VM-Series for AWS

AWS Cloud Formation Template

Deployment Guide

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

http://www.paloaltonetworks.com

Last Update: August 2017

Table of Contents

Version History

Version number	Comments
1.0	Initial GitHub check-in
1.1	Update links in doc to point to GitHub
1.2	Add activities
1.2.1	Updated AWS console, S3 and policy details

1. About CFTs

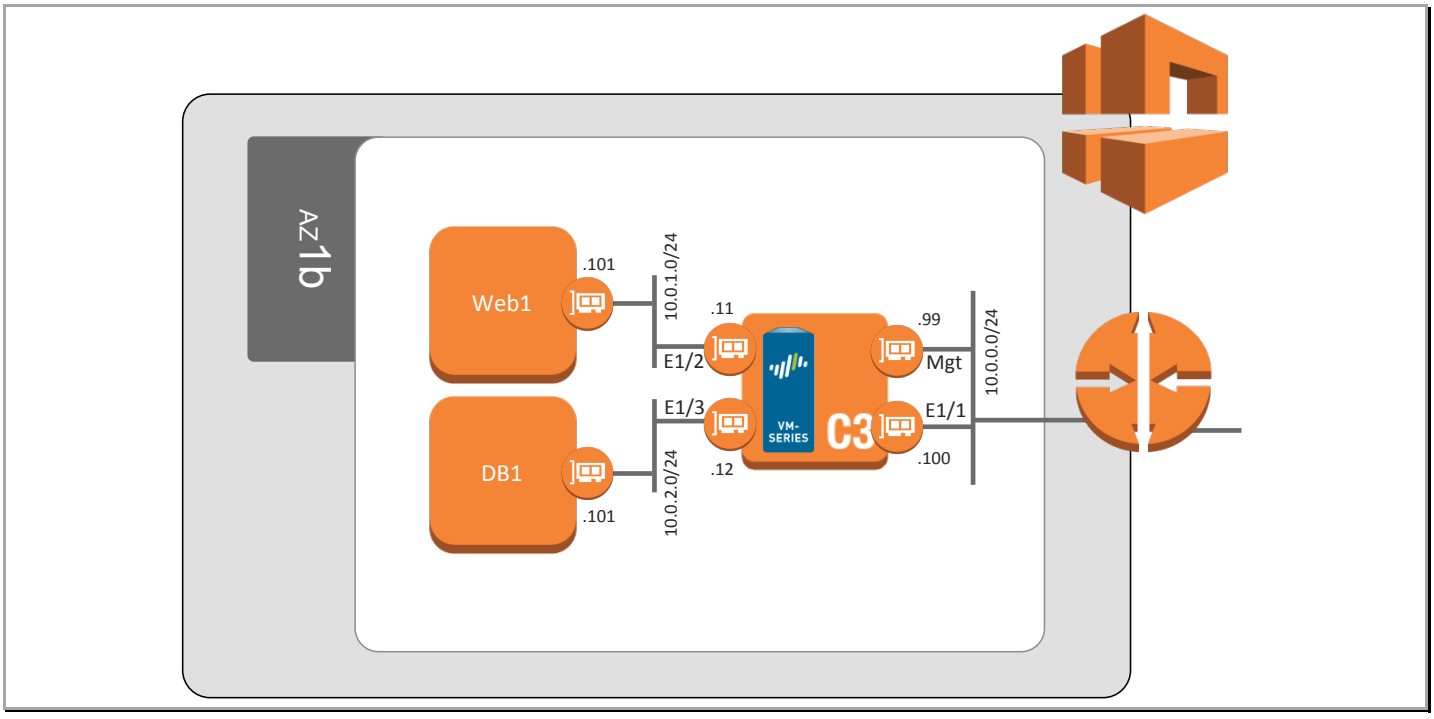
AWS CloudFormation Templates (CFTs), are JSON files that can launch nearly all AWS resources including VPCs, subnets, security groups, route tables, plus many more. AWS CFTs are used for ease of deployment and are key to any auto-scaling environment.

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

This document will explain how to deploy a sample CFT that launches everything that is shown below. This includes, a WordPress server, a MySQL server, a VM-Series firewall and the subnets. In addition, the firewall uses a native bootstrapping feature that allows for additional configuration of the firewall (such as routes, security policies, etc.) Once the sample template has been deployed, the network topology should align with the following:



2. Support Policy

This CFT is released under an as-is, best effort, support policy. These scripts should be seen as community supported and Palo Alto Networks will contribute our expertise as and when possible.

We do not provide technical support or help in using or troubleshooting the components of the project through our normal support options such as Palo Alto Networks support teams, or ASC (Authorized Support Centers) partners and backline support options. The underlying product used (the VM-Series firewall) by the scripts or templates are still supported, but the support is only for the product functionality and not for help in deploying or using the template or script itself.

Unless explicitly tagged, all projects or work posted in our GitHub repository (at https://github.com/PaloAltoNetworks/aws) or sites other than our official Downloads page on https://support.paloaltonetworks.com are provided under the best effort policy.

3. Instances used

When using this sample CFT the following instance types are used:

Instance name	Instance type
WordPress Web Server	t1.micro
WordPress DB Server	t1.micro
VM Series Firewall Bundle 2	c3.xlarge
Security controller	t2.micro

Note: There are costs associated with each instance type launched, please refer to the Amazon EC2 pricing page https://aws.amazon.com/ec2/pricing/

4. Prerequisites

Here are the prerequisites required to successfully launch this template.

4.1 Create an AWS account

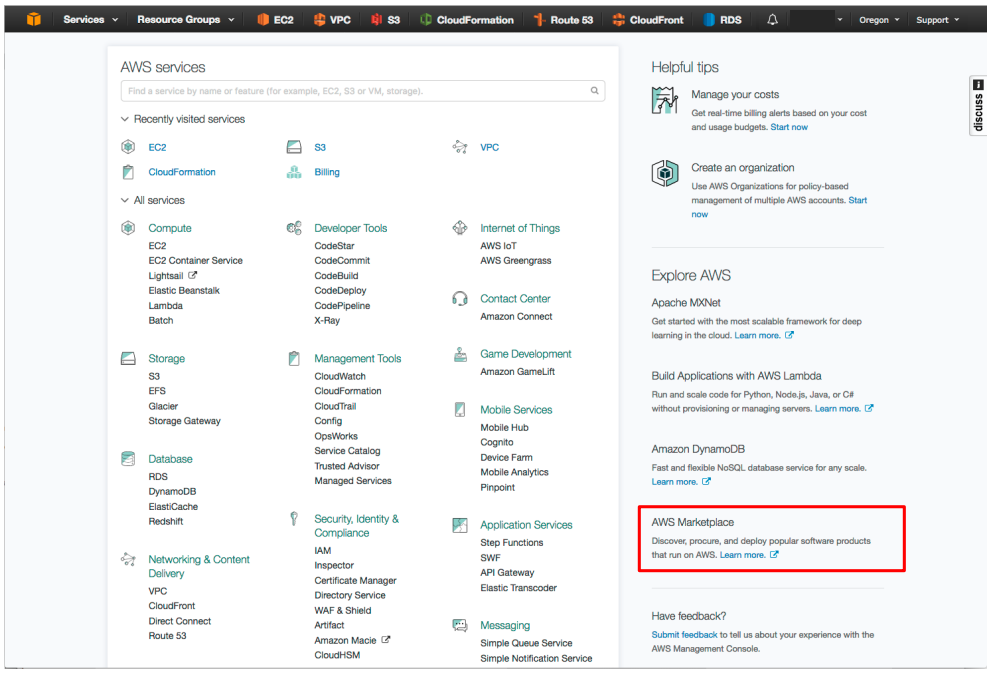
If you do not have an AWS account already, go to https://aws.amazon.com/console/ and create an account. In order to continue you will need to add a method of payment to your AWS account. Use the following https://console.aws.amazon.com/billing/home#/paymentmethods

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

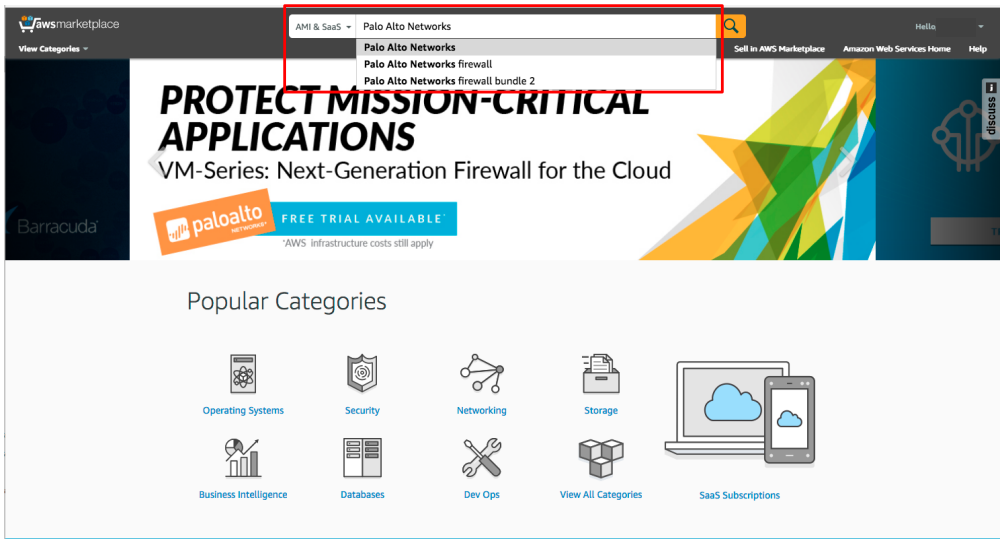
4.2 Review and accept the EULA

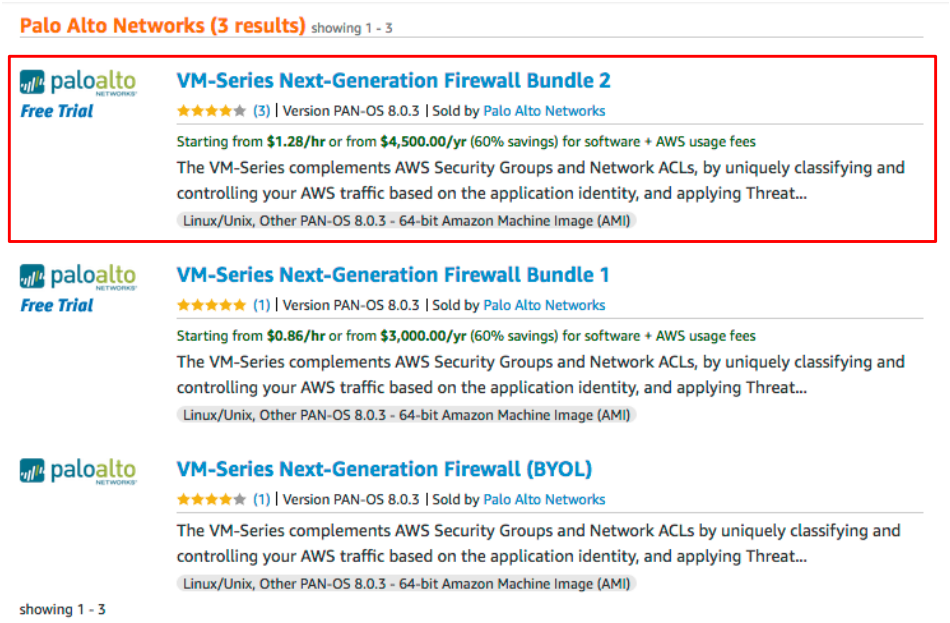
If this is your first time using AWS to launch a VM-Series firewall bundle, you will need to review and accept the software license agreement for the VM-Series.

Click on **AWS Marketplace**.

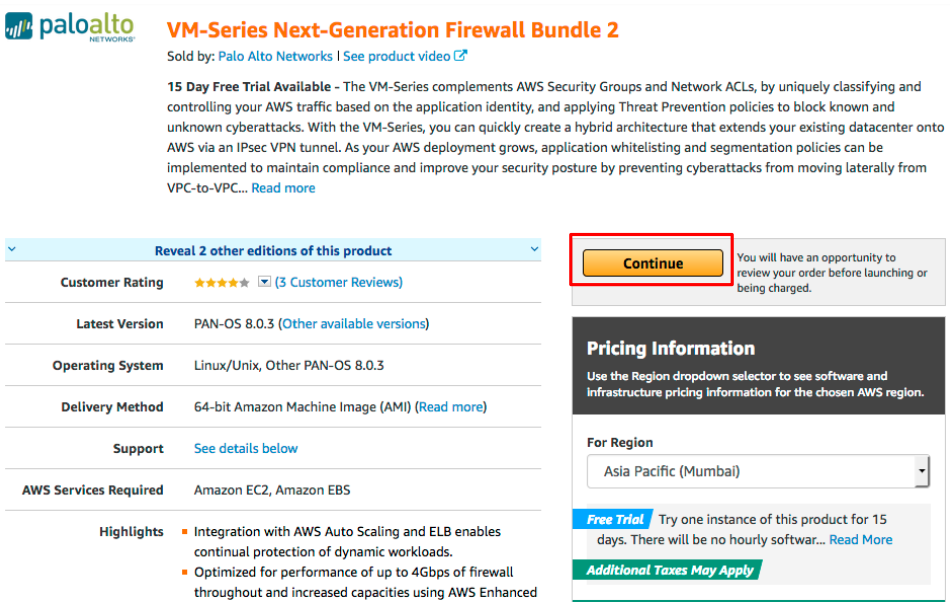


Search for **Palo Alto Networks firewall**



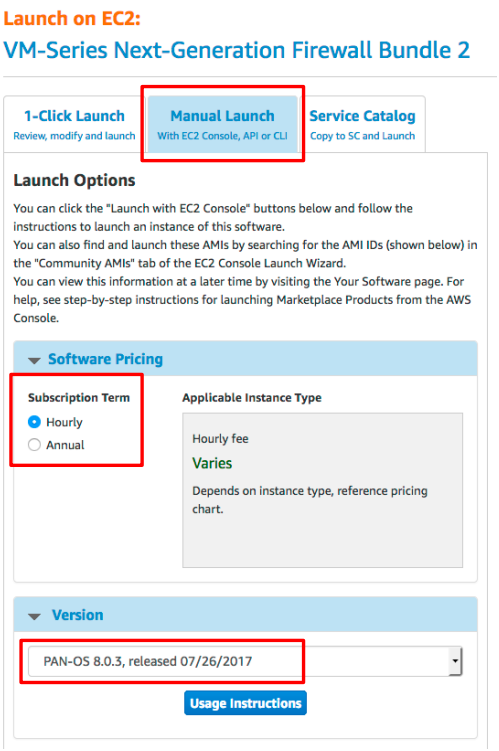


Select **VM-Series Next Generation Firewall Bundle 2**

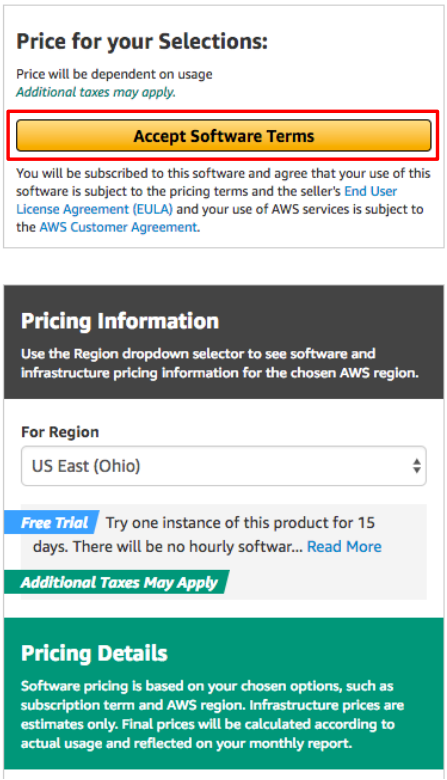


Click **Continue**.

Select Manual Launch, the hourly subscription term and the latest version of PAN-OS.



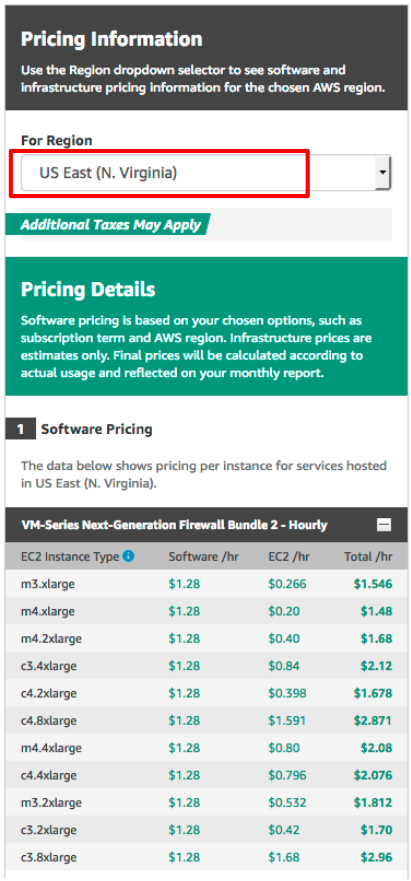
If this is the first time you are accepting software terms, you'll see the following selection on the right hand of the window:



Note: If you had previous accepted the software terms have received the email and are now going through VM-Series selection process again or if you had ran the lab previously and are still within the Trial period, you could go directly to the section 4.3. If you have just finished accepting the software terms, you could continue but check the Trial and Marketplace emails are received.

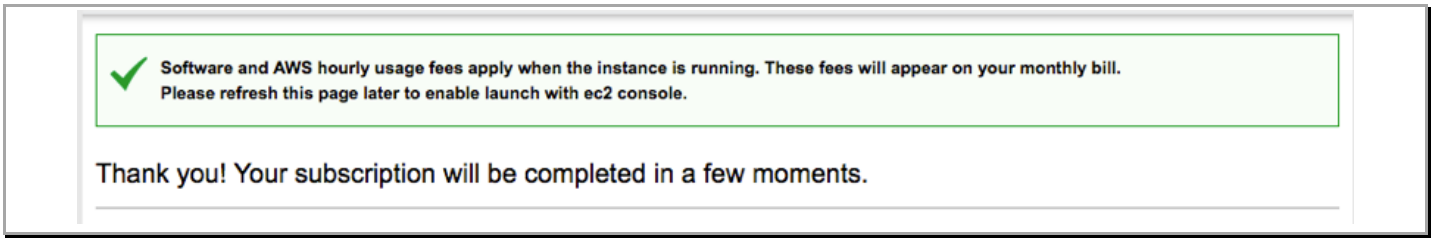
Review the agreement and then click **Accept Software Terms**

If you had previous acknowledged the terms, you will not see the Accept Terms button. Instead you will see the screen below displaying pricing information. This will continue for the duration of the Trial.



Note: the VM-Series instance will be launched through the template later on in the process.

You should see this screen:



You should receive two emails. The first email acknowledging the VM-Series trial and asking you to register it. The second has information on the type of subscription and other pertinent details.

Dear AWS Marketplace Customer,

You have subscribed to the following product in AWS Marketplace:
* VM-Series Next-Generation Firewall Bundle 2 sold by Palo Alto Networks Inc.

You are now able to use this software with AWS. Amazon Machine Image (AMI)-based products can be launched directly from AWS Marketplace, via the AWS Console, or through EC2 APIs. If you have subscribed to a Software as a Service (SaaS) product, you can access it directly from the seller's website or from the Your Software page in AWS Marketplace.

Details needed to launch the software, including AMI IDs, instructions, and recommended security settings can be found by visiting Your Software on AWS Marketplace:
https://aws.amazon.com/marketplace/library/ref=bill_eml_2

Software Pricing and Other Charges

When running this product, you will be charged in accordance with the pricing dimension(s) listed on the detail page. Charges may vary based on your usage or by the size of the instance you choose to run this software on.

In addition to these software fees you are responsible for charges associated with your use of AWS services, including EC2 usage.

You can review pricing for this software here: https://aws.amazon.com/marketplace/pp/ref=bill_eml_2?sku=806j2of0qy5osgjjixq9gqc6g.

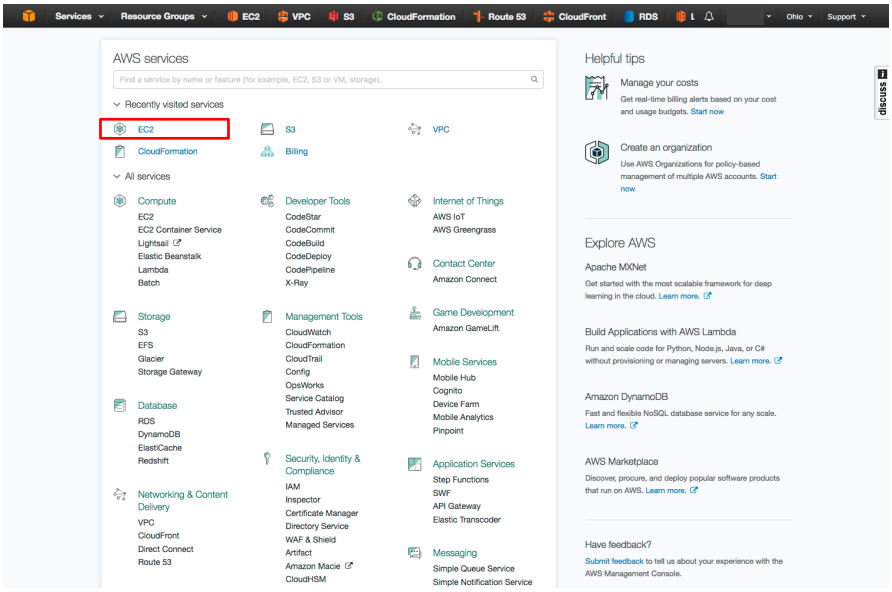
If you have questions, please contact us: https://aws.amazon.com/marketplace/help/contact-us/ref=bill_eml_2

-- The AWS Marketplace Team

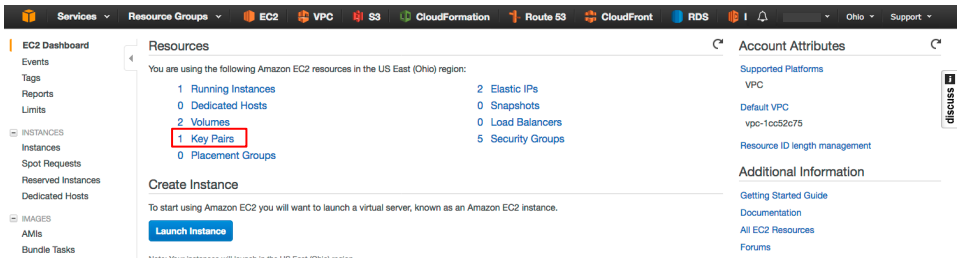
Continue with the next step.

4.3 Create and download an SSH Key Pair

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



Click **Key Pairs**



Click **Create Key Pair**

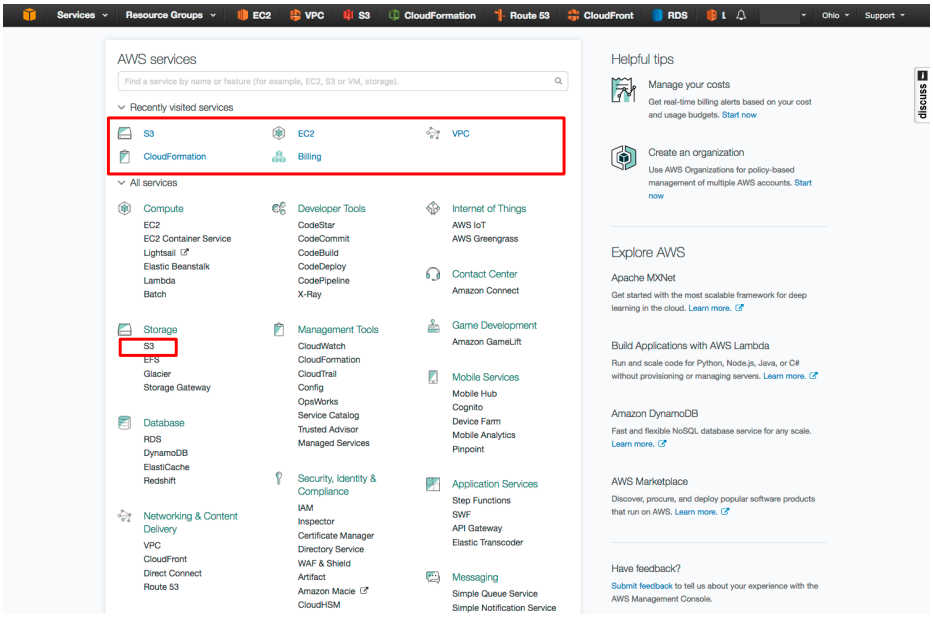
Give it a name.

And click **Create**. When prompted save Key Pair you just created.

4.4 Create a Bootstrap Bucket

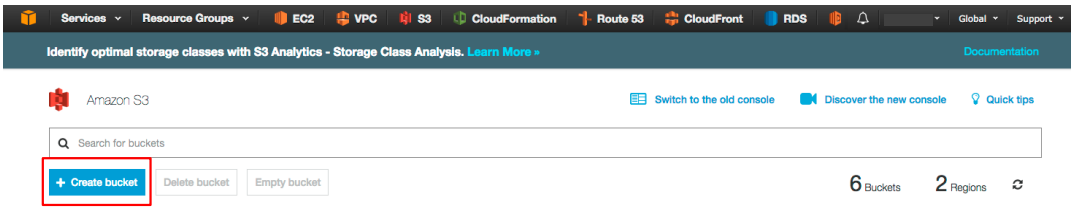
Bootstrapping is a feature of the VM-Series firewall that allows you to load a pre-defined configuration into the firewall during boot-up and to automate its deployment. This ensures that the firewall is configured and ready at initial boot-up, removing the need for manual configuration.

To create a bootstrap bucket, Sign in to the AWS console https://www.amazon.com and click on ***S3***

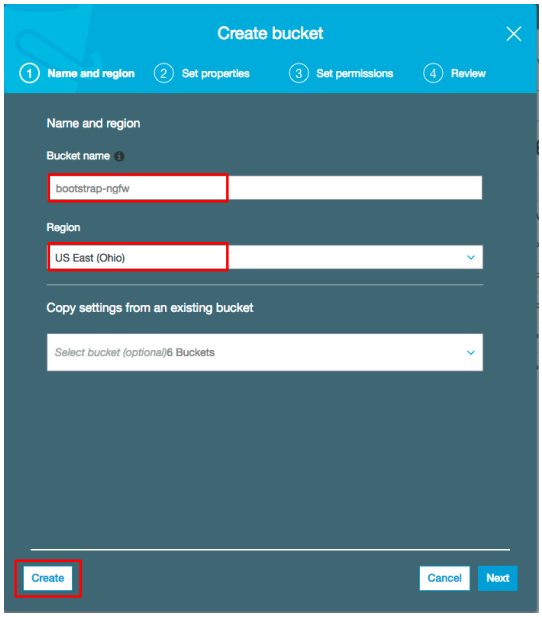


Note: the AWS Console keeps track of the recently visited services as shown in the diagram.

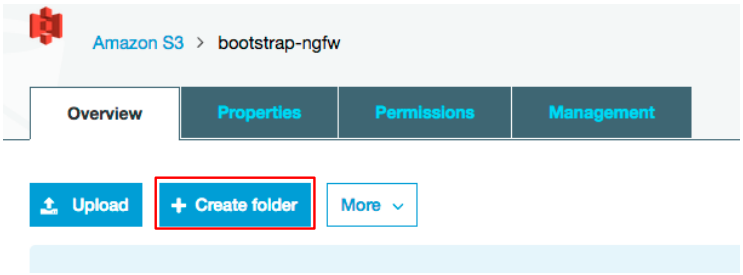
Click ***Create Bucket***:



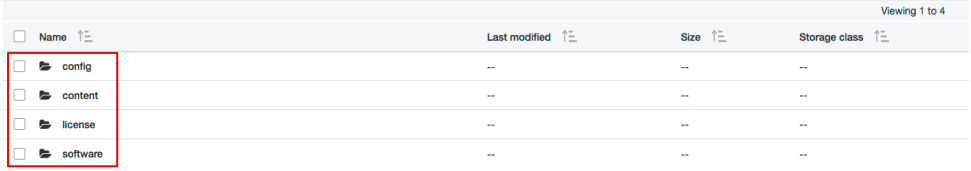
Enter a bucket name and select a region and click **Create** as there is no need to go through the subsequent steps as the default values will be used.



You will need to enter a **globally unique** bucket name. AWS will warn you if the name is not unique. Once the bucket is created, click on the newly created bucket and add four folders called **config, license, software** and **content** by clicking on ***Create Folder***:



Fill in the folder name and click ***Save.*** Repeat the process for the three remaining folders.



Now let's proceed to download the bootstrap files from GitHub.

4.5 Download Bootstrap Files and CFT from GitHub

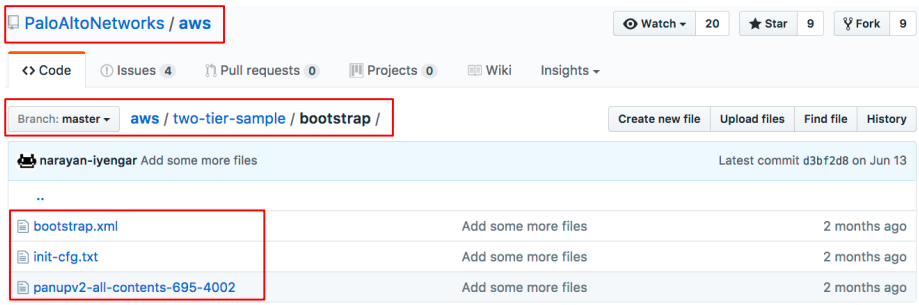
Download the following files and save them in a known location:

https://github.com/PaloAltoNetworks/aws/blob/master/two-tier-sample/bootstrap/bootstrap.xml

https://github.com/PaloAltoNetworks/aws/blob/master/two-tier-sample/bootstrap/init-cfg.txt

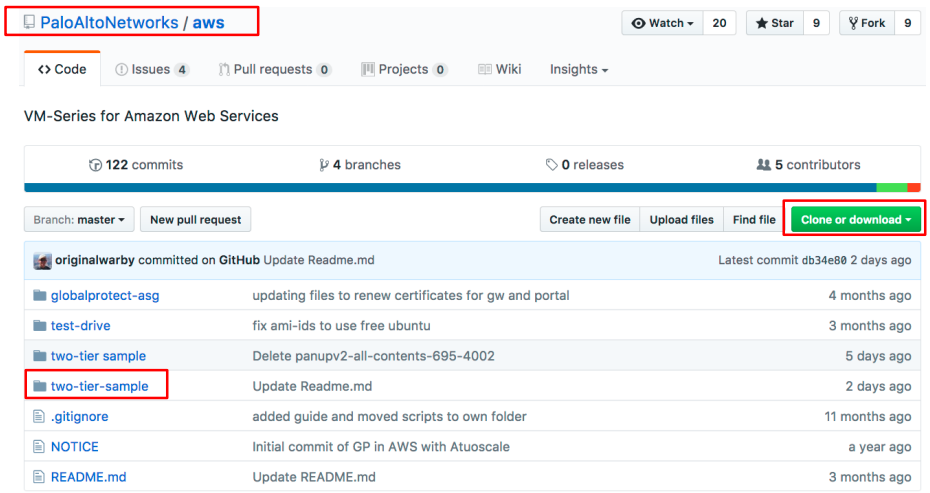
https://github.com/PaloAltoNetworks/aws/blob/master/two-tier-sample/bootstrap/panupv2-all-contents-695-4002

This is the GitHub location where you'll find the files:

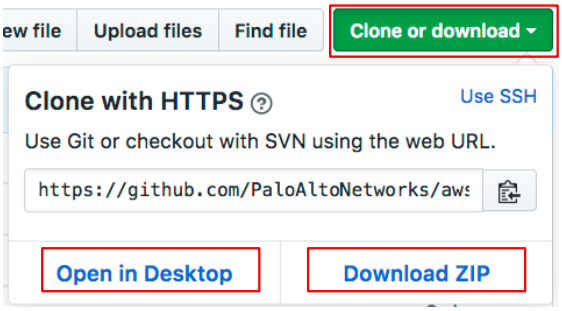


The URL is https://github.com/PaloAltoNetworks/aws/two-tier-sample/bootstrap/

You could either Clone or Download the files from the master branch …/PaloAltoNetworks/aws/

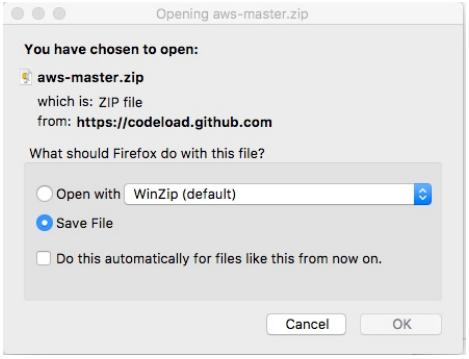


Click on ***Clone or download***:

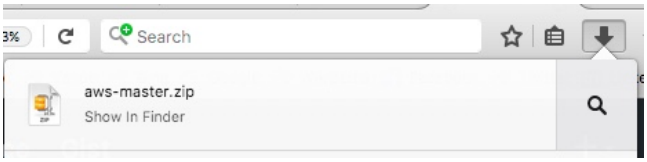


Choose the preferred method. ***Open in Desktop*** requires the GitHub desktop app which is available for Windows and macOS. The ***Download ZIP*** option just requires a app to unpack the zip file and it is the simpler approach to download the files. We'll walk through the two approaches on macOS.

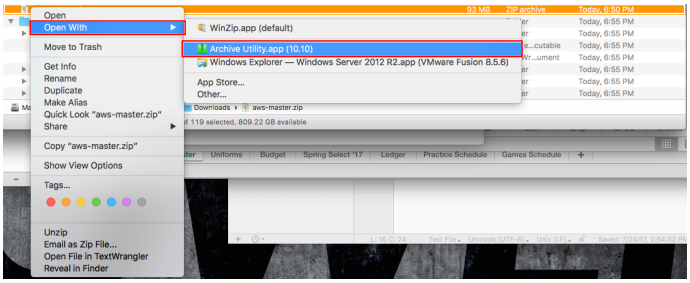
Download ZIP approach: Click on ***Download ZIP*** and select ***Save File***.



Click on the browser's download arrow and show in finder to display the ZIP file.

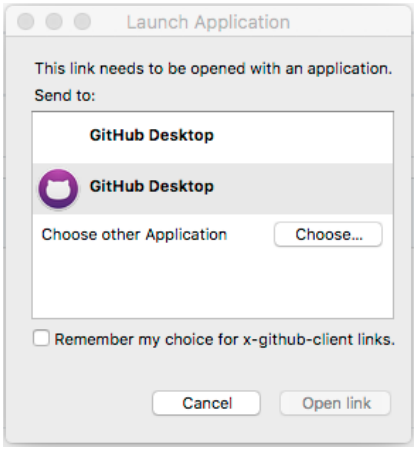


Unpack the aws-master.zip file using whichever utility you happen to use. In our case, we use the Archive Utility app.

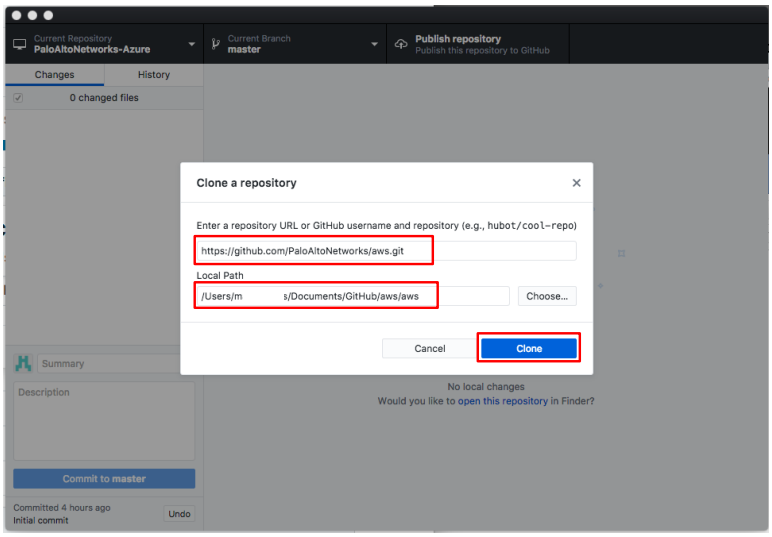


Remember the location of the extracted files and look at the directory structure where the specific files to upload are located at.

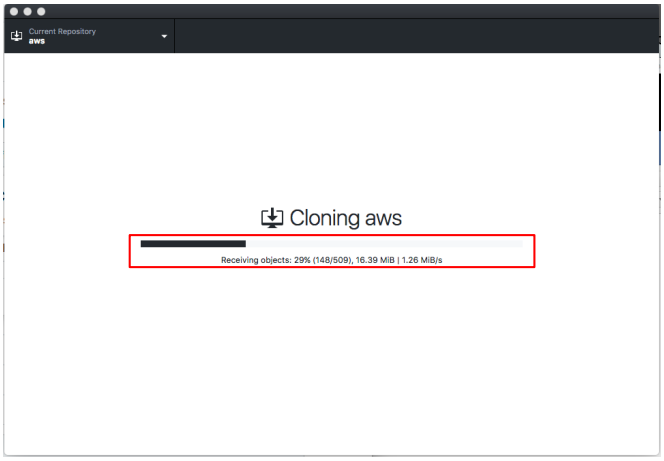
Open in Desktop Approach: Click on ***Open in Desktop*** and select the GitHub Desktop app and click ***Open Link***.



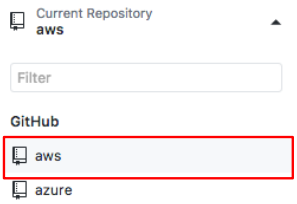
The repository is the master which is automatically filled in. Select the local path you wish to clone it to for future reference. Click on ***Clone***.



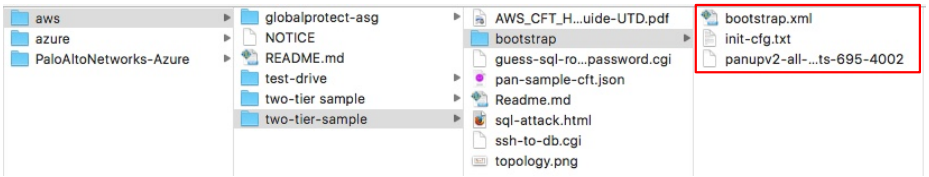
The cloning process takes just a couple of minutes.



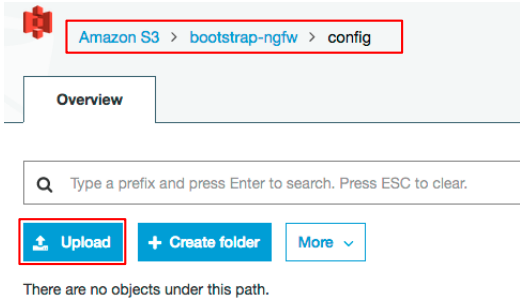
Once it is finished go to Current Repository and you'll see the new one just created.

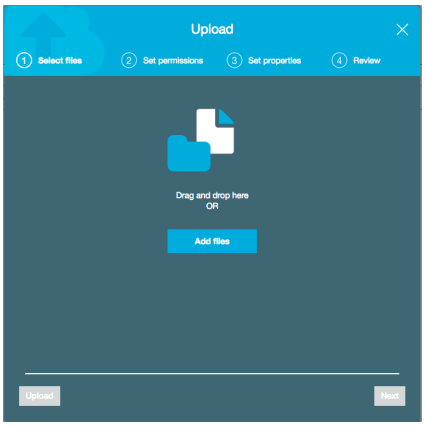


Go the location where the files were cloned to and verify they were copied.

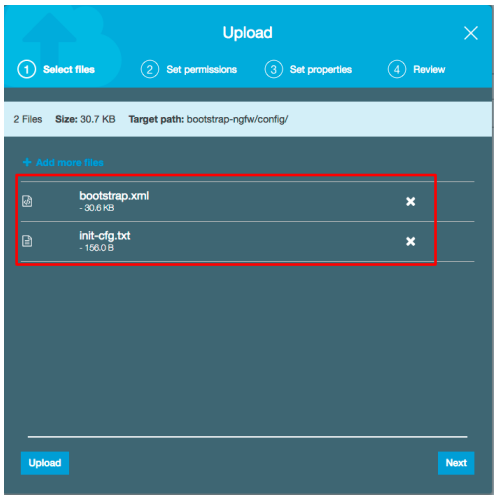


Go back to the AWS S3 console and select the ***config*** folder click ***Upload***:

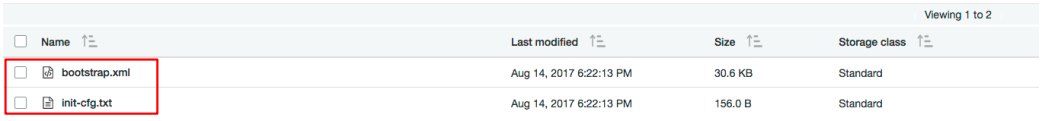




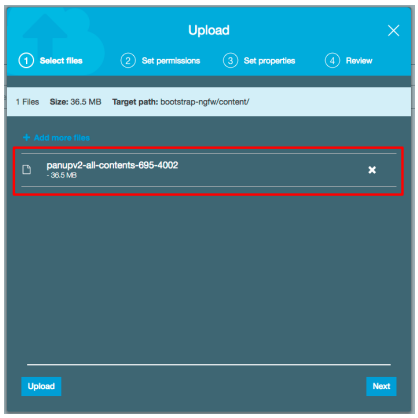
Select ***Add Files*** and select the two files (bootstrap.xml and init-cft.txt) downloaded previously and click ***Upload***:



The two files should be listed under the folder:

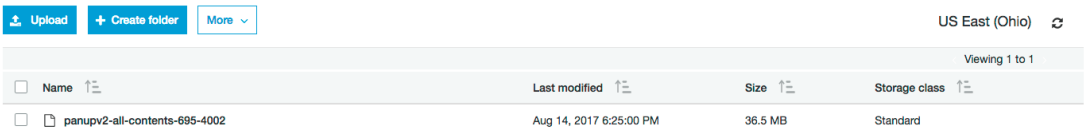


Now click on the **content** folder ins the **S3** console and click ***Upload***. Select ***Add Files*** and select the file (panupv2-all-contents-695-4002) downloaded previously and click ***Upload****:*



The upload takes a few mins. The progress bar show the details current upload.

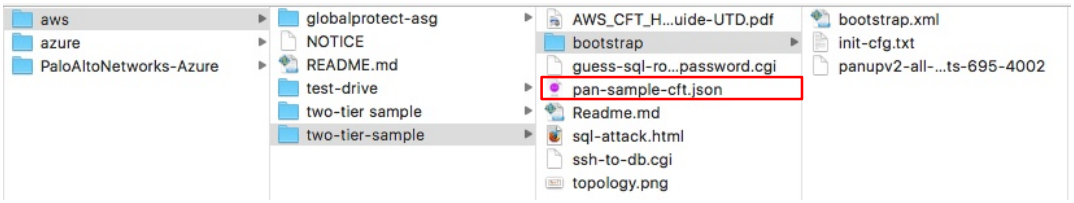
Once completed the file is listed under the folder content.



NOTE: Please create the folders using the console. Creating folders locally on your machine and uploading them may not work as AWS doesn't upload empty folders and the folders are required even when empty**.**

The CloudFormation template – CFT - should have been save when the master was cloned. This is the location:

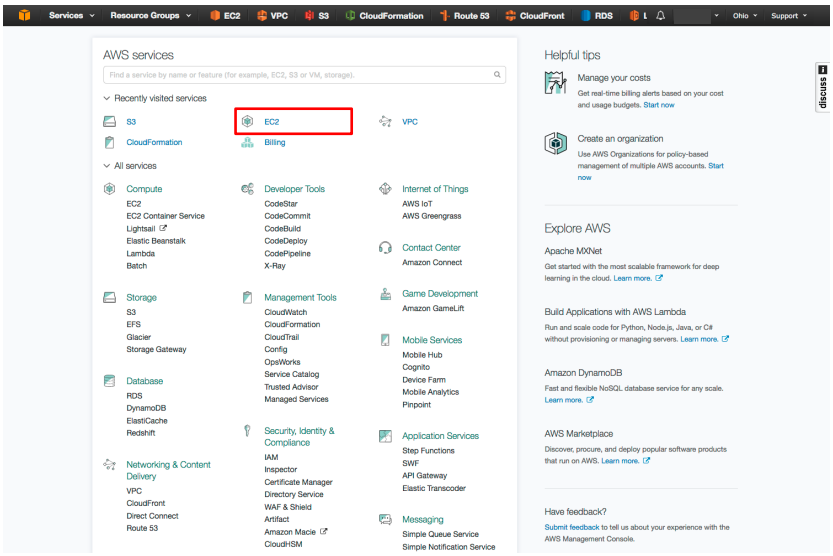
https://github.com/PaloAltoNetworks/aws/blob/master/two-tier-sample/pan-sample-cft.json



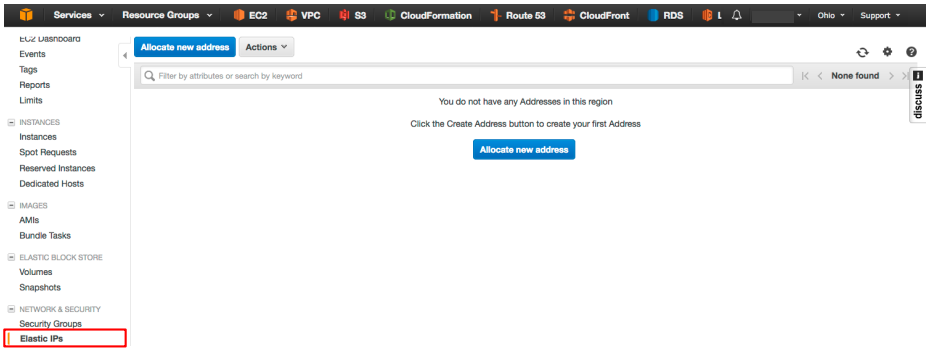
We'll use the CFT once other AWS infrastructure has been created.

4.6 Check Elastic IPs

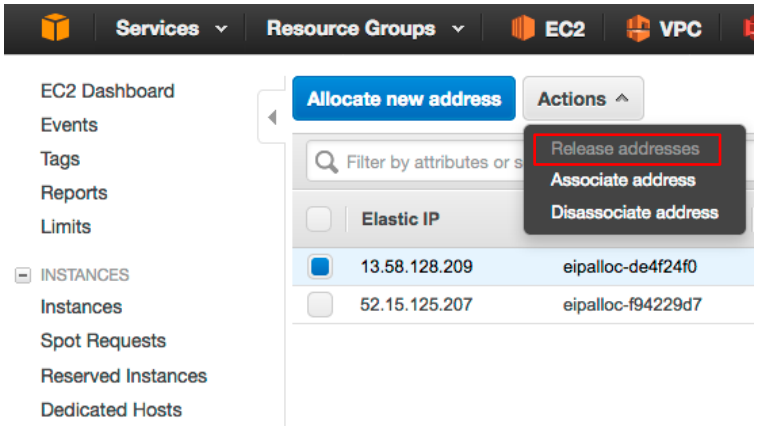
By default, each AWS account has a 5 elastic IP (EIP) limit per region unless a limit increase has been requested (via an AWS support ticket). In order to launch this template, you will need two EIPs. To check any allocated or associated EIPs, on the AWS console click on ***EC2*****:**



And click on Elastic IPs:



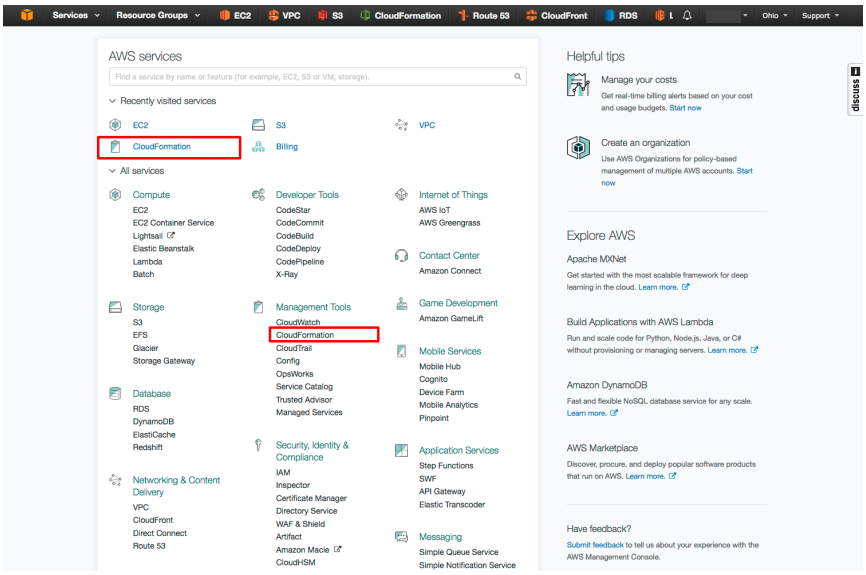
If there are no EIPs allocated, proceed to section 5. If there are more than 3 EIPs allocated and you have not requested an EIP limit increase, the template launch will fail. You can either release an EIP or request a limit increase via an AWS support ticket. In order to release an allocated EIP, simply click on the EIP and click **Actions**, ***Release Addresses***



If the EIP is associated with an instance, you will need to disassociate the address first and then release the address. If you are relying on the address for other work, please be aware that disassociating the address and releasing the address could cause work disruption.

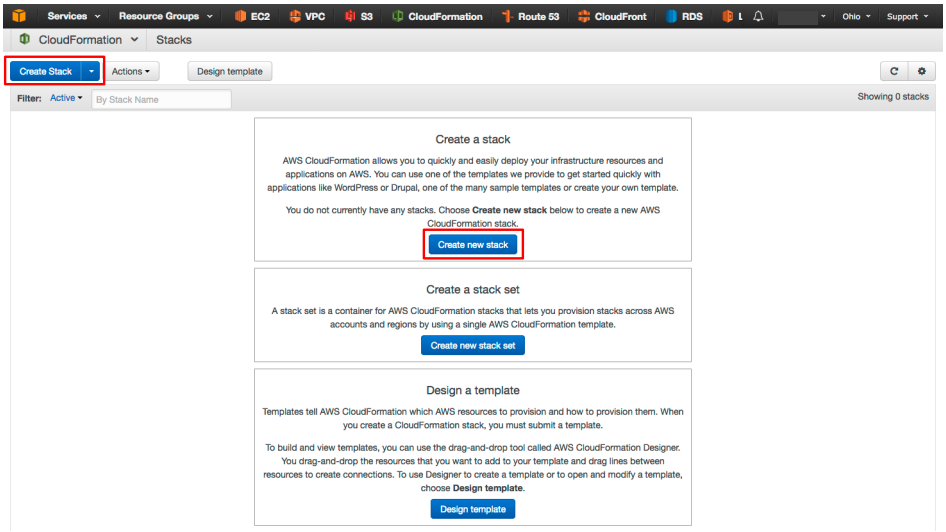
5. Launch the Two-tier CFT

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

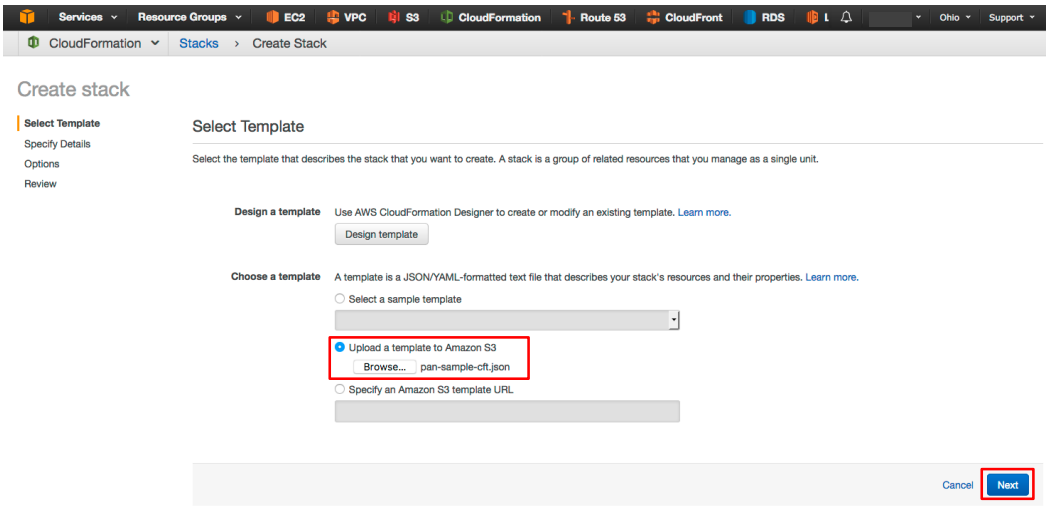


5.1 Create CloudFormation Stack

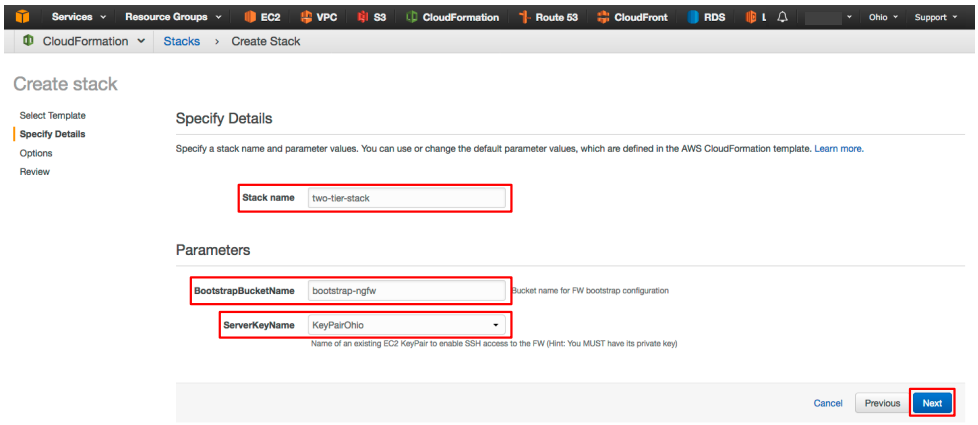
Click ***Create Stack***:



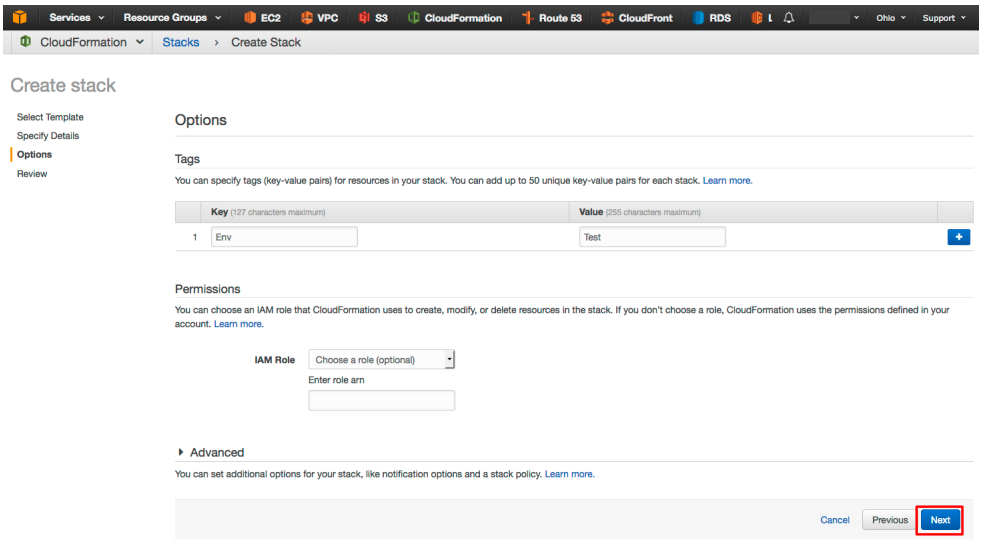
Select ***Browse*** and select the template downloaded in section 4.5 into the box and click **Next**:



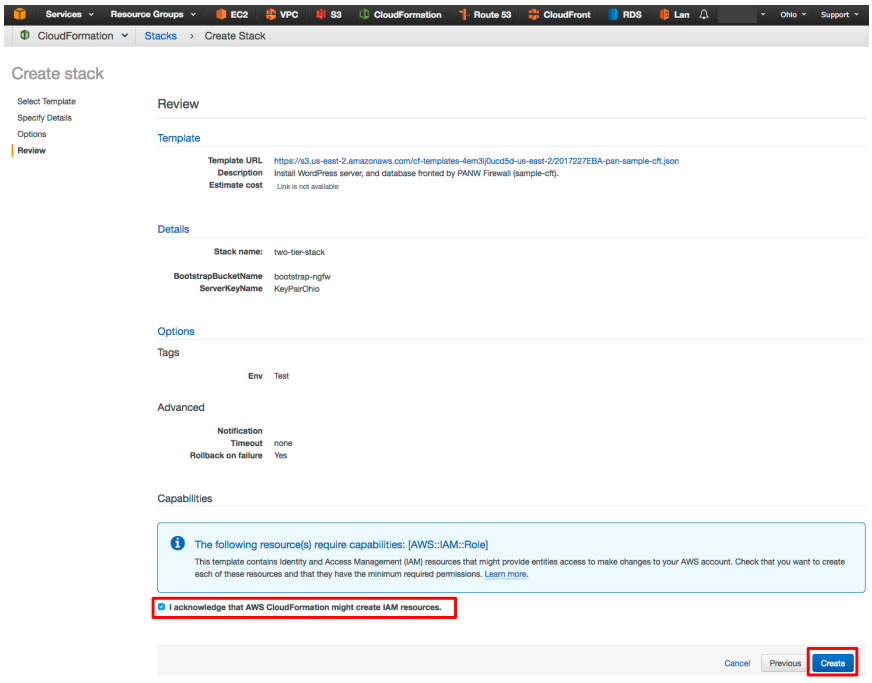
In the next screen specify a "**Stack Name**". This can be anything. In the **Parameters** section, specify the bucket name of the bootstrapping bucket that was created in section 4.4 and select a ***Serverkey*** for which you have the private key. Refer to section 4.3 on how to generate a key pair. Once satisfied, click ***Next***.



On the next screen, you can specify tags (optional) otherwise click ***Next***. You can create Key Value pairs that allow you to filter instances based on those tags. Tags provide a convenient, filtered view of just the instances launched by the template.

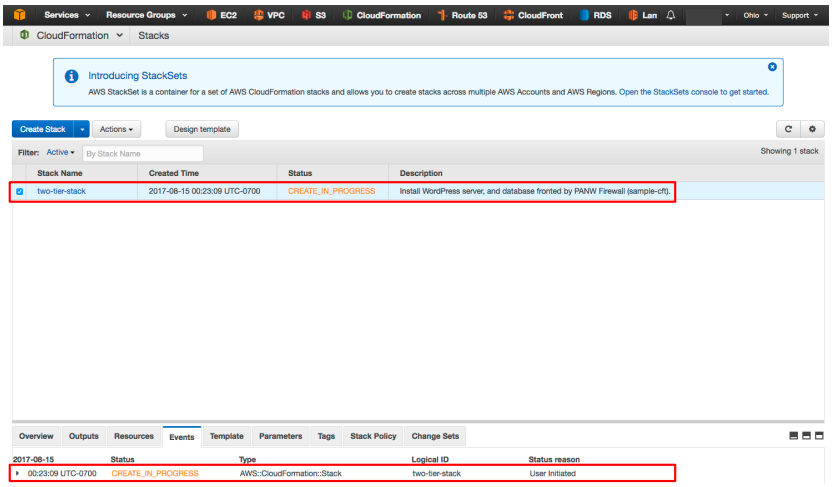


Next, review and check acknowledge at the bottom and click ***Create***.

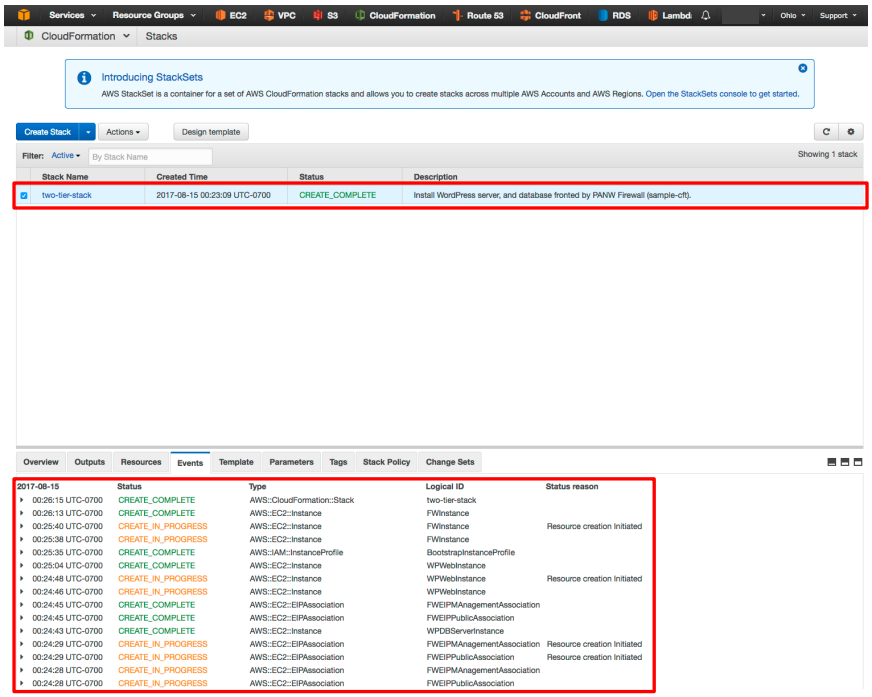


Once launched you should be able to monitor the stack creation progress in the next screen by clicking on the ***Events*** tab.

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

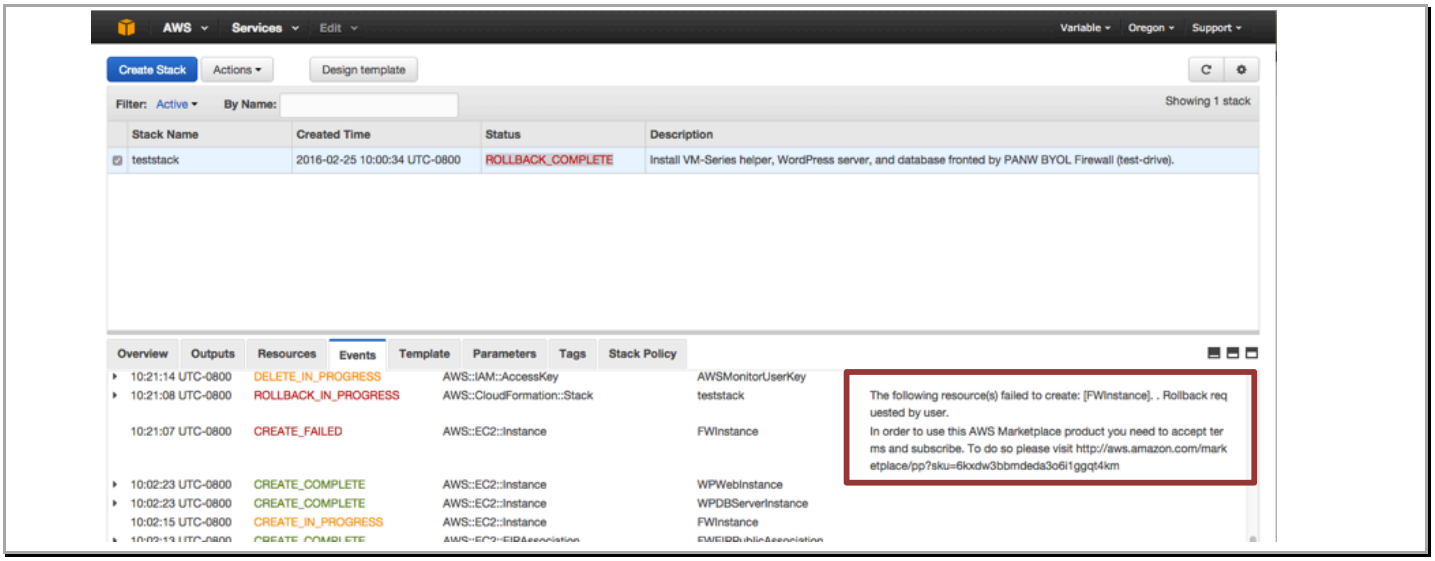


If the CFT was successfully launched, you should see an event as below:



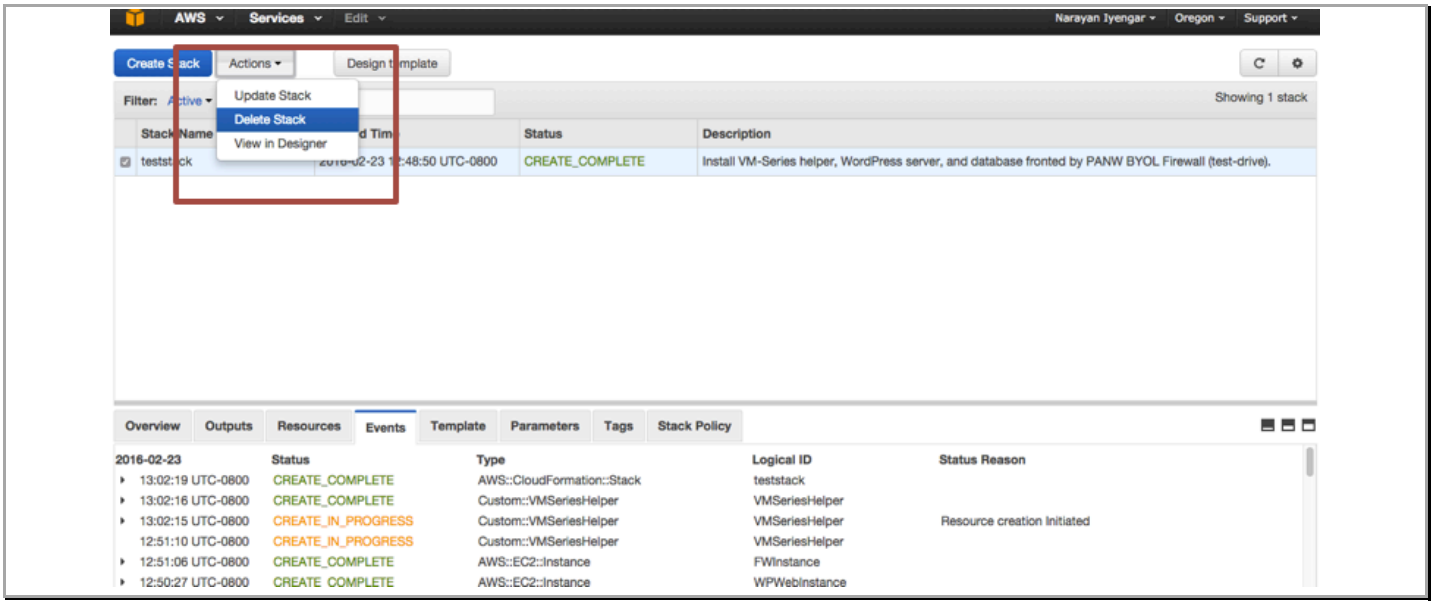
If there were any errors during the creation of the stack, you will need to drill down to the specific event in the ***Events*** tab and ***Outputs*** tab to debug and then create a new stack after fixing any errors.

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



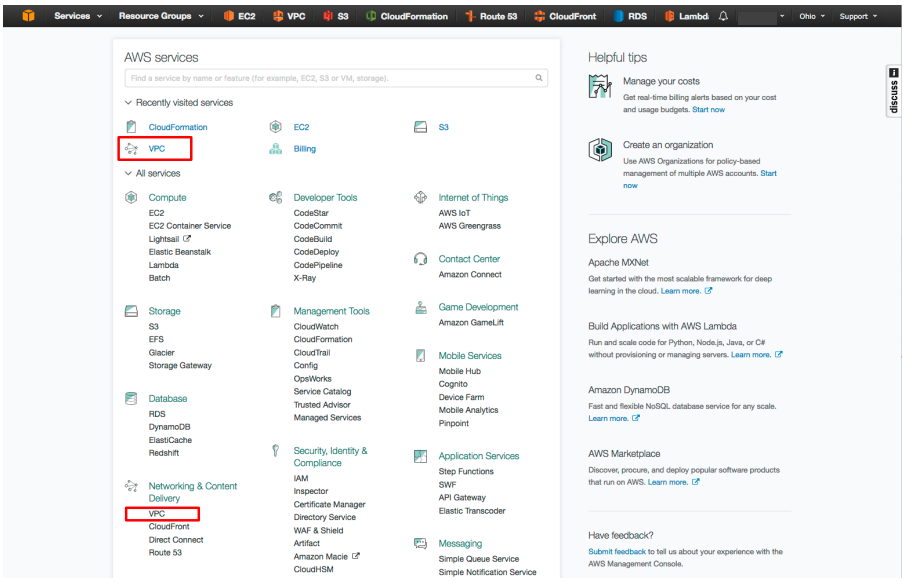
Refer to section 4.2 to review and accept the EULA for the VM-Series NGFW

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

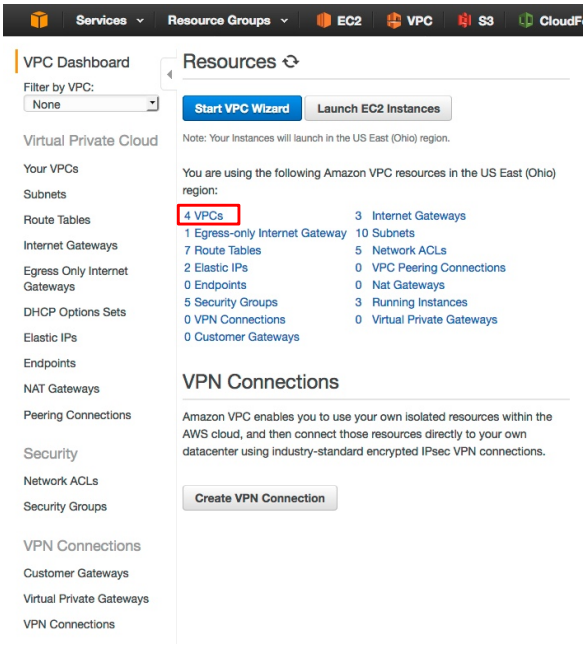


5.2 Review Resources Created by the Template

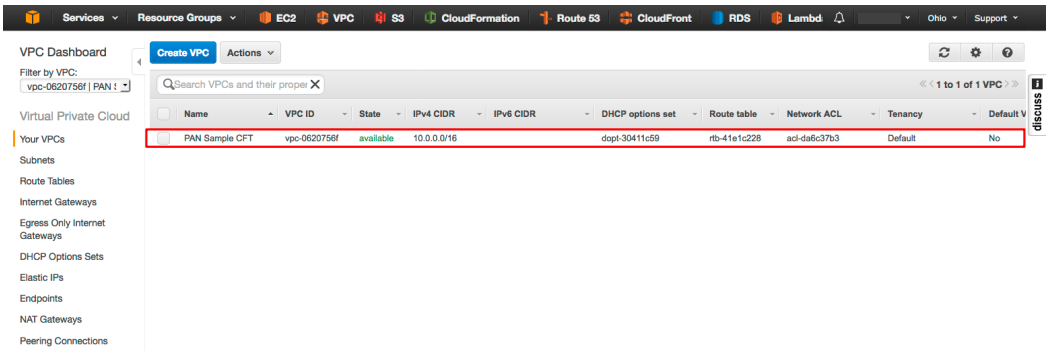
Let's review what the CFT has launched. The newly created VPC can be accessed via:



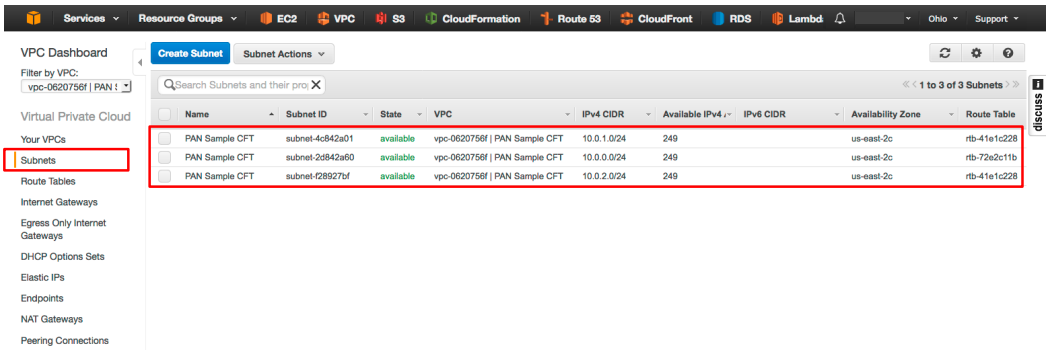
Here you should see all VPCs created in your account:



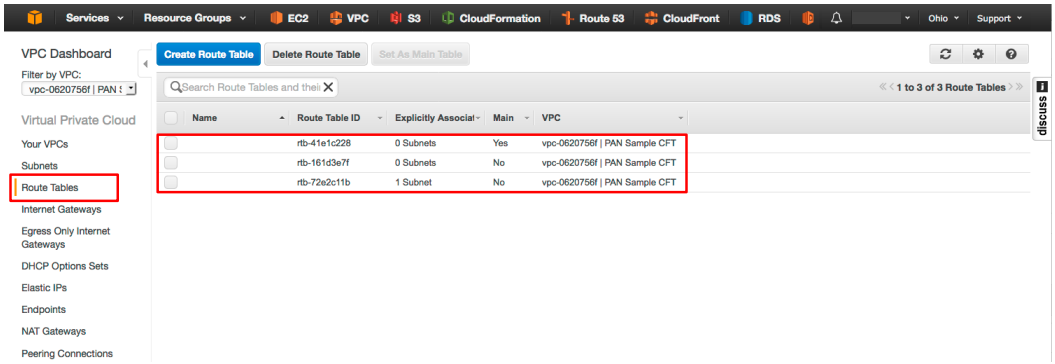
Here is the sample **VPC**:



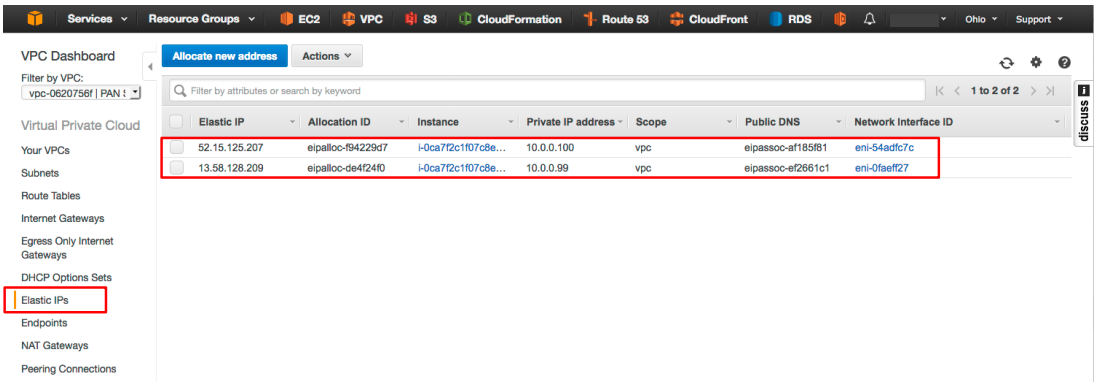
On the left you can review the **subnets associated with the PAN Sample CFT VPC**:



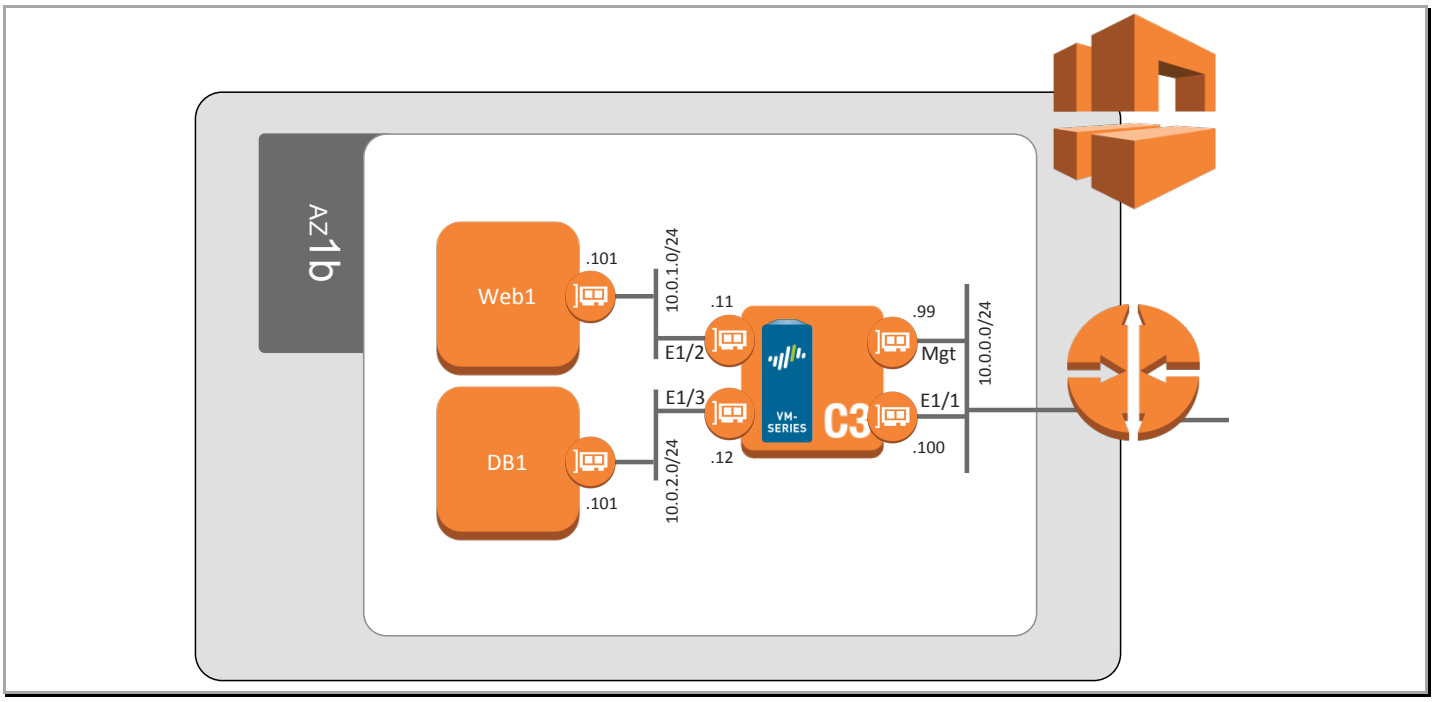
Route tables:



And **Elastic IPs (EIPs)**:



All of this matches the topology shown previously:

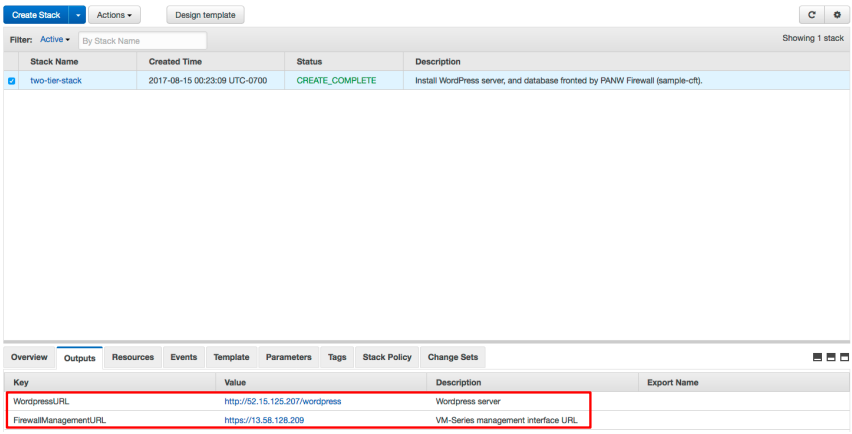


6. VM-Series Access and WebUI Review

Bootstrapping a VM-Series firewall takes approximately 9 minutes. So once the stack has been created successfully, it may be a while before the firewall is up and you are able to log into the firewall.

6.1 Access VM-Series Firewall

Once stack creation is complete, you should see two lines under the **Outputs** tab:



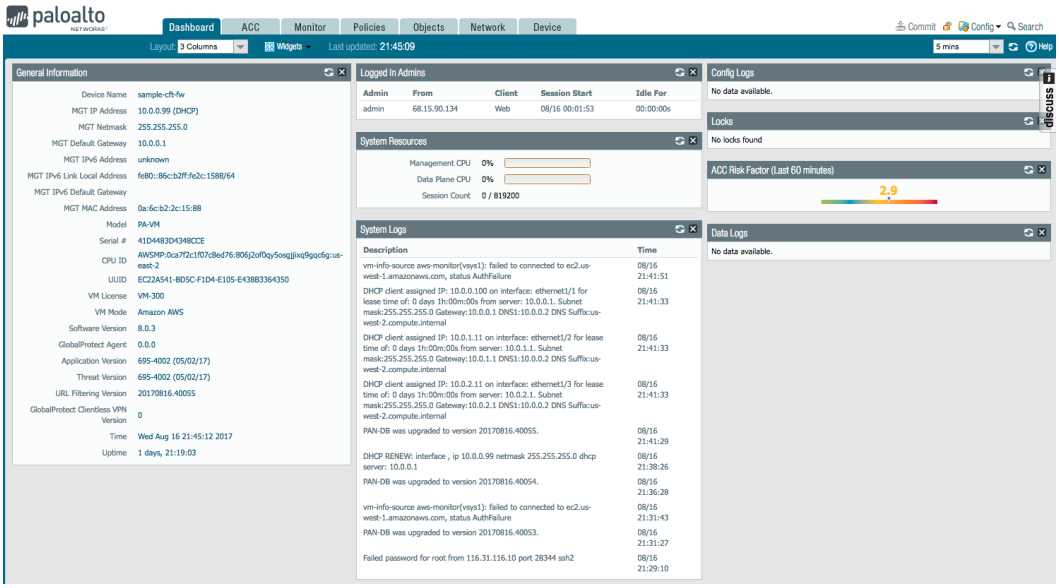
Note: Your setup IP addresses will be different than the ones above for both the Wordpress web server and the VM-Series firewall management interface. Make sure to replace them as needs with your specific IP addresses.

Review the VM-Series Using the browser of your choice, connect to the management interface of the new firewall using the second URL in the previous diagram (https://13.58.128.209/) and login with the username ***admin*** and the password ***paloalto***.

Note: If your browser gives you a certificate warning, you can safely acknowledge it and proceed.

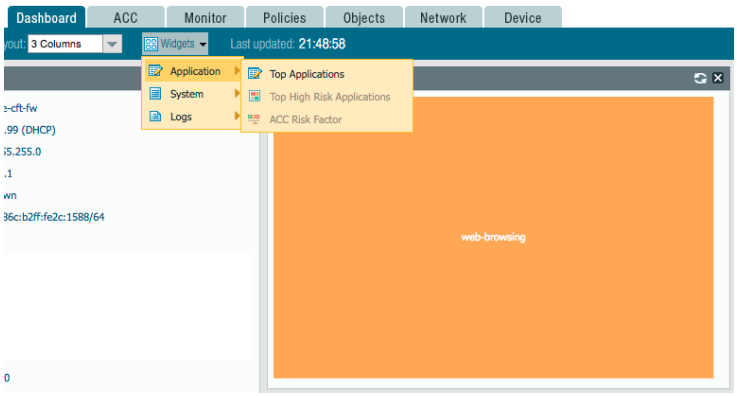
6.2 Login and Dashboard Summary

Upon login, you will see the dashboard for the VM-Series. The dashboard provides a visual summary of the device status. It is widget-based and can be customized to fulfill your specific requirements.



[Optional] Select one of the widgets and move it to a different screen location. Select the widget icon and add an Application, System or Logs widget.

Note: Since this firewall is brand new, it likely doesn't have any traffic yet and your screen won't match the screenshot below. You can return to the dashboard at the end of the lab to see real data.



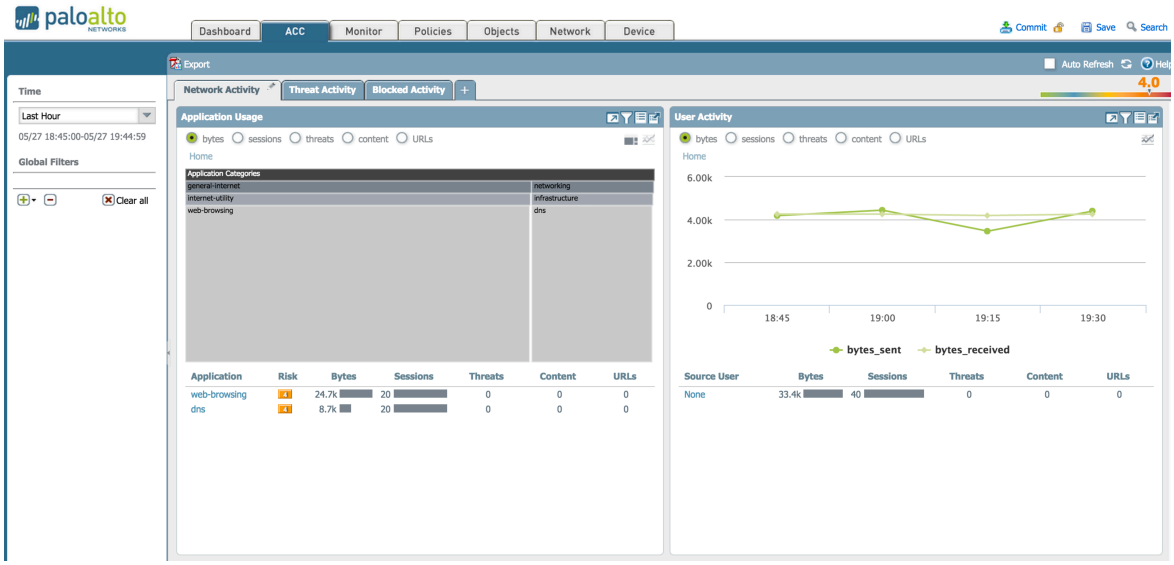
6.3 Review Application Command Center (ACC)

The ACC provides you with a widget-based summary of the applications, the content within, and who the user is over a given time period [default is 1 hour]. With the ACC, you can see the

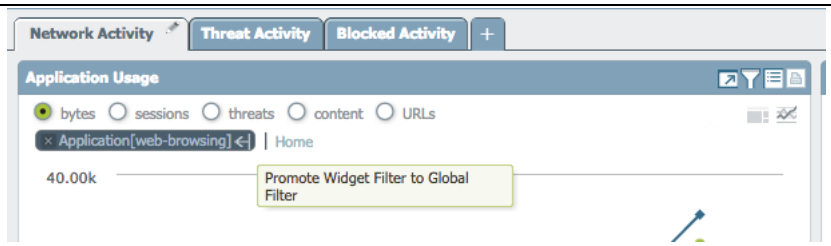
contextual linkage between the application and the content, which allows you to make more informed security decisions.

Select the ***ACC*** Tab.

The default ACC view will show you the network, threat and blocked activity in 3 separate tabs for the past hour. As shown in the image below, the time frame and each tab can be customized to display the relevant application, threat, and user activity depending upon the user role. Additional tabs can be added via the + sign on the right side of the Blocked Activity tab.



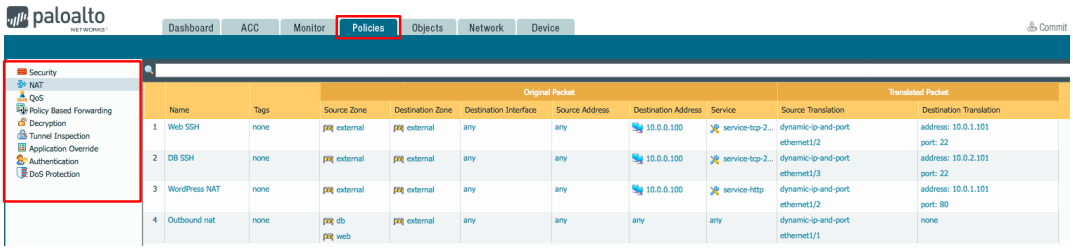
Within each of the widgets, you can select the relevant data point to learn more about what it is and what it means, and you can “Promote” that data point as a filter by clicking on the arrow to the right of the filter, which in turn will force all other widgets to be updated based on that context. Because you are viewing a brand new firewall, there won’t be much data in this view yet.



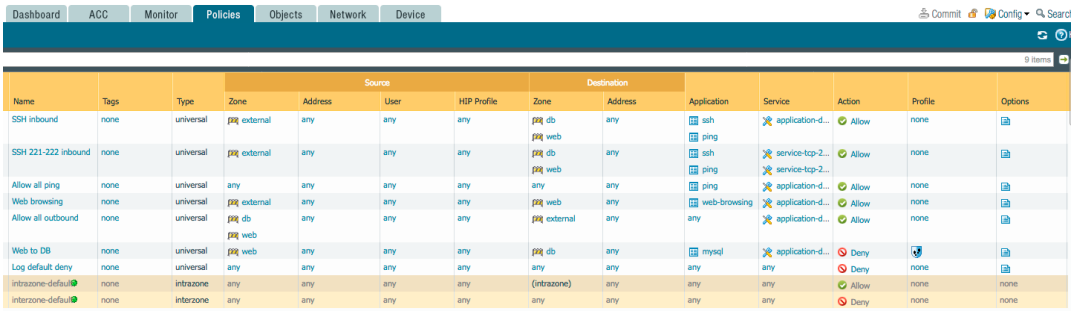
[Optional] Scroll through the information displayed in the ***Network Activity*** Tab. Customize one of the tabs, create/add a new tab.

6.4 Review Security Policies

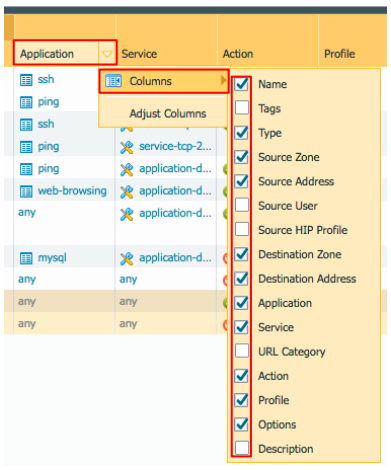
The Policies tab is a where you will define all of your policies. The default view will be your security policies, all of which can be based on the application, the content within, and the user. As shown along the left side of the image, additional policies can be defined for actions such as NAT, Decryption, and DoS.



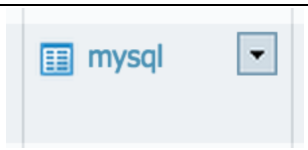
Select the ***Policies*** tab and select the Security option on the left panel.



You can change the columns displayed by placing the cursor on any column, clicking the down arrow and then the side arrow to select the columns to display or not display.

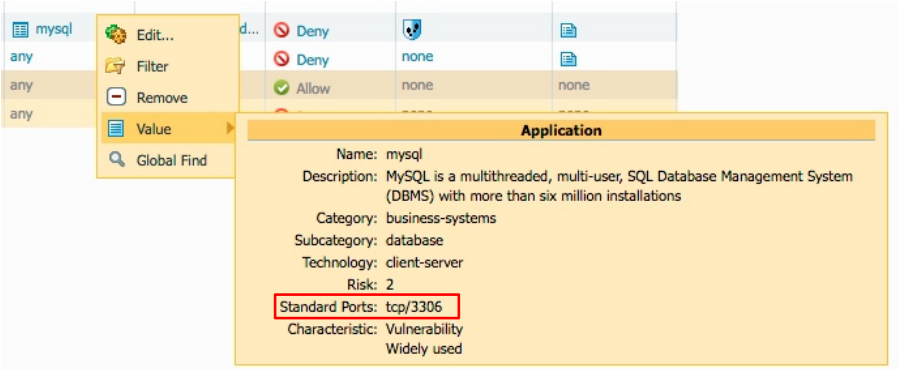


Step 1: In the ***Web to DB*** rule (rule 6) and under the ***Application*** column, click on the small arrow next to ***mysql***.



Then click on ***value*** to see the details for the mysql AppID. You will see details about the application including the standard ports.

Note: The VM-Series is a next generation firewall. It does not simply assume all traffic on TCP port 3306 is MySQL. It inspects the traffic and ensures that it truly is MySQL.



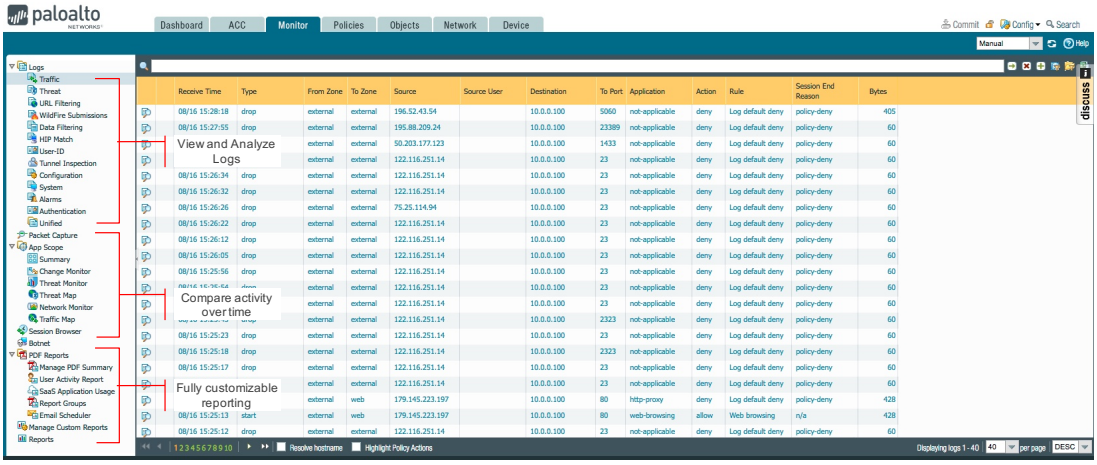
6.5 Review The Monitor Tab

The Monitor tab is where you can perform log analysis and generate reports on all of the traffic flowing through the VM-Series. Logs are stored on box and can also be forwarded to either Panorama, our centralized management solution, or forwarded to a syslog server for analysis and reporting by 3rd party offerings.

Click on the Monitor tab.

[Optional] Navigate through the various log viewers, click Reports to see the various pre-defined reports you can use.

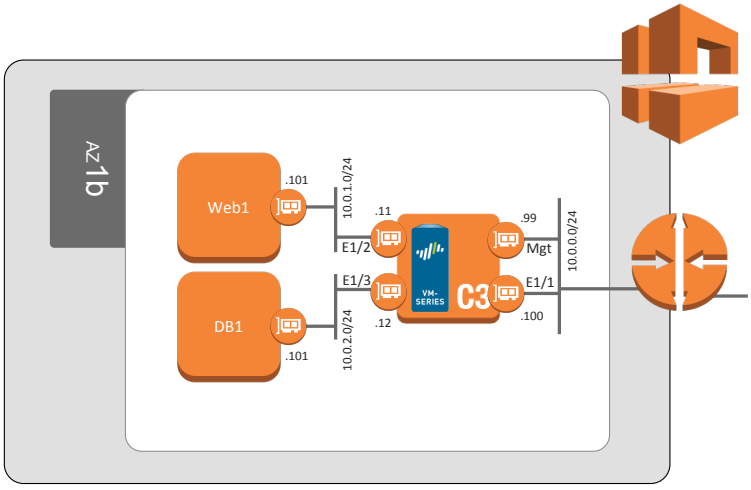
Note: Your firewall is new and doesn't have any data yet so any reports you create at this point will likely be blank. You can return to this step at the end of the lab and create new reports.



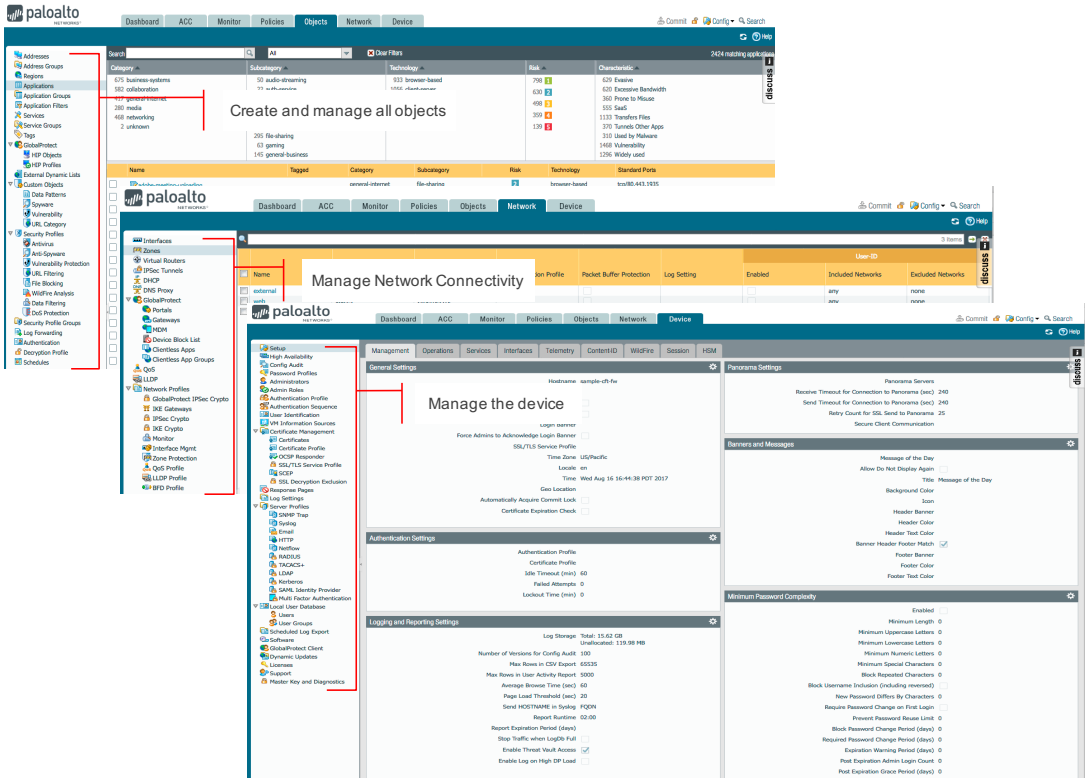
6.6 Review Object, Network and Device Tabs

The Objects, Network, and Device tabs provide you with the various management capabilities. The Objects tab allows you to manage the building blocks for creating policies such as address objects, custom applications, and security profiles. The network tab allows you to create and manage interfaces, security zones, VLANs and other elements that enable connectivity. The device tab allows you to manage high availability, users, software and content updates.

Click the network tab. The network configuration items should align with the following topology:



Click the Device tab. This is where configuration items like DNS, service routes are managed.



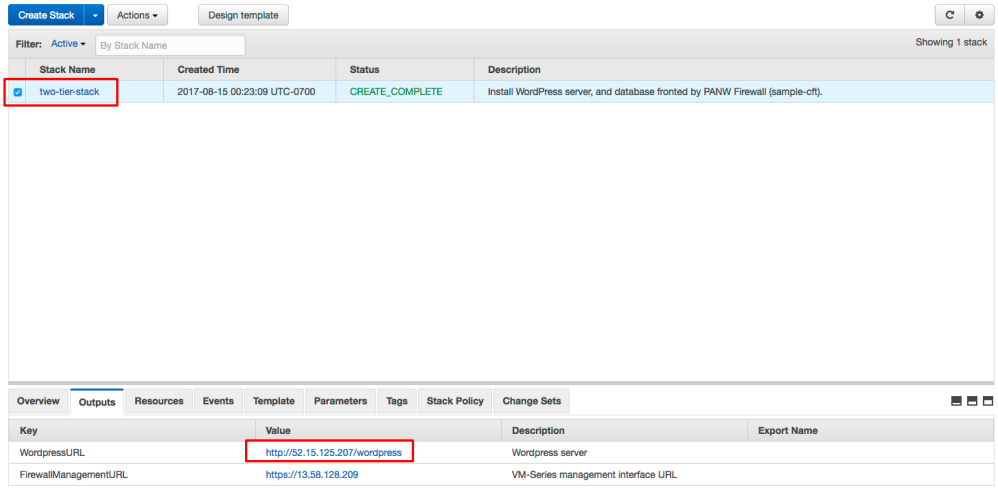
7. Securing Applications

In this activity, you will:

- Generate traffic on the firewall and review the traffic log
- Edit the security policy to allow inter-tier application traffic

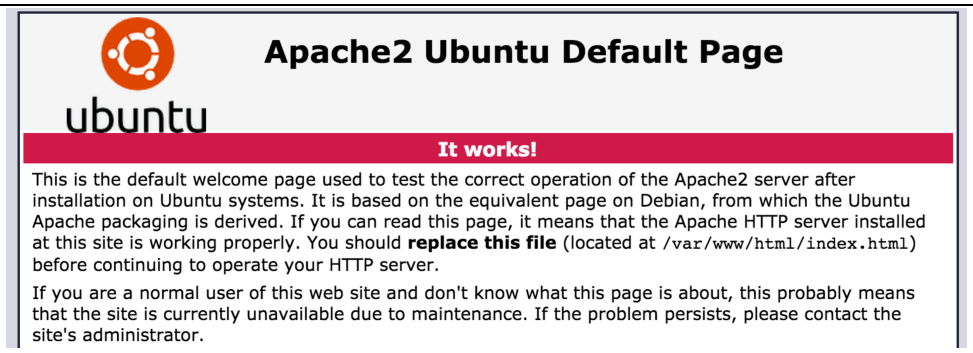
7.1 Verify Static Content on Web Server

Using the first URL seen in the AWS console CloudFormation view when selecting the newly created stack Outputs view.

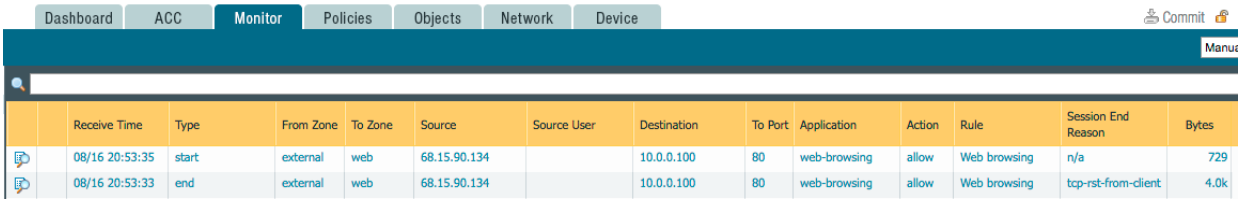


Open a browser tab and browse to the URL http://<<Web Server IP>>/ - based on our stack the URL is http://52.15.125.207/

Note: The URL includes ***/wordpress***, remove the ***wordpress*** portion for this step. Also remember to replace the URL IP addresses with your lab's IPs.



Return to the firewall ***Monitor*** tab and note the traffic log for your web browsing.



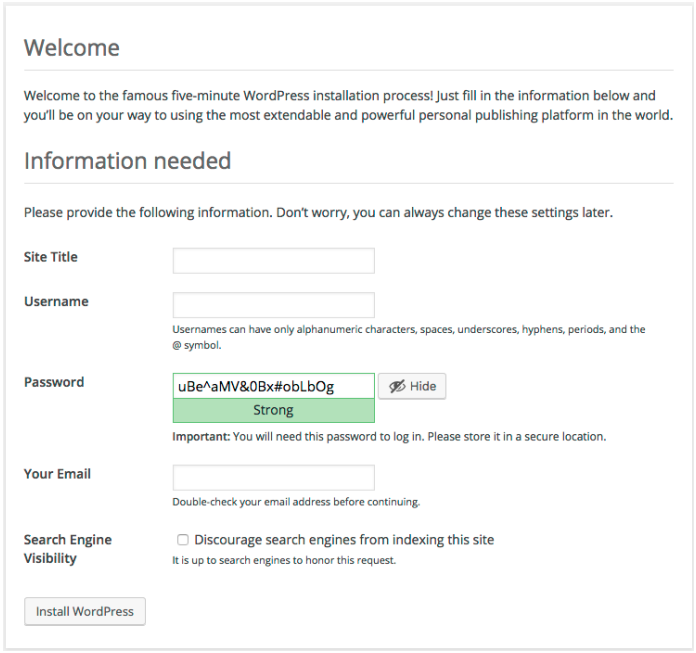
7.2 Verify Dynamic Content on Web Server

In this task, you will generate a WordPress content request from your web browser that will trigger a database query to the MySQL server. Like many web-based applications, WordPress uses a backend database to create, store, and retrieve dynamic content. You will use the WordPress application to show exactly this type of behavior and demonstrate how the VM-Series firewall will secure this traffic.

Browse to WordPress server at http://<<Web Server IP>>/wordpress/wp-admin/install.php

The current security policy rule for MySQL traffic is set to allow.

The http request brings the WordPress landing page which implies communication between the web server and the db server hosting the WordPress DB.



7.3 SSH attack from the Web to the DB Server

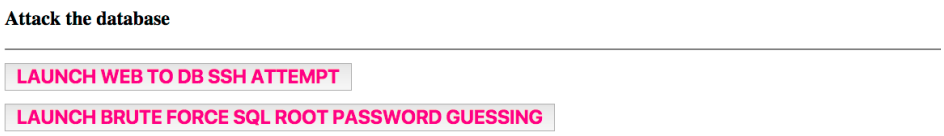
You will generate two simulated east/west (web tier to database tier) attacks and then you will monitor the firewall logs to see the results of the attacks.

The web server is compromised and used to attack the database server. This is a common attack strategy of getting a foothold on the web front-end server and then expanding to the other application tiers with the ultimate goal of accessing all data in the database.

Because the Palo Alto Networks VM-Series firewall has visibility of traffic between the web and database server (east/west traffic), it can detect and automatically block the attacker's attempt to compromise other resources.

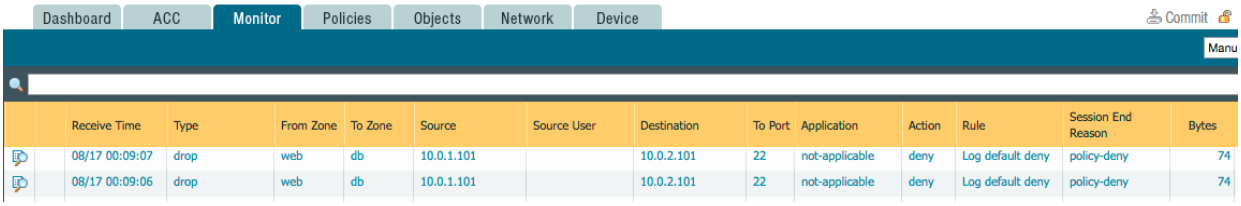
Browse to the SQL attack web page at http://<<Web Server IP>>/sql-attack.html. The specific URL for this lab is http://52.15.125.207/sql-attack.html

The landing page is:



Simulate a compromised web tier by clicking on ***LAUNCH WEB TO DB SSH ATTEMPT.*** This will launch a CGI script that attempts to connect as root to the database server.

Return to the firewall traffic log and note the failed traffic. The VM-Series uses safe application enablement to allow only the correct applications between tiers and SSH is denied between the web and database server.



The traffic is dropped between the web server and db server because the application is does not match the security policies that allows communication between the web and DB servers. Click on ***Return to Attack Launch Page*** to get back to the web server attack page.

We will generate another attack from the web to the DB server.

7.4 SQL attack from the Web to the DB Server

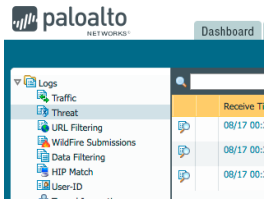
For this attack, you will launch some scripted attacks on the SQL server and use the pre-configured threat protection to show and block those attacks on the VM-Series firewall. As noted above, these are simple, scripted attacks and blocking configurations – there are many other threat protection features available on the Palo Alto Networks VM-Series that are beyond the scope of this demo.

Open a new browser tab and browse to the URL ***http://<<Web Server IP>>/sql-attack.html.*** The actual URL is http://52.15.125.207/sql-attack.html

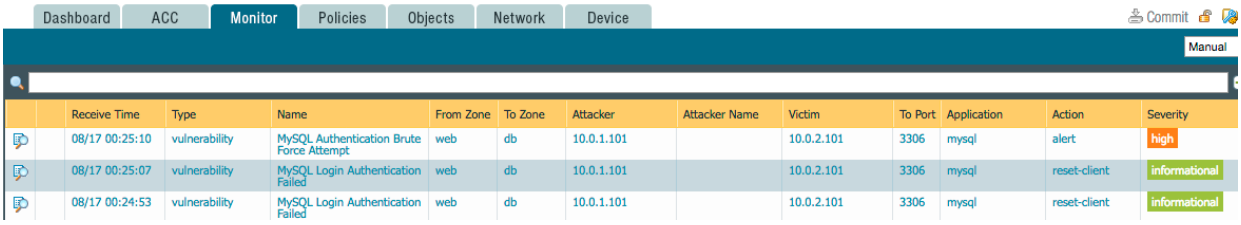
Click on ***Launch Brute Force Attack*** to start a script that will generate multiple failed MySQL authentication attempts.

LAUNCH BRUTE FORCE SQL ROOT PASSWORD GUESSING

Return to the firewall management UI and click the ***Monitor*** tab and then click on ***Threat*** in the left-hand pane under ***Logs***.



Note the new vulnerability log message regarding the failed MySQL events.



Note: The CGI script you launched in Step 2 attempted to login to the MySQL database multiple times with an incorrect password. The VM-Series firewall saw this activity and using the vulnerability profile, reset the connection and logged the activity. If you generate multiple attacks consecutively, the severity of the attack increases. Return back to the web server attack page by clicking ***RETURN TO ATTACK LAUNCH PAGE***.

Brute force MySQL root password attempt launched.

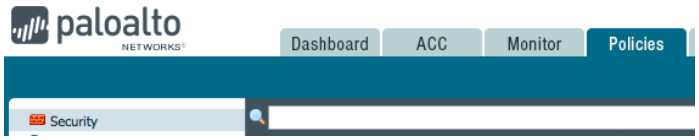
RETURN TO ATTACK LAUNCH PAGE

Now let's review the threat protection profile used to protect against the SQL attack.

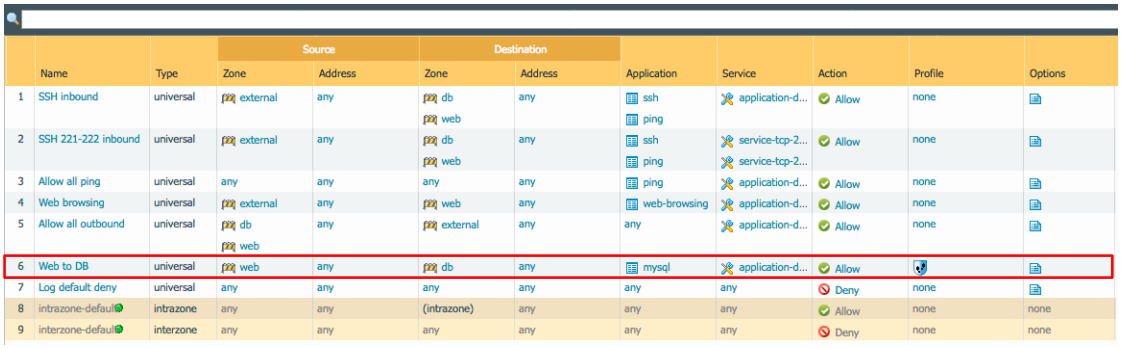
7.5 Review Threat Protection Profile

Review the Vulnerability Protection profile by going to the Policies tab. This profile is used to prevent exploits of vulnerabilities – in the case MySQL. There are many other components of Palo Alto Networks threat protection that are beyond the scope of this lab and are not included in the firewall configuration.

Return to the firewall management UI and click on the ***Policies*** tab and select ***Security*** on the left-hand pane.

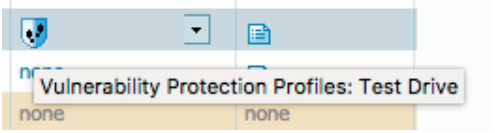


Go to the ***Web to DB*** rule.

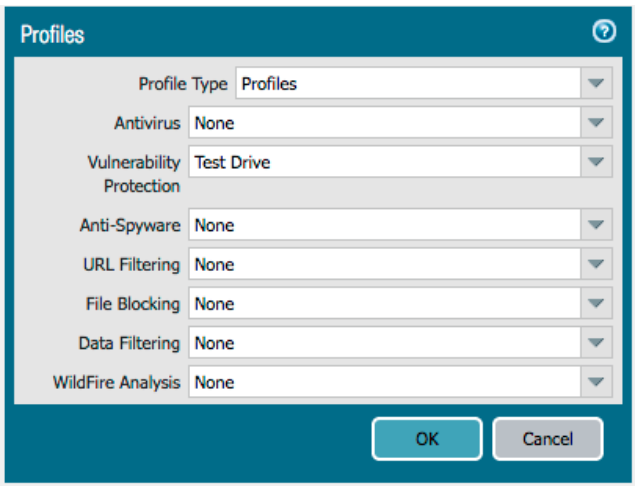


	Name	Type	Source Zone	Source Address	Destination Zone	Destination Address	Application	Service	Action	Profile	Options
1	SSH inbound	universal	external	any	db web	any	ssh ping	application-d...	Allow	none	
2	SSH 221-222 inbound	universal	external	any	db web	any	ssh ping	service-tcp-2... service-tcp-2...	Allow	none	
3	Allow all ping	universal	any	any	any	any	ping	application-d...	Allow	none	
4	Web browsing	universal	external	any	web	any	web-browsing	application-d...	Allow	none	
5	Allow all outbound	universal	db web	any	external	any	any	application-d...	Allow	none	
6	Web to DB	universal	web	any	db	any	mysql	application-d...	Allow		
7	Log default deny	universal	any	any	any	any	any	any	Deny	none	
8	intrazone-default	intrazone	any	any	(intrazone)	any	any	any	Allow	none	none
9	interzone-default	interzone	any	any	any	any	any	any	Deny	none	none

Hover over the icon in the ***Profile*** column and note the ***Test Drive*** vulnerability profile in use.



Now click on the icon in the ***Profile*** column and you will see all the threat protection profiles.



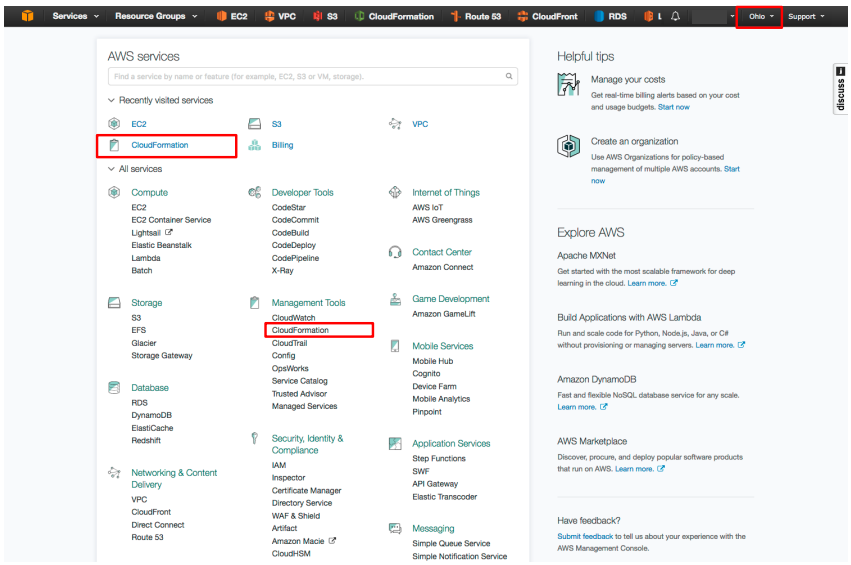
Note the ***Test Drive*** Vulnerability Protection profile. This is a custom profile created just for this Test Drive lab. It is part of the default vulnerability protection profile but is called out separately for the purpose of this demo environment.

Now that you have completed the lab, it is time to erase the resources created through the template.

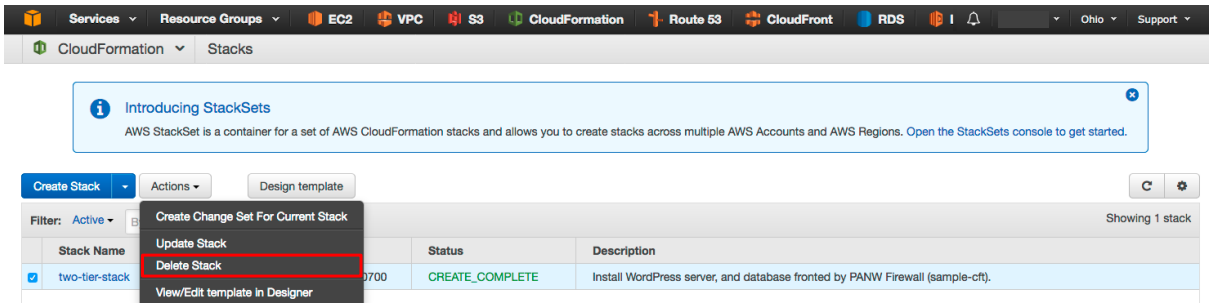
8. Cleanup

8.1 Delete the Stack

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



Select the stack you created, then, under **Actions**, click **Delete Stack:**

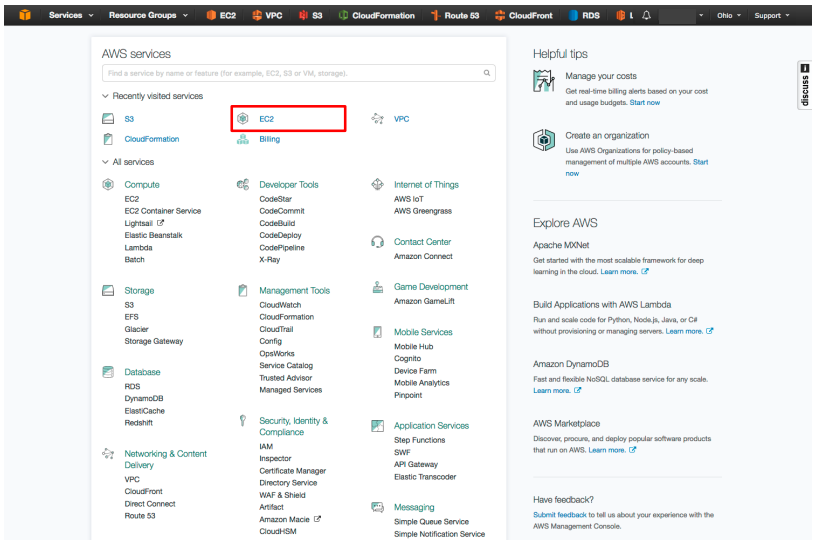


This should delete all the resources created via the template and release any Elastic IPs associated with the firewall.

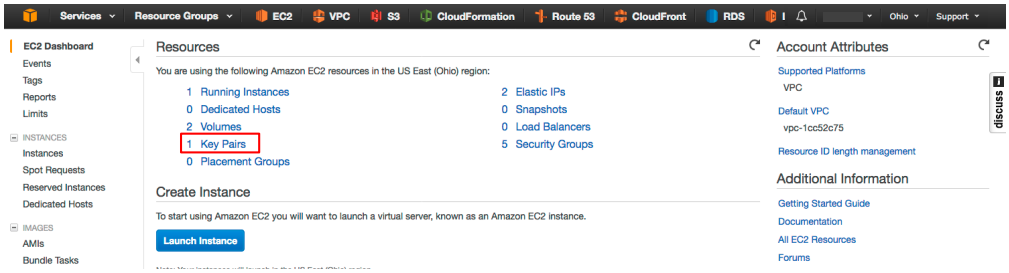
8.2 Delete keys

As part of the lab exercise, a key pair as manually created thus it must be manually removed.

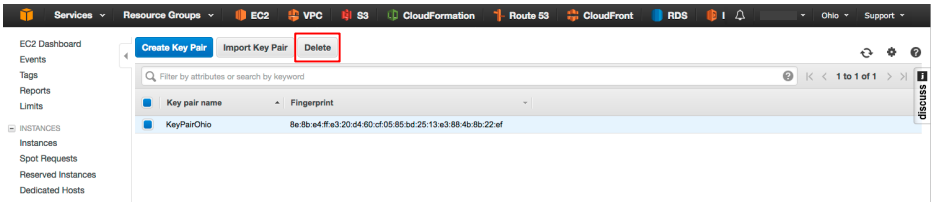
To do that, go to the **EC2** console:



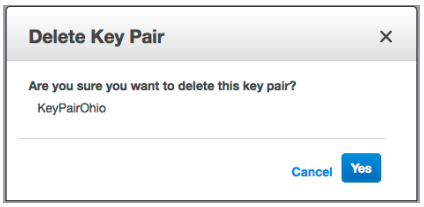
Click on **Key Pairs**:



Select the appropriate key and click **Delete:**



And confirm **Yes** on the next screen:



Congratulations, you have successfully completed the lab.

9. Conclusion

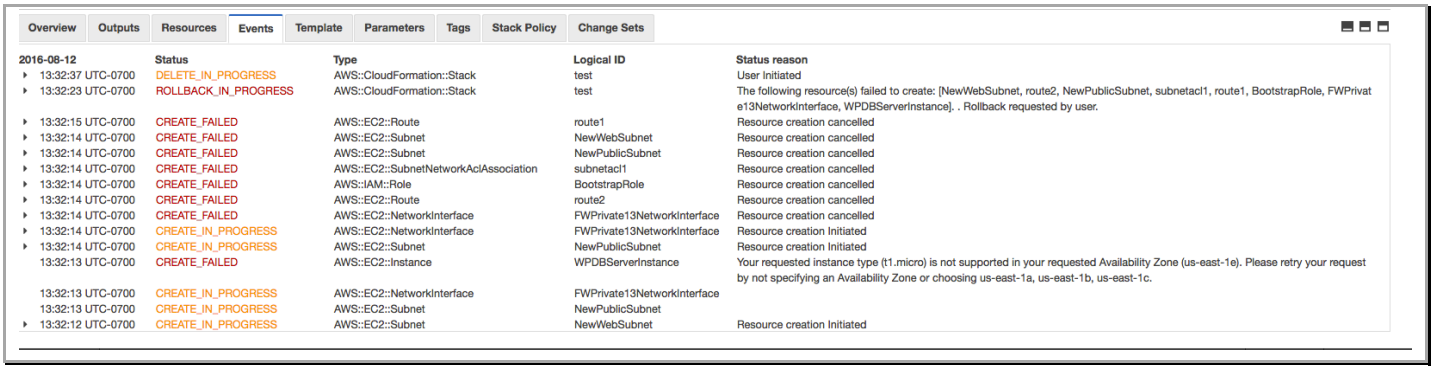
You have successfully deployed a sample CFT in AWS and have experienced how the next generation VM-Series firewall can not only secure traffic inbound into your VPC, but within the VPC itself.

Appendix A

Troubleshooting tips

1. Stack creation fails

Occasionally stack creation fails due to various unknown reasons. Maybe AWS is updating their software, maybe that particular region is having a service outage. These errors are usually transient in nature and generally will go away when the stack is deleted and re-launched (OR launched in a different region) If the errors are consistent, then please read on for other troubleshooting tips. For instance, one of the errors encountered maybe as follows:



2016-08-12	Status	Type	Logical ID	Status reason
13:32:37 UTC-0700	DELETE_IN_PROGRESS	AWS::CloudFormation::Stack	test	User Initiated
13:32:23 UTC-0700	ROLLBACK_IN_PROGRESS	AWS::CloudFormation::Stack	test	The following resource(s) failed to create: [NewWebSubnet, route2, NewPublicSubnet, subnetacl1, route1, BootstrapRole, FWPrivate13NetworkInterface, WPDBServerInstance]. . Rollback requested by user.
13:32:15 UTC-0700	CREATE_FAILED	AWS::EC2::Route	route1	Resource creation cancelled
13:32:14 UTC-0700	CREATE_FAILED	AWS::EC2::Subnet	NewWebSubnet	Resource creation cancelled
13:32:14 UTC-0700	CREATE_FAILED	AWS::EC2::Subnet	NewPublicSubnet	Resource creation cancelled
13:32:14 UTC-0700	CREATE_FAILED	AWS::EC2::SubnetNetworkAclAssociation	subnetacl1	Resource creation cancelled
13:32:14 UTC-0700	CREATE_FAILED	AWS::IAM::Role	BootstrapRole	Resource creation cancelled
13:32:14 UTC-0700	CREATE_FAILED	AWS::EC2::Route	route2	Resource creation cancelled
13:32:14 UTC-0700	CREATE_FAILED	AWS::EC2::NetworkInterface	FWPrivate13NetworkInterface	Resource creation cancelled
13:32:14 UTC-0700	CREATE_IN_PROGRESS	AWS::EC2::NetworkInterface	FWPrivate13NetworkInterface	Resource creation Initiated
13:32:14 UTC-0700	CREATE_IN_PROGRESS	AWS::EC2::Subnet	NewPublicSubnet	Resource creation Initiated
13:32:13 UTC-0700	CREATE_FAILED	AWS::EC2::Instance	WPDBServerInstance	Your requested instance type (t1.micro) is not supported in your requested Availability Zone (us-east-1e). Please retry your request by not specifying an Availability Zone or choosing us-east-1a, us-east-1b, us-east-1c.
13:32:13 UTC-0700	CREATE_IN_PROGRESS	AWS::EC2::NetworkInterface	FWPrivate13NetworkInterface	
13:32:13 UTC-0700	CREATE_IN_PROGRESS	AWS::EC2::Subnet	NewPublicSubnet	
13:32:12 UTC-0700	CREATE_IN_PROGRESS	AWS::EC2::Subnet	NewWebSubnet	Resource creation Initiated

The error indicates that no t1.micro instances are available in the selected availability zone. This is a transient error and the fix is to redeploy the template.

2. EIP Exhaustion

If the account does not have a minimum two unallocated and unassociated elastic IPs, stack creation will fail.

09:09:02 UTC-0600	CREATE_IN_PROGRESS	AWS::EC2::VPCDHCPOptionsAssociation	dchpassoc1	Resource creation Initiated
09:09:02 UTC-0600	CREATE_IN_PROGRESS	AWS::EC2::RouteTable	rtb059a2460	Resource creation Initiated
09:09:02 UTC-0600	CREATE_FAILED	AWS::EC2::EIP	ManagementElasticIP	The maximum number of addresses has been reached.
09:09:02 UTC-0600	CREATE_FAILED	AWS::EC2::EIP	PublicElasticIP	The maximum number of addresses has been reached.
09:09:02 UTC-0600	CREATE_IN_PROGRESS	AWS::EC2::RouteTable	rtb049a2461	Resource creation Initiated
09:09:01 UTC-0600	CREATE_IN_PROGRESS	AWS::EC2::NetworkAcl	aclb765d6d2	Resource creation Initiated
09:09:01 UTC-0600	CREATE_IN_PROGRESS	AWS::EC2::VPCDHCPOptionsAssociation	dchpassoc1	
09:09:01 UTC-0600	CREATE_IN_PROGRESS	AWS::EC2::RouteTable	rtb059a2460	

If you encounter this error, please refer to section 4.6 for more details.

3. Bootstrapping not working

If the VM-Series firewall is up and you are able to access the login page, but unable to login using the username/password: admin/paloalto, then chances are boostrapping has failed. There could be several reasons:

a. Corrupt configuration files

Please ensure that the bootstrap.xml and init-cft.txt files mentioned in section 4.4 are not corrupted.

b. Incorrect bootstrap bucket-name

Another reason for bootstrapping to fail is that the bootstrap bucket name (Parameter: BootstrapBucketName) was mentioned incorrectly during stack creation (template launch). Please make sure the bucket name created in section 4.4 is mentioned when launching the template.