



# Transit VPC on AWS with the VM-Series-Step by Step Guide

This document provides a step by step guide to manually build a Transit VPC on AWS with 3 subscribing VPC's protected by the VM-Series (deployed in the transit hub). The Transit VPC allows you to deploy services such as outbound internet access through a hub and spoke architecture where the hub (Transit VPC) houses common services such as security and spokes house the workloads. We will build the Transit VPC with 2 Availability Zones and a firewall in each Availability Zone for HA. We will use the Virtual Gateway (VGW) in each subscribing VPC to provide redundant tunnels to each firewall in the Transit VPC. If you choose, you can deploy the subscribing VPC in multiple AWS Availability Zones to include redundancy. This document will also utilize eBGP as a dynamic routing protocol to provide routes to subscribing VPC's.

NOTE: This guide takes a manual, step by step approach to building the Transit VPC. A more automate approach can be found in this guide

<https://github.com/PaloAltoNetworks/aws-transit-vpc>

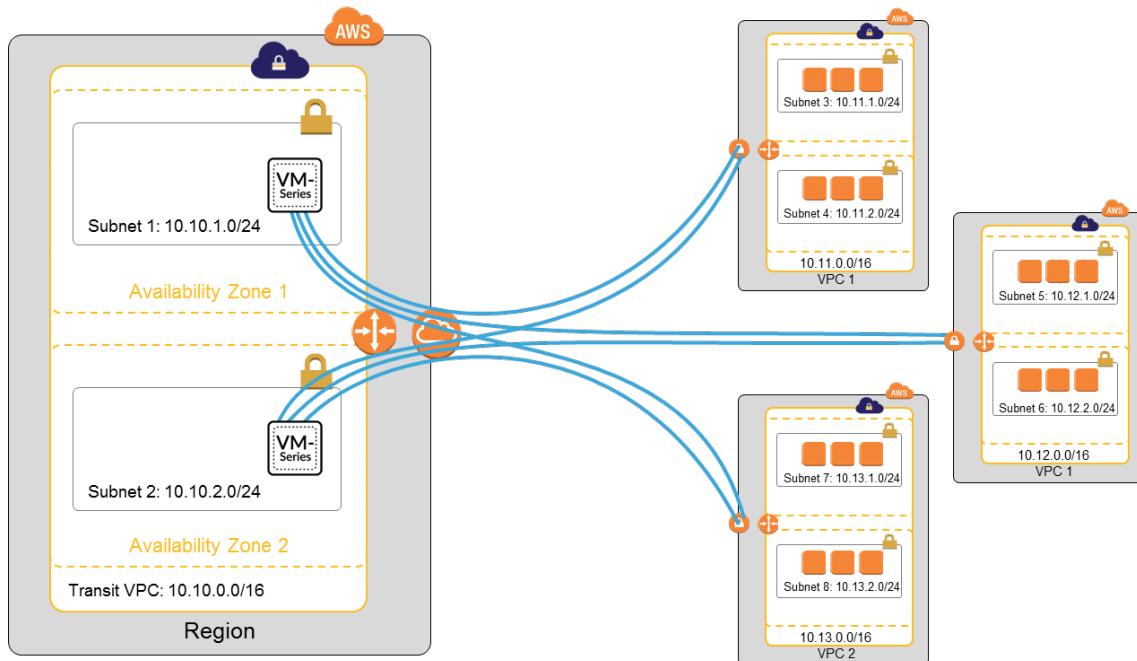
## Overview of the steps to create a Transit VPC:

1. Create a Transit VPC acting as the hub with multiple Availability Zones and AWS IGW
2. Create (3) Subscriber VPC's with a VGW for VPN peering
3. Create VPN tunnels from Subscriber VPC VGW's to Palo Alto Networks VM-Series firewalls located in the hub
4. Configure BGP on VM-Series firewall's

Note: This document will assume that you have the following:

- AWS account
- Proper permissions to create VPC's, route tables, subnets, etc.
- Created a Key pair for the AWS region where you will be building this solution.
- Permissions to deploy EC2 instances from the AWS marketplace.

Overview of the architecture that will be built:



## 1. Create Transit VPC with multiple Availability Zones and IGW

In the AWS console, create the new Transit VPC from the VPC dashboard as depicted below:

**Create VPC**

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an Amazon-provided IPv6 CIDR block with the VPC.

Name tag  i

IPv4 CIDR block\*  i

IPv6 CIDR block\*  No IPv6 CIDR Block i  
 Amazon provided IPv6 CIDR block

Tenancy

Cancel Yes, Create

Next we will create the Subnets and Availability Zone associations:

From the VPC dashboard click on the Subnets menu and configure your subnets as below:

[Subnets](#) > Create subnet

## Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask,

Name tag	TransVPCaz1	i
VPC*	vpc-de3fffa4	i
VPC CIDRs	CIDR	Status
	10.10.0.0/16	associated
Availability Zone	us-east-1a	i
IPv4 CIDR block*	10.10.1.0/24	i

\* Required

Next, create a second subnet:

[Subnets](#) > Create subnet

## Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same as the first subnet.

Name tag	TransVPCaz2	i
VPC*	vpc-de3fffa4	i
VPC CIDRs	CIDR	Status
	10.10.0.0/16	associated
Availability Zone	us-east-1b	i
IPv4 CIDR block*	10.10.2.0/24	i

\* Required

We will now deploy an AWS Internet Gateway (IGW) from the VPC dash board.  
From the VPC dashboard click on the Internet Gateways menu:



## Create internet gateway

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway, enter a name tag and attach it to a VPC.

Name tag  ⓘ

\* Required

Attach the IGW. Click on the **attach to VPC** button and from the Actions drop down in the window select your Transit VPC and select Attach.



## Attach to VPC

Attach an internet gateway to a VPC to enable communication with the internet. Specify the VPC you would like to attach below.

VPC\*  ⓘ

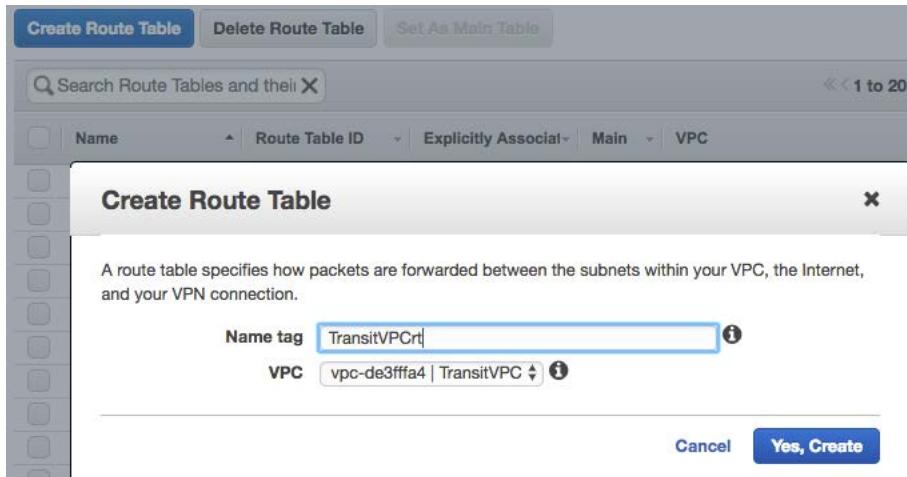
▶ AWS Command Line Interface command

\* Required

Your Internet Gateway screen should look like the screen below:

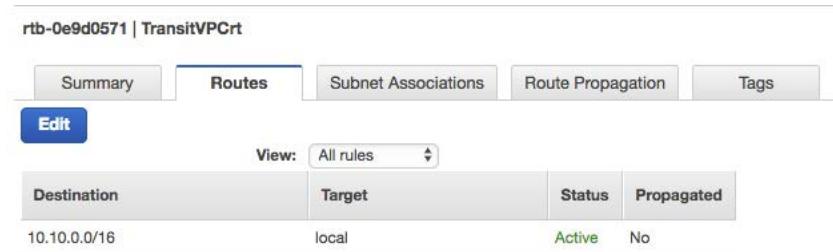


Next, we will create a route table for the Transit VPC: from the VPC dashboard select Route Tables menu and create Route table as below:

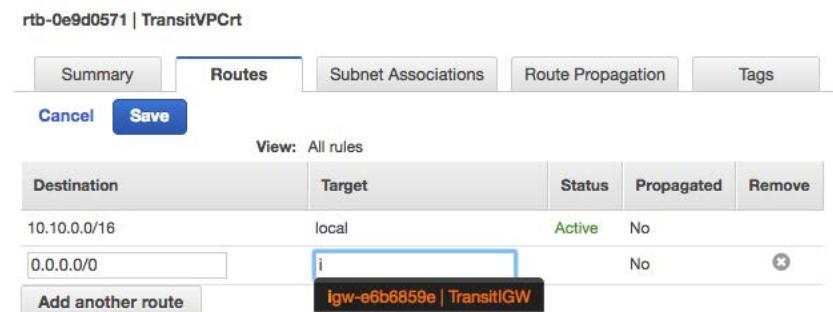


The route table must be associated with your Transit VPC as highlighted above. Once you provide a name and select the Transit VPC from the drop-down menu, select the yes, create button.

Next step creates routes for the new Transit VPC route table. Click in the empty check box next to your new route table and click on the edit button in the bottom window:



From the edit screen click the add another route button to create a default route to the IGW. Make sure you click the save button when you are done:



Your route table should like the image below:

rtb-0e9d0571   TransitVPCrt				
Summary	Routes	Subnet Associations	Route Propagation	Tags
<b>Edit</b>				
Destination	Target	Status	Propagated	
10.10.0.0/16	local	Active	No	
0.0.0.0/0	igw-e6b6859e	Active	No	

Next, from the same window, select the subnet associations tab and select the edit button:

rtb-0e9d0571   TransitVPCrt			
Summary	Routes	Subnet Associations	
<b>Edit</b>			
Subnet	IPv4 CIDR	IPv6 CIDR	
You do not have any subnet associations.			
The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:			
Subnet	IPv4 CIDR	IPv6 CIDR	
subnet-5add9c10   TransVPCaz1	10.10.1.0/24	-	
subnet-b948fae5   TransVPCaz2	10.10.2.0/24	-	

From the edit screen, select the empty check boxes to the left of the subnets you created earlier. Once complete select the save button:

rtb-0e9d0571   TransitVPCrt				
Summary	Routes	Subnet Associations	Route Propagation	Tags
<b>Cancel</b>	<b>Save</b>			
Associate	Subnet	IPv4 CIDR	IPv6 CIDR	Current Route Table
<input checked="" type="checkbox"/>	subnet-5add9c10   TransVPCaz1	10.10.1.0/24	-	Main
<input checked="" type="checkbox"/>	subnet-b948fae5   TransVPCaz2	10.10.2.0/24	-	Main

Next you are going to deploy a VM-Series firewall into each of the Availability Zones:

From the EC2 Dashboard, select the Launch Instance button.

From the Left-Hand Menu, select AWS Market Place and search for Palo Alto Networks.

Select VM-Series Next-Generation Firewall Bundle 1 from the list.

Bundle 2 will provide the highest levels of security. We are selecting Bundle 1 here to easy to cost in a demo environment.

1. Choose AMI    2. Choose Instance Type    3. Configure Instance    4. Add Storage    5. Add Tags    6. Configure Security Group    7. Review

### Step 1: Choose an Amazon Machine Image (AMI)

[Cancel and Exit](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

The screenshot shows the AWS Lambda Step Functions console. At the top, there's a navigation bar with tabs: 'Lambda', 'Step Functions', 'CloudWatch Metrics', and 'CloudWatch Logs'. Below the navigation bar, the title 'TransitVPC' is displayed, along with the status 'Running' and the ARN 'arn:aws:lambda:us-east-1:123456789012:function:TransitVPC'. The main area shows a timeline of steps:

- Step 1: 'Start' at 2018-07-10T14:45:20Z, with a duration of 00:00:00.000. It's associated with the function 'TransitVPC' and the region 'us-east-1'.
- Step 2: 'Invoke' at 2018-07-10T14:45:20Z, with a duration of 00:00:00.000. It's associated with the function 'TransitVPC' and the region 'us-east-1'.
- Step 3: 'End' at 2018-07-10T14:45:20Z, with a duration of 00:00:00.000. It's associated with the function 'TransitVPC' and the region 'us-east-1'.

At the bottom right, there are buttons for 'Edit' and 'Delete'.

Select Continue for the Pricing Details.

### VM-Series Next-Generation Firewall Bundle 1

 <p><b>VM-Series Next-Generation Firewall Bundle 1</b></p> <p>The VM-Series next-generation firewall is an AWS Network Competency and Security Competency approved solution that can be fully integrated into your AWS deployment workflow. Developers and cloud security architects can use native AWS automation features and workload tags combined with a VM-Series bootstrapped configuration stored in an AWS S3 ...</p> <p><a href="#">More info</a></p> <p><a href="#">View Additional Details in AWS Marketplace</a></p>	<p><b>Pricing Details</b></p> <p>Your Free Trial expired on 09/10/2017 - 12:03 PM UTC-4.</p> <p><b>Hourly Fees</b></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Instance Type</th> <th>Software</th> <th>EC2</th> <th>Total</th> </tr> </thead> <tbody> <tr><td>M3 Extra Large</td><td>\$0.86</td><td>\$0.266</td><td><b>\$1.126/hr</b></td></tr> <tr><td>M4 Extra Large</td><td>\$0.86</td><td>\$0.20</td><td><b>\$1.06/hr</b></td></tr> <tr><td>C3 Quadruple Extra Large</td><td>\$0.86</td><td>\$0.84</td><td><b>\$1.70/hr</b></td></tr> <tr><td>C4 Double Extra Large</td><td>\$0.86</td><td>\$0.398</td><td><b>\$1.258/hr</b></td></tr> <tr><td>C4 Eight Extra Large</td><td>\$0.86</td><td>\$1.591</td><td><b>\$2.451/hr</b></td></tr> <tr><td>M4 Quadruple Extra Large</td><td>\$0.86</td><td>\$0.80</td><td><b>\$1.66/hr</b></td></tr> <tr><td>C4 Quadruple Extra Large</td><td>\$0.86</td><td>\$0.796</td><td><b>\$1.656/hr</b></td></tr> <tr><td>M4 Double Extra Large</td><td>\$0.86</td><td>\$0.40</td><td><b>\$1.26/hr</b></td></tr> <tr><td>M3 Double Extra Large</td><td>\$0.86</td><td>\$0.532</td><td><b>\$1.392/hr</b></td></tr> <tr><td>C3 Double Extra Large</td><td>\$0.86</td><td>\$0.42</td><td><b>\$1.28/hr</b></td></tr> <tr><td>C3 Eight Extra Large</td><td>\$0.86</td><td>\$1.68</td><td><b>\$2.54/hr</b></td></tr> </tbody> </table> <p><b>EBS General Purpose (SSD) volumes</b> \$0.10 per GB-month of provisioned storage</p> <p>You will not be charged until you launch this instance.</p>	Instance Type	Software	EC2	Total	M3 Extra Large	\$0.86	\$0.266	<b>\$1.126/hr</b>	M4 Extra Large	\$0.86	\$0.20	<b>\$1.06/hr</b>	C3 Quadruple Extra Large	\$0.86	\$0.84	<b>\$1.70/hr</b>	C4 Double Extra Large	\$0.86	\$0.398	<b>\$1.258/hr</b>	C4 Eight Extra Large	\$0.86	\$1.591	<b>\$2.451/hr</b>	M4 Quadruple Extra Large	\$0.86	\$0.80	<b>\$1.66/hr</b>	C4 Quadruple Extra Large	\$0.86	\$0.796	<b>\$1.656/hr</b>	M4 Double Extra Large	\$0.86	\$0.40	<b>\$1.26/hr</b>	M3 Double Extra Large	\$0.86	\$0.532	<b>\$1.392/hr</b>	C3 Double Extra Large	\$0.86	\$0.42	<b>\$1.28/hr</b>	C3 Eight Extra Large	\$0.86	\$1.68	<b>\$2.54/hr</b>
Instance Type	Software	EC2	Total																																														
M3 Extra Large	\$0.86	\$0.266	<b>\$1.126/hr</b>																																														
M4 Extra Large	\$0.86	\$0.20	<b>\$1.06/hr</b>																																														
C3 Quadruple Extra Large	\$0.86	\$0.84	<b>\$1.70/hr</b>																																														
C4 Double Extra Large	\$0.86	\$0.398	<b>\$1.258/hr</b>																																														
C4 Eight Extra Large	\$0.86	\$1.591	<b>\$2.451/hr</b>																																														
M4 Quadruple Extra Large	\$0.86	\$0.80	<b>\$1.66/hr</b>																																														
C4 Quadruple Extra Large	\$0.86	\$0.796	<b>\$1.656/hr</b>																																														
M4 Double Extra Large	\$0.86	\$0.40	<b>\$1.26/hr</b>																																														
M3 Double Extra Large	\$0.86	\$0.532	<b>\$1.392/hr</b>																																														
C3 Double Extra Large	\$0.86	\$0.42	<b>\$1.28/hr</b>																																														
C3 Eight Extra Large	\$0.86	\$1.68	<b>\$2.54/hr</b>																																														

[Cancel](#) [Continue](#)

Select the Smallest available Instance type. For this guide, we chose m4.xlarge, select Next: Configure Instance Details.

[1. Choose AMI](#)
**2. Choose Instance Type**
[3. Configure Instance](#)
[4. Add Storage](#)
[5. Add Tags](#)
[6. Configure Security Group](#)
[7. Review](#)

**Step 2: Choose an Instance Type**

#	General purpose	m5.24xlarge	96	384	EBS only	Yes	25 Gigabit	Yes
1	General purpose	m4.large	2	8	EBS only	Yes	Moderate	Yes
2	General purpose	<b>m4.xlarge</b>	4	16	EBS only	Yes	High	Yes
3	General purpose	m4.2xlarge	8	32	EBS only	Yes	High	Yes
4	General purpose	m4.4xlarge	16	64	EBS only	Yes	High	Yes

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Instance Details](#)

Configure the instance deployment for the Availability Zones in your Transit VPC. We will start with AZ-1A. Note that you will need to repeat these steps to deploy a firewall instance into AZ-1B. Once you have verified your settings, select Next: Add Storage:

Step 3: Configure Instance Details

No default VPC found. Select another VPC, or [create a new default VPC](#).

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances	<input type="text" value="1"/>	<a href="#">Launch into Auto Scaling Group</a>												
Purchasing option	<input type="checkbox"/> Request Spot instances													
Network	vpc-de3fffa4   TransitVPC No default VPC found. <a href="#">Create a new default VPC</a> .													
Subnet	subnet-5add9c10   TransVPCaz1   us-east-1a	<a href="#">Create new subnet</a> 251 IP Addresses available												
Auto-assign Public IP	<input checked="" type="checkbox"/> Enable													
Placement group	<input type="checkbox"/> Add instance to placement group.													
IAM role	None <a href="#">Create new IAM role</a>													
Shutdown behavior	Stop													
Enable termination protection	<input type="checkbox"/> Protect against accidental termination													
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring <small>Additional charges apply.</small>													
EBS-optimized instance	<input checked="" type="checkbox"/> Launch as EBS-optimized instance													
Tenancy	Shared - Run a shared hardware instance <small>Additional charges will apply for dedicated tenancy.</small>													
<b>▼ Network interfaces</b> <table border="1"> <thead> <tr> <th>Device</th> <th>Network Interface</th> <th>Subnet</th> <th>Primary IP</th> <th>Secondary IP addresses</th> <th>IPv6 IPs</th> </tr> </thead> <tbody> <tr> <td>eth0</td> <td><a href="#">New network interface</a></td> <td>subnet-5add9c10</td> <td>Auto-assign</td> <td><a href="#">Add IP</a></td> <td><a href="#">Add IP</a></td> </tr> </tbody> </table>			Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs	eth0	<a href="#">New network interface</a>	subnet-5add9c10	Auto-assign	<a href="#">Add IP</a>	<a href="#">Add IP</a>
Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs									
eth0	<a href="#">New network interface</a>	subnet-5add9c10	Auto-assign	<a href="#">Add IP</a>	<a href="#">Add IP</a>									
<a href="#">Cancel</a> <a href="#">Previous</a> <a href="#" style="background-color: #0070C0; color: white; border-radius: 5px; padding: 2px 10px;">Review and Launch</a> <a href="#">Next: Add Storage</a>														

Keep the storage defaults and click on the Next: Add Tags button at the bottom of the page:

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/xvda	snap-0f4e4aed67a07840b	60	General Purpose SSD (GP2)	180 / 3000	N/A	<input type="checkbox"/>	Not Encrypted

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Cancel Previous Review and Launch Next: Add Tags

You can add tags if you would like to identify your instance or you can skip this step and move on to Nets: Security group configuration:

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

This resource currently has no tags

Choose the Add tag button or [click to add a Name tag](#).  
Make sure your [IAM policy](#) includes permissions to create tags.

Add Tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group

Create a new Security Group that you can name for the Transit VPC. For the firewall, we need to make sure that the Security Group allows SSH and HTTPS access as shown below. Once the Security Group is configured, select the review and Launch button.

**Important** It is recommended to set the Source of the Security Group to be specific to your location. When clicking the Custom drop-down, AWS will resolve your External IP and designate it as a /32.

1. Choose AMI   2. Choose Instance Type   3. Configure Instance   4. Add Storage   5. Add Tags   6. Configure Security Group   7. Review

### Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group:  Create a new security group  
 Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom <input type="button" value="0.0.0.0/0"/>	e.g. SSH for Admin Desktop <input type="button" value="X"/>
HTTPS	TCP	443	Custom <input type="button" value="0.0.0.0/0"/>	e.g. SSH for Admin Desktop <input type="button" value="X"/>

[Add Rule](#)

**⚠ Warning**  
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

[Cancel](#) [Previous](#) [Review and Launch](#)

Review the settings and select the Launch button:

1. Choose AMI   2. Choose Instance Type   3. Configure Instance   4. Add Storage   5. Add Tags   6. Configure Security Group   7. Review

### Step 7: Review Instance Launch

Hourly Software Fees: \$0.86 per hour on m4.xlarge instance (Additional taxes may apply.)  
 Software charges will begin once you launch this AMI and continue until you terminate the instance.

Annual Subscriptions are available for this product, which can save you up to 60% when compared to hourly prices.  
 To purchase an Annual Subscription go to the [Your Software](#) page after launching the instance.

By launching this product, you will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's [End User License Agreement](#).

**Instance Type** [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
m4.xlarge	13	4	16	EBS only	Yes	High

**Security Groups** [Edit security groups](#)

Security group name:   
 Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/0	
HTTPS	TCP	443	0.0.0.0/0	

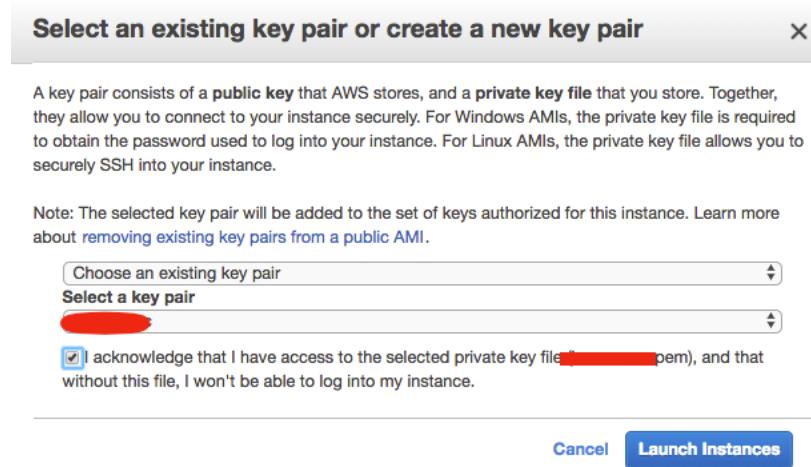
**Instance Details** [Edit instance details](#)

**Storage** [Edit storage](#)

**Tags** [Edit tags](#)

[Cancel](#) [Previous](#) [Launch](#)

Before the instance will launch, you will have to select a Keypair to associate to the instance for access and select the acknowledge box:



You will need to repeat the steps for deploying a firewall instance for the second Availability Zone. If you chose AZ-1a in the above section, you will need to repeat the steps in AZ-1b.

1. Choose AMI   2. Choose Instance Type   3. Configure Instance   4. Add Storage   5. Add Tags   6. Configure Security Group   7. Review

### Step 3: Configure Instance Details

No default VPC found. Select another VPC, or [create a new default VPC](#).

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances	<input type="text" value="1"/>	<a href="#">Launch into Auto Scaling Group</a>
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	<input type="checkbox"/> vpc-de3fffa4   TransitVPC No default VPC found. <a href="#">Create a new default VPC</a> .	
Subnet	<input type="checkbox"/> subnet-b948fae5   TransVPCaz2   us-east-1b 251 IP Addresses available	
Auto-assign Public IP	<input type="checkbox"/> Enable	
Placement group	<input type="checkbox"/> Add instance to placement group.	
IAM role	<input type="checkbox"/> None	
Shutdown behavior	<input type="checkbox"/> Stop	
Enable termination protection	<input type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring <small>Additional charges apply.</small>	
EBS-optimized instance	<input checked="" type="checkbox"/> Launch as EBS-optimized instance	
Tenancy	<input type="checkbox"/> Shared - Run a shared hardware instance	

[▼ Network interfaces](#)

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-b948fae5	Auto-assign	Add IP	Add IP

[Add Device](#)

For the second instance, you can use the same Security Group that was created in the deployment of the first firewall instance:

**Important – If using a new Security Group, ensure to use a more specific Source as recommended above.**

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group:

- Create a new security group
- Select an existing security group

Security Group ID	Name	Description	Actions
sg-548aed1e	default	default VPC security group	<a href="#">Copy to new</a>
sg-d13b5d9b	Transit VPC Security Group FW MGMT	Transit VPC Security Group FW MGMT	<a href="#">Copy to new</a>

Inbound rules for sg-d13b5d9b (Selected security groups: sg-d13b5d9b)

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/0	
HTTPS	TCP	443	0.0.0.0/0	

Cancel Previous Review and Launch

Once the firewalls are deployed and from the EC2 Dashboard click on the instance option from the ec2 dashboard. You will see a list of all instances in your environment. Once the new firewall instance shows a status like below, you will need to SSH into the firewall to setup a username and password to enable the Web Interface:



From the instance you can scroll to the right to find the public IP address. Once you have the public IP address, open an SSH client to access your device. You will need to use the keypair .pem file used to deploy the firewalls to access the new firewall. My public IP address is blocked out. You will need to provide your public IP address for the firewall in the command:

```
~/ssh$ ssh -i yourpemfile.pem admin@awseipofEth1
```

```
~/ssh$ ssh -i yourpemfile.pem admin@awseipofEth1
The authenticity of host [REDACTED] can't be established.
RSA key fingerprint is SHA256:[REDACTED].
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added [REDACTED] (RSA) to the list of known hosts.
Welcome admin.
[admin@PA-VM>
[admin@PA-VM>
[admin@PA-VM>
[admin@PA-VM>
[admin@PA-VM>
```

**NOTE** If you are using MAC/Linux as receive a Public Key denied error, change the permission of you PEM file to proper restrict it.  
chmod 600 yourpemfile.pem

Once you gain access to the firewall, you will need to issue the following commands:

### Configure

```
set mgt-config users admin password
```

This will allow you to set an admin password after you type the password and confirm the password:

Once you have created the password, you must commit the configuration changes.

```
[admin@PA-VM> config
Unknown command: config
[admin@PA-VM> configure
Entering configuration mode
[edit]
[admin@PA-VM# set mgt-config users admin password
[Enter password :
[Confirm password :

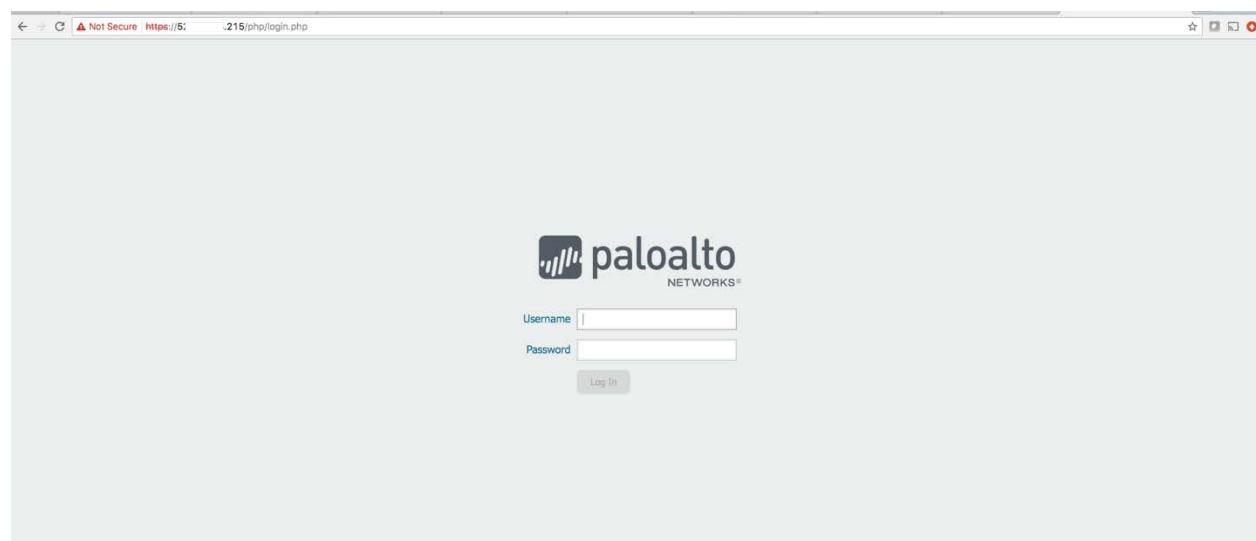
[edit]
[admin@PA-VM# commit

Commit job 2 is in progress. Use Ctrl+C to return to command prompt
...55%99%,.....100%
Configuration committed successfully

[edit]
[admin@PA-VM# ]
```

You will need to complete the SSH steps for both firewalls to access the firewalls from a web browser.

You should now be able to access your firewalls via web browser using https. The username should be admin and the password will be the password you set via the SSH commands:



If you chose to use the VM-Series BYOL AWS Marketplace AMI, you will need to license each of the VM-Series firewalls. If you are not familiar with this process, the following link can be used to help license the firewalls:

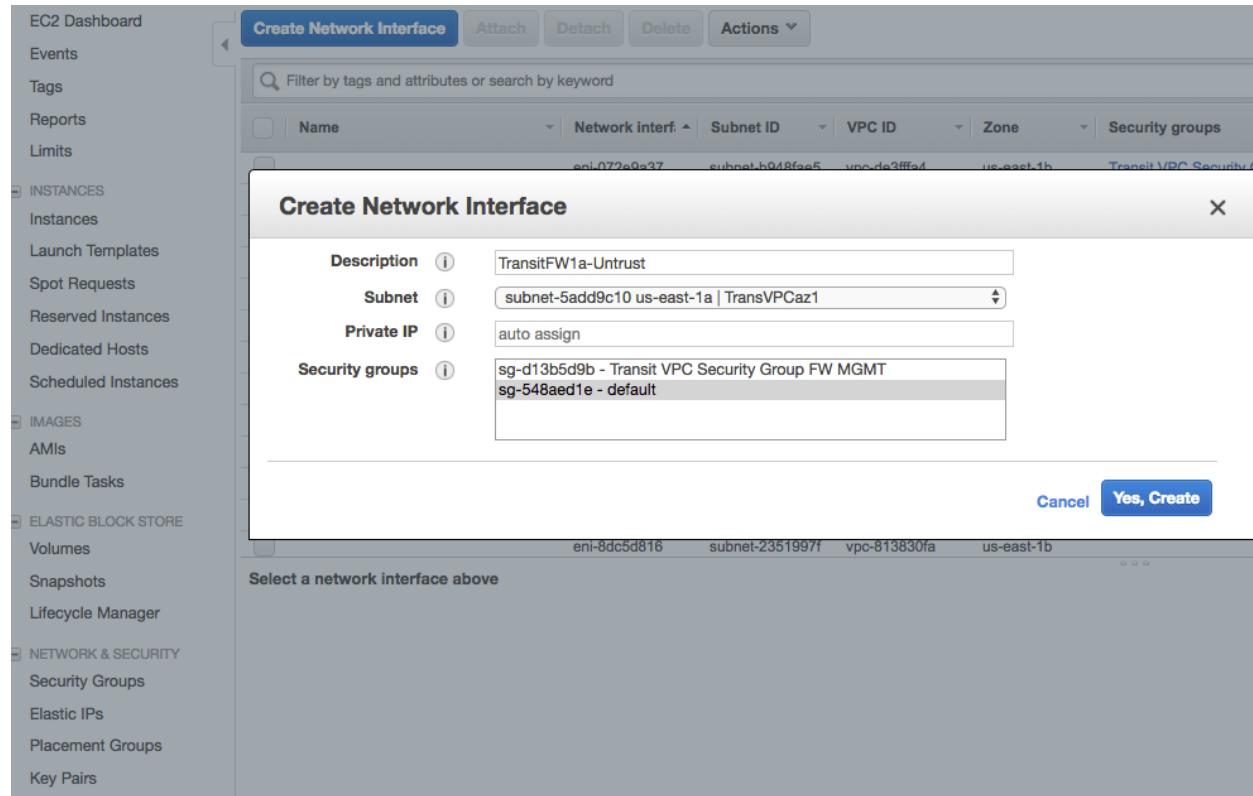
<https://www.paloaltonetworks.com/documentation/81/virtualization/virtualization/license-the-vm-series-firewall/activate-the-license/activate-the-license-for-the-vm-series-firewall-standalone-version>

If you selected either of the AWS Marketplace Bundles, you can ignore this step.

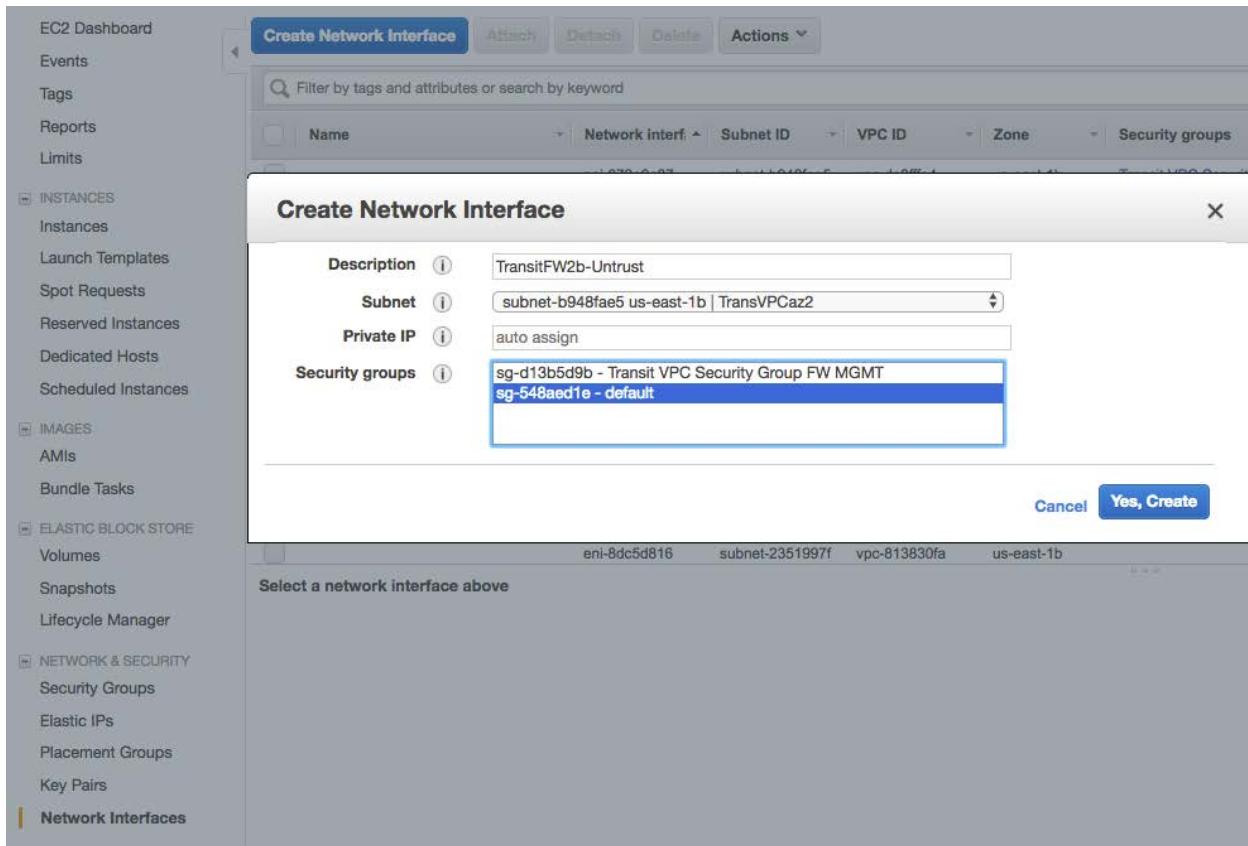
Create the Untrust interface for the new firewalls:

In the deployment of the VM-Series firewall, the management interface was configured. We will now add an Untrust interface to the firewall. From the AWS console, go to the EC2 dashboard. From the EC2 dashboard select the Network Interfaces option from the left panel.

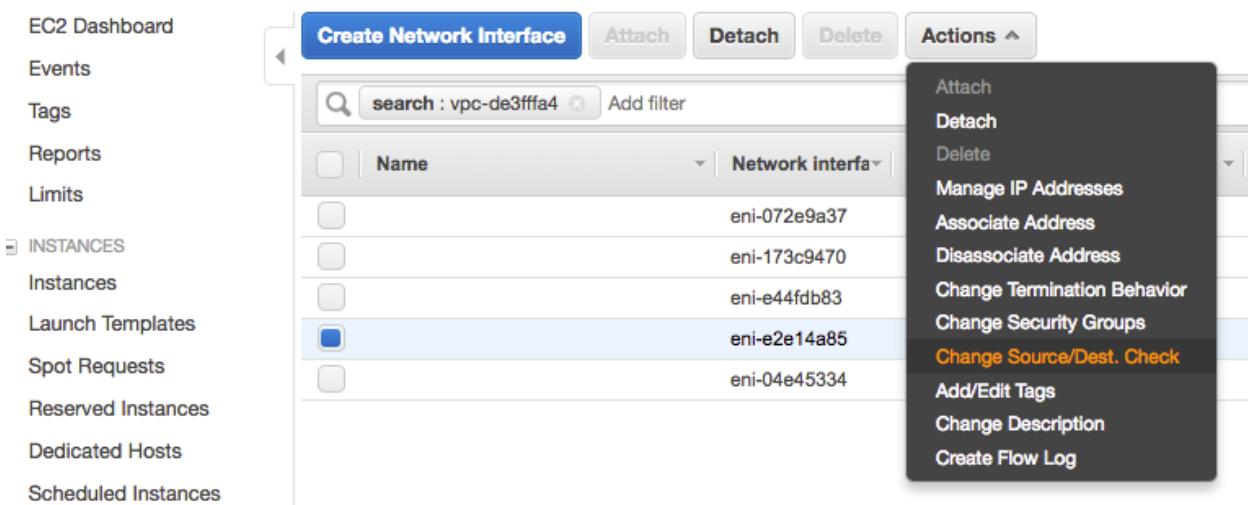
From the main Window select the Create Network Interface. You will need to create a label to identify the eth 1/1 of each firewall for the Untrust interface. You will need to assign a network interface in each subnet. Firewall1 should have been deployed in AZ-a and firewall 2 in AZ-b. Make sure that each label is set accordingly to the correct AZ.

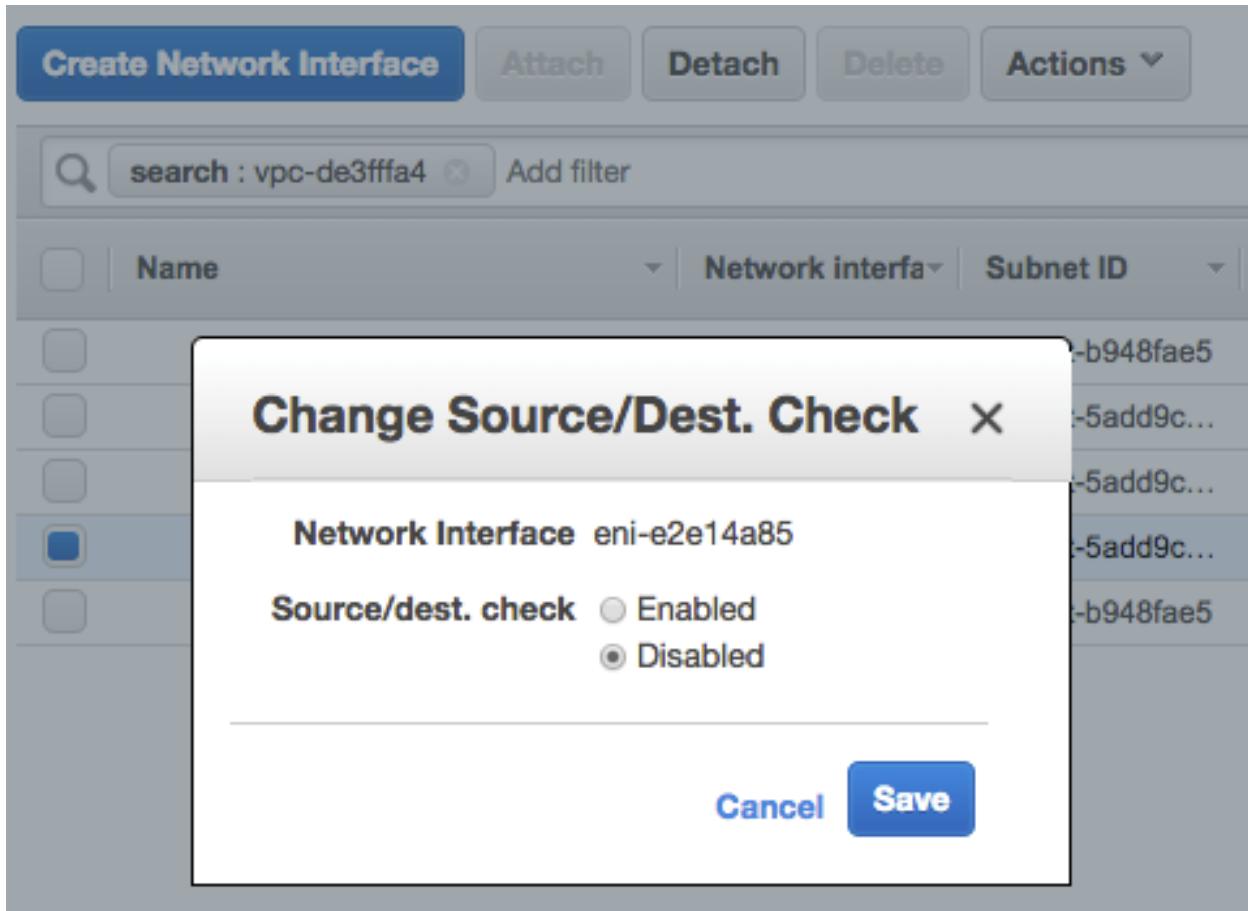


## Firewall2 Network Interface:

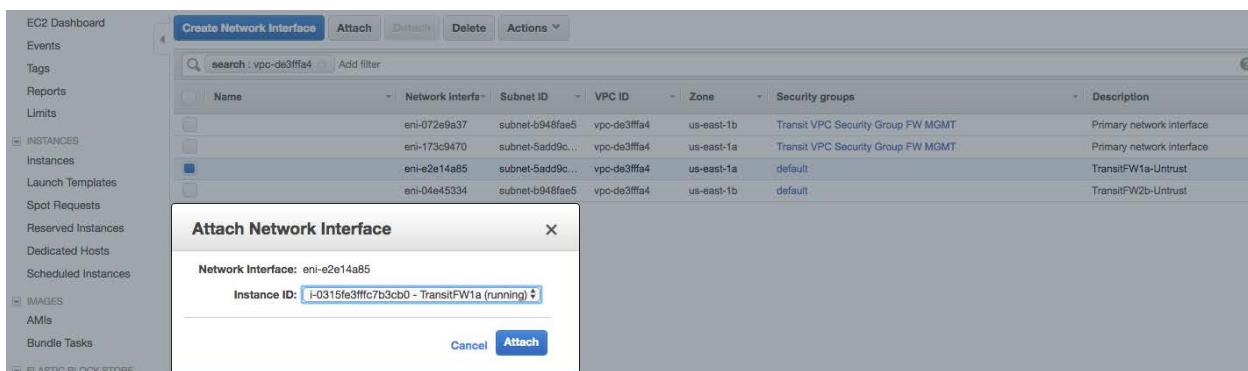


Next, highlight the Network Interface and hit the Actions Drop-Down. Choose the Change Source/Dest Check Option and Disable Source/Destination Check. This allows traffic to route through the firewall even if it is not destined for the firewall's assigned IP address.





After your interfaces are created, select each interface individually to attach to the firewall instance. Check the box next to the interface and select the Attach button. In the pop up window, open the drop-down menu and select the firewall instance. You will need to do this for both interfaces.



Once the network interfaces have been created, enable the interface on each of the firewalls. Log into each of the firewalls. Once you are in each firewall, go to the network tab and interfaces screen. Select Ethernet 1/1:

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone	Features	Comment
ethernet1/1	Layer3		Dynamic-DHCP Client	default	Untagged	none	Untagged	Untrust		
ethernet1/2	Layer3		none	none	Untagged	none	none	none		
ethernet1/3	Layer3		none	none	Untagged	none	none	none		
ethernet1/4	Layer3		none	none	Untagged	none	none	none		
ethernet1/5	Layer3		none	none	Untagged	none	none	none		
ethernet1/6	Layer3		none	none	Untagged	none	none	none		
ethernet1/7	Layer3		none	none	Untagged	none	none	none		

From the interface configuration window, configure the interface as below:

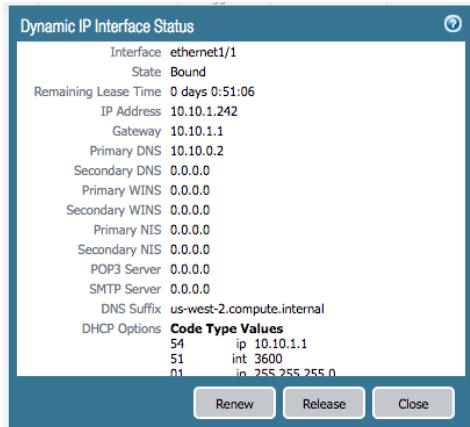
**NOTE** Ensure to select a Virtual Router or you will receive an error on commit.  
You can also choose to create your Untrust Security Zone now.

From the IPv4 tab configure as below. Once configured select ok and commit the changes:

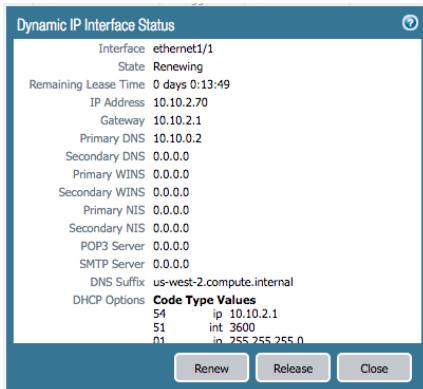
Once the commit completes, you should see the following on your network interface window:

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone
<a href="#">ethernet1/1</a>	Layer3			Dynamic-DHCP Client	default	Untagged	none	Untrust

if you click on the Dynamic DHCP Client link you should have a status as the example below:



Repeat the above interface configuration for the second firewall. Once complete, you should see a DHCP Client link



Once you are at this point commit the changes to the firewall.

Next, we will need to create Elastic IP (EIP) addresses for the new dataplane interfaces created in the last step for each firewall. From the EC2 Dashboard, select Elastic IP's and select allocate new address.

The screenshot shows the AWS EC2 Dashboard with the 'Allocate new address' button highlighted in blue. The left sidebar includes links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, Elastic Block Store, and Network & Security. Under Network & Security, 'Elastic IPs' is selected and highlighted with a red box.

From the Allocate New Address window, click on the allocate button.

The screenshot shows the 'Allocate new address' window. It has fields for 'Allocation ID' and 'Scope'. At the bottom right, there are 'Cancel' and 'Allocate' buttons, with 'Allocate' being the one highlighted.

Once you allocate a new address a window will pop up with new EIP that you will associate with the dataplane interface of the firewall.

The screenshot shows a success message window with a green checkmark icon. The text reads 'New address request succeeded' and 'Elastic IP: 3.13.10.13'. There is a 'Close' button at the bottom right.

From the Elastic IP's window, select the box next to the new address that was created. From the actions drop down select Associate address:

The screenshot shows the 'Allocate new address' window with the 'Associate address' option highlighted in the 'Actions' dropdown menu. Other options in the menu include Release addresses, Disassociate address, Move to VPC scope, and Restore to EC2 scope.

You will need to document the eni from the AWS interfaces console. Below shows an example of the eni from the EC2 dashboard, network interface menu. You will look for and document the Network Interface ID for eth 1/1 of firewall 1 and firewall 2.

Name	Network Interface ID	Subnet ID	VPC ID	Zone	Security groups	Description
SVC VPC FW1 eth1	eni-21a00564	subnet-071aae...	vpc-7eb2b6f19	us-west-2a	default	SVC VPC FW1 eth1

From the associate address window, select resource type, network interface from the network interface drop down select enter the eni ID that was document in the last step for eth 1/1 on the firewalls.

Select the instance OR network interface to which you want to associate this Elastic IP address (34.208.130.13)

Resource type  Instance  Network interface

Network interface

Private IP

Reassociation

**Warning:** If you associate an Elastic IP address with your instance, your current public IP address is released. [Learn more](#).

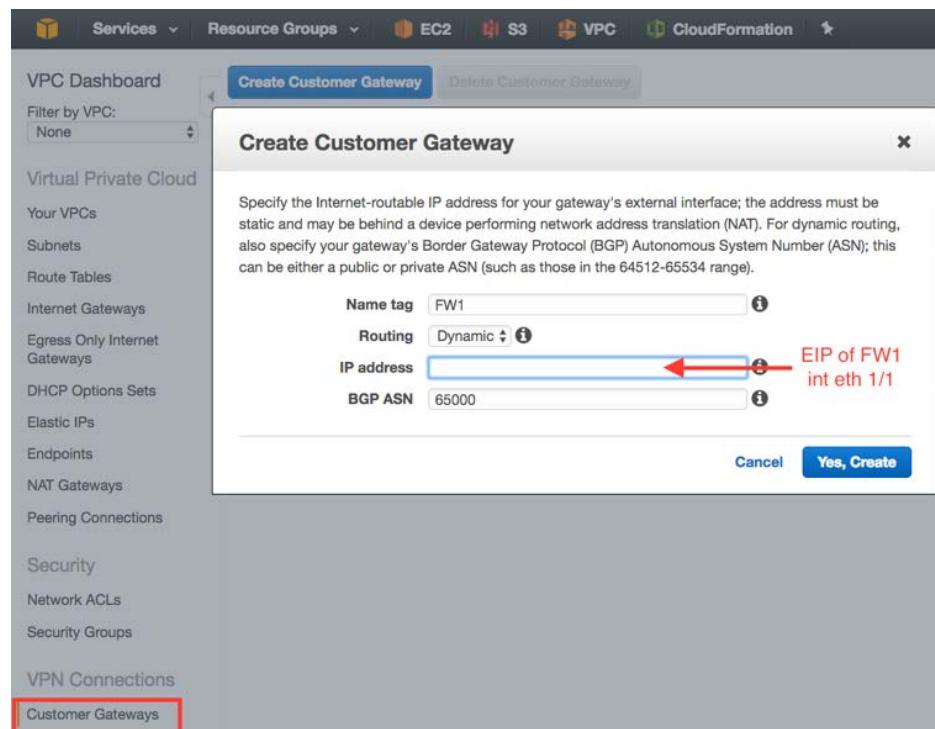
\* Required

Repeat the above steps for the firewall2 to associate a new EIP to firewall 2.

## Create Customer Gateways

In this section, we will create the customer gateways for each of the firewalls in the Transit VPC. We will use the EIP address that was just associated on each of the firewall eth 1/1 interfaces.

From the VPC dashboard select Customer Gateways. From the customer gateway window select Create Customer Gateway. Make sure to match up the EIP with the correct firewall.



Create a second Customer gateway as above for firewall 2 using the EIP of int eth 1/1 of firewall 2. Your completed screen should look like this:

The screenshot shows the AWS VPC Dashboard. On the left, there is a sidebar with various VPC-related options: Virtual Private Cloud (Your VPCs, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways), DHCP Options Sets, Elastic IPs, Endpoints, NAT Gateways, Peering Connections, Security (Network ACLs, Security Groups), VPN Connections, and Customer Gateways (which is currently selected). The main area displays a table of Customer Gateways with the following data:

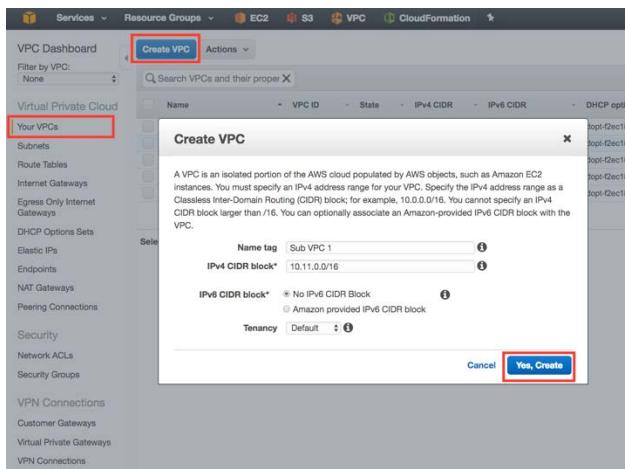
Name	ID	State	Type	IP Address	BGP ASN
FW1	cgw-648a517a	available	ipsec.1	3	20
FW2	cgw-658a517b	available	ipsec.1	5	85

A blue button labeled "Create Customer Gateway" is visible at the top of the main content area.

## Section 2 Create the subscribing VPC's

In this section, we will build the (3) subscribing VPC's that will connect back to the Transit VPC via an IPSec connection between the Virtual Gateway (VGW) and the VM-Series firewalls in the Transit VPC. You can configure a second Availability Zone and subnet for each of the subscribing VPC's if you choose.

From the VPC dashboard select the Your VPC's menu, click on the Create VPC button. In the pop up window create a name tag for the VPC and assign a CIDR block. In this example we have used Sub VPC 1- 10.11.0.0/16, Sub VPC 2 10.12.0.0/16 and Sub VPC 3 10.13.0.0/16.



Create the VPC's for Sub VPC 2 and 3 as above with the associated CIDR block.

Next, we will create the Subnets for each of the subscribing VPC's from the VPC Dashboard, select the Subnets menu. From the subnets menu select the Create Subnet button. In the Create Subnet pop up window, create a name for the subnet, select the VPC for the subnet, assign an Availability Zone and assign an IPv4 CIDR block.

[Subnets](#) > Create subnet

## Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

VPC CIDRs	CIDR	Status	Status Reason
	10.11.0.0/16	associated	

\* Required

Cancel **Create**

Create (2) more subnets associating them to VPC 2 10.12.1.0/24 and VPC 3 10.13.1.0/24

Next, we will create Route Tables for the new Subscribing VPC's. From the VPC Dashboard, select the Route Tables menu item. From the Route Tables window, select the Create Route Table button. From the Create route table pop up window name your Route table and assign the subscribing VPC from the drop down. Once complete select the Yes, Create button.

A route table specifies how packets are forwarded between the subnets within your VPC, the Internet, and your VPN connection.

Name tag: rt-Transit-sub1

VPC: vpc-6152921b | Transit-sub1

Cancel **Yes, Create**

Create route table associated to Sub VPC 2 and Sub VPC 3. Once the route tables are created, we want to associate the correct subnets with each of the route tables. From the Route tables menu, select the box next to VPC1 Route Table. From the bottom of the window select the Subnet Associations tab. Click the Edit button where you will click the box next to the subnet created in the last step. Once the subnet has been selected, select the Save button.

The screenshot shows the AWS VPC Dashboard. On the left sidebar, under 'Route Tables', the 'Edit' button for 'rt-Transit-sub1' is highlighted. The main pane displays two route tables: 'rt-Transit-sub2' and 'rt-Transit-sub1'. The 'rt-Transit-sub1' table is selected. Below it, a detailed view of 'rtb-6052ca1f | rt-Transit-sub1' shows the 'Subnet Associations' tab selected. A table lists a single subnet: 'subnet-e7eeafad | Transit-sub1net' with CIDR '10.11.1.0/24' and 'Main' as the current route table. The 'Save' button is visible at the bottom of this panel.

We will revisit the Route tables for the Subscribing VPC's once we complete the VPN configuration.

Next, we are going to create the Virtual Private Gateways for the Subscribing VPC's. From the VPC Dashboard, select the Virtual Private Gateways menu item. From the Virtual Private Gateway window, select the create Virtual Private gateway button. Provide a name for the gateway.

It is recommended to provide a Custom ASN that is unique per subscribing VPC to allow for BGP propagation. The ASN must be in either the 16 bit or 32 bit private range.

- 16 bit: 64512 to 65535
- 32 bit: 4200000000 – 4294967294

Click the Create Virtual Private Gateway button when complete.

[Virtual Private Gateways](#) > Create Virtual Private Gateway

## Create Virtual Private Gateway

A virtual private gateway is the router on the Amazon side of the VPN tunnel.

Name tag  i

ASN  Amazon default ASN i  
 Custom ASN i

i

Cancel Create Virtual Private Gateway

Create Gateways for Sub VPC 2 and Sub VPC 3.

**IMPORTANT** Ensure to Attach to Virtual Private Gateway to its VPC from the Actions Menu.

## Section 3 Create the VPN Connections

From the VPC Dashboard, select the VPN Connections menu. From the VPN Connections window select the create VPN connection button. In the pop up window, provide a name for the connection. You will need to build a VPN connection from each of the VPC's to both firewalls in the Transit VPC. It is recommended that you use a name descriptor that will be easy to determine which VPC VPN connection belongs to which firewall in the Transit VPC .

**NOTE – Amazon now provides the ability to specify the Inside CIDR for the tunnel to prevent overlap. If you will be creating a significant number of spokes, it is recommended to utilize this feature as Amazon has historically had collision issues with more than ~10 spokes.**

Please see the example below.

[VPN Connections](#) > [Create VPN Connection](#)

### Create VPN Connection

Select the virtual private gateway and customer gateway that you would like to connect via a VPN connection. You must have entered the virtual private gateway and your customer gateway information already.

Name tag  ⓘ

Virtual Private Gateway\*  ⚒

Customer Gateway  Existing  
 New

Customer Gateway ID  ⚒

Routing Options  Dynamic (requires BGP)  
 Static

**Tunnel Options**

Customize tunnel inside CIDR and pre-shared keys for your VPN tunnels. Unspecified tunnel options will be randomly generated by Amazon.

Inside IP CIDR for Tunnel 1  ⓘ

Pre-Shared Key for Tunnel 1  ⓘ

Inside IP CIDR for Tunnel 2  ⓘ

Pre-shared key for Tunnel 2  ⓘ

VPN connection charges apply once this step is complete. [View Rates](#)

[Cancel](#) [Create VPN Connection](#)

You will need to configure a total of 6 VPN Connections for the 3 subscribing VPC's. Please see the example below.

Name	VPN ID	State	Virtual Private Gateway	Customer Gateway	Customer Gateway Address	Type	VPC
VPC1 to FW1	vpn-d17e66c3	available	vgw-8a62ba94   sub vpc 1	cgw-648a517a (3)   FW1	35. 2.0	ipsec.1	vpc-4b32762c
VPC1 to FW2	vpn-d57e66c4	available	vgw-8a62ba94   sub vpc 1	cgw-658a517b (5)   FW2	52. 85	ipsec.1	vpc-4b32762c
VPC2 to FW1	vpn-d77e66c5	available	vgw-8d62ba95   sub vpc 2	cgw-648a517a (3)   FW1	35. 2.0	ipsec.1	vpc-25327642
VPC2 to FW2	vpn-d47e66c6	available	vgw-8d62ba95   sub vpc 2	cgw-658a517b (5)   FW2	52. 85	ipsec.1	vpc-25327642
VPC3 to FW1	vpn-d57e66c7	available	vgw-8862ba96   sub vpc 3	cgw-648a517a (3)   FW1	35. 2.0	ipsec.1	vpc-e6327681
VPC3 to FW2	vpn-d77e66c8	available	vgw-8862ba96   sub vpc 3	cgw-658a517b (5)   FW2	52. 85	ipsec.1	vpc-e6327681

Once the VPN connections have been created, you will need to download the configuration file for each VPN connection. Be very careful to keep each file separate and labeled for which connection it is associated. The configuration file will be used to configure the firewall in PAN-OS. There should be a total of 6 files to download from AWS with configurations for 12 separate tunnels. You will have 6 tunnels per firewall. The files that correspond to firewall 1 needs to be configured on firewall 1. It is recommended that you download the files individually and use them to configure each firewall separately. This will help keep the files and configurations straight as you build the tunnels.

VPC Dashboard

Filter by VPC:

Select a VPC

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

Security

Network ACLs

Security Groups

VPN Connections

Customer Gateways

Virtual Private Gateways

VPN Connections

Create VPN Connection

Download Configuration

Actions

Filter by tags and attributes or search by keyword

Name	VPN ID	State	Virtual Private Gateway
Sub1 To FW2b	vpn-1dbba57c	pending	vgw-5c1eef35   VPG-sub1
Sub2 To FW2b	vpn-1abba57b	pending	vgw-5f1eef36   VPG-sub2
Sub2 To FW1a	vpn-17bba576	pending	vgw-5f1eef36   VPG-sub2
Sub1 To FW1a	vpn-14bba575	pending	vgw-5c1eef35   VPG-sub1

**Download Configuration**

Please choose the configuration to download based on your type of customer gateway

Vendor: Palo Alto Networks

Platform: PA Series

Software: PANOS 7.0+

Cancel Download

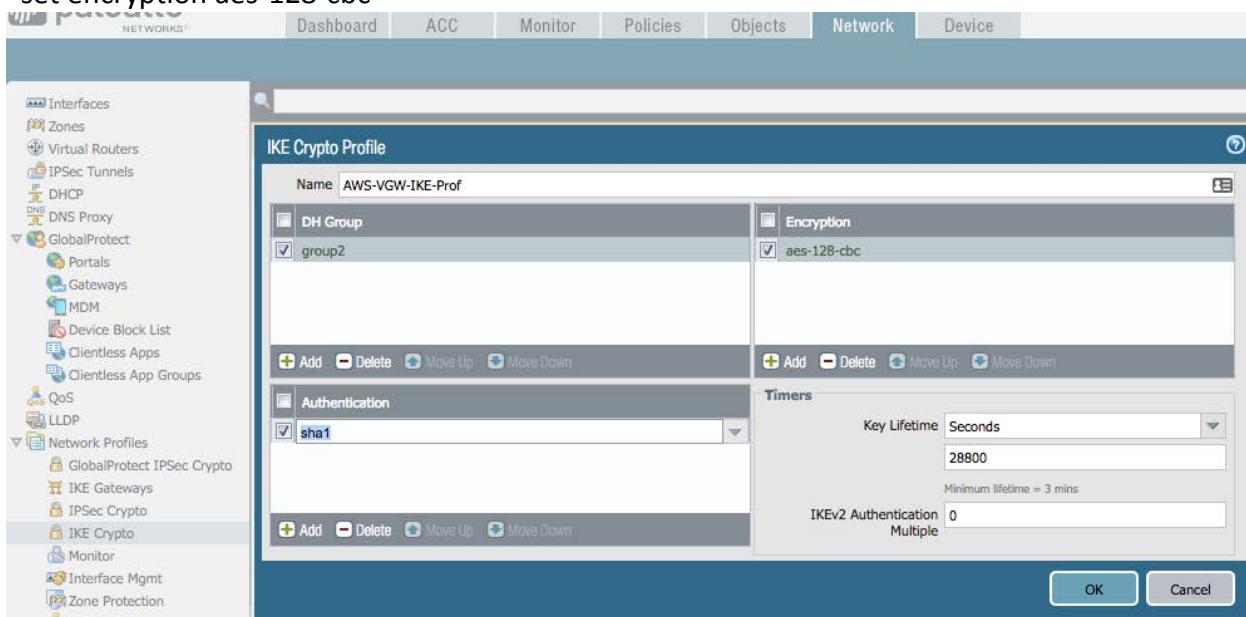
Details Tunnel Details Tags

VPN ID	vpn-14bba575
Virtual Private Gateway	vgw-5c1eef35   VPG-sub1
Customer Gateway Address	18.211.85.165
Category	VPN
Routing	Dynamic

An example would be naming the above file “VPC 1 firewall1.txt”. Renaming the file will help as you begin to create the IKE Gateways and other steps through this process. You will have 3 files that will provide the VPN configuration for each of the VPC’s connecting to firewall 1 in the Transit VPC. You will have an additional 3 files that will provide the VPN configuration for firewall 2 in the Transit VPC. You will need to keep them separate. The file contains the PAN-OS commands that can be pasted into the console of the firewall from an SSH session or can be configured in the Mgmt Web Interface of the firewall. For this example, we used the Web interface.

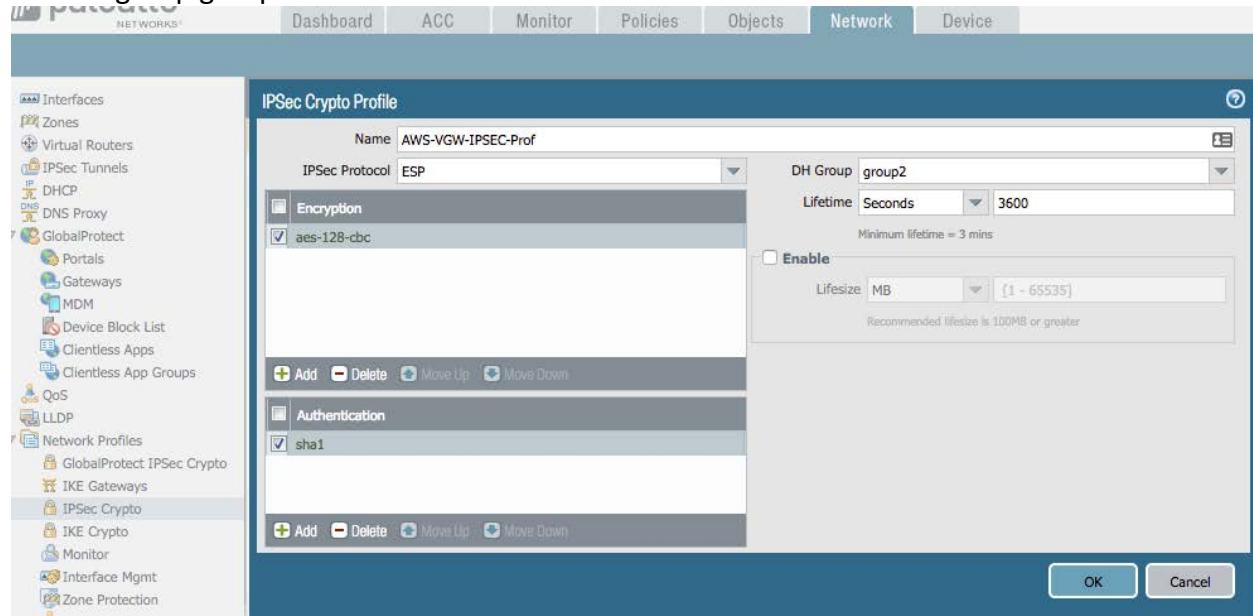
Once you have the corresponding VPN configuration file, log into the firewall web interface. From the Network Tab select IKE Crypto and configure as below. These settings can be verified in the downloaded configuration files.

```
set dh-group group2
set hash sha1
set lifetime seconds 28800
set encryption aes-128-cbc
```



Configure the IPSec Crypto as follows:

```
set esp authentication sha1  
set esp encryption aes-128-cbc  
set dh-group group2 lifetime seconds 3600
```



For the IKE gateway, you will need to build one for each Subscribing VPC Gateway. We used the Name VPC 1-1 and VPC 1-2 as examples to differentiate the gateways. For each of the IKE gateways, you will need to pull the configuration from the VPN file downloaded from the VPN Connection.

For Gateway 1-1 use the file from the VPN Connection 1. As the screen below shows which files need to be used for firewall 1 and which files will be used for firewall 2. In the file there are configurations for (2) tunnels. You will need to create an IKE gateway for each of the tunnels. The highlighted VPN connection configuration files should be used for firewall1. The 3 files not highlight will be used for firewall2.

Name	VPN ID	State	Virtual Private Gateway	Customer Gateway	Customer Gateway
VPC1 to FW1	vpn-d17e66c3	available	vgw-8a62ba94   sub vpc 1	cgw-648a517a (35.2.0)   FW1	35.165.12.0
VPC1 to FW2	vpn-d57e66c4	available	vgw-8a62ba94   sub vpc 1	cgw-658a517b (52.85)   FW2	52.89.84.85
VPC2 to FW1	vpn-d77e66c5	available	vgw-8b62ba95   sub vpc 2	cgw-648a517a (35.2.0)   FW1	35.165.12.0
VPC2 to FW2	vpn-d47e66c6	available	vgw-8b62ba95   sub vpc 2	cgw-658a517b (52.85)   FW2	52.89.84.85
VPC3 to FW1	vpn-d57e66c7	available	vgw-8862ba96   sub vpc 3	cgw-648a517a (35.2.0)   FW1	35.165.12.0
VPC3 to FW2	vpn-d87e66c8	available	vgw-8862ba96   sub vpc 3	cgw-658a517b (52.85)   FW2	52.89.84.85

Below is a sample of the configuration file to be used on VPC 1 firewall 1.

```
!
! -----  

! IPSec Tunnel #1  

! -----  

! #1: Internet Key Exchange (IKE) Configuration  

!  

! A policy is established for the supported ISAKMP encryption,  

! authentication, Difflie-Hellman, lifetime, and key parameters.  

! Please note, these sample configurations are for the minimum requirement of AES128,  

SHA1, and DH Group 2.  

! You will need to modify these sample configuration files to take advantage of AES256,  

SHA256, or other DH groups like 2, 14-18, 22, 23, and 24.  

! The address of the external interface for your customer gateway must be a static  

address.  

! Your customer gateway may reside behind a device performing network address translation  

(NAT).  

! To ensure that NAT traversal (NAT-T) can function, you must adjust your firewall !rules  

to unblock UDP port 4500. If not behind NAT, we recommend disabling NAT-T.  

!  

configure  

edit network ike crypto-profiles ike-crypto-profiles ike-crypto-vpn-d17e66c3-0  

set dh-group group2  

set hash sha1  

set lifetime seconds 28800  

set encryption aes-128-cbc  

top  

!  

With local-address IP please append the configured subnet mask (i.e., /30) on the VPN  

initiating interface (i.e., ethernet 1/1)  

! For example if you have /30 as subnet mask the local-address ip should be  

35.0.0/30  

edit network ike gateway ike-vpn-d17e66c3-0  

set protocol ikev1 ike-crypto-profile ike-crypto-vpn-d17e66c3-0 exchange-mode main  

set protocol ikev1 ddos interval 10 retry 3 enable yes  

set authentication pre-shared-key key N  

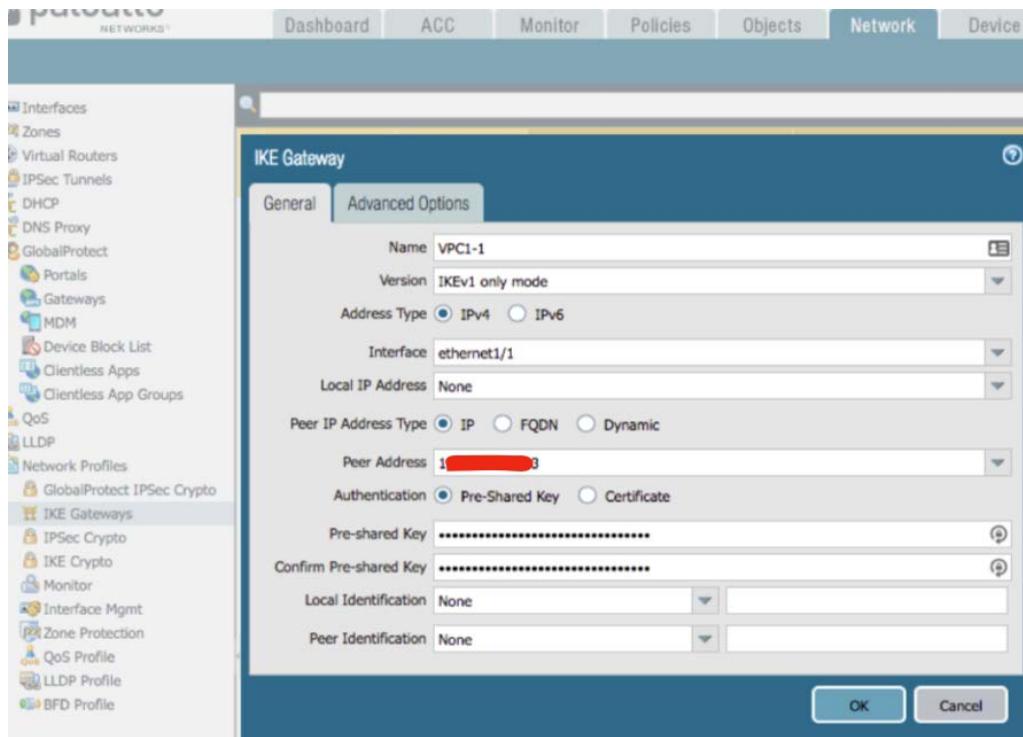
set local-address ip 35.0.0.0  

set local-address interface ethernet1/1  

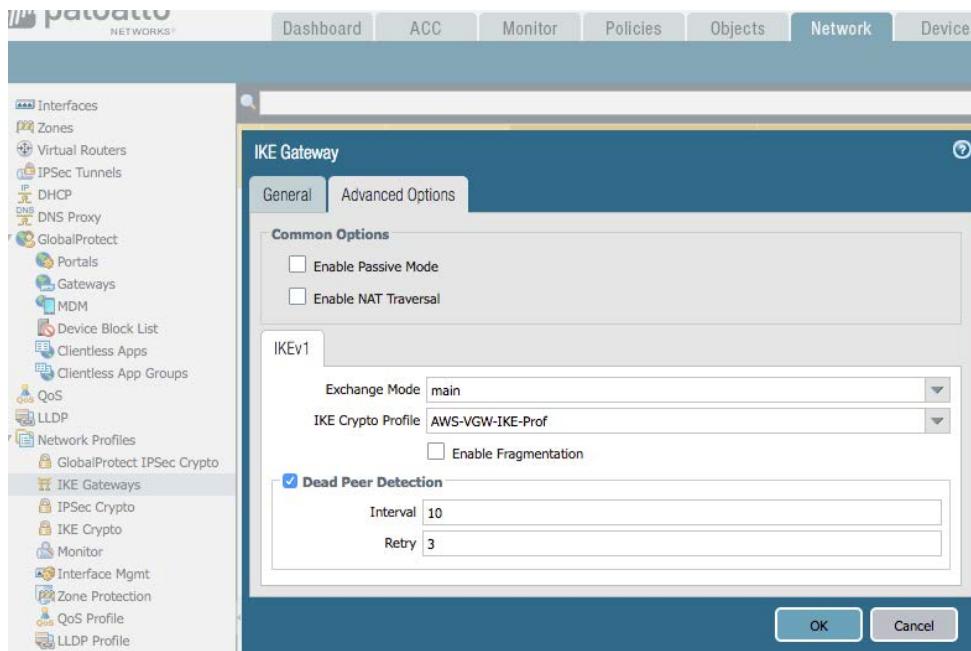
set peer-address ip 35.179.179.179  

top
```

## IKE Gateway General Tab:



## Advanced Options tab:



For tunnel 2 you will need to use the same file as above, but create a new IKE Gateway with the tunnel 2 parameters from the bottom portion of the file:

```
!
! -----
! IPSec Tunnel #2
! -----
! #1: Internet Key Exchange (IKE) Configuration
!
! A policy is established for the supported ISAKMP encryption,
! authentication, Diffie-Hellman, lifetime, and key parameters.
! Please note, these sample configurations are for the minimum requirement of AES128,
! SHA1, and DH Group 2.
! You will need to modify these sample configuration files to take advantage of AES256,
! SHA256, or other DH groups like 2, 14-18, 22, 23, and 24.
! The address of the external interface for your customer gateway must be a static
! address.
! Your customer gateway may reside behind a device performing network address translation
! (NAT).
! To ensure that NAT traversal (NAT-T) can function, you must adjust your firewall !rules
! to unlock UDP port 4500. If not behind NAT, we recommend disabling NAT-T.
!
configure
edit network ike crypto-profiles ike-crypto-profiles ike-crypto-vpn-d17e66c3-1
set dh-group group2
set hash sha1
set lifetime seconds 28800
set encryption aes-128-cbc
top

! With local-address IP please append the configured subnet mask (i.e., /30) on the VPN
! initiating interface (i.e., ethernet 1/1)
! For example if you have /30 as subnet mask the local-address ip should be
35._____.0/30

edit network ike gateway ike-vpn-d17e66c3-1
set protocol ikev1 ike-crypto-profile ike-crypto-vpn-d17e66c3-1 exchange-mode main
set protocol ikev1 dpd interval 10 retry 3 enable yes
set authentication pre-shared-key key 75
set local-address ip 35._____.2.0
set local-address interface ethernet1/1
set peer-address ip 35._____.221
top
```

## IKE Gateway 2 General Tab

The screenshot shows the IKE Gateway configuration in the General tab. The left sidebar lists various network components. The main window has tabs for "General" and "Advanced Options".

**General Tab Fields:**

- Name: VPC1-2
- Version: IKEv1 only mode
- Address Type: IPv4 (selected)
- Interface: ethernet1/1
- Local IP Address: None
- Peer IP Address Type: IP (selected)
- Peer Address: [Redacted]
- Authentication: Pre-Shared Key (selected)
- Pre-shared Key: [Redacted]
- Confirm Pre-shared Key: [Redacted]
- Local Identification: None
- Peer Identification: None

Buttons at the bottom: OK and Cancel.

## Advanced Tab:

The screenshot shows the IKE Gateway configuration in the Advanced Options tab. The left sidebar lists various network components. The main window has tabs for "General" and "Advanced Options".

**Common Options:**

- Enable Passive Mode
- Enable NAT Traversal

**IKEv1:**

- Exchange Mode: main
- IKE Crypto Profile: AWS-VGW-IKE-Prof
- Enable Fragmentation

**Dead Peer Detection:**

- Dead Peer Detection
- Interval: 10
- Retry: 3

Buttons at the bottom: OK and Cancel.

You will need to complete the above steps for Sub VPC 2 and Sub VPC 3 so that your final configuration looks like the example below:

Name	Peer Address	Interface	IP	ID	Type	T0	T1	Version	Mode	Passive Mode	NAT Traversal	Crypto Profile	DPD	Liveness
VPC-1	52. 58	ethernet5/1							Avail	mean		Avg-VSN-1KB-	enabled	1/2/3
VPC-1	26. 3.179	ethernet5/1							Avail	mean		Avg-VSN-1KB-	enabled	1/2/3
VPC-1	35. 78.75	ethernet5/1							Avail	mean		Avg-VSN-1KB-	enabled	1/2/3
VPC-2	35. A.223	ethernet5/1							Avail	mean		Avg-VSN-1KB-	enabled	1/2/3
VPC-2	52. 1.170	ethernet5/1							Avail	mean		Avg-VSN-1KB-	enabled	1/2/3
VPC-2	52. 176	ethernet5/1							Avail	mean		Avg-VSN-1KB-	enabled	1/2/3

Next, we will create the tunnel interfaces on the VM-Series. From the network tab select the Interface menu. From the tunnel tab select Add from the bottom of the window and configure the tunnels as shown below:

From the VPN config file for the VPN connection use the tunnel interface config section of the document. You will have a tunnel interface for tunnel 1 and a tunnel interface for tunnel 2 from the VPN Document downloaded from AWS.

**NOTE – This example shows all tunnel interfaces in the Untrust Zone which will allow traffic to be allowed by virtue of the “intrazone-default” security policy. The reader has the option of controlling traffic with subnet-based policies or mapping the Tunnel interfaces to differing Zones. For more information on Zones, please refer to this guide.**

<https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/getting-started/segment-your-network-using-interfaces-and-zones>

```

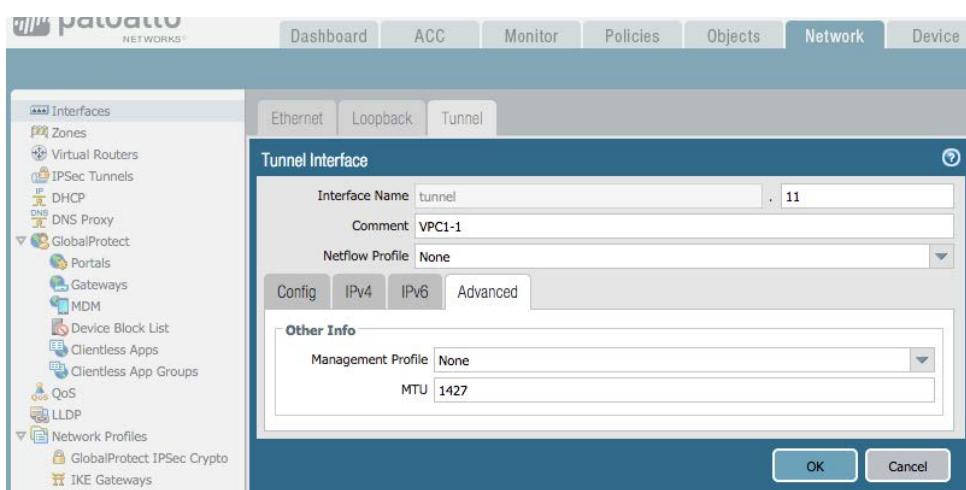
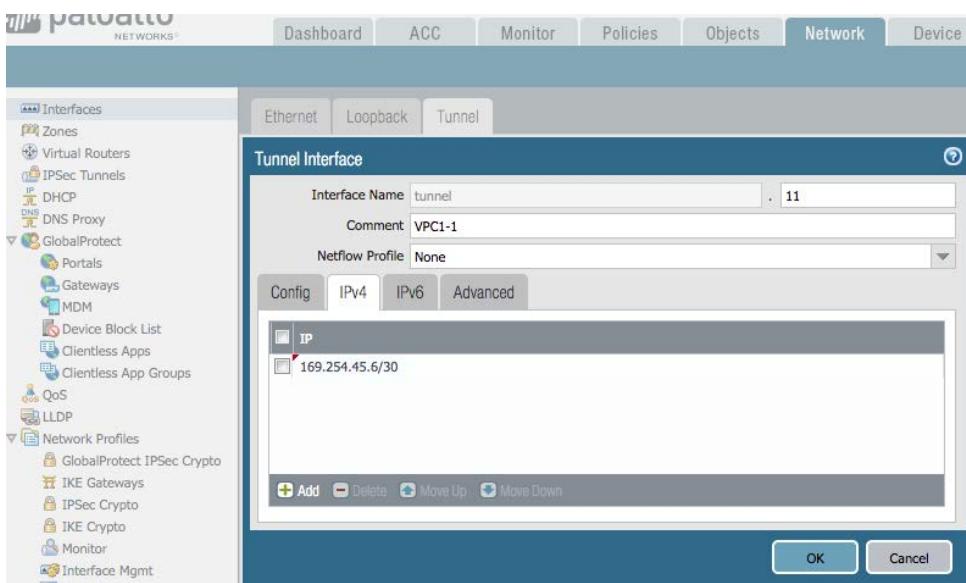
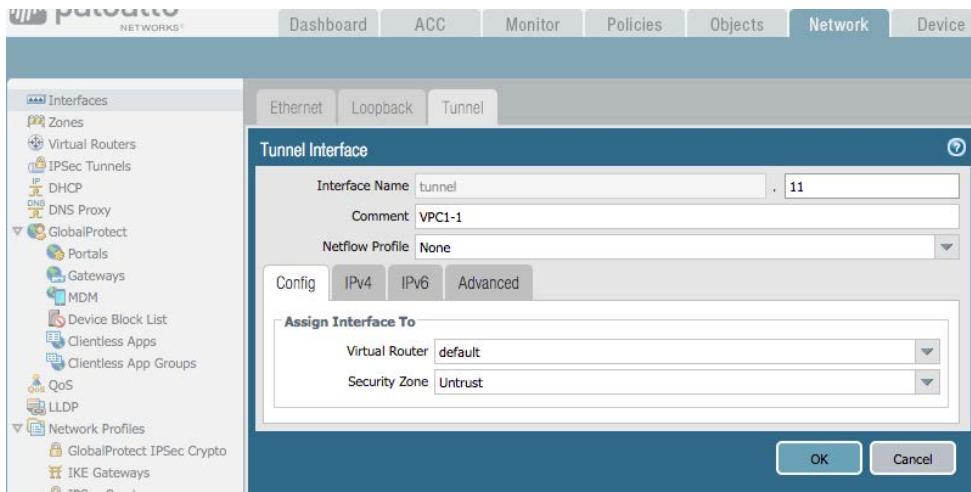
! -----#
! #3: Tunnel Interface Configuration
!
! A tunnel interface is configured to be the logical interface associated
! with the tunnel. All traffic routed to the tunnel interface will be
! encrypted and transmitted to the VPC. Similarly, traffic from the VPC
! will be logically received on this interface.
!
! Association with the IPSec security association is done through the
! "tunnel protection" command.
!
! The address of the interface is configured with the setup for your
! Customer Gateway. If the address changes, the Customer Gateway and VPN
! Connection must be recreated with Amazon VPC.
!

edit network interface tunnel units tunnel.1
set ip 169.1.1.90/30
set mtu 1427
top

!
! Tunnel interface needs to be associated to Zone, we are using untrust zone as an
example, please adjust according
!

set zone untrust network layer3 tunnel.1

```



**You will create (2) tunnels per Subscribing VPC documented in the VPN connection file. Your configuration should look like the example below.**

Interface	Management Profile	IP Address	Virtual Router	Security Zone	Features	Comment
tunnel.1	none	10.2.30	default	VPC1		VPC1 to 1
tunnel.2	none	10.2.30	default	VPC2		VPC2 to 1
tunnel.3	none	200.200	default	VPC1		VPC3 to 1
tunnel.4	none	40.2.30	default	VPC2		VPC1 to 2
tunnel.5	none	100.2.30	default	VPC2		VPC2 to 2
tunnel.6	none	60.2.30	default	VPC3		VPC3 to 2

Now we will create the IPSec tunnels on the VM Series. From the network tab and the IPSec menu, select add at the bottom of the window to create a new IPSec tunnel.

Repeat the steps and match tunnel interfaces to the correct IKE gateways that have been created. Your IPSec Tunnels should look like the following example.

Name	Status	Type	Interface	Local IP	Peer IP	Status	Interface	Virtual Router	Virtual System	Security Zone	Status
VPC1-1	Up	Auto Key	ethernet1/1	35.179	35.179	Up	tunnel.1	default (Show Router)	vpc1	VPC1	Up
VPC1-2	Up	Auto Key	ethernet1/1	35.179	35.179	Up	tunnel.2	default (Show Router)	vpc1	VPC1	Up
VPC2-1	Up	Auto Key	ethernet1/1	35.178	35.178	Up	tunnel.3	default (Show Router)	vpc2	VPC2	Up
VPC2-2	Up	Auto Key	ethernet1/1	35.178	35.178	Up	tunnel.4	default (Show Router)	vpc2	VPC2	Up
VPC3-1	Up	Auto Key	ethernet1/1	35.179	35.179	Up	tunnel.5	default (Show Router)	vpc3	VPC3	Up
VPC3-2	Up	Auto Key	ethernet1/1	35.179	35.179	Up	tunnel.6	default (Show Router)	vpc3	VPC3	Up

Once you are to this point, commit the configuration to the firewall.

To validate the tunnels, from the CLI of the firewall, issue the following command:  
**show vpn ipsec-sa**

```
admin@PA-VM> show vpn ipsec-sa
GwID/client IP  TnID  Peer-Address          Tunnel(Gateway)           Algorithm      SPI(in)   SPI(out)  life(Sec/KB)
-----  -----  -----          -----           -----      -----  -----  -----
2       1      35.179          VPC1-1(VPC1-1)        ESP/A128/SHA1  B70A1906  F73B7FB1  644/0
3       2      35.178          VPC2-1(VPC2-1)        ESP/A128/SHA1  A462A648  65F30F73  644/0
1       3      52.158          VPC3-1(VPC3-1)        ESP/A128/SHA1  9CD3CA26  B9913997  645/0
4       4      35.179          VPC1-2(VPC1-2)        ESP/A128/SHA1  D00AF805  EFEA72E7  1232/0
5       5      52.170          VPC2-2(VPC2-2)        ESP/A128/SHA1  A86C9EBA  91C18940  1063/0
6       6      52.176          VPC3-2(VPC3-2)        ESP/A128/SHA1  9F6E427A  10BAB5C1  1064/0

Show IPsec SA: Total 6 tunnels found. 6 ipsec sa found.

admin@PA-VM>
```

You should see 6 tunnels active, if you do not see the above, the tunnels may not come up automatically. If not, they can be manually triggered using the CLI.

**test vpn ipsec-sa**

```
admin@SVC-VPC-firewall12> test vpn ipsec-sa
Initiate 6 IPsec SA.
```

If you still do not see the 6 active tunnels after manually triggering the tunnels, validate that you have configured your ike gateways and vpn connections correctly in the above steps.

You will need to complete the same steps on firewall 2 with the VPN files for firewall2.

At this point, the VPN connections will Report IPSEC IP and Status Down in the AWS console. This is due to a lack of traffic on the tunnels. They report up once BGP or other traffic is traversing the tunnels.

The screenshot shows a table titled "Tunnel Details" with three tabs: "Tunnels" (selected), "Tunnel Details" (highlighted in yellow), and "Tags". The table has columns: Outside IP Address, Inside IP CIDR, Status, Status Last Changed, and Details. There are two rows of data:

Outside IP Address	Inside IP CIDR	Status	Status Last Changed	Details
1.159.92	169.254.45.228/30	DOWN	July 26, 2018 at 3:14:35 PM UTC-4	IPSEC IS UP
54.210.128	169.254.46.136/30	DOWN	July 26, 2018 at 3:15:34 PM UTC-4	IPSEC IS UP

## Section 4 Configure BGP

Now that we have our communication between the subscribing VPCs and the Transit VPC established, we will configure a dynamic routing protocol to assist with dynamic route learning for each of the VPC's, fault tolerance and symmetric path.

First we will create a static default route. This route will point to the AWS VPC router. From the firewall1 web interface, select the network tab and select the virtual routers menu item. From the window select the default router. You will get a pop-up window for the virtual router. Select the Static Route menu item.

From the pop up window select add at the bottom left of the window to create a new static route. Name the route Default and configure the route as the example below:

The screenshot shows the Palo Alto Networks Firewall interface under the Network tab. On the left, a sidebar lists various network components like Interfaces, Zones, Virtual Routers, and GlobalProtect. The main area displays a table for 'Virtual Router - default' with one row selected for 'default'. Below this, a 'Virtual Router - Static Route - IPv4' configuration dialog is open. The configuration details are as follows:

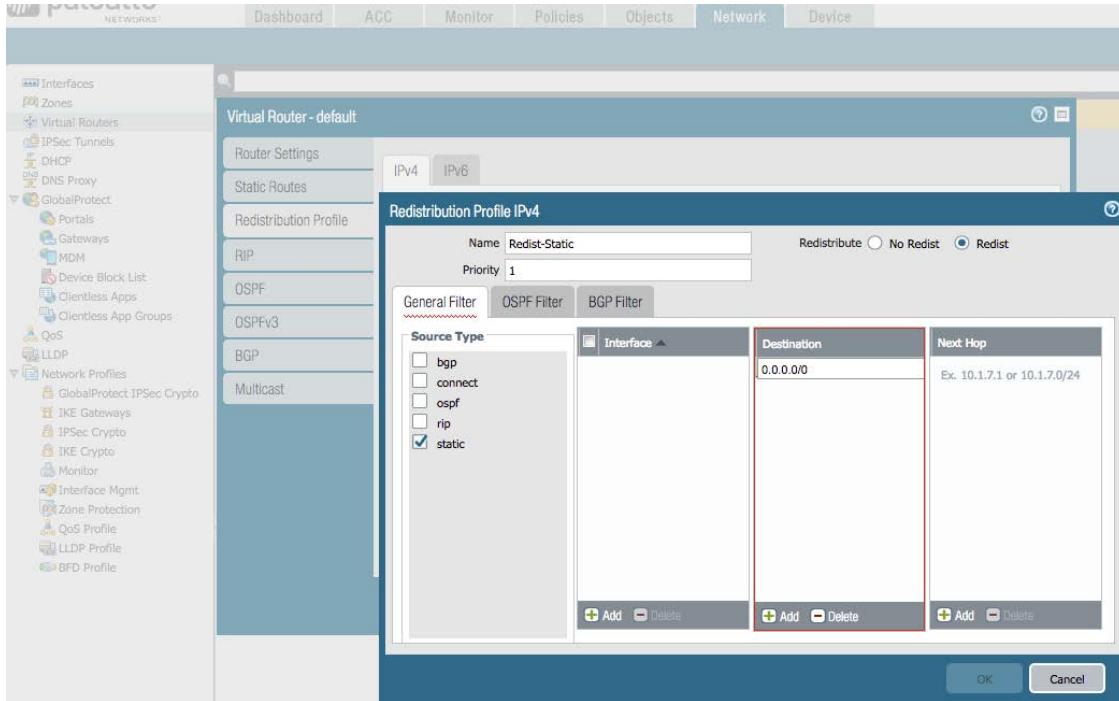
Name	default
Destination	0.0.0.0/0
Interface	ethernet1/1
Next Hop	IP Address 10.10.1.1
Admin Distance	10 - 240
Metric	10
Route Table	Unicast
BFD Profile	Disable BFD

Below the configuration table is a 'Path Monitoring' section with a table for monitoring paths. The table has columns: Name, Enable, Source IP, Destination IP, Ping Interval(sec), and Ping Count. There is an 'Add' button at the bottom left of this section.

At the bottom right of the configuration dialog are 'OK' and 'Cancel' buttons.

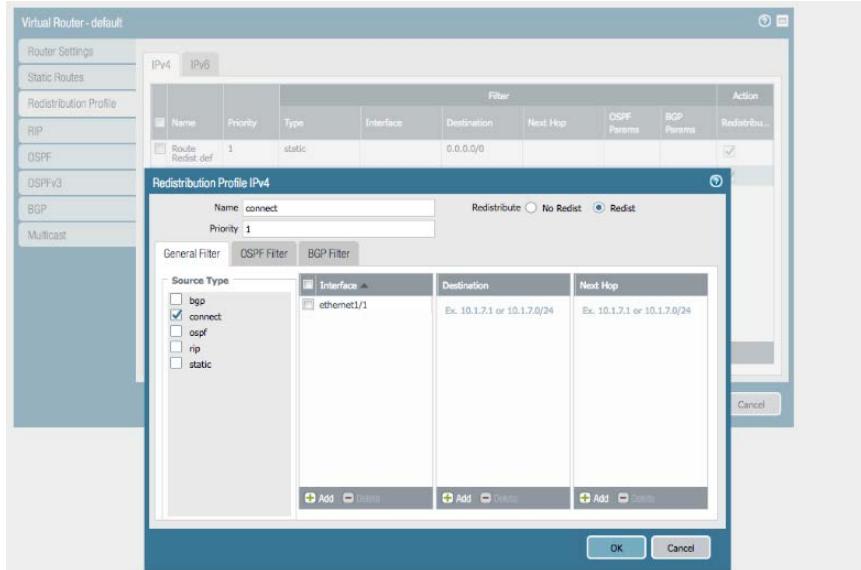
Next, we need to create a Redistribution Profile. From the virtual router, select the Redistribution Profile tab. From the bottom of the virtual router window select add to create a new redistribution profile. The first redistribution profile will create a policy to redistribute the default route. Configure your profile as shown in the example below.

### General Tab:

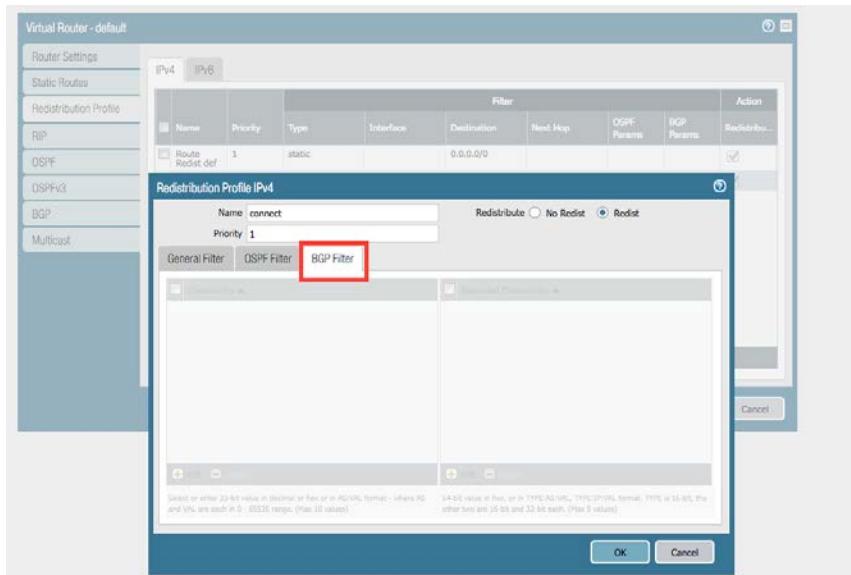


Next we will create a profile to redistribute connected interfaces. From the Redistribution Profile tab select add to create a new profile and configure your connected profile as shown in the example below.

#### General Filter tab:



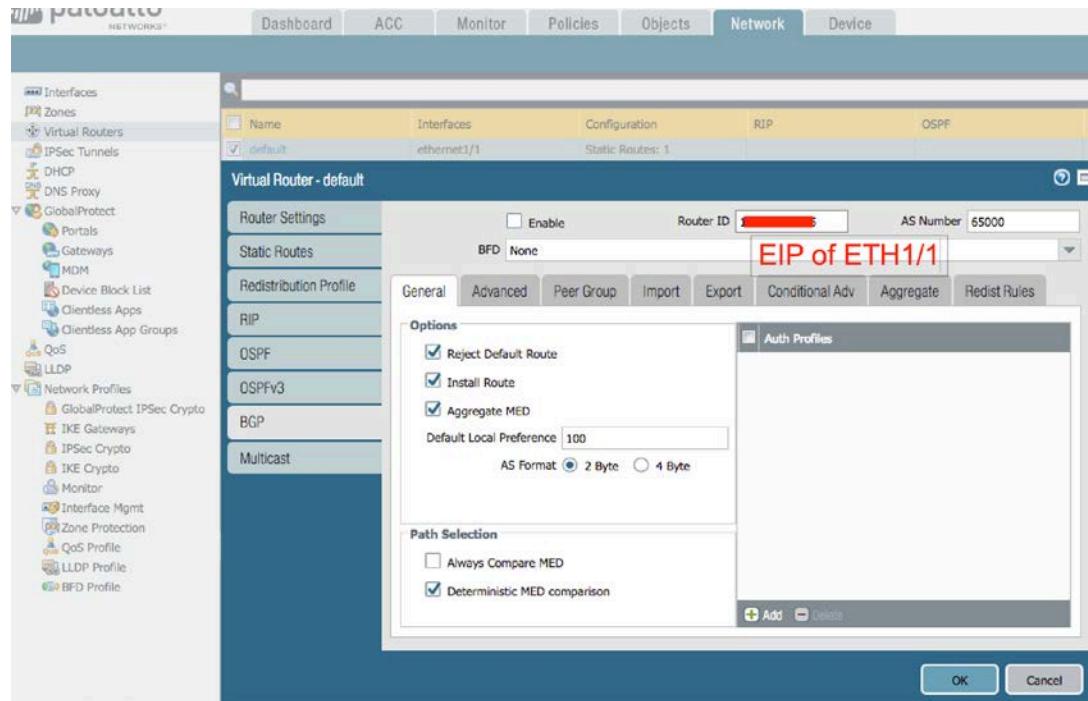
#### BGP Filter tab:



Your Redistribution Profile window should look like the example below:

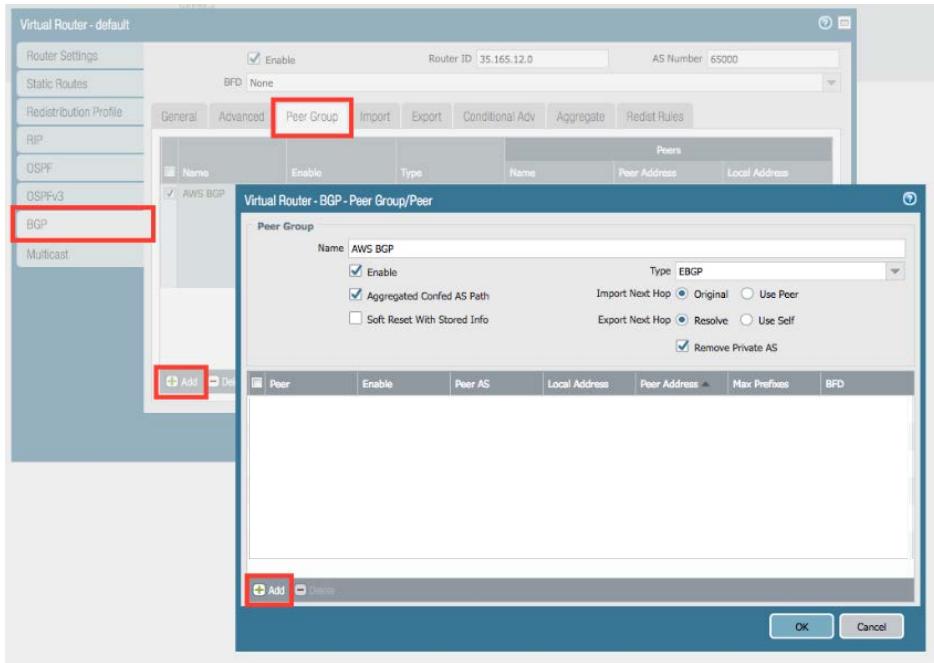
The screenshot shows the Palo Alto Networks Firewall interface. The top navigation bar includes Dashboard, ACC, Monitor, Policies, Objects, Network (selected), and Device. The left sidebar lists various configuration categories: Interfaces, Zones, Virtual Routers (selected), IPSec Tunnels, DHCP, DNS Proxy, GlobalProtect (Portals, Gateways, MDM, Device Block List, Clientless Apps, Clientless App Groups), QoS, LLDP, Network Profiles (GlobalProtect IPSec Crypto, IKE Gateways, IPSec Crypto, IKE Crypto, Monitor, Interface Mgmt, Zone Protection, QoS Profile, LLDP Profile, BFD Profile). The main content area displays the 'Virtual Router - default' configuration. A table at the top shows 'Interfaces' (default, ethernet1/1) and 'Configuration' (RIP, OSPF). Below is a detailed table for the 'Redistribution Profile' tab, with the 'IPv4' tab selected. The table columns are: Name, Priority, Type, Interface, Destination, Next Hop, OSPF Params, BGP Params, and Action. One entry is listed: 'Redist-Static' with Priority 1, Type static, Destination 0.0.0.0/0. At the bottom of the table are 'Add', 'Delete', and 'Clone' buttons, along with 'OK' and 'Cancel' buttons.

Next, we will enable and configure BGP parameters. From the Virtual router window select the BGP tab. Set the Router IP to the EIP assigned to ETH1 in AWS. Configure the general tab as shown in the example below.



Next, we are going to create a BGP peer group. From the BGP tab select the Peer Group tab. At the bottom on the BGP window, click add to create a new peer group. As you create each peer in the group, you will have to match up the local IP address to the correct peer address. These addresses can be found in the AWS VPN configuration files. As you will recall the AWS VPN configuration file contains configuration information for (2) tunnels. You will need the local address and peer address for each tunnel. Below is an example of the config file:

Configure the peer group as shown in the example below.

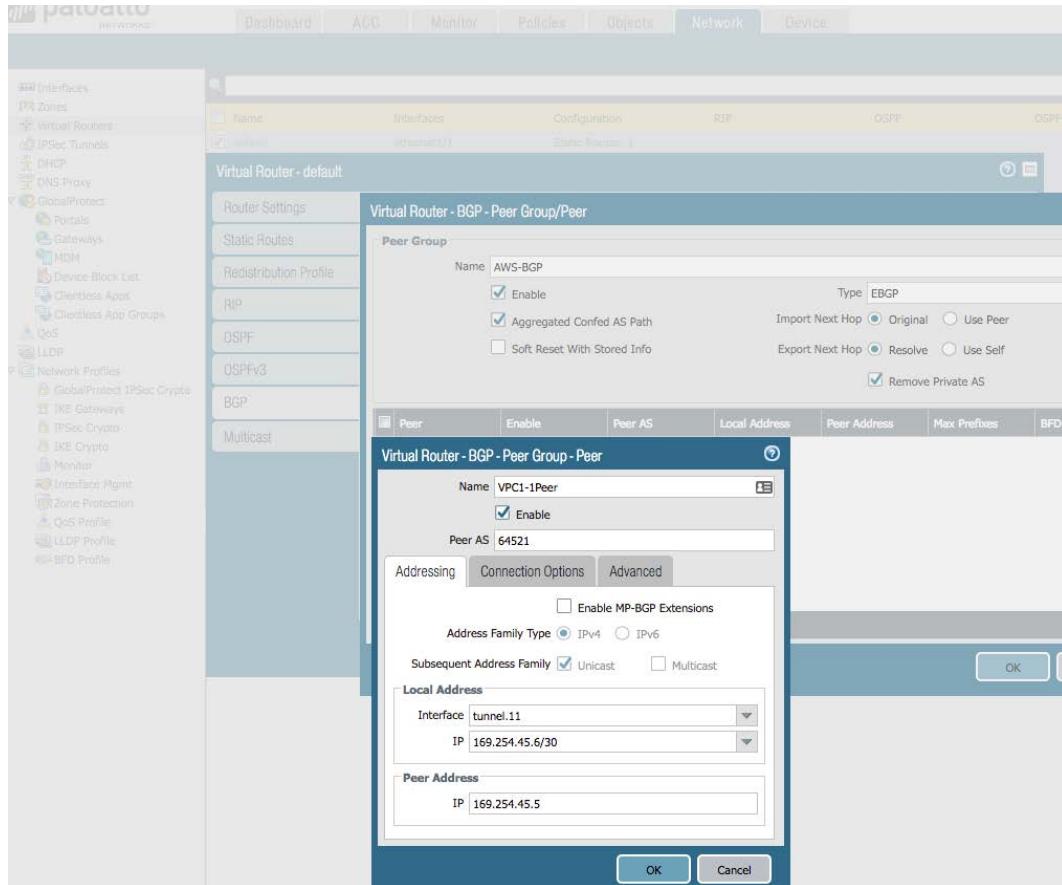


From the Add pop up window, configure the peer as shown in the example below:

```
! -----
! #3: Tunnel Interface Configuration
!
! A tunnel interface is configured to be the logical interface associated
! with the tunnel. All traffic routed to the tunnel interface will be
! encrypted and transmitted to the VPC. Similarly, traffic from the VPC
! will be logically received on this interface.
!
! Association with the IPSec security association is done through the
! "tunnel protection" command.
!
! The address of the interface is configured with the setup for your
! Customer Gateway. If the address changes, the Customer Gateway and VPN
! Connection must be recreated with Amazon VPC.
!
```

```
edit network interface tunnel units tunnel.1
set ip 169.______.90/30
set mtu 1427
top
```

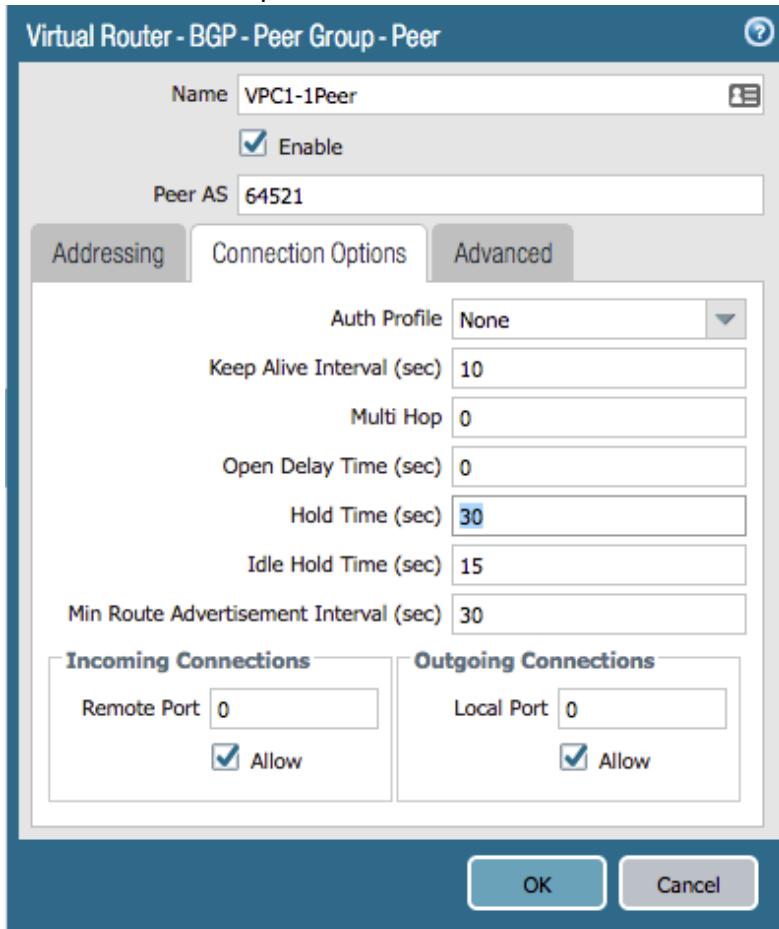
The example above displays information for VPC 1, firewall 1, Tunnel 1. The local address of the firewall is 169.x.x.90/30 and the peer address will be 169.x.x.89. You will need to scroll down the file to get the local and peer address for the second tunnel for VPC 1, firewall1, tunnel 2. See the example below



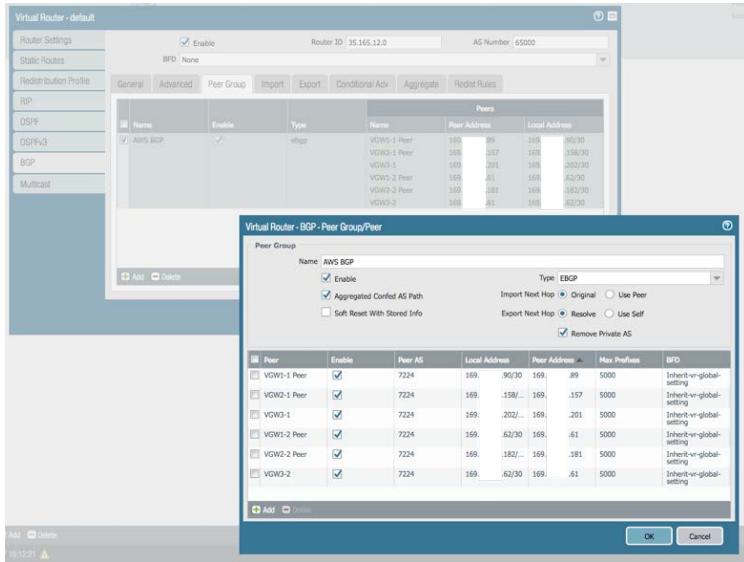
On the Connections Options Tab:

set connection-options keep-alive-interval 10

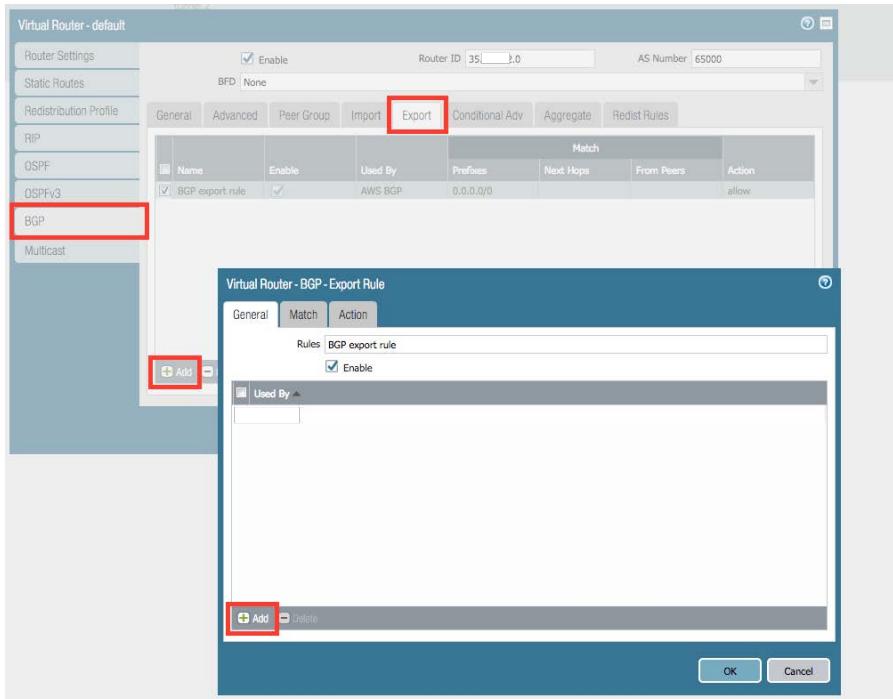
set connection-options hold-time 30



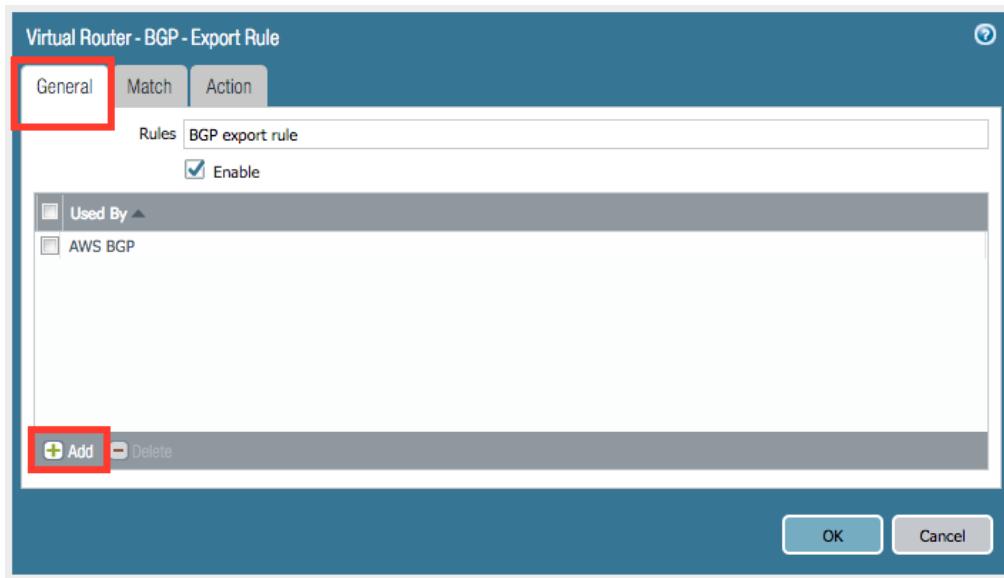
Once you have created the (6) peer connections(?) in the peer group your window should like the following example:



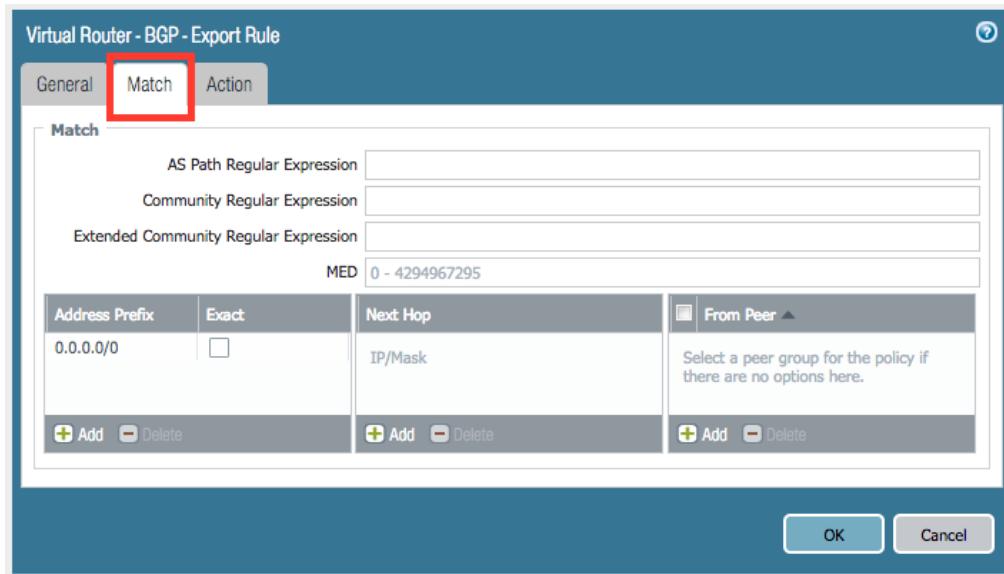
Next, we are going to create a BGP Export rule. From the virtual router BGP menu, select the Export tab. From the bottom of the virtual router window select add to create a new export rule.



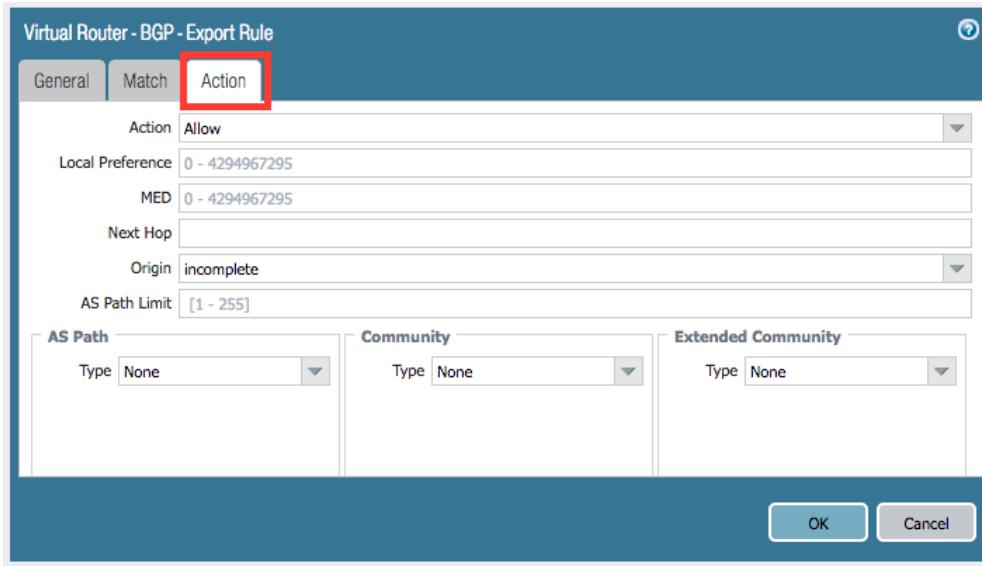
From the pop-up window, click on the add button to create a new peer group configured like the example below.



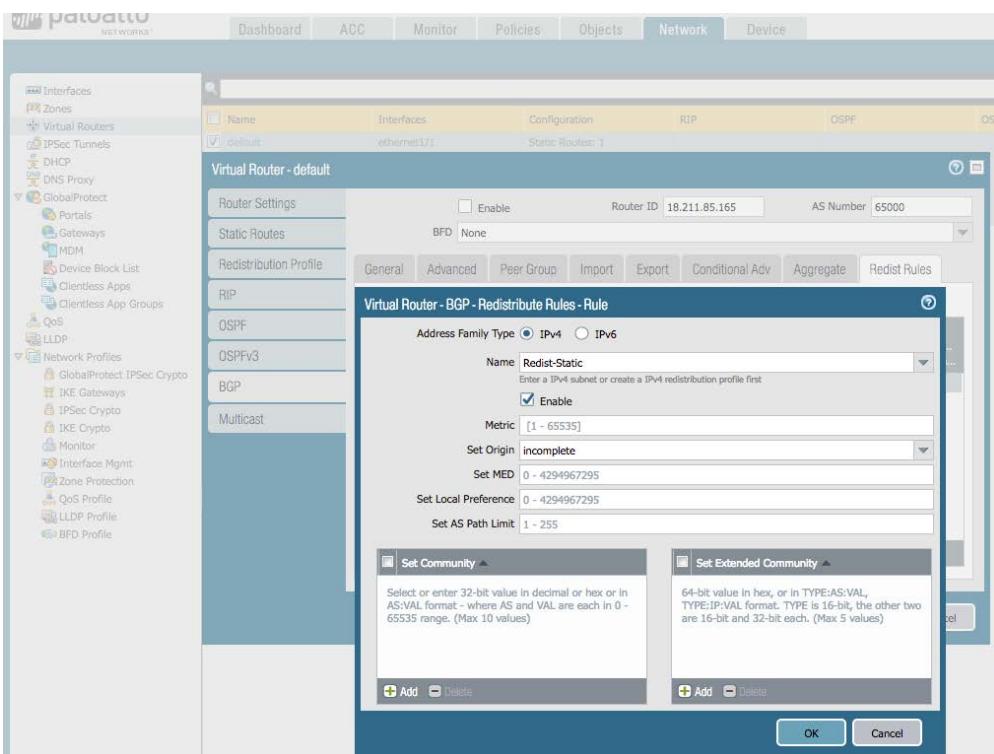
The match tab:



## The Action Tab:



Next, we will configure the BGP Redistribution Rules. From the virtual router select the BGP tab. From the BGP window select the Redist Rules Tab. From the bottom of the Redist Rule window select the Add button. You will get a pop-up window to configure a rule. From the name drop down select the Route Redist def that was created above. Configure the rule as shown below.



From the main BGP window, select the ok button to finish your BGP configuration.

At this point you will want to commit the routing configuration changes to the firewall.

Next, we will validate the routing configuration. Access firewall 1 from an SSH session to access the cli of the firewall.

From the cli, issue the following commands:

```
show routing protocol bgp summary
```

```
admin@PA-VM> show routing protocol bgp summary
=====
router id:          35.165.12.0
virtual router:    default
reject default route: yes
redist default route: allow
Install BGP routes: yes
Graceful Restart: supported
AS size:           2
Local AS:          65000
Local member AS:   0
Cluster id:        0.0.0.0
Default local preference: 100
Always compare MED: no
Aggregate regardless MED: yes
Deterministic MED processing: yes
Accept ORF:         no
Accept CISCO style prefix: yes
mp-bgp-enable:     yes
afi-safi-ipv4-unicast: yes
rib-out entries:   current 18, peak 18
  peer VGW1-2 Peer:      AS 7224, Established, IP 169.254.12.61
    bgpAfIIPv4/unicast pfx: Accepted pfx: 1, Advertised pfx: 3
  peer VGW2-1 Peer:      AS 7224, Established, IP 169.254.12.157
    bgpAfIIPv4/unicast pfx: Accepted pfx: 1, Advertised pfx: 3
  peer VGW3-1:           AS 7224, Established, IP 169.254.13.201
    bgpAfIIPv4/unicast pfx: Accepted pfx: 1, Advertised pfx: 3
  peer VGW1-1 Peer:      AS 7224, Established, IP 169.254.14.89
    bgpAfIIPv4/unicast pfx: Accepted pfx: 1, Advertised pfx: 3
  peer VGW2-2 Peer:      AS 7224, Established, IP 169.254.14.181
    bgpAfIIPv4/unicast pfx: Accepted pfx: 1, Advertised pfx: 3
  peer VGW3-2:           AS 7224, Established, IP 169.254.15.61
    bgpAfIIPv4/unicast pfx: Accepted pfx: 1, Advertised pfx: 3
admin@PA-VM>
```

Next, we will check to make sure that the default routes are being advertised:

```
show routing protocol bgp rib-out
```

```
admin@PA-VM> show routing protocol bgp rib-out
=====
VIRTUAL ROUTER: default (id 1)
=====
Prefix      Nexthop    Peer   Originator   Adv Status  Aggr Status  AS-Path
0.0.0.0/0    169.254.14.98  VGW1-1 Peer 0.0.0.0   advertised  no aggregation  65000
10.1.1.0/32  169.254.14.98  VGW1-1 Peer 0.0.0.0   advertised  no aggregation  65000
10.10.1.0/24 169.254.14.98  VGW1-1 Peer 0.0.0.0   advertised  no aggregation  65000
0.0.0.0/0    169.254.12.158  VGW2-1 Peer 0.0.0.0   advertised  no aggregation  65000
10.1.1.0/32  169.254.12.158  VGW2-1 Peer 0.0.0.0   advertised  no aggregation  65000
10.10.1.0/24 169.254.12.158  VGW2-1 Peer 0.0.0.0   advertised  no aggregation  65000
0.0.0.0/0    169.254.13.202  VGW3-1   0.0.0.0   advertised  no aggregation  65000
10.1.1.0/32  169.254.13.202  VGW3-1   0.0.0.0   advertised  no aggregation  65000
10.10.1.0/24 169.254.13.202  VGW3-1   0.0.0.0   advertised  no aggregation  65000
0.0.0.0/0    169.254.12.62   VGW1-2 Peer 0.0.0.0   advertised  no aggregation  65000
10.1.1.0/32  169.254.12.62   VGW1-2 Peer 0.0.0.0   advertised  no aggregation  65000
10.10.1.0/24 169.254.12.62   VGW1-2 Peer 0.0.0.0   advertised  no aggregation  65000
0.0.0.0/0    169.254.14.182  VGW2-2 Peer 0.0.0.0   advertised  no aggregation  65000
10.1.1.0/32  169.254.14.182  VGW2-2 Peer 0.0.0.0   advertised  no aggregation  65000
10.10.1.0/24 169.254.14.182  VGW2-2 Peer 0.0.0.0   advertised  no aggregation  65000
0.0.0.0/0    169.254.15.62   VGW3-2   0.0.0.0   advertised  no aggregation  65000
10.1.1.0/32  169.254.15.62   VGW3-2   0.0.0.0   advertised  no aggregation  65000
10.10.1.0/24 169.254.15.62   VGW3-2   0.0.0.0   advertised  no aggregation  65000
total routes shown: 18
admin@PA-VM>
```

Finally, we will validate learning routes from each VPC in AWS.  
show routing protocol bgp loc-rib

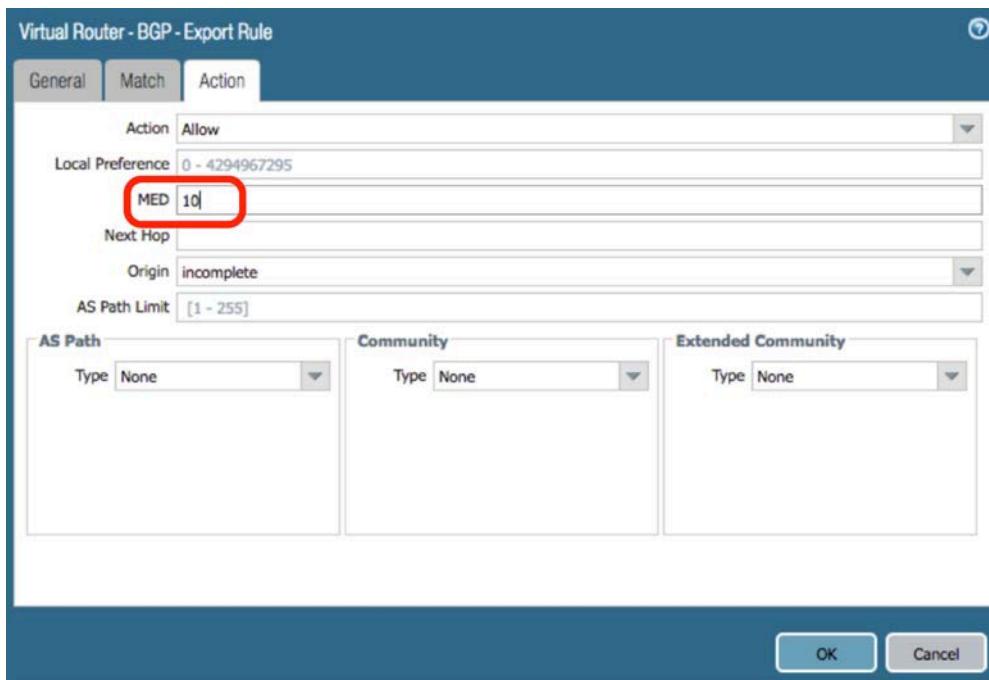
```
admin@PA-VM> show routing protocol bgp loc-rib

VIRTUAL ROUTER: default (id 1)
=====
Prefix      Nexthop      Peer      Weight  LocPrf Org      MED flap AS-Path
10.20.0.0/16 169.254.14.89  VGW1-1 Peer      0      100 igp    200  0 7224
10.30.0.0/16 169.254.12.157 VGW2-1 Peer      0      100 igp    200  0 7224
10.40.0.0/16 169.254.13.201 VGW3-1 Peer      0      100 igp    200  0 7224
*10.20.0.0/16 169.254.12.61  VGW1-2 Peer      0      100 igp    100  0 7224
*10.30.0.0/16 169.254.14.181 VGW2-2 Peer      0      100 igp    100  0 7224
*10.40.0.0/16 169.254.15.61  VGW3-2 Peer      0      100 igp    100  0 7224
*0.0.0.0/0     10.10.1.1      Local      0      100 i/c     0      0
*10.1.1.1/32   Local      0      100 i/c     0      0
*10.10.1.0/24  Local      0      100 i/c     0      0

total routes shown: 9
```

You have now completed the BGP configuration for firewall 1. You will need to perform the same steps for the Routing configuration on firewall 2.

In Order to prevent routing asymmetry will configure Firewall 2 with a higher Multi-Exit Discriminator (MED).



Once routing has been configured, the VPN connections will report the number of Routes learned.

Outside IP Address	Inside IP CIDR	Status	Status Last Changed	Details
3.233.183.193	169.254.45.4/30	UP	July 26, 2018 at 4:01:55 PM UTC-4	2 BGP ROUTES
2.201.48.137	169.254.44.36/30	UP	July 26, 2018 at 4:03:04 PM UTC-4	2 BGP ROUTES

The last step is to configure route propagation or configure a static route pointing to the VGW in the AWS console. In the VPC console go to Route Tables and select the Route Table tied to your spoke Subnets. In the route propagation table, select Edit and Check the box for the attached VGW and hit Save.

Summary    Routes    Subnet Associations    **Route Propagation**    Tags

**Cancel** **Save**

Virtual Private Gateway    Propagate

vgw-5c1eef35 | VPG-sub1

Move to the Routes tab and you will now see the propagated routes targeting the VGW.

Summary    **Routes**    Subnet Associations    Route Propagation    Tag

**Edit**

View: All rules

Destination	Target	Status	Propagated
10.11.0.0/16	local	Active	No
0.0.0.0/0	vgw-5c1eef35	Active	Yes
10.12.0.0/16	vgw-5c1eef35	Active	Yes

At this point you should have built a Transit VPC on AWS with the VM-Series. You can setup an ec2 instance in a subscribing VPC to test outbound functionality. This provides the connectivity between the subscribing VPC and the Transit VPC.