FORTINET

AWS BEST PRACTICES

High Availability Setup and Automating Route Table Change for an Active-Passive FortiGate Next Generation Firewall Deployment

Q3 2017

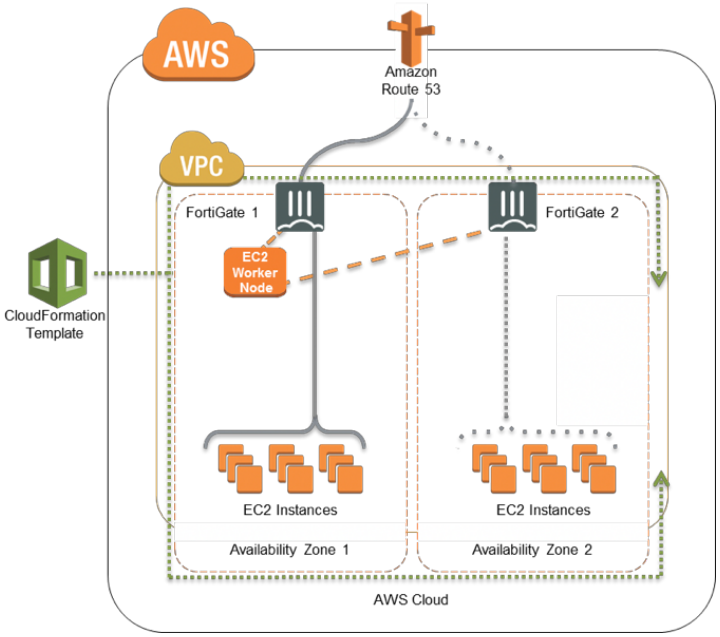
DEPLOYMENT GUIDE

PROBLEM STATEMENT

AWS best practice is to architect redundant Availability Zones (AZ) in each VPC for failover redundancy and maximum uptime in the event of an instance failure. However, there are manual steps required to maintain security redundancy. Fortinet has an automated solution to address this and create a truly automated failover and reversion.

SOLUTION

- In an Active-Passive FortiGate HA environment in AWS, if the Active firewall has an issue and cannot process the traffic, a manual change is necessary for the route table to go through the Secondary Firewall. This is not ideal and might increase the outage time.
- To work around this, a python script can be used to automate the process. The python script monitors the primary firewall, and if the primary firewall goes down, it makes the appropriate API calls to automate the route table changes needed to move to the secondary firewall.
- When the primary firewall is restored, the python script will make the API calls to AWS to change the route table back to the primary firewall.
- HA example:

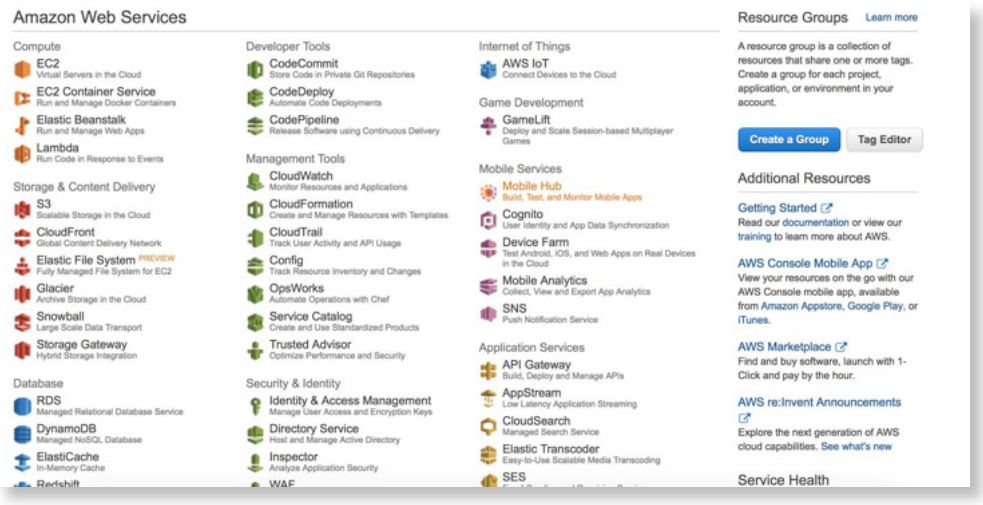


FORTIGATE HA SETUP: VPC_CFT STEPS

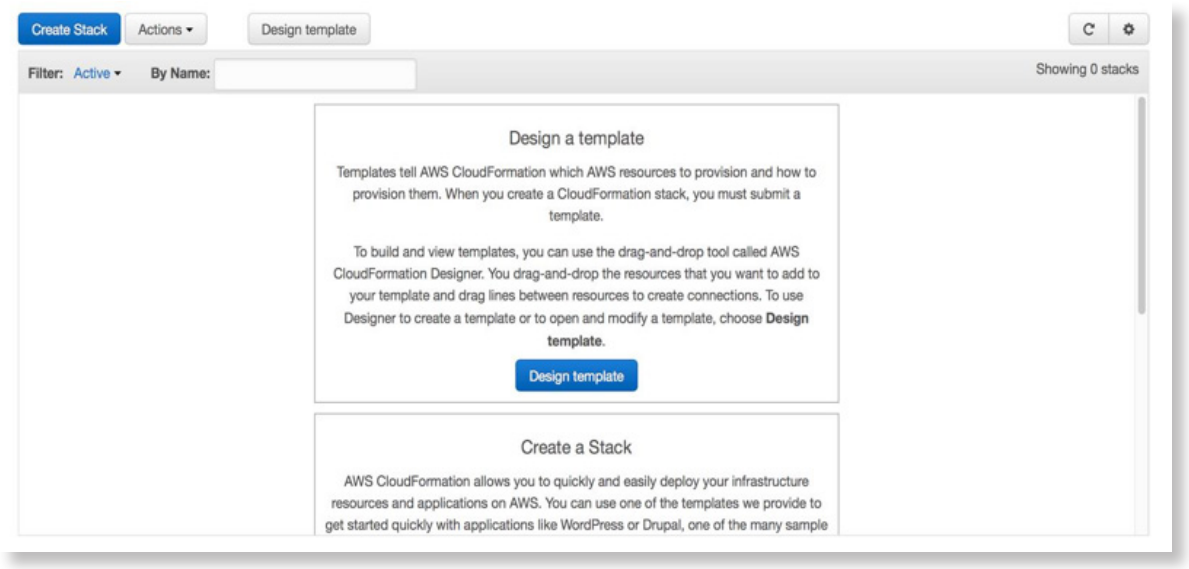
Step 1. Download the CloudFormation template. https://s3.amazonaws.com/fortigatetemplates/FortiGate-HAtemplate5.4.5_ondemand.template

Step 2. Log in to AWS Management Console using your AWS login credentials. https://aws.amazon.com

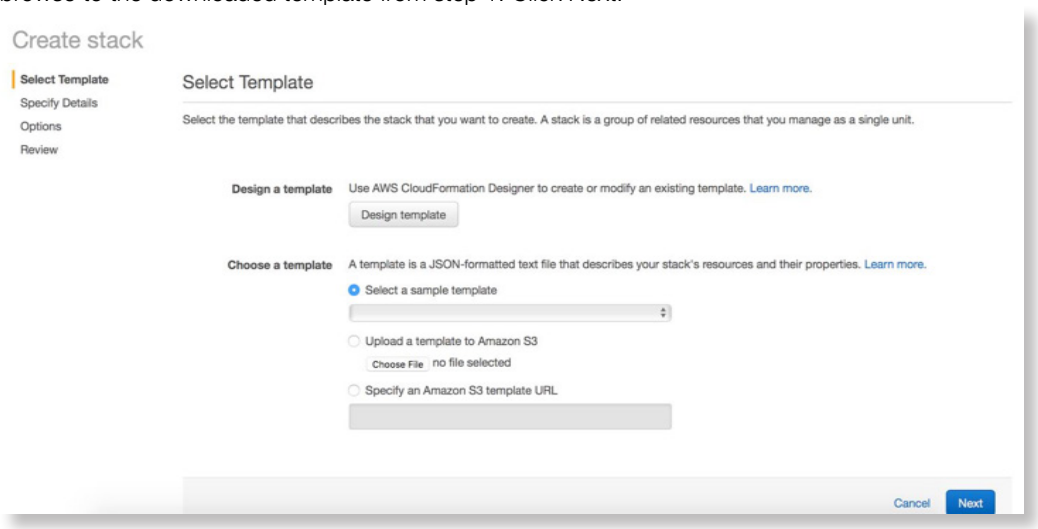
Step 3. Navigate to CloudFormation service in the Management Tools Section of the Management Console.

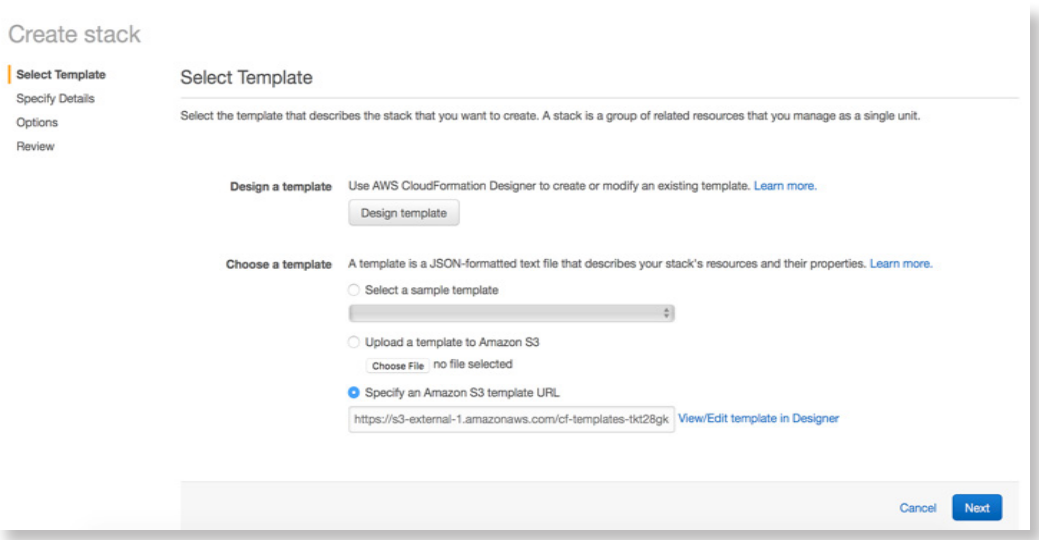


Step 4. Click on Create Stack.



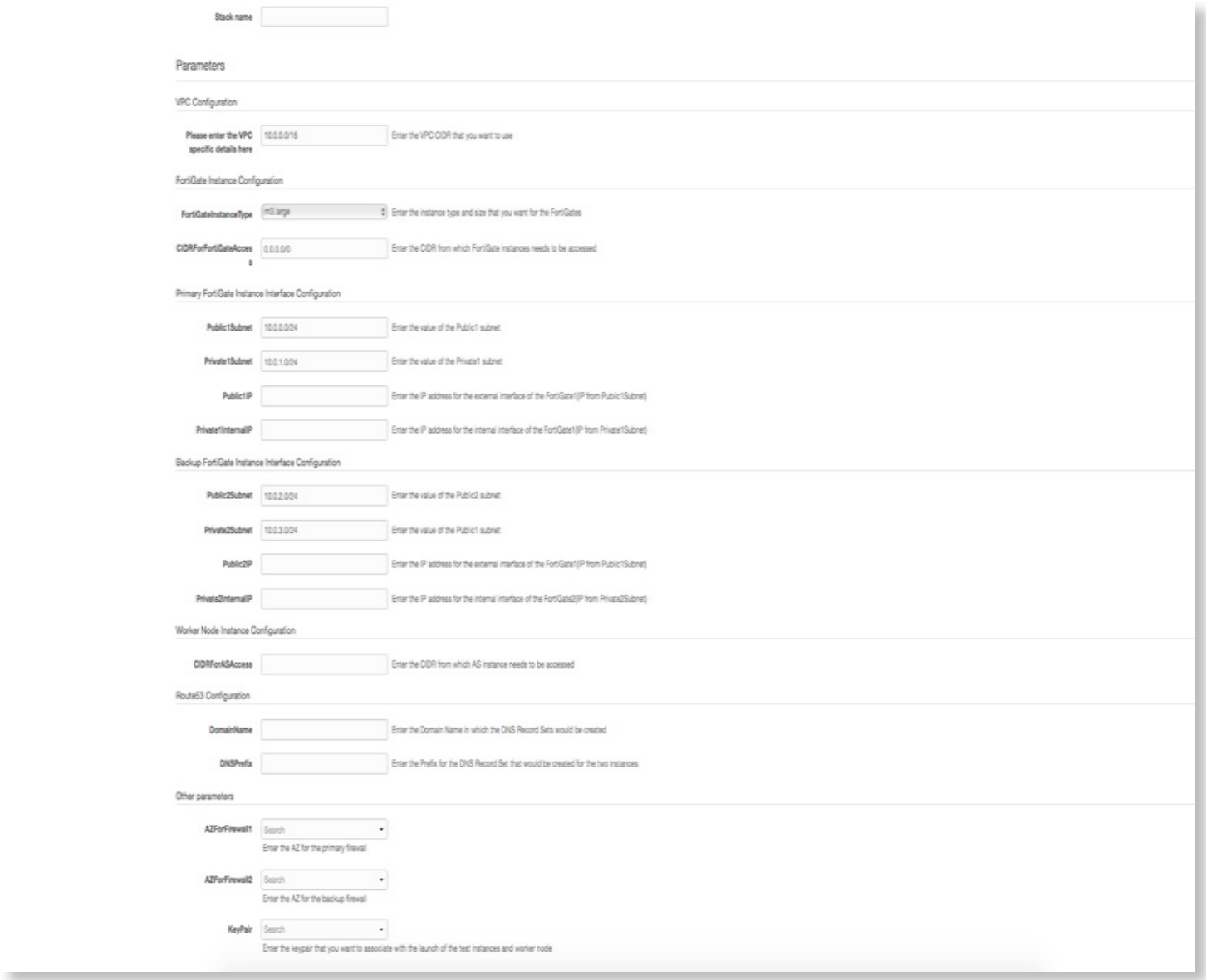
Step 5. Choose the option "**Upload a template to Amazon S3**," click on "**Choose File**," and browse to the downloaded template from step 1. Click Next.



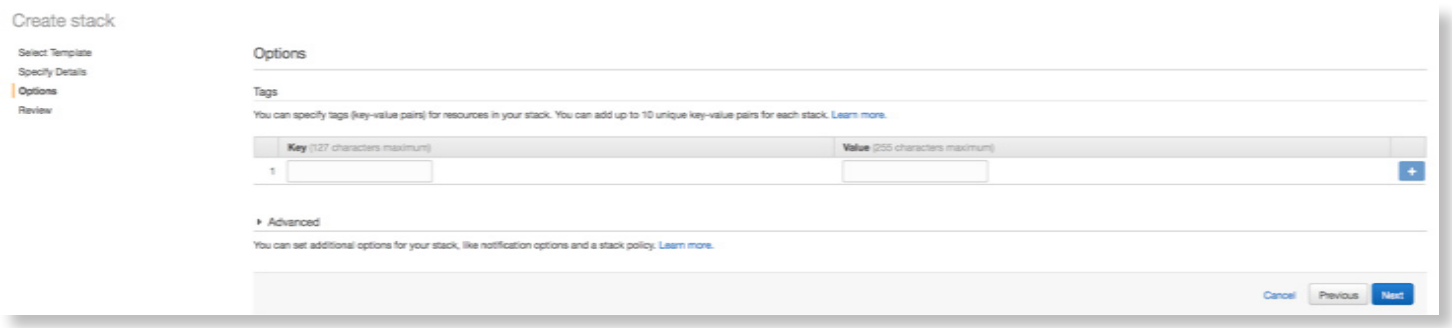


Step 6. Create a stack name to identify the CloudFormation stack.

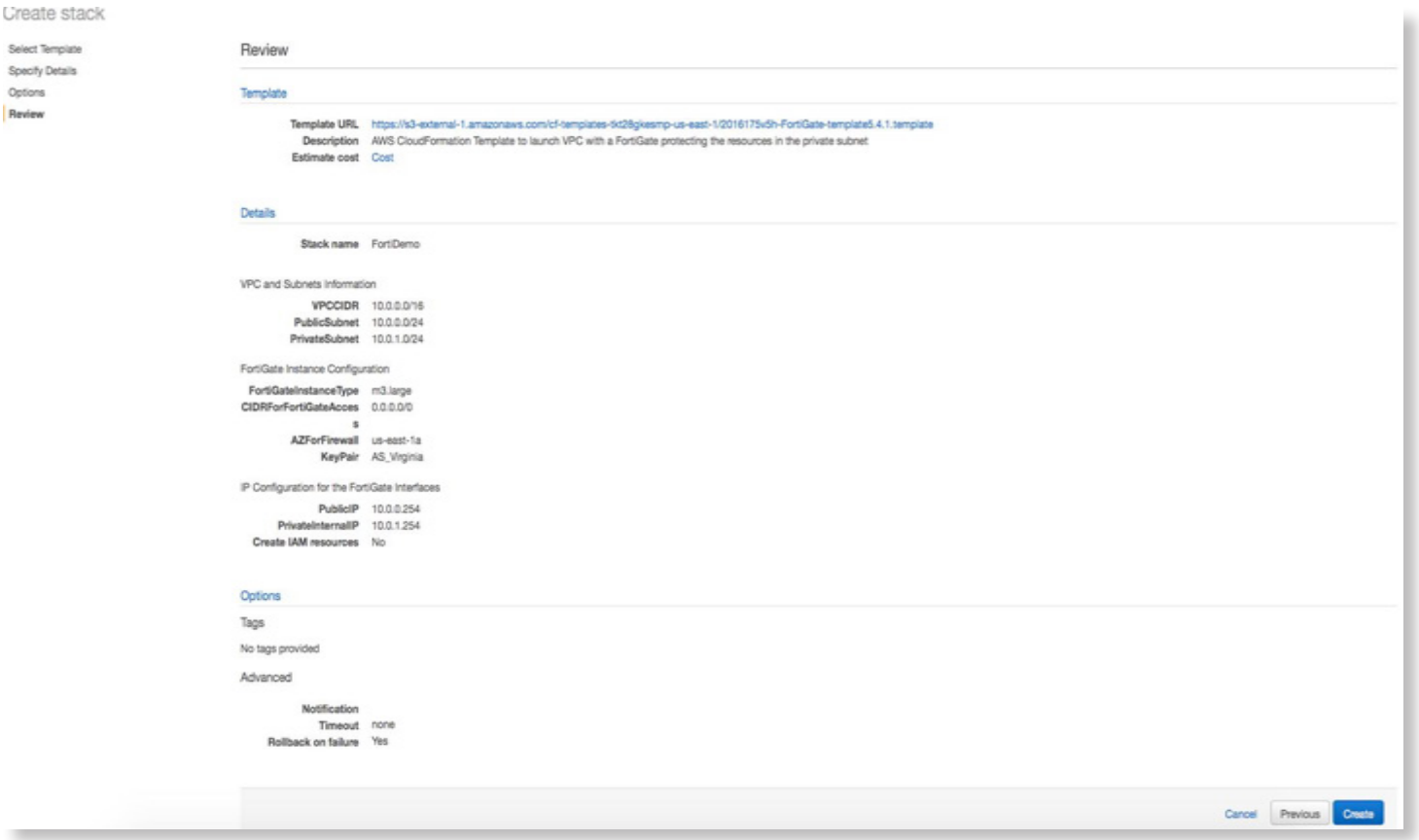
Step 7. Choose the appropriate values for the parameters listed in the parameter section. There are some default values, but these can be changed according to deployment needs. A short description for each parameter is provided to summarize what the parameter is used for and what value to choose. The parameters are split into different sections for convenience. **Make sure to provide information for all the parameters.** The VPC CIDR cannot be greater than /16 and cannot be less than /28. For an AWS recommended fault tolerance, the AZ for each firewall1 and firewall2 should be different. The keypair would be the same keypair that would be used to create the firewalls and the worker node.



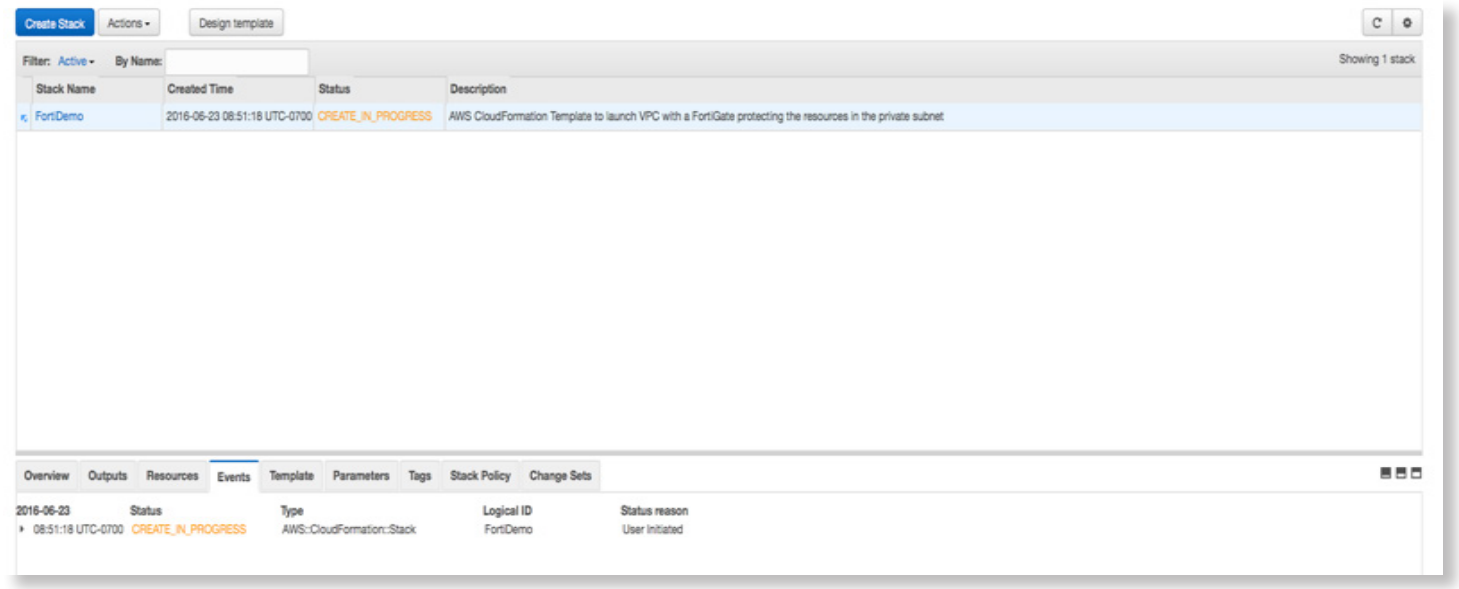
Step 8. Click Next and provide a key name (optional).



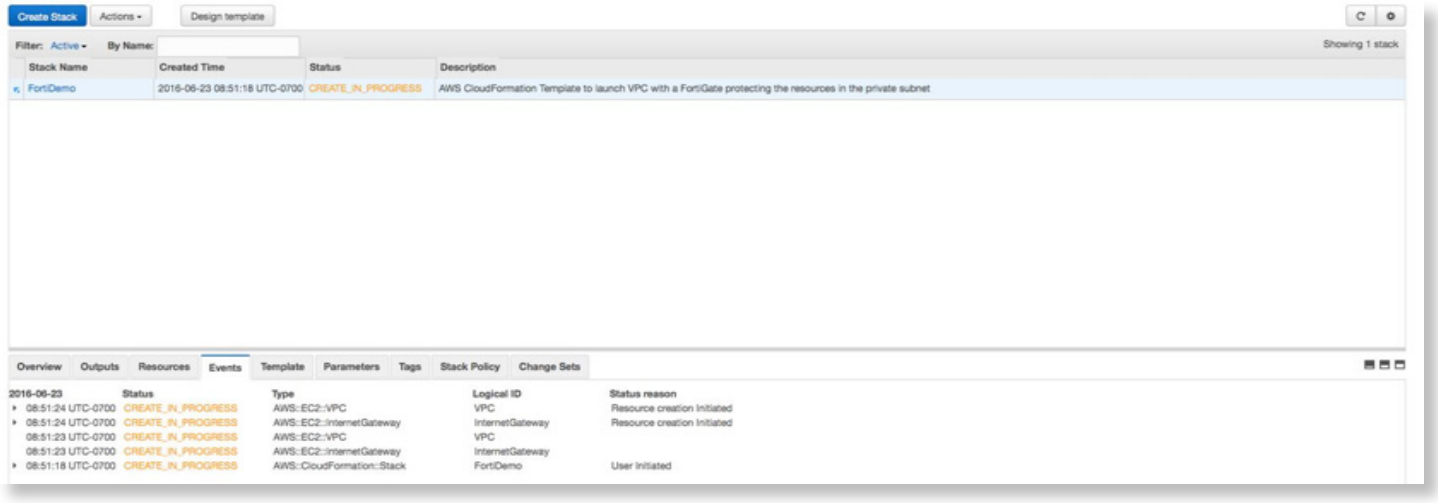
Step 9. Click Create.

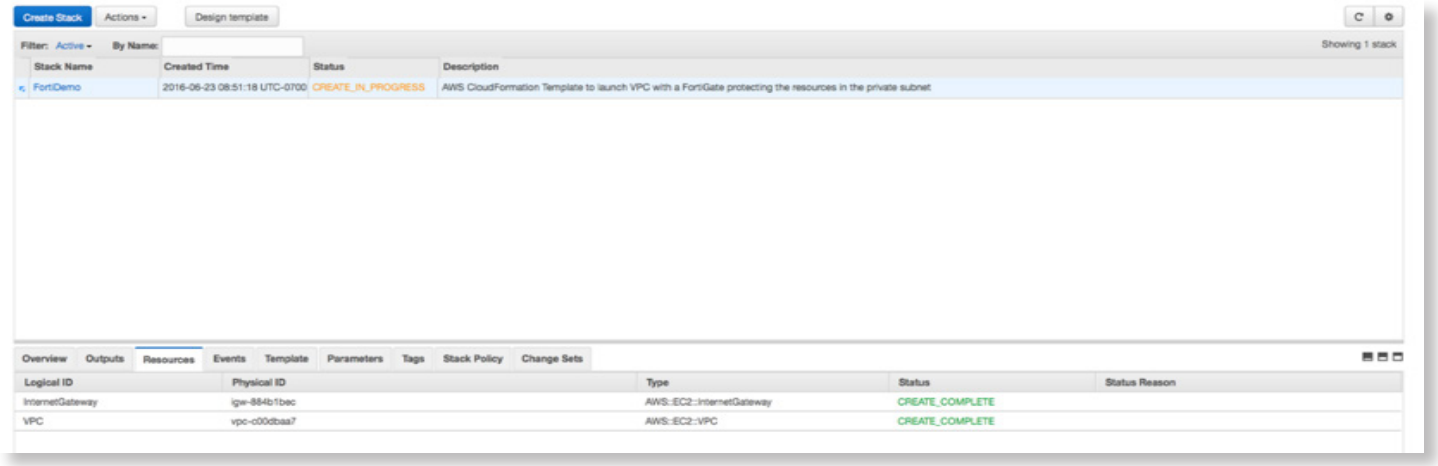


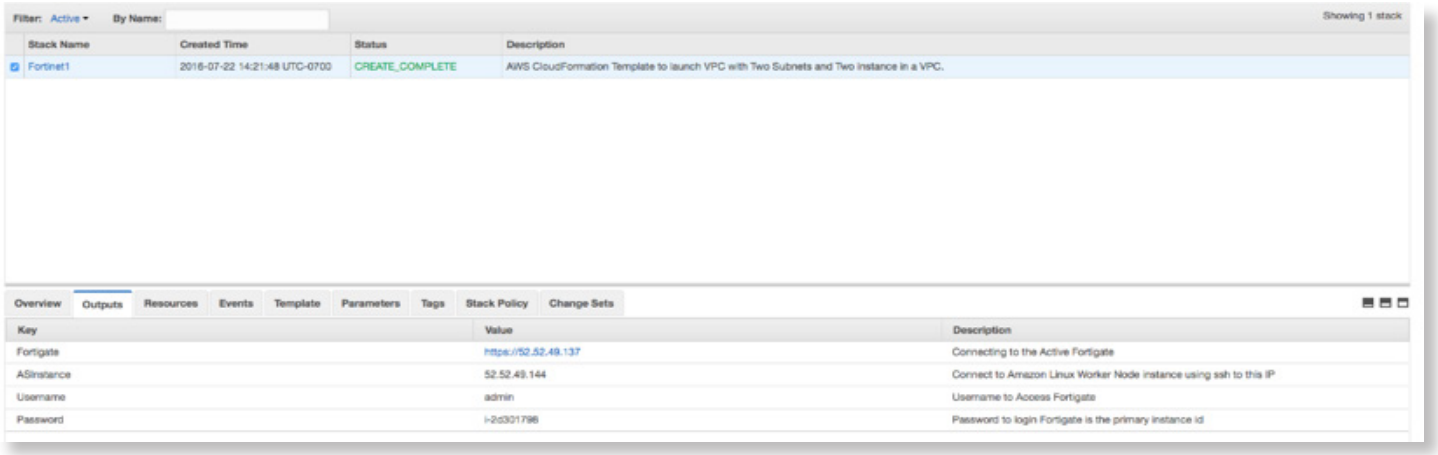
Step 10. Wait for the CloudFormation service to finish creating all the resources. The "**events**" tab should list the information the template is creating. The "**resources**" tab should list the resources as they are created.



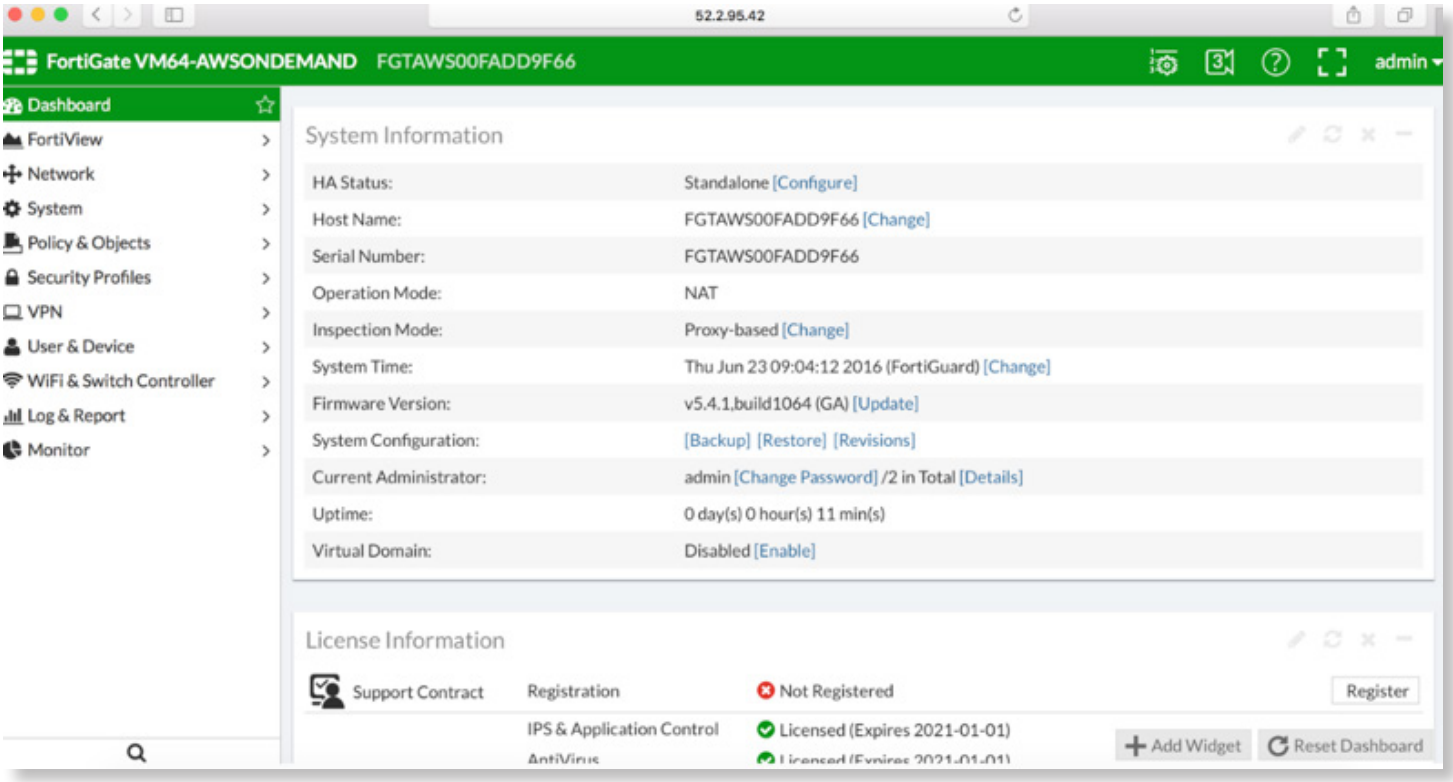
Step 11. Once the stack is created, the Output section has the login information for the Firewall and the Worker Node.





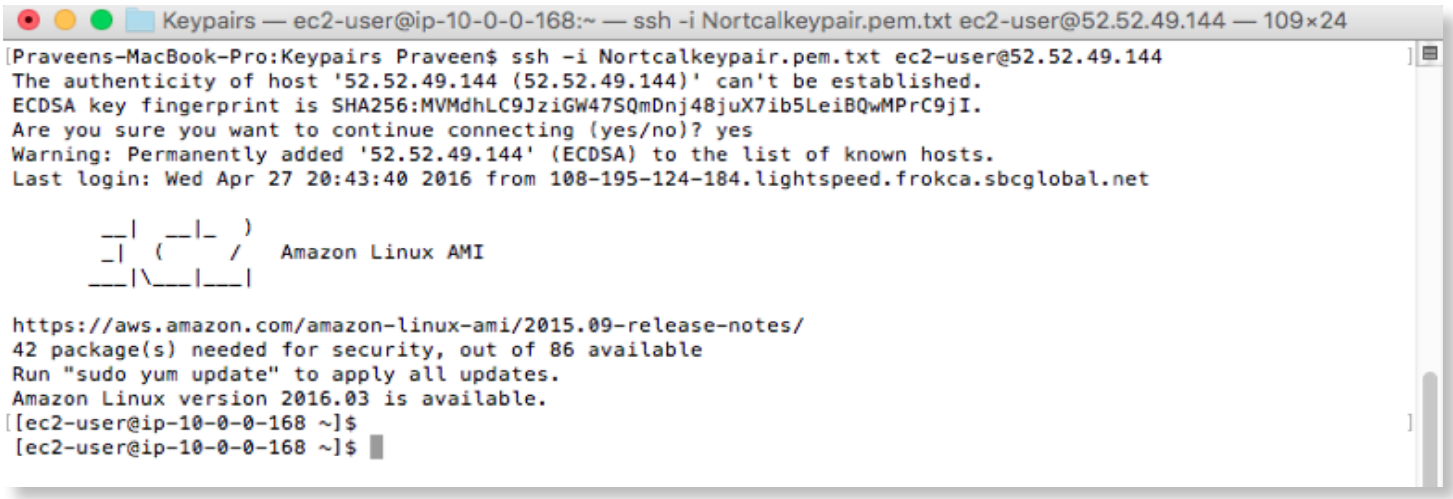


Step 12. Log in to the Firewall through ssh/https; configure the Firewall with your required security features.



Step 13. Log in to the Worker Node through ssh. The IP address of the Worker Node is listed in the results section of the CloudFormation stack. The Worker Node is an Amazon Linux AMI that has the scripts required to monitor the FortiGates.

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EC2_GetStarted.html#ec2-connect-to-instance-linux
Example screenshot of the command to log in and how it looks after login.



Step 14. Navigate to the folder **fortigateha** once you are logged into the worker node. • cd fortigateha

Step 15. Execute the python script fortigateha.py with the runtime variable stack name. **python fortigateha.py**

Once this is done, FortiGate HA setup is complete.

```
Keypairs — ec2-user@ip-10-0-0-168:~/fortigateha — ssh -i Nortcalkeypair.pem.txt ec2-user@52.52.49.144 — 109...
Praveens-MacBook-Pro:Keypairs Praveen$ ssh -i Nortcalkeypair.pem.txt ec2-user@52.52.49.144
The authenticity of host '52.52.49.144 (52.52.49.144)' can't be established.
ECDSA key fingerprint is SHA256:MVMdhLC9JziGW47SQmDnj48juX7ib5LeiBQwMPrC9jI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '52.52.49.144' (ECDSA) to the list of known hosts.
Last login: Wed Apr 27 20:43:40 2016 from 108-195-124-184.lightspeed.frokca.sbcglobal.net

       __|  __|_  )
       _|  (     /   Amazon Linux AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-ami/2015.09-release-notes/
42 package(s) needed for security, out of 86 available
Run "sudo yum update" to apply all updates.
Amazon Linux version 2016.03 is available.
[ec2-user@ip-10-0-0-168 ~]$
[ec2-user@ip-10-0-0-168 ~]$ cd fortigateha/
[ec2-user@ip-10-0-0-168 fortigateha]$
```

```
Praveen — ec2-user@ip-10-0-0-168:~/fortigateha — ssh -i Desktop/Keypairs/Nortcalkeypair.pem.txt ec2-user@52.52.49...
[ec2-user@ip-10-0-0-168 fortigateha]$ python fortigateha.py Fortinet1
```

Step 16. Once the script is started, the output will look like:

```
Praveen — ec2-user@ip-10-0-0-168:~/fortigateha — ssh -i Desktop/Keypairs/Nortcalkeypair.pem.txt ec2-user@52.52.49...

[ec2-user@ip-10-0-0-168 fortigateha]$ python fortigateha.py Fortinet1
The Primary Instance is i-2d301798
The Backup Instance is i-e3117da6
The primary IP is 10.0.0.254
PING 10.0.0.254 (10.0.0.254) 56(84) bytes of data.
64 bytes from 10.0.0.254: icmp_seq=1 ttl=255 time=0.668 ms

--- 10.0.0.254 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.668/0.668/0.668/0.000 ms
The primary IP is 10.0.0.254
PING 10.0.0.254 (10.0.0.254) 56(84) bytes of data.
64 bytes from 10.0.0.254: icmp_seq=1 ttl=255 time=0.482 ms

--- 10.0.0.254 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.482/0.482/0.482/0.000 ms
The primary IP is 10.0.0.254
PING 10.0.0.254 (10.0.0.254) 56(84) bytes of data.
64 bytes from 10.0.0.254: icmp_seq=1 ttl=255 time=0.462 ms

--- 10.0.0.254 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
```

Congratulations: You have created an active:passive automated HA architecture in your AWS VPC.

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

116380-0-0-EN September 11, 2017