure an IPsec or OpenVPN tunnel from your remote networks to the Netgate appliance instance and set up the appropriate firewall rules, routes, and security policies to allow access to your private subnet through a VPN tunnel.

Allow direct inbound access from the internet to hosts

If you wish to enable direct inbound access from the internet to hosts on the private subnet, you can set up port forwarding on the WAN interface to direct traffic to particular hosts in the private subnet.

13.5 Establishing a VPN connection to a VPC in another region

To establish a VPN that allows instances on the VPC subnet(s) that sit behind a Netgate appliance to communicate with instances that reside in a VPC in another region, the Netgate appliance has a VPC configuration wizard that assists by configuring both the Netgate appliance as well as the VPC configuration elements that would normally have to be set manually through the AWS Management Console.

For detailed instructions, see the AWS VPC User Guide.

13.6 Upgrading a VPC Instance

Periodically, new releases of the AMI are issued to track new releases of pfSense® that may provide new functionality, bug fixes, and security updates.

The lower risk approach to upgrading is to bring up a new instance alongside the existing one and executing a cutover. These instructions detail the procedure for moving your existing instance to one running the latest version.

1. Back up the configuration of your existing instance by navigating to Backup/Restore under the Diagnostics menu in the Web GUI. Click the Download configuration button under the Backup Configuration heading and save your config file to your local system.

2. Bring up a new instance of the pfSense Certified Router/Firewall/VPN running the latest version.

3. When creating the instance, make sure the interfaces match the interfaces on the existing instance. Make sure that the new instance is in the same VPC as the existing instance and that it has the same number of interfaces attached and that the interfaces are connected to the same Subnets.

4. Make sure any interfaces on the new instance that will communicate with private Subnets have the Source/Destination check disabled.

5. Allocate a new Elastic IP and associate it to the WAN interface of the new instance to allow yourself management access.

6. Restore the backed up configuration file to the new instance. Navigate to Backup/Restore under the Diagnostics menu in the Web GUI. Under the Restore Configuration heading, click the Choose File button and browse for the configuration file you backed up from the existing instance earlier. Once you have selected that file, click the Restore configuration button. The configuration file will be uploaded and the instance will reboot automatically.

7. If you had packages installed on the old instance, navigate to Packages under the System menu in the pfSense web GUI and install the same packages.
8. If there was any external dependency on the public IP address of the existing instance, you can remove the Elastic IP Address from the upgraded instance and move the Elastic IP Address from the existing instance to the upgraded instance. External dependencies that might cause you to want to do this include things like VPN’s configured to external devices that rely on the existing instance’s Elastic IP address, or access lists on external devices that allow access to traffic from the existing instance’s IP address. There may be other reasons why you would wish to keep the existing address as well (to preserve existing bookmarks to the Web GUI, reduce the need for updates to existing internal documentation, etc). The process for moving the old Elastic IP address to the new instance is as follows:

- Disassociate the Elastic IP address from the new instance. In the EC2 Management Console, click on Elastic IPs under the Network & Security heading. Check the box next to the Elastic IP address assigned to the new instance and click on the Disassociate Address button.

- Disassociate the Elastic IP address from the old instance. The procedure is the same as in the previous step, just repeated for the Elastic IP address of the old instance this time.

- Associate the Elastic IP address that was previously associated to the old instance to public interface of the new instance. In the EC2 Management Console, click on Elastic IPs. Check the box next to the Elastic IP address you are moving and click the Associate Address button. Fill in the correct value for the Instance or Network Interface and select the Private IP Address of the public interface on the new instance. Click the Associate button. The management interface of the new instance should now be accessible.

9. Move any default routes that pointed to an interface on the old instance to point to the equivalent interface on the new instance. In the VPC Management Console, click on Route Tables under the Virtual Private Cloud heading. Check the box next to a Route Table associated with the VPC that the instances is located in.

- In the detail pane that appears at the bottom of the screen, click on the Routes tab.

- If a route exists for 0.0.0.0/0 with a Target that is an interface ID of an interface on the old instance, click the Edit button above the table displaying the routes.

- Click the red X next to the row for 0.0.0.0/0 to remove the existing route.

- There should be a blank row with empty fields for a new route. Enter 0.0.0.0/0 in the Destination field and the Network Interface ID of the interface on the new instance in the Target field. Click on the Save button.

- If there were multiple private subnets in the VPC which were pointed to interfaces on the pfSense instance, repeat this process for the other Route Tables associated with the VPC.

- The new instance should now be functioning as the old one did.
This guide will explain how to use the AWS VPC Wizard to simplify the configuration of a VPN to a remote VPC. The administrator is asked for the minimum amount of basic information required to establish the VPN. The configurations, both on the AWS VPC side and on the pfSense side are then automatically created. When the wizard is finished executing, a functioning VPN connection to a VPC should be established.

### 14.1 AWS Access Keys

In order to connect to the AWS API to make certain required configuration changes, the AWS VPC Wizard requires Access Keys to retrieve and modify VPC configurations.

**See also:**
Find more information about AWS Security Credential, including Access Keys by reading [AWS Security Credentials](#).

Access keys consist of two parts:

1. An access key ID
   - For example, `AKIAIOSFODNN7EXAMPLE`.
2. A secret access key
   - For example, `wJalrXUtnFEMI/K7MDENG/bPxRfipcyEXAMPLEKEY`.

Access keys are like a username/password and needed for programmatic requests to AWS, including the AWS VPC Wizard. Use both the access key ID and secret access key together to authenticate requests.

**Important:** Manage access keys as securely as a user name and password.

#### 14.1.1 Managing Access Keys

To create, modify, or delete IAM user access keys, do the following:

1. Sign in to the [IAM console](#).
2. In the navigation bar on the upper right, choose a user name, and then choose [My Security Credentials](#).
3. On the [AWS IAM Credentials](#) tab, in the [Access keys for CLI, SDK, and API access](#) section, choose [Create access key](#).
4. Choose [Download .csv file](#) to save the access key ID and secret access key to a .csv file on your computer. Store the file in a secure location. There is no access to the secret access key again after this dialog box closes.
After the .csv file has been downloaded, choose Close. When an access key is created, the key pair is active by default, and the pair can be used right away.

- To disable an active access key, choose Make inactive.
- To reenable an inactive access key, choose Make active.
- To delete an access key, choose its X button at the far right of the row. Then choose Delete to confirm.

When an access key is deleted, it’s gone forever and cannot be retrieved. However, new keys can always be created.

To create, modify, or delete another IAM user’s access keys, do the following:

1. Sign in to the IAM console.
2. In the navigation pane, choose Users.
3. Choose the name of the user whose access keys to manage, and then choose the Security credentials tab.
4. In the Access keys section, choose Create access key.
5. Choose Download .csv file to save the access key ID and secret access key to a CSV file on your computer.

### 14.1.2 Rotating Access Keys

As a security best practice, we recommend to regularly rotate (change) IAM user access keys. Rotating access keys can be done from the AWS Management Console.

To rotate access keys for an IAM user without interrupting the applications (console), create a second access key while the first access key is still active:

1. Sign in to the IAM console.
2. In the navigation pane, choose Users.
3. Choose the name of the user whose access keys to manage, and then choose the Security credentials tab.
4. In the Access keys section, choose Create access key.
5. Choose Download .csv file to save the access key ID and secret access key to a CSV file on your computer.
6. The new access key is active by default. At this point, the user has two active access keys.

After waiting some period of time to ensure that all applications and tools have been updated, delete the first access key:

1. Sign in to the IAM console.
2. In the navigation pane, choose Users.
3. Choose the name of the user whose access keys to manage, and then choose the Security credentials tab.
4. Locate the access key to delete and choose its X button at the far right of the row. Then choose Delete to confirm.

### 14.1.3 Determining When Access Keys Need Rotating

To determine when access keys need rotating (console), do the following:

1. Sign in to the IAM console.
2. In the navigation pane, choose Users.
3. If necessary, add the Access key age column to the users table by completing the following steps:
   1. Above the table on the far right, click the settings icon.
2. In Manage columns, select Access key age.

3. Choose Close to return to the list of users.

4. The Access key age column shows the number of days since the oldest active access key was created. Use this information to find users with access keys that need rotating. The column displays None for users with no access key.

14.2 Using the Wizard

1. Gather your AWS Access Key ID and Secret Key.

2. Navigate to VPN > AWS VPC Wizard in the main menu in the pfSense® webGUI.

3. The first screen of the wizard prompts for the AWS Credentials. Enter the Access Key ID and Secret Access Key in the appropriate text fields and select the Region to connect to in the dropdown menu, then click Next.
The wizard will then query the AWS API using those credentials to find which VPC’s exist in the selected region. If the credentials were rejected, an error message will be displayed and return to the first screen.

4. The next screen will prompt to select from the available VPC’s in the selected region. Select the one to connect to from the dropdown menu. The wizard will not create a new VPC; it will only connect to an existing VPC. Click **Next** after selecting the desired VPC.

Note: If the desired VPC’s to connect to isn’t available, create one via the **AWS Management Console** and try...
The wizard will then query the AWS API to check whether there is a VPN Gateway attached to the selected VPC. If none exists, one will be created via the API. Then the next screen will be displayed.

5. On the next screen, specify routing and network data.

A description of what should be entered for each of these fields follows.

**Routing Type**  AWS offers either **static** routing or **BGP** routing. Select the appropriate type from the dropdown menu. If unsure, static routing is likely to be adequate.

**BGP AS Number**  If static routing was chosen, leave this field blank. Otherwise it is possible to specify an AS number to use. If left blank, the value will default to 65000.

**Local Public IP Address**  On an AWS Netgate appliance instance, this should be the public IP address of the Elastic IP associated with the instance. If configuring a hardware device running pfSense, this could be the public address assigned to the WAN (or other) interface of the device.

**Local subnets**  The subnets connected to the pfSense instance that should be routed over the tunnel from hosts in the remote VPC. As an example, if connecting a pfSense instance to a remote VPC in the AWS us-east-1 region, enter the subnets (or a single subnet) that are local to the pfSense instance and when hosts in your VPC in **us-east-1** attempted to reach addresses within those subnets, the traffic will be sent through the VPN tunnel that is being configured.

**Note:**  When selecting static routing as the routing type, there will be a delay that is typically between 2-5 minutes before the next screen is displayed. This is because static routes must be added to the VPN Connection via the AWS API. This operation fails until the VPN Connection reaches the “available” state. This can take a few minutes to occur.

Click **Next** when done.

The wizard will then query the AWS API to find whether a Customer Gateway is configured with the selected Public IP Address. If none exists, one will be created. If one already exists, the ID will be retrieved and it will
be used.

The wizard will then query the AWS API to see if a VPC Connection already exists that matches the data entered. If one exists, it will be used. Otherwise one will be created.

If static routing was selected, static routes will be added to the VPN Connection for the Local subnets entered. Route propagation will be enabled for the VPN Gateway in each of the Route Tables that are associated with the VPC. All of these configurations are carried out in the AWS API, nothing has been changed in the pfSense VPN configurations yet.

**Warning: Important Note on Billing:** Once this step is carried out and the VPN Connection is created, AWS will start billing your AWS account the hourly rate for a VPN Connection. This is $0.05 as of this writing, and that is a charge that goes entirely to AWS itself. They will do this until the VPN Connection is deleted via the VPC Management Console.

Nothing in pfSense will ever cause AWS to stop billing for this VPN Connection. Whether it works or not, whether the pfSense instance is up or down, whether the IPsec tunnels have been deleted or reconfigured, AWS will continue to bill the hourly fee for a VPN Connection if the creation of it succeeds until it is deleted through their web interface.

The wizard helps establish an initial configuration that works and configures the appropriate elements in AWS’s API to facilitate this. You are responsible for making sure you understand what you’re being billed for and disabling any functions, including VPN Connections, that are no longer necessary.

6. If the operations of the previous step succeeded, the next screen will appear.

![VPN Configuration Wizard](image)

Select an **Interface** to act as the local endpoint of the VPN tunnels that will be created. In most cases, this should be the WAN interface. It should generally be whatever interface is associated with the Local Public IP Address entered in the previous step.

On an AWS Netgate pfSense instance, this will be whatever interface the Elastic IP is associated with. On a hardware device running pfSense that has the Local Public IP Address directly configured on an interface, this will be the interface that the Local Public IP Address is configured on.
After clicking **Next**, the wizard will configure the VPN and associated settings within pfSense itself using data returned by the AWS API in the previous step.

It will configure 2 IPsec tunnels, a firewall rule, 2 Aliases (referenced by the firewall rule), and 2 Virtual IP Addresses. If **BGP** was selected as the **Routing Type** in the previous step, it will install the **OpenBGPD** package automatically and configure it appropriately.

7. The next screen will appear and prompt to apply the configuration changes that have been made.

![Apply configuration changes and bring up VPN](image)

After clicking **Next**, all the configuration changes that were made will be applied.

8. The wizard will be completed and the browser will be redirected to the IPsec status page. The VPN to the VPC should now be fully configured.
Note: Sometimes there is a delay of 5-10 minutes before the tunnels are fully functional and passing traffic. This has been observed particularly often during the setup of tunnels using BGP routing.

14.3 Testing Connectivity

Verify that the IPsec tunnels are functioning by attempting to ping the “inside tunnel addresses” of the VPC side of the tunnel by navigating to Firewall -> Virtual IP. There should be two virtual IP addresses configured that have Descriptions like “Inside address for tunnel to <remote IP address>”.

© Copyright 2020 Rubicon Communications LLC
Amazon provides inside addresses for each end of the tunnel in a /30 subnet in IPv4 link local address space (169.254.x.y). Typically, the first usable address in the /30 is the inside address for the VPC end of the tunnel and the other usable address is the inside address for your end of the tunnel. So if you ping from one of the virtual IP addresses configured on the pfSense® instance to the IP address that is one less (for example, if the virtual IP address were 169.254.253.22, ping from 169.254.253.22 to 169.254.253.21), that checks whether the other end of the tunnel is responding and whether the tunnel is functioning properly.

**Note:** It sometimes takes a few minutes for the tunnels to begin working after the configuration wizard completes.

To ping, log into the pfSense instance via SSH and execute `ping` from a shell prompt. For the previous example of 169.254.253.22, the proper syntax is:

```
ping -S 169.254.253.22 169.254.253.21
```

When pinging from a shell prompt, it is possible leave the command running indefinitely and interrupt it there is a response.
It is also possible to ping via the Diagnostics -> Ping page by selecting the appropriate source address and entering the remote tunnel inside address in the Host field. This will only send a limited number of ping packets, so it may be necessary to repeat this a few times.

### 14.4 VPC Configuration Details

The AWS documentation for connecting a hardware device to a VPC provides a great amount of detail on configuring VPN Connections to VPC.

The main configuration elements that exist in Amazon’s data model are the Virtual Private Gateway, the Customer Gateway, and the VPN Connection. In order to configure a VPN connection to a VPC, all 3 of these need to exist. The Virtual Private Gateway is the VPN endpoint on Amazon’s side. The customer gateway is the VPN endpoint on the pfSense® instance/device being configured. The VPN Connection is the IPsec VPN between Amazon and the pfSense instance/device.

A Virtual Private Gateway needs to exist and be associated to the VPC. A particular VPN Gateway can only be associated to one VPC at a time. Once the VPC to connect to has been selected, the wizard invokes the AWS API call DescribeVpnGateways to determine if a VPN Gateway already exists that is attached to the VPC. If none exists, it creates one with the CreateVpnGateway API call and attaches it to the VPC with the AttachVpnGateway call.

A Customer Gateway needs to be created for the public IP address of the device or virtual machine that will be used to connect to the VPC. The wizard invokes the AWS API call DescribeCustomerGateways to determine if a Customer Gateway already exists. If none exists, one is created with the CreateCustomerGateway API call.

The VPN Connection connects the Virtual Private Gateway and Customer Gateway. The wizard checks to see if there is an existing VPN Connection configured that connects those endpoints by invoking the AWS API call DescribeVpnConnections. If none exists, one is created using the CreateVpnConnection call. One of the fields returned by this call is a block of XML configuration data that contains configuration data assigned by AWS for use with configuring the VPN Connection. This data is stored and used in subsequent steps to make the required configuration changes within pfSense.
Any objects created through API calls by the wizard will be tagged with names like auto-created by pfSense VPC <your_VPC_ID>. This is accomplished by calling the AWS API call CreateTags and using Name as the key for the tag.

In addition to creation of the items mentioned above, required adjustments are made to Security Groups and Route Tables to facilitate communication over the VPN. The Security Groups associated with the VPC are updated to allow inbound access from the local subnets on the pfSense end of the VPN. They are checked first via the DescribeSecurityGroups AWS API call to determine if the access is already allowed. Any of the subnets that is not already allowed has inbound access added via the AuthorizeSecurityGroupIngress AWS API call.

Route Tables associated with the VPC are updated to receive routes from the VPN Gateway used by the VPN Connection. They are checked first via the DescribeRouteTables AWS API call. If the VPN Gateway ID is not included in the list of VPN Gateways propagating routes, route propagation for the VPN Gateway is enabled on that table using the EnableVgwRoutePropagation AWS API call.

For VPN Connections using static routing, static routes for the specified subnets are added to the VPN Connection. This is done via the CreateVpnConnectionRoute AWS API call.

### 14.5 pfSense Configuration Details

On the pfSense® side, there are numerous configurations added to support the VPN to the VPC.

#### 14.5.1 Aliases

First, aliases are created for use in a firewall rule. These aliases are intended to contain the subnets that traffic should be allowed to ingress over the IPsec tunnel. One alias represents the local subnets on the pfSense side and is given a name like VPC_Local_vpc_12345678 and the other represents the remote subnets on the VPC side and is given a name like VPC_Remote_vpc_12345678.

#### 14.5.2 Virtual IP addresses

Next, virtual IP addresses are added on the lo0 (loopback) interface. These virtual IP addresses are the local “inside addresses” of the IPsec tunnels. These addresses are used as the local address for BGP communication when BGP routing is selected. These addresses are IPv4 link local addresses (see RFC 3297). AWS assigns /30’s out of the network 169.254.0.0/16 for this purpose.

**Note:** These addresses are also useful as a ping target to execute a basic test of whether the tunnel is functioning properly. Executing a ping from a source address of one of these IP addresses to the corresponding inside address of the other end of the tunnel helps determine whether the tunnel negotiation is completing properly.

#### 14.5.3 Firewall rules

Next, a firewall rule is added on the IPsec interface that allows traffic from the VPC networks to the local subnets. This rule uses the previously created Aliases as source/destination targets.
14.5.4 IPsec

Then, IPsec phase 1 and phase 2 associations are set up. Most of the settings required are extracted from a block of XML data that was returned by the CreateVpnConnection call made during the AWS configuration step. This includes parameters like endpoint IP addresses, encryption ciphers, timer values, etc.

If BGP routing was selected, the configurations for the OpenBGPD BGP daemon are established. The required settings are determined using the AS number entered into the wizard and the parameters returned by the CreateVpnConnection call made during the AWS configuration step.

14.6 Tested Configurations

Various topologies may be possible to establish using the AWS VPC Configuration Wizard. This section enumerates some of the configurations that were successfully tested.

14.6.1 Platforms

- Various hardware platforms.
- 64-bit virtual machines in VMware vSphere/ESX.
- Amazon EC2 instances (Xen virtual machines) of the Netgate pfSense® Router/Firewall/VPN AWS AMI.

14.6.2 Local network/routing configurations

- pfSense with a public address configured on the WAN interface.
- pfSense with a private address configured on the WAN interface behind a 1:1 NAT.
- pfSense with a private address configured on the WAN interface behind a PAT (1:many NAT).

14.6.3 VPC Topologies

- pfSense connected to a single VPC.
- pfSense connected to multiple VPC’s in different regions.
- Amazon EC2 instance of the pfSense Router/Firewall/VPN AWS AMI connected to a VPC belonging to the same AWS account in a different region.
- Amazon EC2 instance of the pfSense Router/Firewall/VPN AWS AMI connected to a VPC belonging to a different AWS account in the same region.

The configuration recommended for the greatest amount of stability is to have a public IPv4 address directly configured on the WAN interface of your pfSense firewall, but VPNs have been successfully established under all of the conditions listed above.

Whether any of these solutions is appropriate should be evaluated in the context of personal needs and existing infrastructure. Other configurations not listed above may be possible as well.
14.7 AWS VPC Wizard FAQ

Contents

• AWS VPC Wizard FAQ
  – 1. What level of redundancy is provided by the two tunnels?
  – 2. I quit the wizard before finishing. Now what?
  – 3. What are the AWS charges for this?
  – 4. Can I use the wizard to connect to the GovCloud region?

14.7.1 1. What level of redundancy is provided by the two tunnels?

Amazon provides two tunnel endpoints that will allow traffic to be sent between your networks and the remote VPC you are connected to. The racoon daemon in pfSense® is only capable of establishing an active phase 2 association for a particular source/destination pair on a single tunnel.

Phase 2 associations between the local subnets and the remote VPC subnet are configured in the pfSense GUI for both tunnels, but racoon will only actually establish an association for the first tunnel. This means that racoon will only ever try to send traffic destined for the remote VPC subnet over the first tunnel.

If that tunnel goes down, the second tunnel may be up and inbound traffic from the remote VPC may be sent to your local networks over that tunnel automatically. But outbound traffic to your remote VPC would not automatically fail over to the second tunnel. In order for you to send your outbound traffic over the second tunnel, you would need to disable the phase 2 associations for the first tunnel and apply the changes.

14.7.2 2. I quit the wizard before finishing. Now what?

To finish setting up the VPN, go back to the wizard and run through it again. It should reuse any partial configurations that were generated before it was stopped and create the new elements that are required.

14.7.3 3. What are the AWS charges for this?

AWS determines their own pricing and provides details for EC2 pricing and VPC pricing. There are many types of charges that may be incurred for operating instances on AWS (e.g. charges related to running an instance, bandwidth, storage, elastic IPs, etc).

The charge of specific interest in this case is the hourly charge for a VPN Connection. As of this writing, it costs $0.05 (USD) per hour in most regions to have a VPN Connection configured and available. AWS will charge whether the VPN Connection is being used or not as long as it is configured. This will be configured by the third step of the wizard and will never be removed by pfSense.

If the VPN Connection is no longer needed and billing for it needs to be stopped, visit AWS’s VPC Management Console and delete the VPN Connection manually.

14.7.4 4. Can I use the wizard to connect to the GovCloud region?

This hasn’t been officially tested, but at least one user has reported that they were able to successfully connect to the GovCloud region. They manually added the region `us-gov-west-1` to the list of regions in the first step of the wizard.
and were able to successfully connect to their VPC in that region. This may be supported in a future build, but to try without official support, do the following:

1. Under the System > Advanced menu, make sure the Enable Secure Shell box is checked. This is already done by default on AWS instances, but is off by default on pfSense hardware devices.

2. Log into the instance via SSH.

3. Make sure the root filesystem is mounted as read/write. On an AWS instance or a hardware device running on an SSD, this should be true. On a hardware device using Compact Flash or an SD card for storage, it will probably be necessary to remount the root filesystem in read/write mode by running:

   ```
   mount -uw /
   ```

4. Edit the file `/usr/local/www/wizards/vpc_vpn_wizard.xml` using vi. Look for a section of the file that looks like this:

   ```xml
   <option>
       <name>sa-east-1</name>
       <value>sa-east-1</value>
   </option>
   ```

   That should appear directly after several similar `<option>` specifications containing all of the other available regions. Right underneath that section, add the following:

   ```xml
   <option>
       <name>us-gov-west-1</name>
       <value>us-gov-west-1</value>
   </option>
   ```

   Then save the file and exit vi.

5. If the filesystem had to be remounted in read/write mode earlier, remount it in read-only mode by running:

   ```
   mount -u /
   ```

   The GovCloud region should now appear as a choice in the first step of the wizard.

References
CHAPTER FIFTEEN

SUPPORT RESOURCES

15.1 Commercial Support

In order to keep prices low, the software is not bundled with a support subscription. For users who need commercial support, Netgate Global Support can be purchased at https://www.netgate.com/support.

15.2 Community Support

Community support for pfSense® software is available through the Netgate Forum.
16.1 Netgate Training

Netgate training offers training courses for increasing your knowledge of pfSense® products and services. Whether you need to maintain or improve the security skills of your staff or offer highly specialized support and improve your customer satisfaction; Netgate training has got you covered.

https://www.netgate.com/training

16.2 Resource Library

To learn more about how to use your pfSense appliance and for other helpful resources, make sure to browse our Resource Library.

https://www.netgate.com/resources

16.3 Professional Services

Support does not cover more complex tasks such as CARP configuration for redundancy on multiple firewalls or circuits, network design, and conversion from other firewalls to pfSense®. These items are offered as professional services and can be purchased and scheduled accordingly.

https://www.netgate.com/our-services/professional-services.html

16.4 Community Options

If you elected not to get a paid support plan, you can find help from the active and knowledgeable pfSense community on our forums.

https://forum.netgate.com/