

FIELD TECH NOTES

AWS Transit Gateway - Manual Build

Jason Meurer
CE, AMER

Introduction

This guide will walk the reader through a manual build of an AWS Transit Gateway (TGW) with two spoke VPCs and a Security VPC. The Security VPC will contain 2 Palo Alto Networks VM-Series firewalls configured to enable outbound and Intra-VPC inspection.

AWS Transit Gateway is a service that enables customers to connect their Amazon Virtual Private Clouds (VPCs) and their on-premises networks to a single gateway. As you grow the number of workloads running on AWS, you need to be able to scale your networks across multiple accounts and Amazon VPCs to keep up with the growth. Today, you can connect pairs of Amazon VPCs using peering. However, managing point-to-point connectivity across many Amazon VPCs, without the ability to centrally manage the connectivity policies, can be operationally costly and cumbersome. For on-premises connectivity, you need to attach your AWS VPN to each individual Amazon VPC. This solution can be time consuming to build and hard to manage when the number of VPCs grows into the hundreds.

With AWS Transit Gateway, you only have to create and manage a single connection from the central gateway in to each Amazon VPC, on-premises data center, or remote office across your network. Transit Gateway acts as a hub that controls how traffic is routed among all the connected networks which act like spokes. This hub and spoke model significantly simplifies management and reduces operational costs because each network only has to connect to the Transit Gateway and not to every other network. Any new VPC is simply connected to the Transit Gateway and is then automatically available to every other network that is connected to the Transit Gateway. This ease of connectivity makes it easy to scale your network as you grow.



Expected Outcome

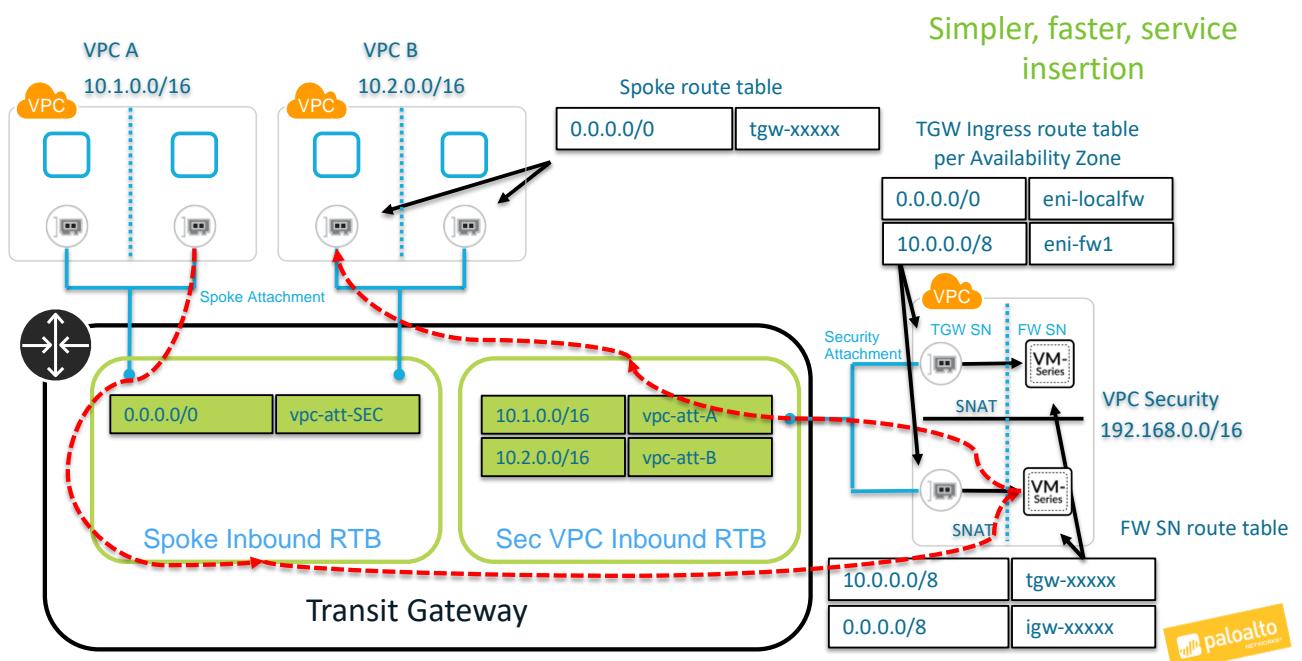
This guide will walk through the following configurations.

- Building 3 VPCs (2 Spokes and 1 Security)
- Build a Transit Gateway with 2 route tables
- Perform the necessary Transit Gateway attachments and associations.
- Update the Transit Gateway Route Tables accordingly.
- Deploy 2 VM-Series firewalls manually with proper routing, security and NAT policies.
- Update the VPC route tables accordingly.
- Deploy a testing client and testing web server.

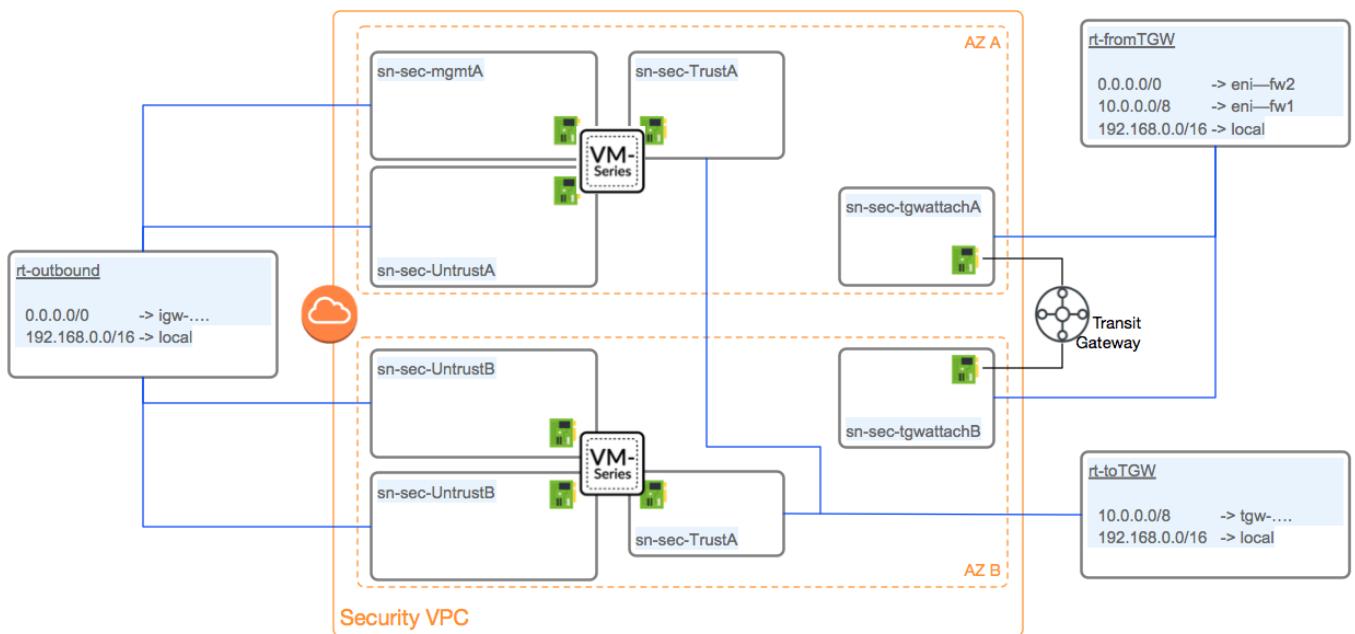
Diagrams

Overall Flow

VPC INSERTION



Security VPC Subnets and Route Tables



Prerequisites

Before You Begin

This guide assumes prior knowledge of and access to the AWS console. The guide also assumes prior knowledge of the Palo Alto Networks VM-Series firewall. The reader should now login into the AWS console and access the desired region.

VPCs

Overview

This section will walk through the creation of 3 VPCs. The 2 spoke VPCs will each have 1 private subnet. It is suggested for demonstration purposes to place the subnets for each spoke in different Availability Zones. This will show the outbound traffic traversing firewalls in the local AZ.

The Security VPC will have 8 total subnets spread across 2 Availability Zones. Each Availability Zone will contain a subnet for Management, Untrust, Trust interfaces of the firewall and a subnet dedicated to the AWS TGW attachment as per AWS's recommendation.

Process Flow

Procedure 1: [VPC Creations](#)

- Step 1 In the AWS console, open the VPC Service.
- Step 2 Select Your VPCs in the left-hand menu and hit the Create VPC button.

Step 3 Specify a Name and CIDR for the spoke VPC.

[VPCs](#) > Create VPC

Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You can specify an IPv4 CIDR block or an IPv6 CIDR block. You cannot specify both at the same time. You can also specify a name tag and a tenancy setting. You can optionally associate a transit gateway with the VPC.

The screenshot shows the 'Create VPC' configuration page. It includes fields for 'Name tag' (tgw-spoke1), 'IPv4 CIDR block*' (10.1.0.0/16), 'IPv6 CIDR block' (radio buttons for 'No IPv6 CIDR Block' and 'Amazon provided IPv6 CIDR block'), and 'Tenancy' (Default). Each field has an information icon (i) to its right.

Name tag	tgw-spoke1	i
IPv4 CIDR block*	10.1.0.0/16	i
IPv6 CIDR block	<input checked="" type="radio"/> No IPv6 CIDR Block <input type="radio"/> Amazon provided IPv6 CIDR block	i
Tenancy	Default	i

Step 4 Select the Create Button and Close on the next page to return to the VPC list.

- Step 5 Repeat the process to create the second spoke VPC and the Security VPCs.

[VPCs > Create VPC](#)

Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You can specify an IPv4 CIDR block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally specify an IPv6 CIDR block.

Name tag

tgw-spoke2



IPv4 CIDR block*

10.2.0.0/16



IPv6 CIDR block

No IPv6 CIDR Block



Amazon provided IPv6 CIDR block

Tenancy

Default



[VPCs > Create VPC](#)

Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You can specify an IPv4 CIDR block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally specify an IPv6 CIDR block.

Name tag

tgw-security



IPv4 CIDR block*

192.168.0.0/16



IPv6 CIDR block

No IPv6 CIDR Block



Amazon provided IPv6 CIDR block

Tenancy

Default



Subnets

Overview

The section covers creating subnets in each of the VPCs. In order to demonstrate cross zone functionality, it is suggested to create the spoke subnets in different zones and security subnets in each of those zones. E.g.

- Spoke 1 - 1 subnet in us-west-2a
- Spoke 2 - 1 subnet in us-west-2b
- Security - 4 subnets each in both us-west-2a and us-west-2b

Process Flow

Procedure 2: Spoke Subnet Creations

Step 1 In the AWS console, open the VPC Service.

Step 2 Select Subnets in the left-hand menu and select the Create Subnet button.

Step 3 Specify a name, the Spoke VPC, AZ and 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 /

Name tag	sn-spoke1-azA	i
VPC*	vpc-04c0c19e2358fe675	i
VPC CIDRs	<input type="text" value="spoke1"/> vpc-04c0c19e2358fe675 tgw-spoke1	Status associated
Availability Zone	us-west-2a	i
IPv4 CIDR block*	10.1.1.0/24	i

Step 4 Select the Create Button and Close to return to the subnets list.

Step 5 Repeat the Process for Spoke 2.

[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 /

Name tag	sn-spoke2-azB	i
VPC*	vpc-057bcf257337d2c17	i
VPC CIDRs	<input type="text" value="spoke2"/> vpc-057bcf257337d2c17 tgw-spoke2	Status associated
Availability Zone	us-west-2b	i
IPv4 CIDR block*	10.2.1.0/24	i

Procedure 3: [Create Security Subnets](#)

The Security VPC contains the following subnets. This section will walk through the first subnet creation. It is up to the reader to create the remaining 7.

Availability Zone A

- MgmtA - 192.168.1.0/24
- UntrustA - 192.168.11.0/24
- TrustA - 192.168.21.0/24
- TGWattachA - 192.168.31.0/24

Availability Zone B

- MgmtB - 192.168.2.0/24
- UntrustB - 192.168.12.0/24
- TrustB - 192.168.22.0/24
- TGWattachB - 192.168.32.0/24

- Step 1** In the AWS console, open the VPC Service.
- Step 2** Select Subnets in the left-hand menu and select the Create Subnet button.
- Step 3** Specify a name, the Security VPC, AZ and 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 .

The screenshot shows the 'Create subnet' wizard. The 'Name tag' field contains 'sn-sec-mgmtA'. The 'VPC*' dropdown is set to 'vpc-0e4b45f63192ed059'. The 'VPC CIDRs' section has a search bar with 'sec' and a dropdown menu showing 'vpc-0e4b45f63192ed059' and 'tgw-security'. The 'Status' is 'associated'. The 'Availability Zone' dropdown is set to 'us-west-2a'. The 'IPv4 CIDR block*' field contains '192.168.1.0/24'.

- Step 4** Select the Create Button and Close to return to the Subnets list.

- Step 5** Repeat the process for the remaining subnets.

After Completion, the reader should have 10 subnets in total.

<input type="checkbox"/> Name	Subnet ID	State	VPC	IPv4 CIDR	Availability Zone
<input type="checkbox"/> sn-sec-mgmtA	subnet-0775dfe210e63f589	available	vpc-0e4b45f63192ed059 tgw-security	192.168.1.0/24	us-west-2a
<input type="checkbox"/> sn-sec-mgmtB	subnet-08b6d0d503dc99401	available	vpc-0e4b45f63192ed059 tgw-security	192.168.2.0/24	us-west-2b
<input type="checkbox"/> sn-sec-tgwattachA	subnet-0f2fe020a6e3952c3	available	vpc-0e4b45f63192ed059 tgw-security	192.168.31.0/24	us-west-2a
<input type="checkbox"/> sn-sec-tgwattachB	subnet-0f23ba1e7f856192f	available	vpc-0e4b45f63192ed059 tgw-security	192.168.32.0/24	us-west-2b
<input type="checkbox"/> sn-sec-trustA	subnet-007f2fb87f35959be	available	vpc-0e4b45f63192ed059 tgw-security	192.168.21.0/24	us-west-2a
<input type="checkbox"/> sn-sec-trustB	subnet-01063f49e71926249	available	vpc-0e4b45f63192ed059 tgw-security	192.168.22.0/24	us-west-2b
<input type="checkbox"/> sn-sec-untrustA	subnet-0eb0b88253b617308	available	vpc-0e4b45f63192ed059 tgw-security	192.168.11.0/24	us-west-2a
<input type="checkbox"/> sn-sec-untrustB	subnet-0ce217c3356e50e82	available	vpc-0e4b45f63192ed059 tgw-security	192.168.12.0/24	us-west-2b
<input type="checkbox"/> sn-spoke1-azA	subnet-0bb505e7f70e5ac73	available	vpc-04c0c19e2358fe675 tgw-spoke1	10.1.1.0/24	us-west-2a
<input type="checkbox"/> sn-spoke2-azB	subnet-0323cd5dcc298f26c	available	vpc-057bcf257337d2c17 tgw-spoke2	10.2.1.0/24	us-west-2b

Transit Gateway

Overview

At this stage, the Transit Gateway has been created along with the attachments. Once the TGW is created, the reader will then be able to create the VPC route tables to establish connectivity to the TGW.

Process Flow

Procedure 4: [Transit Gateway Creation](#)

Step 1 In the AWS console, open the VPC Service.

Step 2 Select Transit Gateways in the left-hand menu and select the Create Transit Gateway button.

- Step 3** Specify a Name and optionally a description. While not required, the reader may wish to disable "Default route table association" and "Default route table propagation". This will prevent undesired association into the security route table.

[Transit Gateways](#) > Create Transit Gateway

Create Transit Gateway

A Transit Gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same account or across accounts.

Name tag i

Description i

Configure the Transit Gateway

Amazon side ASN i

DNS support enable i

VPN ECMP support enable i

Default route table association enable i

Default route table propagation enable i

Configure sharing options for cross account

Auto accept shared attachments enable i

- Step 4** Select the Create Button and Close to return to the Transit Gateways list.

- Step 5** Wait for the TGW to move out of Pending and into the available state before moving on.

Create Transit Gateway		Actions ▼	
🔍 Filter by tags and attributes or search by keyword			
<input type="checkbox"/>	Name	Transit Gateway ID	State
<input type="checkbox"/>	tgw-security	tgw-05125b13e839f07f5	360174888430 available

Procedure 5: **Transit Gateway Route Tables**

- Step 1** In the AWS console, open the VPC Service.
- Step 2** Select Transit Gateway Route Tables in the left-hand menu and select the Create Transit Gateway Route Table button.
- Step 3** Specify a Name and the TGW ID.

[Transit Gateway Route Tables](#) > Create Transit Gateway Route Table

Create Transit Gateway Route Table

A route table controls how traffic flows for all associated attachments.

Name tag	rtb-security	i
Transit Gateway ID*	tgw-05125b13e839f07f5	C
<input type="text" value="sec"/>		
Transit Gateway ID	Name tag	Description
tgw-05125b13e839f07f5	tgw-security	TGW for Security Service Insertion

- Step 4** Select the Create button and the close button to return to Route Table List.
- Step 5** Repeat the process for the Spoke Route table.

[Transit Gateway Route Tables](#) > Create Transit Gateway Route Table

Create Transit Gateway Route Table

A route table controls how traffic flows for all associated attachments.

Name tag	rtb-spoke	i
Transit Gateway ID*	tgw-05125b13e839f07f5	C
<input type="text" value="sec"/>		
Transit Gateway ID	Name tag	Description
tgw-05125b13e839f07f5	tgw-security	TGW for Security Service Insertion

Procedure 6: **Transit Gateway Attachments**

- Step 1** In the AWS console, open the VPC Service.
- Step 2** Select Transit Gateway Attachments in the left-hand menu and select the Create Transit Gateway Attachment button.
- Step 3** Select the Transit Gateway ID and Attachment Type VPC.
- Step 4** Provide a Name and specify the Security VPC ID.
- Step 5** Specify the Attachment Subnets previously created in each zone.

(i) The Subnet IDs will not be visible until after the VPC is selected.

[Transit Gateway Attachments](#) > Create Transit Gateway Attachment

Create Transit Gateway Attachment

Select a Transit Gateway and the type of attachment you would like to create.

Transit Gateway ID*	tgw-05125b13e839f07f	<input type="button" value="C"/>
Attachment type	<input checked="" type="radio"/> VPC <input type="radio"/> VPN	

VPC Attachment

Select and configure your VPC attachment.

Attachment name tag	attach-sec	<input type="button" value="i"/>								
DNS support	<input checked="" type="checkbox"/> enable	<input type="button" value="i"/>								
IPv6 support	<input type="checkbox"/> enable	<input type="button" value="i"/>								
VPC ID*	vpc-0e4b45f63192ed059	<input type="button" value="C"/> <input type="button" value="i"/>								
Subnet IDs*	<input type="button" value="subnet-0f2fe020a6e3952c3"/> <input type="button" value="subnet-0f23ba1e7f856192f"/>									
<table border="1"> <thead> <tr> <th>Availability Zone</th> <th>Subnet ID</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> us-west-2a</td> <td>subnet-0f2fe020a6e3952c3 (sn-sec-tgwattachA)</td> </tr> <tr> <td><input checked="" type="checkbox"/> us-west-2b</td> <td>subnet-0f23ba1e7f856192f (sn-sec-tgwattachB)</td> </tr> <tr> <td><input type="checkbox"/> us-west-2c</td> <td>No subnet available</td> </tr> </tbody> </table>			Availability Zone	Subnet ID	<input checked="" type="checkbox"/> us-west-2a	subnet-0f2fe020a6e3952c3 (sn-sec-tgwattachA)	<input checked="" type="checkbox"/> us-west-2b	subnet-0f23ba1e7f856192f (sn-sec-tgwattachB)	<input type="checkbox"/> us-west-2c	No subnet available
Availability Zone	Subnet ID									
<input checked="" type="checkbox"/> us-west-2a	subnet-0f2fe020a6e3952c3 (sn-sec-tgwattachA)									
<input checked="" type="checkbox"/> us-west-2b	subnet-0f23ba1e7f856192f (sn-sec-tgwattachB)									
<input type="checkbox"/> us-west-2c	No subnet available									

- Step 6** Select the Create Button and Close on the following screen.

Step 7 Repeat the process for the Spoke VPCs.

[Transit Gateway Attachments](#) > Create Transit Gateway Attachment

Create Transit Gateway Attachment

Select a Transit Gateway and the type of attachment you would like to create.

Transit Gateway ID*	tgw-05125b13e839f07f5	
Attachment type	<input checked="" type="radio"/> VPC <input type="radio"/> VPN	

VPC Attachment

Select and configure your VPC attachment.

Attachment name tag	attach-spoke1									
DNS support	<input checked="" type="checkbox"/> enable									
IPv6 support	<input type="checkbox"/> enable									
VPC ID*	vpc-04c0c19e2358fe675	 								
Subnet IDs*	subnet-0bb505e7f70e5ac73									
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Availability Zone</th> <th style="text-align: left;">Subnet ID</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> us-west-2a</td> <td>subnet-0bb505e7f70e5ac73 (sn-spoke1-azA)</td> </tr> <tr> <td><input type="checkbox"/> us-west-2b</td> <td>No subnet available</td> </tr> <tr> <td><input type="checkbox"/> us-west-2c</td> <td>No subnet available</td> </tr> </tbody> </table>			Availability Zone	Subnet ID	<input checked="" type="checkbox"/> us-west-2a	subnet-0bb505e7f70e5ac73 (sn-spoke1-azA)	<input type="checkbox"/> us-west-2b	No subnet available	<input type="checkbox"/> us-west-2c	No subnet available
Availability Zone	Subnet ID									
<input checked="" type="checkbox"/> us-west-2a	subnet-0bb505e7f70e5ac73 (sn-spoke1-azA)									
<input type="checkbox"/> us-west-2b	No subnet available									
<input type="checkbox"/> us-west-2c	No subnet available									

[Transit Gateway Attachments](#) > Create Transit Gateway Attachment

Create Transit Gateway Attachment

Select a Transit Gateway and the type of attachment you would like to create.

Transit Gateway ID*	tgw-05125b13e839f07f5	
Attachment type	<input checked="" type="radio"/> VPC <input type="radio"/> VPN	

VPC Attachment

Select and configure your VPC attachment.

Attachment name tag	attach-spoke2									
DNS support	<input checked="" type="checkbox"/> enable									
IPv6 support	<input type="checkbox"/> enable									
VPC ID*	vpc-057bcf257337d2c17	 								
Subnet IDs*	subnet-0323cd5dcc298f26c									
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Availability Zone</th> <th style="text-align: left;">Subnet ID</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> us-west-2a</td> <td>No subnet available</td> </tr> <tr> <td><input checked="" type="checkbox"/> us-west-2b</td> <td>subnet-0323cd5dcc298f26c (sn-spoke2-azB)</td> </tr> <tr> <td><input type="checkbox"/> us-west-2c</td> <td>No subnet available</td> </tr> </tbody> </table>			Availability Zone	Subnet ID	<input type="checkbox"/> us-west-2a	No subnet available	<input checked="" type="checkbox"/> us-west-2b	subnet-0323cd5dcc298f26c (sn-spoke2-azB)	<input type="checkbox"/> us-west-2c	No subnet available
Availability Zone	Subnet ID									
<input type="checkbox"/> us-west-2a	No subnet available									
<input checked="" type="checkbox"/> us-west-2b	subnet-0323cd5dcc298f26c (sn-spoke2-azB)									
<input type="checkbox"/> us-west-2c	No subnet available									

Procedure 7: **Transit Gateway Associations**

- Step 1** In the AWS console, open the VPC Service.
- Step 2** Select Transit Gateway Route Tables in the left-hand menu and select the Spoke Route Table.
- Step 3** In the bottom pane, select the Associations Tab and Select the Create Association Button.

The screenshot shows the AWS VPC service interface. At the top, there are two buttons: 'Create Transit Gateway Route Table' and 'Actions'. Below this is a search bar labeled 'Filter by tags and attributes or search by keyword'. A table lists two route tables: 'rtb-spoke' and 'rtb-security'. The 'rtb-spoke' row has a blue checkbox checked. The table columns are 'Name', 'Transit Gateway route table ID', 'Transit Gateway ID', and 'State'. The 'rtb-spoke' row shows 'tgw-rtb-04e45a9880feeee07d', 'tgw-05125b13e839f07f5', and 'available'. The 'rtb-security' row shows 'tgw-rtb-050af4853f2e27106', 'tgw-05125b13e839f07f5', and 'available'. Below the table, it says 'Transit Gateway Route Table: tgw-rtb-04e45a9880feeee07d'. Underneath, there are tabs for 'Details', 'Associations' (which is highlighted in orange), 'Propagations', 'Routes', and 'Tags'. The 'Create association' button is located below the tabs and is circled in red. Below the tabs, there is another search bar labeled 'Filter by attributes or search by keyword'. At the bottom, it says 'This route table does not have any associated attachments'.

- Step 4** Select the Spoke VPC 1 from the Choose Attachment drop down.

[Transit Gateway Route Tables](#) > Create association

Create association

Associating an attachment to a route table allows traffic to be sent from the attachment to the target route table. An attachment can only be associated with one route table at a time.

Transit Gateway ID	tgw-05125b13e839f07f5								
Transit Gateway route table ID	tgw-rtb-04e45a9880feeee07d								
Choose attachment to associate*	<input type="text" value="tgw-attach-05840181403b9b830"/> ▼ C								
<input type="text" value="spoke1"/> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Attachment ID</th> <th>Name tag</th> <th>Resource ID</th> <th>Resource owner ID</th> </tr> </thead> <tbody> <tr> <td>tgw-attach-05840181403b9b830</td> <td>attach-spoke1</td> <td>vpc-04c0c19e2358fe675</td> <td>360174888430</td> </tr> </tbody> </table>		Attachment ID	Name tag	Resource ID	Resource owner ID	tgw-attach-05840181403b9b830	attach-spoke1	vpc-04c0c19e2358fe675	360174888430
Attachment ID	Name tag	Resource ID	Resource owner ID						
tgw-attach-05840181403b9b830	attach-spoke1	vpc-04c0c19e2358fe675	360174888430						

- Step 5** Select the Create Button and then Close.

- Step 6** Repeat the process for Spoke 2.

Step 7 Wait for both Associations to be "associated" before proceeding.

The screenshot shows the AWS Transit Gateway Route Table Associations tab. At the top, there is a search bar labeled "Filter by tags and attributes or search by keyword". Below it is a table with columns: Name, Transit Gateway route table ID, Transit Gateway ID, and State. Two entries are listed:

Name	Transit Gateway route table ID	Transit Gateway ID	State
rtb-spoke	tgw-rtb-04e45a9880feeee07d	tgw-05125b13e839f07f5	available
rtb-security	tgw-rtb-050af4853f2e27106	tgw-05125b13e839f07f5	available

Below the table, a section titled "Transit Gateway Route Table: tgw-rtb-04e45a9880feeee07d" is shown. It has tabs for Details, Associations (which is selected), Propagations, Routes, and Tags. Under the Associations tab, there are buttons for "Create association" and "Delete association". A search bar is present. Another table lists associations:

Attachment ID	Resource type	Resource ID	State
tgw-attach-05840181403b9b830	VPC	vpc-04c0c19e2358fe675	associated
tgw-attach-041471e816ed92070	VPC	vpc-057bcf257337d2c17	associated

A red circle highlights the word "associated" in the last two rows of the second table.

Step 8 Move to Propagations Tab and select the Create Propagation button.

Step 9 Select the Security VPC in the drop down.

i The reader should note that the Security VPC is now propagated to the Spoke route table and in the subsequent steps the inverse propagation will be performed.

[Transit Gateway Route Tables > Create propagation](#)

Create propagation

Adding a propagation will allow routes to be propagated from an attachment to the target Transit Gateway route table. An attachment can be p

Transit Gateway ID tgw-05125b13e839f07f5

Transit Gateway route table ID tgw-rtb-04e45a9880feee07d

Choose attachment to propagate*	tgw-attach-0cd616e7af8004363	<input type="button" value="C"/>								
<input type="text" value="sec"/> <table border="1"> <thead> <tr> <th>Attachment ID</th> <th>Name tag</th> <th>Resource ID</th> <th>Resource owner ID</th> </tr> </thead> <tbody> <tr> <td>tgw-attach-0cd616e7af8004363</td> <td>attach-sec</td> <td>vpc-0e4b45f63192ed059</td> <td>360174888430</td> </tr> </tbody> </table>			Attachment ID	Name tag	Resource ID	Resource owner ID	tgw-attach-0cd616e7af8004363	attach-sec	vpc-0e4b45f63192ed059	360174888430
Attachment ID	Name tag	Resource ID	Resource owner ID							
tgw-attach-0cd616e7af8004363	attach-sec	vpc-0e4b45f63192ed059	360174888430							

Step 10 Select the Create Propagation button and close on the next screen.

Step 11 Once complete, select the Routes Tab in the bottom pane to verify that the Security VPC route has been propagated.

The screenshot shows the 'Create propagation' step in the AWS Transit Gateway Route Tables interface. It includes fields for 'Transit Gateway ID' (tgw-05125b13e839f07f5), 'Transit Gateway route table ID' (tgw-rtb-04e45a9880feee07d), and a dropdown for 'Choose attachment to propagate' containing 'tgw-attach-0cd616e7af8004363'. A search bar shows 'sec'. Below is a table with columns: Attachment ID, Name tag, Resource ID, and Resource owner ID. The table shows one row: tgw-attach-0cd616e7af8004363, attach-sec, vpc-0e4b45f63192ed059, and 360174888430 respectively.

Transit Gateway Route Table: tgw-rtb-04e45a9880feee07d

Details Associations Propagations **Routes** Tags

The table below will return a maximum of 1000 routes.

Create route Replace route Delete route

Filter by attributes or search by keyword

CIDR	Attachment	Resource type	Route type	Route state
192.168.0.0/16	tgw-attach-0cd616e7af8004363 vpc-0e4b45f63192ed059	VPC	propagated	active

Step 12 In this use case, all Outbound traffic will flow through the firewalls. A manual route is necessary to handle that traffic.

Step 13 Select the Create Route button. Specify 0.0.0.0/0 for the CIDR and the Security Attachment.

[Transit Gateway Route Tables](#) > Create route

Create route

Add a static route to your Transit Gateway route table.

Transit Gateway ID tgw-05125b13e839f07f5

Transit Gateway route table ID tgw-rtb-04e45a9880feee07d

CIDR* 0.0.0.0/0 

Blackhole 

Choose attachment tgw-attach-0cd616e7af8004363 

Attachment ID	Resource ID	Name tag	Resource owner ID	Association route table
tgw-attach-0cd616e7af8004363	vpc-0e4b45f63192ed059	attach-sec	360174888430	tgw-rtb-050af4853f2e27106

Step 14 Select the Create Button and verify the newly created route.

[Create Transit Gateway Route Table](#) Actions ▾

 Filter by tags and attributes or search by keyword

<input type="checkbox"/> Name	Transit Gateway route table ID	Transit Gateway ID	State
<input checked="" type="checkbox"/> rtb-spoke	tgw-rtb-04e45a9880feee07d	tgw-05125b13e839f07f5	available
<input type="checkbox"/> rtb-security	tgw-rtb-050af4853f2e27106	tgw-05125b13e839f07f5	available

Transit Gateway Route Table: tgw-rtb-04e45a9880feee07d

Details Associations Propagations **Routes** Tags

The table below will return a maximum of 1000 routes.

[Create route](#) [Replace route](#) [Delete route](#)

 Filter by attributes or search by keyword

<input type="checkbox"/> CIDR	Attachment	Resource type	Route type	Route state
<input type="checkbox"/> 0.0.0.0/0	tgw-attach-0cd616e7af8004363 vpc-0e4b45f63192ed059	VPC	static	active
<input type="checkbox"/> 192.168.0.0/16	tgw-attach-0cd616e7af8004363 vpc-0e4b45f63192ed059	VPC	propagated	active

Step 15 Repeat Process for the security route table for both spoke VPCs.

Filter by tags and attributes or search by keyword

	Name	Transit Gateway route table ID	Transit Gateway ID	State
<input type="checkbox"/>	rtb-spoke	tgw-rtb-04e45a9880feee07d	tgw-05125b13e839f07f5	available
<input checked="" type="checkbox"/>	rtb-security	tgw-rtb-050af4853f2e27106	tgw-05125b13e839f07f5	available

Transit Gateway Route Table: tgw-rtb-050af4853f2e27106

Details Associations **Associations** Propagations Routes Tags

Create association Delete association

Filter by attributes or search by keyword

	Attachment ID	Resource type	Resource ID	State
<input type="checkbox"/>	tgw-attach-0cd616e7af8004363	VPC	vp-0e4b45f63192ed059	associated

	Name	Transit Gateway route table ID	Transit Gateway ID	State
<input type="checkbox"/>	rtb-spoke	tgw-rtb-04e45a9880feee07d	tgw-05125b13e839f07f5	available
<input checked="" type="checkbox"/>	rtb-security	tgw-rtb-050af4853f2e27106	tgw-05125b13e839f07f5	available

Transit Gateway Route Table: tgw-rtb-050af4853f2e27106

Details Associations **Propagations** Routes Tags

Create propagation Delete propagation

Filter by attributes or search by keyword

	Attachment ID	Resource type	Resource ID	State
<input type="checkbox"/>	tgw-attach-041471e816ed92070	VPC	vp-057bcf257337d2c17	enabled
<input type="checkbox"/>	tgw-attach-05840181403b9b830	VPC	vp-04c0c19e2358fe675	enabled

	Name	Transit Gateway route table ID	Transit Gateway ID	State
<input type="checkbox"/>	rtb-spoke	tgw-rtb-04e45a9880feee07d	tgw-05125b13e839f07f5	available
<input checked="" type="checkbox"/>	rtb-security	tgw-rtb-050af4853f2e27106	tgw-05125b13e839f07f5	available

Transit Gateway Route Table: tgw-rtb-050af4853f2e27106

Details Associations Propagations **Routes** Tags

The table below will return a maximum of 1000 routes.

Create route Replace route Delete route

Filter by attributes or search by keyword

	CIDR	Attachment	Resource type	Route type	Route state
<input type="checkbox"/>	10.1.0.0/16	tgw-attach-05840181403b9b830 vp-04c0c19e2358fe675	VPC	propagated	active
<input type="checkbox"/>	10.2.0.0/16	tgw-attach-041471e816ed92070 vp-057bcf257337d2c17	VPC	propagated	active

Step 16 Both route tables should now have their corresponding attachments and route to the opposing VPC attachments.

VPC Route Tables

Overview

With the attachments now created in the VPC, the guide will step through the necessary route table creations in each of the VPCs.

Procedure 8: [Security VPC Internet Gateway](#)

Step 1 In the AWS console, open the VPC Service.

Step 2 Select Internet Gateways in the left-hand menu and select the Create internet gateway button.

Step 3 Specify a name for the IGW.

[Internet gateways](#) > Create internet gateway

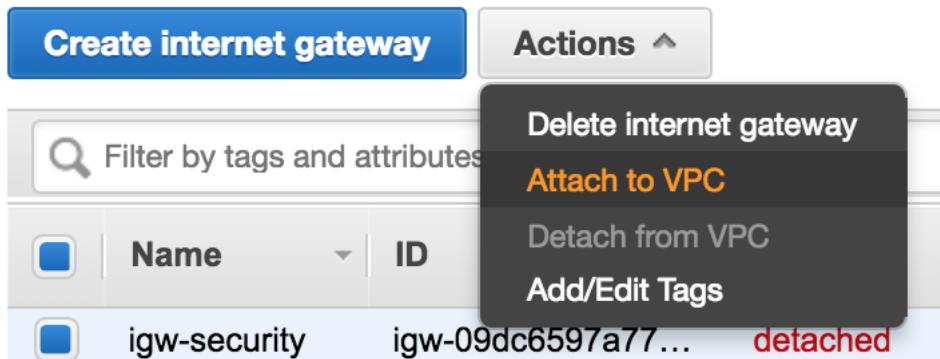
Create internet gateway

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway, enter a name and then click Create.

Name tag	igw-security	i
* Required		

Step 4 Select the Create and button and close on the following screen.

Step 5 Highlight the newly created Internet Gateway, select the Actions dropdown and Attach to VPC.



- Step 6** Select the security VPC from the dropdown and hit the Attach button.

[Internet gateways](#) > Attach to VPC

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*	vpc-0e4b45f63192ed059	
<input type="text" value="security"/>		
AWS Command Line	VPC ID	Name
* Required	vpc-0e4b45f63192ed059	tgw-security

Procedure 9: Spoke Route Tables

- Step 1** In the AWS console, open the VPC Service.

- Step 2** Select Route Tables in the left-hand menu and select the Create route table button.

- Step 3** Provide a name and Select Spoke 1.

[Route Tables](#) > Create route table

Create route table

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

Name tag	rt-spoke1	
VPC*	vpc-04c0c19e2358fe675	
<input type="text" value="spoke1"/>		
* Required	vpc-04c0c19e2358fe675	tgw-spoke1

- Step 4** Select the Create button and close on the following screen.

- Step 5** Repeat the process for Spoke 2.

[Route Tables](#) > Create route table

Create route table

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

Name tag	rt-spoke2	
VPC*	vpc-057bcf257337d2c17	
<input type="text" value="spoke2"/>		
* Required	vpc-057bcf257337d2c17	tgw-spoke2

Step 6 Select rt-spoke1 and select the Route tab in the bottom pane.

The screenshot shows the AWS Lambda console with the 'CreateSpoke' function selected. The 'Configuration' tab is active. The 'Handler' field is set to 'lambda_function.lambda_handler'. The 'Role' dropdown is set to 'Lambda execution role (aws-lambda-execution-role)'. The 'Code' section shows the S3 location 'arn:aws:s3:::palo-alto-networks-aws-transit-gateway-manual-build/lambda-create-spoke.zip'. The 'Environment' section shows the variable 'TGW_ID' with the value 'tgw-05125b13e839f07f5'. The 'Layers' section lists the 'AWS Lambda Layer Version' layer. The 'Triggers' section shows a CloudWatch Logs trigger named 'CloudWatchLogsLogGroup'. The 'Logs' section shows the log group 'arn:aws:logs:us-east-1:123456789012:log-group:/aws/lambda/CreateSpoke' with a log entry: '2019-07-16T14:45:12+00:00 -> {"level": "INFO", "message": "Lambda function CreateSpoke triggered by CloudWatchLogsLogGroup"}'.

Step 7 Select the Edit route button and Add Route on the following screen.

Step 8 Specify 0.0.0.0/0 as the Destination and the TGW Attachment as the Target.
[Edit routes](#)

The screenshot shows the AWS Lambda console with the 'CreateSpoke' function selected. The 'Configuration' tab is active. The 'Handler' field is set to 'lambda_function.lambda_handler'. The 'Role' dropdown is set to 'Lambda execution role (aws-lambda-execution-role)'. The 'Code' section shows the S3 location 'arn:aws:s3:::palo-alto-networks-aws-transit-gateway-manual-build/lambda-create-spoke.zip'. The 'Environment' section shows the variable 'TGW_ID' with the value 'tgw-05125b13e839f07f5'. The 'Layers' section lists the 'AWS Lambda Layer Version' layer. The 'Triggers' section shows a CloudWatch Logs trigger named 'CloudWatchLogsLogGroup'. The 'Logs' section shows the log group 'arn:aws:logs:us-east-1:123456789012:log-group:/aws/lambda/CreateSpoke' with a log entry: '2019-07-16T14:45:12+00:00 -> {"level": "INFO", "message": "Lambda function CreateSpoke triggered by CloudWatchLogsLogGroup"}'.

Step 9 Select Save Routes and Close on the following screen.

Step 10 Select Subnet Associations from the bottom pane and the Edit subnet associations button.

The screenshot shows the AWS Route Tables page. At the top, there's a search bar labeled "Filter by tags and attributes or search by keyword". Below it is a table with columns: Name, Route Table ID, Explicitly Associated with, and Main. Five rows are listed: rt-spoke1 (selected), rt-spoke2, rt-spoke3, rt-spoke4, and rt-spoke5. The "Explicitly Associated with" column shows "-" for all rows except rt-spoke1, which has "rtb-089bb9eadf24d1cda". The "Main" column shows "Yes" for rt-spoke1, rt-spoke3, and rt-spoke5; "No" for rt-spoke2; and "-" for rt-spoke4. Below the table, it says "Route Table: rtb-089bb9eadf24d1cda". Underneath, there are tabs: Summary, Routes, Subnet Associations (which is highlighted with a yellow background), Route Propagation, and Tags. The "Edit subnet associations" button is located within the Subnet Associations tab and is circled in red. At the bottom, there are dropdown menus for Subnet ID, IPv4 CIDR, and IPv6 CIDR.

Step 11 Select the Spoke subnet and Save.

[Edit subnet associations](#)

The screenshot shows the "Edit subnet associations" dialog for route table "rtb-089bb9eadf24d1cda (rt-spoke1)". At the top, it says "Route table rtb-089bb9eadf24d1cda (rt-spoke1)". Below that, it says "Associated subnets subnet-0bb505e7f70e5ac73". The main area is a table with columns: Subnet ID, IPv4 CIDR, IPv6 CIDR, and Current Route Table. One row is shown: subnet-0bb505e7f70e5ac73 | sn-spoke1... 10.1.1.0/24 - Main. There's also a search bar at the top of this table.

Step 12 Repeat the Process for Route Table of Spoke 2.

Procedure 10: Security VPC Route Tables

- Step 1 In the AWS console, open the VPC Service.
- Step 2 Select Route Tables in the left-hand menu and select the Create route table button.
- Step 3 Specify an Outbound Name as this will be the Internet facing route table and select the Security VPC.

[Route Tables](#) > [Create route table](#)

Create route table

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

Name tag: rt-outbound

VPC*: vpc-0e4b45f63192ed059

* Required

Filter: sec

vpc-0e4b45f63192ed059	tgw-security
-----------------------	--------------

- Step 4 Select the Create button and Close on the following screen.
- Step 5 Highlight the newly created route table, select the Route tab in the bottom pane.

Name	Route Table ID	Explicitly Associated with	Main	VPC ID	Owner
rtb-025b31a5409a38d80	-	-	Yes	vpc-04c0c19e2358fe675 ...	360174888430
rt-outbound	rtb-0272583625eb1d5cc	-	No	vpc-0e4b45f63192ed059 ...	360174888430
rt-spoke1	rtb-089bb9eadf24d1cda	subnet-0bb505e7f70e5ac73	No	vpc-04c0c19e2358fe675 ...	360174888430
rt-spoke2	rtb-08a2faf3cc7d817a7	subnet-0323cd5dcc298f26c	No	vpc-057bcf257337d2c17 ...	360174888430
rtb-09175d4db2f93e1b9	-	-	Yes	vpc-057bcf257337d2c17 ...	360174888430
rtb-094c2fd3f470c598d	-	-	Yes	vpc-0e4b45f63192ed059 ...	360174888430

Route Table: rtb-0272583625eb1d5cc

Summary **Routes** Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
192.168.0.0/16	local	active	No

- Step 6** Specify 0.0.0.0/0 as the destination and the previously created IGW as the Target.

[Route Tables](#) > Edit routes

Edit routes

Destination	Target	Status
192.168.0.0/16	local	active
0.0.0.0/0	igw-09dc6597a777b3991	

Add route

igw-09dc6597a777b3991 igw-security

- Step 7** Select the Save button and close on the following screen.

- Step 8** Highlight the Outbound Route table, select Subnet Associations in the bottom pane and select Edit subnet Associations.

Create route table Actions ▾

Filter by tags and attributes or search by keyword

Name	Route Table ID	Explicitly Associated with	Main
rtb-025b31a5409a38d80	-	Yes	
rt-outbound	rtb-0272583625eb1d5cc	-	No
rt-spoke1	rtb-089bb9eadf24d1cda	subnet-0bb505e7f70e5ac73	No
rt-spoke2	rtb-08a2faf3cc7d817a7	subnet-0323cd5dcc298f26c	No
	rtb-09175d4db2f93e1b9	-	Yes
	rtb-094c2fd3f470c598d	-	Yes

Route Table: rtb-0272583625eb1d5cc

Subnets Routes Subnet Associations Route Propagation Tags

Edit subnet associations

You do not have any subnet associations.

Step 9 Select the Management and Untrust subnets and hit the Save button.

[Route Tables](#) > Edit subnet associations

Edit subnet associations

Route table rtb-0272583625eb1d5cc (rt-outbound)

Associated subnets [subnet-0eb0b88253b617308](#) [subnet-0ce217c3356e50e82](#) [subnet-0775dfe210e63f589](#) [subnet-08b6d0d503dc99401](#)

Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
subnet-08b6d0d503dc99401 sn-sec-mgmtB	192.168.2.0/24	-	Main
subnet-0775dfe210e63f589 sn-sec-mgmtA	192.168.1.0/24	-	Main
subnet-007f2fb87f35959be sn-sec-trustA	192.168.21.0/24	-	Main
subnet-0ce217c3356e50e82 sn-sec-untrustB	192.168.12.0/24	-	Main
subnet-0f23ba1e7fb56192f sn-sec-tgwattachB	192.168.32.0/24	-	Main
subnet-0f2fe020a6e3952c3 sn-sec-tgwattachA	192.168.31.0/24	-	Main
subnet-0eb0b88253b617308 sn-sec-untrustA	192.168.11.0/24	-	Main
subnet-01063f49e71926249 sn-sec-trustB	192.168.22.0/24	-	Main

Step 10 Select the Create route table button. The route targeting the TGW will now be created.

Step 11 Specify a name and select the Security VPC.

[Route Tables](#) > Create route table

Create route table

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

Name tag	rt-toTGW	i
VPC*	vpc-0e4b45f63192ed059	C i
* Required	<input type="text" value="sec"/> <div style="border: 1px solid #ccc; padding: 2px;"> vpc-0e4b45f63192ed059 tgw-security </div>	

Step 12 Select the Create button and Close on the following screen.

Step 13 Highlight the route table for the TGW, Select Routes in the bottom pane and select the Edit routes button.

[Route Tables](#) > Edit routes

Edit routes

Destination	Target	Status
192.168.0.0/16	local	active
10.0.0.0/8	tgw-05125b13e839f07f5	
Add route	tgw-05125b13e839f07f5	attach-sec

Step 14 Select the Save routes button and Close on the following screen.

Step 15 Highlight the route table for the TGW, Select Subnet Associations in the bottom pane and select the Edit subnet associations button.

Step 16 Select the Trust subnets.

[Route Tables](#) > [Edit subnet associations](#)

Edit subnet associations

Route table rtb-083214417cbc0a976 (rt-toTGW)

Associated subnets [subnet-01063f49e71926249](#) [subnet-007f2fb87f35959be](#)

<input type="checkbox"/>	Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
<input type="checkbox"/>	subnet-08b6d0d503dc99401 sn-sec-mgmtB	192.168.2.0/24	-	rtb-0272583625eb1d5cc
<input type="checkbox"/>	subnet-0775dfe210e63f589 sn-sec-mgmtA	192.168.1.0/24	-	rtb-0272583625eb1d5cc
<input checked="" type="checkbox"/>	subnet-007f2fb87f35959be sn-sec-trustA	192.168.21.0/24	-	Main
<input type="checkbox"/>	subnet-0ce217c3356e50e82 sn-sec-untrustB	192.168.12.0/24	-	rtb-0272583625eb1d5cc
<input type="checkbox"/>	subnet-0f23ba1e7f856192f sn-sec-tgwattachB	192.168.32.0/24	-	Main
<input type="checkbox"/>	subnet-0f2fe020a6e3952c3 sn-sec-tgwattachA	192.168.31.0/24	-	Main
<input type="checkbox"/>	subnet-0eb088253b617308 sn-sec-untrustA	192.168.11.0/24	-	rtb-0272583625eb1d5cc
<input checked="" type="checkbox"/>	subnet-01063f49e71926249 sn-sec-trustB	192.168.22.0/24	-	Main

Step 17 Select the Save Button.

Firewall Instances

Overview

This section will deploy 2 VM-Series firewalls. One in each Availability Zone. The firewalls will be configured with 3 interfaces: Management, Trust and Untrust.

- ⓘ While the guide does not implement a load balancer for an inbound use case, the guide will perform an interface swap during the build to facilitate inbound if desired. Refer to the follow article for more information.
[Management Interface Mapping](#)
- ⚠ This guide will utilize 4 EIPS. The reader may choose to utilize a Jumpbox to conserve EIPS in lieu of granting EIPs to the Management interfaces. That is outside the scope of this guide.

Procedure 11: [Firewall Creation](#)

- Step 1 In the AWS console, open the EC2 Service.
- Step 2 Select Instances in the left-hand menu and select the Launch Instance button.
- Step 3 Select AWS Marketplace in the left-menu and search for "Palo Alto Networks".
- Step 4 We will select Bundle 2 from the results as this will be short test and it is desirable to have a fully licensed VM-Series firewall. .

(i) Licensing is outside the scope of this guide. For more information please refer to the [Licensing Types](#) page.

Step 1: Choose an Amazon Machine Image (AMI)

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.

Cancel and Exit

Q, Palo Alto Networks|

Quick Start (0)
My AMIs (0)
AWS Marketplace (6)
Community AMIs (280)

Categories
All Categories
Infrastructure Software (5)
Developer Tools (2)

Operating System
Clear Filter
All Linux/Unix
Gentoo (1)
Ubuntu (1)
Other Linux (4)

Software Pricing Plans
Hourly (2)
Annual (2)
Bring Your Own License (4)

Software Free Trial
Free Trial (2)

Region
Current Region (6)
All Regions (24)

VM-Series Next-Generation Firewall Bundle 2
★★★★★ (0) | PAN-OS 8.1.0 Previous versions | By Palo Alto Networks
\$1.29/hr or \$4,500/yr (80% savings) for software + AWS usage fees
Linux/Unix, Other PAN-OS 8.1.0 | 64-bit (x86) Amazon Machine Image (AMI) | Updated: 3/14/18
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. ...
More info

Palo Alto Networks Panorama
★★★★★ (0) | Panorama 8.1.2 Previous versions | By Palo Alto Networks Inc.
Bring Your Own License + AWS usage fees
Linux/Unix, Other 8.1.2 | 64-bit (x86) Amazon Machine Image (AMI) | Updated: 7/29/18
Panorama network security management enables you to control your distributed network of our firewalls from one central location. View all your firewall traffic, manage all aspects ...
More info

VM-Series Next-Generation Firewall Bundle 1
★★★★★ (1) | PAN-OS 8.1.0 Previous versions | By Palo Alto Networks
\$0.86/hr or \$3,000/yr (80% savings) for software + AWS usage fees
Linux/Unix, Other PAN-OS 8.1.0 | 64-bit (x86) Amazon Machine Image (AMI) | Updated: 3/14/18
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. ...
More info

VM-Series Next-Generation Firewall (BYOL)
★★★★★ (1) | PAN-OS 8.1.0 Previous versions | By Palo Alto Networks
Bring Your Own License + AWS usage fees
Linux/Unix, Other PAN-OS 8.1.0 | 64-bit (x86) Amazon Machine Image (AMI) | Updated: 3/12/18
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. ...
More info

Select

Select

Select

Select

Step 5 Select Continue on the Marketplace/EULA page.

◆ If this is the first PayGo based deployment of the AWS account, the reader will be required to accept the EULA before proceeding.

Step 6 If this is not a capacity-based testing environment, the default size for the region will be sufficient. This guide was built in US-West-2, using an m4-xlarge instance. . Select the Configure Instance Details button.

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	m4.large	2	8	EBS only	Yes	Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	m4.xlarge	4	16	EBS only	Yes	High	Yes
<input type="checkbox"/>	General purpose	m4.2xlarge	8	32	EBS only	Yes	High	Yes
<input type="checkbox"/>	General purpose	m4.4xlarge	16	64	EBS only	Yes	High	Yes

Cancel Previous **Review and Launch** Next: Configure Instance Details

Step 7 On the Configure Instance Details screen, perform the following configuration outside of the defaults.

- (1) Number of Instances: 1
- (2) Network: Security VPC
- (3) Subnet: UntrustA NOTE: Interface Swap will be performed.
- (4) Auto-assign Public IP: Disable
- (5) Network Interfaces. Add Device. Specify MGMTA
- (6) Expand Advanced Details and paste the following into the User Date field As Text
 - (a) mgmt-interface-swap=enable

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 t

Number of instances	<input type="text" value="1"/>	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-0e4b45f63192ed059 tgw-security	Create new VPC
Subnet	subnet-0eb0b88253b617308 sn-sec-untrustA us- 251 IP Addresses available	Create new subnet
Auto-assign Public IP	<input type="button" value="Disable"/>	
Placement group	<input type="checkbox"/> Add instance to placement group.	
Capacity Reservation	Open Create new Capacity Reservation	
IAM role	None Create new IAM role	
CPU options	<input type="checkbox"/> Specify CPU options	
Shutdown behavior	<input type="button" value="Stop"/>	
Stop - Hibernate behavior	<input type="checkbox"/> Enable hibernation as an additional stop behavior	
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>	
Elastic Inference	<input type="checkbox"/> Add an Elastic Inference accelerator <small>Additional charges apply.</small>	

The screenshot shows the 'Network interfaces' section with two entries: eth0 and eth1. Both have 'Auto-assign' selected. A message box states: 'We can no longer assign a public IP address to your instance' because multiple network interfaces are specified. The 'Advanced Details' section shows a user data input field containing 'mgmt-interface-swap=enable'.

Step 8 Select the Add Storage Button, no changes are necessary.

Step 9 Select the Add Tags Button. The Reader could optionally add tags here such a Name.

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

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 tags](#)

Key (127 characters maximum)	Value (255 characters maximum)
Name	sec-FW1
Add another tag (Up to 50 tags maximum)	

Step 10 Select the Configure Security Groups Button. Modify the Create a New Security Group Parameters to Allow All Traffic from 0.0.0.0/0 as this will be the Untrust SG. The guide will walk the reader through Management Lock down subsequently.

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 access your 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. [Learn more about Amazon EC2 security groups](#).

Assign a security group:	<input checked="" type="radio"/> Create a new security group	<input type="radio"/> Select an existing security group		
Security group name:	AllowAll			
Description:	Allow Allow to Untrust			
Type	Protocol	Port Range	Source	Description
All traffic	All	0 - 65535	Custom 0.0.0.0/0	e.g. SSH for Admin
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.				

Step 11 Select Review and Launch.

Step 12 Review the parameters and select the Launch button.

Step 13 Either Create a new key pair or Select an existing key pair as necessary. Select Launch Instances.

Step 14 Repeat the process deploying a Second Firewall into the corresponding Subnets in the second Availability Zone.

Step 15 While the firewalls are deploying. Select Security Groups from the left-hand menu. Select Create Security Group button.

Step 16 Add 2 rules with a Source of My IP for HTTPS and SSH.

Create Security Group

Security group name	AllowMgmt
Description	Management access to the firewall.
VPC	vpc-0e4b45f63192ed059 tgw-security

Security group rules:

Inbound Outbound

Type	Protocol	Port Range	Source
HTTPS	TCP	443	My IP
SSH	TCP	22	My IP

Add Rule

Step 17 Select Instances from the left-hand menu and highlight the Firewall.

Step 18 Select Description in Bottom Pane, ETH1 and then select the link to the ENI.

Instance ID	i-020f7cf7215bc7dae	Public DNS (IPv4)	-
Instance state	running	IPv4 Public IP	-
Instance type	m4.xlarge	IPv6 IPs	-
Elastic IPs		Private DNS	ip-192-168-11-118.us-west-2.compute.internal
Availability zone	us-west-2a	Private IPs	192.168.1.39, 192.168.11.118
Security groups	AllowAll, view inbound rules, view outbound rules	VPC ID	vpc-0e4b45f63192ed059
Scheduled events	No scheduled events	Subnet ID	subnet-0eb0b88253b617308
AMI ID	PA-VM-AWS-8.1.0-8736f7a7-35b2-4e03-a8eb-6a749a987428-ami-28669055.4 (ami-9a29b8e2)	Network interfaces	eth0 eth1
Platform	-	Source/dest. check	T2/T3 Unlimited
IAM role	-	EBS-optimized	-
Key pair name	aws-oregon	Root device type	Root device
Owner	360174888430	Block devices	-
Launch time	January 7, 2019 at 12:38:47 PM UTC-5 (less than one hour)	Elastic Graphics ID	-
Termination protection	False	Elastic Inference accelerator ID	-
Lifecycle	normal	Capacity Reservation	-
Monitoring	basic	Priority Reservation Options	-
Alarm status	None		
Kernel ID	-		
DALM ID	-		

Network Interface eth1

Interface ID	eni-034999489fca66ef8
VPC	vpc-0e4b45f63192ed059
Attachment Owner	System
Attachment Status	attached
Attachment Time	Mon Jan 07 12:38:47 GMT-500 2019
Delete on Terminate	true
Private IP Address	192.168.1.39

Step 19 This will navigate to the Network Interfaces menu. Select Actions in the Dropdown and Change Security groups.

Step 20 Select the newly created AllowMgmt security group and save.

Change Security Groups

Network Interface eni-034999489fca66ef8

Security groups

Selected groups: sg-08a4615a902fd94cc

Step 21 Return to the Instance and select the link for ETH0 which is the Untrust interface.

Step 22 In the Actions Dropdown, select Change Source/Dest Check.

Step 23 Disable Source/Dest. Check and save.

Change Source/Dest. Check

Network Interface eni-0130aa689a9b52275

Source/dest. check

Enabled
Disabled

Step 24 Repeat the Security Group assignment and source/dest check on the second firewall.

Procedure 12: Trust Interface creation

- Step 1** In the AWS console, open the EC2 Service.
- Step 2** Select Network Interfaces in the left-hand menu and select the Create Network Interface button.
- Step 3** Provide a description of the interface, specify the Trust Subnet in Availability Zone A and specify the Allow All Security Group.

Create Network Interface

Description	<input type="text" value="Trust vnic FW1"/>
Subnet	<input type="text" value="subnet-007f2fb87f35959be us-west-2a sn-sec-trustA"/>
Private IP	<input type="text" value="auto assign"/>
Security groups	<input type="checkbox"/> sg-0fc6e3984ac9f24cc - AllowAll <input type="checkbox"/> sg-08a4615a902fd94cc - AllowMgmt <input type="checkbox"/> sg-034044acafda78918 - default

- Step 4** Select Yes, Create.
- Step 5** Highlight the newly created Interface, hit the Actions Dropdown and Select Change Source/Dest. Check. Set check to Disabled and Save.

Change Source/Dest. Check

Network Interface	eni-06e46e0486374d725
Source/dest. check	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

- Step 6** With the interface still highlighted, select the Actions dropdown and Attach.
- Step 7** Select FW1 from the Dropdown and Attach.

Attach Network Interface

Network Interface:	eni-06e46e0486374d725
Instance ID:	<input type="text" value="i-020f7cf7215bc7dae - sec-FW1 (running)"/>

- Step 8** Repeat the Network Interface Process for the second firewall.

Procedure 13: Elastic IP Addresses

- Step 1** In the AWS console, open the EC2 Service.
- Step 2** Select Elastic IPs in the left-hand menu and select the Allocate new address button.
- Step 3** Accept the defaults and hit the Allocate button and Close in the following screen.

[Addresses](#) > Allocate new address

Allocate new address

Allocate a new Elastic IP address by selecting the scope in which it will be used

Scope VPC 

IPv4 address pool Amazon pool
 Owned by me

- Step 4** Repeat this process 3 more times for a total of 4 EIPs.
- Step 5** Select Instances in the left-hand menu and highlight Firewall1.
- Step 6** Select ETH0 in the Description pane and open the ENI link.
- Step 7** Select Actions in the Dropdown and Select Associate Address.
- Step 8** Select one of previously allocated addresses in the Address dropdown and hit the Associate Address button.

Associate Elastic IP Address 

Select the address you wish to associate with eni-0130aa689a9b52275

Address	<input type="text" value="34.208.163.20"/>	
Allow reassociation	<input type="checkbox"/>	
Associate to private IP address	<input type="text" value="192.168.11.118*"/>	

* denotes the primary private IP address

[Cancel](#) [Associate Address](#)

- Step 9** Repeat this process on Firewall 1 ETH1.
- Step 10** Repeat this process on Firewall 2 ETH0.
- Step 11** Repeat this process on Firewall 2 ETH1.

This Procedure will result in both firewalls having EIPs associated with their first two interfaces.

Firewall Configuration

Overview

The reader will now access the firewalls to perform initial configuration and apply policies to allow communications. The firewalls will first be configured with a secure password via ssh. Once completed, the remaining configuration will occur via browser.

Procedure 14: Admin Password

- Step 1** In the AWS console, open the EC2 Service.
- Step 2** Select Instances in the left-hand menu and select FW1.
- Step 3** Select ETH1 in the Description tab of the bottom pane and copy the Public IP address.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (II)
sec-FW1	i-020f7cf7215bc7dae	m4.xlarge	us-west-2a	running	2/2 checks ...	None	
sec-FW2	i-05fbe62bb424145fc	m4.xlarge	us-west-2b	running	2/2 checks ...	None	

Instance: i-020f7cf7215bc7dae (sec-FW1) Elastic IP: 50.112.212.234																																																																																												
<input checked="" type="radio"/> Description <input type="radio"/> Status Checks <input type="radio"/> Monitoring <input type="radio"/> Tags <input type="radio"/> Usage Instructions																																																																																												
<table border="1"> <tr> <td>Instance ID</td><td>i-020f7cf7215bc7dae</td> <td>Public DNS (IPv4)</td><td>-</td> </tr> <tr> <td>Instance state</td><td>running</td> <td>IPv4 Public IP</td><td>34.208.163.20</td> </tr> <tr> <td>Instance type</td><td>m4.xlarge</td> <td>IPv6 IPs</td><td>-</td> </tr> <tr> <td>Elastic IPs</td><td>34.208.163.20* 50.112.212.234*</td> <td>Private DNS</td><td>ip-192-168-11-118.us-west-2.compute.internal</td> </tr> <tr> <td>Availability zone</td><td>us-west-2a</td> <td>Private IPs</td><td>192.168.1.39, 192.168.11.118, 192.168.21.6</td> </tr> <tr> <td>Security groups</td><td>AllowAll, view inbound rules, view outbound rules</td> <td>Secondary private IPs</td><td>-</td> </tr> <tr> <td>Scheduled events</td><td>No scheduled events</td> <td>VPC ID</td><td>vpc-0e4b45f63192ed059</td> </tr> <tr> <td>AMI ID</td><td>PA-VM-AWS-8.1.0-8736f7a7-35b2-4e03-a8eb-6a749a987428-ami-28669055.4 (ami-9a29b8e2)</td> <td>Subnet ID</td><td>subnet-0eb0b88253b617308</td> </tr> <tr> <td>Platform</td><td>-</td> <td>Network interfaces</td><td>eth0 eth1</td> </tr> <tr> <td>IAM role</td><td>-</td> <td>Source/dest. check</td><td>T2/T3 Unlimited</td> </tr> <tr> <td>Key pair name</td><td>aws-oregon</td> <td>EBS-optimized</td><td>-</td> </tr> <tr> <td>Owner</td><td>360174888430</td> <td>Root device type</td><td>Root device</td> </tr> <tr> <td>Launch time</td><td>January 7, 2019 at 12:38:47 PM UTC-5 (less than one hour)</td> <td>Elastic Graphics ID</td><td>-</td> </tr> <tr> <td>Termination protection</td><td>False</td> <td>Capacity Reservation</td><td>-</td> </tr> <tr> <td>Lifecycle</td><td>normal</td> <td>Capacity Reservation Settings</td><td>-</td> </tr> <tr> <td>Monitoring</td><td>basic</td> <td></td><td></td> </tr> <tr> <td>Alarm status</td><td>None</td> <td></td><td></td> </tr> <tr> <td>Kernel ID</td><td>-</td> <td></td><td></td> </tr> <tr> <td>RAM disk ID</td><td>-</td> <td></td><td></td> </tr> <tr> <td>Placement group</td><td>-</td> <td></td><td></td> </tr> <tr> <td>Virtualization</td><td>hvm</td> <td></td><td></td> </tr> <tr> <td>Reservation</td><td>r-08958d6150ec0dea6</td> <td></td><td></td> </tr> <tr> <td>AMI launch index</td><td>0</td> <td></td><td></td> </tr> </table>	Instance ID	i-020f7cf7215bc7dae	Public DNS (IPv4)	-	Instance state	running	IPv4 Public IP	34.208.163.20	Instance type	m4.xlarge	IPv6 IPs	-	Elastic IPs	34.208.163.20* 50.112.212.234*	Private DNS	ip-192-168-11-118.us-west-2.compute.internal	Availability zone	us-west-2a	Private IPs	192.168.1.39, 192.168.11.118, 192.168.21.6	Security groups	AllowAll, view inbound rules, view outbound rules	Secondary private IPs	-	Scheduled events	No scheduled events	VPC ID	vpc-0e4b45f63192ed059	AMI ID	PA-VM-AWS-8.1.0-8736f7a7-35b2-4e03-a8eb-6a749a987428-ami-28669055.4 (ami-9a29b8e2)	Subnet ID	subnet-0eb0b88253b617308	Platform	-	Network interfaces	eth0 eth1	IAM role	-	Source/dest. check	T2/T3 Unlimited	Key pair name	aws-oregon	EBS-optimized	-	Owner	360174888430	Root device type	Root device	Launch time	January 7, 2019 at 12:38:47 PM UTC-5 (less than one hour)	Elastic Graphics ID	-	Termination protection	False	Capacity Reservation	-	Lifecycle	normal	Capacity Reservation Settings	-	Monitoring	basic			Alarm status	None			Kernel ID	-			RAM disk ID	-			Placement group	-			Virtualization	hvm			Reservation	r-08958d6150ec0dea6			AMI launch index	0		
Instance ID	i-020f7cf7215bc7dae	Public DNS (IPv4)	-																																																																																									
Instance state	running	IPv4 Public IP	34.208.163.20																																																																																									
Instance type	m4.xlarge	IPv6 IPs	-																																																																																									
Elastic IPs	34.208.163.20* 50.112.212.234*	Private DNS	ip-192-168-11-118.us-west-2.compute.internal																																																																																									
Availability zone	us-west-2a	Private IPs	192.168.1.39, 192.168.11.118, 192.168.21.6																																																																																									
Security groups	AllowAll, view inbound rules, view outbound rules	Secondary private IPs	-																																																																																									
Scheduled events	No scheduled events	VPC ID	vpc-0e4b45f63192ed059																																																																																									
AMI ID	PA-VM-AWS-8.1.0-8736f7a7-35b2-4e03-a8eb-6a749a987428-ami-28669055.4 (ami-9a29b8e2)	Subnet ID	subnet-0eb0b88253b617308																																																																																									
Platform	-	Network interfaces	eth0 eth1																																																																																									
IAM role	-	Source/dest. check	T2/T3 Unlimited																																																																																									
Key pair name	aws-oregon	EBS-optimized	-																																																																																									
Owner	360174888430	Root device type	Root device																																																																																									
Launch time	January 7, 2019 at 12:38:47 PM UTC-5 (less than one hour)	Elastic Graphics ID	-																																																																																									
Termination protection	False	Capacity Reservation	-																																																																																									
Lifecycle	normal	Capacity Reservation Settings	-																																																																																									
Monitoring	basic																																																																																											
Alarm status	None																																																																																											
Kernel ID	-																																																																																											
RAM disk ID	-																																																																																											
Placement group	-																																																																																											
Virtualization	hvm																																																																																											
Reservation	r-08958d6150ec0dea6																																																																																											
AMI launch index	0																																																																																											
Network Interface eth1 <table border="1"> <tr> <td>Interface ID</td><td>eni-034999489fcfa66ef8</td> </tr> <tr> <td>VPC ID</td><td>vpc-0e4b45f63192ed059</td> </tr> <tr> <td>Attachment Owner</td><td>360174888430</td> </tr> <tr> <td>Attachment Status</td><td>attached</td> </tr> <tr> <td>Attachment Time</td><td>Mon Jan 07 12:38:47 GMT-500 2019</td> </tr> <tr> <td>Delete on Terminate</td><td>true</td> </tr> <tr> <td>Private IP Address</td><td>192.168.1.39</td> </tr> <tr> <td>Private DNS Name</td><td>-</td> </tr> <tr> <td>Public IP Address</td><td>50.112.212.234 </td> </tr> <tr> <td>Source/Dest. Check</td><td>true</td> </tr> <tr> <td>Description</td><td>-</td> </tr> <tr> <td>Security Groups</td><td>AllowMgmt</td> </tr> </table>	Interface ID	eni-034999489fcfa66ef8	VPC ID	vpc-0e4b45f63192ed059	Attachment Owner	360174888430	Attachment Status	attached	Attachment Time	Mon Jan 07 12:38:47 GMT-500 2019	Delete on Terminate	true	Private IP Address	192.168.1.39	Private DNS Name	-	Public IP Address	50.112.212.234	Source/Dest. Check	true	Description	-	Security Groups	AllowMgmt																																																																				
Interface ID	eni-034999489fcfa66ef8																																																																																											
VPC ID	vpc-0e4b45f63192ed059																																																																																											
Attachment Owner	360174888430																																																																																											
Attachment Status	attached																																																																																											
Attachment Time	Mon Jan 07 12:38:47 GMT-500 2019																																																																																											
Delete on Terminate	true																																																																																											
Private IP Address	192.168.1.39																																																																																											
Private DNS Name	-																																																																																											
Public IP Address	50.112.212.234																																																																																											
Source/Dest. Check	true																																																																																											
Description	-																																																																																											
Security Groups	AllowMgmt																																																																																											

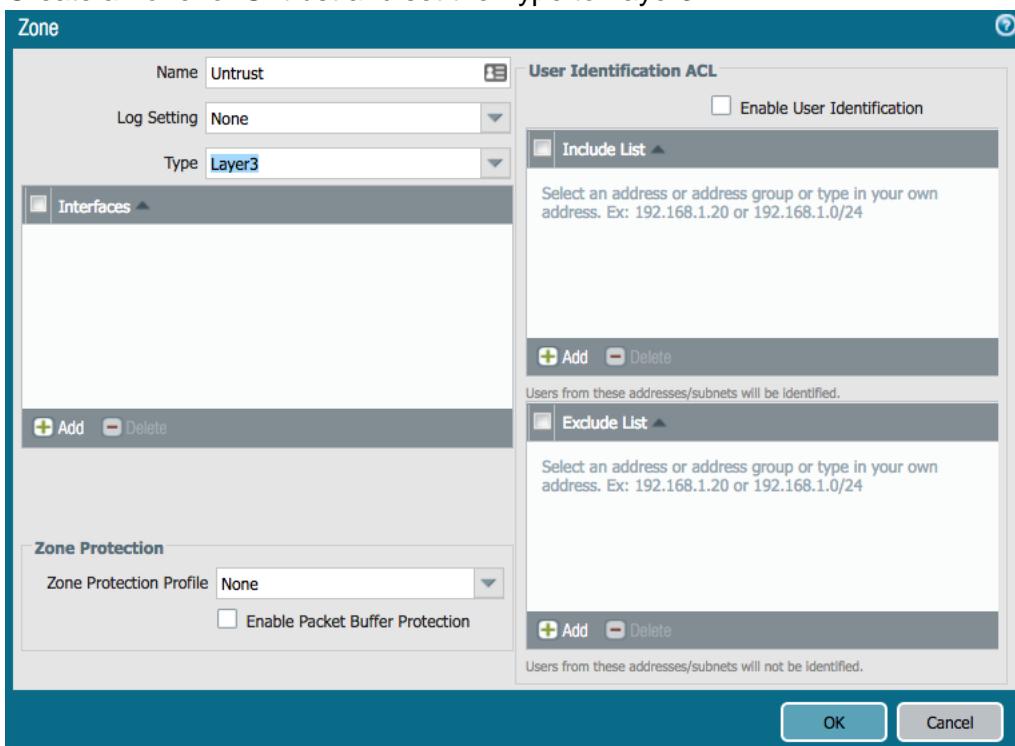
- Step 4** In SSH client of the readers choosing. Connect to the Public IP address specifying the Private Key designated during instance creation and admin as the account. E.g.

(1) `~/.ssh$ ssh -i aws-oregon.pem admin@50.112.212.234`

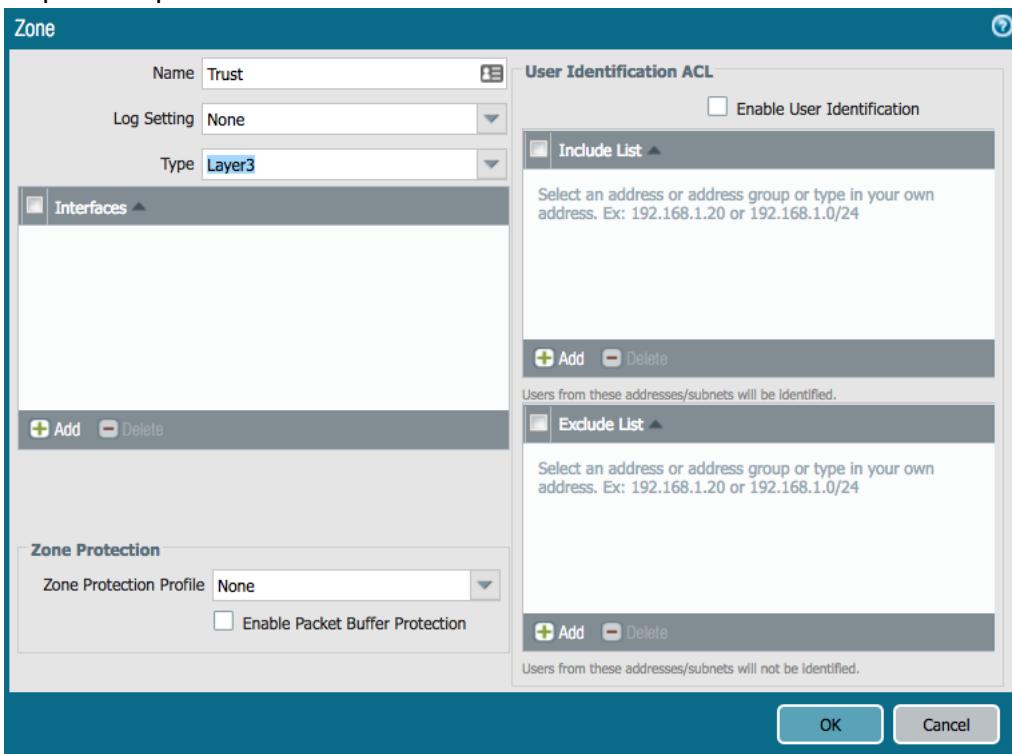
- Step 5 Type 'configure' at the Firewall Command prompt.
- Step 6 To specific the password, use the following command.
 - (1) set mgt-config users admin password
- Step 7 Specify and confirm a security password.
- Step 8 Type 'commit' once the firewall has returned to the command prompt.
- Step 9 Type 'exit' to leave configuration mode, type 'exit' again to end the SSH session.
- Step 10 Repeat this process on FW2.

Procedure 15: Firewall Configuration

- Step 1 Open a New Browser tab and HTTPS to the same IPs addresses used to set the password.
- Step 2 Accept the Self Signed Certificate and login in with Username admin and the password previously configured.
- Step 3 Close the Welcome Message to access the Dashboard.
- Step 4 Access the Network Tab, Zones on the left-hand menu and Select Add at the bottom of the Window.
- Step 5 Create a Zone for Untrust and set the Type to Layer3.

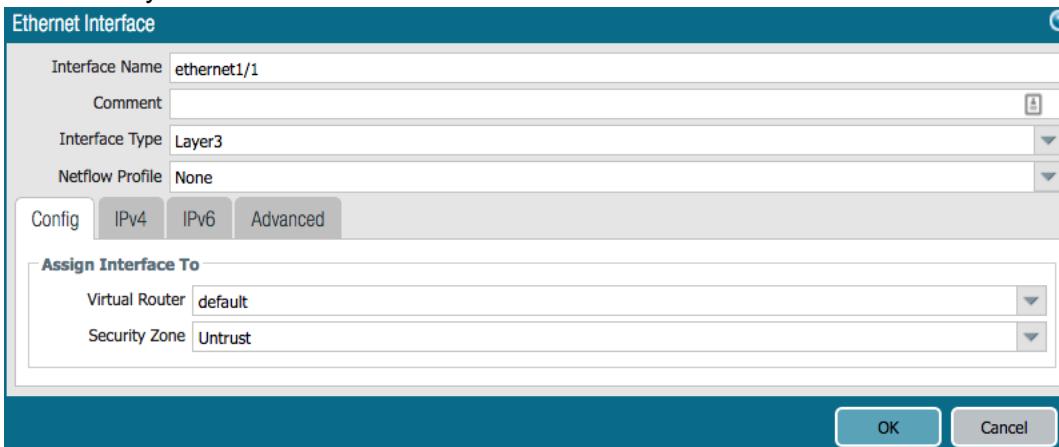


Step 6 Repeat the process for the Trust Zone.

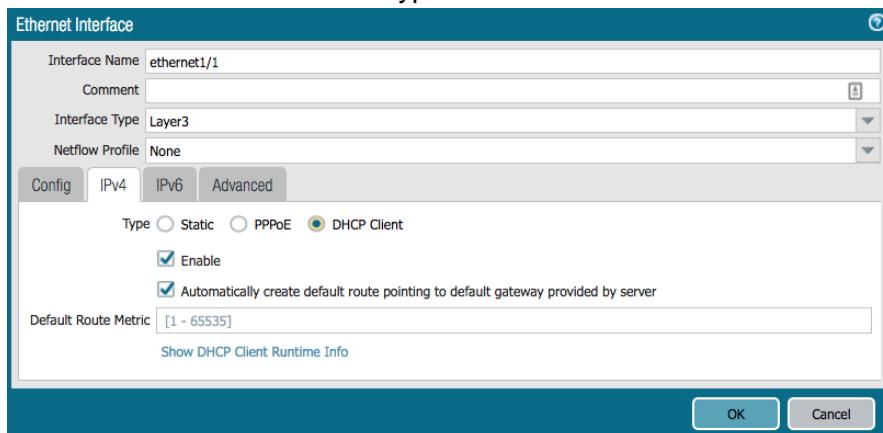


Step 7 Access the Network Tab, Interfaces on the left-hand menu and Select Ethernet 1/1.

Step 8 Set Interface Type to Layer3 and Access the Config Tab. Set the Virtual Router to Default and the Security Zone to Untrust.



Step 9 Access the IPv4 Tab and set type to DHCP.



Step 10 Select OK to Close.

Step 11 Repeat the Process for Ethernet 1/2.

- ① Set the Security Zone to Trust
- ② Uncheck " Automatically create default route pointing to default gateway provided by server" box in the DHCP Settings.

Step 12 Select Virtual Routers in the left-hand menu and open the 'default' VR.

Step 13 Select Static Routes in the left-hand menu and hit the add button.

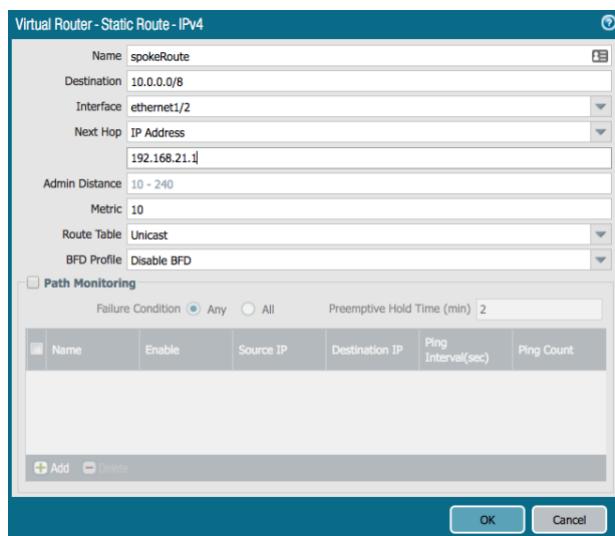
(1) Name: SpokeRoute

(2) Destination: 10.0.0.0/8

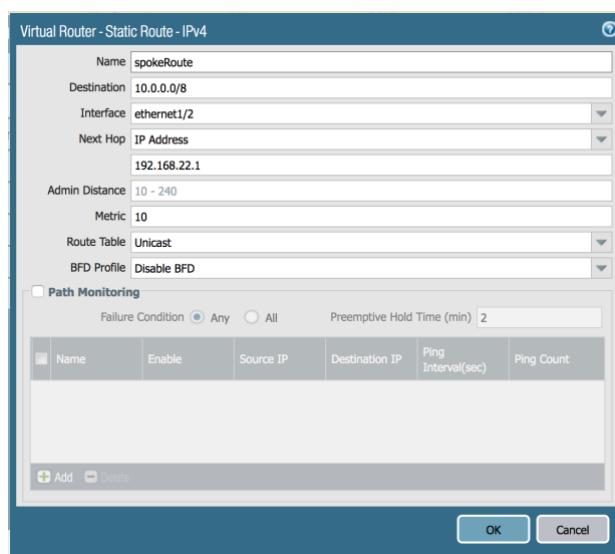
(3) Interface: ethernet1/2

(4) Next Hop: 192.168.2x.1 (Specify the .1 address of the Trust subnet.)

(a) FW1 (next hop = 192.168.21.1)



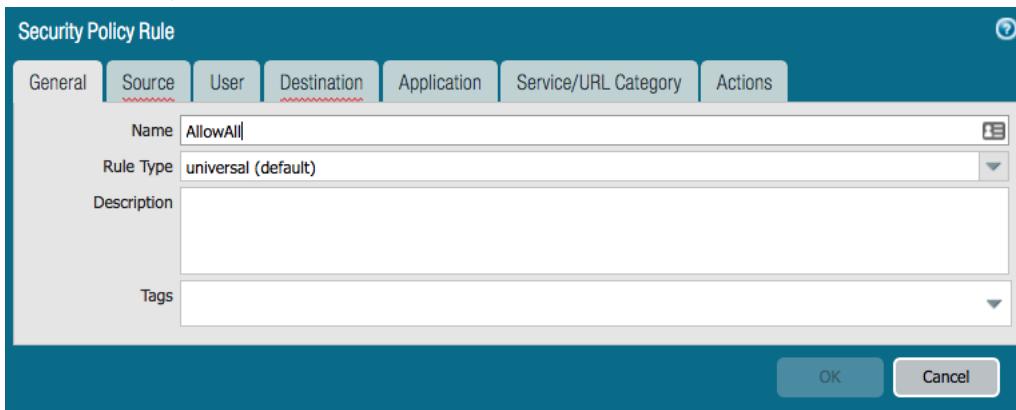
(b) FW2 (next hop = 192.168.22.1)



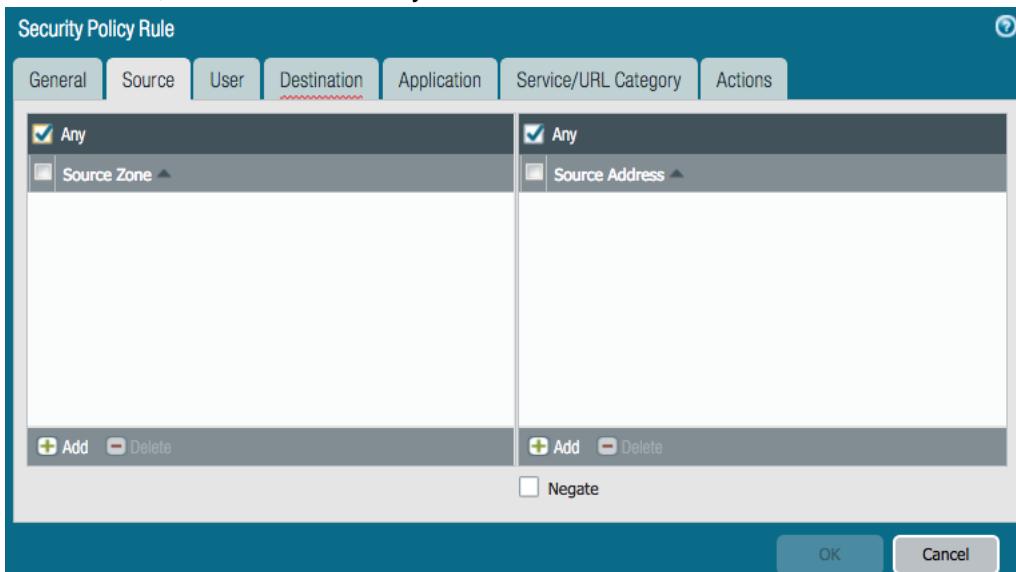
Step 14 Select OK twice to exit.

Step 15 Select the Policies Tab, Security in the left-hand menu and Add in the bottom of the window.

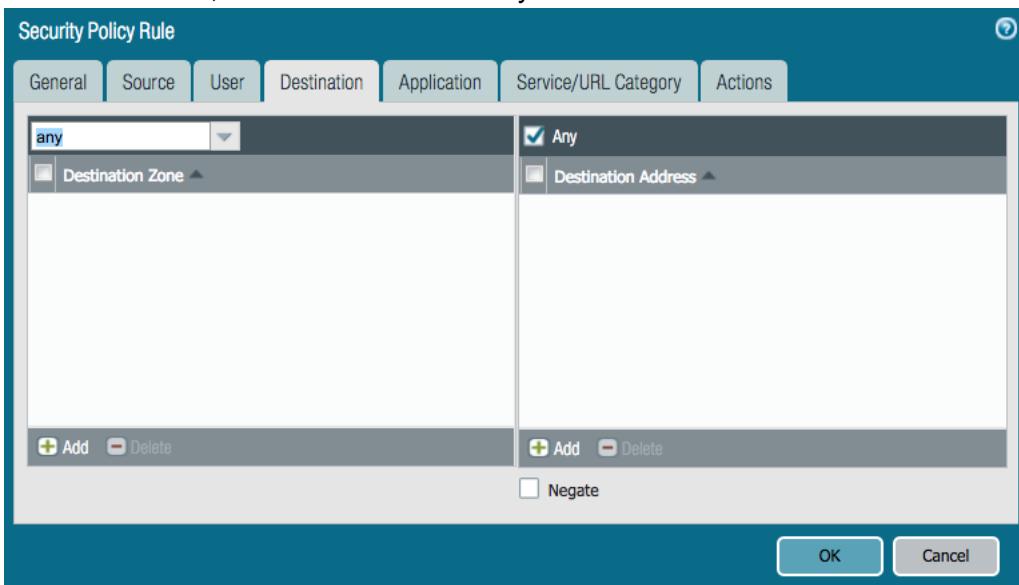
Step 16 General Tab, Name=AllowAll



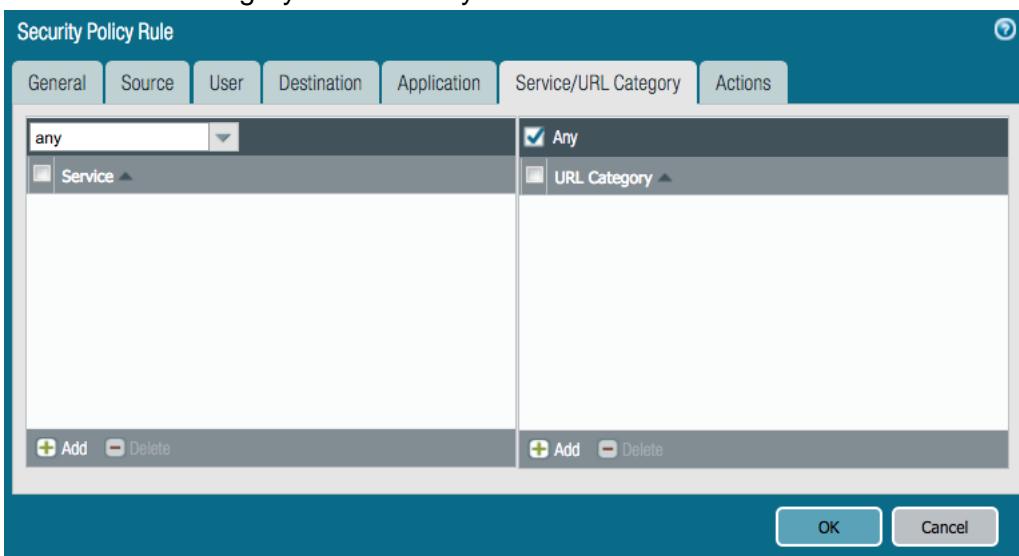
Step 17 Source Tab, Source Zone = Any



Step 18 Destination Tab, Destination Zone = Any



Step 19 Service/URL Category. Service=any

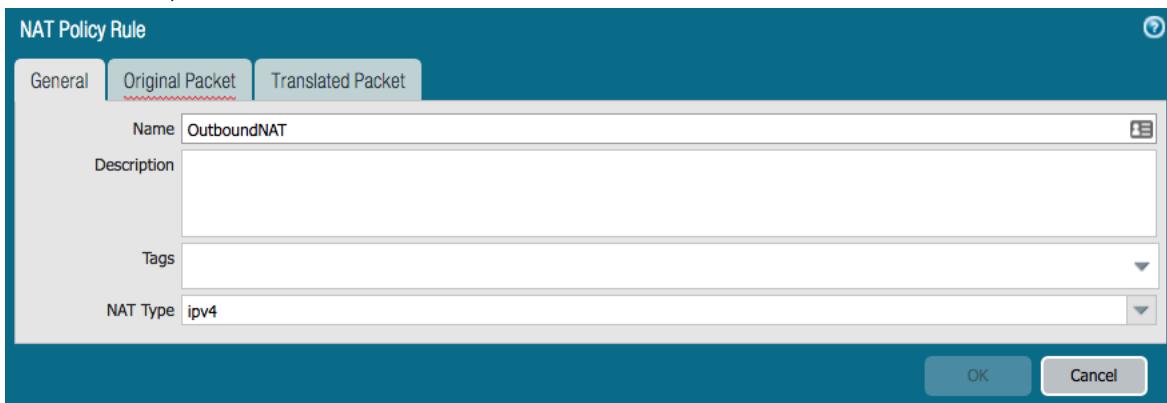


Step 20 Select OK to accept all other defaults.

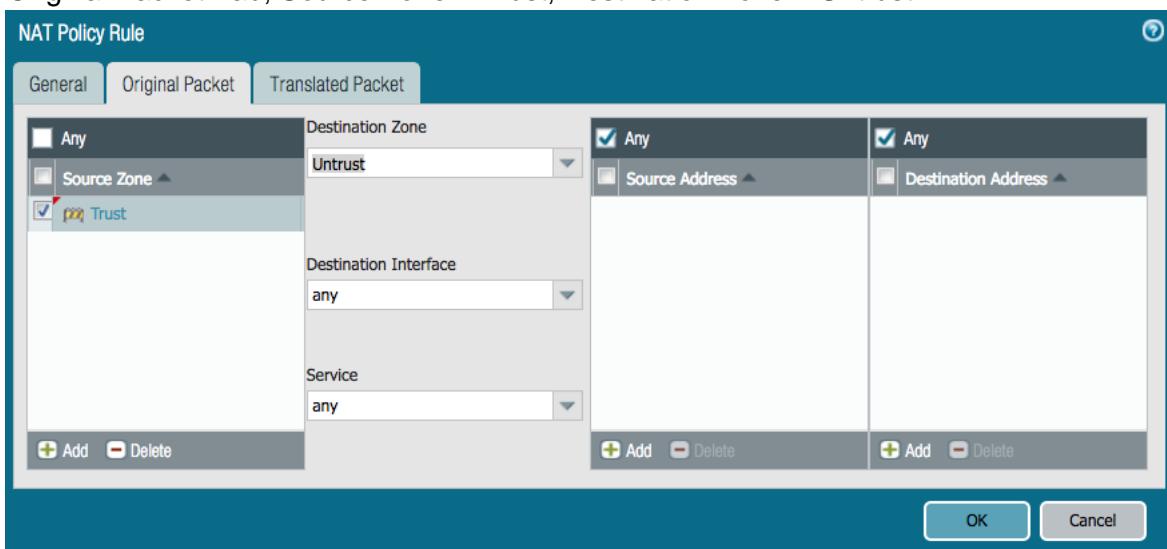
Name	Tags	Type	Source				Destination			Rule Usage			Application	Service	Action
			Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	Hit	Hit Count			
1 AllowAll	none	universal	any	any	any	any	any	any	0	-	-	any	any	Allow	
2 intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	0	-	-	any	any	Allow	
3 interzone-default	none	interzone	any	any	any	any	any	any	0	-	-	any	any	Deny	

Step 21 Select NAT in the left-hand menu and Add button at the bottom of the window.

Step 22 General Tab, Name = OutboundNAT.

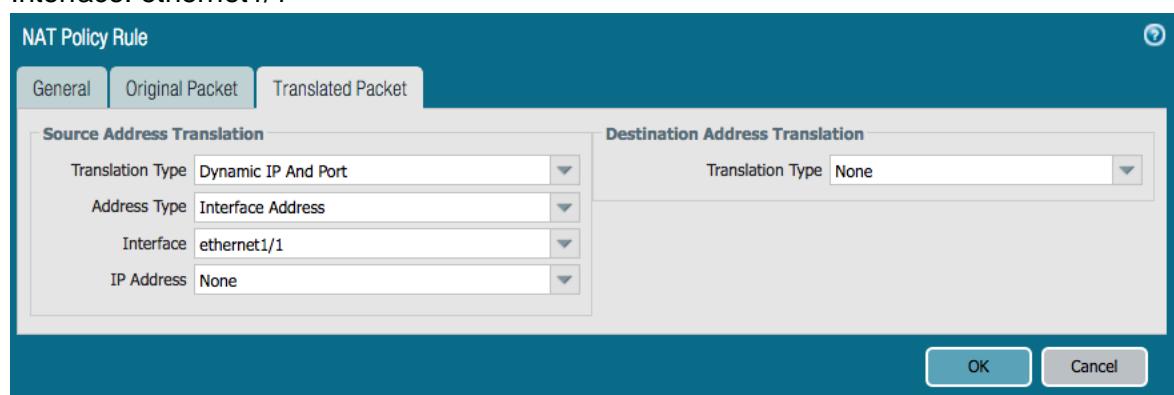


Step 23 Original Packet Tab, Source Zone = Trust, Destination Zone = Untrust.



Step 24 Translated Packet Tab. Source Address Translation.

- (1) Translation Type: Dynamic IP and Port
- (2) Address Type: Interface Address
- (3) Interface: ethernet1/1



Step 25 Select OK.

Step 26 Select Commit and Hit the Commit button.

Step 27 Repeat the Process for Firewall 2.

Route Table Updates

Overview

Now that the firewall ENIs have been created, the VPC Route Tables can be created to direct traffic arriving from the TGW Attachment to the firewalls. While there are different options for routing the East/West and Outbound traffic, this guide will utilize FW1 for East/West and FW2 for Outbound.

Only one firewall is used for East/West routing to eliminate the need to Source NAT.

- (i) This guide does not cover firewall fault tolerance or scaling. Options for fault tolerance including [AWS HA](#) or route update scripting to update the route table in the event of a failure.
- (i) Scaling beyond the throughput of the firewall would involve segmenting spoke traffic toward specific firewalls and is outside the scope of this guide.

Procedure 16: Attachment Route Table

- Step 1 In the AWS console, open the EC2 Service.
- Step 2 Select Instances in the left-hand menu and highlight FW1.
- Step 3 Select ETH2 in the Description Tab and copy the Interface ID.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs
sec-FW1	i-020f7cf7215bc7dae	m4.xlarge	us-west-2a	running	2/2 checks ...	None		34.208.163.20	-
sec-FW2	i-05fbe62bb424145fc	m4.xlarge	us-west-2b	running	2/2 checks ...	None		54.71.246.247	-

Instance: i-020f7cf7215bc7dae (sec-FW1) Elastic IP: 50.112.212.234

Description Status Checks Monitoring Tags Usage Instructions

Instance ID: i-020f7cf7215bc7dae	Public DNS (IPv4): -
Instance state: running	IPv4 Public IP: 34.208.163.20
Instance type: m4.xlarge	IPv6 IPs: -
Elastic IPs: 34.208.163.20* 50.112.212.234*	Private DNS: ip-192-168-11-118.us-west-2.compute.internal
Availability zone: us-west-2a	Private IPs: 192.168.1.39, 192.168.11.118, 192.168.21.6
Security groups: AllowAll, view inbound rules, view outbound rules	Secondary private IPs: vpc-0e4b45f63192ed059
Scheduled events: No scheduled events	Subnet ID: subnet-0eb0b88253b617308
AMI ID: PA-VM-AWS-8.1.0-87367a7-35b2-4e03-a8eb-6a749a987428-ami-28669055.4 (ami-9a29b8e2)	Network interfaces: eth0 eth1 eth2
Platform: -	Source/dest. check: T2/T3 Unlimited
IAM role: -	EBS-optimized: Interface ID: eni-06e46a0486374d725
Key pair name: aws-oregon	VPC ID: vpc-0e4b45f63192ed059
Owner: 360174888430	Root device type: Attachment Owner: 360174888430
Launch time: January 7, 2019 at 12:38:47 PM UTC-5 (2 hours)	Block devices: Attachment Status: attached
Termination protection: False	Elastic Graphics ID: Attachment Time: Mon Jan 07 12:54:57 GMT-500
Lifecycle: normal	Creation Idenitifer: eni-06e46a0486374d725
Monitoring: basic	2019

Network Interface eth2

Interface ID: eni-06e46a0486374d725
VPC ID: vpc-0e4b45f63192ed059
Attachment Owner: 360174888430
Attachment Status: attached
Attachment Time: Mon Jan 07 12:54:57 GMT-500

- Step 4 Paste the contents into text editor.
- Step 5 Repeat for FW2.
- Step 6 In the AWS console, open the VPC Service.

Step 7 Select Route Tables in the left-hand menu and select the Create Route table button.

Step 8 Provide a Name and select the Security VPC.

[Route Tables](#) > Create route table

Create route table

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

Name tag i

VPC* C i

* Required

vpc-0e4b45f63192ed059 tgw-security

Step 9 Select the Create button and Close on the following screen.

Step 10 Highlight the newly created Route Table, select the Routes Tab and hit the Edit Routes button.

Step 11 Add two routes utilizing the previously copied ENI IDs.

(1) 10.0.0.0/8 -> ENI of ETH2 FW1

(2) 0.0.0.0/0 -> ENI of ETH2 FW2

Step 12 Save and Close.

Step 13 Select the Subnet Associations Tab in the bottom pane and hit the Edit Subnet Associations button.

Step 14 Select the TGW Attachment Subnets and hit Save.

[Route Tables](#) > Edit subnet associations

Edit subnet associations

Route table rtb-08156cf2d722d3731 (rt-fromTGW)

Associated subnets

<input type="checkbox"/>	Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
<input type="checkbox"/>	subnet-08b6d0d503dc99401 sn-sec-mgmtB	192.168.2.0/24	-	rtb-0272583625eb1d5cc
<input type="checkbox"/>	subnet-0775dfe210e63f589 sn-sec-mgmtA	192.168.1.0/24	-	rtb-0272583625eb1d5cc
<input type="checkbox"/>	subnet-007f2fb87f35959be sn-sec-trustA	192.168.21.0/24	-	rtb-083214417cbc0a976
<input type="checkbox"/>	subnet-0ce217c3356e50e82 sn-sec-untrustB	192.168.12.0/24	-	rtb-0272583625eb1d5cc
<input checked="" type="checkbox"/>	subnet-0f23ba1e7f856192f sn-sec-tgwattachB	192.168.32.0/24	-	Main
<input checked="" type="checkbox"/>	subnet-0f2fe020a6e3952c3 sn-sec-tgwattachA	192.168.31.0/24	-	Main
<input type="checkbox"/>	subnet-0eb0b88253b617308 sn-sec-untrustA	192.168.11.0/24	-	rtb-0272583625eb1d5cc
<input type="checkbox"/>	subnet-01063f49e71926249 sn-sec-trustB	192.168.22.0/24	-	rtb-083214417cbc0a976

Client Systems

Overview

This section steps the reader through deploying 2 test systems, one in each spoke to perform flow tests and review the traffic in the Firewall Monitor.

Info This guide will use Ubuntu running on free tier instances. The reader may choose to use other systems that are more suitable to the business use case.

Procedure 17: Client System

- Step 1 In the AWS console, open the EC2 Service.
- Step 2 Select Instances in the left-hand menu and select the Launch Instance button.
- Step 3 Search for Ubuntu and select Ubuntu Server 18.04 LTS.
- Step 4 Leave the Free Tier Eligible instance size highlighted and select Configure Instance Details.
- Step 5 In the Network Parameter, specific the Spoke1 VPC and select Add Storage.
- Step 6 Accept the defaults and select Add Tags. Tags are optional, the reader may choose to specific a Name tag.
- Step 7 Select the Configure Security Group button.
- Step 8 The reader will connect to the system with SSH through the firewall. Therefore, a security is necessary to allow SSH.

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 tra create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group:	<input checked="" type="radio"/> Create a new security group	<input type="radio"/> Select an existing security group	
Security group name:	allowssh		
Description:	allowssh		
Type	Protocol	Port Range	Source
SSH	TCP	22	Custom 0.0.0.0/0
Add Rule			

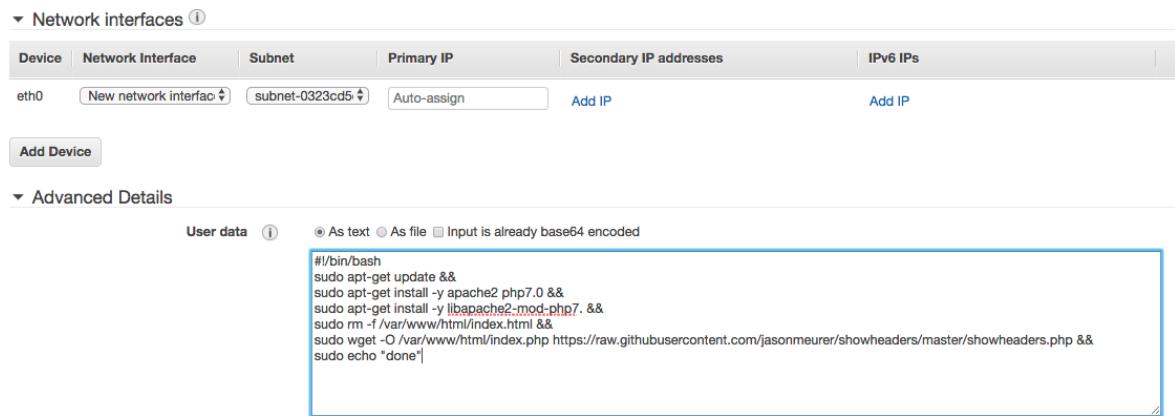
- Step 9 Select the Review and Launch button.
- Step 10 Review the Parameters and select the Launch button.
- Step 11 Specify the correct Key Pair in the pop-up and Launch the Instance.

Procedure 18: Web Server

- Step 1 In the AWS console, open the EC2 Service.
- Step 2 Select Instances in the left-hand menu and select the Launch Instance button.
- Step 3 Search for Ubuntu and select Ubuntu Server 18.04 LTS.
- Step 4 Leave the Free Tier Eligible instance size highlighted and select Configure Instance Details.
- Step 5 In the Network Parameter, specific the Spoke2 VPC.
- Step 6 Expand the Advanced Details Section and paste the following As Text.

 Be careful of word wrap introduced by the document editor specifically on the wget command

```
#!/bin/bash
sudo apt-get update &&
sudo apt-get install -y apache2 php7.0 &&
sudo apt-get install -y libapache2-mod-php7. &&
sudo rm -f /var/www/html/index.html &&
sudo wget -O /var/www/html/index.php
https://raw.githubusercontent.com/jasonmeurer/showheaders/master/showheaders.php &&
sudo echo "done"
```



The screenshot shows the 'Advanced Details' section of the EC2 instance configuration. Under 'User data', the 'As text' radio button is selected. The text input field contains the provided shell script. The 'Advanced Details' section has a blue border around the user data input area.

- Step 7 Add Storage.
- Step 8 Accept the defaults and select Add Tags. Tags are optional, the reader may choose to specific a Name tag.
- Step 9 Select the Configure Security Group button.

Step 10 The reader will connect to the system with SSH through the firewall. Additionally, the website is configured on port 80. Therefore, security rules are necessary to allow SSH and HTTP.

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 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
SSH	TCP	22	Anywhere <input type="text" value="0.0.0.0, ::/0"/>
HTTP	TCP	80	Anywhere <input type="text" value="0.0.0.0, ::/0"/>

Step 11 Select the Review and Launch button.

Step 12 Review the Parameters and select the Launch button.

Step 13 Specify the correct Key Pair in the pop-up and Launch the Instance.

Firewall Configuration - Inbound

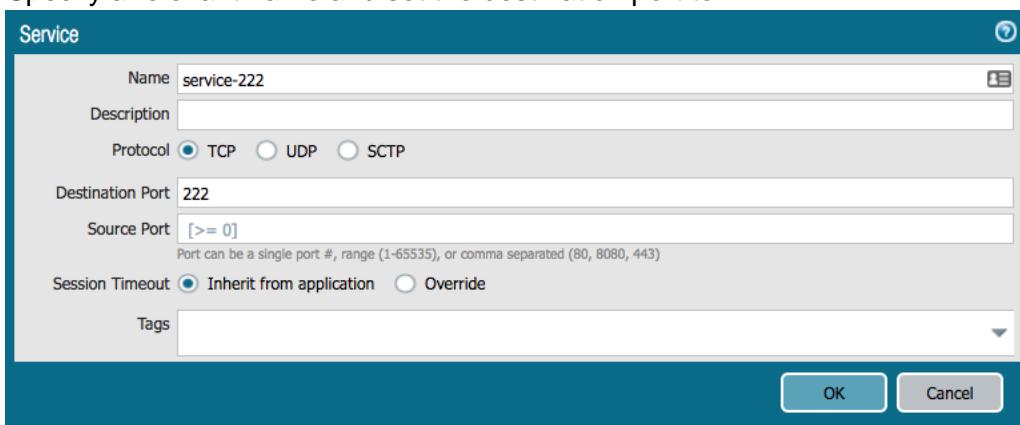
Overview

The test systems do not currently allow for inbound access from the Internet. The reader will now configure an inbound NAT rule through FW1 to allow access to the test client to perform tests.

The NAT policy will perform Port translation from port 222 externally to port 22 on the instance. The reader could create a second NAT policy utilizing a second external port to gain access to the web server.

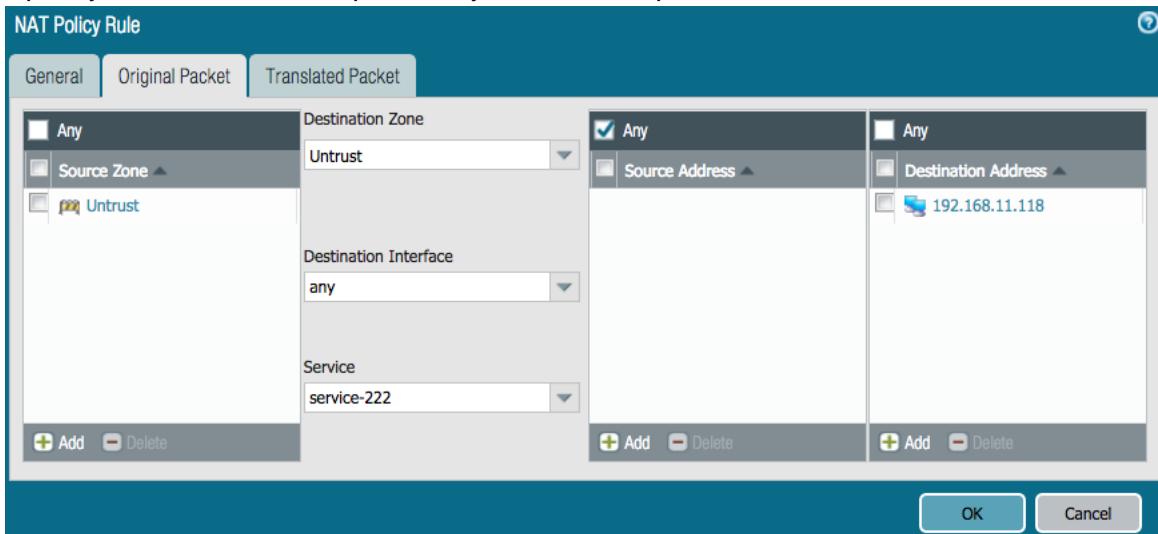
Procedure 19: [Nat Policy Configuration](#)

- Step 1** In the AWS console, open the EC2 Service.
- Step 2** Select Instances in the left-hand menu and highlight client system. Copy the IP address.
- Step 3** Repeat the process for Eth0 of FW1.
- Step 4** Switch to the browser connected to FW1.
- Step 5** Open the Objects Tab, Select Services from the left-hand menu and hit the Add button.
- Step 6** Specify a relevant name and set the destination port to 222.



- Step 7** Open the Policies tab, select NAT in the left-hand menu and hit the Add button at the bottom.
- Step 8** Provide a Rule name such as inboundMgmt.
- Step 9** Move to the Original Packet tab. Set both the Source and Destination Zones to Untrust.
- Step 10** Specify the firewall IP of ETH0 as the Destination Address.

Step 11 Specify the Service as the previously created 222 port.



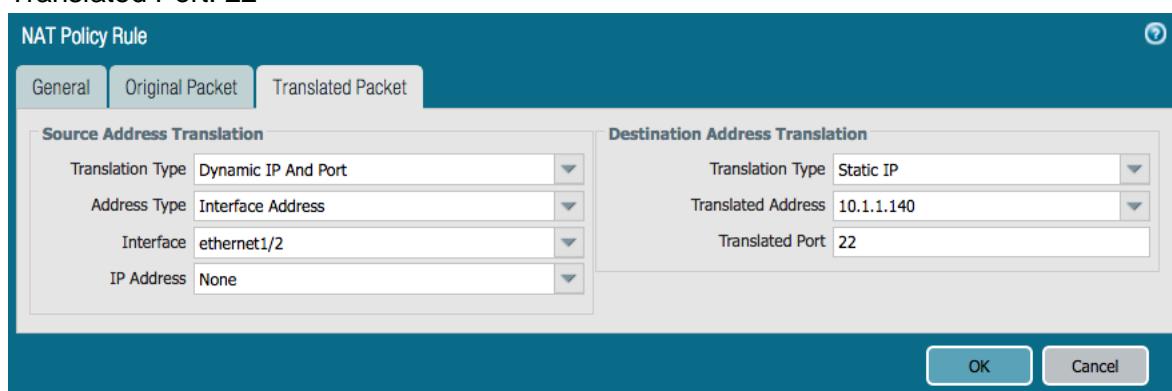
Step 12 Move to the Translated Packet Tab.

Step 13 Source Address Translation

- (1) Translation Type: Dynamic IP and Port
- (2) Address Type: Interface Address
- (3) Interface: ethernet1/2

Step 14 Destination Address Translation

- (1) Translation Type: Static IP
- (2) Translated Address: IP of the client system
- (3) Translated Port: 22



Step 15 Commit the Policy.

Validation

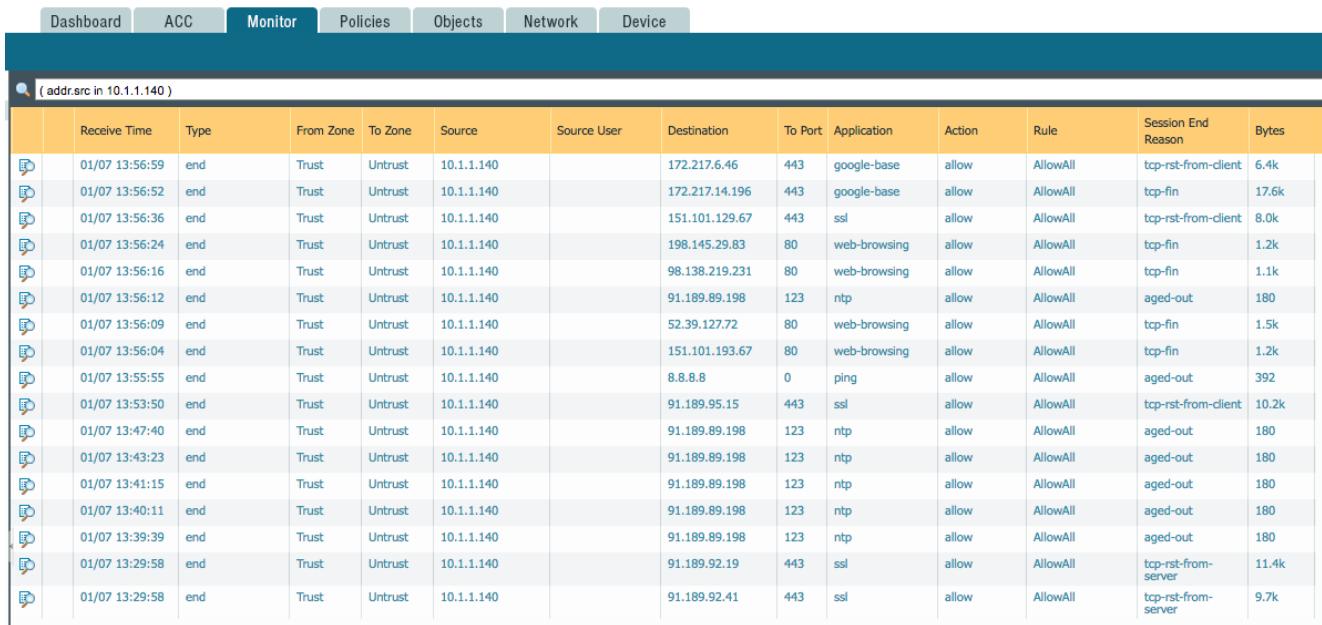
Overview

The reader will now access the client system via SSH to perform both East/West and Outbound testing.

Procedure 20: Access the Client System

- Step 1** In the AWS console, open the EC2 Service.
- Step 2** Select Instances in the left-hand menu and highlight FW1 system. Copy the Public IP of ETH0.
- Step 3** From a terminal window, ssh to the public IP on port 222 utilizing a Username of Ubuntu and the designated key.
 (1) `~/.ssh$ ssh -p 222 -i aws-oregon.pem ubuntu@34.208.163.20`
- Step 4** Once access to the cli has been gained, the reader can test access to Internet and to the web server IP address utilizing the curl command.

Step 5 FW2 - Outbound Traffic



The screenshot shows the Palo Alto Networks Firewall UI with the 'Monitor' tab selected. The title bar indicates the logs are for source IP 10.1.1.140. The table below lists 20 outbound traffic entries:

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
🔗	01/07 13:56:59	end	Trust	Untrust	10.1.1.140		172.217.6.46	443	google-base	allow	AllowAll	tcp-rst-from-client	6.4k
🔗	01/07 13:56:52	end	Trust	Untrust	10.1.1.140		172.217.14.196	443	google-base	allow	AllowAll	tcp-fin	17.6k
🔗	01/07 13:56:36	end	Trust	Untrust	10.1.1.140		151.101.129.67	443	ssl	allow	AllowAll	tcp-rst-from-client	8.0k
🔗	01/07 13:56:24	end	Trust	Untrust	10.1.1.140		198.145.29.83	80	web-browsing	allow	AllowAll	tcp-fin	1.2k
🔗	01/07 13:56:16	end	Trust	Untrust	10.1.1.140		98.138.219.231	80	web-browsing	allow	AllowAll	tcp-fin	1.1k
🔗	01/07 13:56:12	end	Trust	Untrust	10.1.1.140		91.189.89.198	123	ntp	allow	AllowAll	aged-out	180
🔗	01/07 13:56:09	end	Trust	Untrust	10.1.1.140		52.39.127.72	80	web-browsing	allow	AllowAll	tcp-fin	1.5k
🔗	01/07 13:56:04	end	Trust	Untrust	10.1.1.140		151.101.193.67	80	web-browsing	allow	AllowAll	tcp-fin	1.2k
🔗	01/07 13:55:55	end	Trust	Untrust	10.1.1.140		8.8.8.8	0	ping	allow	AllowAll	aged-out	392
🔗	01/07 13:53:50	end	Trust	Untrust	10.1.1.140		91.189.95.15	443	ssl	allow	AllowAll	tcp-rst-from-client	10.2k
🔗	01/07 13:47:40	end	Trust	Untrust	10.1.1.140		91.189.89.198	123	ntp	allow	AllowAll	aged-out	180
🔗	01/07 13:43:23	end	Trust	Untrust	10.1.1.140		91.189.89.198	123	ntp	allow	AllowAll	aged-out	180
🔗	01/07 13:41:15	end	Trust	Untrust	10.1.1.140		91.189.89.198	123	ntp	allow	AllowAll	aged-out	180
🔗	01/07 13:40:11	end	Trust	Untrust	10.1.1.140		91.189.89.198	123	ntp	allow	AllowAll	aged-out	180
🔗	01/07 13:39:39	end	Trust	Untrust	10.1.1.140		91.189.89.198	123	ntp	allow	AllowAll	aged-out	180
🔗	01/07 13:29:58	end	Trust	Untrust	10.1.1.140		91.189.92.19	443	ssl	allow	AllowAll	tcp-rst-from-server	11.4k
🔗	01/07 13:29:58	end	Trust	Untrust	10.1.1.140		91.189.92.41	443	ssl	allow	AllowAll	tcp-rst-from-server	9.7k

Step 6 FW1 - East/West Traffic.

(addr:src in 10.1.1.140)														
	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes	
🔗	01/07 14:01:10	end	Trust	Trust	10.1.1.140		10.2.1.91	22	ssh	allow	AllowAll	tcp-fin	4.1k	
🔗	01/07 13:59:41	end	Trust	Trust	10.1.1.140		10.2.1.91	80	web-browsing	allow	AllowAll	tcp-fin	1.1k	
🔗	01/07 13:59:39	end	Trust	Trust	10.1.1.140		10.2.1.91	80	web-browsing	allow	AllowAll	tcp-fin	1.1k	

For More Information

AWS Transit Gateway

<https://aws.amazon.com/transit-gateway/>

Palo Alto Network Cloud Resources

https://live.paloaltonetworks.com/t5/Cloud-Integration/ct-p/Cloud_Templates