AWS TRANSIT VPC WITH FORTIGATE NEXT-GENERATION FIREWALL

DEPLOYMENT GUIDE

This Fortinet Transit VPC Deployment Guide covers architectural design details and configuration steps for deploying a Transit VPC on Amazon Web Services (AWS). It includes links to AWS CloudFormation templates that launch, configure, and deploy the needed AWS services to deploy the Transit VPC solution on AWS.

The guide is intended for IT infrastructure architects, administrators, and DevOps professionals who have practical experience architecting for AWS.

AWS TRANSIT VPC CONCEPT

Transit VPC is a concept of having a Virtual Private Cloud (VPC) network with virtualized firewalls in AWS. The Transit VPC acts as the hub to all the traffic passing between the Spoke VPCs and the on-premises data center. For example, three branch offices ("spokes") connect to a central office (the "hub") over VPN links. The on-premises customer data center is a "spoke" from the perspective of the firewall inside the Transit VPC, with similar security and routing policies applied to it.

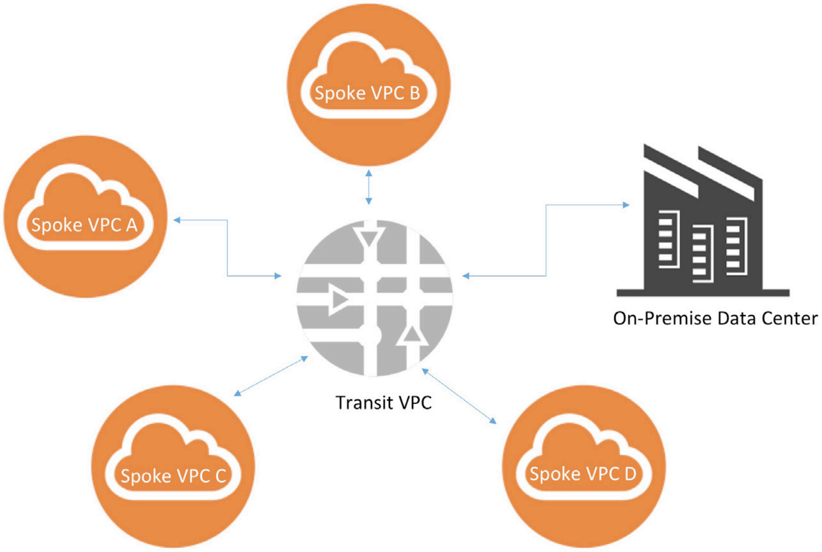


FIGURE 1: TRANSIT VPC CONCEPT

Amazon Virtual Private Cloud (Amazon VPC) provides customers with the ability to create as many virtual networks as they need, as well as different options for connecting those networks to each other and to non-AWS infrastructure. There are two common strategies for connecting multiple, geographically dispersed VPCs and remote networks to:

- Implement a hub-and-spoke network topology that routes all traffic through a network Transit center (a Transit VPC)
- Create a meshed network that uses individual connections between all networks.

Both approaches can create an efficient and available Transit network.

The Transit VPC in AWS consists of a VPC network that can be split into two or more subnets. Each of these subnets is associated with its own route tables and security groups. The Transit VPC is defined for an AWS Region, with the VPC subnets being equally divided among two Availability Zones per Region. This helps provide redundancy and high availability for the purposes of maintaining that high availability.

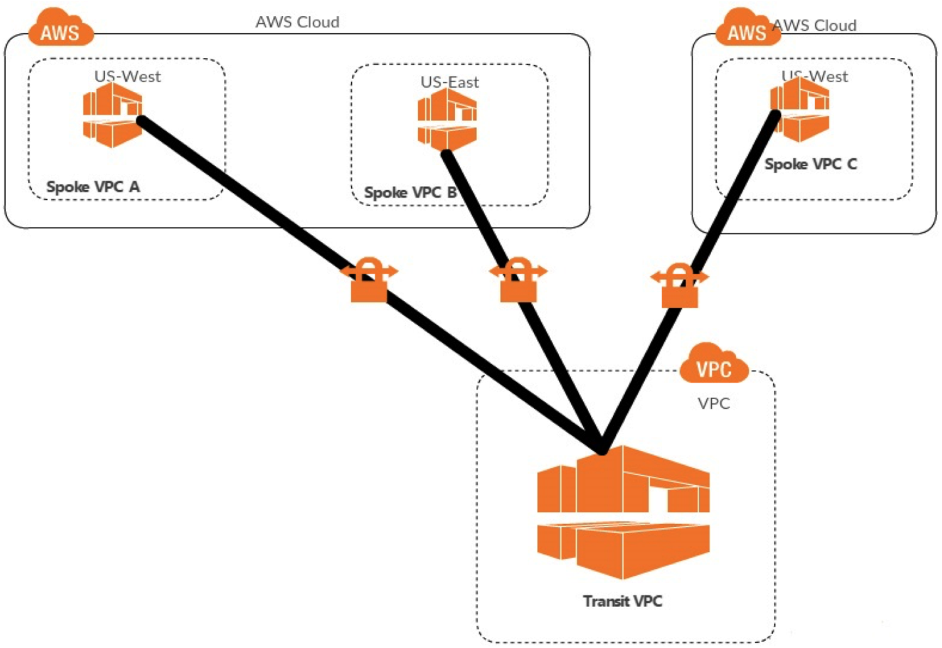
TRANSIT VPC CLOUDFORMATION TEMPLATE

The Transit VPC is orchestrated and brought online using custom CloudFormation templates. The parameters for creating the components of Transit VPC are defined in the CloudFormation template.

FORTINET TRANSIT VPC DEPLOYMENT IN AWS

As stated, one of the common strategies for connecting multiple, geographically dispersed VPCs and remote networks is to create a Transit VPC that serves as a global network Transit center.

A Transit VPC simplifies network management and minimizes the number of connections required to connect multiple VPCs and remote networks.



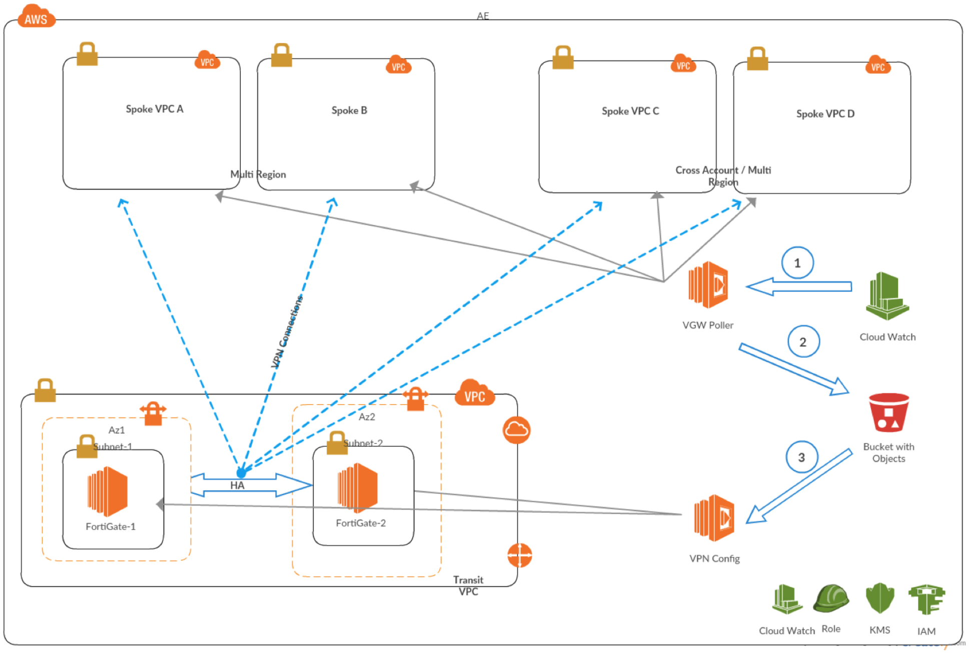
This design can save time and effort and reduce costs, as it is implemented virtually without the traditional expense of establishing a physical presence in a co-location Transit hub or deploying physical network gear.

The CloudFormation template configures and runs FortiGate in AWS. The solution below is used to display FortiGate's features in AWS:

- FortiGate VPN appliance in a typical hub-and-spoke network topology to connect multiple VPCs across Regions and Accounts
- Automate VPN connection configuration and setup as new spoke VPCs join the topology
- Support both BYOL and pay-as-you-go licensing options

HIGH-LEVEL NETWORK ARCHITECTURE

In the diagram below, each FortiGate will be connected to the entire Spoke VPCs independently and in a redundant manner. Both FortiGates operate in Active-Active mode.



The core components for this solution include:

- AWS VPC, VGW
- Fortinet NGFW Appliances—FortiGate (BYOL/pay as you go)
- AWS S3
- AWS EC2
- AWS Lambda
- AWS CloudWatch
- AWS IAM Roles
- AWS KMS

HIGH-LEVEL SOLUTION DESIGN SUMMARY

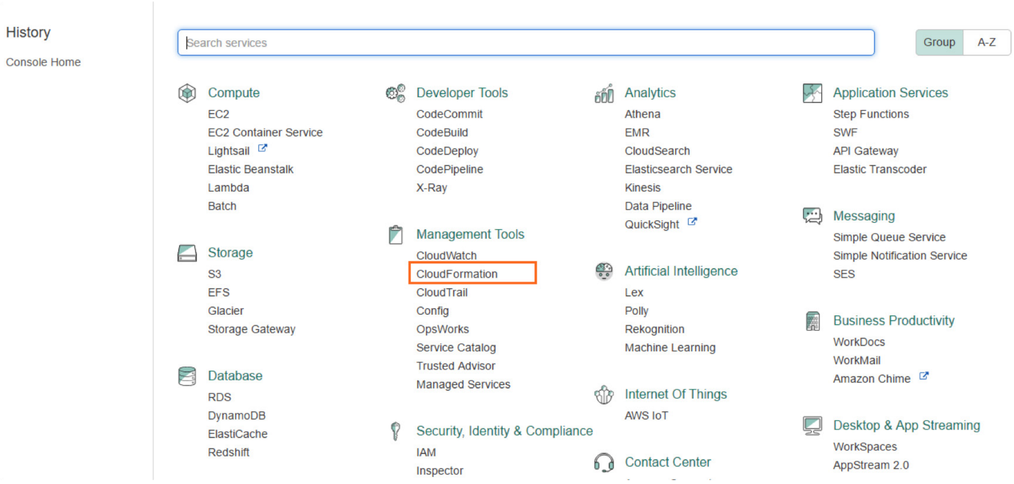
1. The solution deploys a Transit VPC
   - In a user-provided AWS region.
   - In a user-provided CIDR.
2. It deploys one or more spoke VPCs.
   - Spoke VPCs can be spread across multiple regions
   - Spoke VPCs can be in one or more AWS Accounts and are connected to the Transit network.
   - Spoke VPCs do not overlap with each other or with the Transit VPC.
3. This highly available design deploys two FortiGate VPN appliances into separate Availability Zones of a dedicated Transit VPC.
   - Each FortiGate instance has an associated Amazon CloudWatch alarm that enables automatic recovery of the instance if the EC2 hardware fails.
4. Spoke VPCs are connected to the Transit network through dynamically routed VPN connections between their Virtual Private Gateways (VGWs) and the FortiGate instances.
5. The user has an option to select FortiGate BYOL or pay as you go. If the user opts for the BYOL option, the associated license file should be uploaded as an accessible URL endpoint (AWS S3 or others) and provided as an input to the template.
6. FortiManager optionally can be deployed in a separate subnet in the Transit VPC. However, the integration to Fortinet Appliances has to be performed manually.

The automated process for adding a new spoke VPC, as part of this solution, is as follows:

7. Every five minutes, an Amazon CloudWatch event invokes the VGW Poller Lambda function, which iterates through each AWS Region of one or more customer accounts, searching for appropriately tagged Spoke VGWs (default tag key transitvpc:spoke, default tag value true) that do not have existing Transit VPC VPN connections.
8. When the VGW Poller identifies an applicable Spoke VGW, it creates the corresponding customer gateways (if required) and VPN connections to each FortiGate Appliance, and then saves this connection information to an Amazon S3 bucket using S3 SSE-KMS. All data in the S3 bucket is encrypted using a solution-specific AWS KMS managed customer master key (CMK).
9. The S3 Put event invokes the VPN Configurator Lambda function, which parses the VPN connection information and generates the necessary config files to create new VPN connections.
10. The VPN Config (Lambda function) pushes the configuration to the VPN Appliance instances using SSH.
11. As soon as the VPN configuration is applied onto the FortiGate instances, the VPN tunnels come up and Border Gateway Protocol (BGP) neighbor relationships are established to the Spoke VPCs.

GETTING STARTED

1. Open AWS console with your credentials and select the deployment location.
2. Click on **Services** and navigate to **CloudFormation** under **Management Tools**.



History

Console Home

Search services

Group | A-Z

Compute
EC2
EC2 Container Service
Lightsail
Elastic Beanstalk
Lambda
Batch

Storage
S3
EFS
Glacier
Storage Gateway

Database
RDS
DynamoDB
ElastiCache
Redshift

Developer Tools
CodeCommit
CodeBuild
CodeDeploy
CodePipeline
X-Ray

Management Tools
CloudWatch
CloudFormation
CloudTrail
Config
OpsWorks
Service Catalog
Trusted Advisor
Managed Services

Security, Identity & Compliance
IAM
Inspector

Analytics
Athena
EMR
CloudSearch
Elasticsearch Service
Kinesis
Data Pipeline
QuickSight

Artificial Intelligence
Lex
Polly
Rekognition
Machine Learning

Internet Of Things
AWS IoT

Contact Center

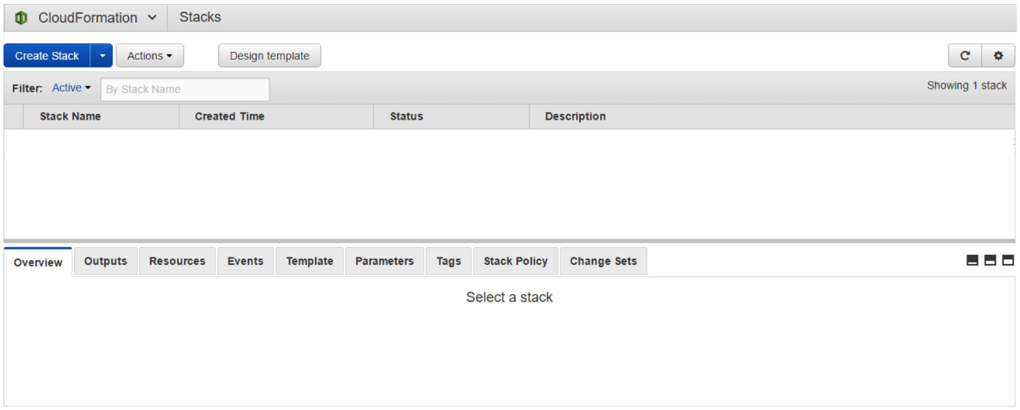
Application Services
Step Functions
SWF
API Gateway
Elastic Transcoder

Messaging
Simple Queue Service
Simple Notification Service
SES

Business Productivity
WorkDocs
WorkMail
Amazon Chime

Desktop & App Streaming
WorkSpaces
AppStream 2.0

3. Click on **Create Stack**.



CloudFormation | Stacks

Create Stack | Actions | Design template

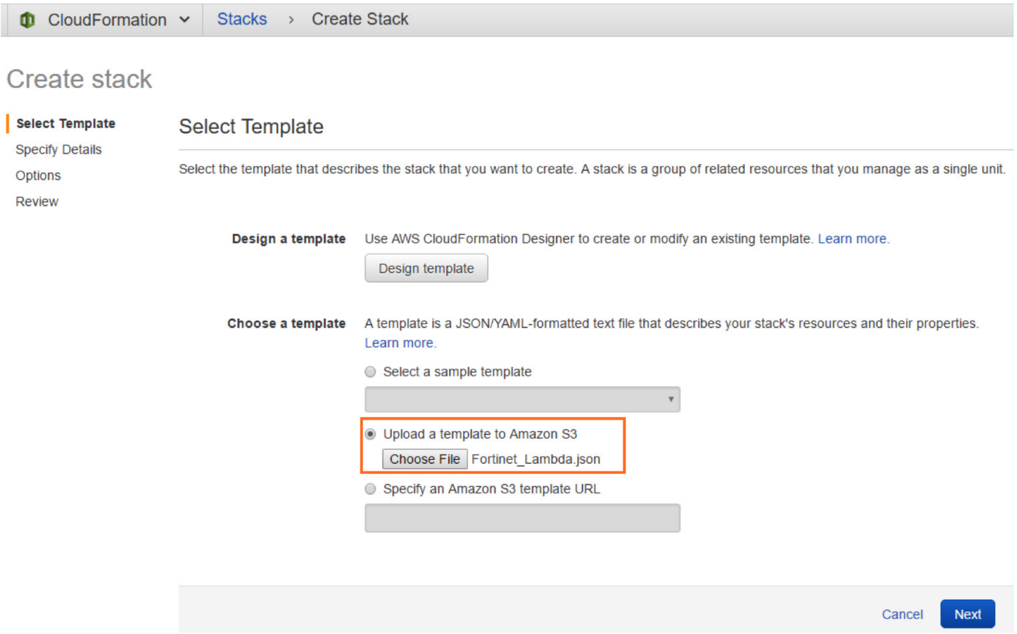
Filter: Active | By Stack Name | Showing 1 stack

Stack Name	Created Time	Status	Description

Overview | Outputs | Resources | Events | Template | Parameters | Tags | Stack Policy | Change Sets

Select a stack

4. On **Select Template** page, choose to upload a template to Amazon S3 and click on **Next**.



CloudFormation | Stacks › Create Stack

Create stack

Select Template
Specify Details
Options
Review

Select Template

Select the template that describes the stack that you want to create. A stack is a group of related resources that you manage as a single unit.

Design a template Use AWS CloudFormation Designer to create or modify an existing template. Learn more.

Design template

Choose a template A template is a JSON/YAML-formatted text file that describes your stack's resources and their properties. Learn more.

○ Select a sample template

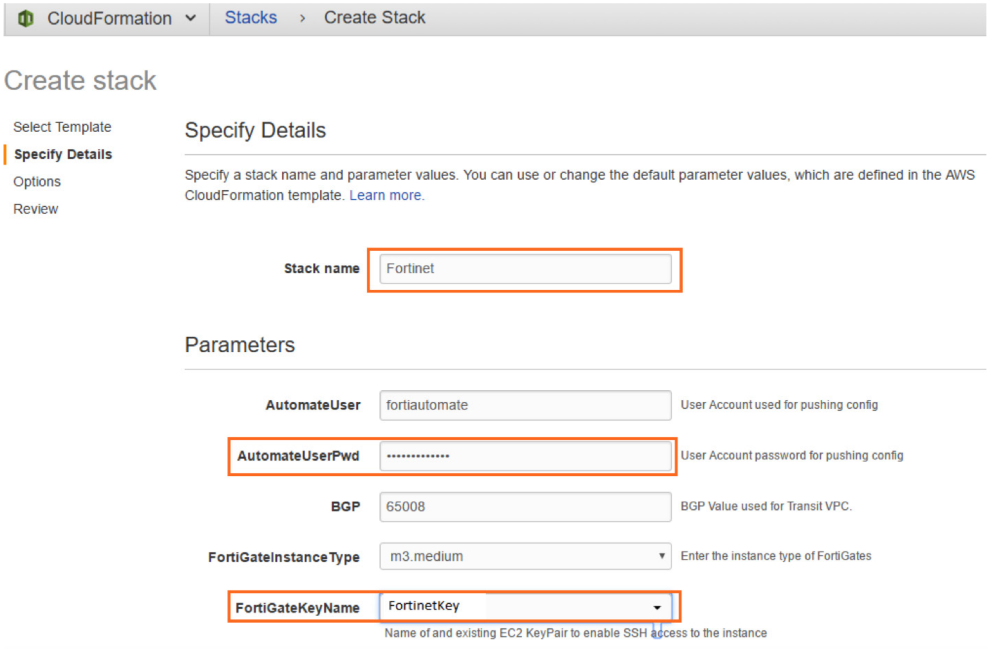
● Upload a template to Amazon S3

Choose File Fortinet_Lambda.json

○ Specify an Amazon S3 template URL

Cancel | Next

5. A **Specify Details** page opens. Enter the **Stack name**, and in the **Parameters** section, enter **AutomateUserPwd** and give the **FortiGateKeyName** (the key pair should be present in the AWS account).



Create stack

Specify Details

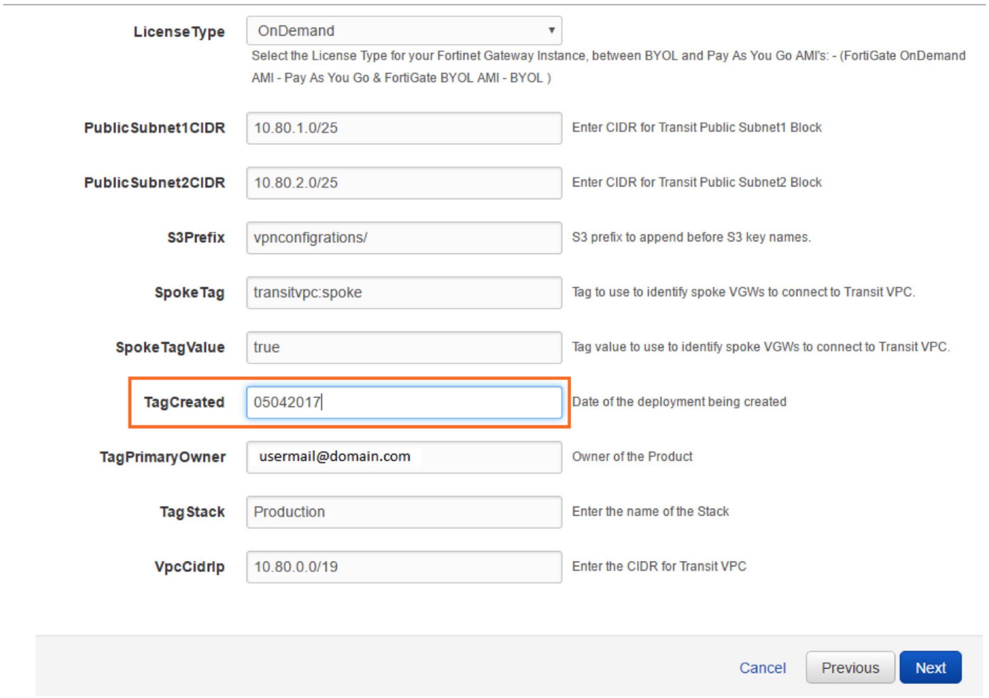
Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. Learn more.

Stack name: Fortinet

Parameters

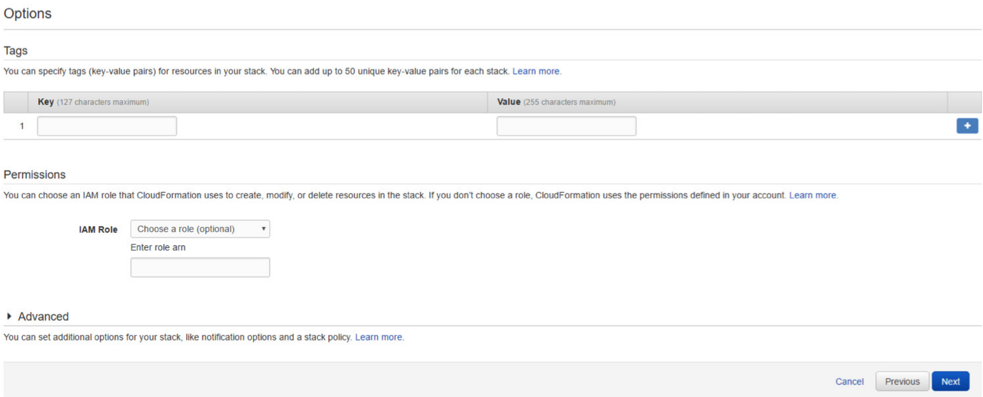
AutomateUser	fortiautomate	User Account used for pushing config
AutomateUserPwd	••••••••••••••	User Account password for pushing config
BGP	65008	BGP Value used for Transit VPC.
FortiGateInstanceType	m3.medium	Enter the instance type of FortiGates
FortiGateKeyName	FortinetKey	Name of and existing EC2 KeyPair to enable SSH access to the instance

6. Enter the **Date of the deployment being created** in the **TagCreated** section on the same page and click on **Next**, which leads to the **Options** page.



LicenseType	OnDemand	Select the License Type for your Fortinet Gateway Instance, between BYOL and Pay As You Go AMI's: - (FortiGate OnDemand AMI - Pay As You Go & FortiGate BYOL AMI - BYOL)
PublicSubnet1CIDR	10.80.1.0/25	Enter CIDR for Transit Public Subnet1 Block
PublicSubnet2CIDR	10.80.2.0/25	Enter CIDR for Transit Public Subnet2 Block
S3Prefix	vpnconfigrations/	S3 prefix to append before S3 key names.
SpokeTag	transitvpc:spoke	Tag to use to identify spoke VGWs to connect to Transit VPC.
SpokeTagValue	true	Tag value to use to identify spoke VGWs to connect to Transit VPC.
TagCreated	05042017	Date of the deployment being created
TagPrimaryOwner	usermail@domain.com	Owner of the Product
TagStack	Production	Enter the name of the Stack
VpcCidrIp	10.80.0.0/19	Enter the CIDR for Transit VPC

7. On this page, enter the **Tags** giving values for the **Key** section and **Value** section and click on **Next**.



Options

Tags

You can specify tags (key-value pairs) for resources in your stack. You can add up to 50 unique key-value pairs for each stack. Learn more.

	Key (127 characters maximum)	**Value** (255 characters maximum)	
1			+

Permissions

You can choose an IAM role that CloudFormation uses to create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses the permissions defined in your account. Learn more.

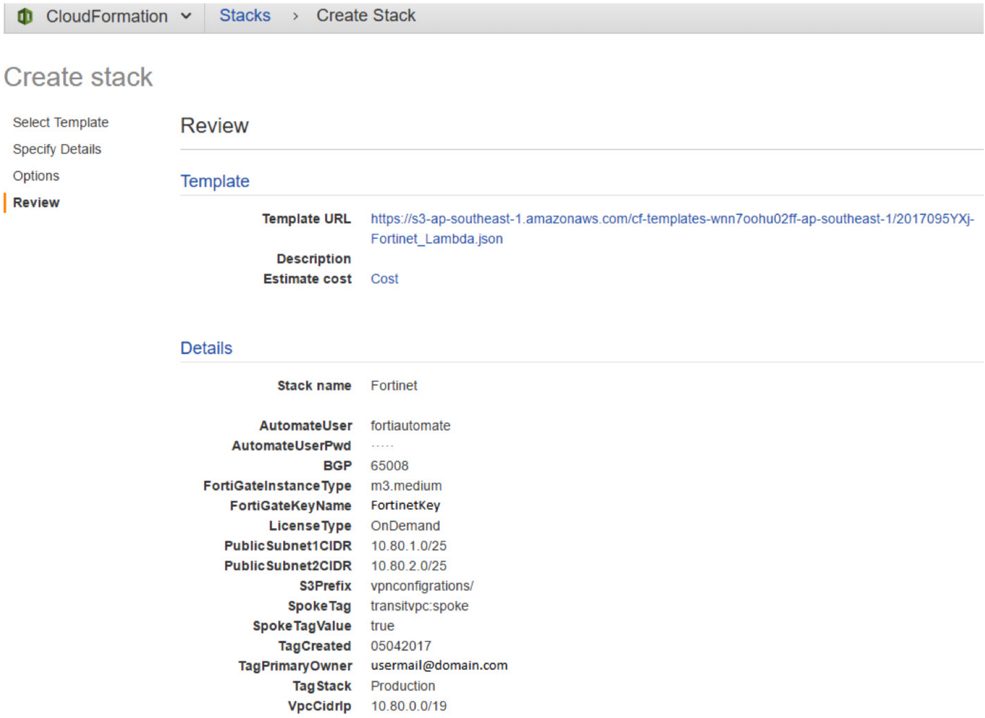
IAM Role Choose a role (optional)

Enter role arn

Advanced

You can set additional options for your stack, like notification options and a stack policy. Learn more.

8. A **Review** page opens, which gives the overview of the details entered.



Create stack

Review

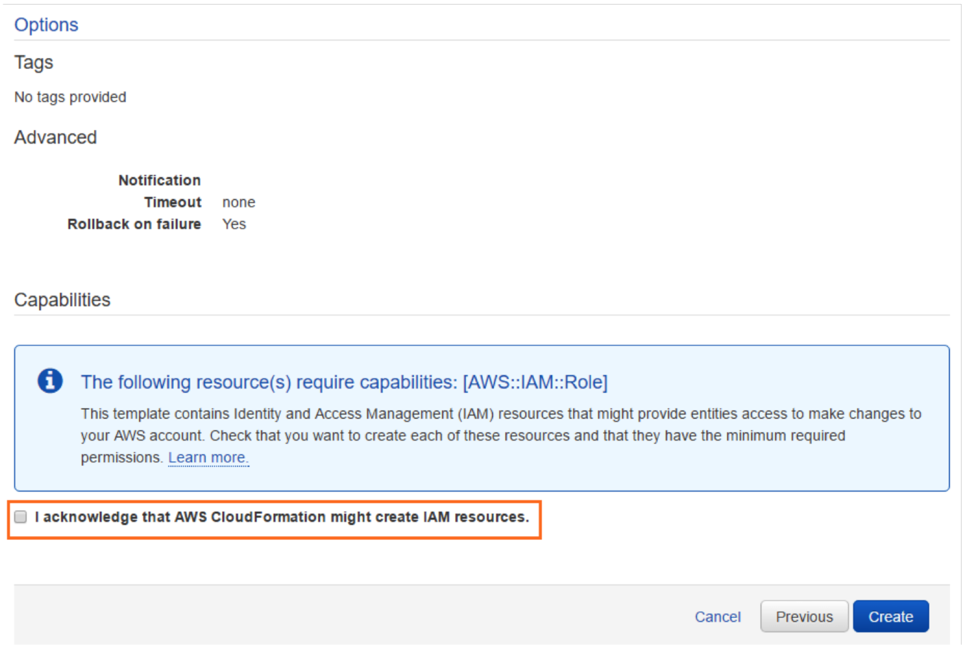
Template

Template URL	https://s3-ap-southeast-1.amazonaws.com/cf-templates-wnn7oohu02ff-ap-southeast-1/2017095YXj-Fortinet_Lambda.json
Description	
Estimate cost	Cost

Details

Stack name	Fortinet
AutomateUser	fortiautomate
AutomateUserPwd	·····
BGP	65008
FortiGateInstanceType	m3.medium
FortiGateKeyName	FortinetKey
LicenseType	OnDemand
PublicSubnet1CIDR	10.80.1.0/25
PublicSubnet2CIDR	10.80.2.0/25
S3Prefix	vpnconfigrations/
SpokeTag	transitvpc:spoke
SpokeTagValue	true
TagCreated	05042017
TagPrimaryOwner	usermail@domain.com
TagStack	Production
VpcCidrIp	10.80.0.0/19

9. Check the box ***I acknowledge that AWS CloudFormation might create IAM resources*** and click on **Create**.



Options

Tags

No tags provided

Advanced

Notification	
Timeout	none
Rollback on failure	Yes

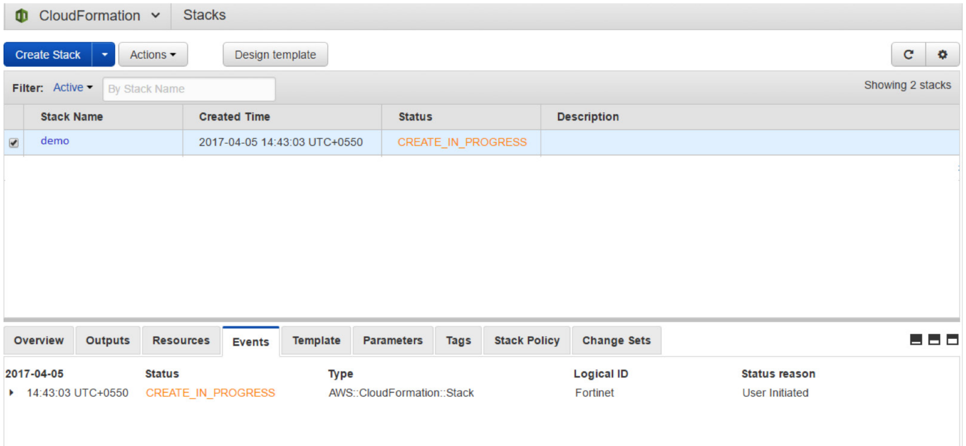
Capabilities

The following resource(s) require capabilities: [AWS::IAM::Role]

This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. Learn more.

□ **I acknowledge that AWS CloudFormation might create IAM resources.**

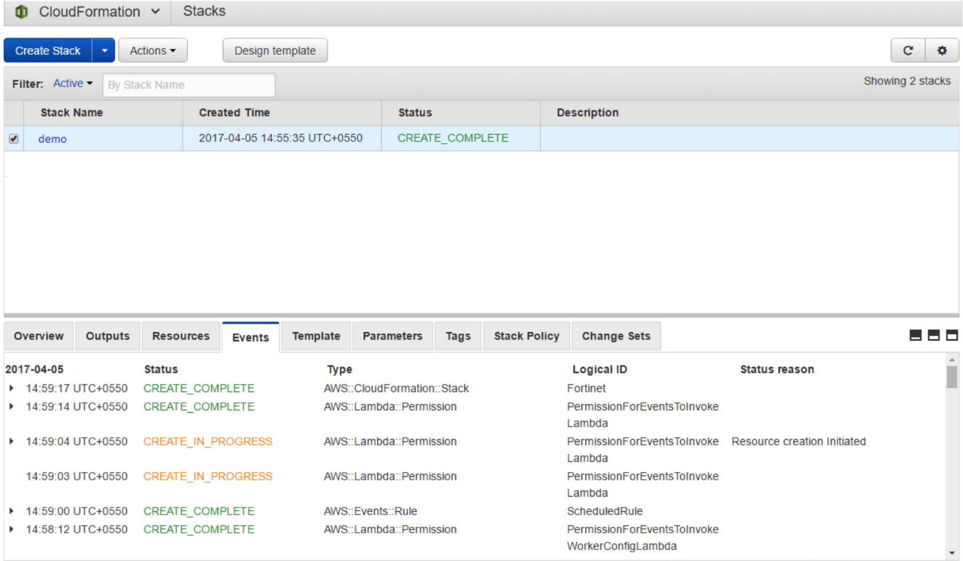
10. This leads to the **Create Stack** page, which shows the progress of the stack created. Click on the **Outputs** sections below to view the events.



Showing 2 stacks

	Stack Name	Created Time	Status	Description
☑	demo	2017-04-05 14:43:03 UTC+0550	CREATE_IN_PROGRESS	

2017-04-05	Status	Type	Logical ID	Status reason
14:43:03 UTC+0550	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	Fortinet	User Initiated



Showing 2 stacks

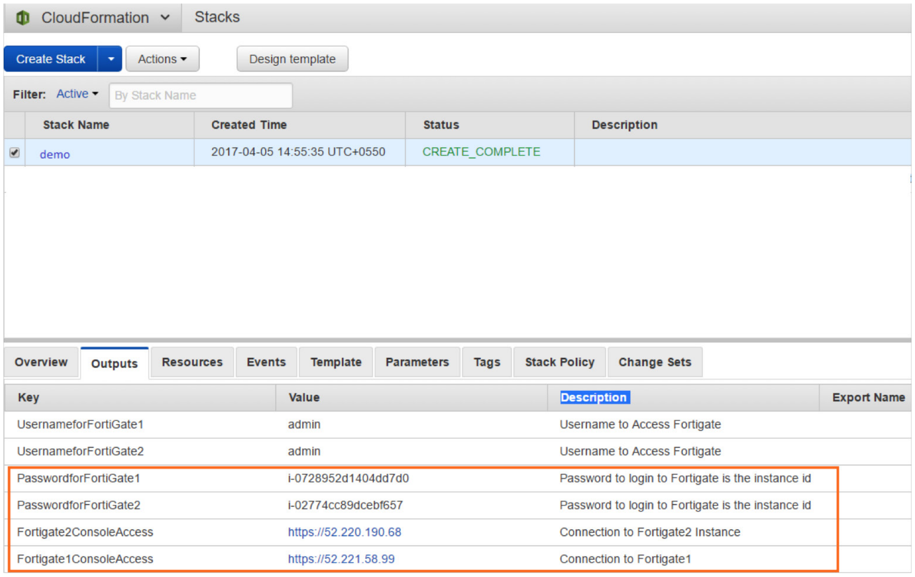
	Stack Name	Created Time	Status	Description
☑	demo	2017-04-05 14:55:35 UTC+0550	CREATE_COMPLETE	

2017-04-05	Status	Type	Logical ID	Status reason
14:59:17 UTC+0550	CREATE_COMPLETE	AWS::CloudFormation::Stack	Fortinet	
14:59:14 UTC+0550	CREATE_COMPLETE	AWS::Lambda::Permission	PermissionForEventsToInvokeLambda	
14:59:04 UTC+0550	CREATE_IN_PROGRESS	AWS::Lambda::Permission	PermissionForEventsToInvokeLambda	Resource creation Initiated
14:59:03 UTC+0550	CREATE_IN_PROGRESS	AWS::Lambda::Permission	PermissionForEventsToInvokeLambda	
14:59:00 UTC+0550	CREATE_COMPLETE	AWS::Events::Rule	ScheduledRule	
14:58:12 UTC+0550	CREATE_COMPLETE	AWS::Lambda::Permission	PermissionForEventsToInvokeWorkerConfigLambda	

11. The following are the resources created after the CloudFormation deployment:

- VPC
- 2 FortiGate EC2 Instances
- S3 Bucket
- Lambda Function: This solution uses two AWS Lambda functions, the VGW Poller and the Worker Config.
- IAM Roles and Policies

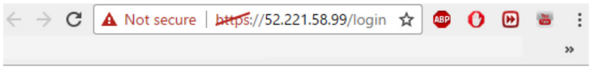
12. We can access the FortiGate console by copying the **Value** of the **Key** from **Outputs** of CloudFormation and browsing it.



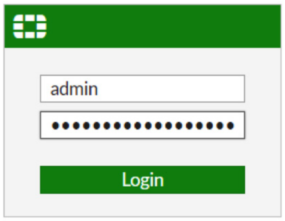
	Stack Name	Created Time	Status	Description
☑	demo	2017-04-05 14:55:35 UTC+0550	CREATE_COMPLETE	

Key	Value	Description	Export Name
UsernameforFortiGate1	admin	Username to Access Fortigate	
UsernameforFortiGate2	admin	Username to Access Fortigate	
PasswordforFortiGate1	i-0728952d1404dd7d0	Password to login to Fortigate is the instance id	
PasswordforFortiGate2	i-02774cc89dcebf657	Password to login to Fortigate is the instance id	
Fortigate2ConsoleAccess	https://52.220.190.68	Connection to Fortigate2 Instance	
Fortigate1ConsoleAccess	https://52.221.58.99	Connection to Fortigate1	

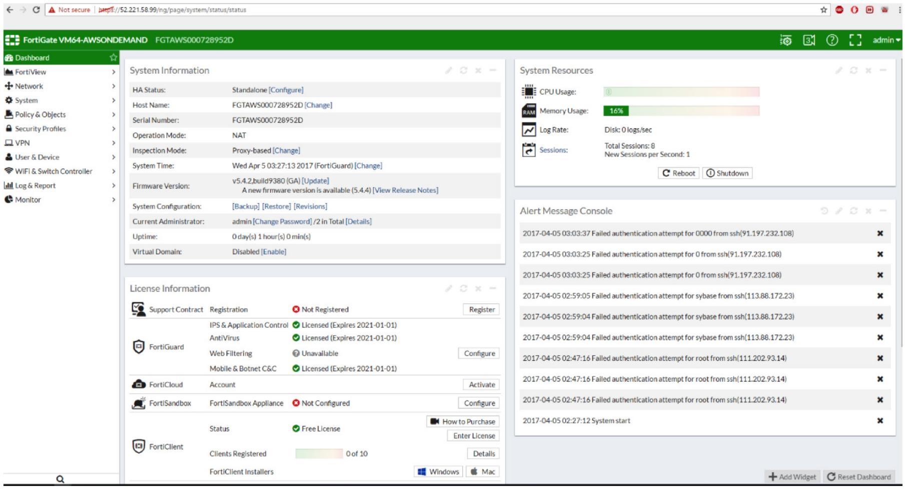
13. Give the admin username and password relevant to the console.



~~https~~://52.221.58.99/login



admin
••••••••••••••••••



~~https~~://52.221.58.99/ng/page/system/status/status

System Information

HA Status:	Standalone [Configure]
Host Name:	FGTAWS000728952D [Change]
Serial Number:	FGTAWS000728952D
Operation Mode:	NAT
Inspection Mode:	Proxy-based [Change]
System Time:	Wed Apr 5 03:27:13 2017 (FortiGuard) [Change]
Firmware Version:	v5.4.2,build9380 (GA) [Update] A new firmware version is available (5.4.4) [View Release Notes]
System Configuration:	[Backup] [Restore] [Revisions]
Current Administrator:	admin [Change Password] /2 in Total [Details]
Uptime:	0 day(s) 1 hour(s) 0 min(s)
Virtual Domain:	Disabled [Enable]

License Information

Support Contract	Registration	Not Registered
FortiGuard	IPS & Application Control	Licensed (Expires 2021-01-01)
	AntiVirus	Licensed (Expires 2021-01-01)
	Web Filtering	Unavailable
	Mobile & Botnet C&C	Licensed (Expires 2021-01-01)
FortiCloud	Account	
FortiSandbox	FortiSandbox Appliance	Not Configured
FortiClient	Status	Free License
	Clients Registered	0 of 10
	FortiClient Installers	

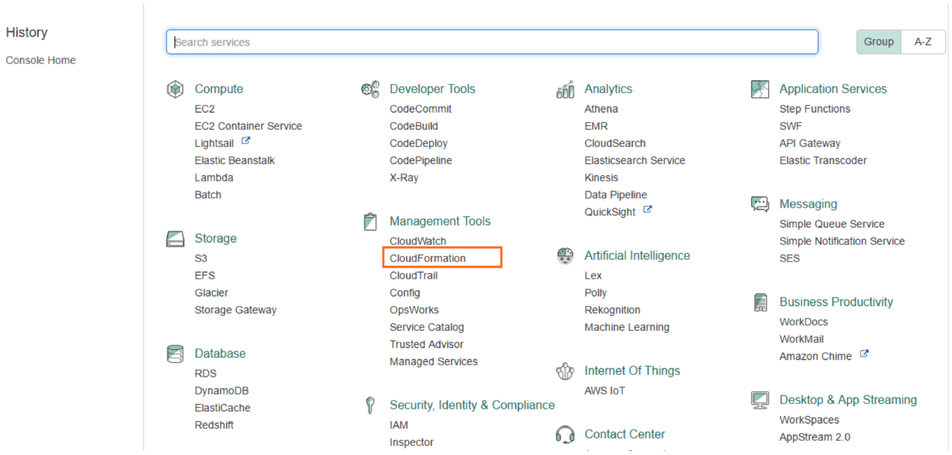
System Resources

CPU Usage:	0
Memory Usage:	16%
Log Rate:	Disk: 0 logs/sec
Sessions:	Total Sessions: 8 New Sessions per Second: 1

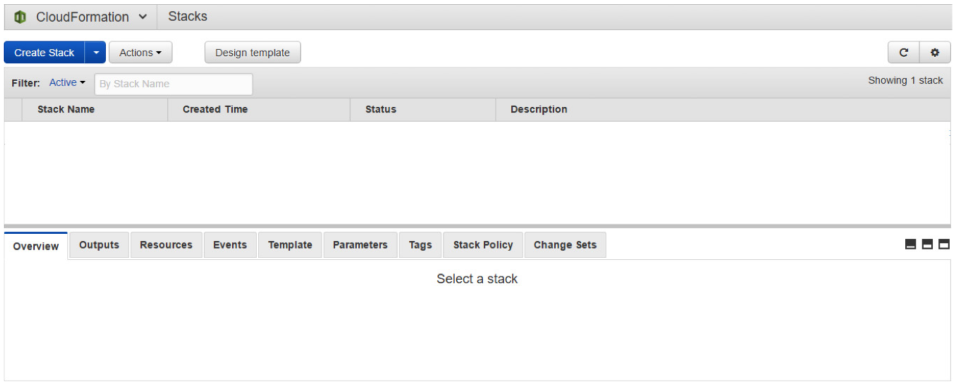
Alert Message Console

```
2017-04-05 03:03:37 Failed authentication attempt for 0000 from ssh(91.197.232.108)
2017-04-05 03:03:25 Failed authentication attempt for 0 from ssh(91.197.232.108)
2017-04-05 03:03:25 Failed authentication attempt for 0 from ssh(91.197.232.108)
2017-04-05 02:59:05 Failed authentication attempt for sybase from ssh(113.88.172.23)
2017-04-05 02:59:04 Failed authentication attempt for sybase from ssh(113.88.172.23)
2017-04-05 02:59:04 Failed authentication attempt for sybase from ssh(113.88.172.23)
2017-04-05 02:47:16 Failed authentication attempt for root from ssh(111.202.93.14)
2017-04-05 02:47:16 Failed authentication attempt for root from ssh(111.202.93.14)
2017-04-05 02:47:16 Failed authentication attempt for root from ssh(111.202.93.14)
2017-04-05 02:27:12 System start
```

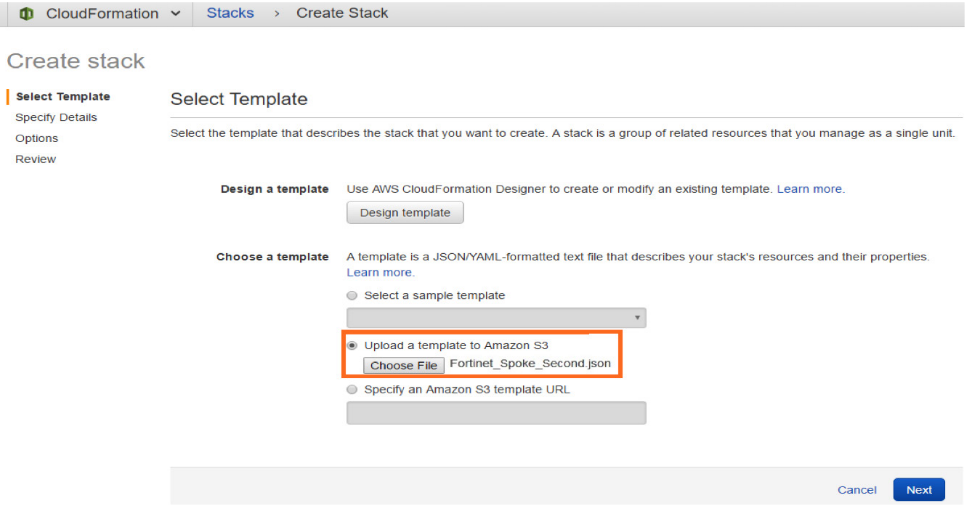
14. Open another AWS account.
15. Click on **Services** and navigate to **CloudFormation** under **Management Tools**.



16. Click on **Create Stack**.



17. On the **Select Template** page, choose **Upload a template to Amazon S3** and click on **Next**.



Select Template

Select the template that describes the stack that you want to create. A stack is a group of related resources that you manage as a single unit.

Design a template: Use AWS CloudFormation Designer to create or modify an existing template. Learn more.

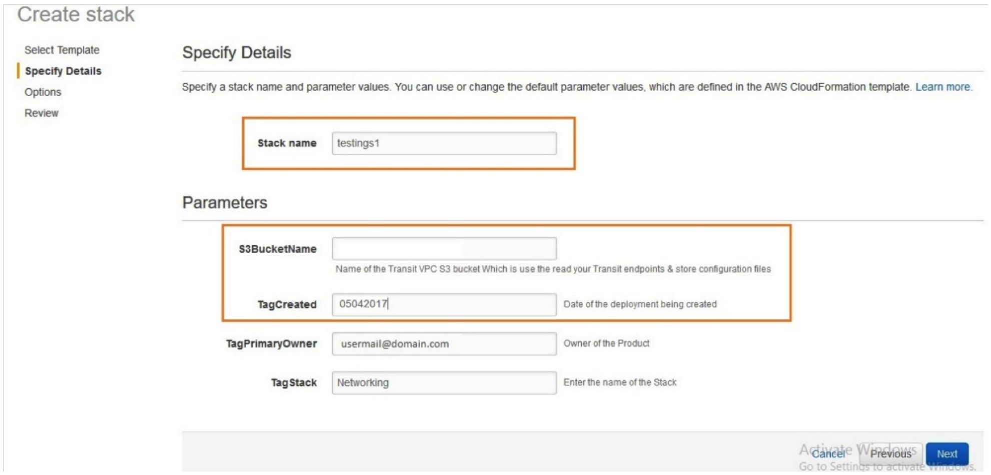
Choose a template: A template is a JSON/YAML-formatted text file that describes your stack's resources and their properties. Learn more.

○ Select a sample template

● Upload a template to Amazon S3 — Fortinet_Spoke_Second.json

○ Specify an Amazon S3 template URL

18. A **Specify Details** page opens. Enter the **Stack name**. In the **Parameters** section, enter **S3BucketName** of the Transit VPC S3 bucket that is used to read the Transit endpoints and store configuration files. Enter the **Date of the deployment being created** in TagCreated and click on **Next**.



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 template. Learn more.

Stack name: testings1

Parameters

S3BucketName:
Name of the Transit VPC S3 bucket Which is use the read your Transit endpoints & store configuration files

TagCreated: 05042017 — Date of the deployment being created

TagPrimaryOwner: usermail@domain.com — Owner of the Product

TagStack: Networking — Enter the name of the Stack

19. This creates a Lambda function.

For more information or support on FortiGate Transit VPC design, please contact aws@fortinet.com. For CloudFormation download and feedback, please visit Github Fortinet Solutions https://github.com/fortinetsolutions.

REFERENCE:

- https://aws.amazon.com/answers/networking/aws-global-Transit-network/
- https://www.serro.com/Transit-vpc-introduction-Transit-vpc-inside-aws/

FORTINET®

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990