VM-Series for AWS

Auto Scaling GlobalProtect in AWS Deployment Guide

Last Update: May 2016

http://www.paloaltonetworks.com

Table of Contents

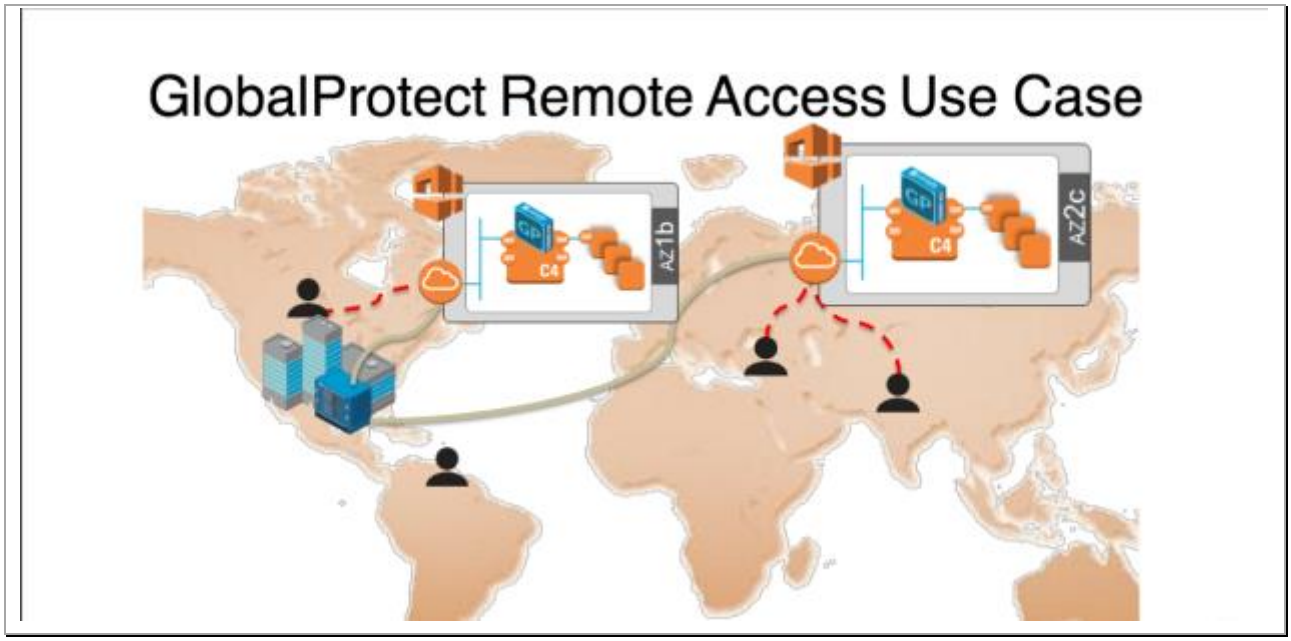
1. Global Protect

GlobalProtect allows remote users to access corporate resources and internet resources using the same security policy enforcement as though there were on premises. To provide Next-Generation Security Platform closer to the remote users, GlobalProtect gateways can be deployed in AWS. This allows instantiation of portals and gateways near remote users without the additional cost of infrastructure.

Leveraging the global presence and built in redundancy provided by AWS, GlobalProtect can be quickly deployed worldwide where your users are. Traffic is inspected with the same PAN-OS security as the corporate firewall but in a globally diverse deployment. The result is security that follows users – even when they are mobile and a better user experience.

2. GlobalProtect and Auto Scaling

Deploying GlobalProtect on AWS provides the ability to scale as needed to address both planned and unplanned scaling demands. Planned scaling may be need for known events such as the initial login rush that occurs every day and then then drop off that may occur at the end of the day. Another scenario may be a conference or sales kick-off where many users all try to connect at once to a regional gateway. Unplanned demand may be associated with events such as “snowmageddon” where users are snowed in and work from home.



3. About CFTs

AWS CloudFormation Templates (CFTs), are JSON files that can launch nearly all AWS resources including VPCs, subnets, security groups, route tables, plus many more. AWS CFTs are used for ease of deployment and are key to any auto-scaling environment.

For more information on CFTs and sample CFTs refer to Amazon's documentation

https://aws.amazon.com/cloudformation/aws-cloudformation-templates/

There are also many sample templates available here https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/sample-templates-services-us-west-2.html

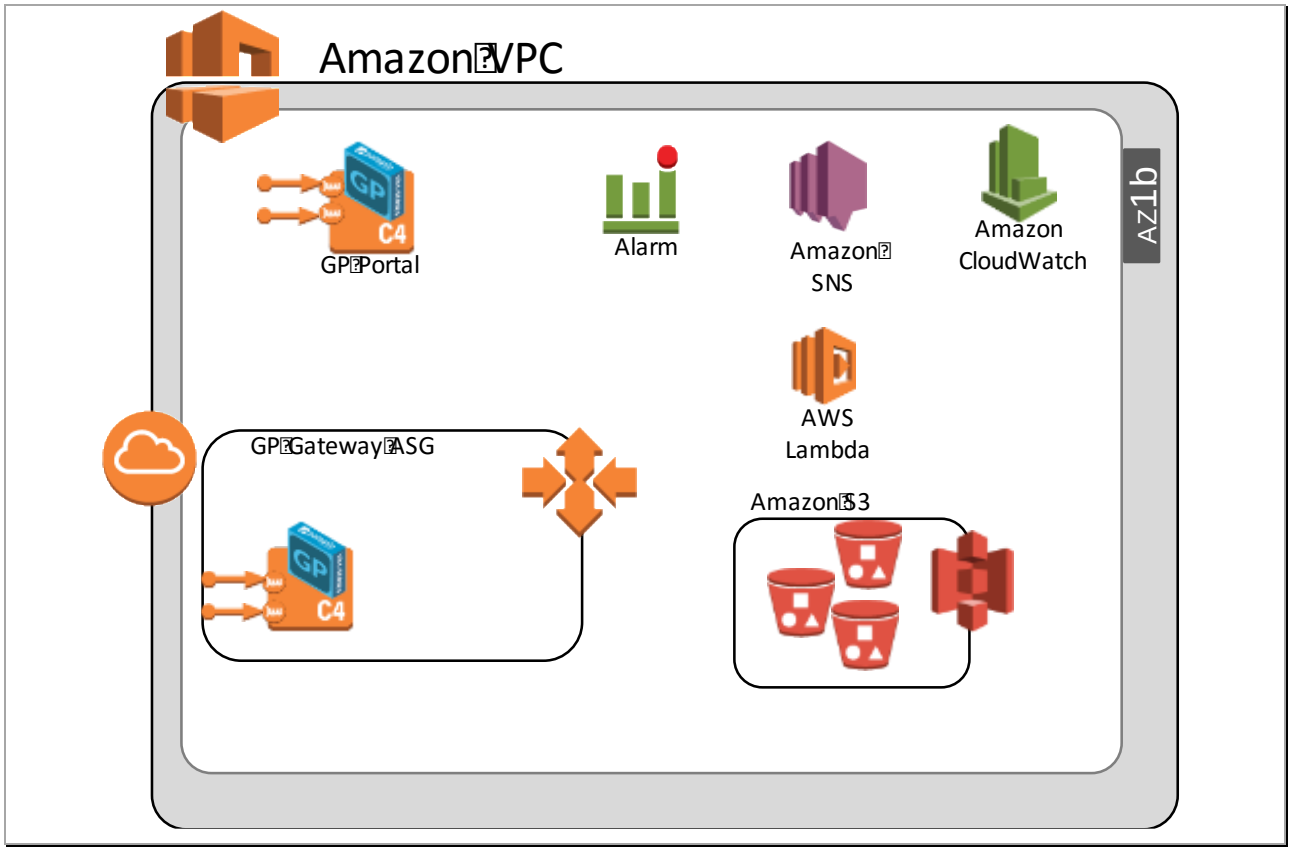
Additional templates provided by Palo Alto Networks can be found on the following Github page

https://github.com/paloaltonetworks/aws

4. About this guide

This guide will walk through the process of launching an AWS CFT that will deploy a GlobalProtect Portal and an AWS AutoScaling group with the ability to automatically launch and configure additional GlobalProtect Gateways based on customizable thresholds.

The template referenced by this document will deploy all the resources needed for the purposes of this demo and setup the appropriate permissions and get to the topology below:



This solution provides a good starting point to understand how to deploy a Global Protect solution in AWS w/ dynamic scaling.

If new to Cloudformation templates, please refer to the following guide:

https://s3-us-west-2.amazonaws.com/sample-cft/AWS_CFT_How_To_Guide_v7.docx

5. AWS Services Used

The template utilizes several AWS services. Some of the main ones are:

5.1 AWS Auto Scaling

Auto Scaling is an AWS service designed to launch or terminate Amazon EC2 instances automatically based on user-defined policies, schedules, and health checks. Auto Scaling Groups (ASG) define minimum EC2 instances, maximum EC2 instances, and metrics used to determine when to scale in or scale out.

https://docs.aws.amazon.com/autoscaling/latest/userguide/WhatIsAutoScaling.html

5.2 AWS Lambda

AWS lambda is a compute (micro)service that allows a user to run small snippets of code (JavaScript or Python scripts) to accomplish various tasks. This eliminates the use of Linux instances as worker nodes and having to maintain them.

https://docs.aws.amazon.com/lambda/latest/dg/welcome.html

Note: AWS Lambda service is currently only available in 4 regions (Northern Virginia, Oregon, Frankfurt, Ireland and Tokyo). Please refer to the following page to check for further updates: https://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/

5.3 Amazon S3

Amazon Simple Storage Service is storage service where the necessary scripts and bootstrap files are stored.

https://docs.aws.amazon.com/AmazonS3/latest/dev/Introduction.html

5.4 Amazon SNS

Amazon Simple Notification Service is a web service that coordinates and manages the delivery or sending of messages to subscribing endpoints or clients. In this case the service is used to send messages to trigger Lambda functions

https://docs.aws.amazon.com/sns/latest/dg/welcome.html

5.5 Amazon CloudWatch

Amazon CloudWatch monitors your Amazon Web Services (AWS) resources and the applications you run on AWS in real-time. You can use CloudWatch to collect and track metrics, which are the variables you want to measure for your resources and applications. CloudWatch alarms send notifications or automatically make changes to the resources you are monitoring based on rules that you define.

https://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/WhatIsCloudWatch.html

6. Template Deployment Prerequisites

Here are the prerequisites required to successfully launch this template.

6.1 Create an AWS account

If you do not have an AWS account already, go to https://aws.amazon.com/console/ and create an account.

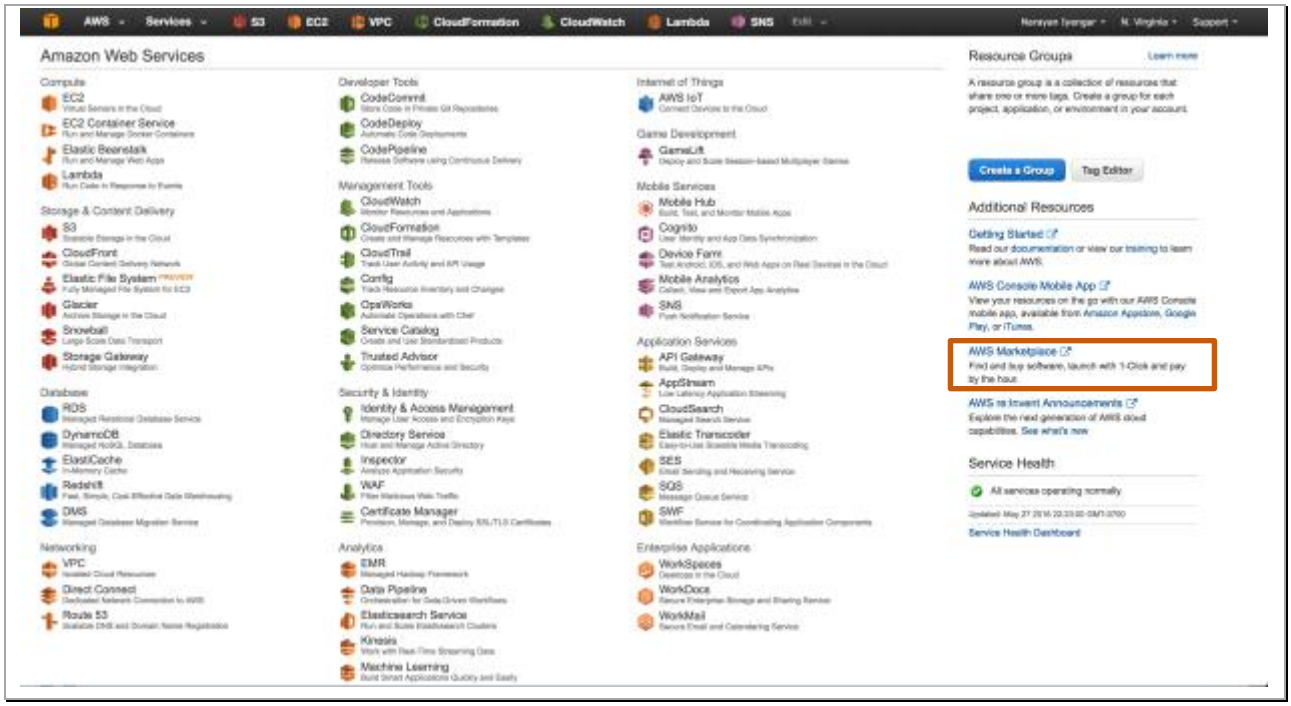
6.2 Add a credit card to your AWS account

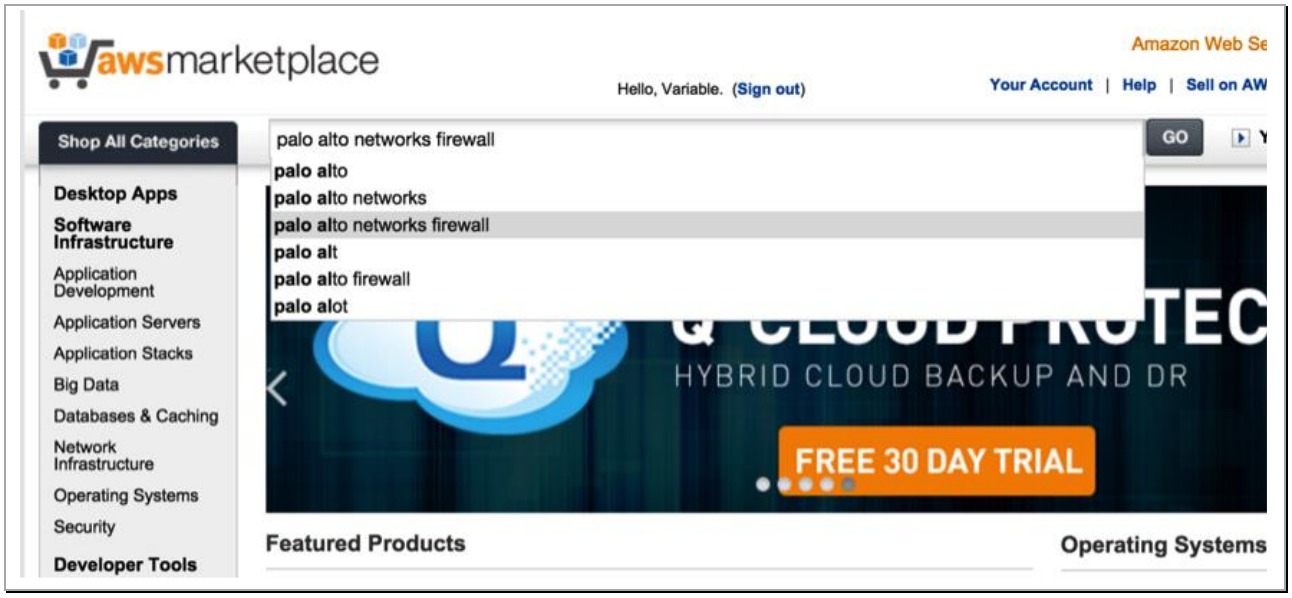
In order to continue you will need to add a method of payment to your AWS account. Use the following https://console.aws.amazon.com/billing/home#/paymentmethods

If creating a new account, you may receive a phone call from AWS for verification purposes.

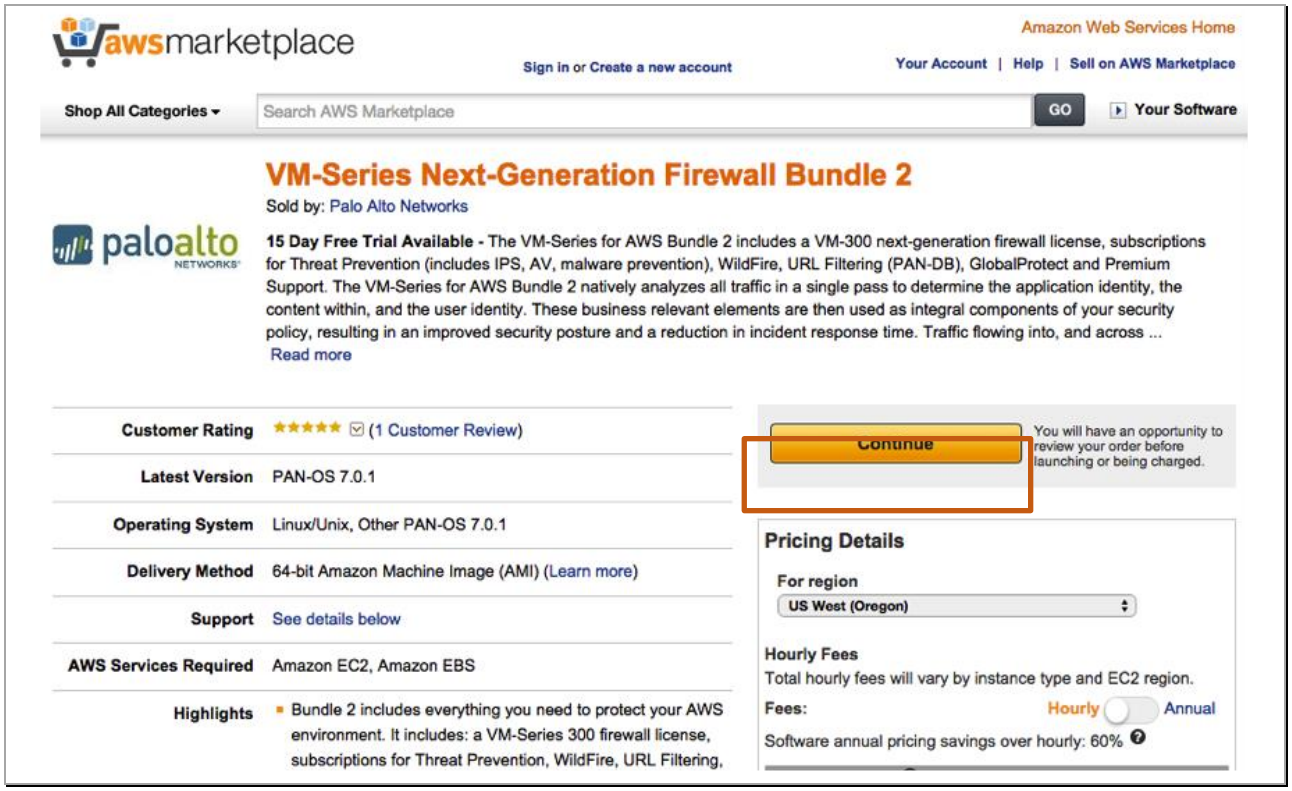
6.3 Review and accept the EULA

If this is your first time using AWS to launch a VM-Series firewall bundle, you will need to review and accept the software license agreement for the VM-Series.
Click on **AWS Marketplace** and search for **Palo Alto Networks firewall**:

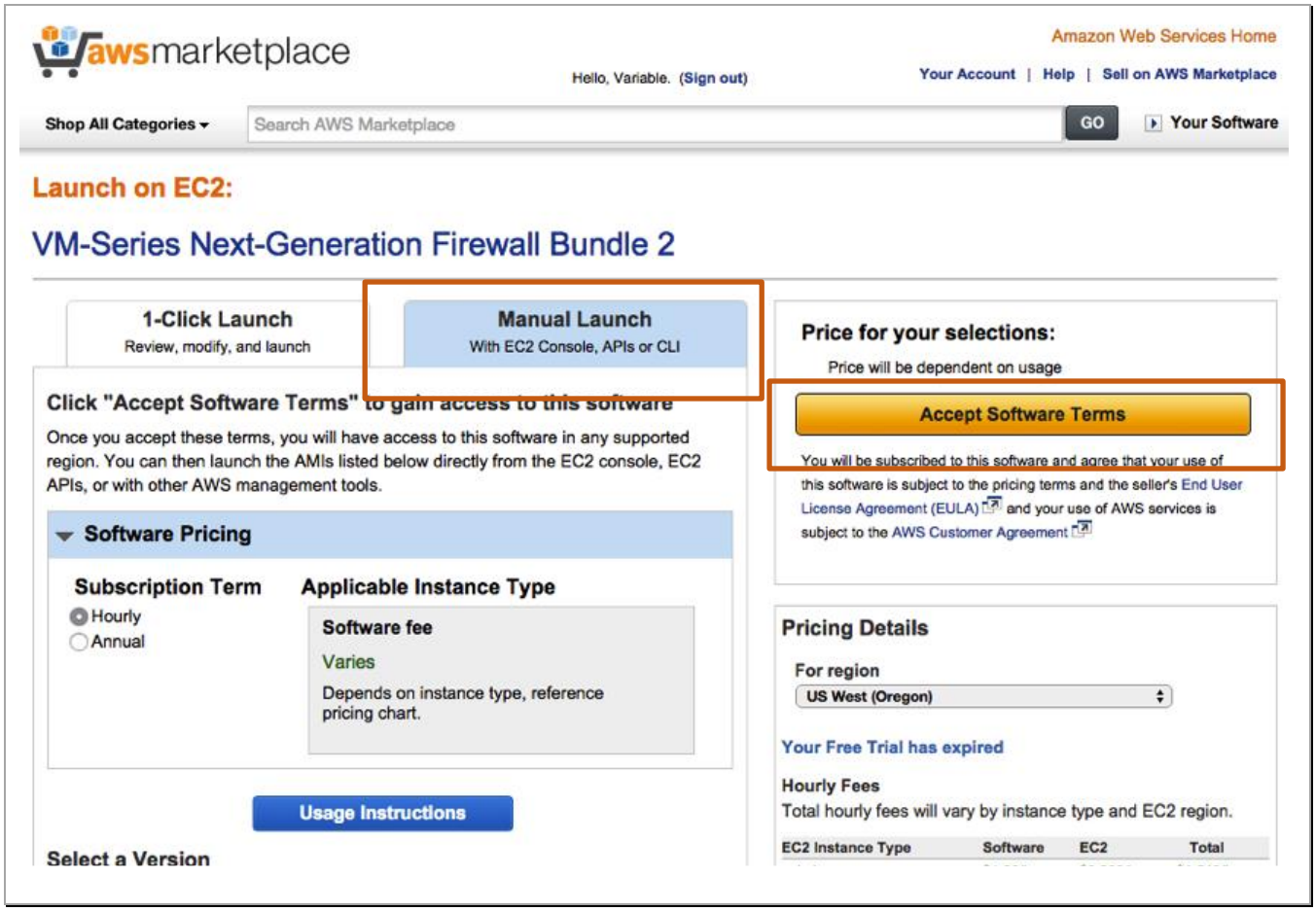




Select **VM-Series Next Generation Firewall Bundle 2**

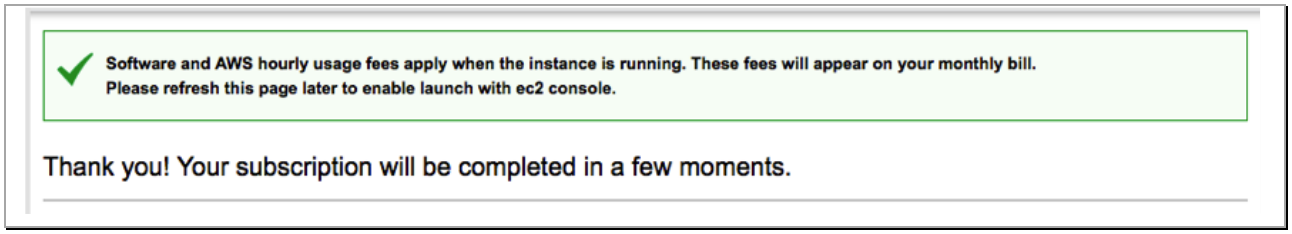


Click **Continue**.



Click on **Manual** Launch, Review the agreement and then click **Accept Software Terms**

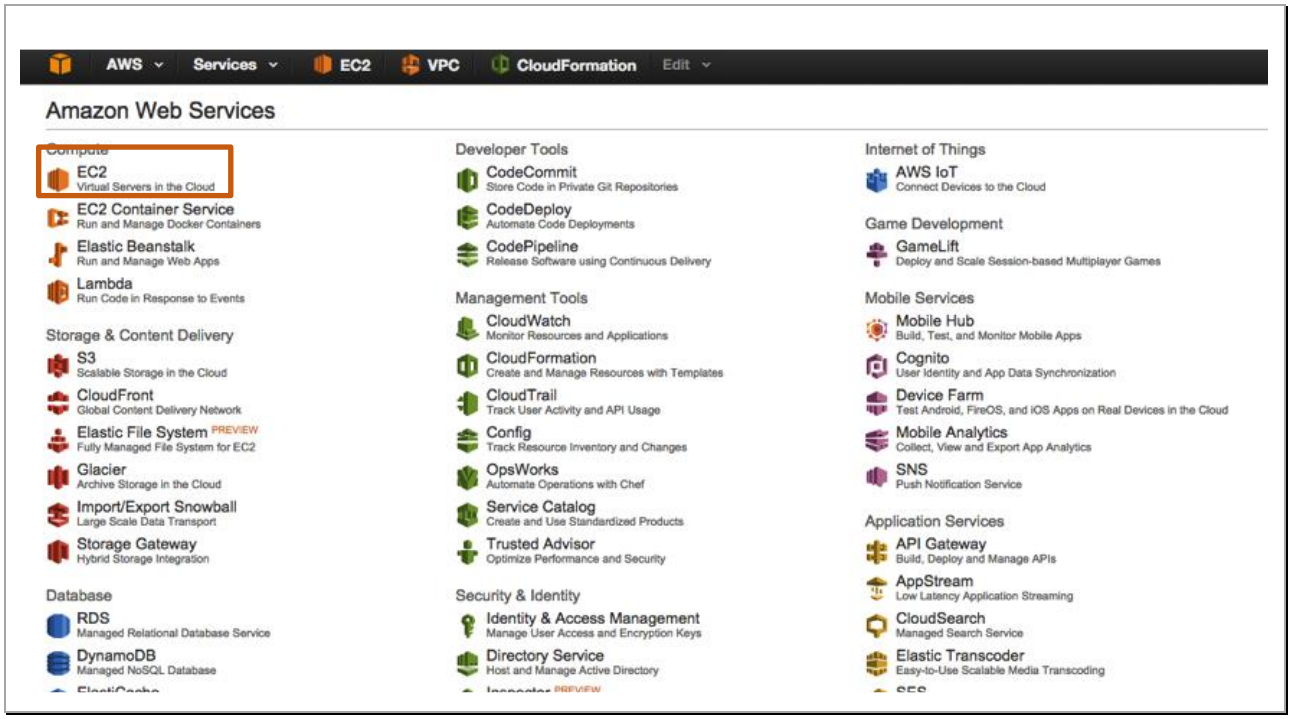
You should see this screen:



You can now close the browser tab or window and continue with the next step.

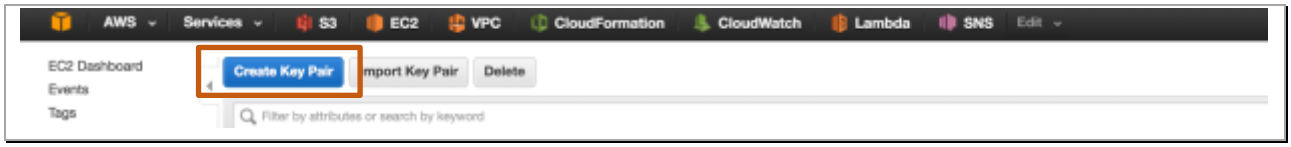
6.4 Create and download an SSH keypair

Sign into the AWS console https://www.amazon.com and click on **EC2**

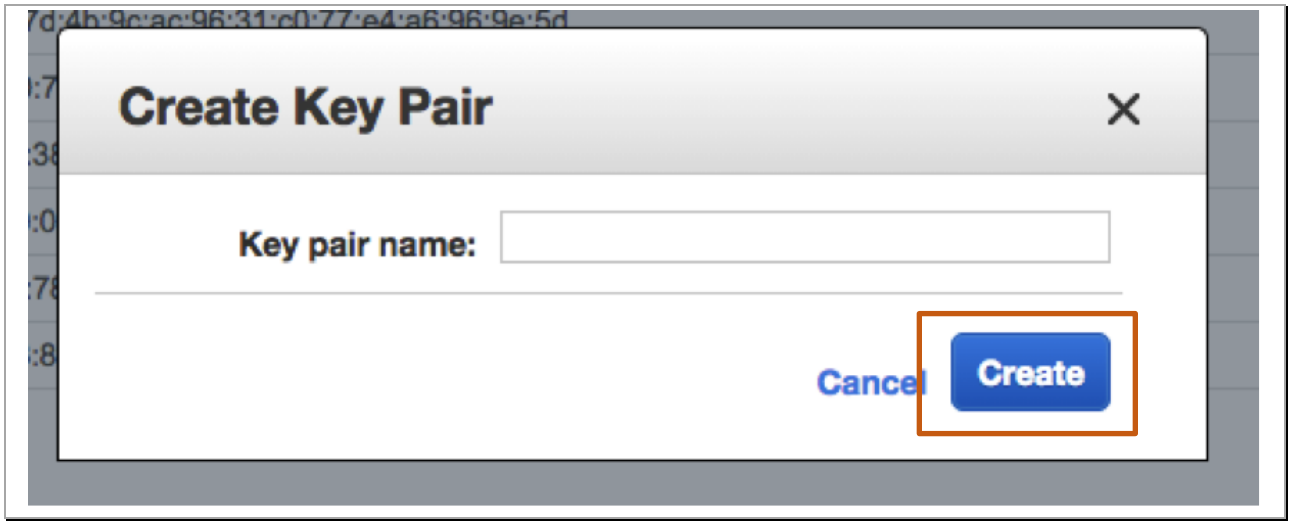


Click **KeyPairs**

Click **Create Key Pair**



Give the key-pair a name:



And click **Create**. This should now prompt you to save the just generated private key. Save the key.

7. PAN-OS Prerequisites

This template relies on the bootstrapping feature that is part of PAN-OS 7.1. For more information on bootstrapping the VM-Series in AWS please refer to the following documentation:
https://www.paloaltonetworks.com/documentation/71/virtualization/virtualization/bootstrap-the-vm-series-firewall/bootstrap-the-vm-series-firewall-in-aws

8. Download the Files

The CloudFormation template can be found here:

https://github.com/PaloAltoNetworks/aws/blob/master/globalprotect-asg/gp-asg.json

The bootstrap files can be found here:

https://github.com/PaloAltoNetworks/aws/blob/master/globalprotect-asg/bootstrap-gateway.zip

https://github.com/PaloAltoNetworks/aws/blob/master/globalprotect-asg/bootstrap-portal.zip

And the accompanying scripts can be found here:

https://github.com/PaloAltoNetworks/aws/blob/master/globalprotect-asg/config_fw.zip

Download and save the gp-asg.json, config_fw.zip, bootstrap-gateway.zip and bootstrap-portal.zip files and store them in a known locations.

Unzip the bootstrap-gateway.zip and bootstrap-portal.zip files into their corresponding directories.

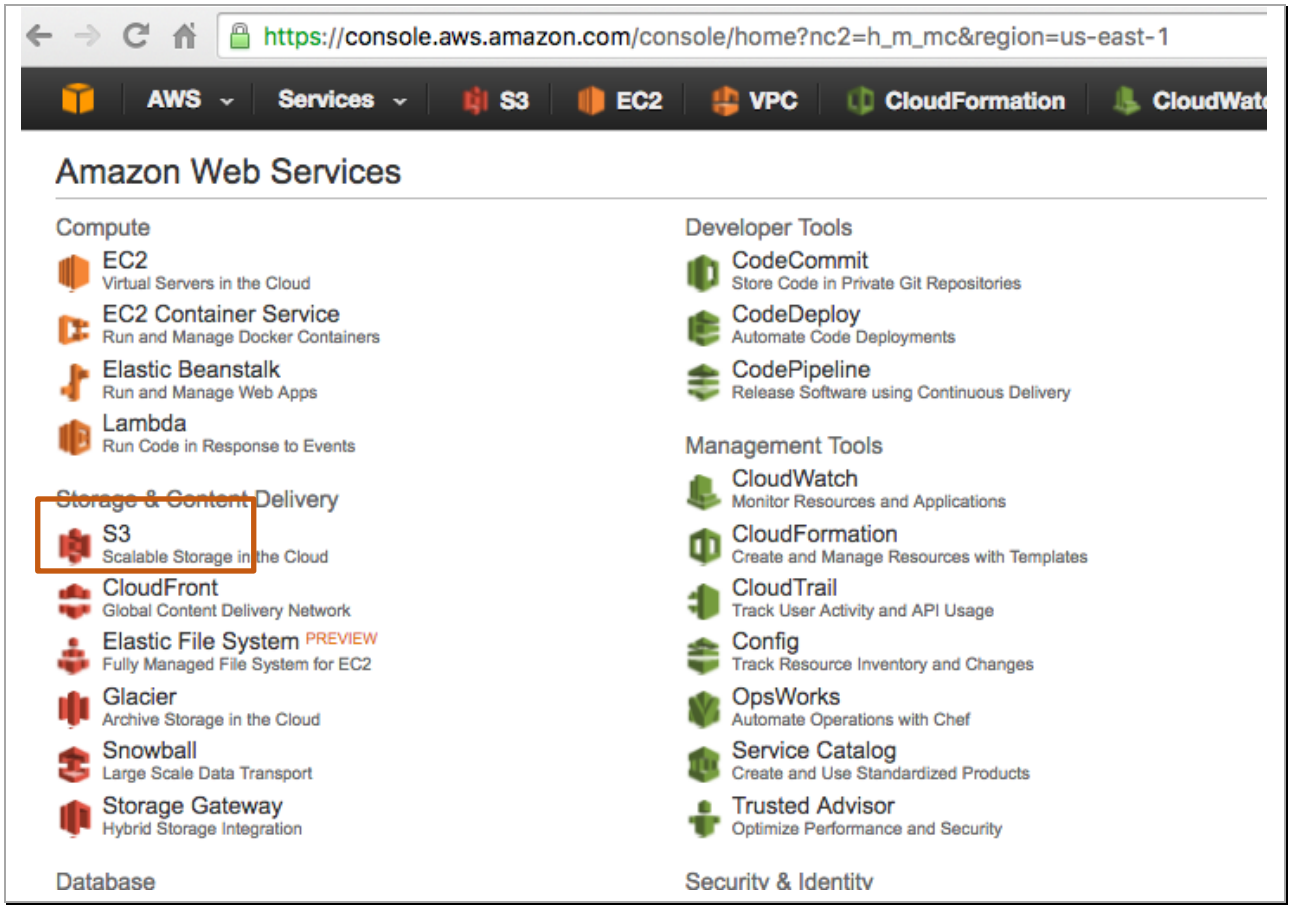
The “bootstrap-gateway” and “bootstrap-portal” directories have bootstrapping and configuration information for the gateways and portal respectively.

They also have configuration information that configures the firewall as a GlobalProtect Gateway or GlobalProtect Portal.

The config_fw.zip file contains all the necessary lambda scripts

9. Create S3 Buckets

In order to launch the demo template three S3 buckets will be required. Log into the AWS console and click on **S3:**

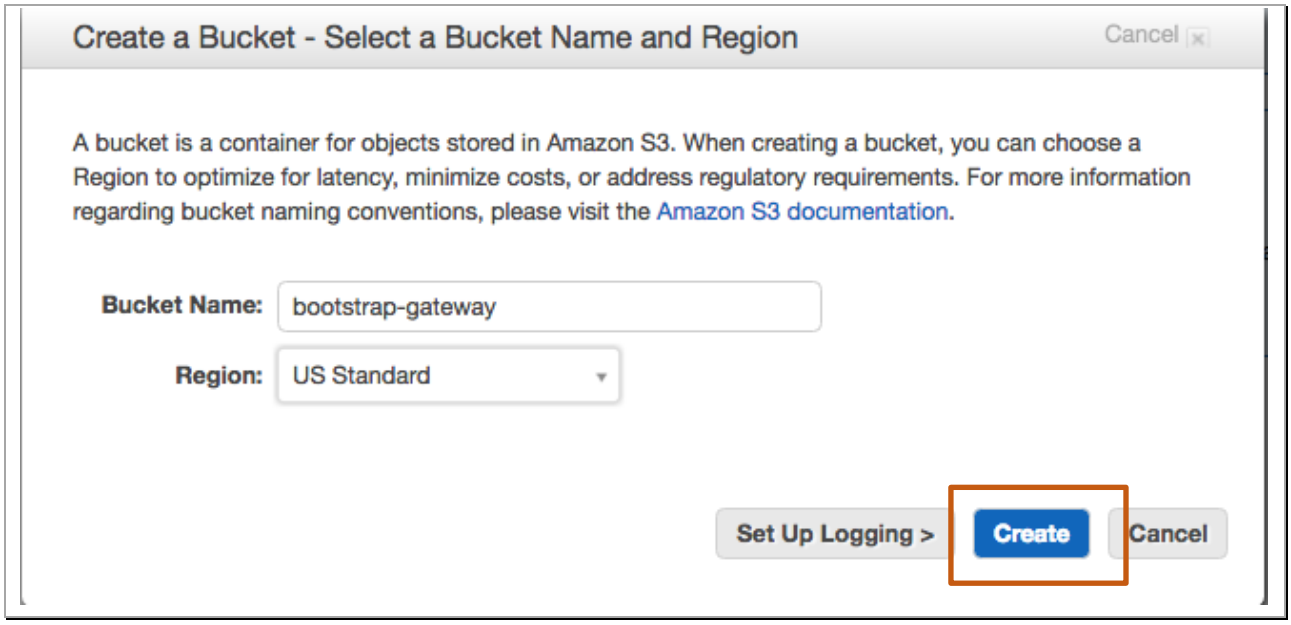


And click “**Create Bucket”** button**:**

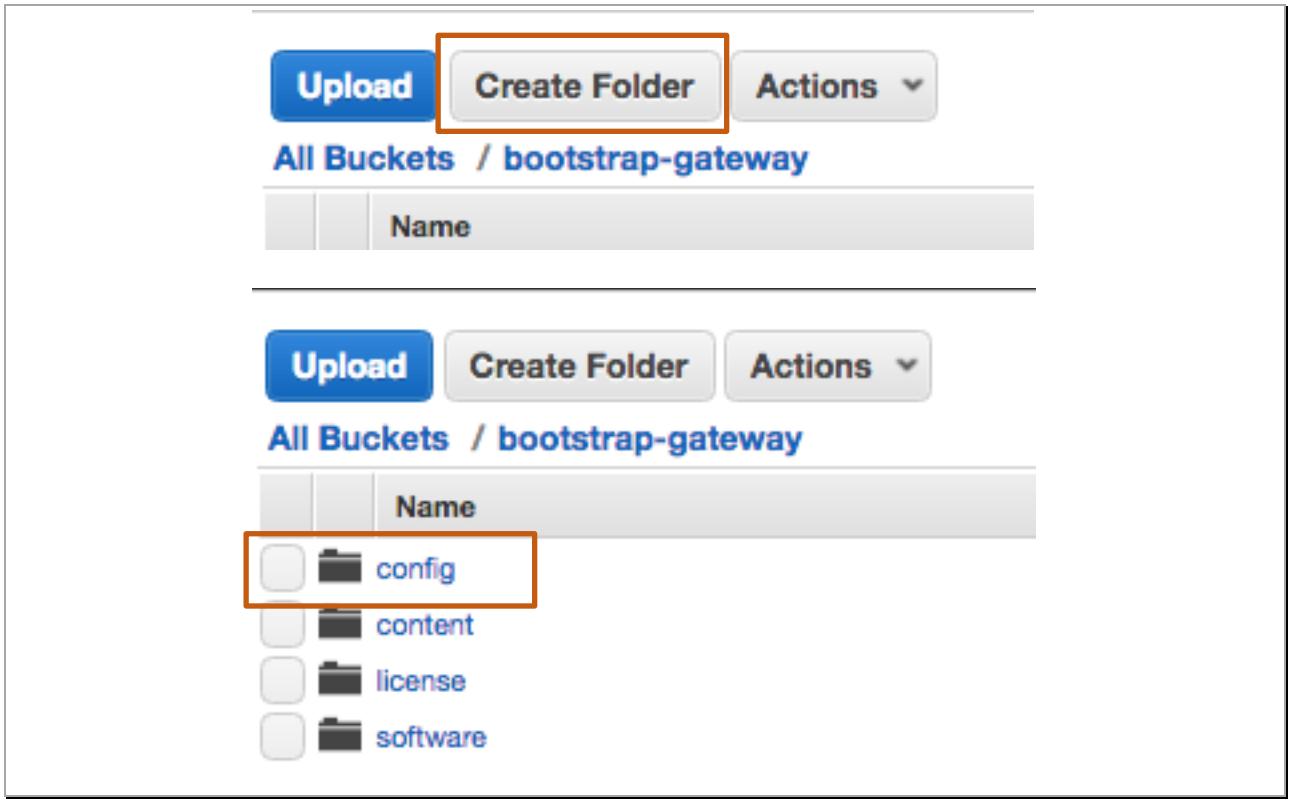
Type-in a bucket name (needs to be unique) and select the region in which the bucket will reside. This should be the same region where the template will be deployed ***and*** Lambda is available. This bucket will be used to store bootstrap files for the GP Gateway.

Note: Keep in mind that as of writing this document AWS lambda is only supported in 5 regions (N. Virginia, Oregon, Ireland, Frankfurt, and Tokyo).

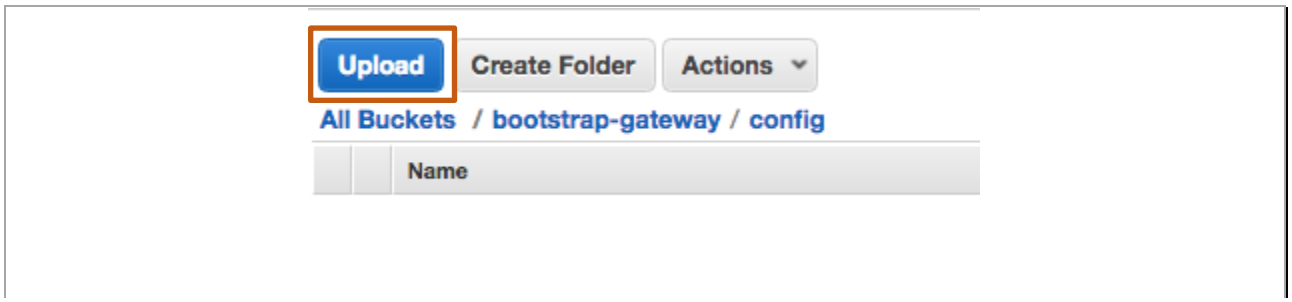
Note: If launching the CFT in N. Virginia, select the region as "**US Standard"**

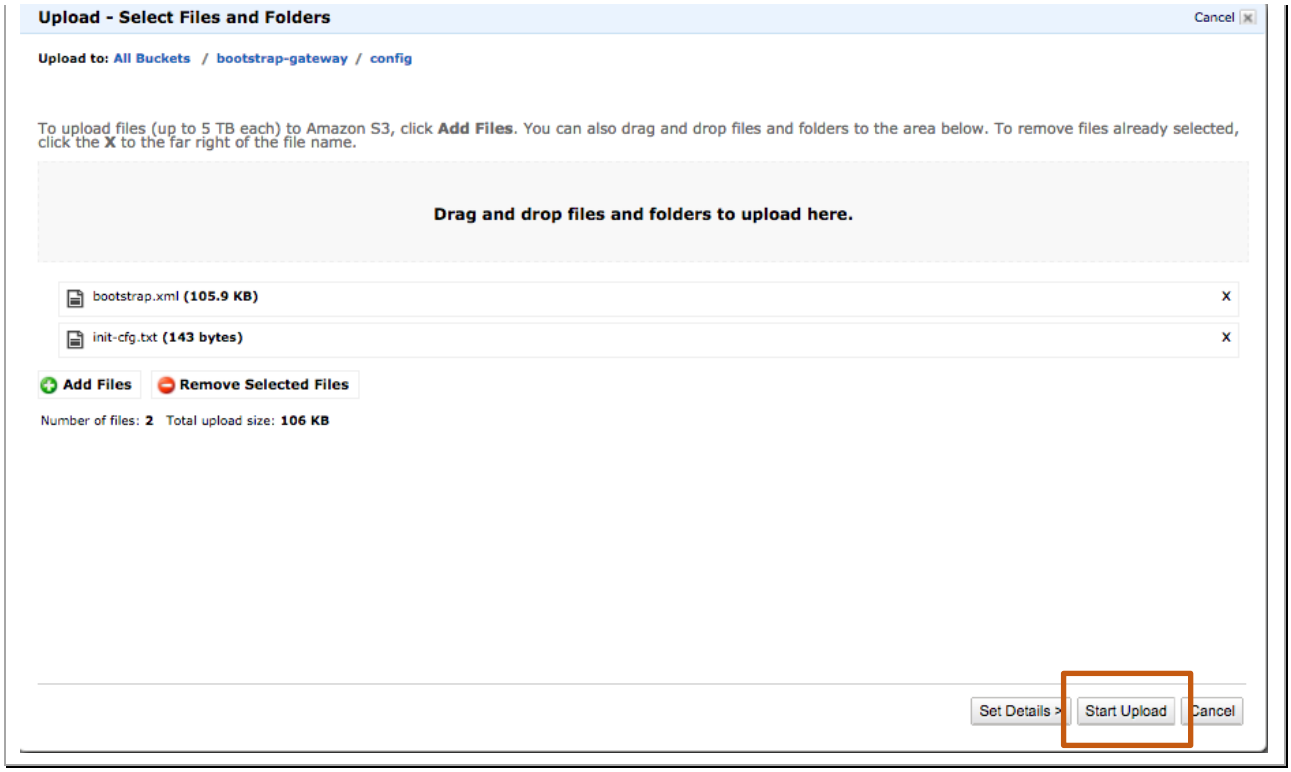


Once the bucket is created, click on the bucket name to navigate to the bucket and create **four** sub-buckets called **config, content, license** and **software** respectively. Navigate to the **config** bucket and click "**Upload"**



In the next dialog box, drag and drop the two files – **init-cfg.txt** and **bootstrap.xml** from the **gateway** folder created in the previous step and click "**Start Upload**":



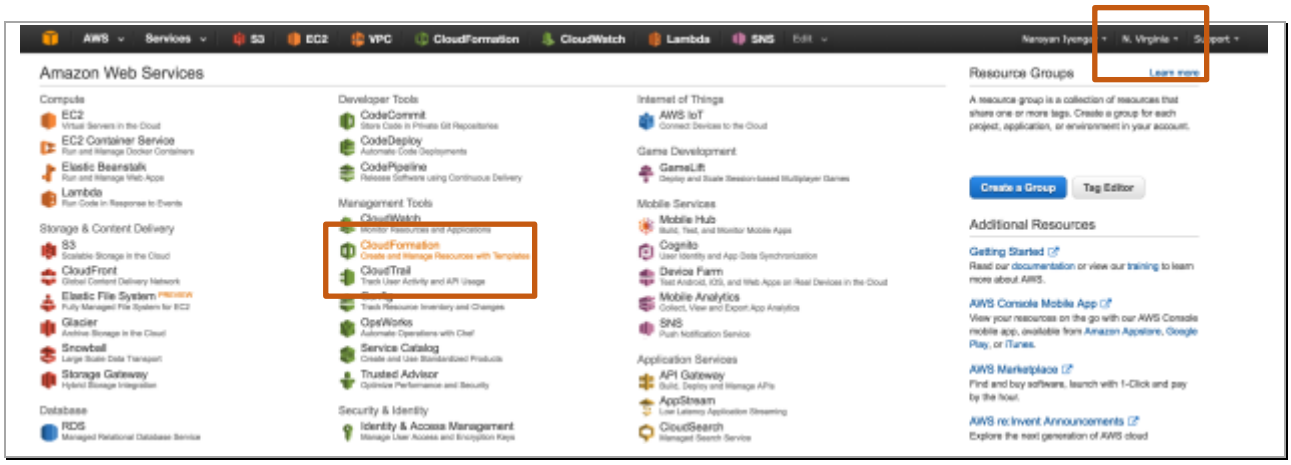


Repeat the above steps and create a bucket to upload the portal's bootstrap configuration files.

Lastly create an S3 bucket in the same region as the gateway and portal bootstrap buckets and upload the config_fw.zip file into that bucket (this is the bucket where the lambda scrips reside).

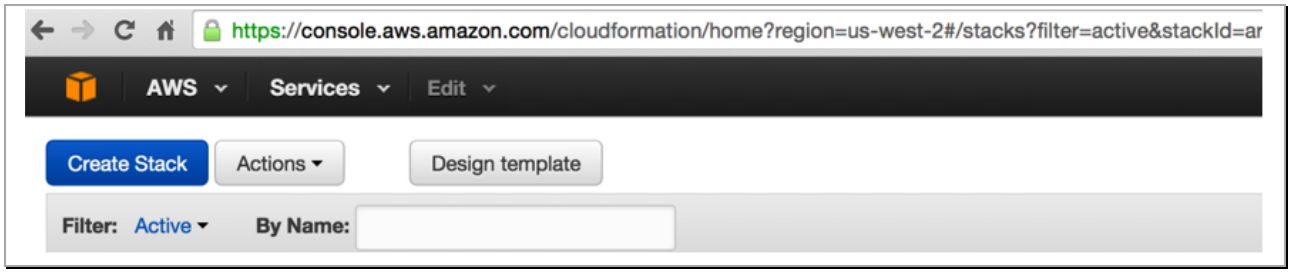
10. Launch the CFT

Login in to the AWS console https://console.aws.amazon.com and click on **CloudFormation**

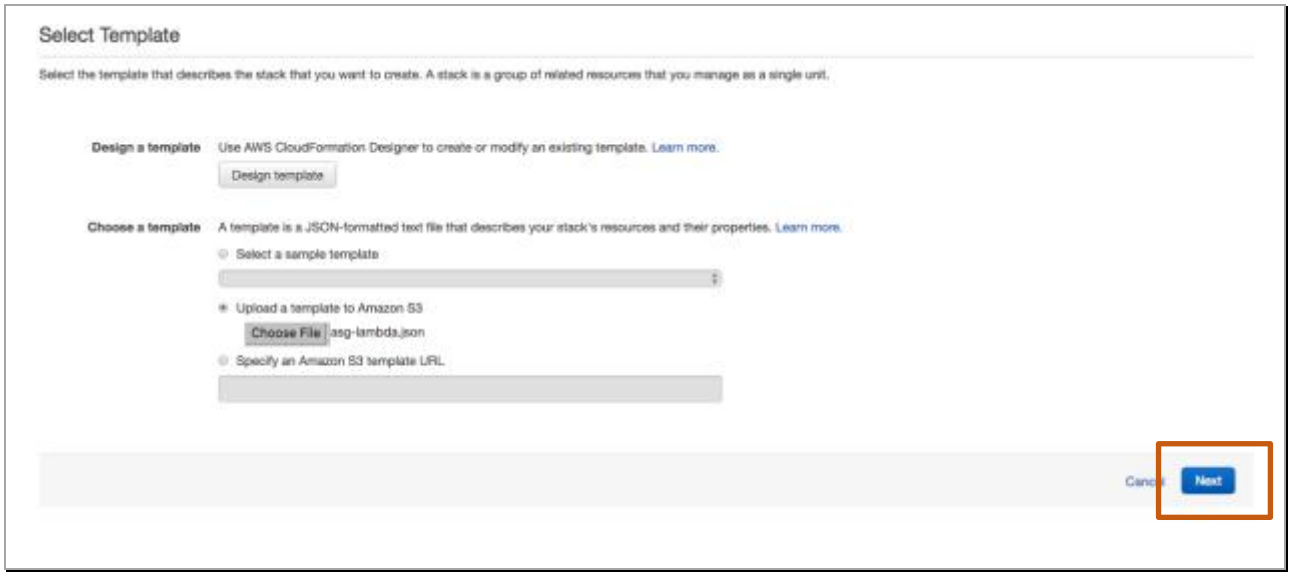


Note: Please make sure that your region (on the top right) is set to a region where Lambda is available (and the S3 buckets were created).

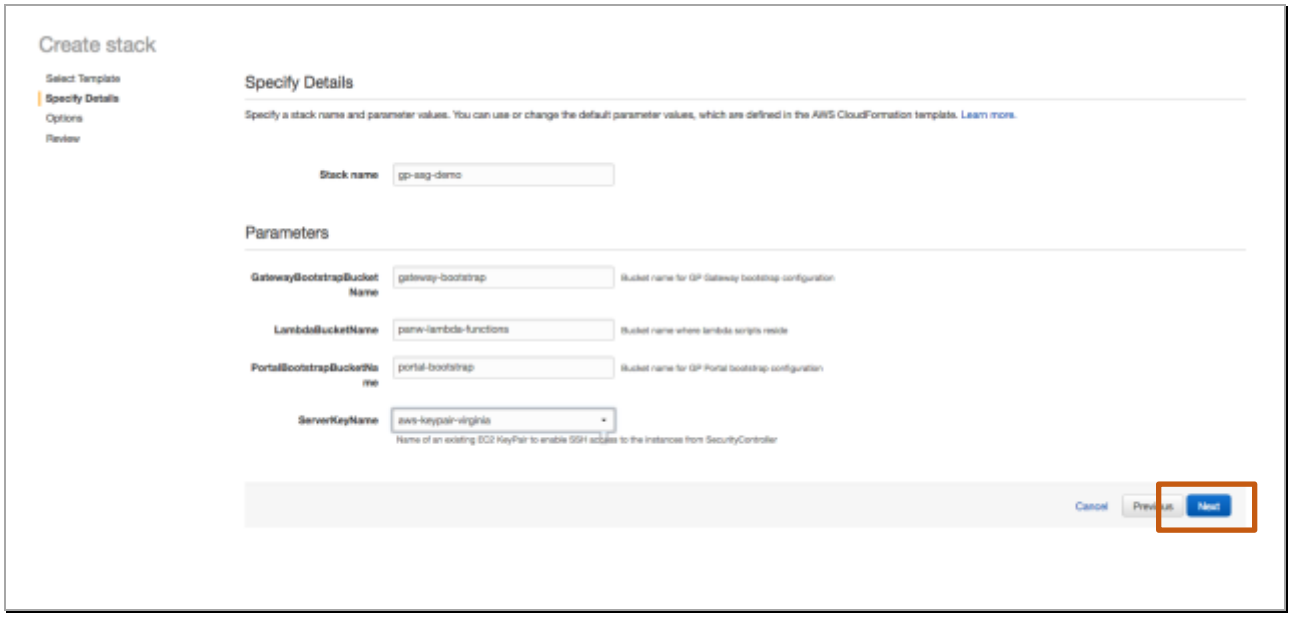
Click **Create Stack**:



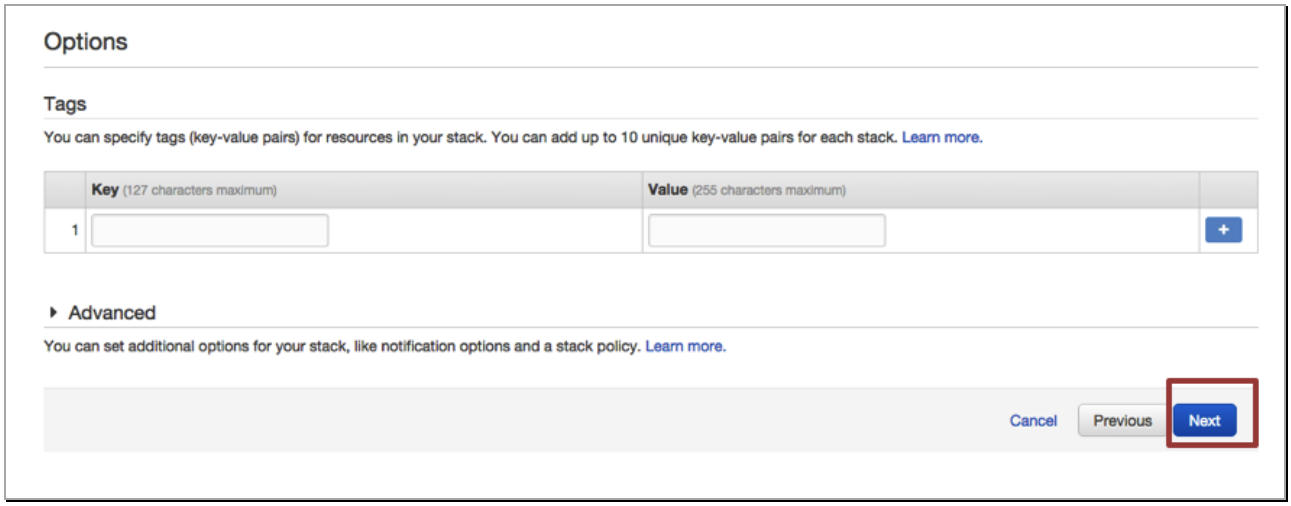
Select "**Upload a template to S3**" and click the "**Choose File**" button. Then select the gp-asg.json template file. Then, click **Next**:



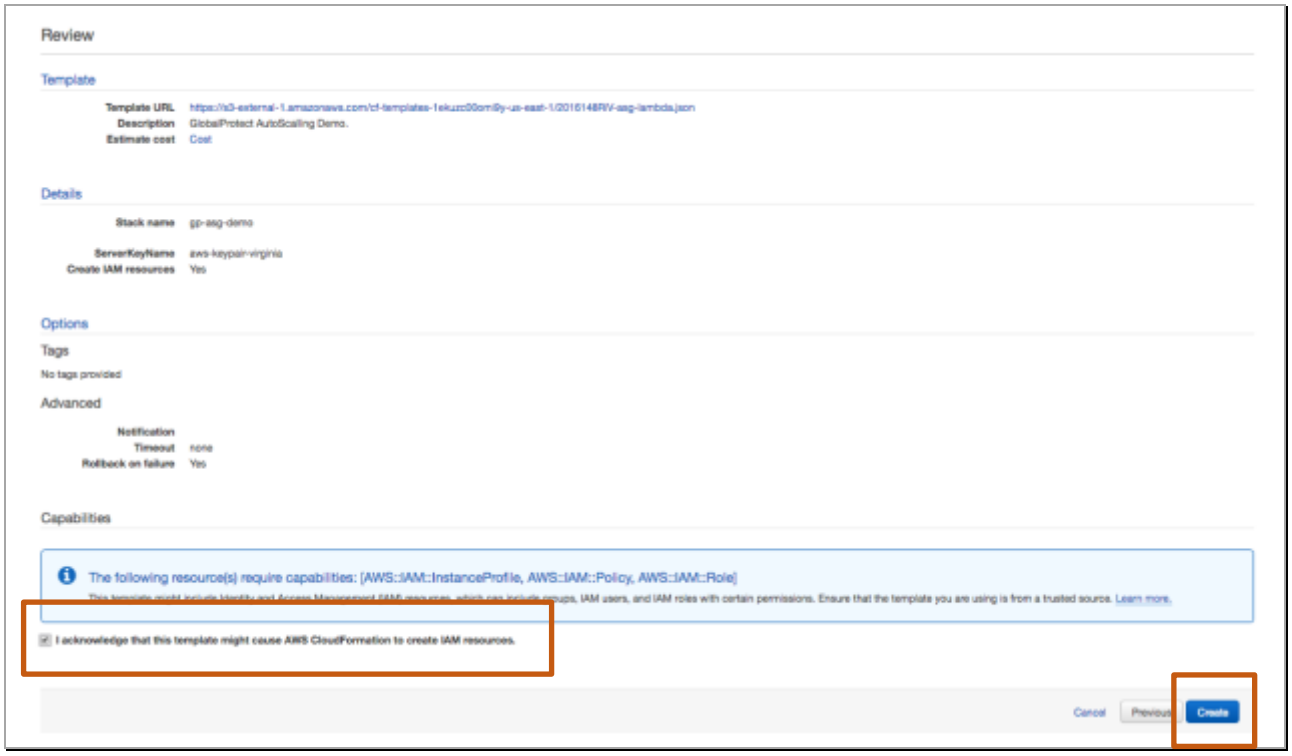
In the next screen specify a "**Stack Name**". Specify the gateway bootstrap bucket name for the **GatewayBootstrapBucketName** parameter, portal bootstrap bucket name for the **PortalBootstrapBucketName** parameter and the bucket name where the lambda scripts reside for the **LambdaBucketName** parameter.
Select a **Serverkey** for which you have the private key. Refer to section 2.4 on how to generate a keypair. Once satisfied, click **Next**.



On the next screen you can specify tags (optional) otherwise click **Next**.

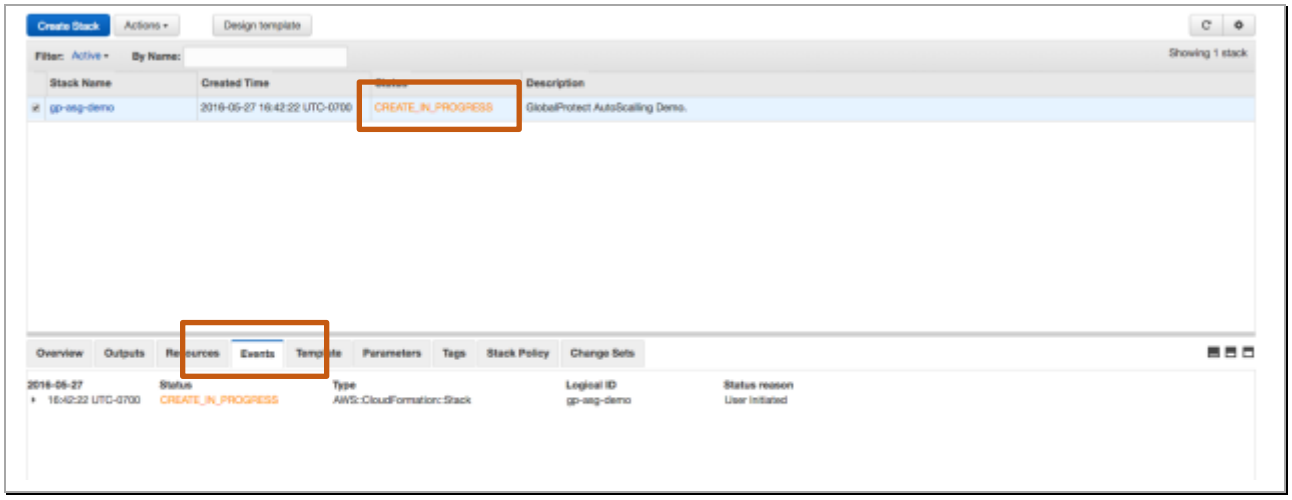


Next, review and check acknowledge at the bottom and click **Create**.

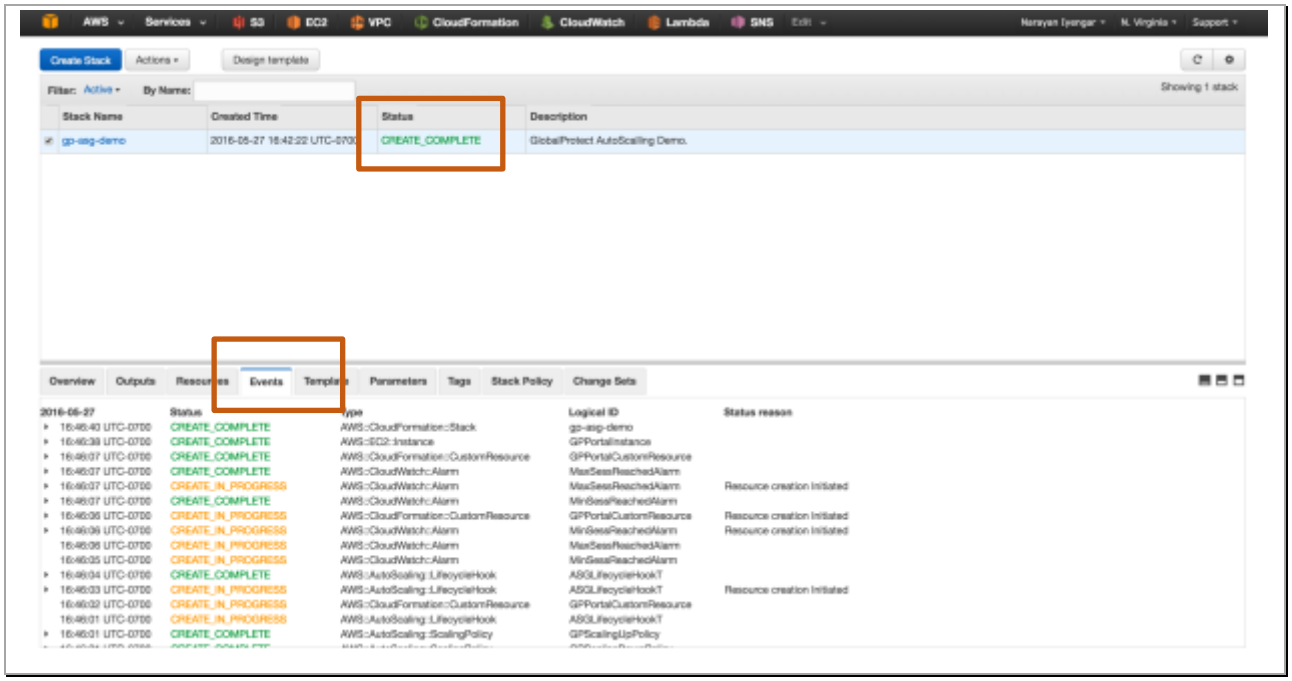


Once launched you should be able to monitor the stack creation progress in the next screen by clicking on the **Events** tab.

Note: The template takes about 10-15 minutes to fully deploy and be operational.

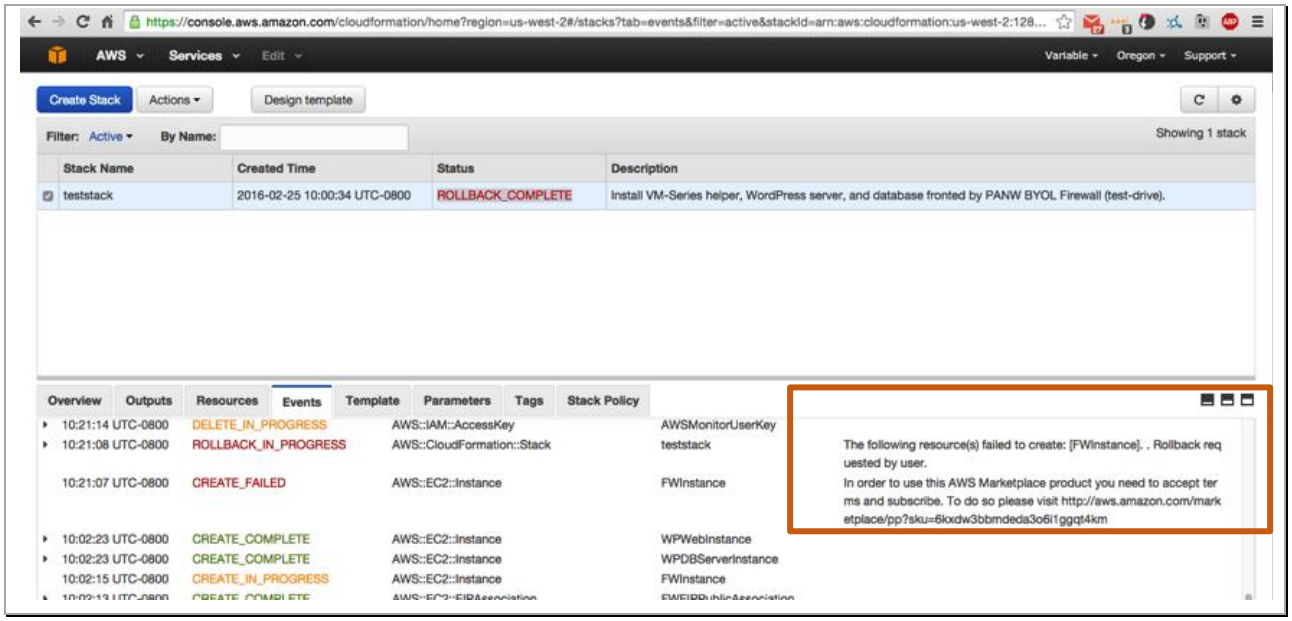


If the CFT was successfully launched, you should see an event as below:



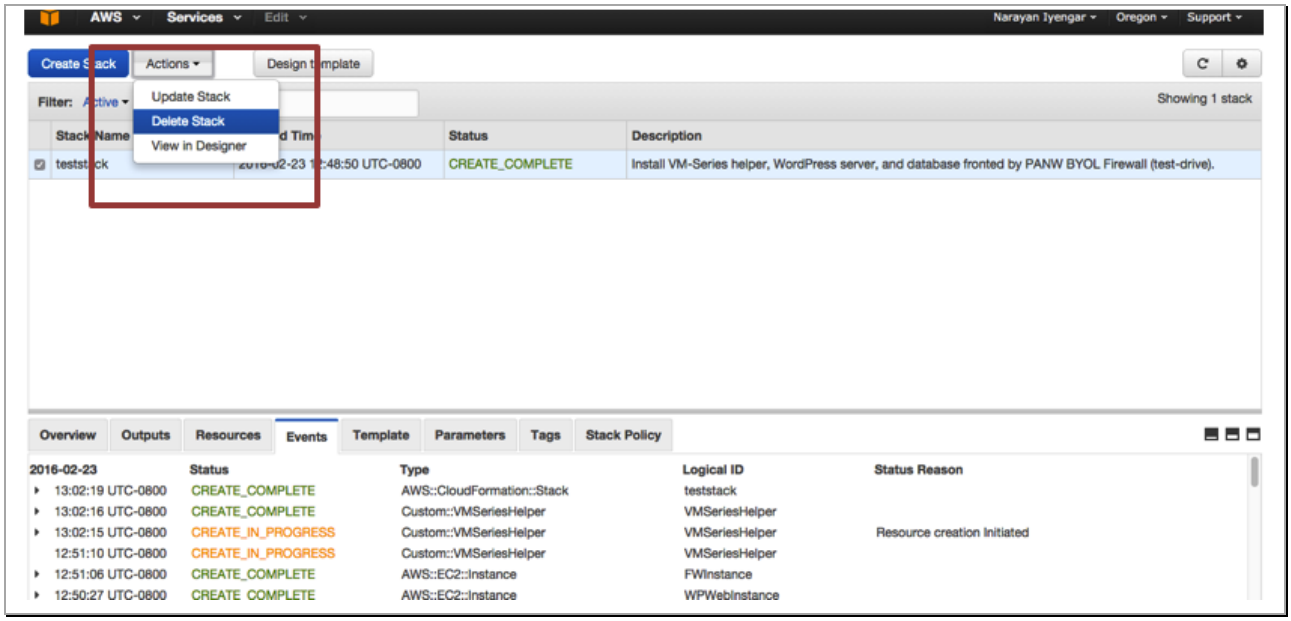
If there were any errors during the creation of the stack, you will need to drill down to the specific event in the **Events** tab and **Outputs** tab to debug and then create a new stack after fixing any errors. Scroll through the logs and find the chronologically first error. Normally, subsequent errors are a result of the initial error and the first error is the actual issue.

For instance, if you did not accept the VM-Series EULA, then you will get an error as seen below



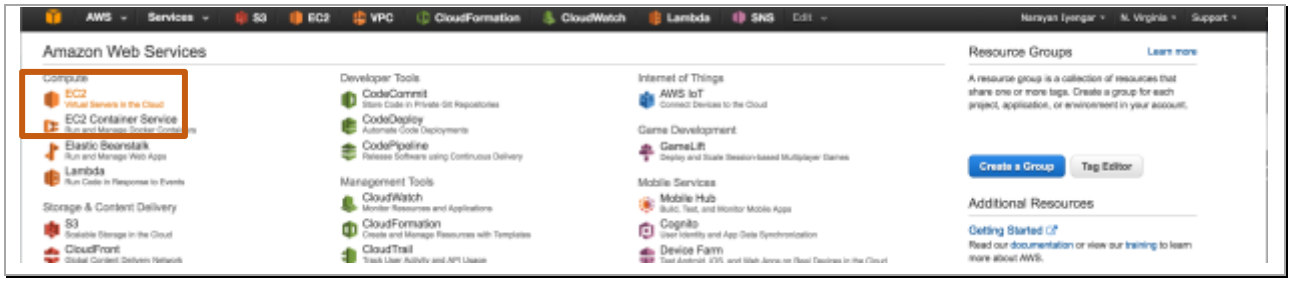
Refer to section 2.3 to review and accept the EULA for the VM-Series NGFW

Note: If you need to relaunch the CFT, first delete the current stack under Actions, Delete Stack.

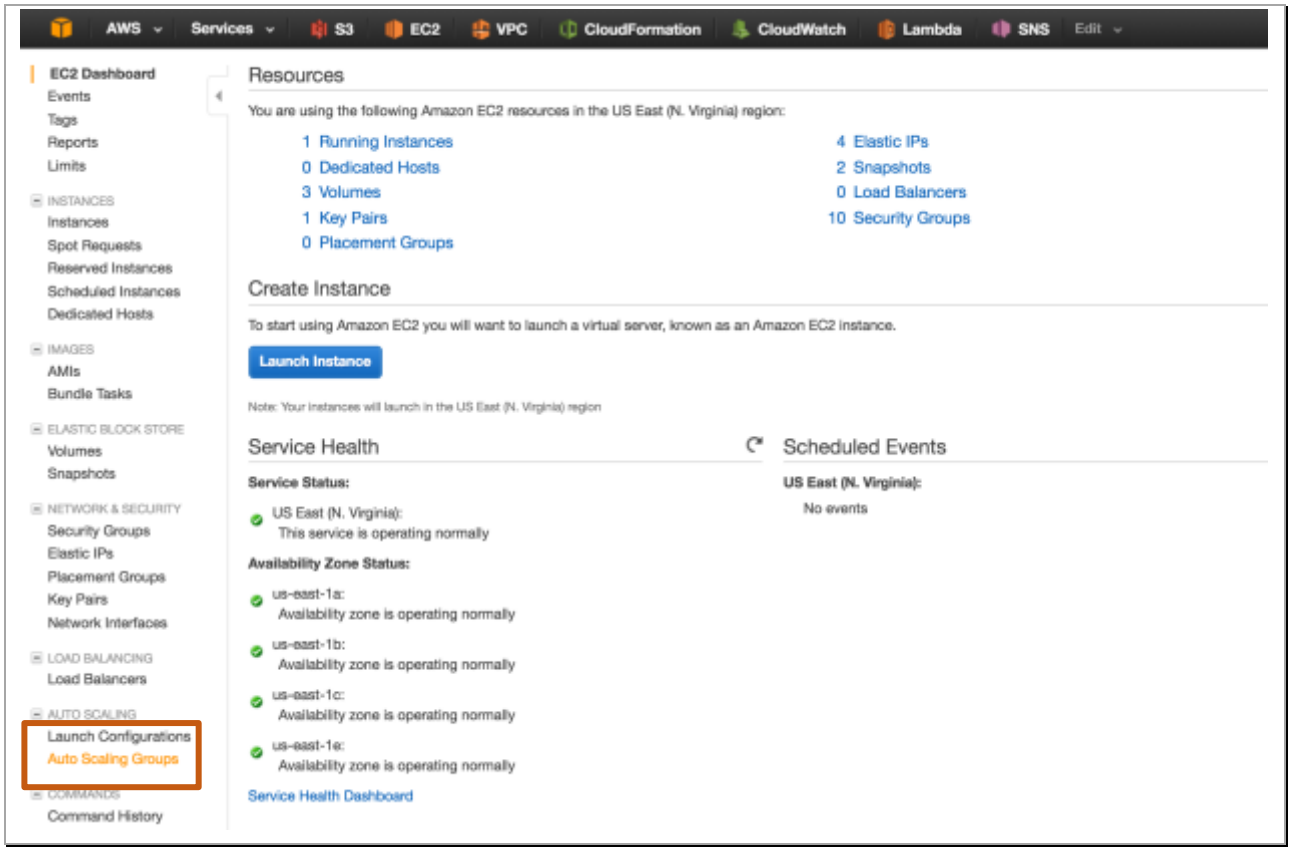


11. Launch the First Gateway

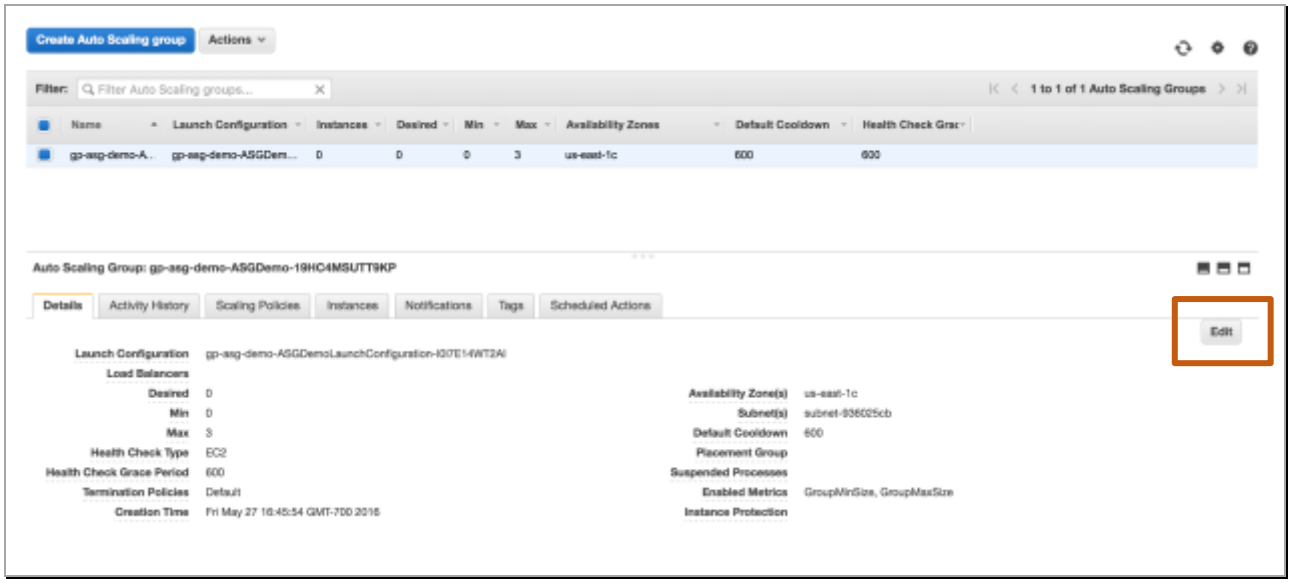
After the template has been deployed successfully, go back to the console and click on "**EC2**":



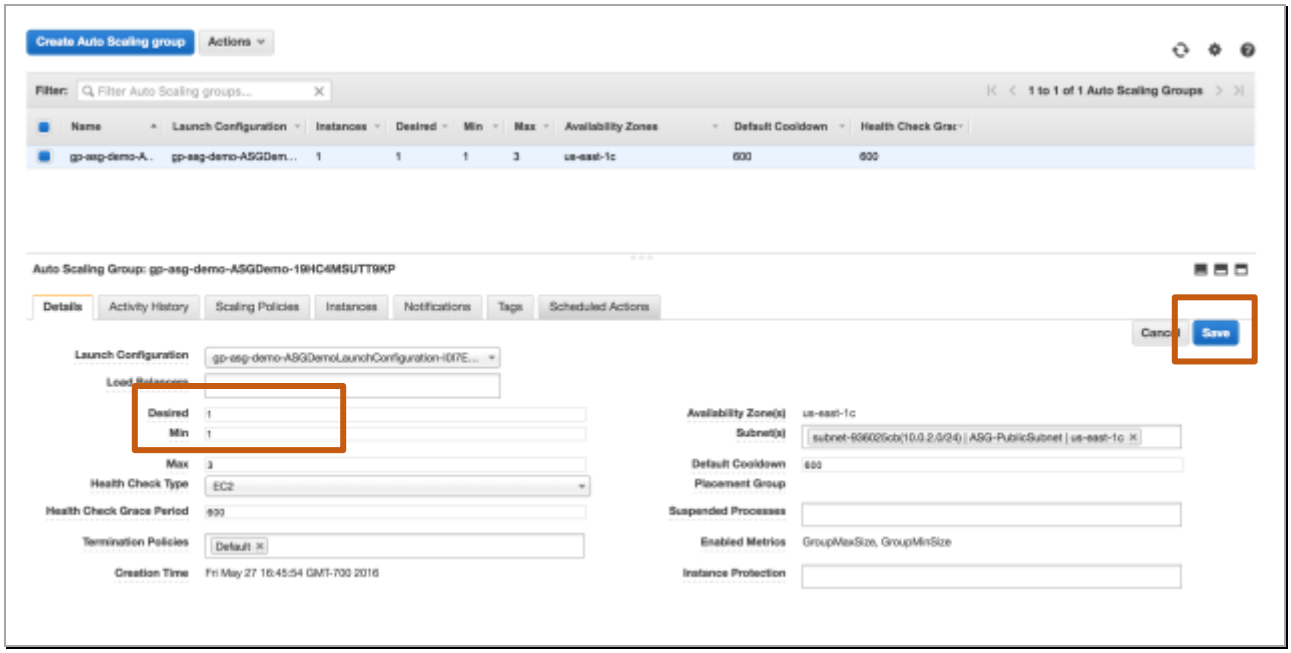
And click on "**Auto Scaling Groups**"



You should see the auto scaling group created by the template. Click "**Edit**"

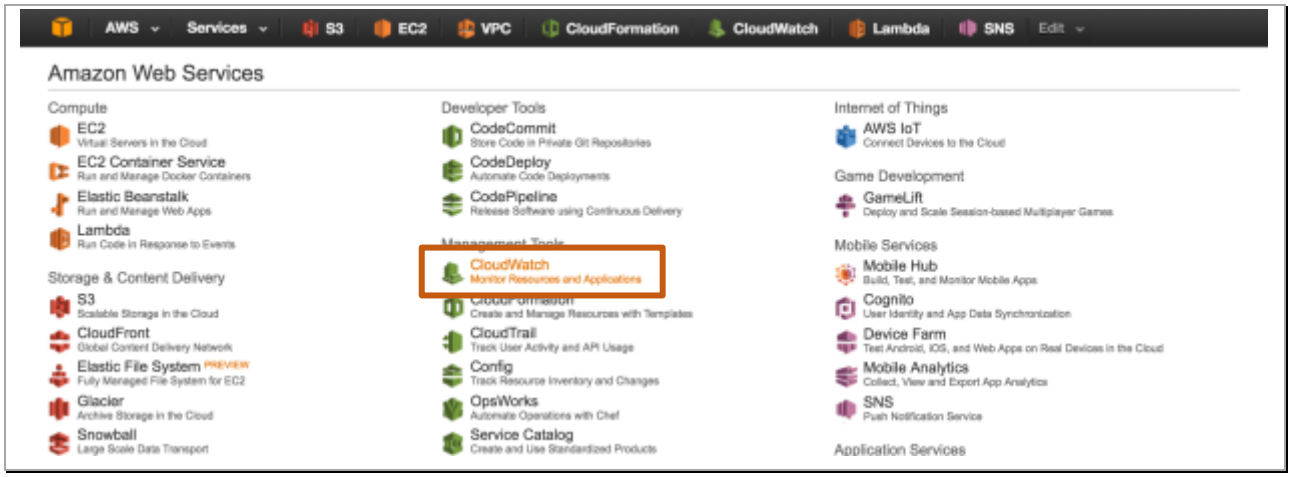


and change the "**Desired"** and "**Min**" fields to "1" and click "**Save**":

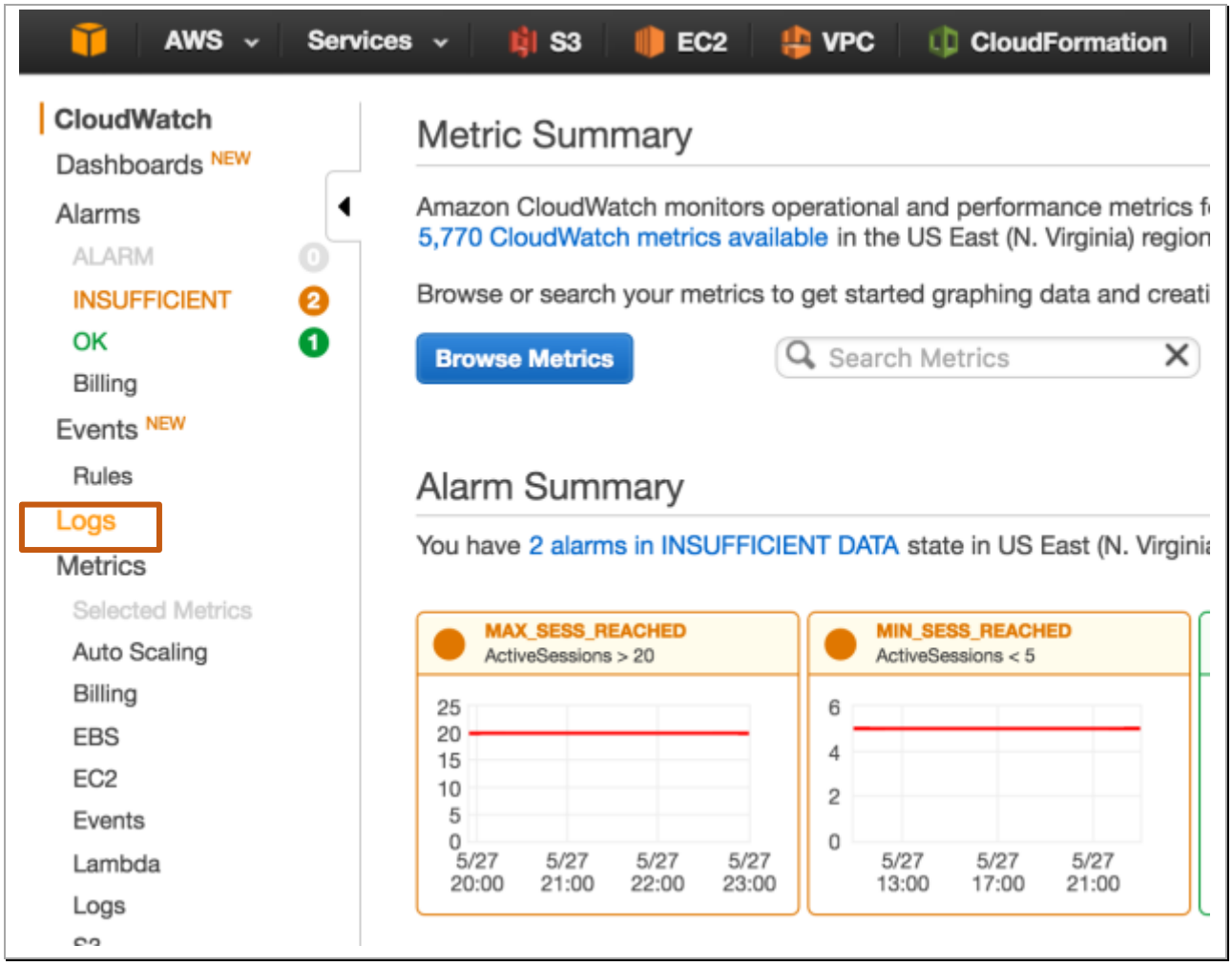


This will trigger an auto scale event and launch a new VM-Series firewall and bootstrap it as a GlobalProtect Gateway. You can see this by clicking on "**Instances**" on the left:

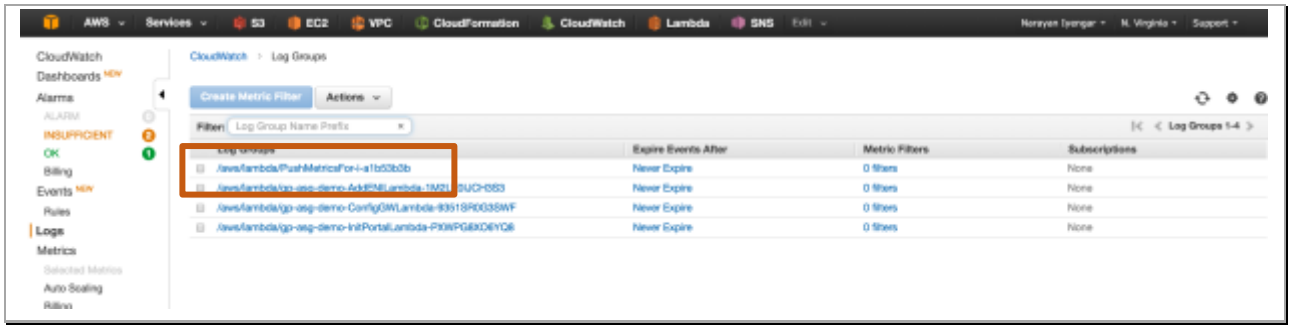
From launch to configured, it takes about 10 minutes. You can monitor the logs if so desired by clicking on "**CloudWatch**" on the AWS console



and then on "**Logs"** on the left:



A good indication that the GlobalProtect Gateway is up is the creation of the "**PushMetrics**" log group:



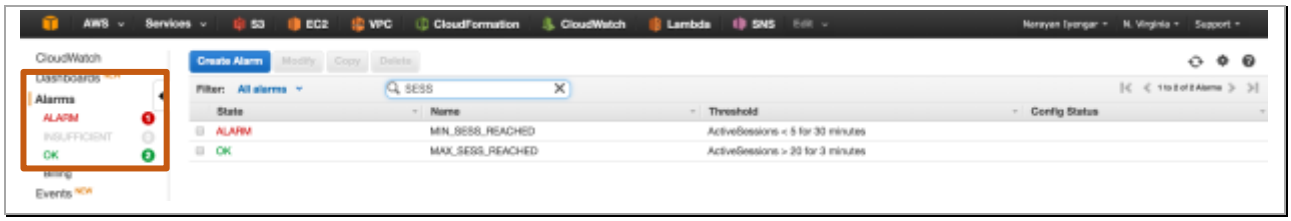
This indicates that the gateway is up and publishing metrics to CloudWatch.

12. Scale-out/Scale-In Policy

In order to determine when to scale-out (add new gateways) or scale-in (remove gateways from service) the number of active sessions on a gateway is published to CloudWatch. Each gateway that is part of the Auto Scale Group will publish its active session count per minute.

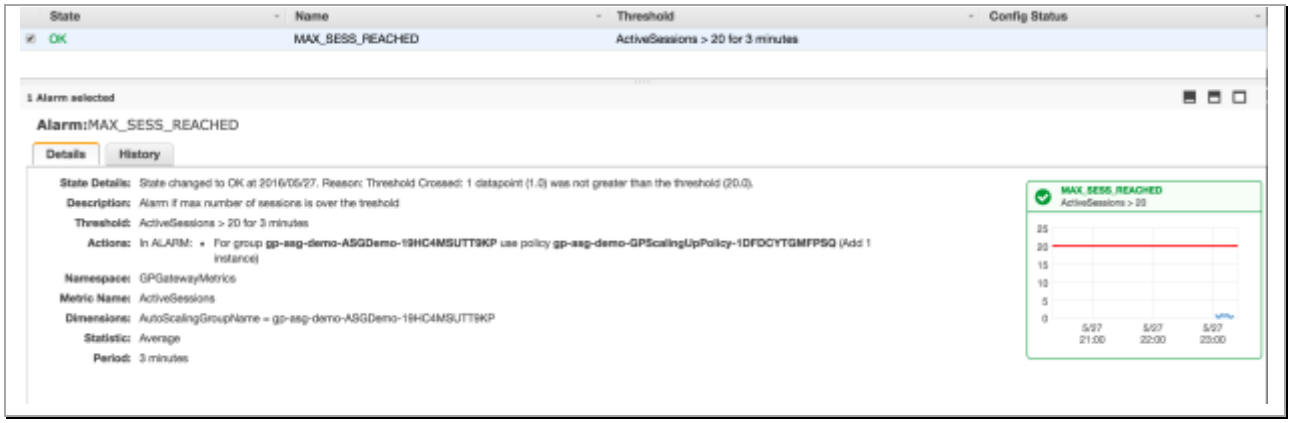
The template – for demonstration purposes – has set a very low threshold for an auto scale event to occur.

To verify click on "**Alarms**" on the left and click on the "**OK**" link:



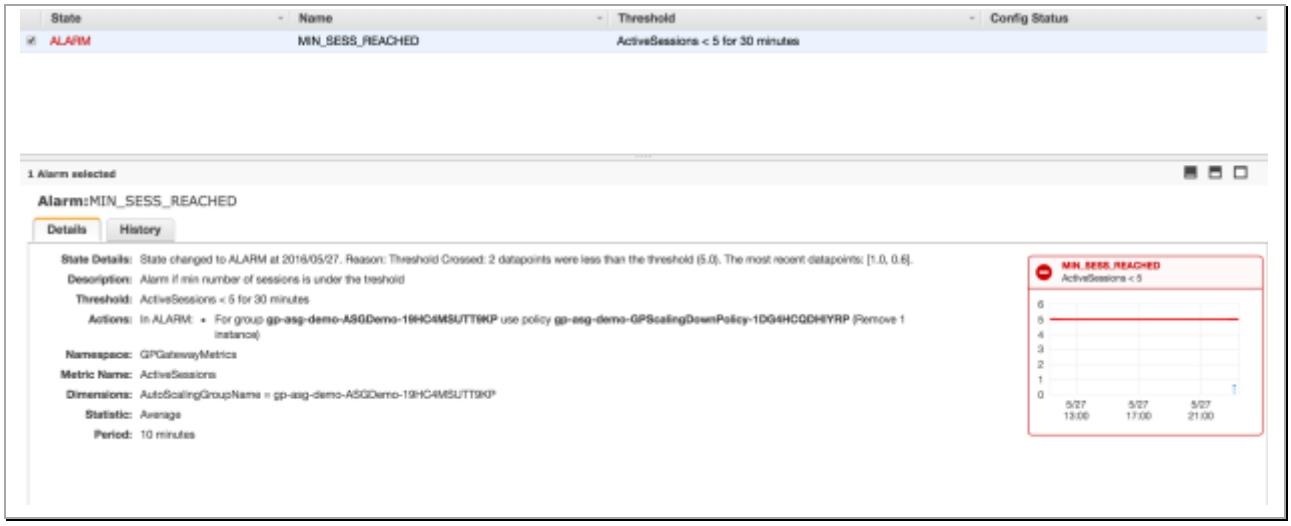
In the above screen capture, you see two alarms. MAX_SESS_REACHED and MIN_SESS_REACHED. These alarms are triggered based on metrics published by the gateways in the Auto Scale Group.

If the number of active sessions is greater than 20 for more than 3 minutes, the MAX_SESS_REACHED alarm is triggered, which in turn triggers scale-out event, which deploys a new GP gateway within the Auto Scale Group



Similarly, if the number of sessions is less than 5 and stays that way for 30 minutes, the MIN_SESS_REACHED alarm is triggered (as in the screenshot above) and a scale-in event happens and a GP gateway is terminated.

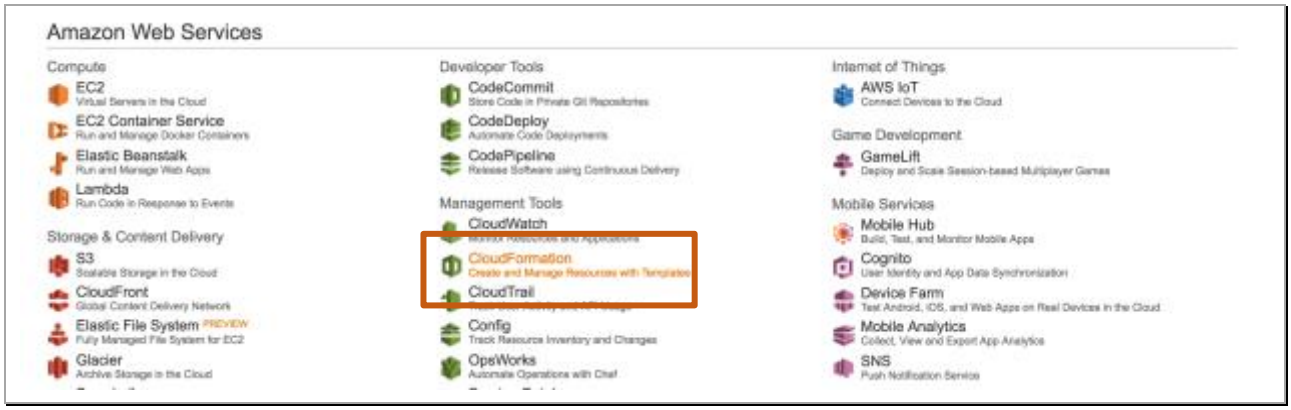
Note: There will always be at least one gateway (depending on your configuration for the minimum number of gateways)



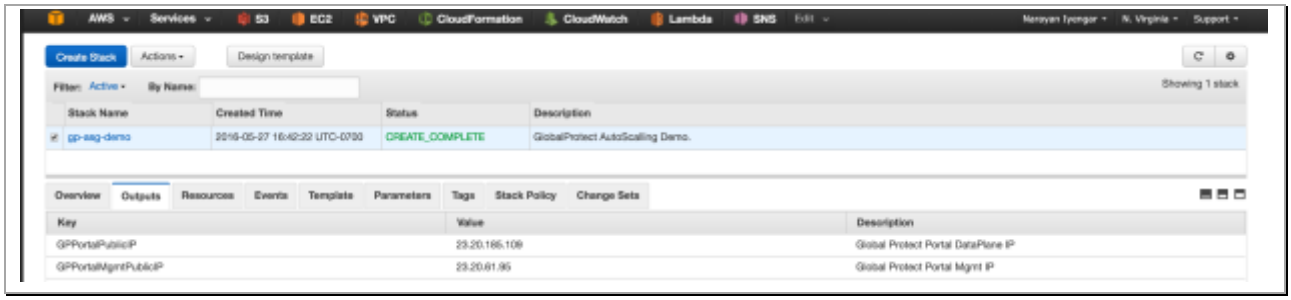
13. Trigger an Auto Scale Event

This should ideally be done on a VM so as to not disrupt any other activity. For the purpose of this guide and demonstration, a Windows VM was used.

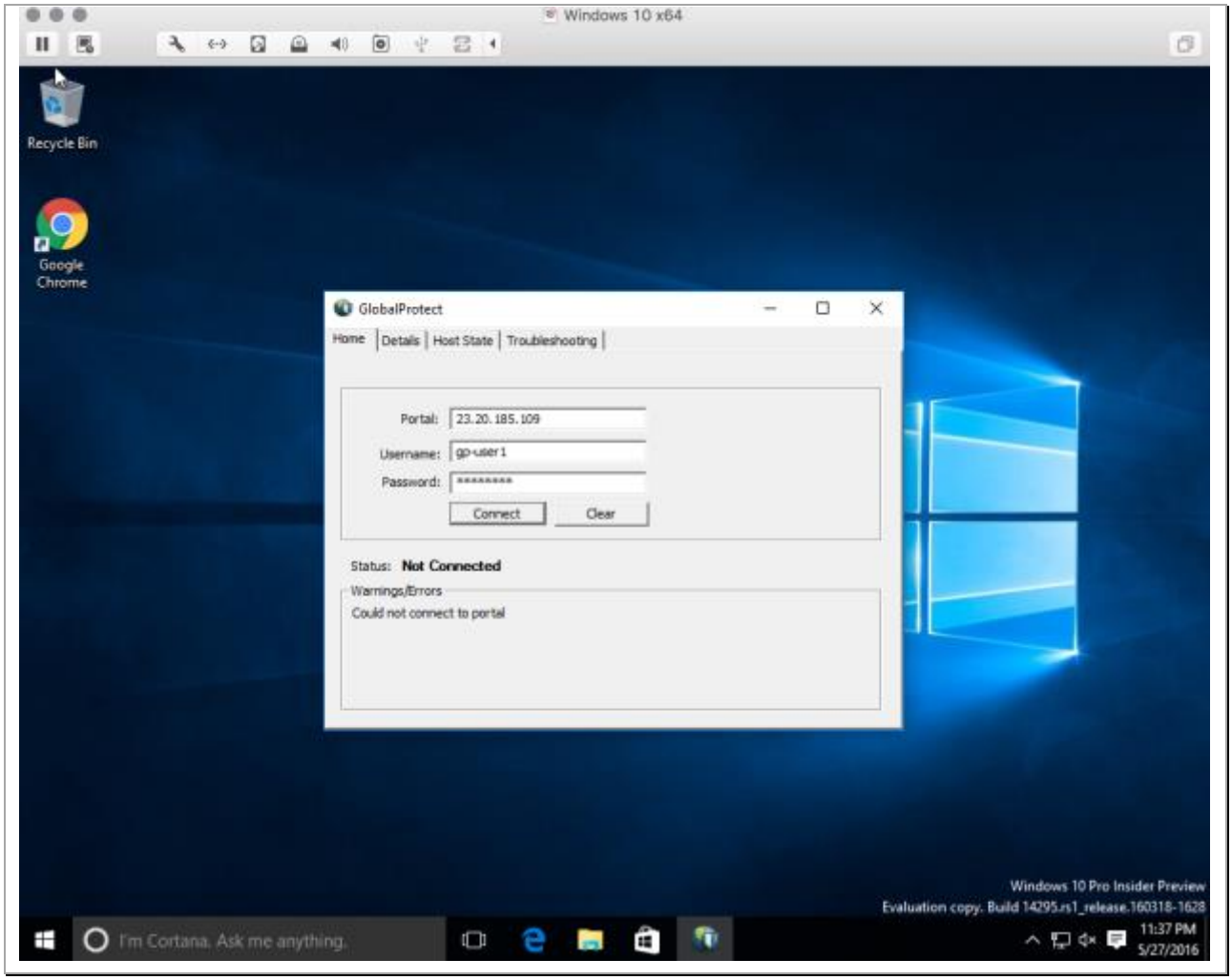
To determine the GP Portal address, head on over to CloudFormation in the AWS console



and select the stack that was just deployed. Under the "**Outputs**" tab note the **GPPortalPublicIP** address

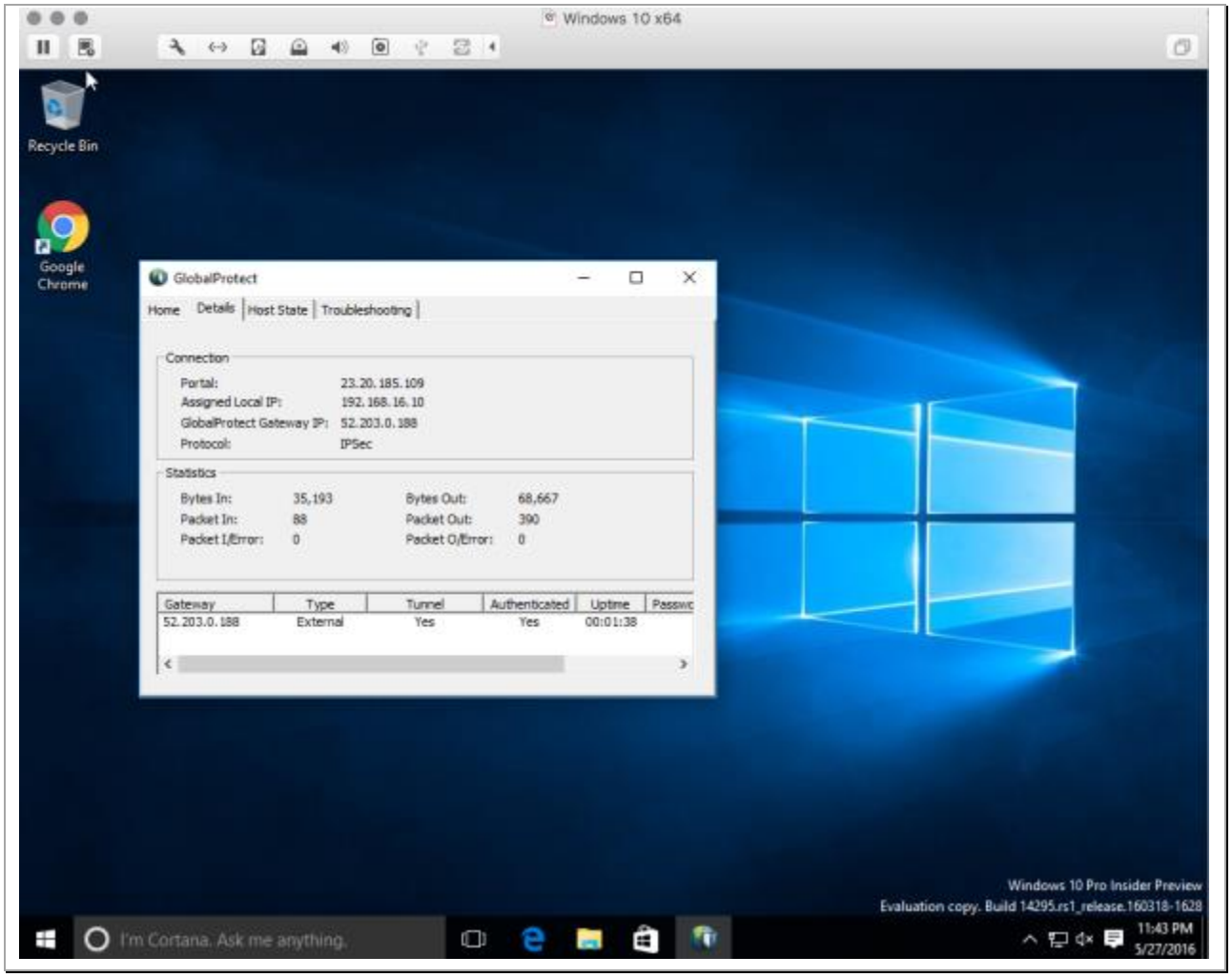


In the GlobalProtect client panel specify the above **GPPortalPublicIP** address as the Portal address. The username and password is gp-user1/paloalto or gp-user2/paloalto

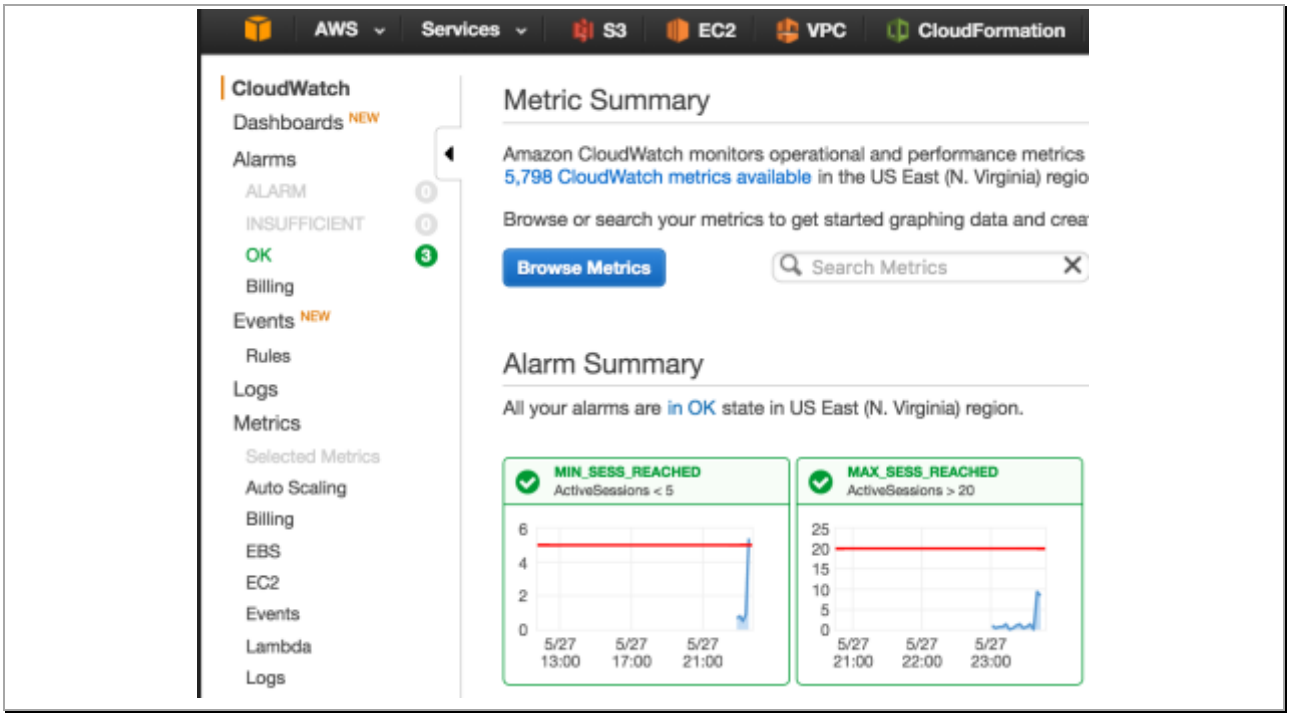


If you get an error (as seen above) that the client could not connect to the portal, you may need to disable the GlobalProtect client on your host machine. The portal and gateways use self-signed certificate and so corporate firewalls may not allow the connection to go through.

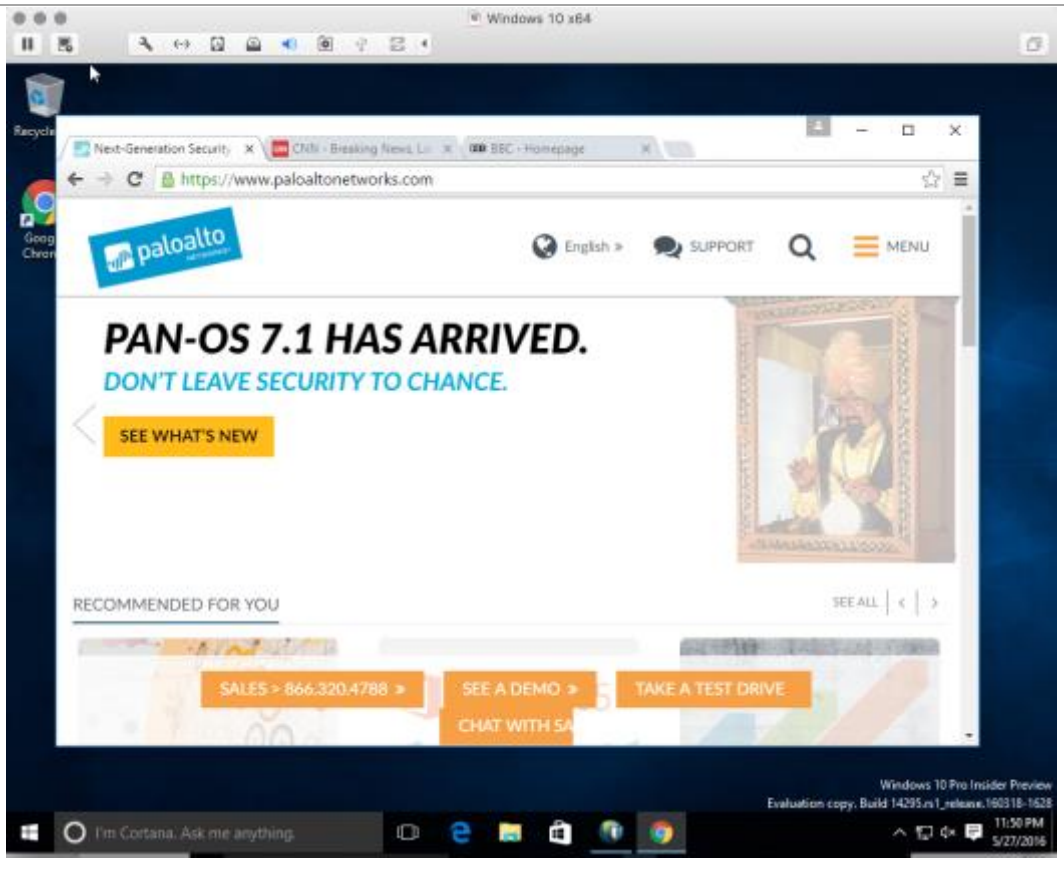
Once connected you should see the Portal and Gateway information in the client "**Details**" tab:



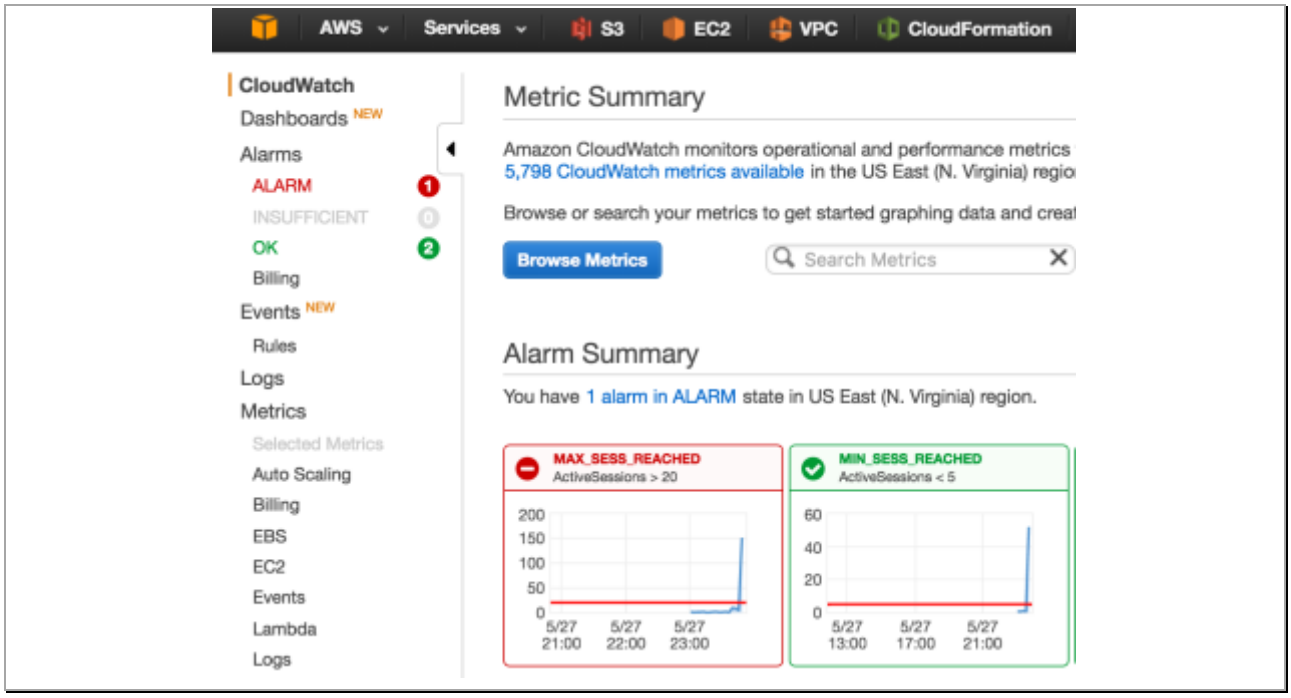
To verify that by connecting to the gateway the session count goes up head on over the AWS console and click on CloudWatch and you should see a small spike in the metrics for MAX_SESSION_REACHED:



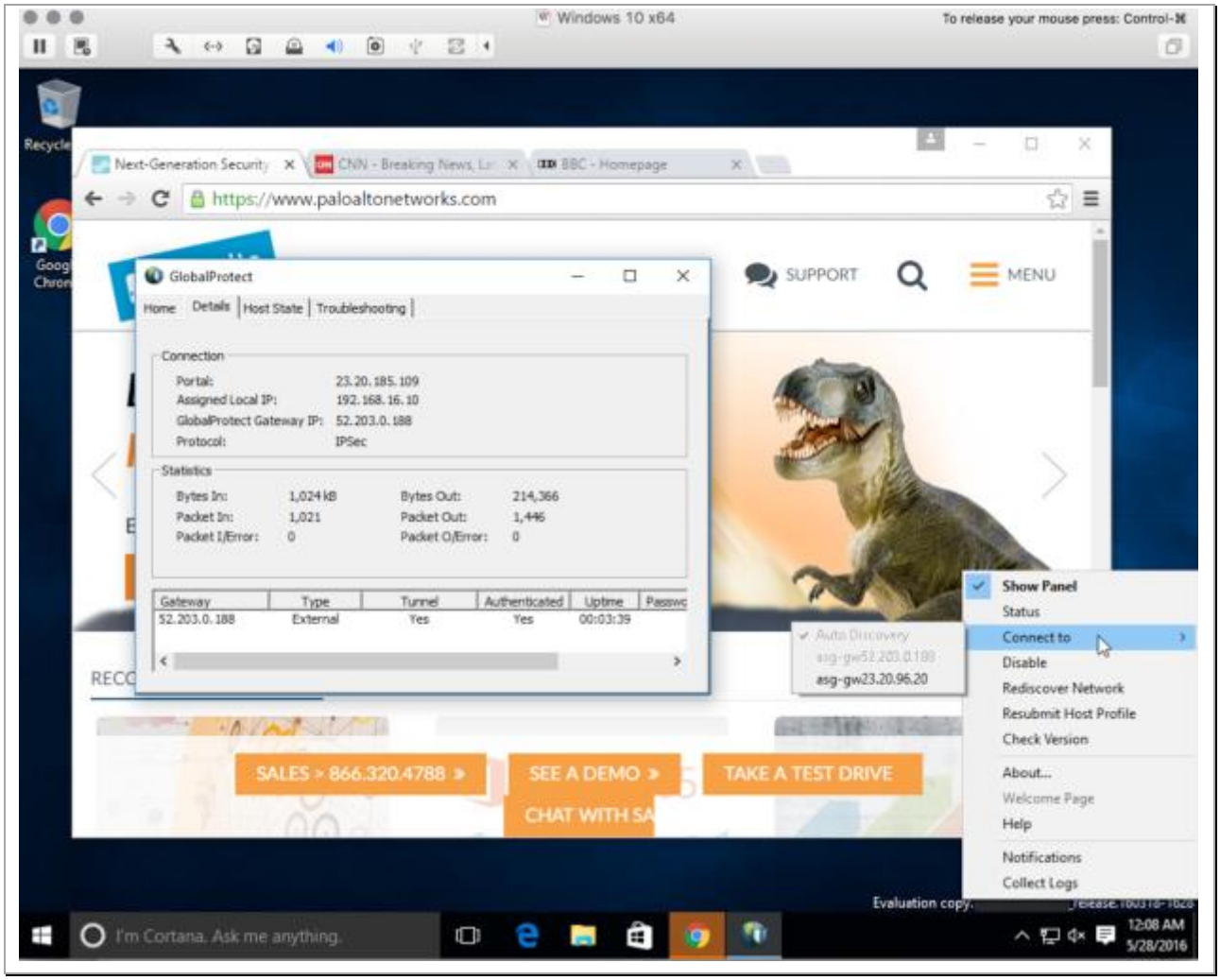
To trigger an event, in the VM open up a web browser and pick a few of your favorite websites to visit:



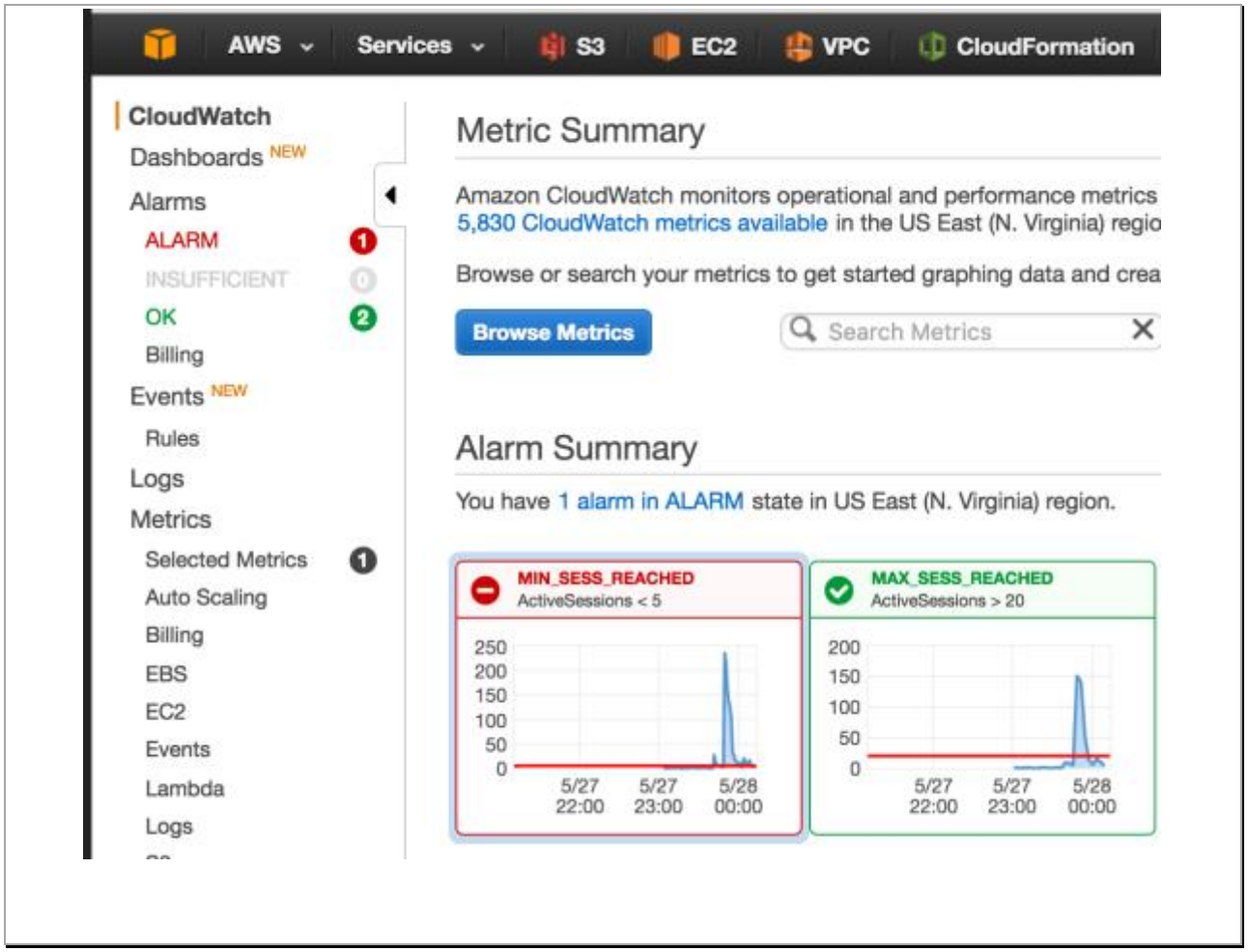
This will cause the session count to go up, trigger the alarm and cause a scale-out event and a new gateway will be provisioned, bootstrapped, configured and added to the Auto Scale Group.



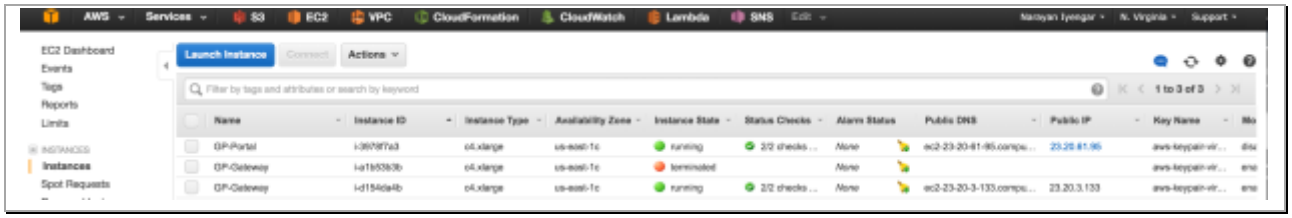
Once the new gateway is up, it will be added to the pool of gateways. Verify this in the GP Client by selecting "**Rediscover Network**":



To trigger a scale-in event, close all the browser sessions (or shutdown the VM) and that will trigger a scale-in event

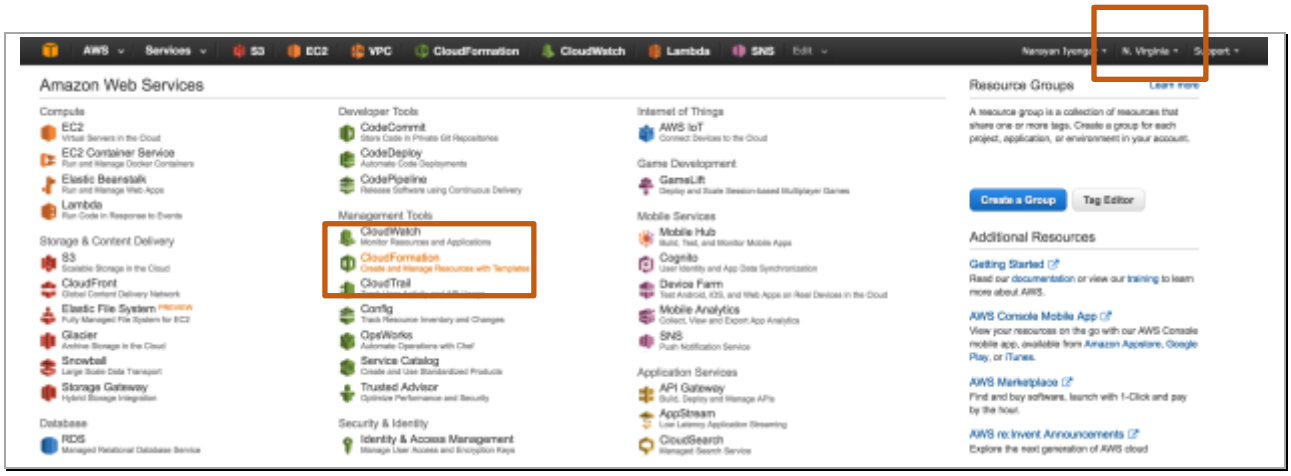


and a gateway will be removed from service

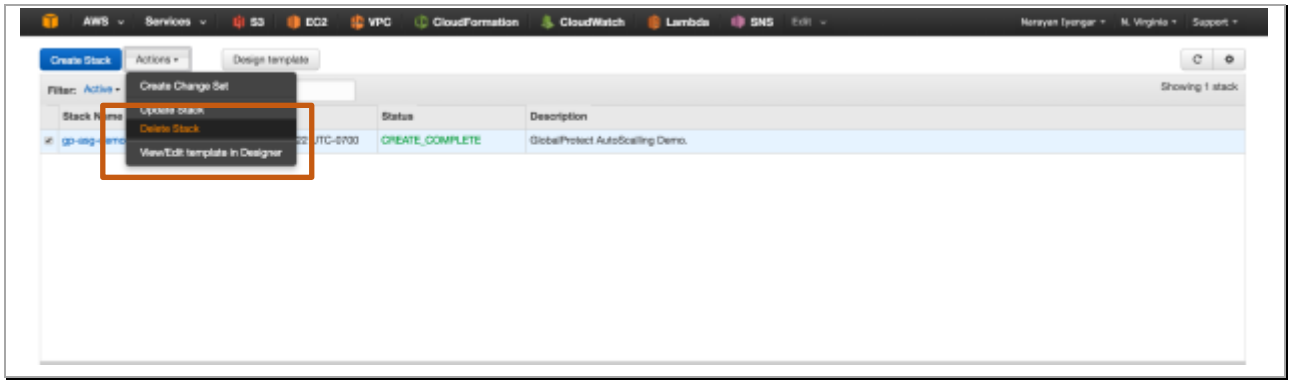


14. Cleanup

Once done with the template, feel free to play around with various things. If done, cleanup as follows. In the AWS management console, click on **CloudFormation**:

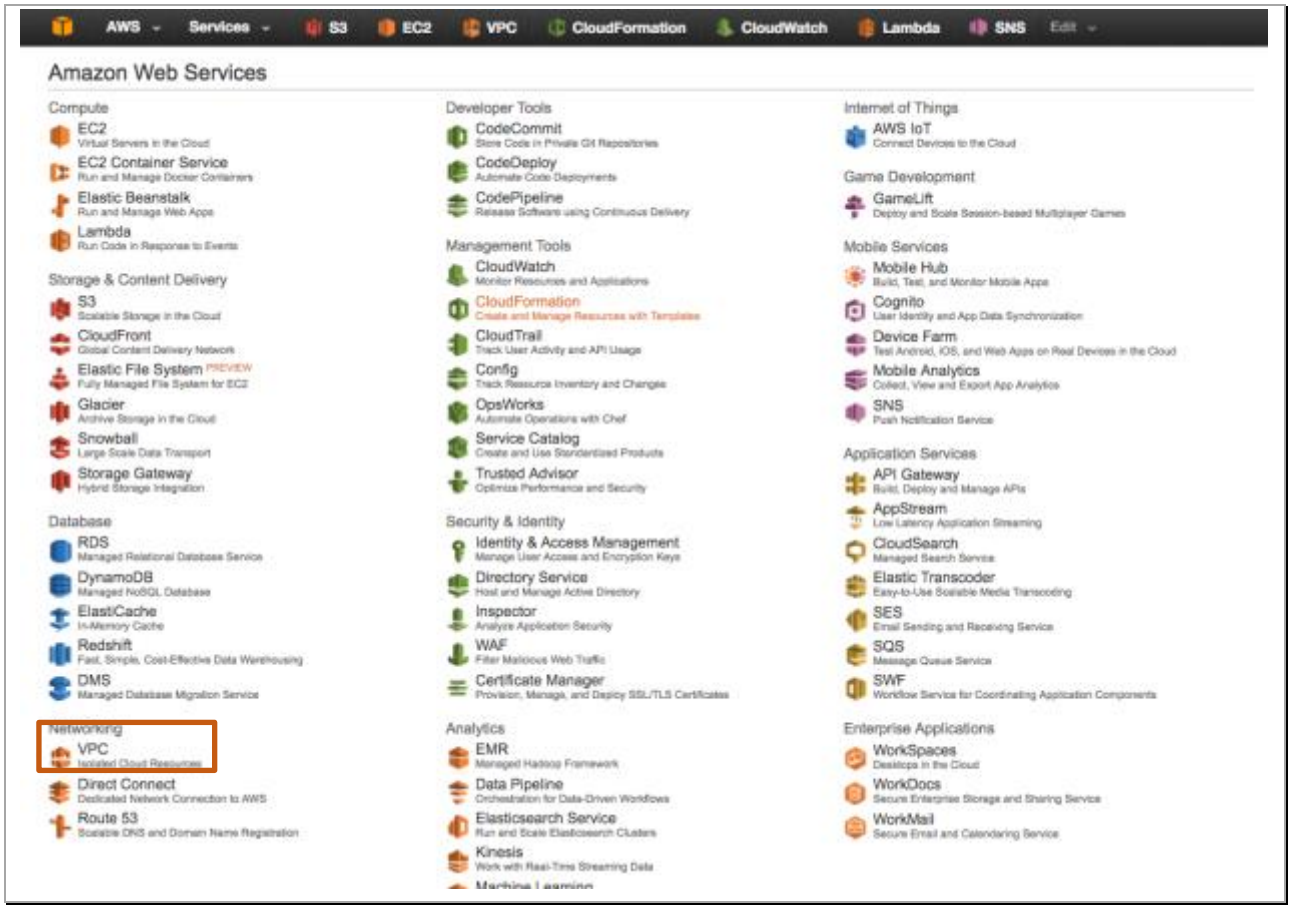


Under **Actions**, click **Delete Stack:**

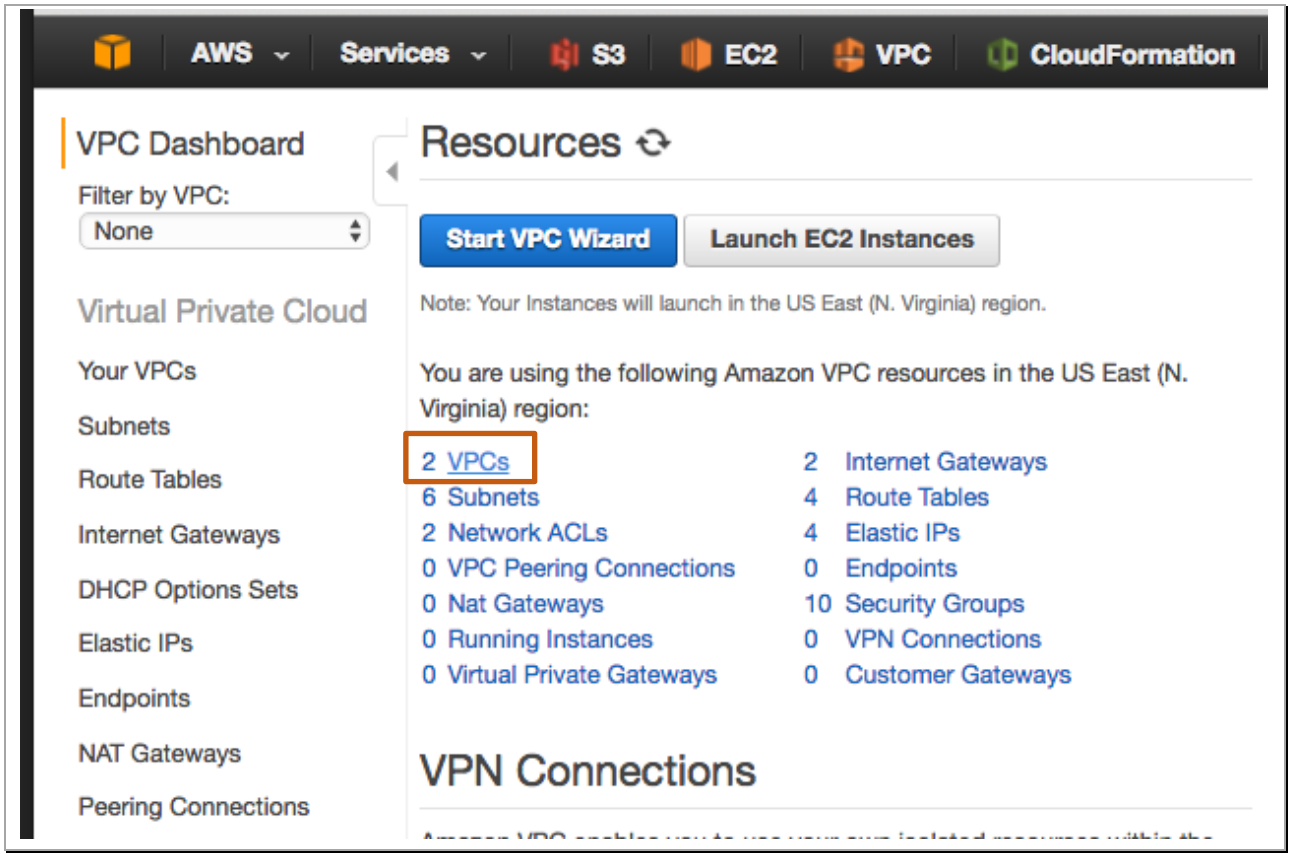


This should delete all the resources created via the template.

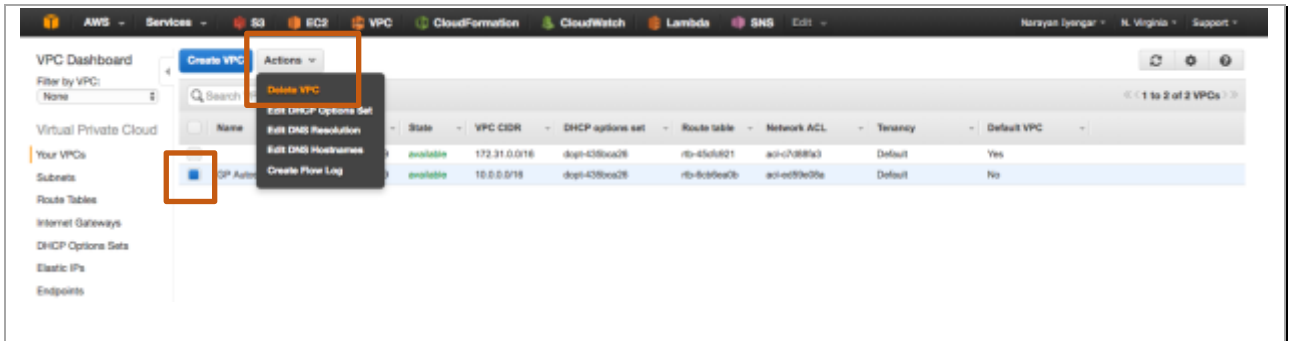
Note: There are cases when deleting a stack fails due to some dependencies that AWS is not able to automatically delete. So, if stack deletion fails, head on over to the VPC console

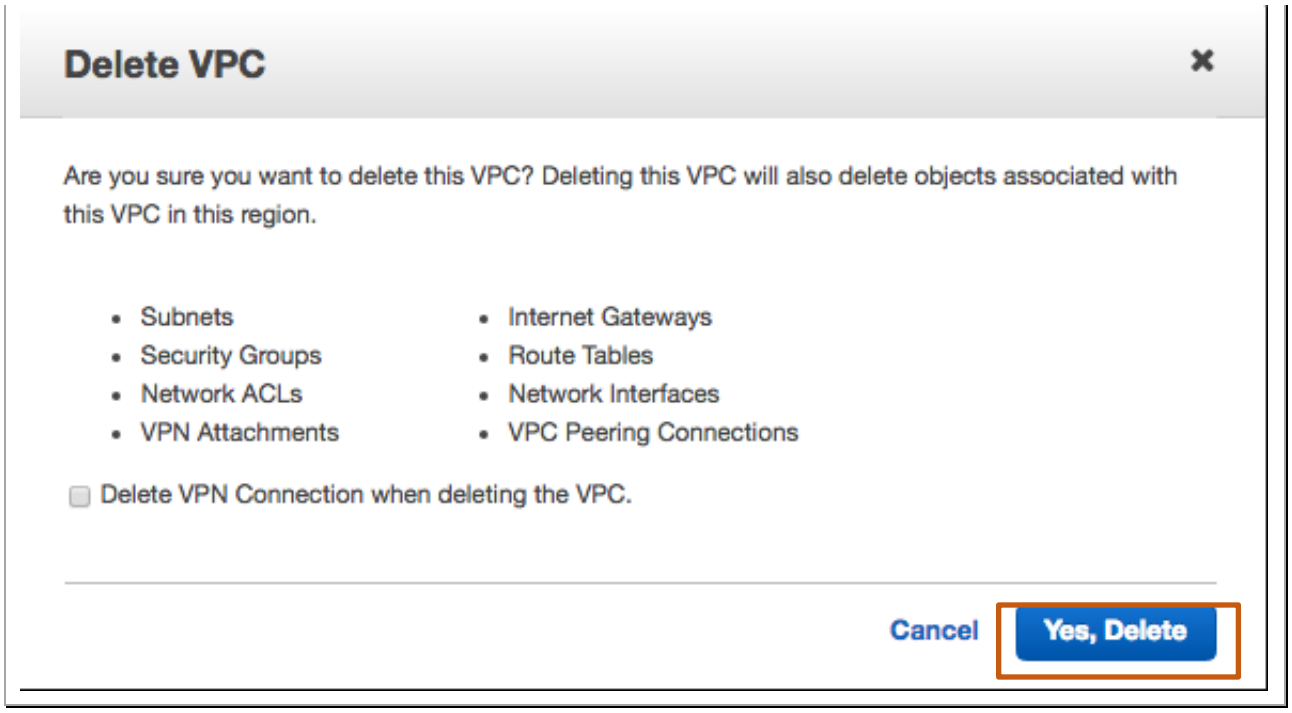


and select **VPCs**



Select the VPC in question and select "**Delete VPC**" from the "**Actions**" menu and click "**Yes**, **Delete**"





15. Conclusion

You have successfully deployed and demonstrated GlobalProtect in an AWS Auto Scaling environment