



Auto Scaling GlobalProtect in AWS Deployment Guide

<http://www.paloaltonetworks.com>

Table of Contents

1. Global Protect	3
2. GlobalProtect and Auto Scaling	3
3. About CFTs.....	4
4. About this guide.....	4
5. AWS Services Used.....	5
5.1 AWS Auto Scaling	5
5.2 AWS Lambda.....	6
5.3 Amazon S3	6
5.4 Amazon SNS	6
5.5 Amazon CloudWatch	6
6. Template Deployment Prerequisites	6
6.1 Create an AWS account.....	7
6.2 Add a credit card to your AWS account.....	7
6.3 Review and accept the EULA.....	7
6.4 Create and download an SSH keypair	10
7. PAN-OS Prerequisites.....	12
8. Download the Files.....	12
9. Create S3 Buckets	13
10. Launch the CFT.....	16
11. Launch the First Gateway	21
12. Scale-out/Scale-In Policy.....	25
13. Trigger an Auto Scale Event.....	26
14. Cleanup.....	32
15. Conclusion	36

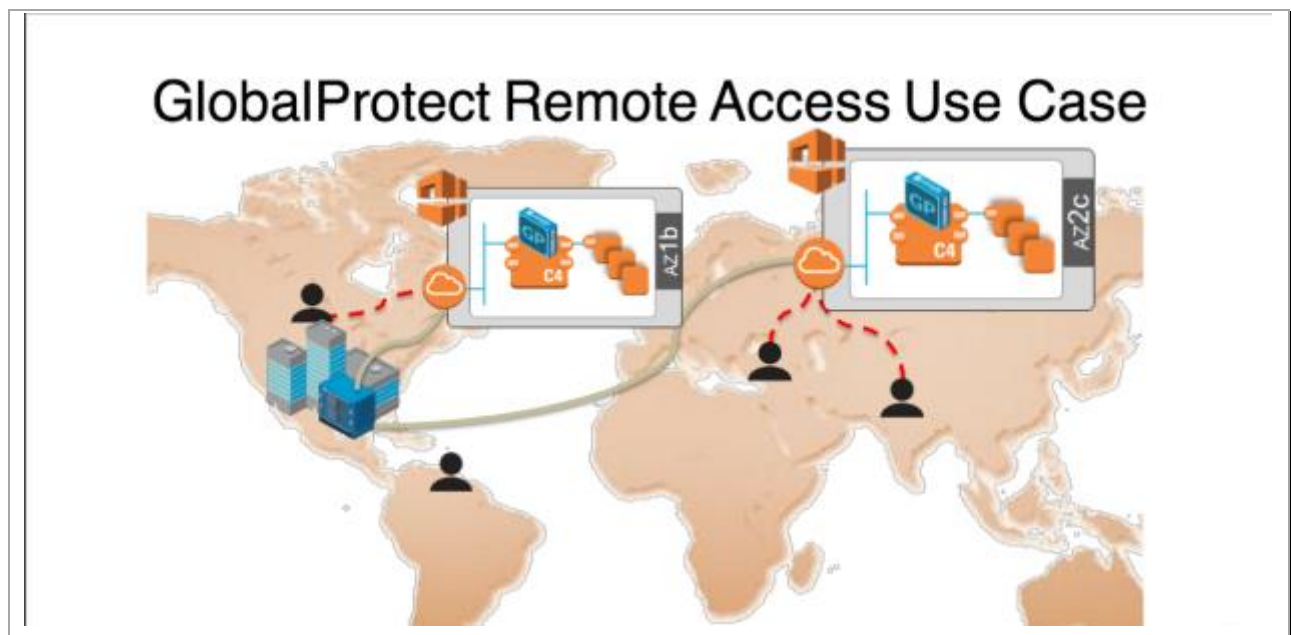
1. Global Protect

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>

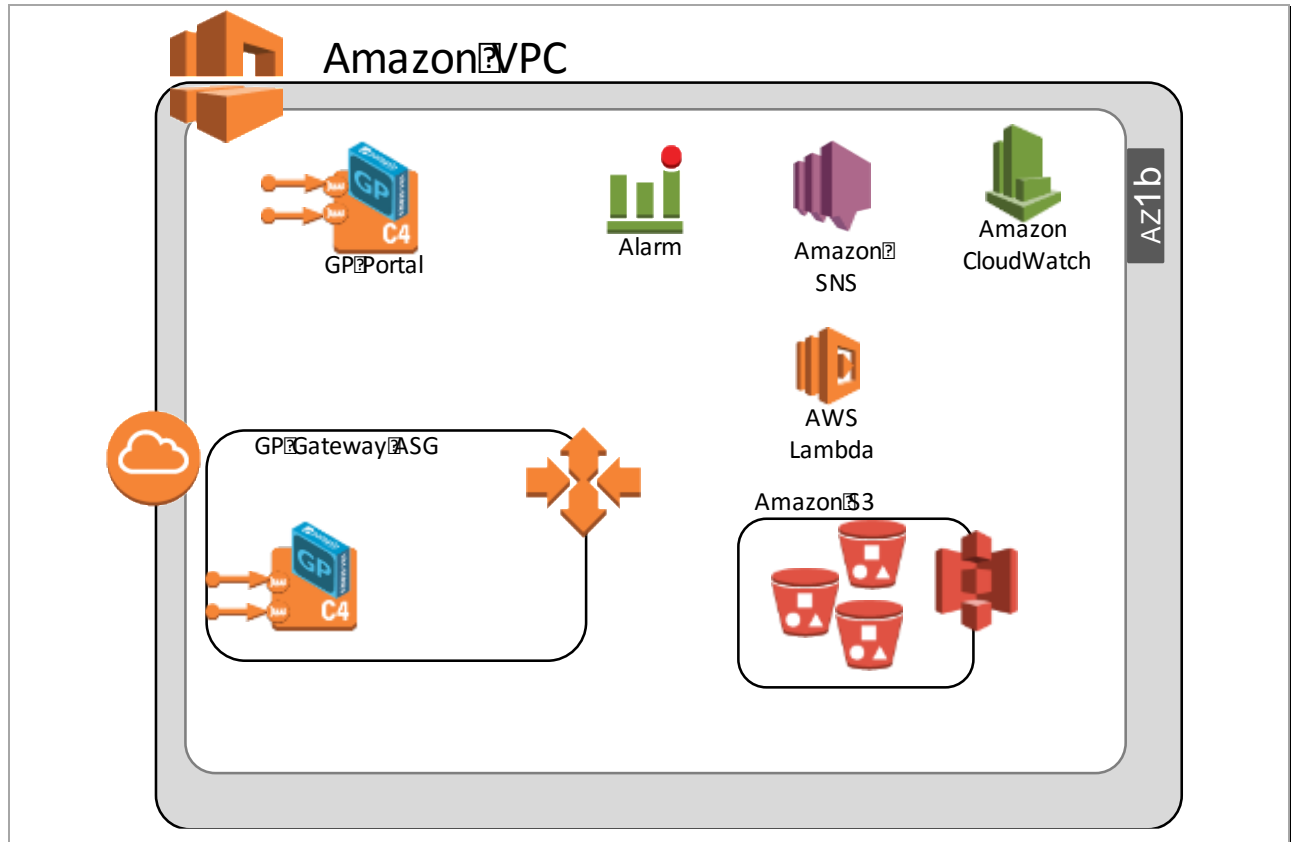
Additional templates provided by Palo Alto Networks can be found on the following Github page

<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.

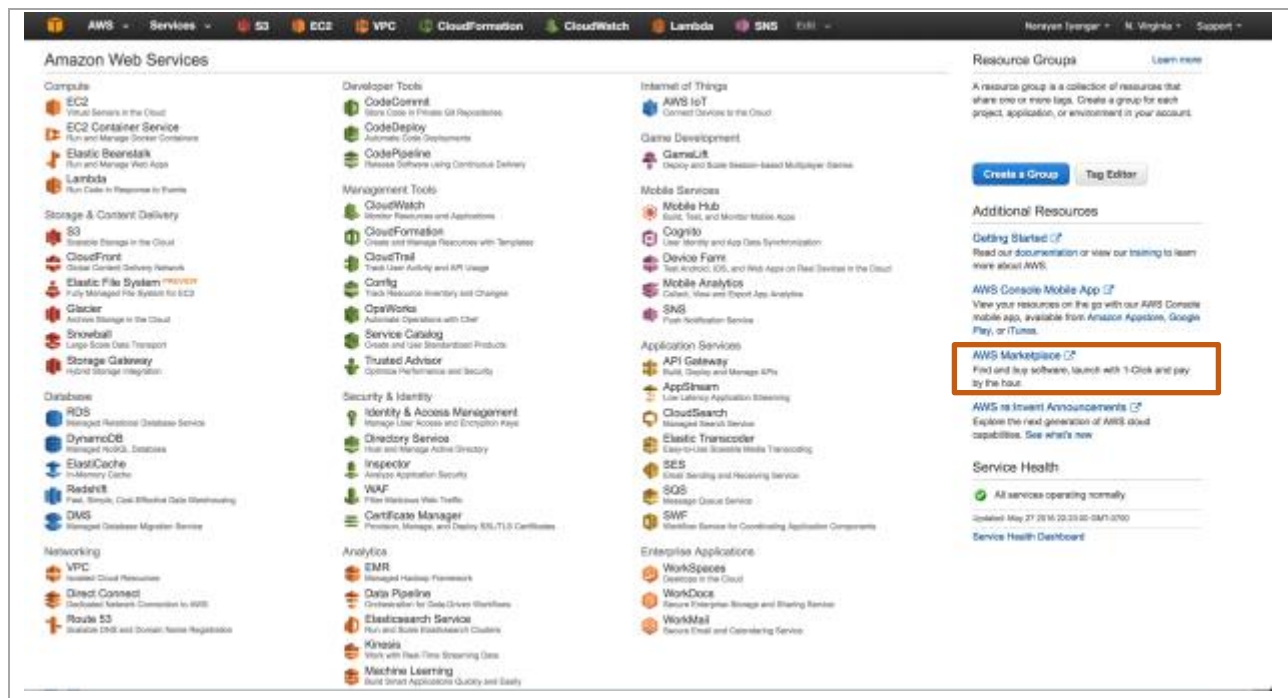
6.2 Add a credit card to your AWS account

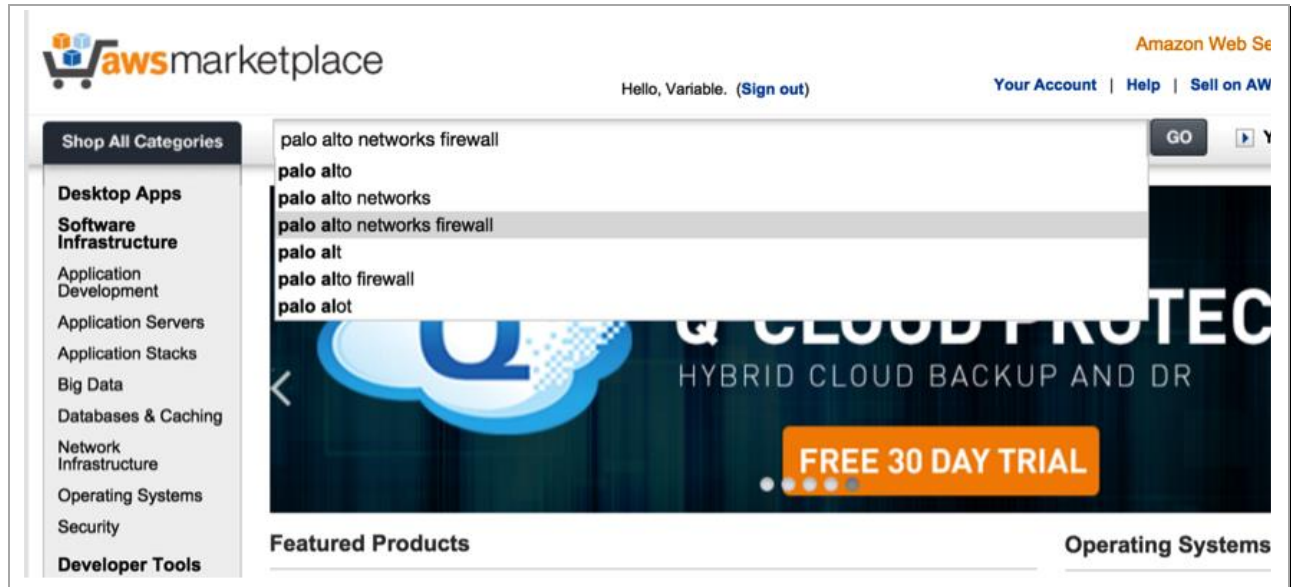
In order to continue you will need to add a method of payment to your AWS account. Use the following <https://console.aws.amazon.com/billing/home#/paymentmethods>

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

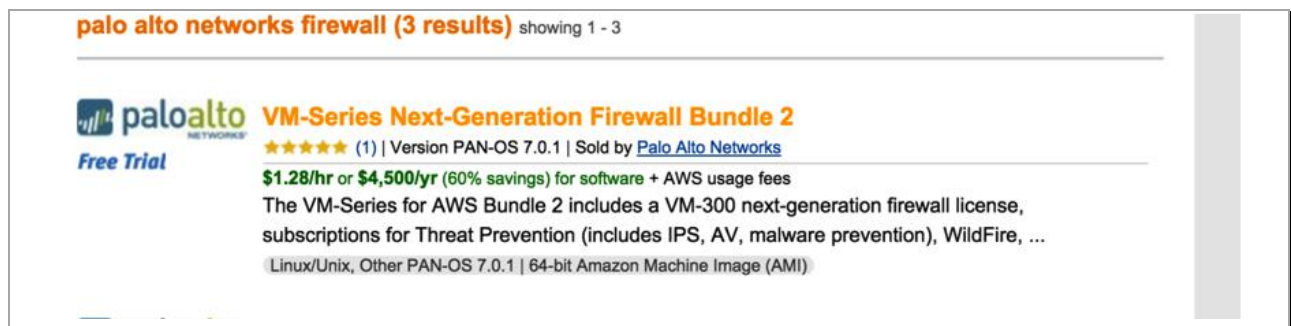
6.3 Review and accept the EULA

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



The screenshot displays the AWS Marketplace interface for the Palo Alto Networks VM-Series Next-Generation Firewall Bundle 2. The header includes the AWS Marketplace logo, a search bar, and navigation links. The product title is prominently displayed in orange. Below the title, the seller is identified as Palo Alto Networks. A detailed description of the bundle's features is provided, followed by a 'Read more' link. The page is divided into two main sections: product specifications on the left and pricing details on the right. The 'Continue' button is highlighted with an orange box, indicating the next step in the purchase process.

awsmarketplace Amazon Web Services Home
Sign in or Create a new account Your Account | Help | Sell on AWS Marketplace

Shop All Categories ▾ Search AWS Marketplace GO ▶ Your Software

VM-Series Next-Generation Firewall Bundle 2

Sold by: Palo Alto Networks

15 Day Free Trial Available - The VM-Series for AWS Bundle 2 includes a VM-300 next-generation firewall license, subscriptions for Threat Prevention (includes IPS, AV, malware prevention), WildFire, URL Filtering (PAN-DB), GlobalProtect and Premium Support. The VM-Series for AWS Bundle 2 natively analyzes all traffic in a single pass to determine the application identity, the content within, and the user identity. These business relevant elements are then used as integral components of your security policy, resulting in an improved security posture and a reduction in incident response time. Traffic flowing into, and across ...
[Read more](#)

Customer Rating	★★★★★ (1 Customer Review)
Latest Version	PAN-OS 7.0.1
Operating System	Linux/Unix, Other PAN-OS 7.0.1
Delivery Method	64-bit Amazon Machine Image (AMI) (Learn more)
Support	See details below
AWS Services Required	Amazon EC2, Amazon EBS
Highlights	■ Bundle 2 includes everything you need to protect your AWS environment. It includes: a VM-Series 300 firewall license, subscriptions for Threat Prevention, WildFire, URL Filtering,

Continue You will have an opportunity to review your order before launching or being charged.

Pricing Details

For region
US West (Oregon) ▾

Hourly Fees
Total hourly fees will vary by instance type and EC2 region.

Fees: Hourly ☒ Annual ☐
Software annual pricing savings over hourly: 60% ?

Click **Continue**.

Launch on EC2:

VM-Series Next-Generation Firewall Bundle 2

1-Click Launch
Review, modify, and launch

Manual Launch
With EC2 Console, APIs or CLI

Click "Accept Software Terms" to gain access to this software

Once you accept these terms, you will have access to this software in any supported region. You can then launch the AMIs listed below directly from the EC2 console, EC2 APIs, or with other AWS management tools.

Software Pricing

Subscription Term
☒ Hourly
☐ Annual

Applicable Instance Type
Software fee
Varies
Depends on instance type, reference pricing chart.

Usage Instructions

Select a Version

Price for your selections:
Price will be dependent on usage

Accept Software Terms

You will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's End User License Agreement (EULA) and your use of AWS services is subject to the AWS Customer Agreement.

Pricing Details
For region
US West (Oregon)

Your Free Trial has expired

Hourly Fees
Total hourly fees will vary by instance type and EC2 region.

EC2 Instance Type	Software	EC2	Total

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

You should see this screen:

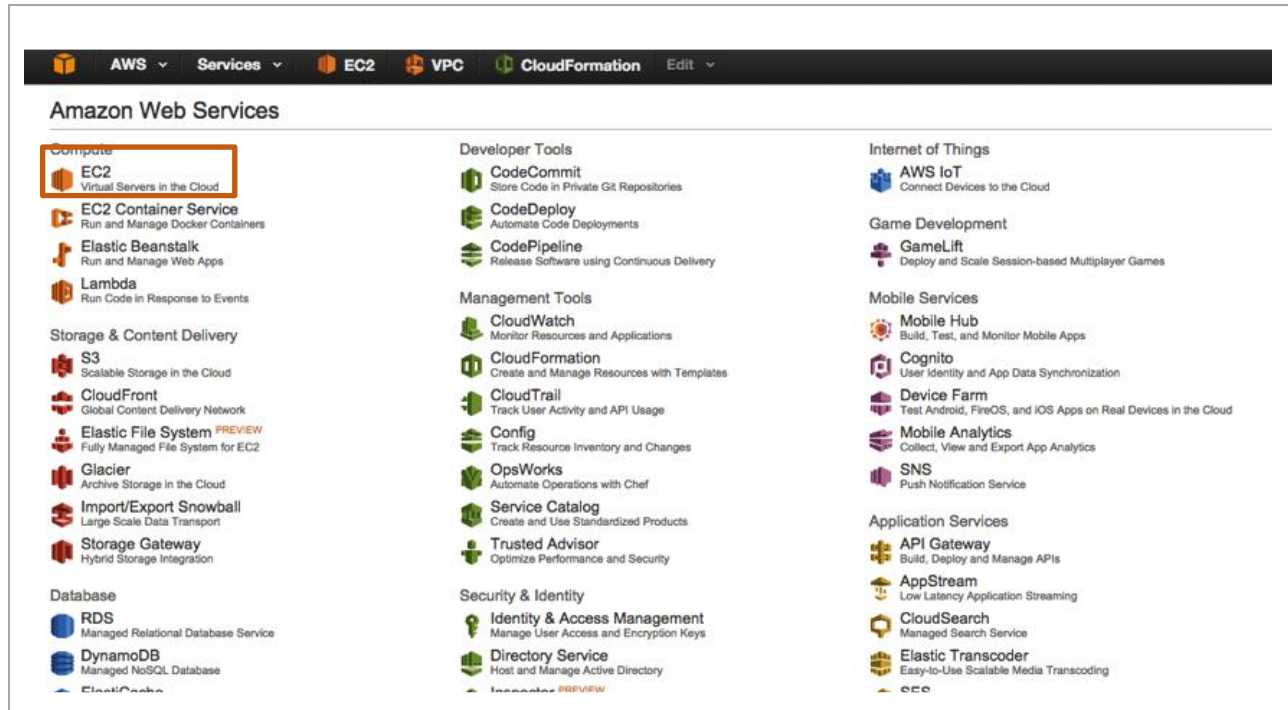
✓ Software and AWS hourly usage fees apply when the instance is running. These fees will appear on your monthly bill. Please refresh this page later to enable launch with ec2 console.

Thank you! Your subscription will be completed in a few moments.

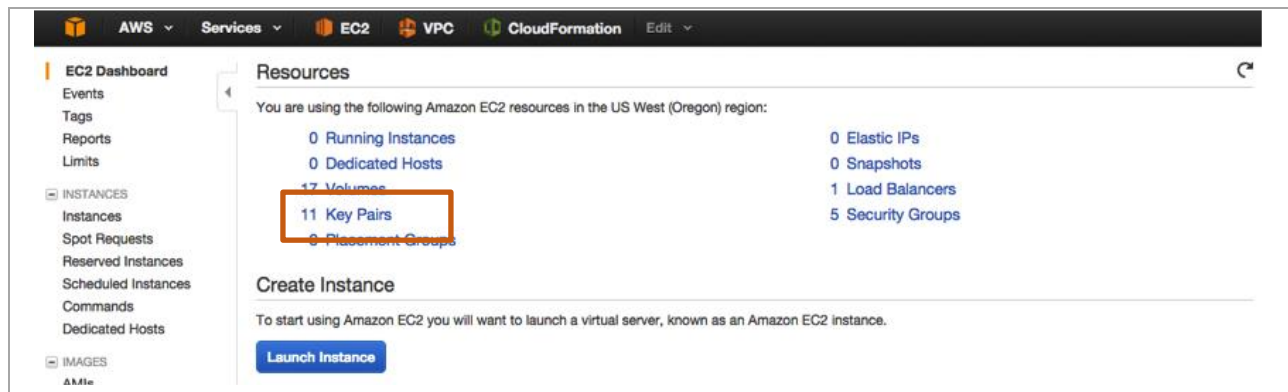
You can now close the browser tab or window and continue with the next step.

6.4 Create and download an SSH keypair

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



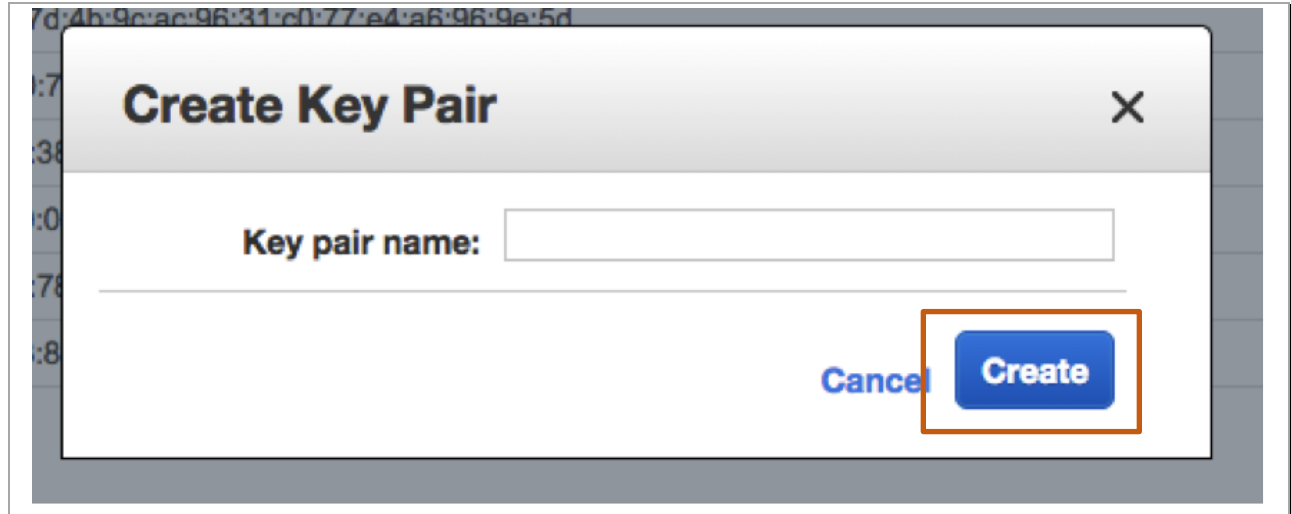
Click **KeyPairs**



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/bootstra-p-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.

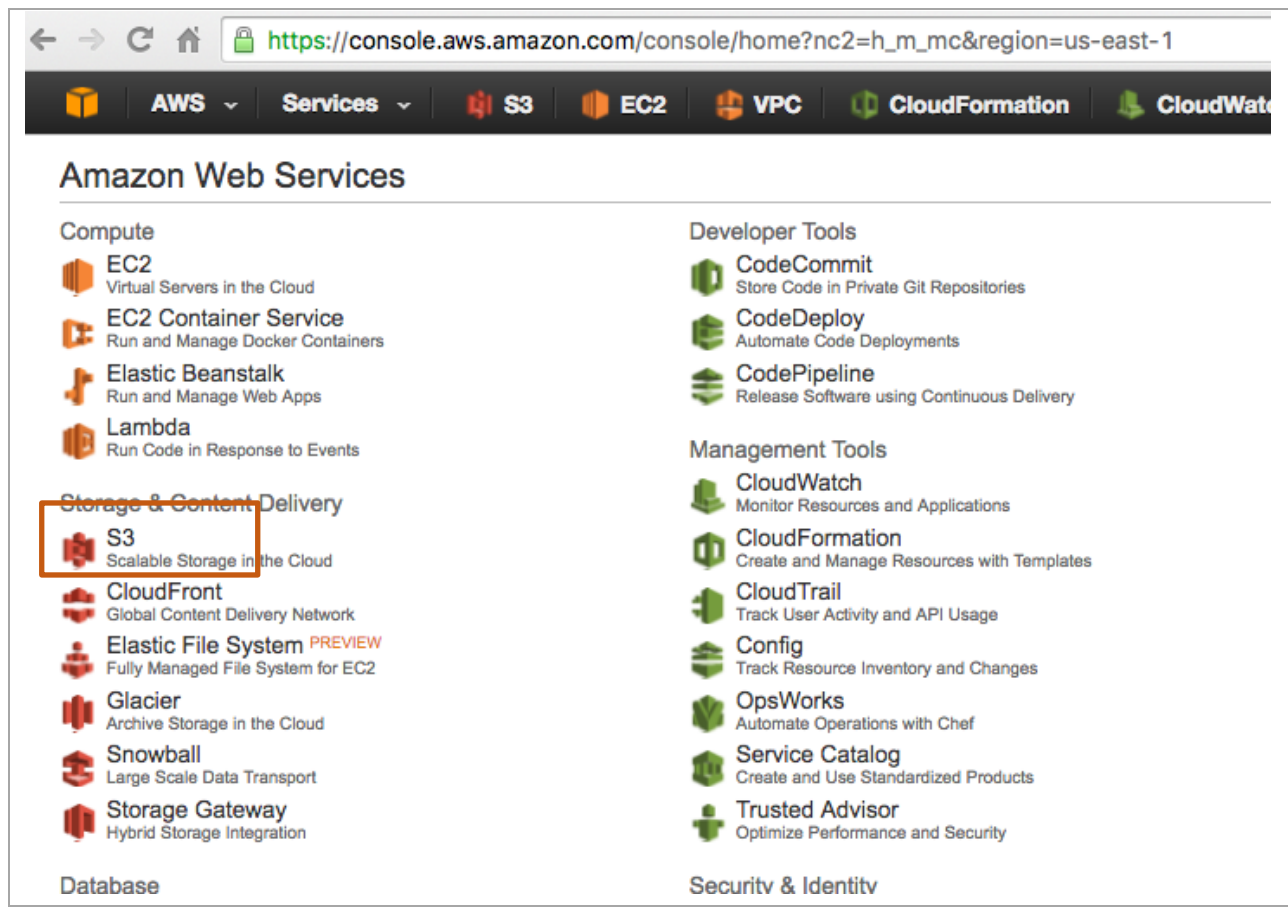
The “bootstrap-gateway” and “bootstrap-portal” directories have bootstrapping and configuration information for the gateways and portal respectively.

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

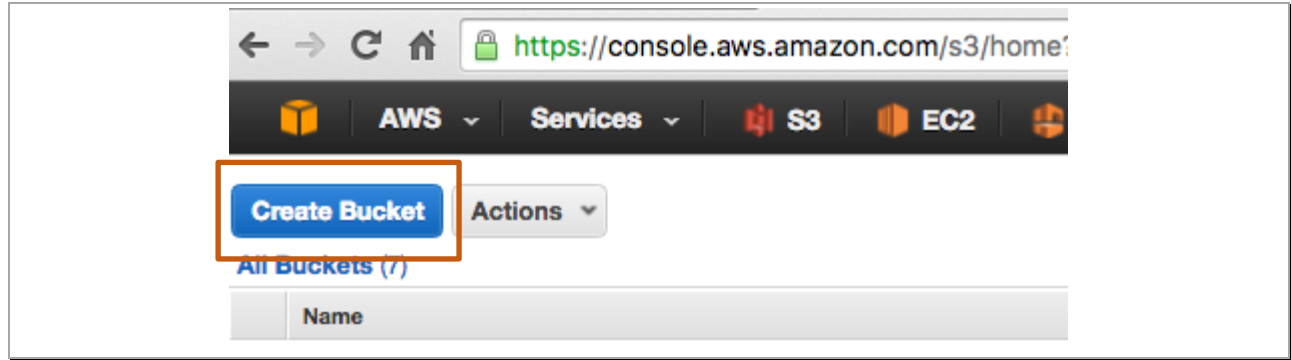
The config_fw.zip file contains all the necessary lambda scripts

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**:



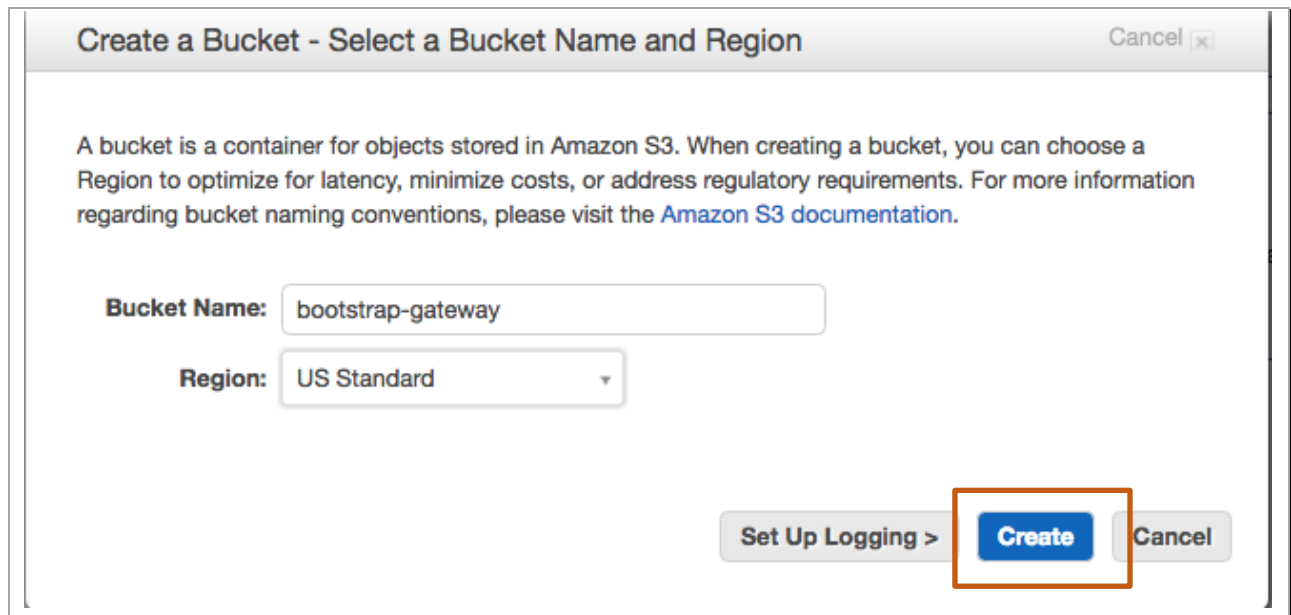
And click “**Create Bucket**” button:



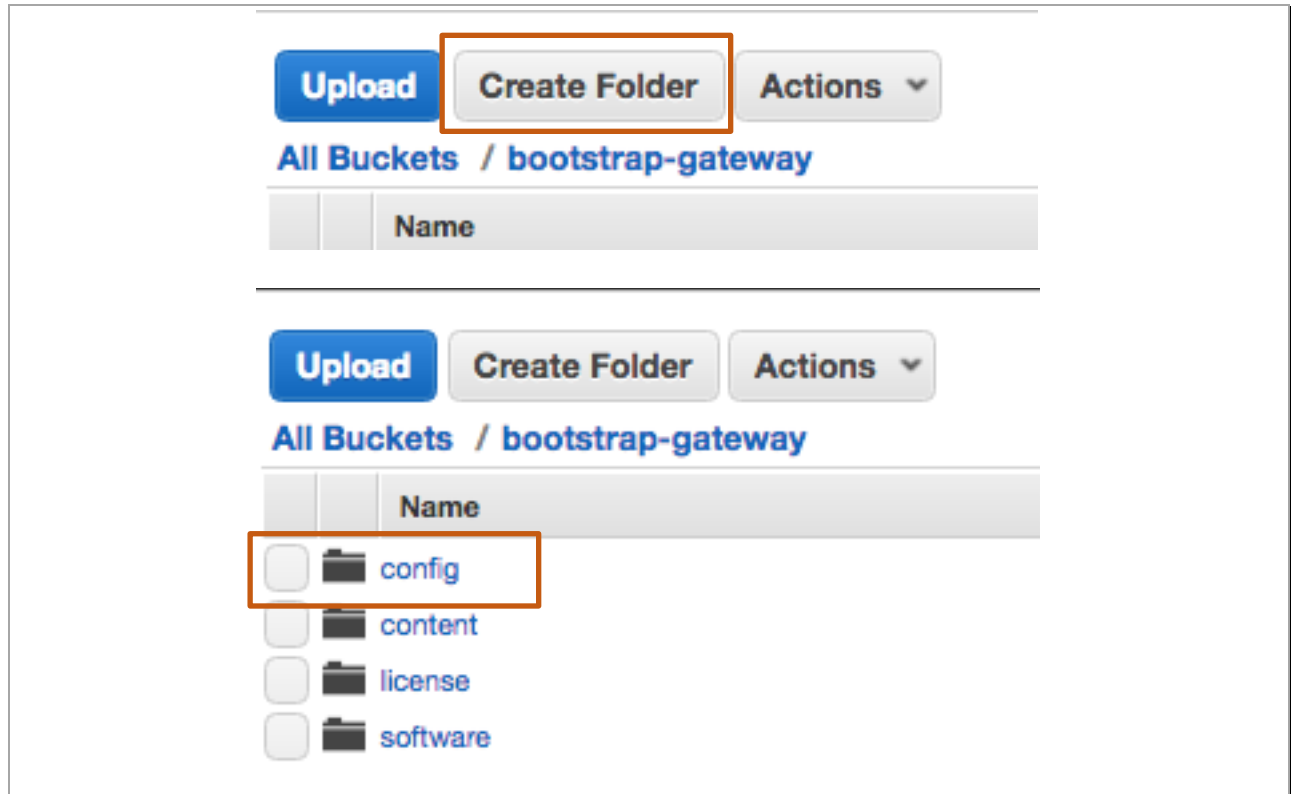
Type-in a bucket name (needs to be unique) and select the region in which the bucket will reside. This should be the same region where the template will be deployed **and** Lambda is available. This bucket will be used to store bootstrap files for the GP Gateway.

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).

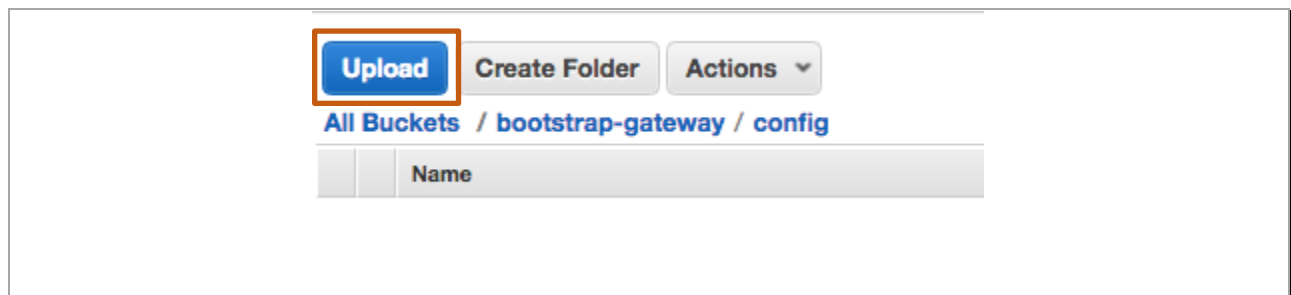
Note: If launching the CFT in N. Virginia, select the region as “**US Standard**”

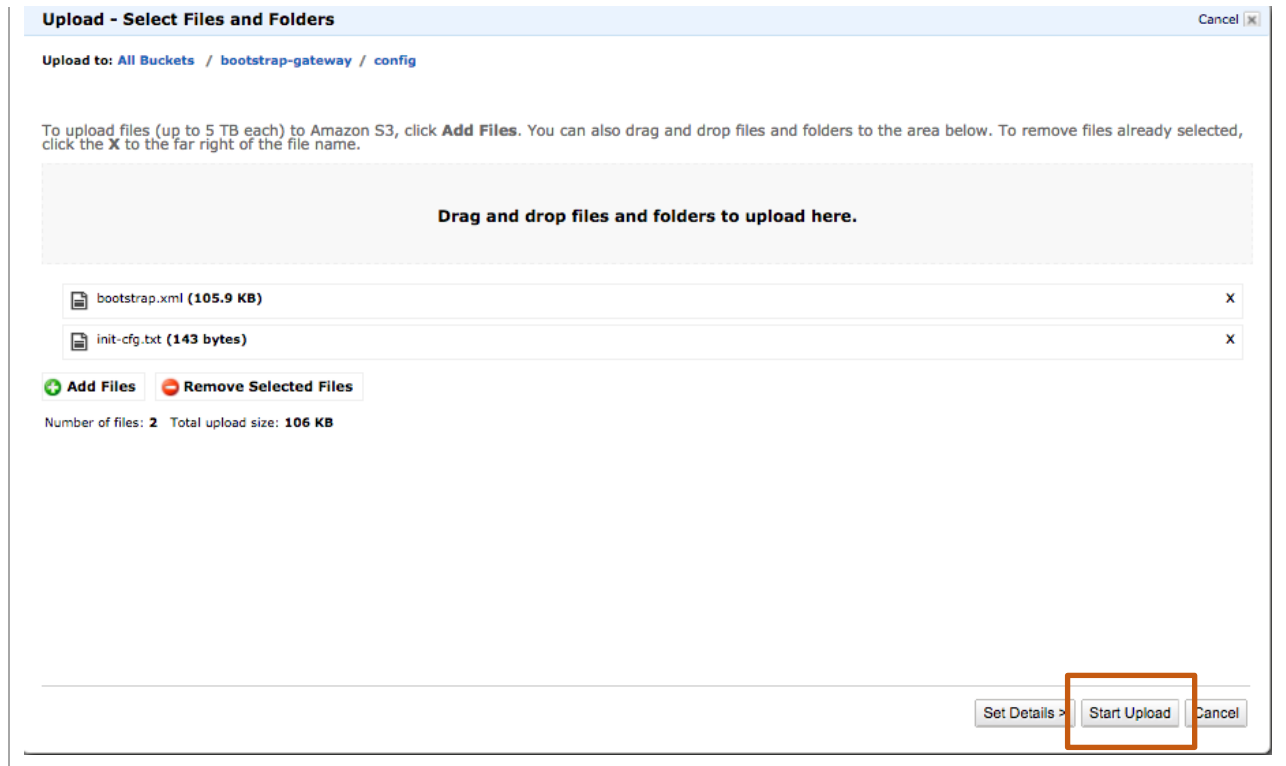


Once the bucket is created, click on the bucket name to navigate to the bucket and create **four** sub-buckets called **config**, **content**, **license** and **software** respectively. Navigate to the **config** bucket and click “**Upload**”



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**”:



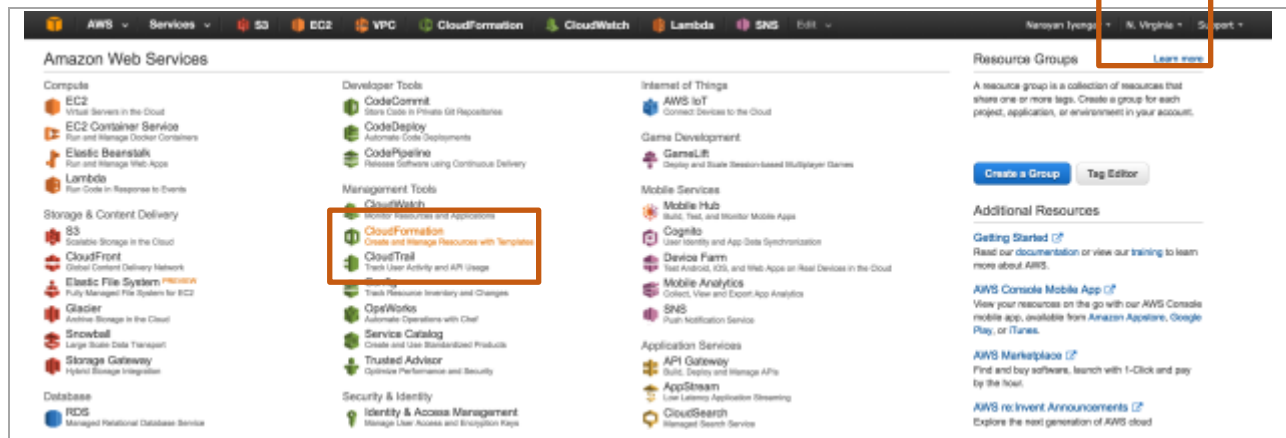


Repeat the above steps and create a bucket to upload the portal's bootstrap configuration files.

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).

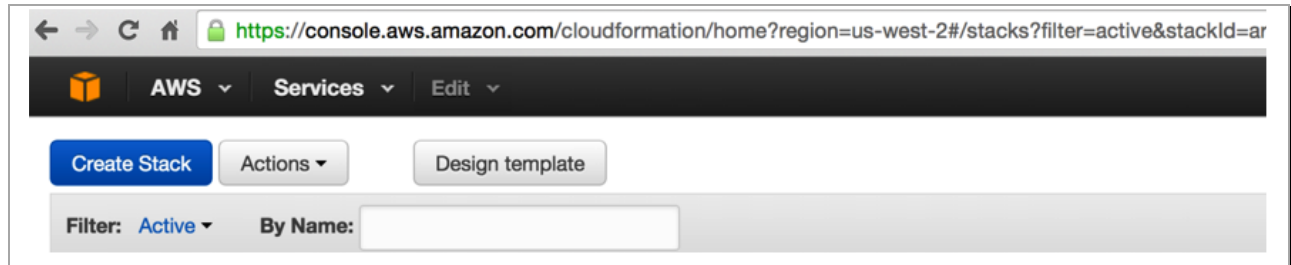
10. Launch the CFT

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

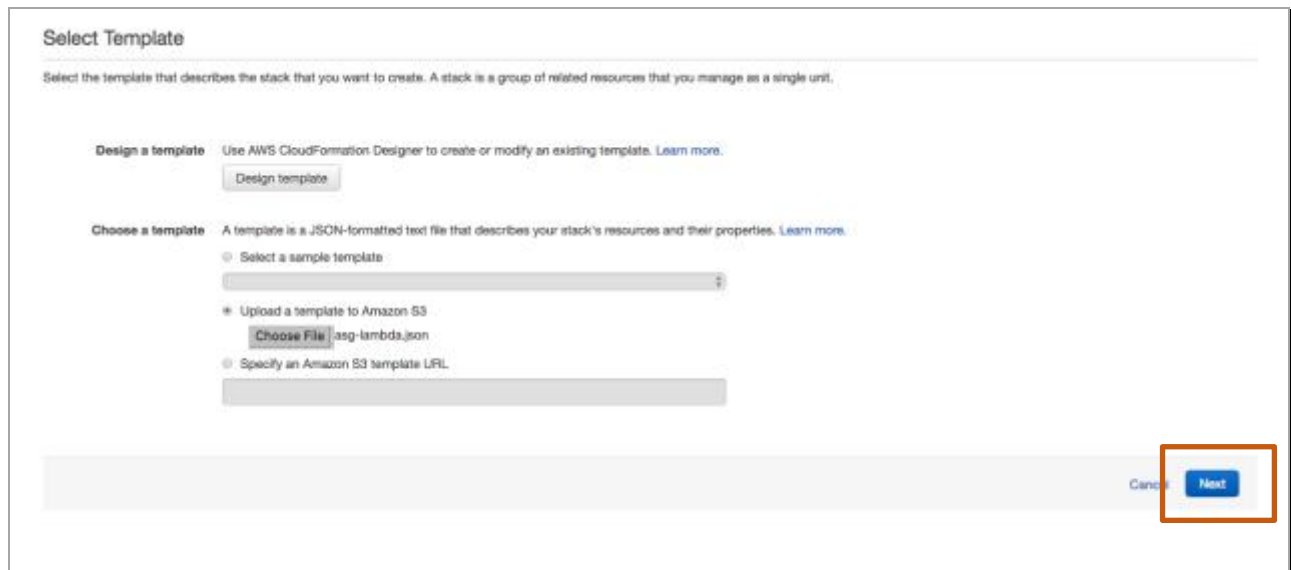


Note: Please make sure that your region (on the top right) is set to a region where Lambda is available (and the S3 buckets were created).

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**.

Create stack

Select Template
Specify Details
Options
Review

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:

Parameters

GatewayBootstrapBucketName: Bucket name for GP Gateway bootstrap configuration

LambdaBucketName: Bucket name where lambda scripts reside

PortalBootstrapBucketName: Bucket name for GP Portal bootstrap configuration

ServerKeyName: Name of an existing EC2 KeyPair to enable SSH access to the instances from SecurityController

[Cancel](#) [Previous](#) [Next](#)

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

Options

Tags

You can specify tags (key-value pairs) for resources in your stack. You can add up to 10 unique key-value pairs for each stack. [Learn more.](#)

	Key (127 characters maximum)	Value (255 characters maximum)	
1	<input type="text"/>	<input type="text"/>	+

Advanced

You can set additional options for your stack, like notification options and a stack policy. [Learn more.](#)

[Cancel](#) [Previous](#) [Next](#)

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

Review

Template

Template URL: <https://us-east-1.amazonaws.com/cloud-formation/templates/1-ekuzc90m0y-us-east-1/2016148RVV-ang-lambda.json>
 Description: GlobalProtect AutoScaling Demo.
 Estimate cost: Cost

Details

Stack name: gp-ang-demo
 ServerKeyName: aws-keypair-virginia
 Create IAM resources: Yes

Options

Tags
 No tags provided

Advanced

Notification Timeout: none
 Rollback on failure: Yes

Capabilities

i The following resource(s) require capabilities: [AWS::IAM::InstanceProfile, AWS::IAM::Policy, AWS::IAM::Role]
 This template would create Identity and Access Management (IAM) resources, which can include groups, IAM users, and IAM roles with certain permissions. Ensure that the template you are using is from a trusted source. [Learn more.](#)

☒ I acknowledge that this template might cause AWS CloudFormation to create IAM resources.

Cancel Previous **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.

Create Stack Actions Design template

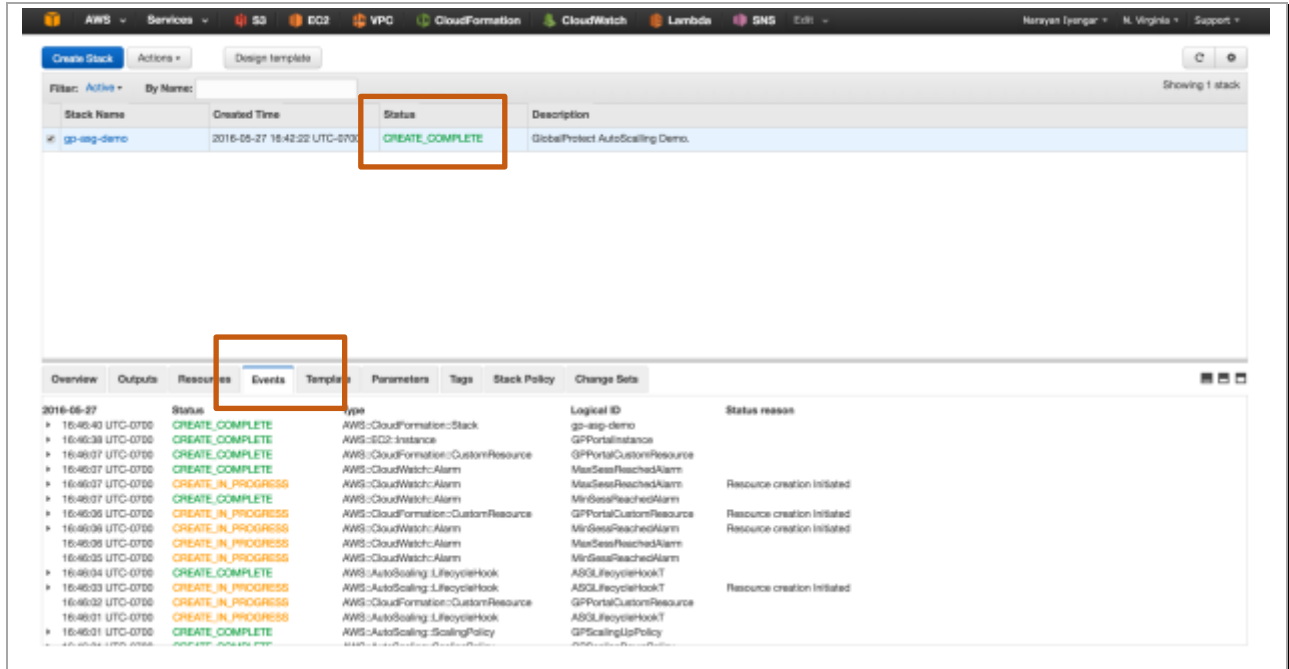
Filter: Active By Name: Showing 1 stack

Stack Name	Created Time	Status	Description
gp-ang-demo	2016-05-27 16:42:22 UTC-0700	CREATE_IN_PROGRESS	GlobalProtect AutoScaling Demo.

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

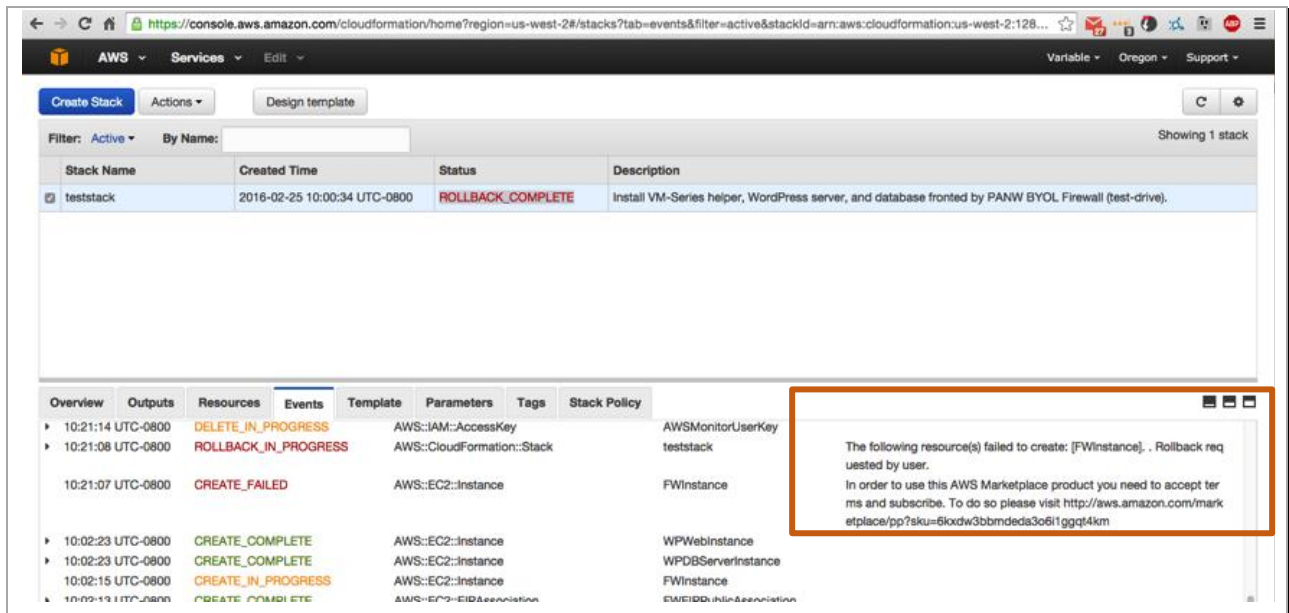
Date	Status	Type	Logical ID	Status reason
2016-05-27 16:42:22 UTC-0700	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	gp-ang-demo	User initiated

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



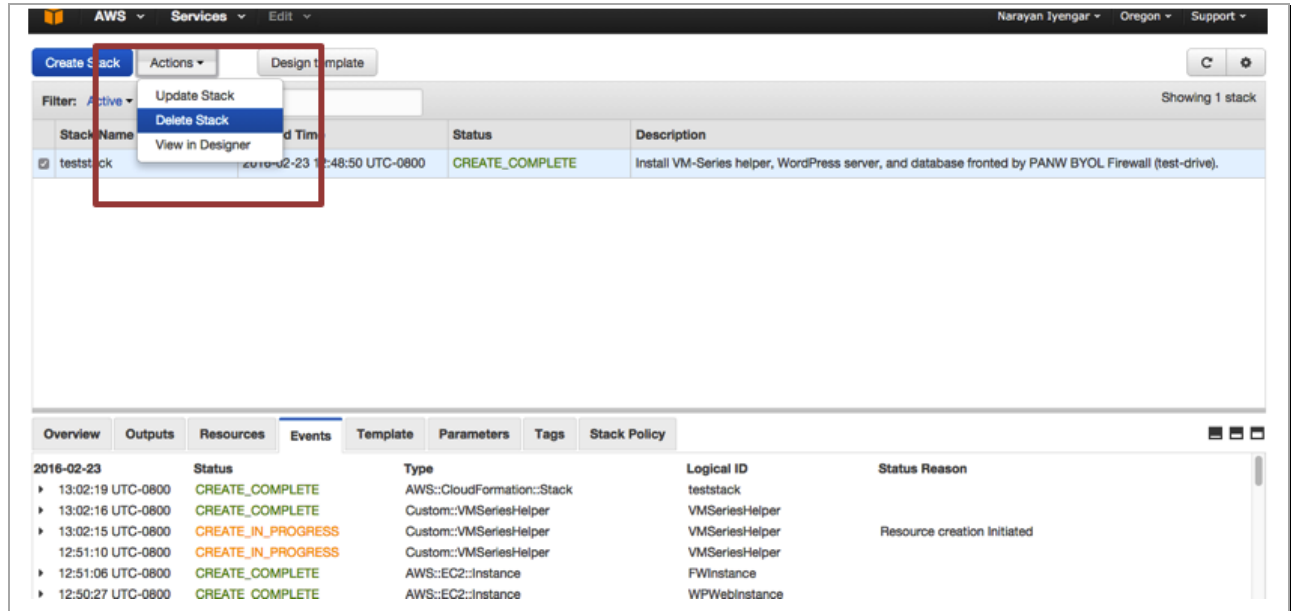
If there were any errors during the creation of the stack, you will need to drill down to the specific event in the **Events** tab and **Outputs** tab to debug and then create a new stack after fixing any errors. Scroll through the logs and find the chronologically first error. Normally, subsequent errors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



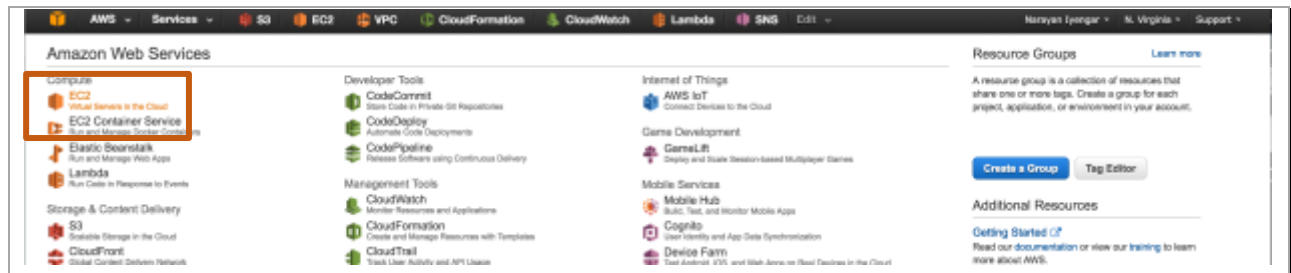
Refer to [section 2.3](#) to review and accept the EULA for the VM-Series NGFW

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



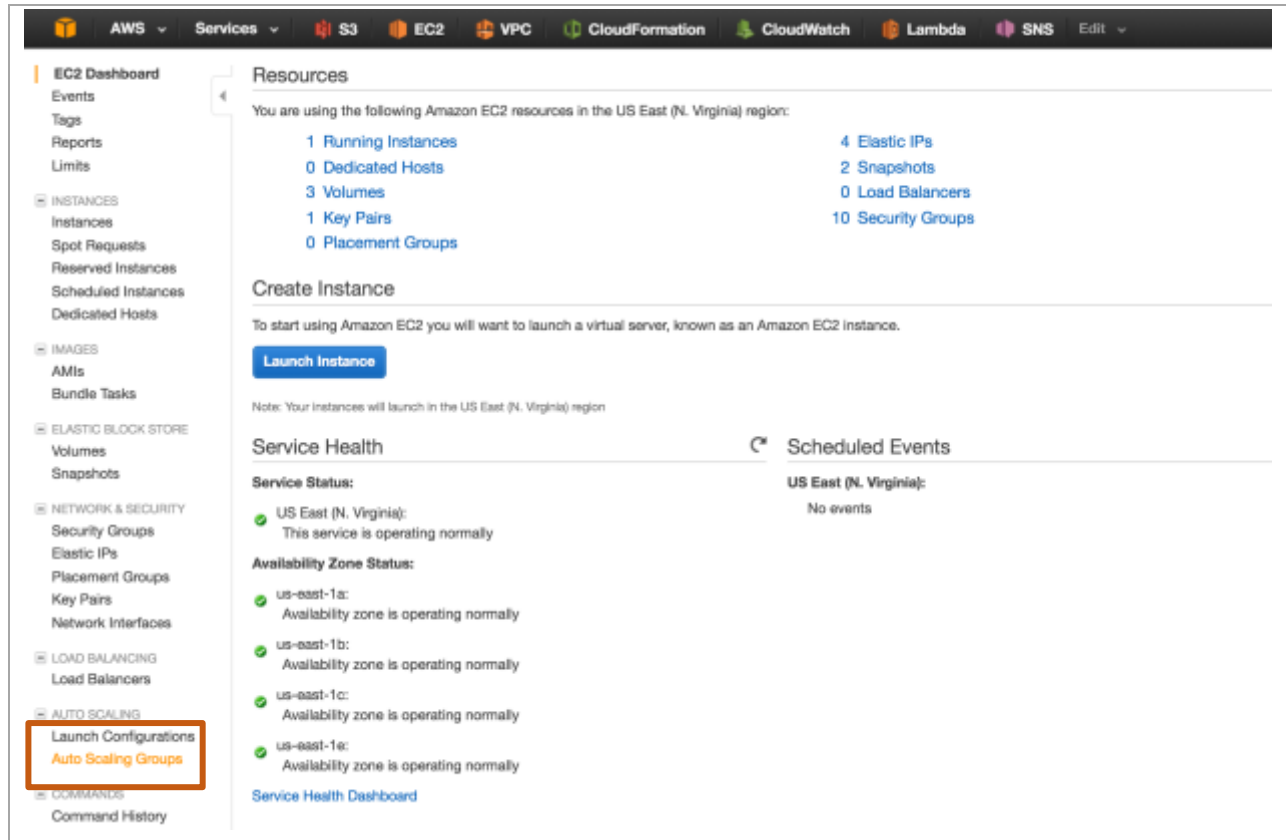
11. Launch the First Gateway

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

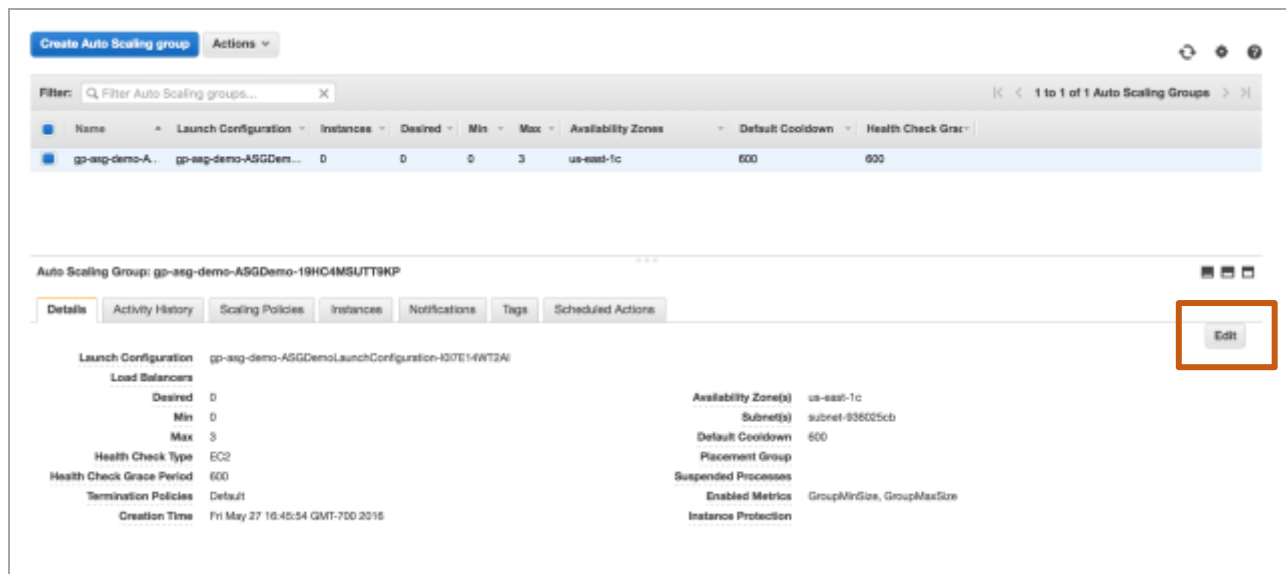


And click on “Auto Scaling Groups”

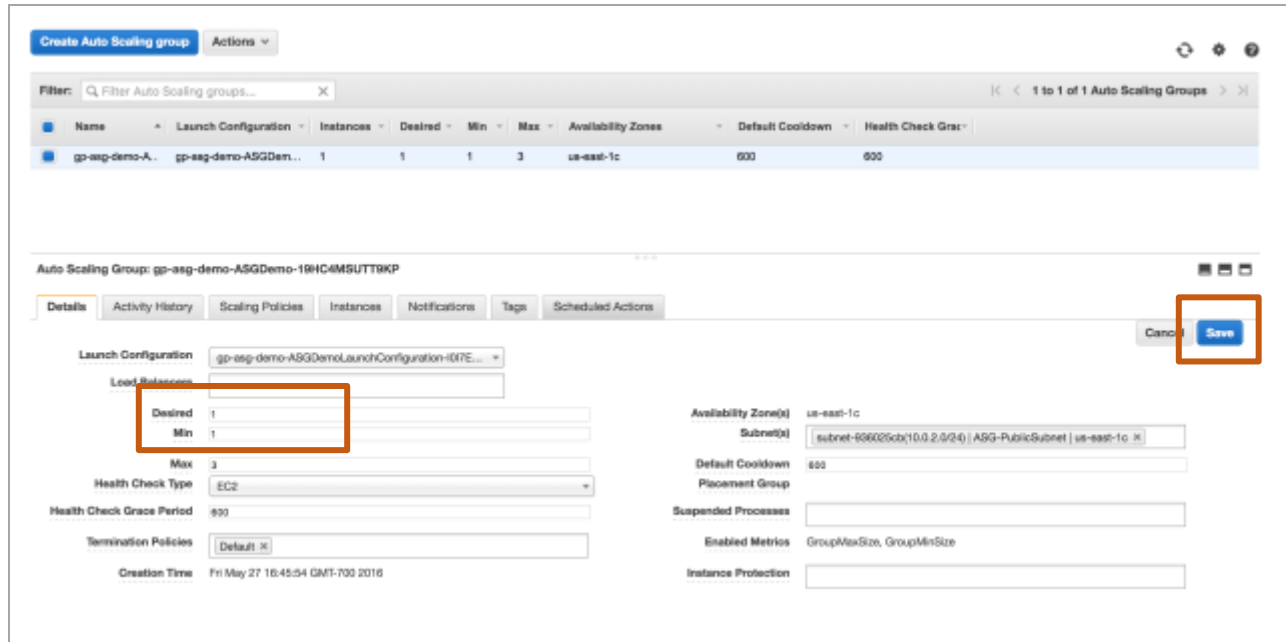
Auto Scaling GlobalProtect in AWS Deployment Guide



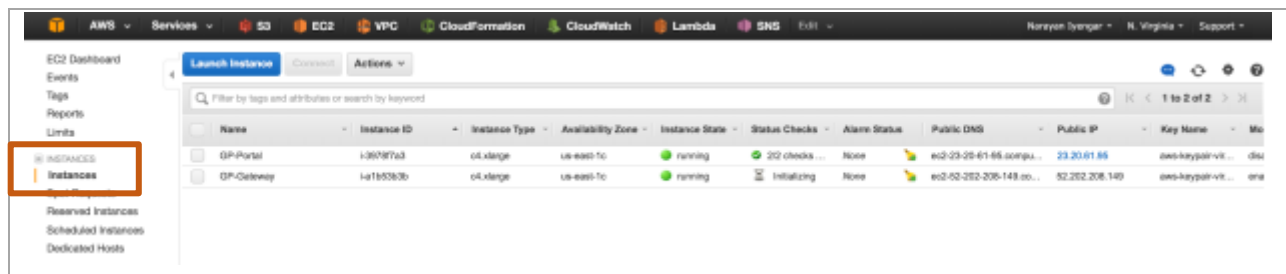
You should see the auto scaling group created by the template. Click “**Edit**”



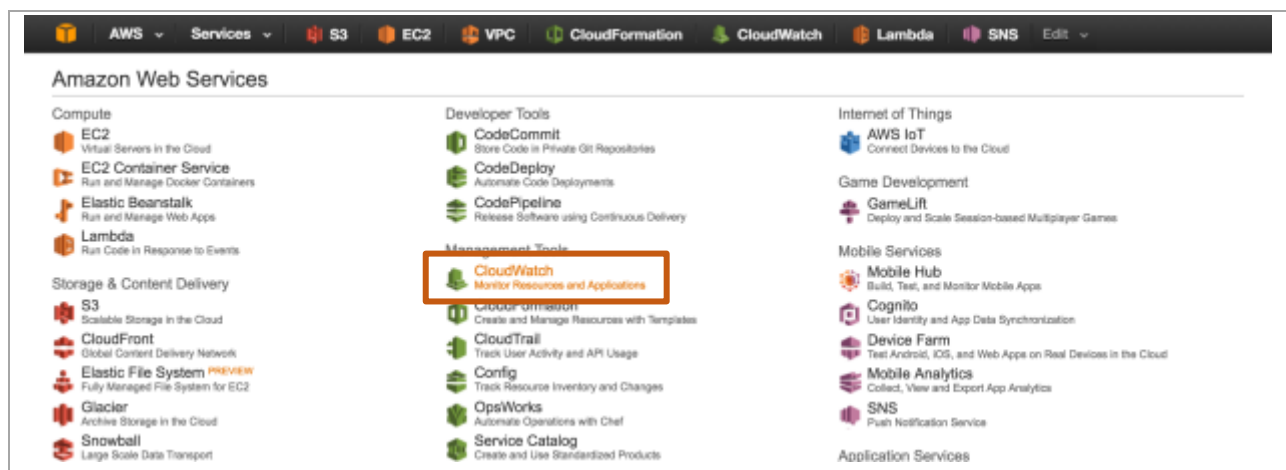
and change the “**Desired**” and “**Min**” fields to “1” and click “**Save**”:



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:

CloudWatch

Dashboards **NEW**

Alarms

ALARM 0

INSUFFICIENT 2

OK 1

Billing

Events **NEW**

Rules

Logs

Metrics

Selected Metrics

Auto Scaling

Billing

EBS

EC2

Events

Lambda

Logs

Metrics

Metric Summary

Amazon CloudWatch monitors operational and performance metrics for **5,770 CloudWatch metrics available** in the US East (N. Virginia) region

Browse or search your metrics to get started graphing data and creating alarms

Browse Metrics Search Metrics X

Alarm Summary

You have **2 alarms in INSUFFICIENT DATA** state in US East (N. Virginia)

MAX_SESS_REACHED
ActiveSessions > 20

MIN_SESS_REACHED
ActiveSessions < 5

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

CloudWatch Log Groups

Create Metric Filter Actions

Filter Log Group Name Prefix

Log Group Name	Expire Events After	Metric Filters	Subscriptions
/aws/lambda/LogGroup-1a1b53b3b	Never Expire	0 Shards	None
/aws/lambda/LogGroup-1a1b53b3b	Never Expire	0 Shards	None
/aws/lambda/LogGroup-1a1b53b3b	Never Expire	0 Shards	None
/aws/lambda/LogGroup-1a1b53b3b	Never Expire	0 Shards	None

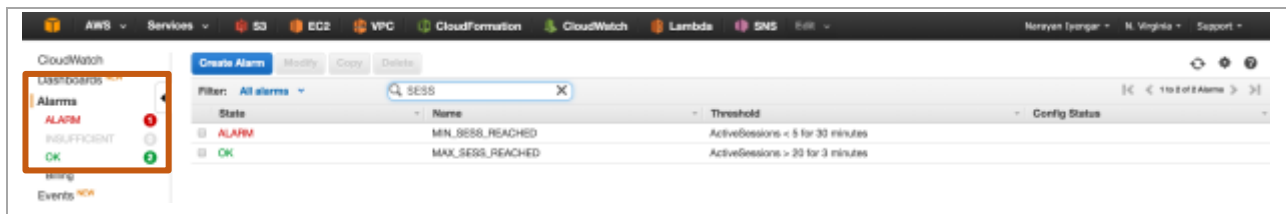
This indicates that the gateway is up and publishing metrics to CloudWatch.

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.

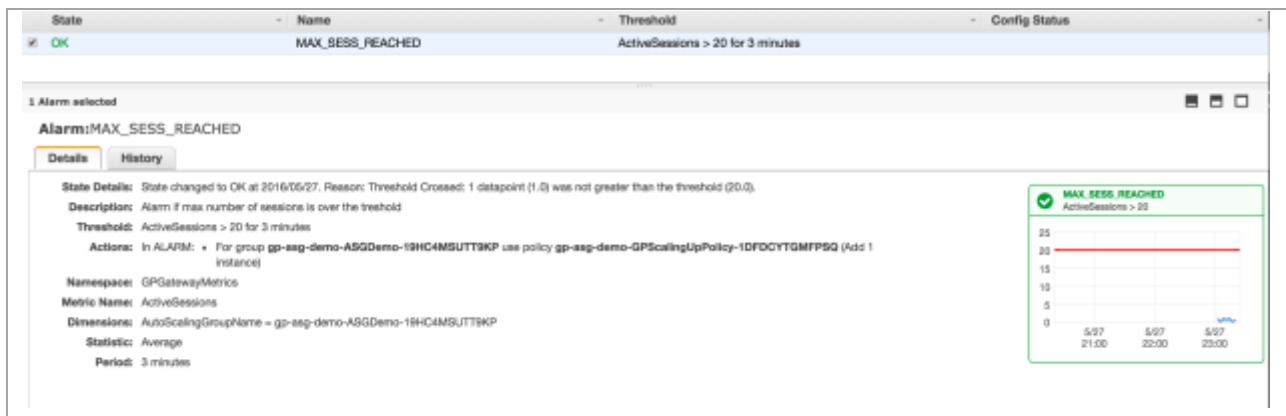
The template – for demonstration purposes – has set a very low threshold for an auto scale event to occur.

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



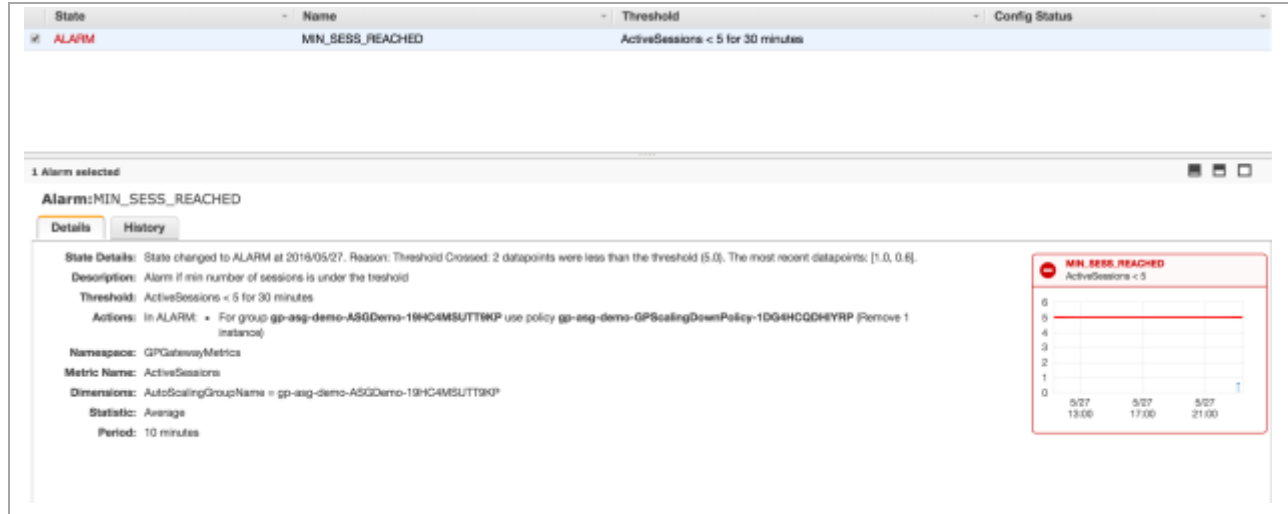
In the above screen capture, you see two alarms. MAX_SESS_REACHED and MIN_SESS_REACHED. These alarms are triggered based on metrics published by the gateways in the Auto Scale Group.

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)



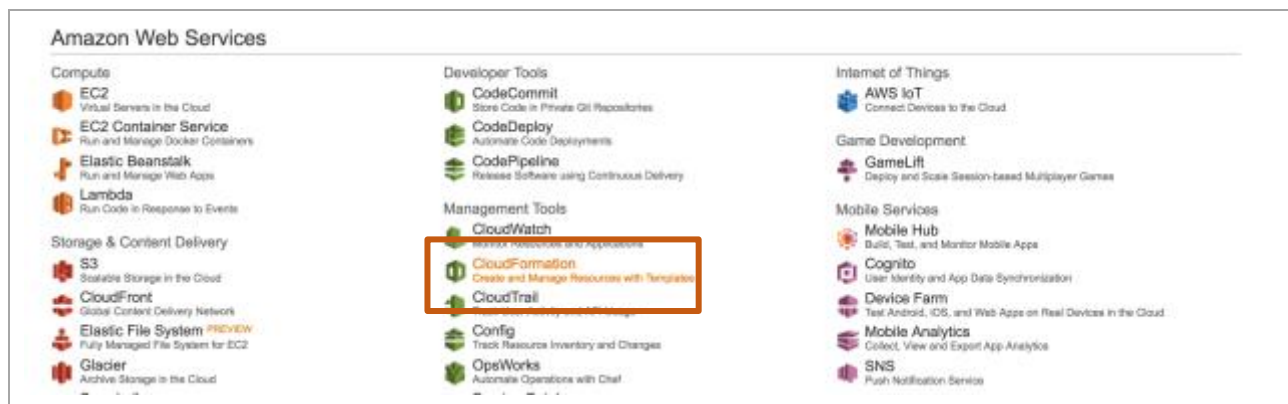
13. Trigger an Auto Scale Event

To trigger an auto scale event, you will need to establish connection with the newly deployed GP Portal. To avoid any disruption of other activity, it is recommended to use a virtual machine (Windows or Mac), if available. To download the GP Client for your particular OS refer to this link:

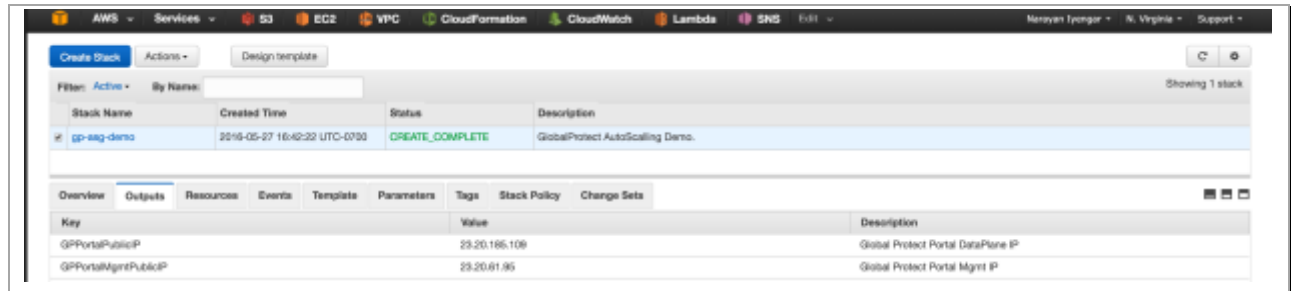
<https://www.palatonetworks.com/documentation/31/globalprotect/gp-agent-user-guide>

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



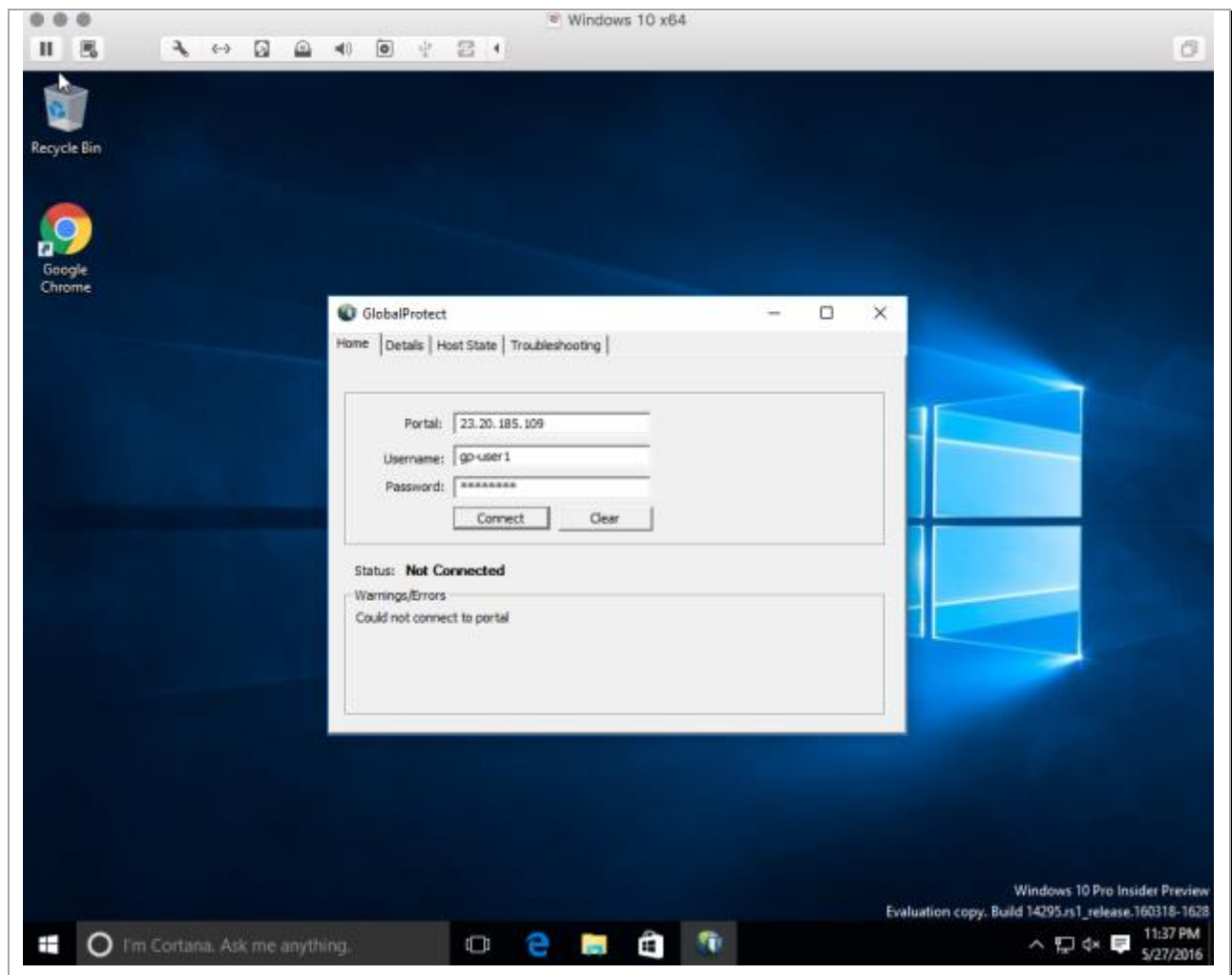
and select the stack that was just deployed. Under the “**Outputs**” tab note the **GPPortalPublicIP** address



Stack Name	Created Time	Status	Description
gp-sag-demo	2016-05-27 16:42:32 UTC-0700	CREATE_COMPLETE	GlobalProtect AutoScaling Demo.

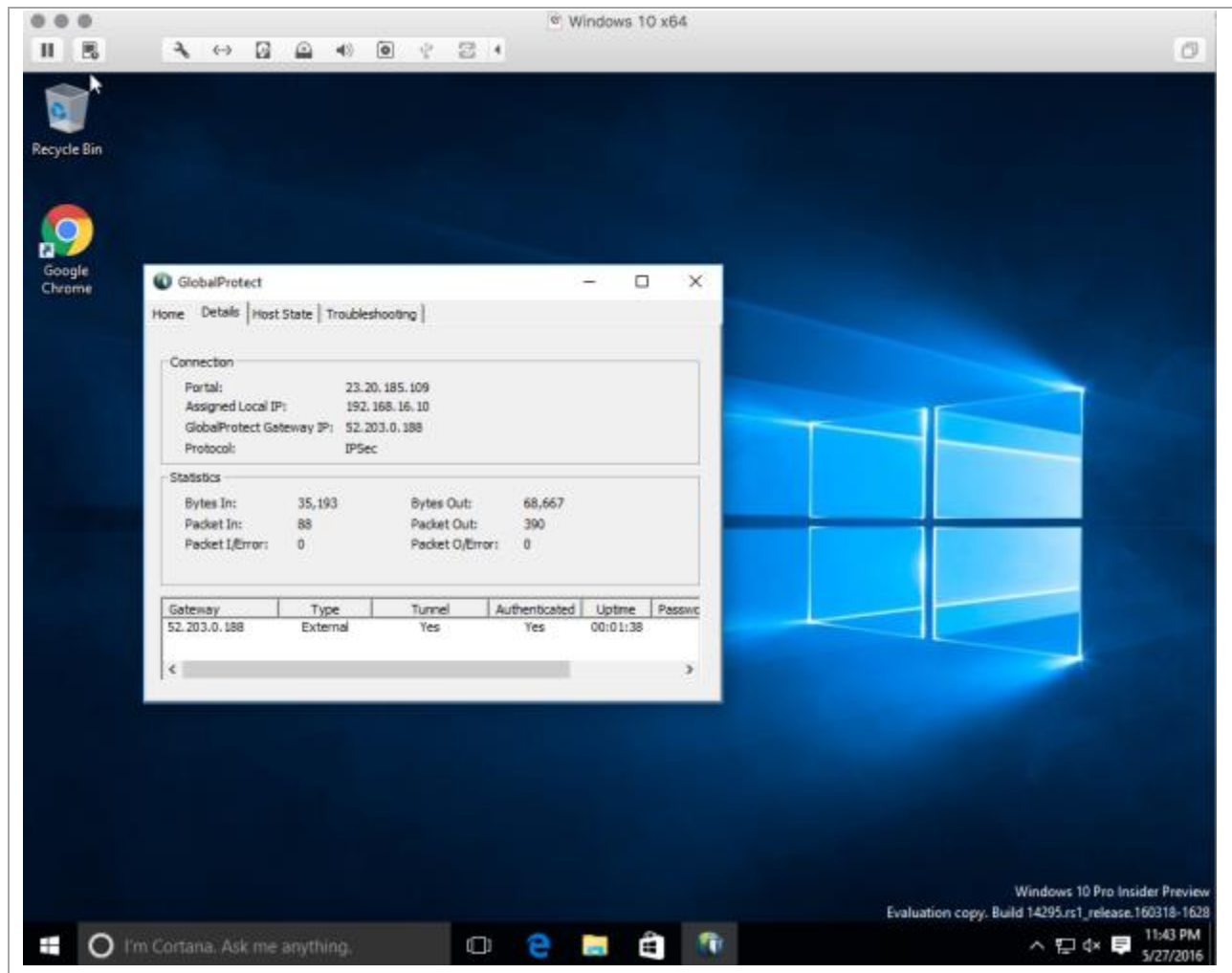
Key	Value	Description
GPPortalPublicIP	23.20.185.109	Global Protect Portal DataPlane IP
GPPortalMgmtPublicIP	23.20.61.95	Global Protect Portal Mgmt IP

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

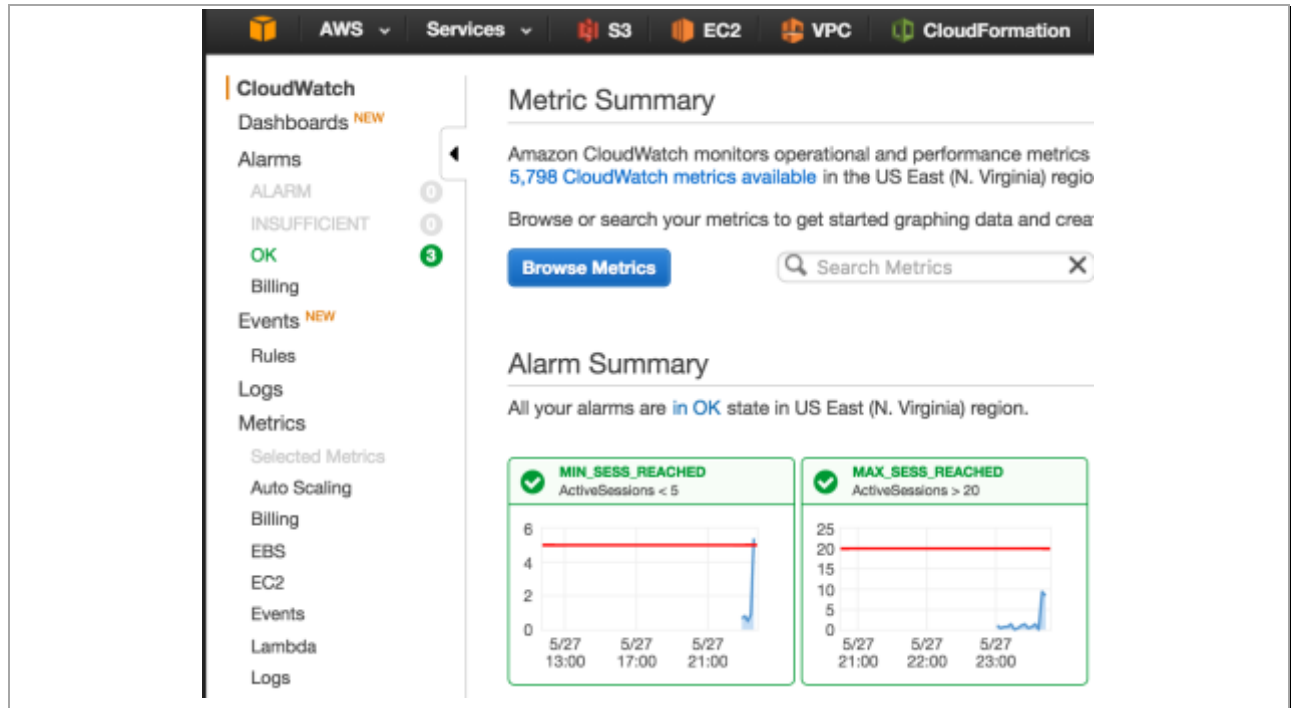


If you get an error (as seen above) that the client could not connect to the portal, you may need to disable the GlobalProtect client on your host machine. The portal and gateways use self-signed certificate and so corporate firewalls may not allow the connection to go through.

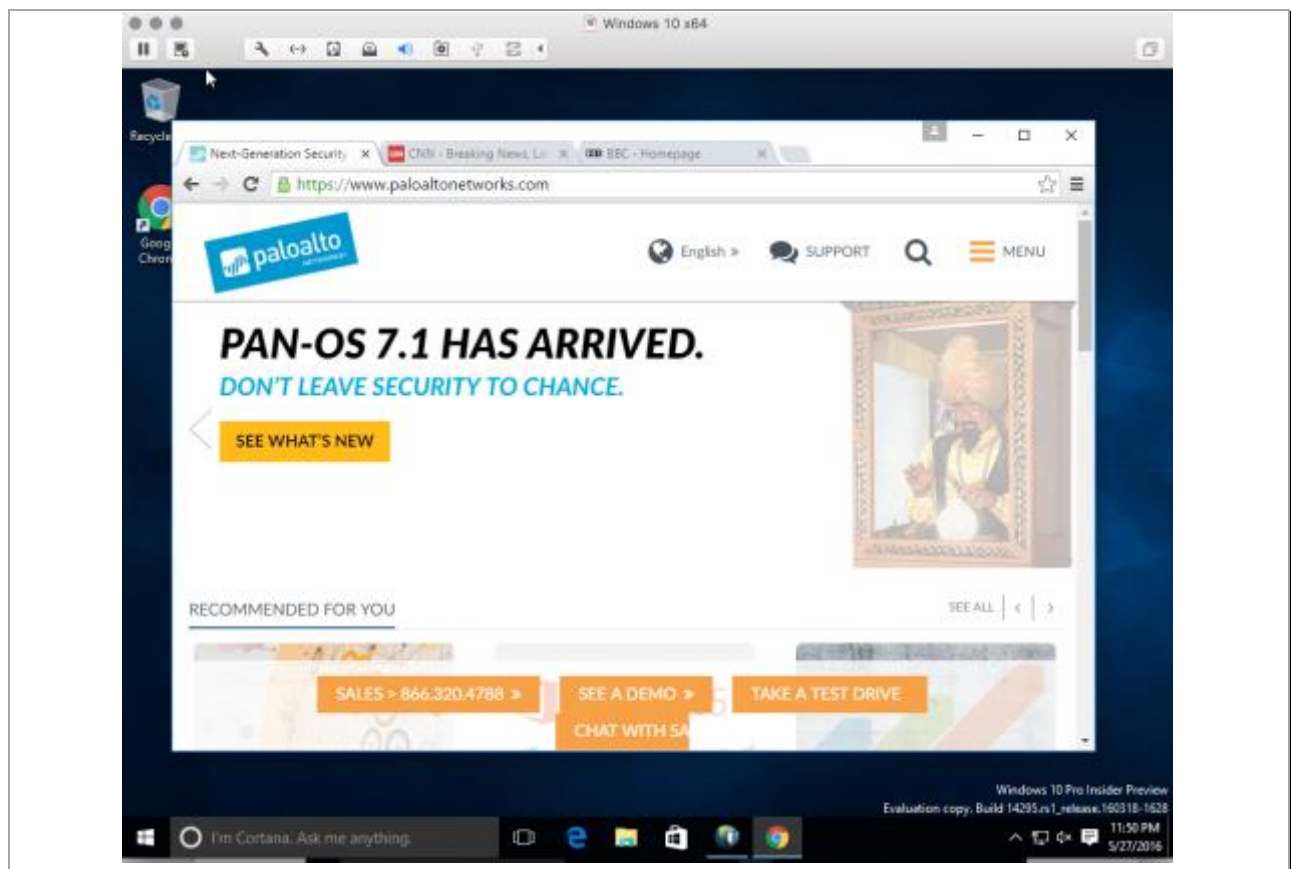
Once connected you should see the GlobalProtect Portal and Gateway information in the client **"Details"** tab:



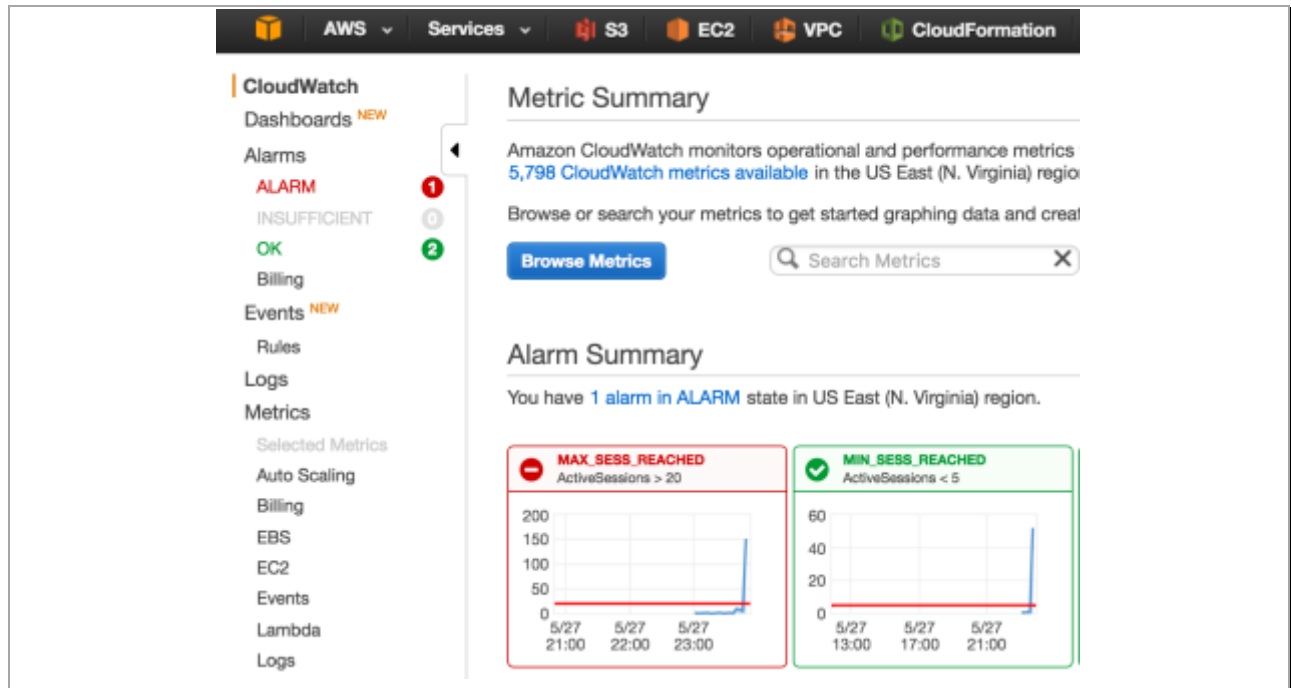
To verify that by connecting to the gateway the session count goes up head on over the AWS console and click on CloudWatch and you should see a small spike in the metrics for MAX_SESSION_REACHED:



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



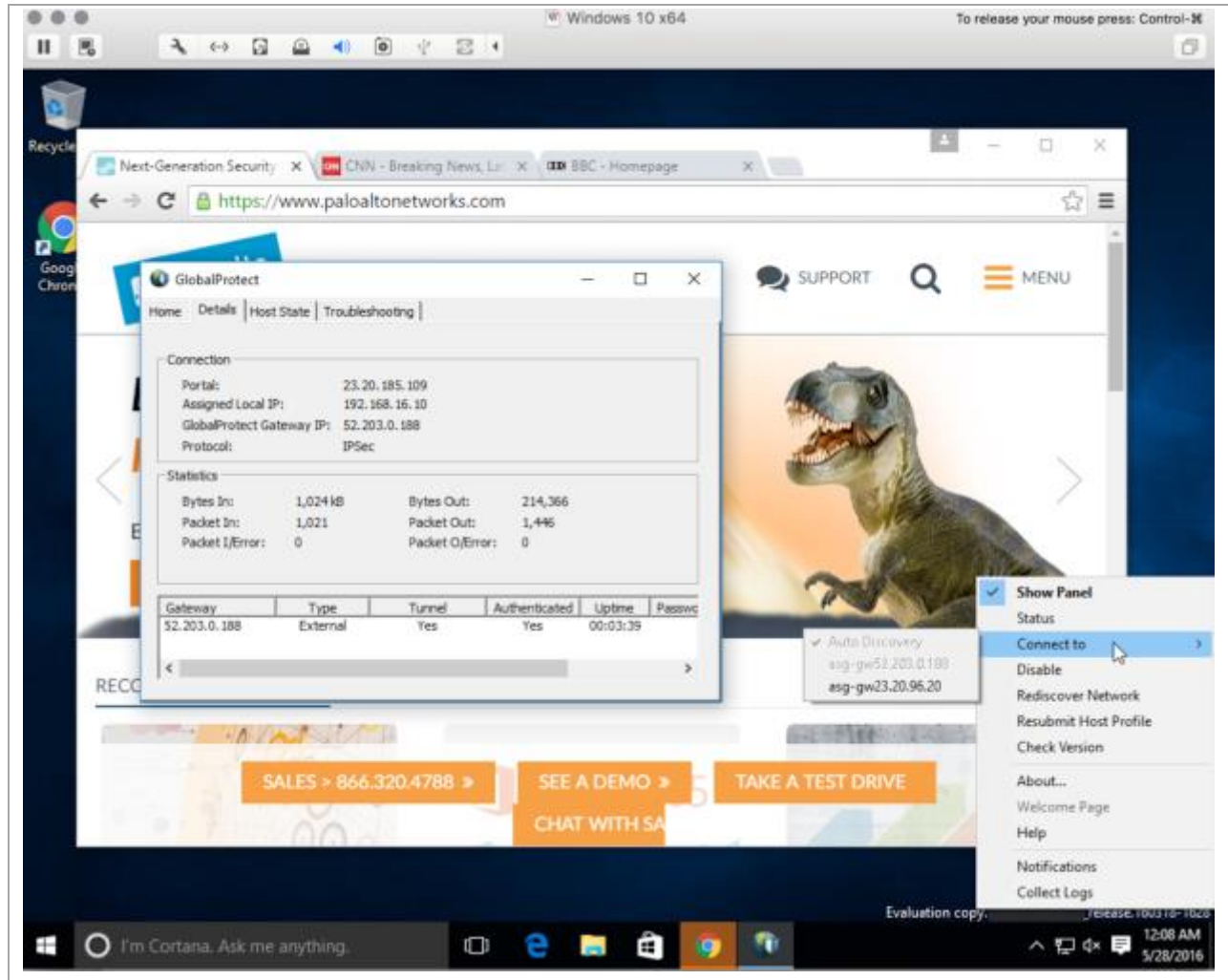
This will cause the session count to go up, trigger the alarm and cause a scale-out event and a new gateway will be provisioned, bootstrapped, configured and added to the Auto Scale Group.



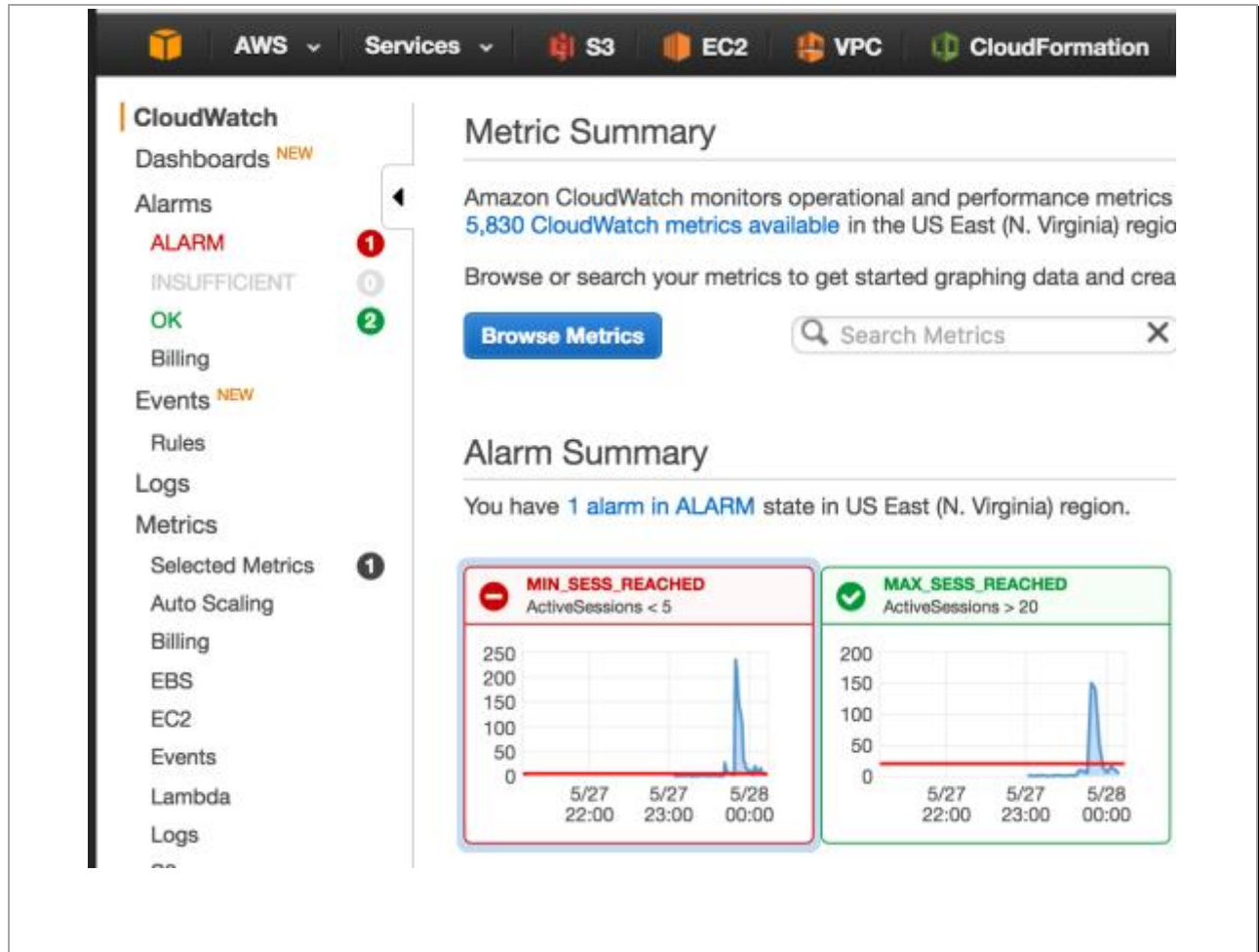
The screenshot shows the AWS EC2 console 'Instances' page. A table lists the instances, including their names, IDs, types, availability zones, states, and public IPs.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS	Public IP	Key Name	Mo
GP-Portal	i-39797a3	c4.xlarge	us-east-1c	running	2/2 checks ...	None	ec2-33-20-61-85.compu...	23.20.61.85	aws-keypair-vit...	dis
GP-Gateway	i-e1b53b3b	c4.xlarge	us-east-1c	running	2/2 checks ...	None	ec2-52-202-208-148.co...	52.202.208.148	aws-keypair-vit...	ena
GP-Gateway	i-d154da4b	c4.xlarge	us-east-1c	running	Initializing	None	ec2-33-20-3-133.compu...	23.20.3.133	aws-keypair-vit...	ena

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

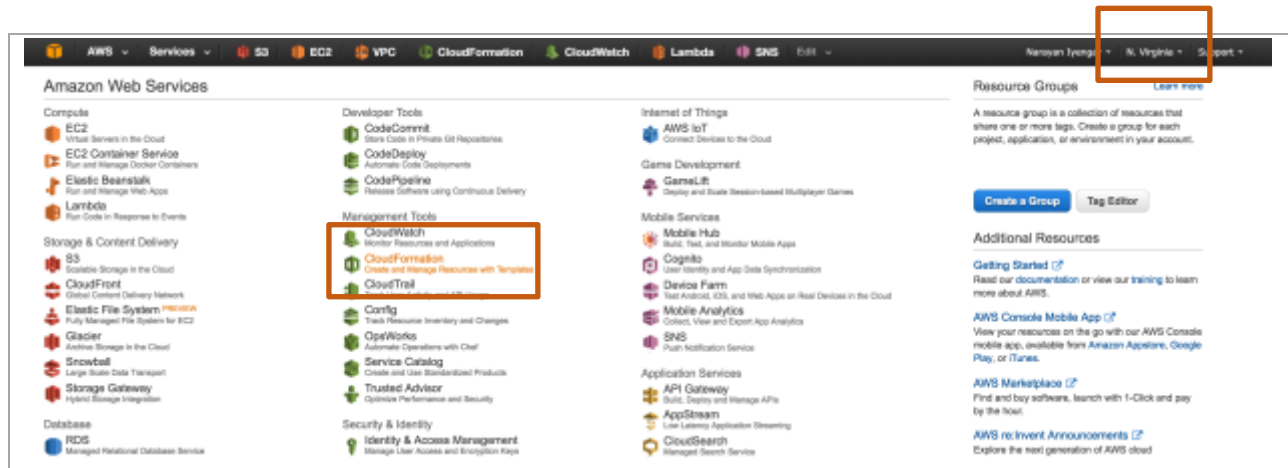


and a gateway will be removed from service

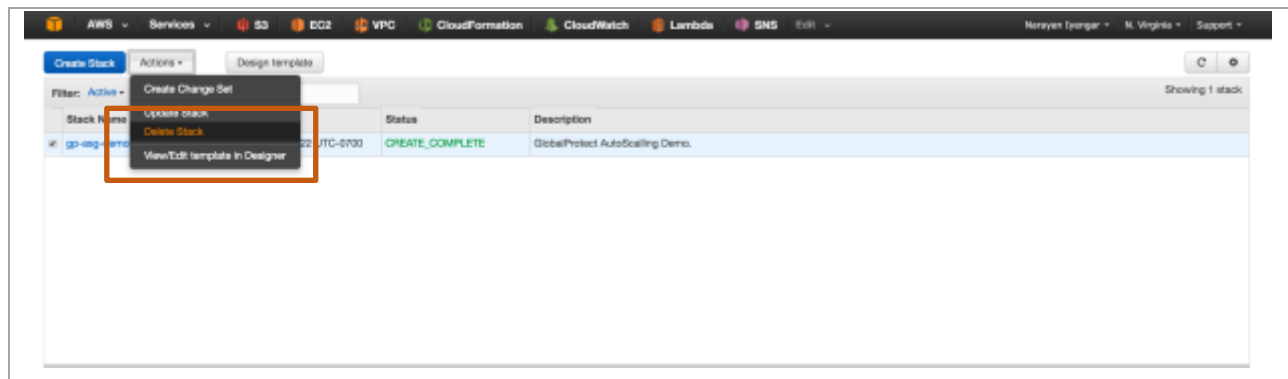


14. Cleanup

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**:

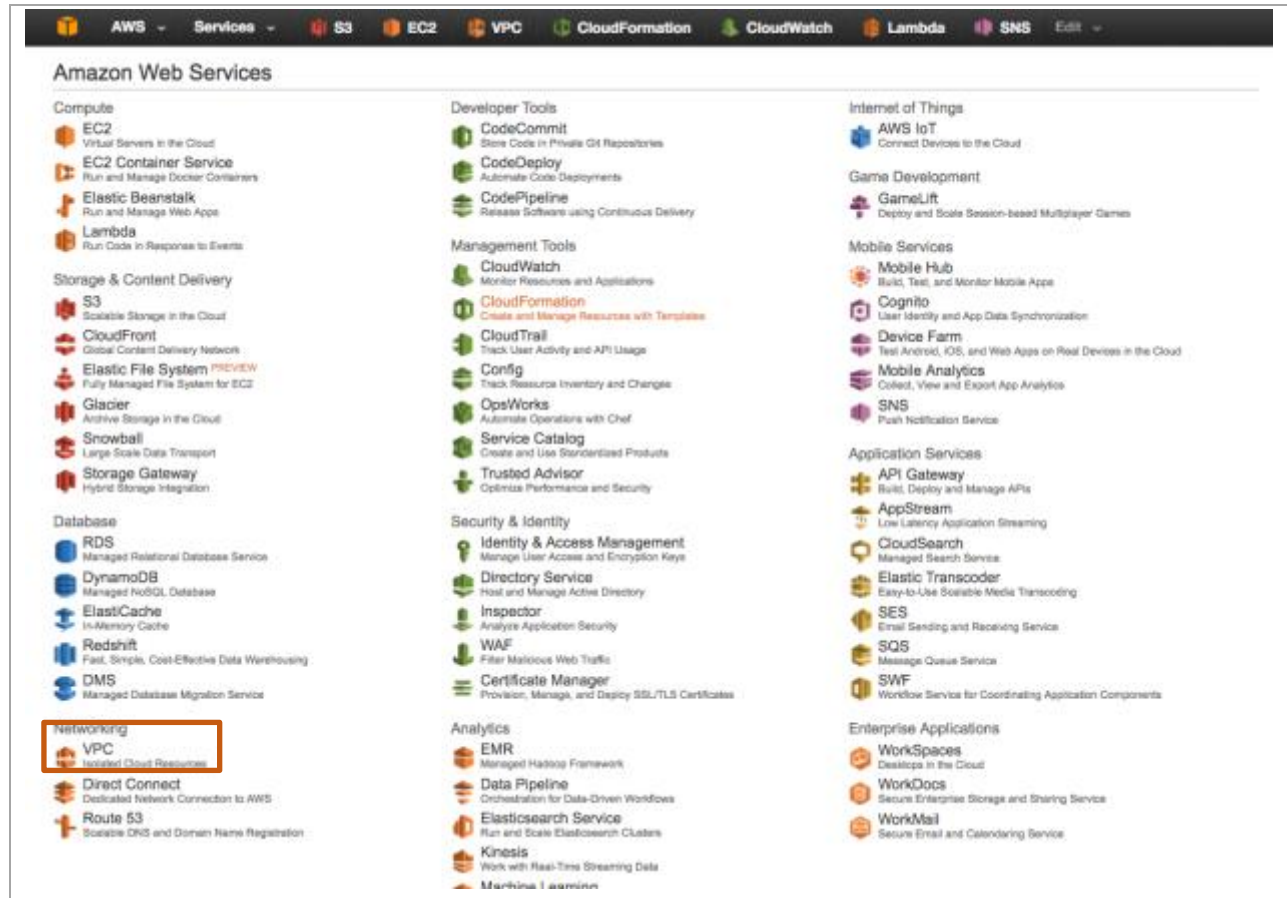


Under **Actions**, click **Delete Stack**:

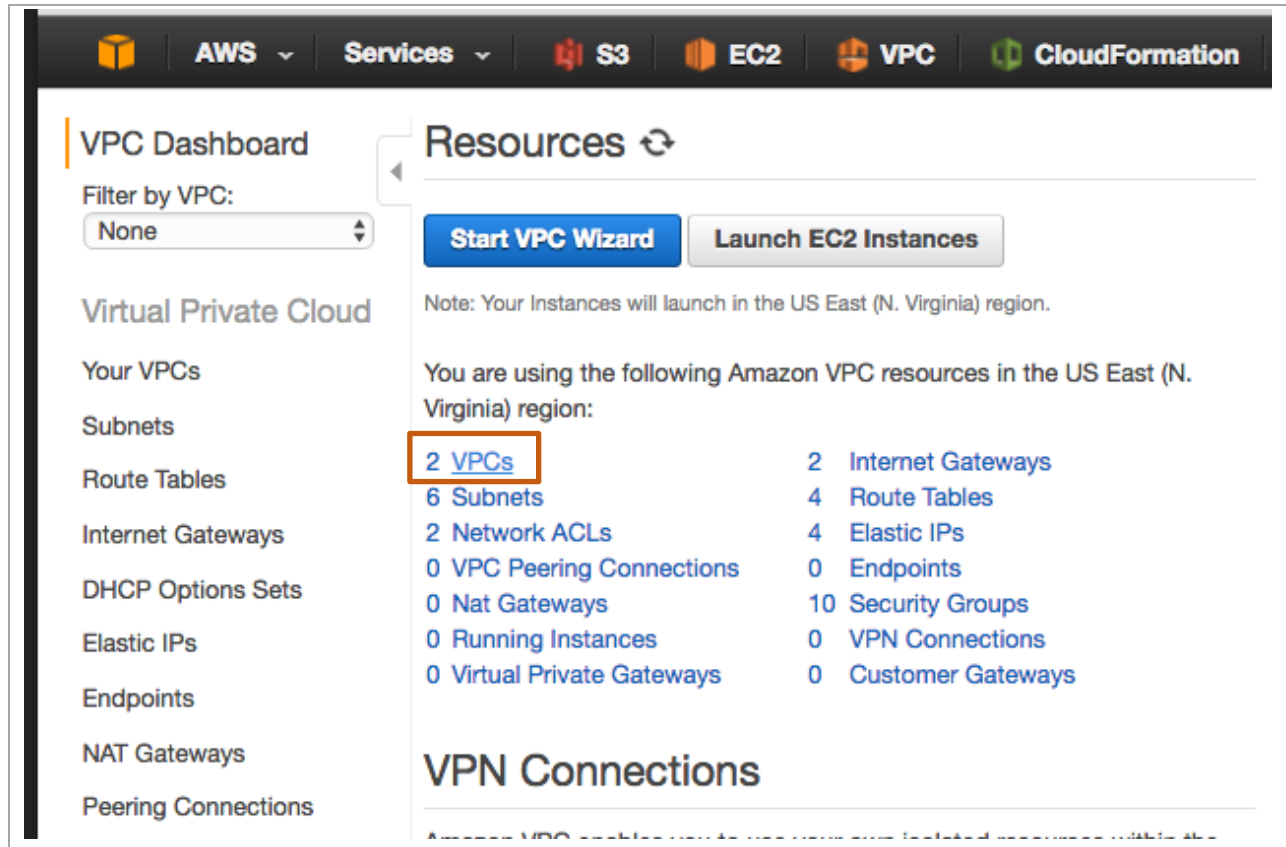


This should delete all the resources created via the template.

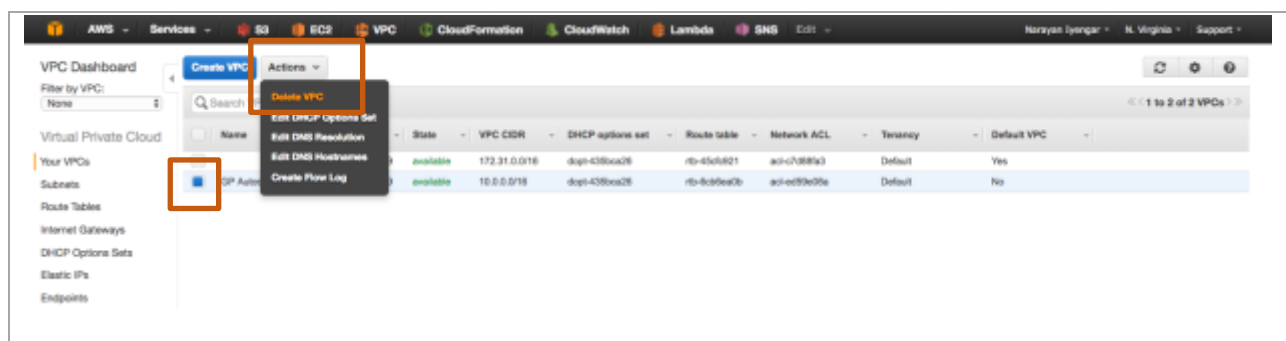
Note: There are cases when deleting a stack fails due to some dependencies that AWS is not able to automatically delete. So, if stack deletion fails, head on over to the VPC console

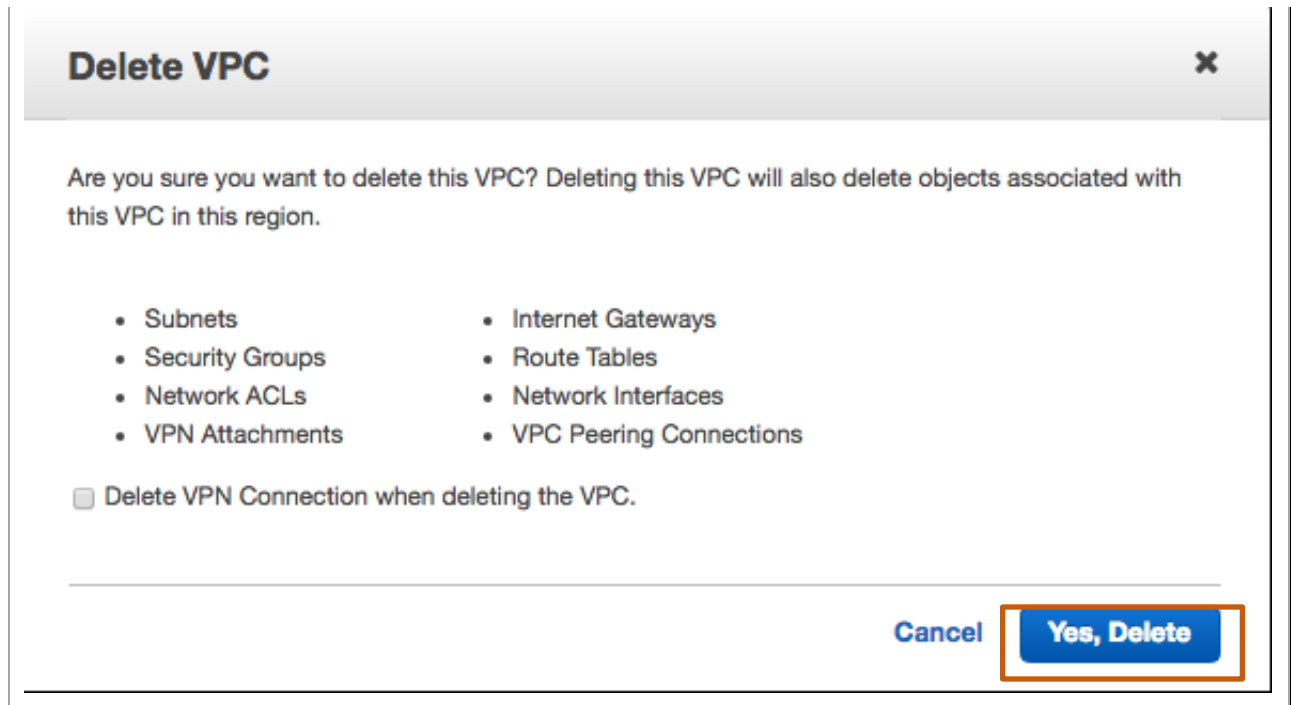


and select **VPCs**



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