

Transit VPC for AWS



AWS Transit VPC Deployment Guide

How to deploy a two-tiered application environment secured by the VM-Series firewall

<http://www.paloaltonetworks.com>

Table of Contents

Version History	3
1. About.....	4
2. Topology	4
3. Support Policy.....	5
4. Prerequisites	6
5. Create Buckets for Transit VPC	6
6. Initialize the Transit VPC account.....	7
7. Subscribing VPC bucket	12
8. Subscribing VPC deployment options	12
8.1 Option 1: Initialize and launch the subscribing VPC.....	12
8.2 Option 2: Launch a subscriber VPC.....	16
8.3 Option 3: Tag an existing VPC.....	17
9. When everything works	18

Version History

Version number	Comments
1.0	Initial GitHub check-in

1. About

This document will explain how to deploy a Transit VPC solution in AWS. For some more information on what a Transit VPC is and its benefits please refer to this link:

<https://aws.amazon.com/blogs/aws/aws-solution-transit-vpc/>

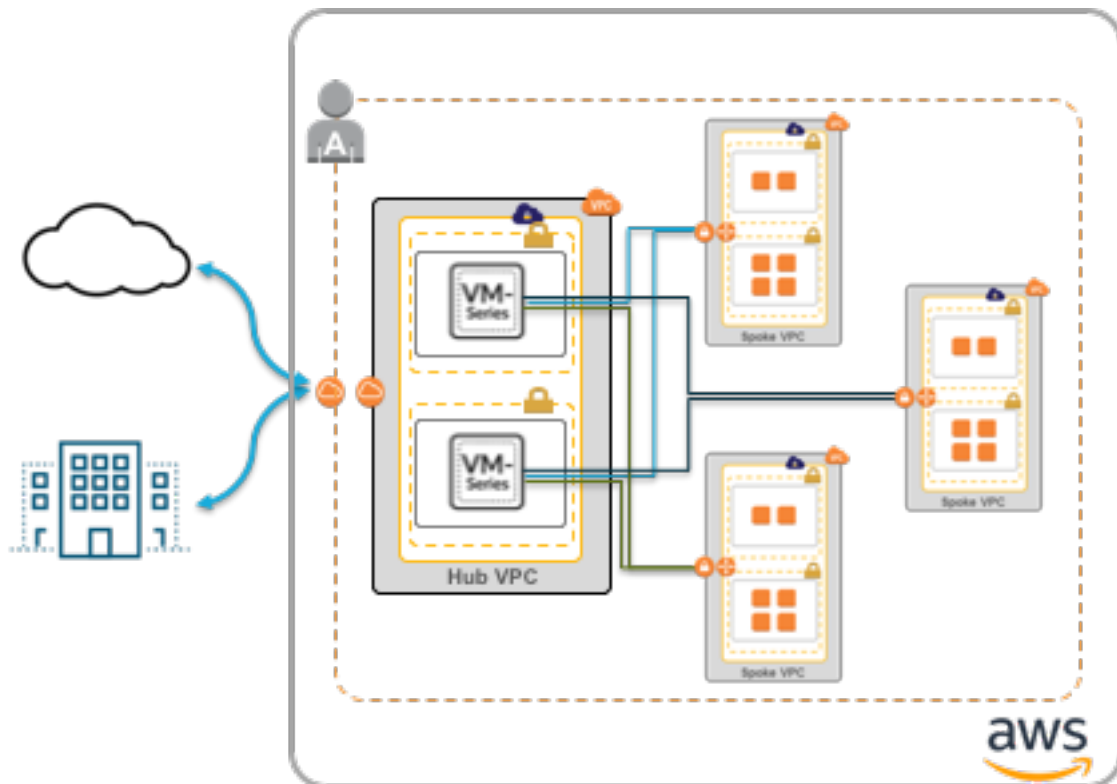
Note: This is a pretty advanced deployment that requires familiarity with AWS and Palo Alto Networks. For a more entry level solution please refer to the following two-tier solution.

<https://github.com/PaloAltoNetworks/aws/tree/master/two-tier-sample>

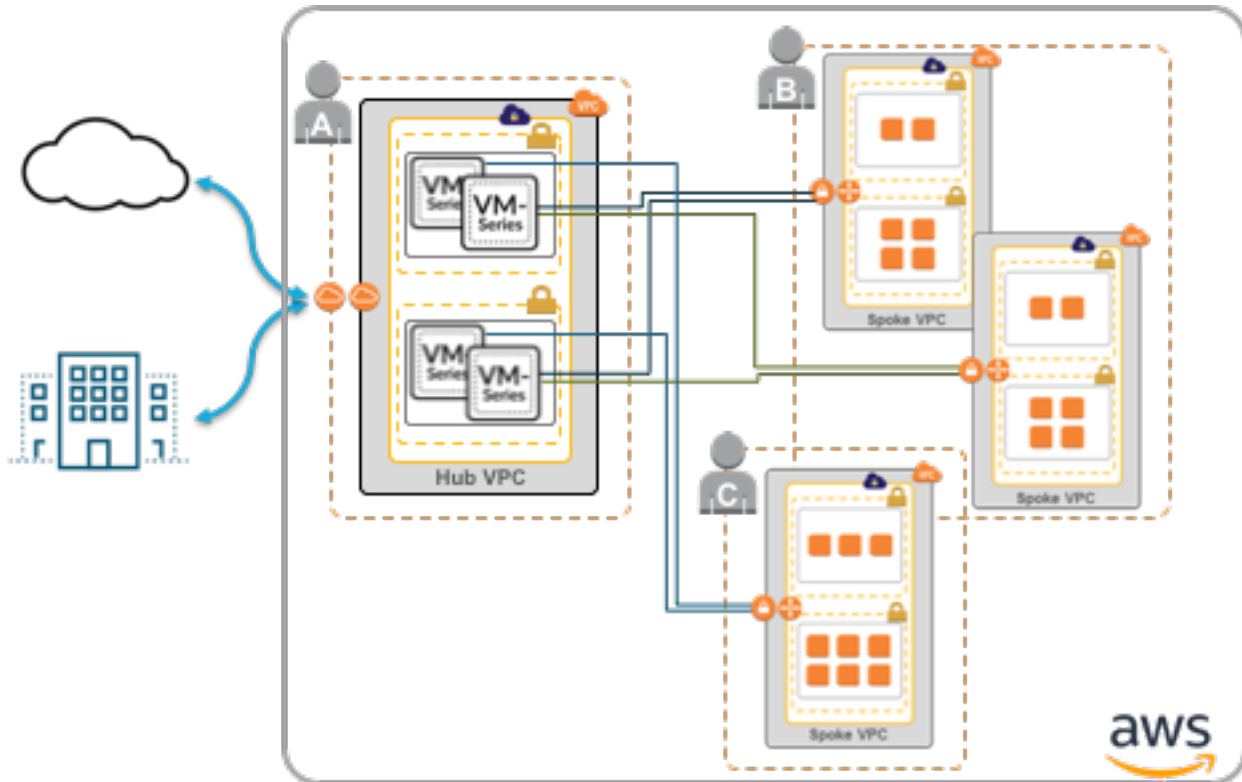
2. Topology

Here is a topology of what will be deployed. The transit VPC solution deploys a classic hub-and-spoke (or spine-leaf) topology.

The solution can be deployed in a single account:



Or across multiple accounts:



A transit VPC can be used to secure outbound traffic to the internet, traffic flowing in-between spoke VPCs and traffic to over a hybrid connection back to corporate.

The solution uses AWS Step Functions and thereby will only run in regions where Step Functions are available. As of writing this document those regions are:

us-east-1 (N. Virginia), us-east-2 (Ohio), us-west-2 (Oregon), ca-central-1 (Canada), eu-west-1 (Ireland), eu-west-2 (London), eu-central-1 (Frankfurt), ap-southeast-1 (Singapore), ap-southeast-2 (Sydney) and ap-northeast-1 (Tokyo).

Please check the following link for a more up to date list: <https://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/>

3. Support Policy

This solution is released under an as-is, best effort, support policy. These scripts should be seen as community supported and Palo Alto Networks will contribute our expertise as and when possible. We do not provide technical support or help in using or troubleshooting the components of the project through our normal support options such as Palo Alto Networks support teams, or ASC (Authorized Support

Centers) partners and backline support options. The underlying product used (the VM-Series firewall) by the scripts or templates are still supported, but the support is only for the product functionality and not for help in deploying or using the template or script itself.

4. Prerequisites

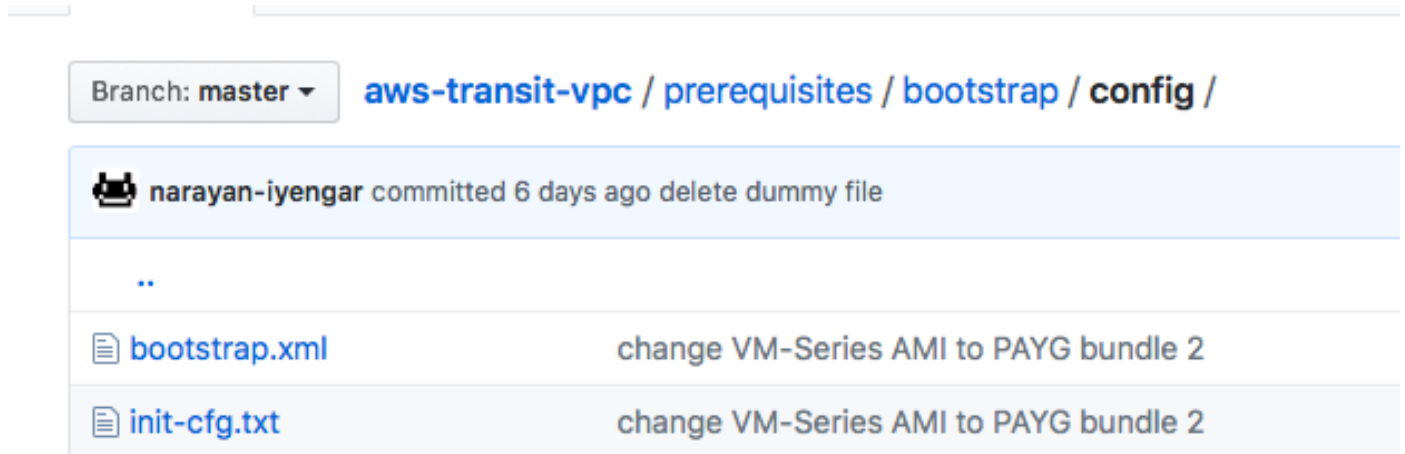
Here are the prerequisites required to successfully launch this template:

1. AWS account
2. Clone or download the files from the following GitHub repository on to your local machine:
<https://github.com/PaloAltoNetworks/aws-transit-vpc>

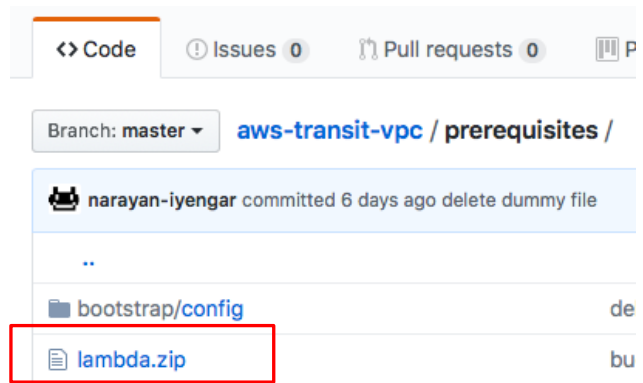
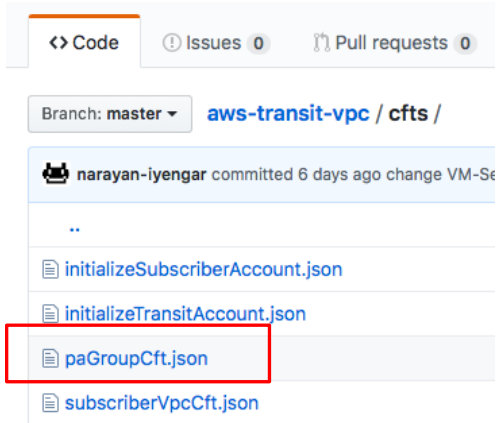
5. Create Buckets for Transit VPC

In the AWS S3 console, create bucket with config, content, license and software folders.

In the config folder in S3 add the bootstrap.xml and init-cfg.txt files from the cloned repositories prerequisites/bootstrap/config folder



Create another bucket in S3 and add the paGroupCft.json and lambda.zip files from the clones repository into this bucket.



Note: The buckets need to be in the same region in which you will deploy the Transit VPC template.

6. Initialize the Transit VPC account

In the AWS CloudFormation console create a new stack and select the `InitializeTransitAccount.json` template and fill in the parameters as follows:

Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation

1 Stack name

Parameters

Required Parameters

2 PaGroupTemplateUrl Palo Alto Cloudformation Template url

3 DeLicenseApiKey PA license deactivation API Key

4 UserName Palo Alto Login User Name

5 Password Palo Alto Login User Password

6 paBootstrapBucketName Existing S3 bucket which is having PA-Bootstrap configuration

7 LambdaFunctionsBucketName Existing S3 bucket name which is having the Lambda funtions zip

8 VpnConfigBucketName
Creates a S3-bucket for VPN Configuration files. NOTE: S3 bucket names are globally unique, regardless of the AWS Region and / creation failure

9 sshKey Search
SSH key to associate with PA Server

az1 us-east-1a
Select AvailabilityZone 1

10

az2 us-east-1b
Select AvailabilityZone 2

Palo Alto Networks Transit VPC Deployment Guide

Default Parameters

11	SubscriberAWSAccountNumber	<input type="text"/>	Subscriber AWS Account number(s) required for Assume Role, Provide comma separated valid 12-digit AWS Account Number account numbers, those accounts no longer subscribed with TransitAccount
12	PaloAltoGroupCapacity	<input type="text" value="4"/>	The Maximum number of VPCs supported for PA-Group
13	LambdaZipFile	<input type="text" value="lambda.zip"/>	Lambda code zip filename which is stored in above mentioned Repository
14	transitVpcCidr	<input type="text" value="10.100.0.0/24"/>	Give the VPC CIDR range to create Transit VPC
15	dmzAz1Cidr	<input type="text" value="10.100.0.0/27"/>	Give the CIDR range to create DMZ Subnet AZ1
	dmzAz2Cidr	<input type="text" value="10.100.0.32/27"/>	Give the CIDR range to create DMZ Subnet AZ2
	pdmzAz1Cidr	<input type="text" value="10.100.0.128/27"/>	Give the CIDR range to create pDMZ Subnet AZ1
	pdmzAz2Cidr	<input type="text" value="10.100.0.160/27"/>	Give the CIDR range to create pDMZ Subnet AZ2
	mgmtAz1Cidr	<input type="text" value="10.100.0.64/27"/>	Give the CIDR range to create MGMT Subnet AZ1
	mgmtAz2Cidr	<input type="text" value="10.100.0.96/27"/>	Give the CIDR range to create MGMT Subnet AZ2
16	trustedSource	<input type="text" value="1.1.1.1/32"/>	Trusted source to allow access to PA MGMT interface
17	NatInstanceType	<input type="text" value="t2.micro"/>	Instance type to use for NAT

1. Name for the stack
2. The URL for where the PaGroupCft.json is located in S3.

Palo Alto Networks Transit VPC Deployment Guide



3. The current solution uses PAYG Bundle 2, so this parameter is not required. You may type in something random.
4. If you are using the supplied bootstrap file, then the username has to be **admin**
5. If you are using the supplied bootstrap file, then the password has to be **ReanCloud123!**

You can load the supplied bootstrap file onto a VM-Series firewall and change the username and password if you desire. Please make sure you upload the new bootstrap file to your bootstrap bucket. And then you can supply the updated username and password whilst launching the template.

6. Bootstrap bucket name.
7. Name of bucket where the paGroupCft.json and lambda.zip files are located.
8. A unique bucket name (to be created) to store VPN config data.
9. Pick an SSH key.
10. Pick the availability zones where the solution will be deployed.
11. Enter the AWS account number where the spoke or subscribing VPC template will be deployed.
12. Enter the maximum number of subscribing VPCs per pair of firewalls. Once the number of subscribing VPCs hits this threshold, a new set of firewalls will be launched and subsequent VPCs will connect to those firewalls.
13. Name of the zip file that contains the lambda code.

Palo Alto Networks Transit VPC Deployment Guide

14. CIDR block of the trasnit VPC

15. The CIDR block of the DMZ (untrust), pDMZ (trust) and Mgmt subnets for both AZs

16. The trusted source from which you want to lock down ssh access to.

17. The instance size for the NAT instance. The default should be fine for most deployments. This NAT instance will be used as a bastion host.

Click through to kick of stack creation.

You should see a stack create complete when the transit VPC account has been successfully initialized.

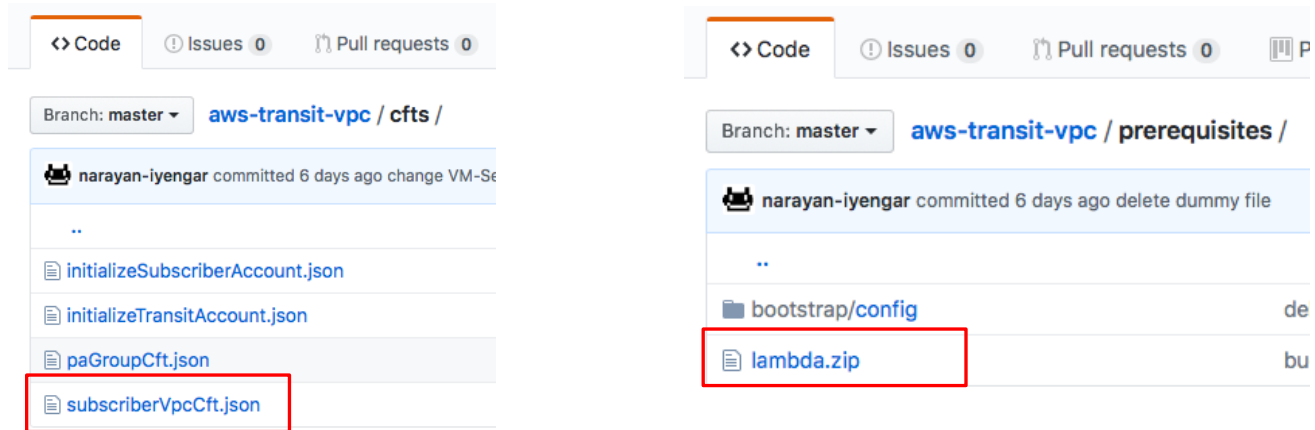
Filter: Active ▾ By Stack Name				
	Stack Name	Created Time	Status	Description
<input checked="" type="checkbox"/>	trasnit-vpc	2018-01-29 13:51:25 UTC-0800	CREATE_COMPLETE	Create Transit VPC

Overview	Outputs	Resources	Events	Template	Parameters	Tags	Stack Policy	Change Sets	Rollback Triggers
Filter by: Status ▾ Search events									
2018-01-29		Status	Type	Logical ID		Status Reason			
▶ 13:54:21 UTC-0800		CREATE_COMPLETE	AWS::CloudFormation::Stack	trasnit-vpc					
▶ 13:54:18 UTC-0800		CREATE_COMPLETE	AWS::CloudFormation::CustomResource	GetGatewayId					
▶ 13:54:17 UTC-0800		CREATE_IN_PROGRESS	AWS::CloudFormation::CustomResource	GetGatewayId		Resource creation Initiated			
▶ 13:54:00 UTC-0800		CREATE IN PROGRESS	AWS::CloudFormation::CustomResource	GetGatewayId					

Note that this will not launch any firewalls or have VPN connections. Firewalls will be auto-launched when the first susbscribing VPC is ready to connect.

7. Subscribing VPC bucket

In the AWS S3 console create a bucket and upload the lambda.zip and subscriberVpcCft.json files into it.



8. Subscribing VPC deployment options

There are three deployment modes you can choose from when deploying the subscribing VPC.

NOTE: The initializeSubscribingAccount.json file has to be run once per subscribing account. The template sets up the necessary cross IAM roles, lambda functions and DyanmoDB tables necessary for the subscribing VPC to be launched and connected to the transit VPC successfully.

NOTE: The solution will not resolve VPC CIDR conflicts. So you have to be aware of susbcribing VPCs CIDR ranges and make sure they do not overlap with each other.

8.1 Option 1: Initialize and launch the subscribing VPC

In the AWS CloudFormation console, create a new stack and select the initializeSubscriberAccount.json template and fill in the parameters as follows:

Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the

1 **Stack name**

Parameters

Required Parameters

2 **TransitSNSTopicArn** Transit Account SNS Topic ARN

3 **TransitAssumeRoleArn** Transit Account Assume Role ARN

4 **TransitAWSAccountNumber** Transit AWS Account number required for Assum

5 **LambdaFunctionsBucketName** Existing S3 bucket name which is having the La

6 **CloudTrailS3BucketName**
Creates a S3-Bucket Name for storing the CloudTrails logs. NOTE: S3 bucket names are globally unique, stack creation failure

7 **SshKey** Search
SSH key to associate with NAT Server in NewVPC

az1 us-east-1a
Select AvailabilityZone 1

8

az2 us-east-1b
Select AvailabilityZone 2

Palo Alto Networks Transit VPC Deployment Guide

Default Parameters

9	LaunchSubscriberVpc	<input type="text" value="No"/>	Select a Value
10	LambdaZipFile	<input type="text" value="lambda.zip"/>	Lambda code zip filename which is stored in above mentioned Req
11	VpcCidrRange	<input type="text" value="10.10.0.0/17"/>	Give the VPC CIDR range to create VPC
	SubnetCidr1	<input type="text" value="10.10.1.0/24"/>	Give the CIDR range to create subnet
12	SubnetCidr2	<input type="text" value="10.10.2.0/24"/>	Give the CIDR range to create subnet
	SubnetCidr3	<input type="text" value="10.10.3.0/24"/>	Give the CIDR range to create subnet
	SubnetCidr4	<input type="text" value="10.10.4.0/24"/>	Give the CIDR range to create subnet
13	trustedSource	<input type="text" value="1.1.1.1/32"/>	Trusted source to allow access to PA MGMT interface

1. Enter a stack name
2. Enter the Transit SNS Topic ARN. This can be found in the outputs section in the CloudFormation console of the Transit VPC stack

Overview	Outputs	Resources	Events	Template	Parameters	Tags	Stack Policy	Change Sets	Rollback Triggers
TransitVpcDmzAz2SubnetGateway					10.100.0.33	GatewayIP2			
PaBootstrapBucketName					transit-vpc-bootstrap	IAM role to allow access to transit VPC S3 bucket			
TransitVpcUntrustedSecurityGroupId					sg-7e75be09	Untrusted security group ID			
PaBootstrapBucketAccessRole					transit-vpc-paBootstrapBucketAccessRole-ZPGE2KOZ6S82	IAM role to allow access to transit VPC S3 bucket			
TransitVpcMgmtAz1SubnetId					subnet-61e5944e	MGMT AZ1 Subnet ID			
transitVpc					vpc-b97269c1	Transit VPC ID			
TransitAssumeRoleArn					arn:aws:iam::[REDACTED]:role/TransitAssumeRole-transit-vpc	Transit Assume Role Arn, This will be given and Parameter while la...			
TransitVpcDmzAz1SubnetGateway					10.100.0.1	GatewayIP1			
TransitVpcTrustedSecurityGroupId					sg-c7844eb0	Trusted security group ID			
TransitVpcDmzAz1SubnetId					subnet-b48bb5ff	DMZ AZ2 Subnet ID			
TransitSnsArn					arn:aws:sns:us-east-1:[REDACTED]:transitSns-transit-vpc	Transit SNS Topic Arn, This will be given and Parameter while laun...			
PaGroupInstanceProfileName					transit-vpc-paGroupInstanceProfile-5SMSWTB9RSOI	Instance profile for PA-Group			

3. Enter the Transit Assume Role ARN.

Palo Alto Networks Transit VPC Deployment Guide

Overview	Outputs	Resources	Events	Template	Parameters	Tags	Stack Policy	Change Sets	Rollback Triggers
TransitVpcDmzAz2SubnetGateway					10.100.0.33				GatewayIP2
PaBootstrapBucketName					transit-vpc-bootstrap				IAM role to allow access to transit VPC S3 bucket
TransitVpcUntrustedSecurityGroupId					sg-7e75be09				Untrusted security group ID
PaBootstrapBucketAccessRole					transit-vpc-paBootstrapBucketAccessRole-ZPGE2KOZ6S82				IAM role to allow access to transit VPC S3 bucket
TransitVpcMgmtAz1SubnetId					subnet-61e5944e				MGMT AZ1 Subnet ID
transitVpc					vpc-b97269c1				Transit VPC ID
TransitAssumeRoleArn					arn:aws:iam::[REDACTED]:role/TransitAssumeRole-transit-vpc				Transit Assume Role Arn, This will be given and Parameter while la...
TransitVpcDmzAz1SubnetGateway					10.100.0.1				GatewayIP1
TransitVpcTrustedSecurityGroupId					sg-c7844eb0				Trusted security group ID
TransitVpcDmzAz1SubnetId					subnet-b48bb5ff				DMZ AZ2 Subnet ID
TransitSnsArn					arn:aws:sns:us-east-1:[REDACTED]:transitSns-transit-vpc				Transit SNS Topic Arn, This will be given and Parameter while laun...
PaGroupInstanceProfileName					transit-vpc-paGroupInstanceProfile-5SMSWTB9RSOI				Instance profile for PA-Group

4. Enter the AWS account number where the transit VPC template was launched. Even if you are launching the subscribing VPC template in the same account, enter the account number in use.
5. Enter the S3 bucket name where the subscriber VPC lambda.zip and subscriberVpcCft.json files are stored.
6. Enter a unique bucket name where cloudtrail logs will be stored. Since AWS provides no way to check if the bucket name is unique when launching a CFT, make sure you append the bucket name with your username or part of your account number to make it unique.
7. Pick your SSH key
8. Pick the AZs you want the subscriber VPC to be launched in.
9. Select Yes to launch the subscribing VPC automatically
10. The name of the zip file that contains the lambda code.
11. Subscriber VPC CIDR
12. CIDR for various subnets within the VPC
13. IP address to lock down security group for SSH access.

Click through to create the stack. Once stack creation is complete, move to the next step.

8.2 Option 2: Launch a subscriber VPC

Launch the initializeSubscriberAccount.json template as shown in [Section 8.1](#), but choose No for Step 9.

Once stack creation is successful you can launch the susbcriberVpcCft.json and fill in the parameters as follows:

Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudForm:

1
Stack name

Parameters

2

AvailabilityZone1

us-east-1a

Select AvailabilityZone 1

3

AvailabilityZone2

us-east-1b

Select AvailabilityZone 2

4

NatInstanceType

t2.micro

Instance type to use for NAT

5

sshKey

Search

SSH key to associate with PA Server

subnetCidrRange1

10.10.1.0/24

Give the CIDR range to create subnet

subnetCidrRange2

10.10.2.0/24

Give the CIDR range to create subnet

6

subnetCidrRange3

10.10.3.0/24

Give the CIDR range to create subnet

subnetCidrRange4

10.10.4.0/24

Give the CIDR range to create subnet

7

trustedSource

1.1.1.1/32

Trusted source to allow access to PA MGMT interface

vpcCidrRange

10.10.0.0/17

Give the VPC CIDR range to create VPC

1. Enter a stack name
2. Enter the AZs where you want this launched. Make sure you pick the same AZs as you did when launching the initializeSubscriberVpcCft.json
3. Pick a NAT instance type. This is only used as a bastion host.

4. Pick your SSH key
5. Pick the CIDR range for 4 subnets.
6. Modify the trusted source from where you want to restrict SSH access into your NAT instance.
7. Pick the CIDR range for your VPC.

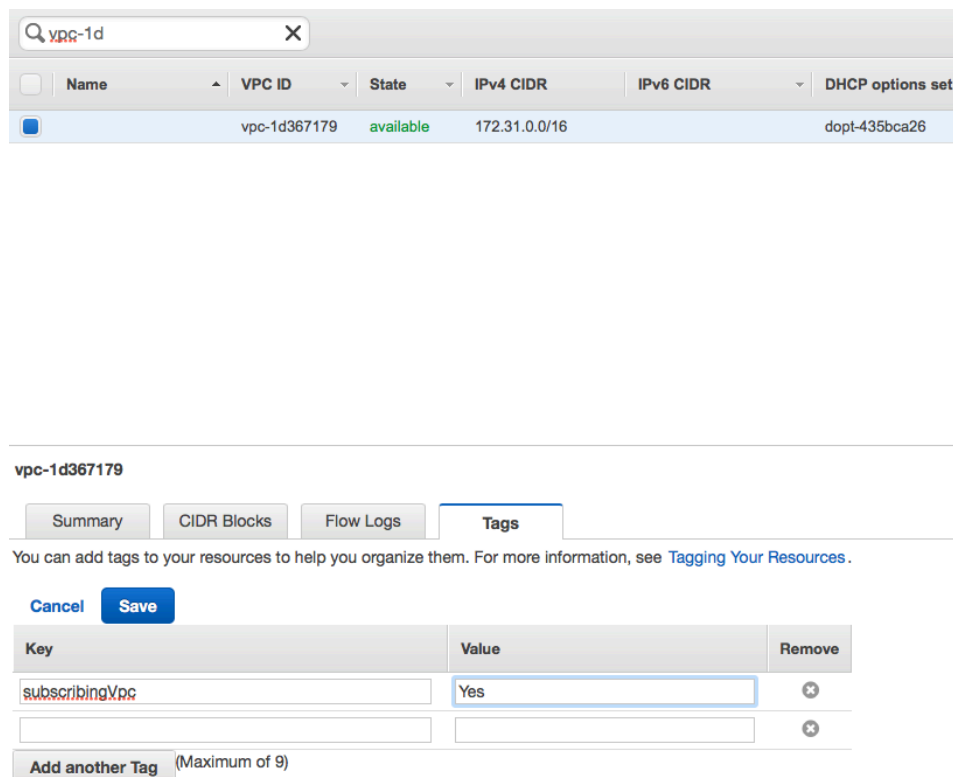
Click through to create the stack.

8.3 Option 3: Tag an existing VPC

NOTE: For this option to work, your existing VPC should NOT have an IGW or VGW pre-deployed. A VGW will be deployed for you.

If you already have an existing VPC with assets deployed and want to connect this VPC to the Transit VPC, then launch the initializeSubscriberAccount.json template as shown in [Section 8.1](#), but choose No for Step 9. Once stack creation is complete, you can add a TAG to the existing VPC, to start the automated process to connect the VPC to the Transit VPC.

In your AWS VPC console, select the Tags tab and add the following key-value pair:



The screenshot shows the AWS VPC console interface. At the top, there is a search bar with 'vpc-1d' entered. Below it is a table listing VPCs. The first VPC is 'vpc-1d367179' with state 'available' and IPv4 CIDR '172.31.0.0/16'. Below the table, the 'Tags' tab is selected for the VPC 'vpc-1d367179'. The 'Tags' section shows a table with one tag: 'subscribingVpc' with a value of 'Yes'. There are 'Cancel' and 'Save' buttons above the tag table. At the bottom, there is a button 'Add another Tag' with a note '(Maximum of 9)'.

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set
	vpc-1d367179	available	172.31.0.0/16		dopt-435bca26

vpc-1d367179

Summary | CIDR Blocks | Flow Logs | **Tags**

You can add tags to your resources to help you organize them. For more information, see [Tagging Your Resources](#).

[Cancel](#) [Save](#)

Key	Value	Remove
subscribingVpc	Yes	

[Add another Tag](#) (Maximum of 9)

Click Save.

9. When everything works

Launching this template kicks off a series of automated tasks and will launch a new stack in the Transit VPC account called PaGroup.

<div> <div>Create Stack ▾</div> <div>Actions ▾</div> <div>Design template</div> </div>			
<div> <div>Filter: Active ▾</div> <div>By Stack Name</div> </div>			
	Stack Name	Created Time	Status
<input type="checkbox"/>	PaGroup58	2018-01-29 16:28:37 UTC-0800	CREATE_COMPLETE
<input type="checkbox"/>	subscriber-1	2018-01-29 16:18:20 UTC-0800	CREATE_COMPLETE
<input type="checkbox"/>	susbcriber-account	2018-01-29 16:05:06 UTC-0800	CREATE_COMPLETE
<input type="checkbox"/>	trasnit-vpc	2018-01-29 13:51:25 UTC-0800	CREATE_COMPLETE

The PaGroup stack launches a pair of VM-Series firewalls, which are bootstrapped. Once the firewalls are up, IPSec tunnels are brought up between the AWS VGW (virtual private gateway) and the VM-Series.

Note: All of the automation is triggered via cloudtrail logs. Cloudtrail logs are written to S3 and that PUT operation triggers lambda functions. Cloudtrail logs can take upto 5 minutes to show up in S3, so please be patient.

In the screenshot below you can see a pair of VM-Series firewalls:

search: PaGroup <input type="text"/> Add filter											1 to 2 of 2	
<input type="checkbox"/>	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs	Key Name	Monitoring
<input type="checkbox"/>	PaGroup58-N1	i-02d0b14e9222be68c	c4.xlarge	us-east-1a	running	2/2 checks ...	None		35.169.156.27	-	aws-keypair-vi...	disabled
<input type="checkbox"/>	PaGroup58-N2	i-03e9b090618a849c9	c4.xlarge	us-east-1b	running	2/2 checks ...	None		34.195.133.28	-	aws-keypair-vi...	disabled

Two VPN tunnels in the subscribing VPC:

Filter by tags and attributes or search by keyword										1 to 2 of 2	
<input type="checkbox"/>	Name	VPN ID	State	Virtual Private Gateway	Customer Gateway	Customer Gateway Address	Type	Category	VPC		
<input type="checkbox"/>	vpc-fa342f82...	vpn-f4382495	available	vgw-594eba30 PaGroup58	cgw-0ffc0b66 PaGroup58-N2	34.195.133.28	ipsec.1	VPN	vpc-fa342f82 S...		
<input type="checkbox"/>	vpc-fa342f82...	vpn-f5382494	available	vgw-594eba30 PaGroup58	cgw-0cfc0b65 PaGroup58-N1	35.169.156.27	ipsec.1	VPN	vpc-fa342f82 S...		

And two customer gateways in the subscribing VPC:

Filter by tags and attributes or search by keyword							
<input type="checkbox"/>	Name	ID	State	Type	IP Address	BGP ASN	VPC
<input type="checkbox"/>	PaGroup58-N1	cgw-0cfc0b65	available	ipsec.1	35.169.156.27	64827	vpc-fa342f82 Subscribe-vpc
<input type="checkbox"/>	PaGroup58-N2	cgw-0ffc0b66	available	ipsec.1	34.195.133.28	64828	vpc-fa342f82 Subscribe-vpc

10. Accessing the Firewall

In order to access the firewall's web UI or the CLI, it is recommended that you use the NAT instance that has been deployed in the Transit VPC. In order to do that you will need to setup an SSH tunnel from your localhost to the remote NAT instance.

For Web UI:

```
$ssh -i <AWS SSH key> -l ec2-user <public IP address of NAT instance> -L 4000:<private IP address of fw eth0>:443 -nNtv
```

You can then point your browser to <https://localhost:4000>

For CLI:

```
$ssh -i <AWS SSH key> -l ec2-user <public IP address of NAT instance> -L 4000:<private IP address of fw eth0>:22 -nNtv
```

You can now ssh to localhost:4000 using the admin/ReanCloud123! credentials.

```
$ssh admin@localhost -p 4000
```

NOTE: You can use any port of you choosing other than 4000

11. Routing Tests

At this point if all the tunnels are up between VPCs you can deploy VMs in the subscribing VPC(s) and pass traffic.

Please make sure that you modify the security groups to allow ICMP (if doing ping tests).

Also please change the VPC route tables to allow route propagation.

rtb-f484b889

Summary	Routes	Subnet Associations	Route Propagation
---------	--------	---------------------	-------------------

[Cancel](#) [Save](#)

Virtual Private Gateway	Propagate
-------------------------	-----------

vgw-594eba30 | PaGroup58 ☒

12. Cleanup

You can clean up the setup by deleting the stacks deployed. You may have to manually delete some resources that were created by lambda functions.

If you had tagged a VPC, then you can simply remove the tag and wait for VPN connections and VGWs to be deleted.