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: May 2016

Table of Contents

Version History **4**
1. About CFTs **5**
2. Support Policy **5**
3. Instances used **6**
4. Prerequisites **6**
4.1 Create an AWS account 6
4.2 Add a credit card to your AWS account 6
4.3 Review and accept the EULA 6
4.4 Create and download an SSH keypair 11
4.5 Create a Bootstrap Bucket 12
4.6 Download the Template 17
4.7 Check Elastic IPs 17
5. Launch The CFT **19**
6. Review what was created **23**
7. Access the VM-Series Firewall **27**
8. Review the VM-Series WebUI **28**
Task 1 – Login and Dashboard summary 28
Task 2 – Review PAN-OS WebUI – Application Command Center (ACC) 30
Task 3 – Review PAN-OS WebUI – Security Policies 32
Task 4 – Review PAN-OS WebUI – Monitor tab 34
Task 5 – Review the WebUI – Object, Network, Device Tabs 35
Activity 2 – Safely Enable Applications **37**
Task 1 – Verify Static Content on Web Server 37
Task 2 – Verify Dynamic Content on Web Server 38
Task 3 – Allow MySQL on the VM-Series Firewall 39
Task 4 – Re-verify Dynamic Content on Web Server 41
Activity 3 – Safe Application Enablement **43**
Task 1 – Attempt to SSH from the web server to the DB server 43
Task 2 – Review the threat protection profile 43
Task 3 – Trigger the SQL brute force attack and review logs 45
9. Cleanup **46**
9.1 Delete the Stack 46

9.2 Delete keys 47
10. Conclusion 49
Appendix A 50
Troubleshooting tips 50

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. About CFTs

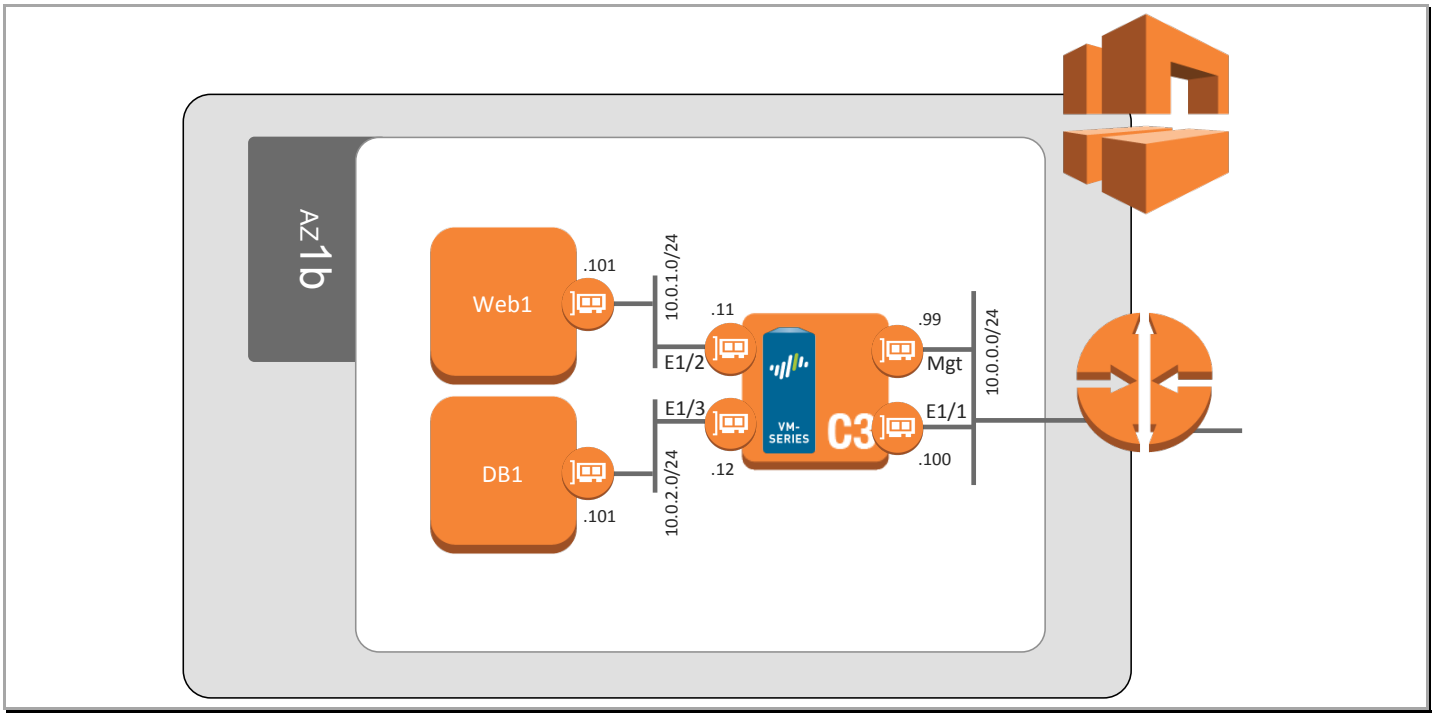
AWS CloudFormation Templates (CFTs), are JSON files that can launch nearly all AWS resources including VPCs, subnets, security groups, route tables, plus many more. AWS CFTs are used for ease of deployment and are key to any auto-scaling environment.

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.

4.2 Add a credit card to your AWS account

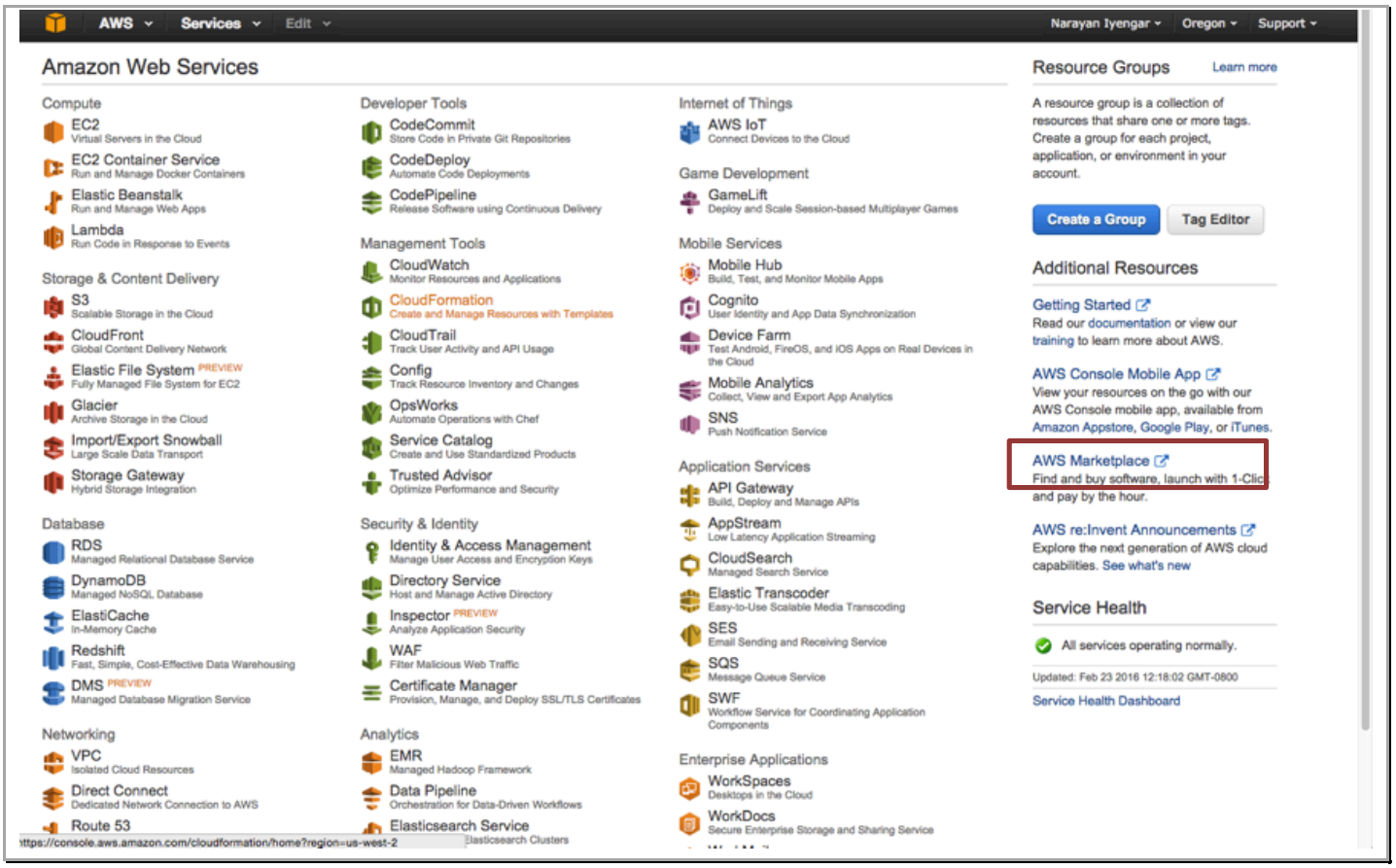
In order to continue you will need to add a method of payment to your AWS account. Use the following https://console.aws.amazon.com/billing/home#/paymentmethods

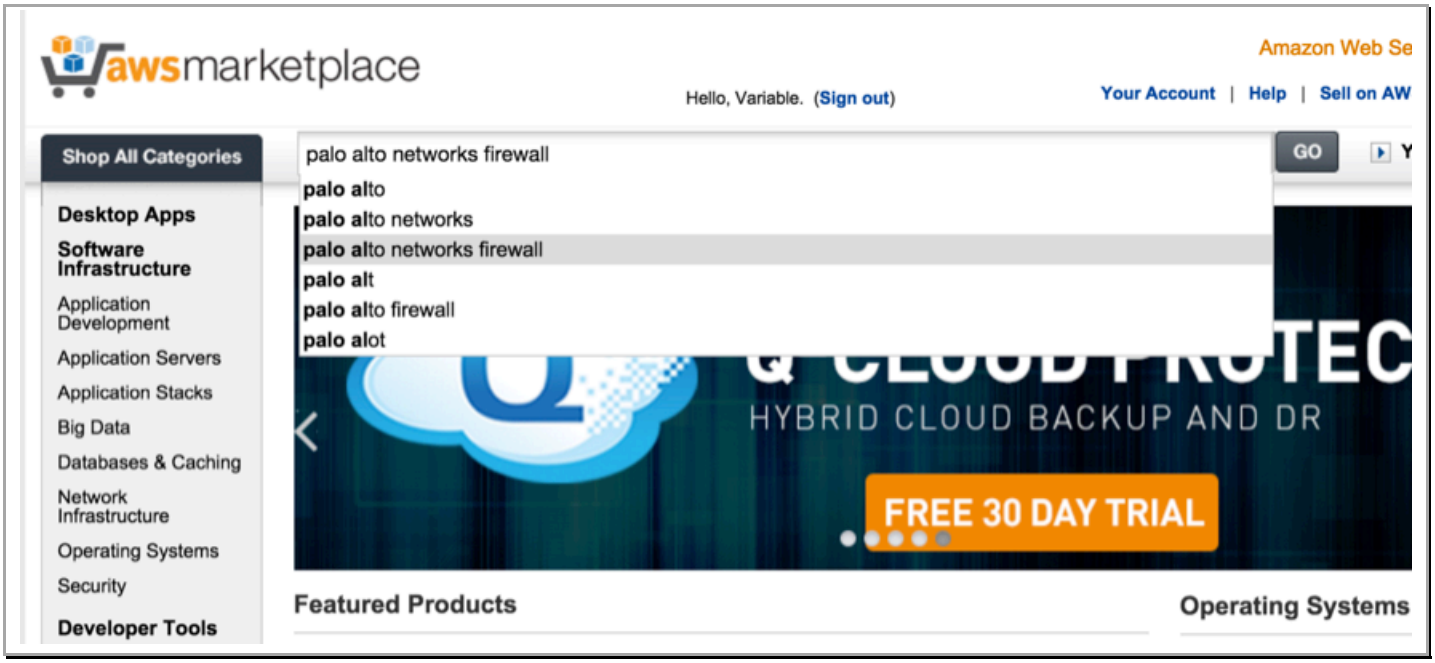
If creating a new account, you may receive a phone call from AWS for verification purposes.

4.3 Review and accept the EULA

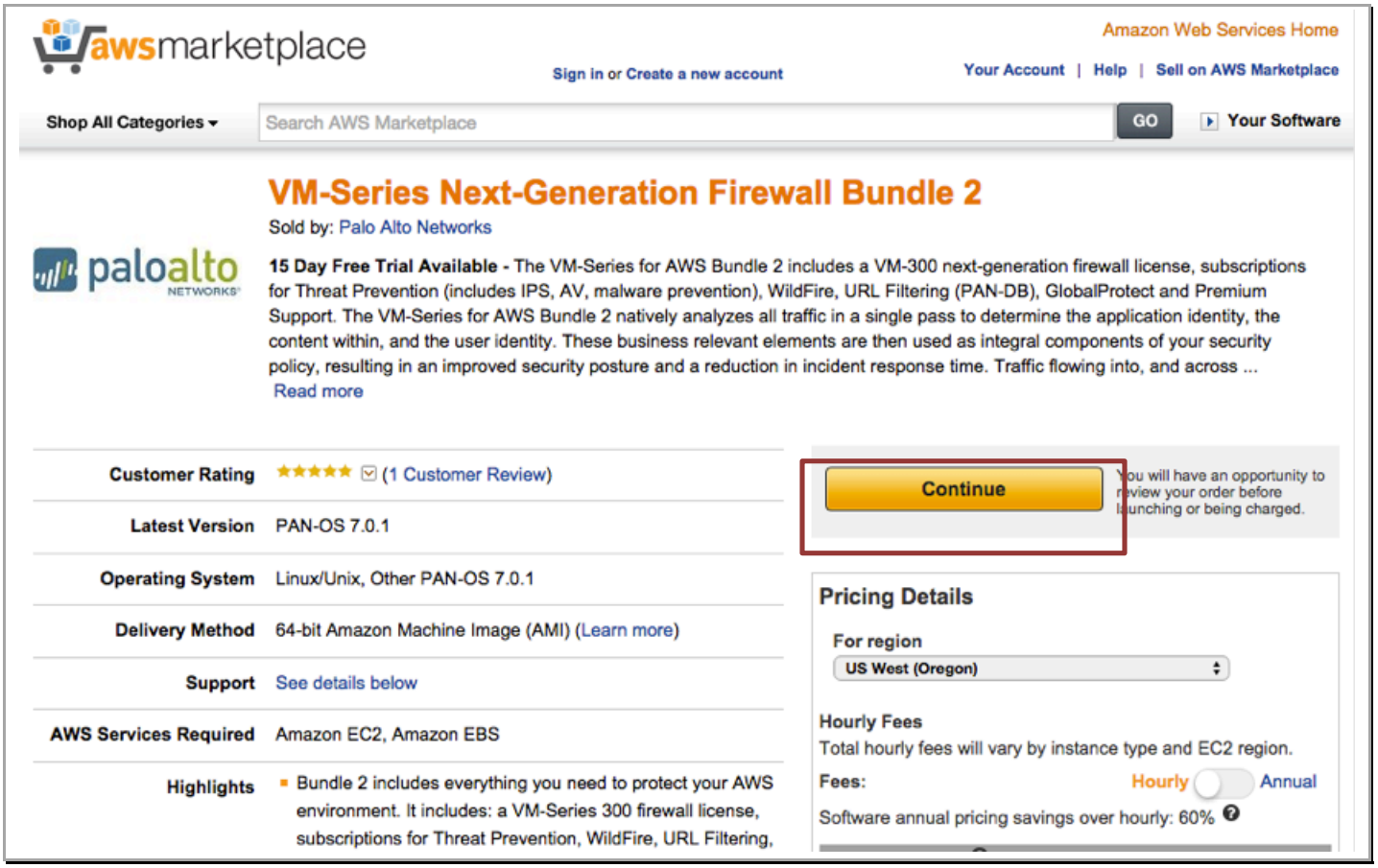
If this is your first time using AWS to launch a VM-Series firewall bundle you will need to review and accept the software license agreement for the VM-Series.

Click on **AWS Marketplace** and search for **Palo Alto Networks firewall**:

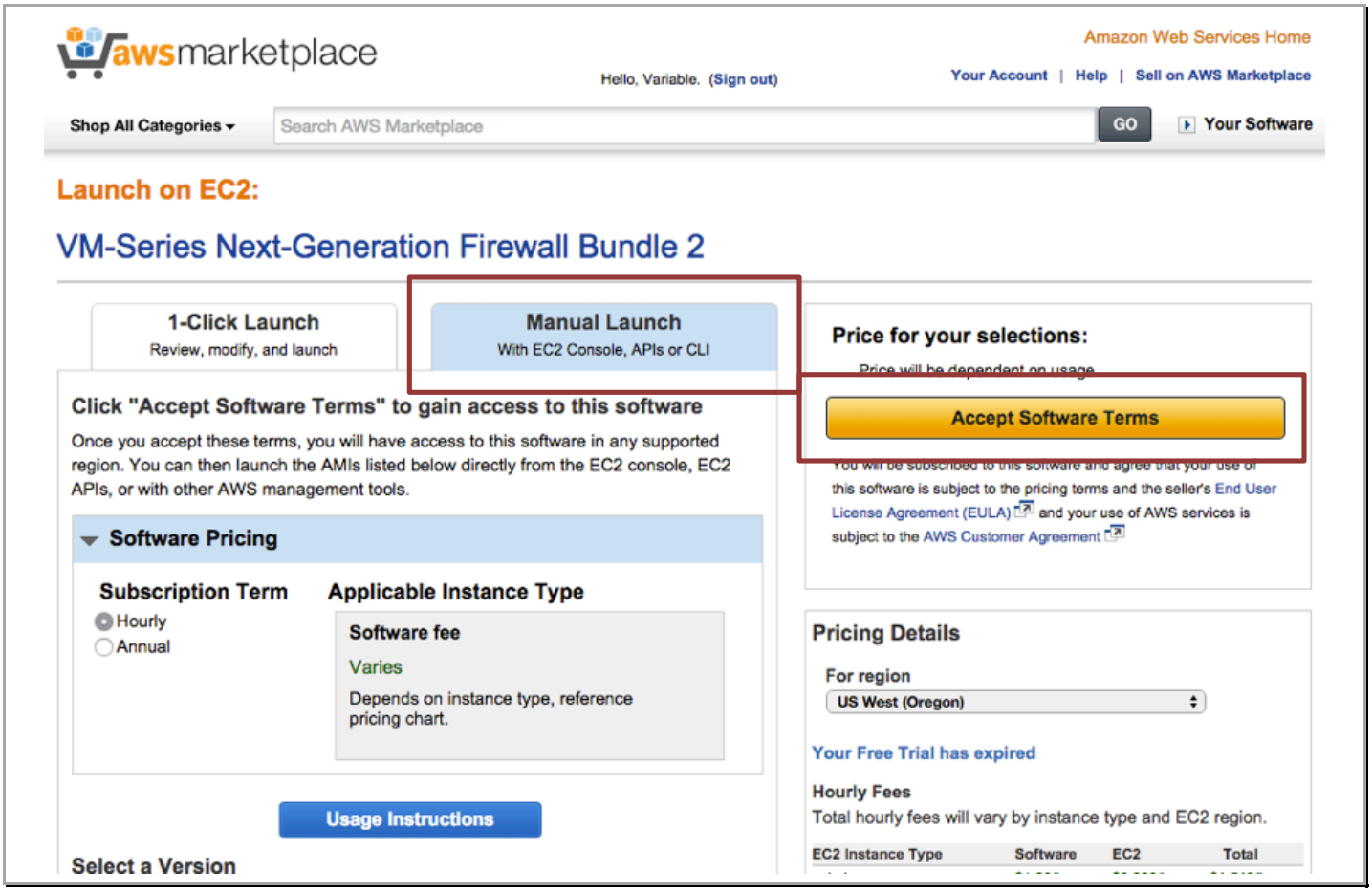




Select **VM-Series Next Generation Firewall Bundle 2**

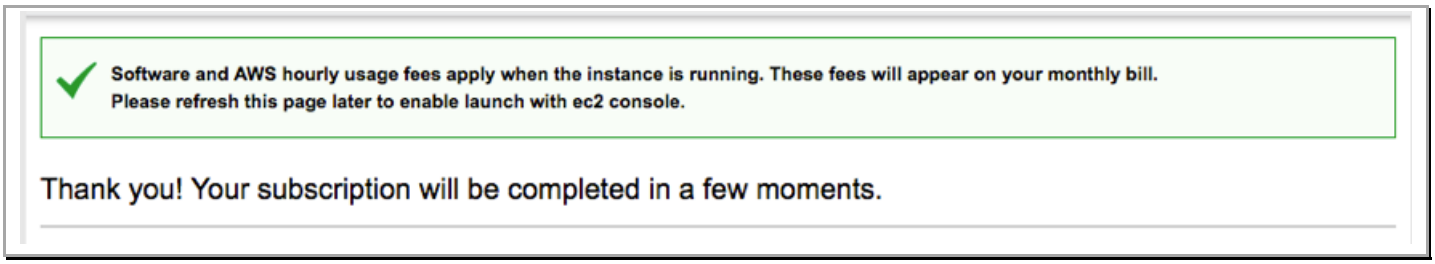


Click **Continue**.



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

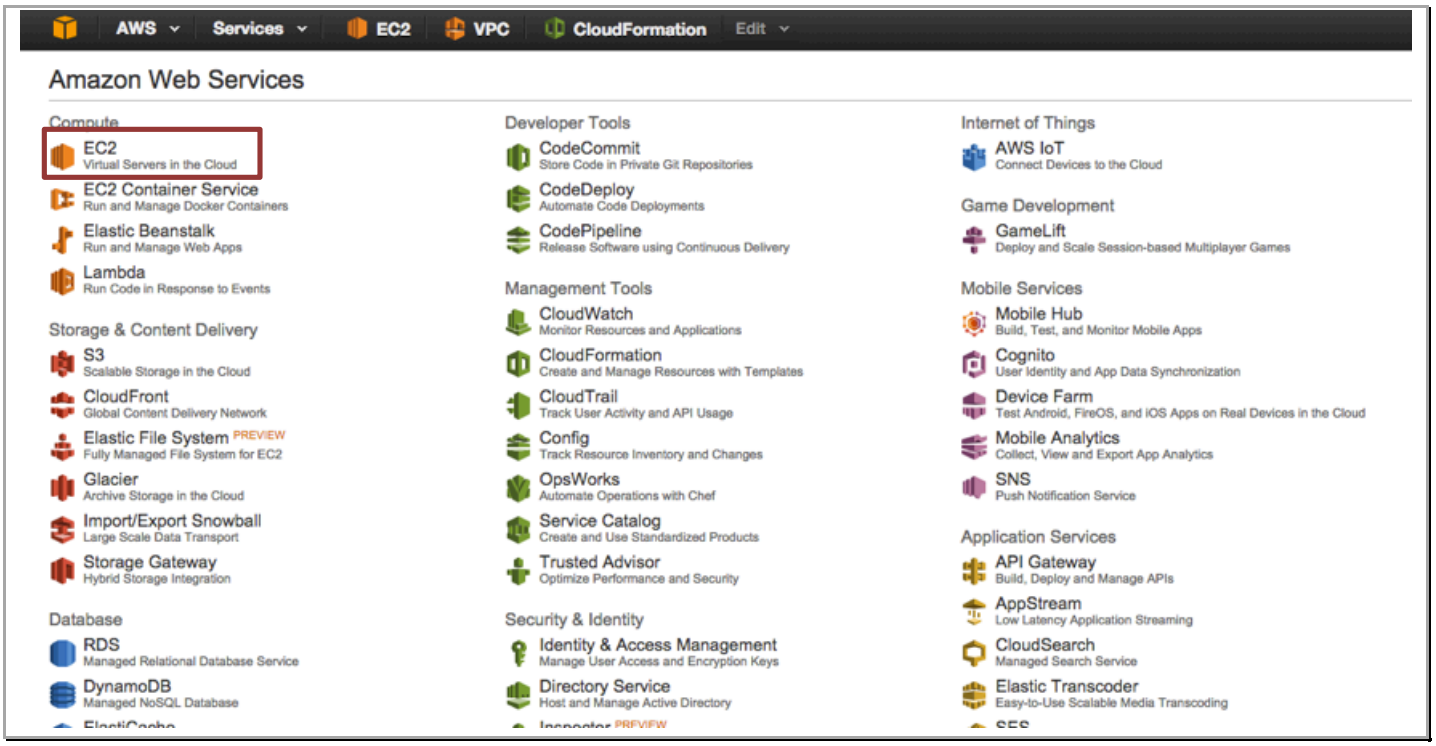
You should see this screen:



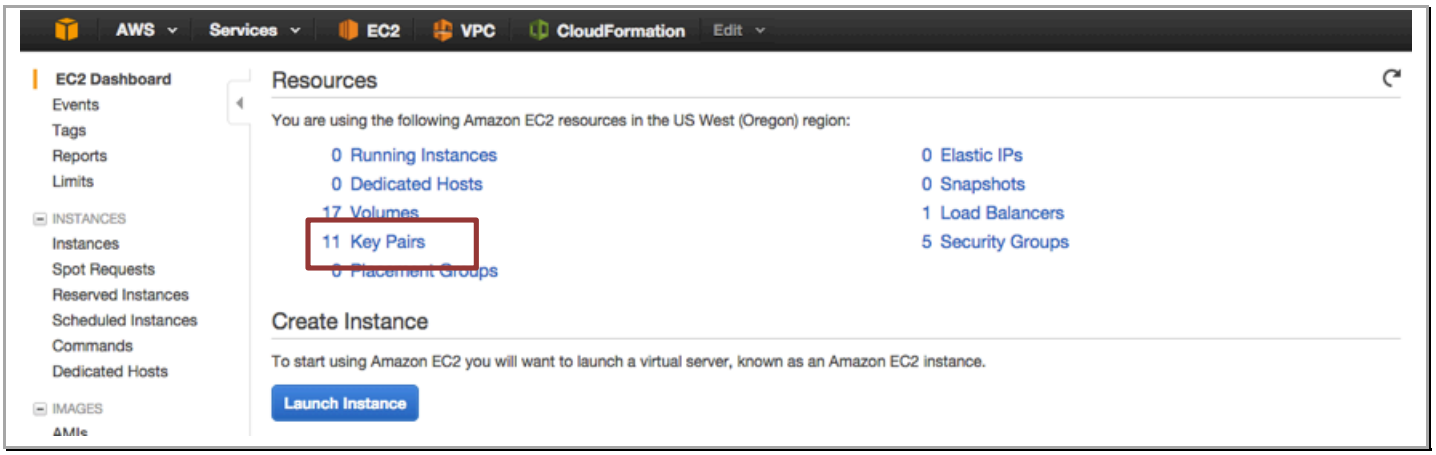
You can now proceed to the next step.

4.4 Create and download an SSH keypair

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

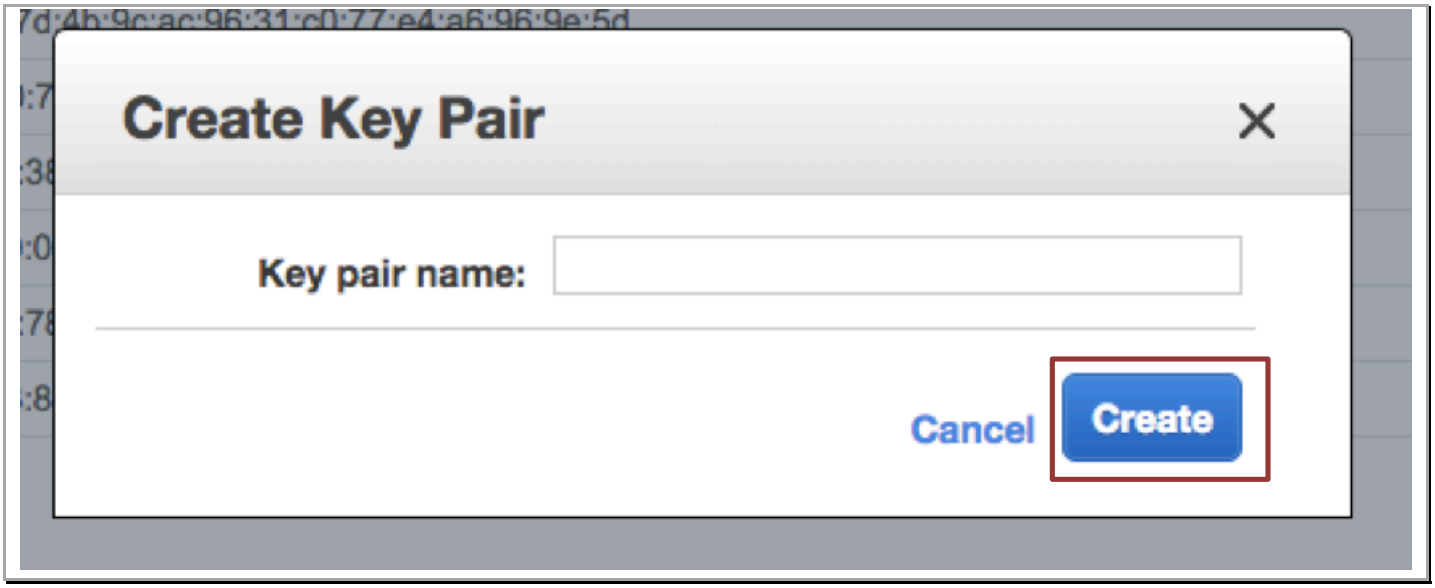


Click **KeyPairs**



Click **Create Key Pair**

Give it a name.

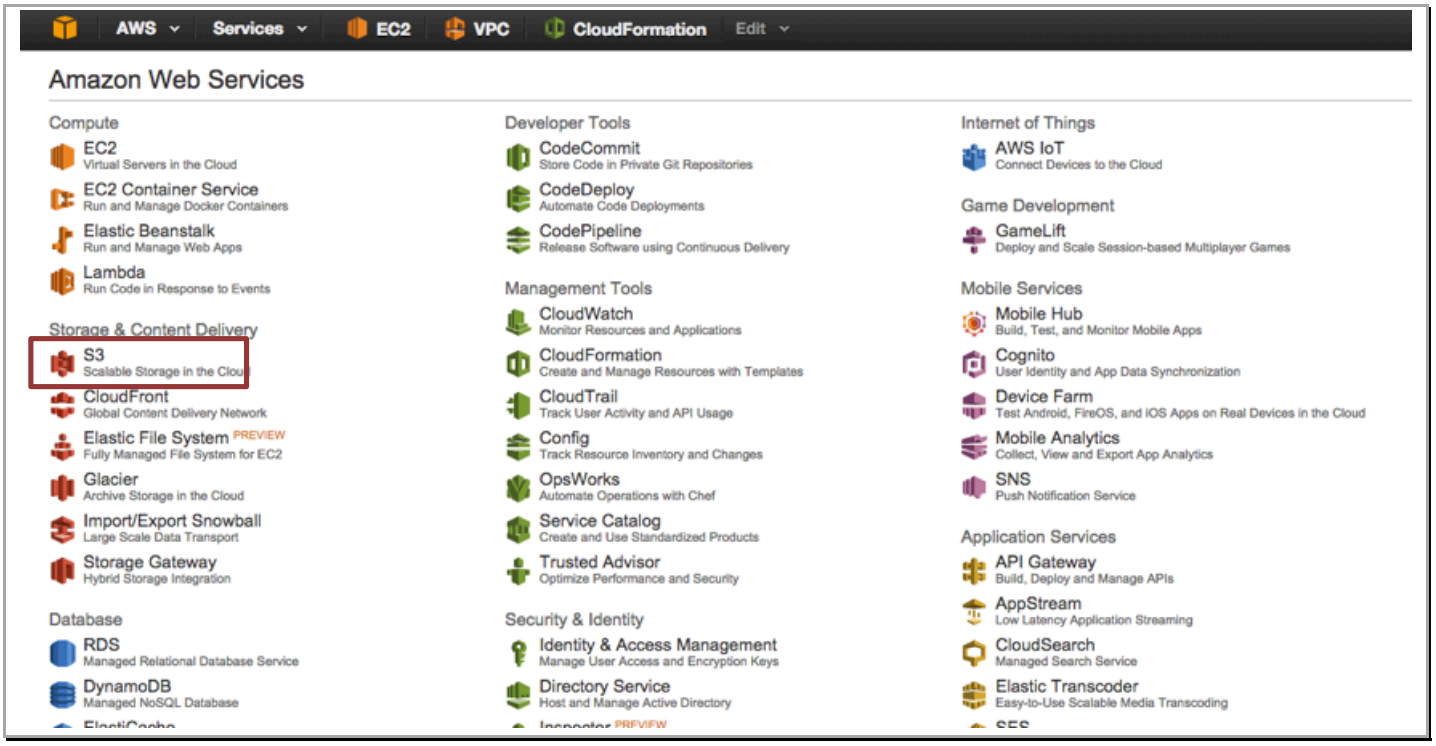


And click **Create**. This should now prompt you to save the just generated private key. Save the key.

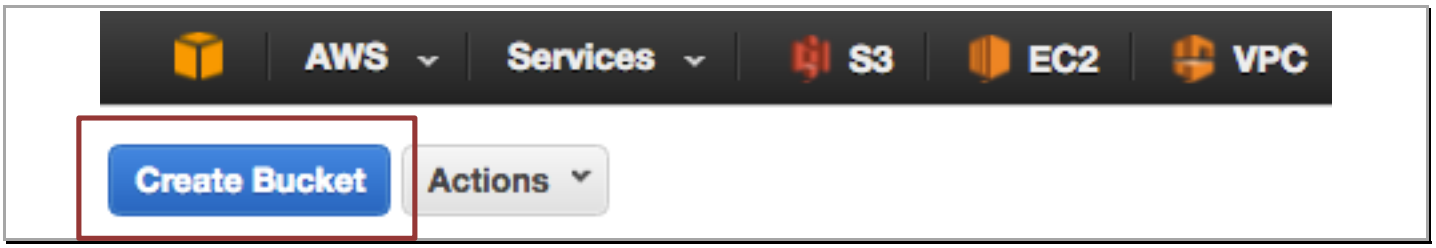
4.5 Create a Bootstrap Bucket

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

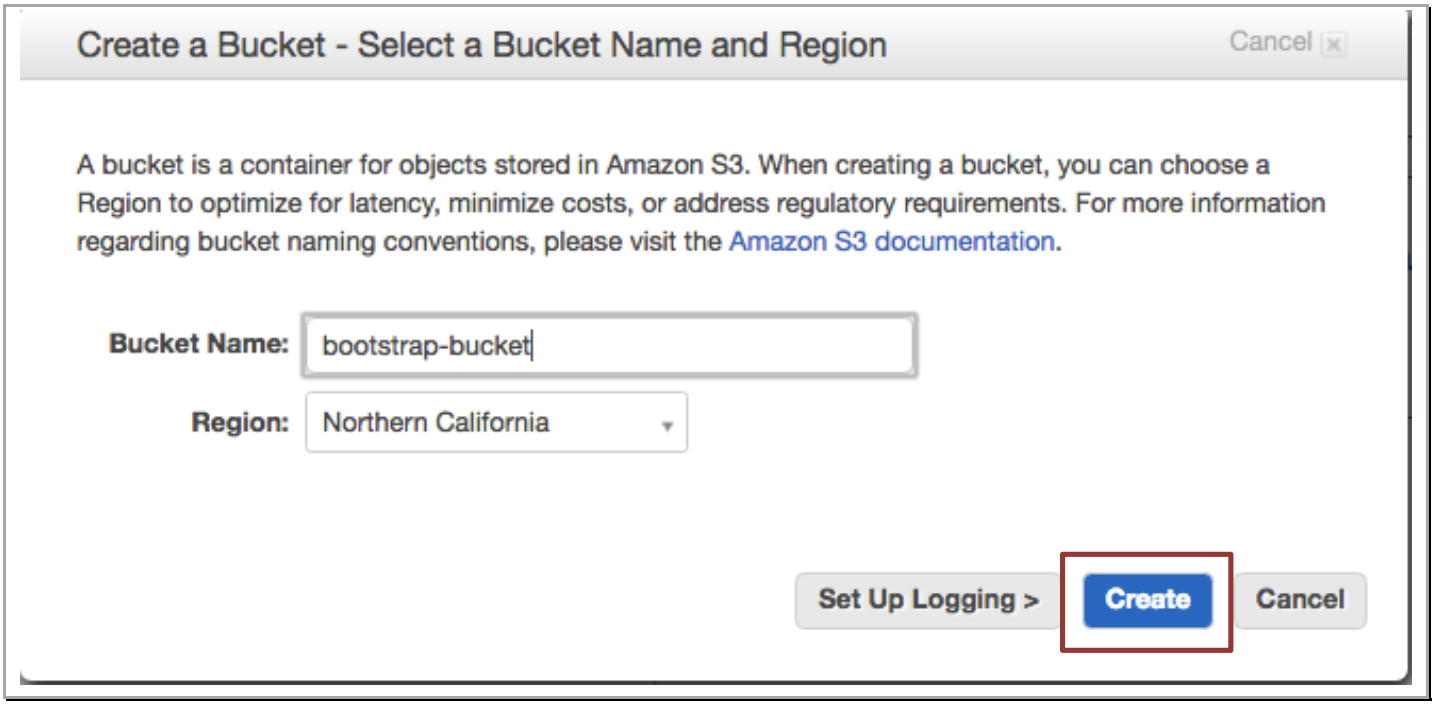
In order to create a Bootstrap bucket, Sign into the AWS console https://www.amazon.com and click on **S3**



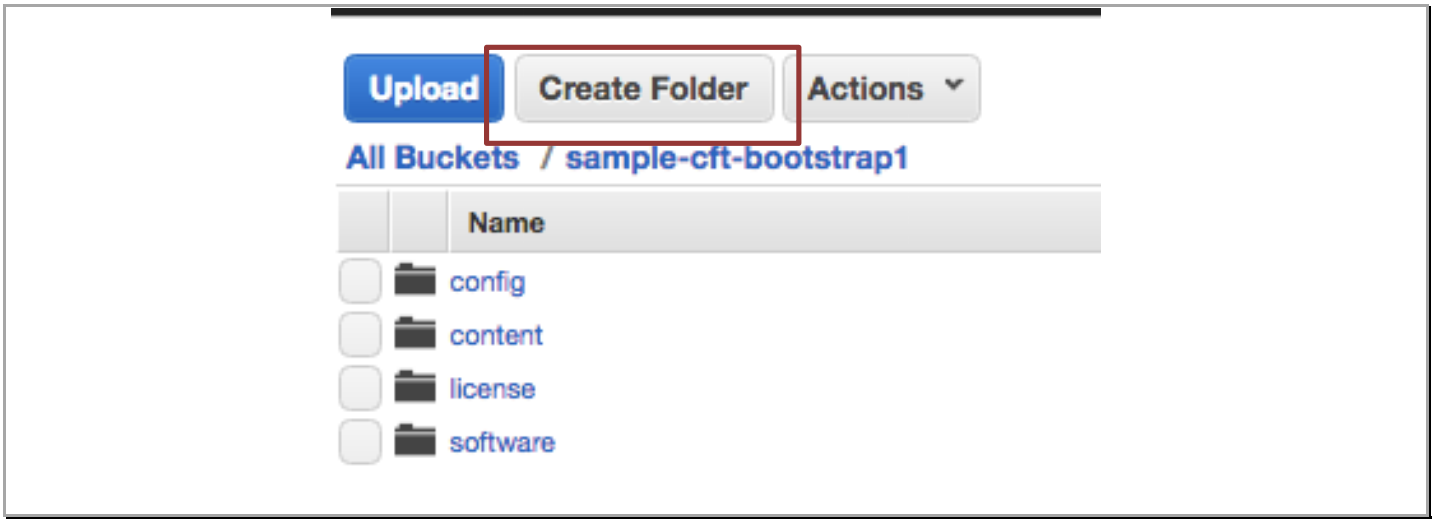
Click **Create Bucket**:



Enter a bucket name and select a region and click **Create**:



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**:



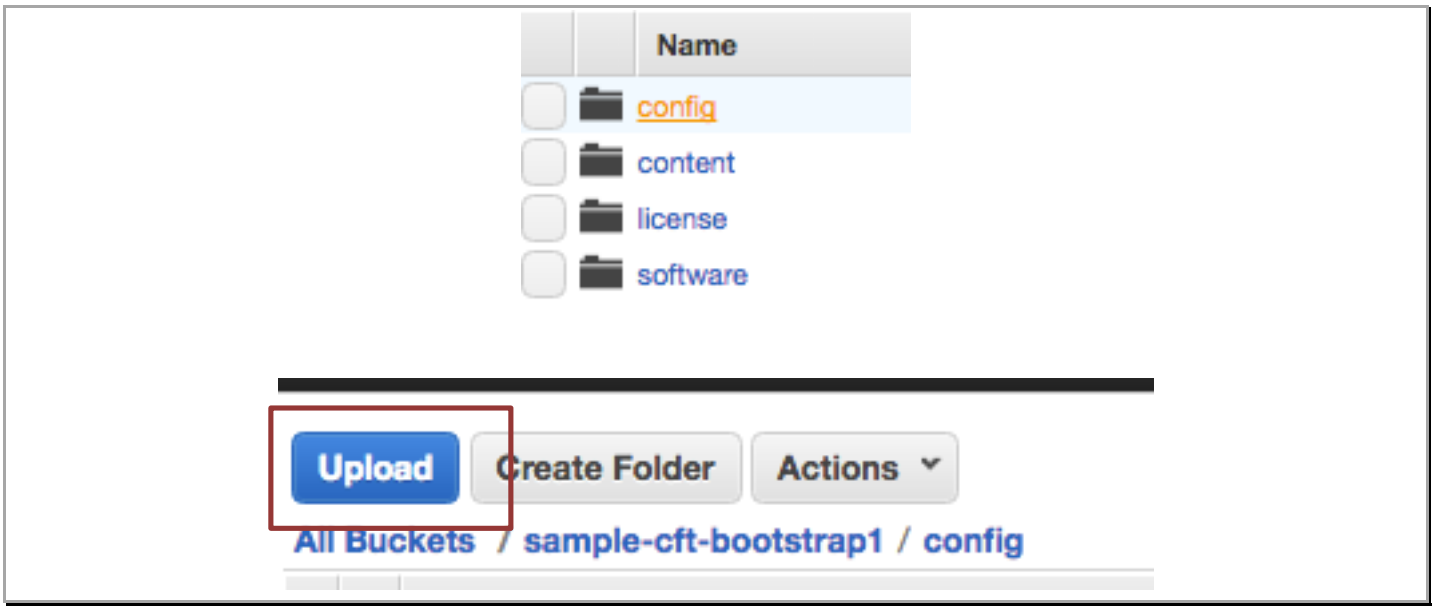
Download the following files and save them in a known location:

https://raw.githubusercontent.com/PaloAltoNetworks/aws/master/two-tier sample/bootstrap/bootstrap.xml

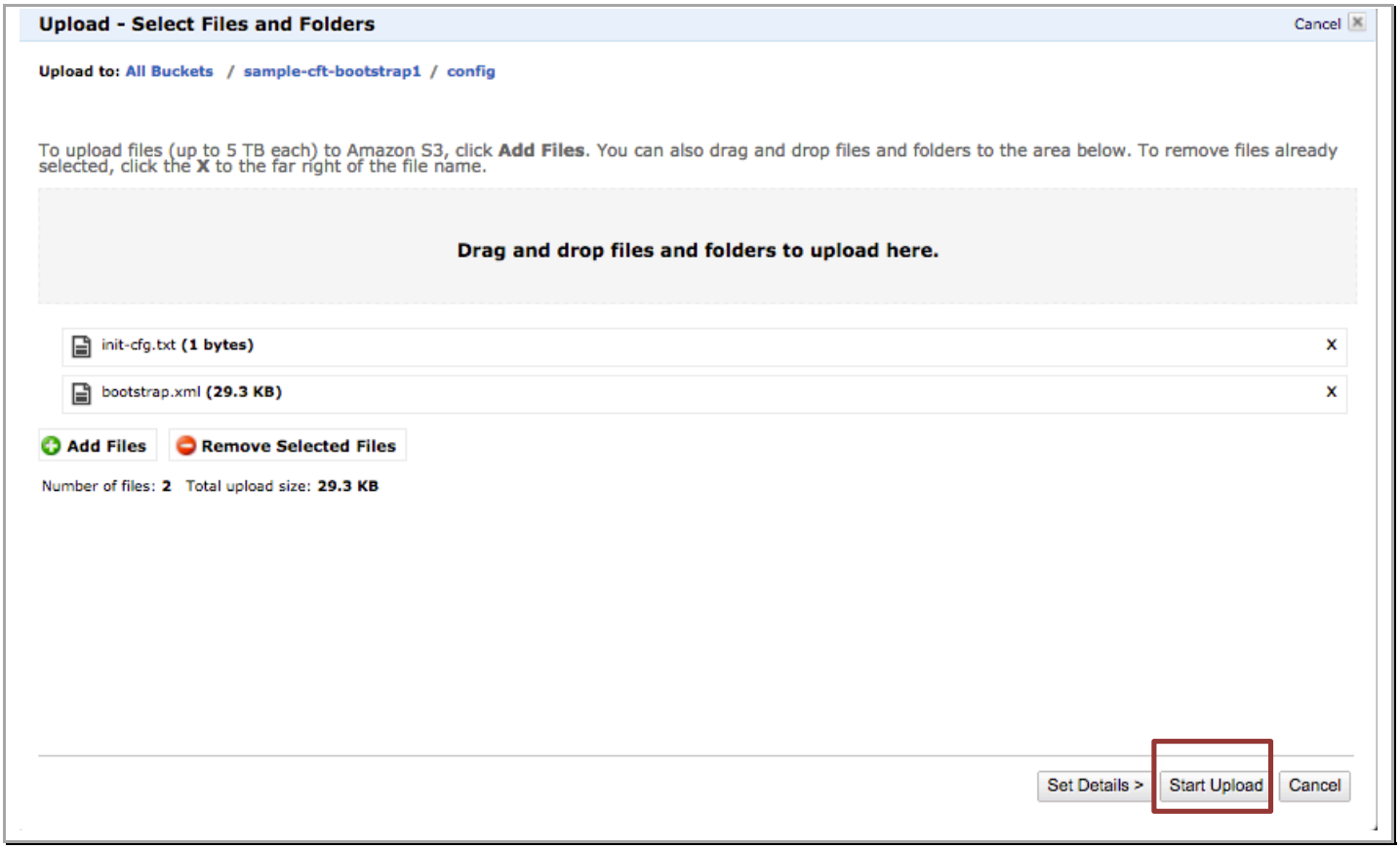
https://raw.githubusercontent.com/PaloAltoNetworks/aws/master/two-tier sample/bootstrap/init-cfg.txt

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

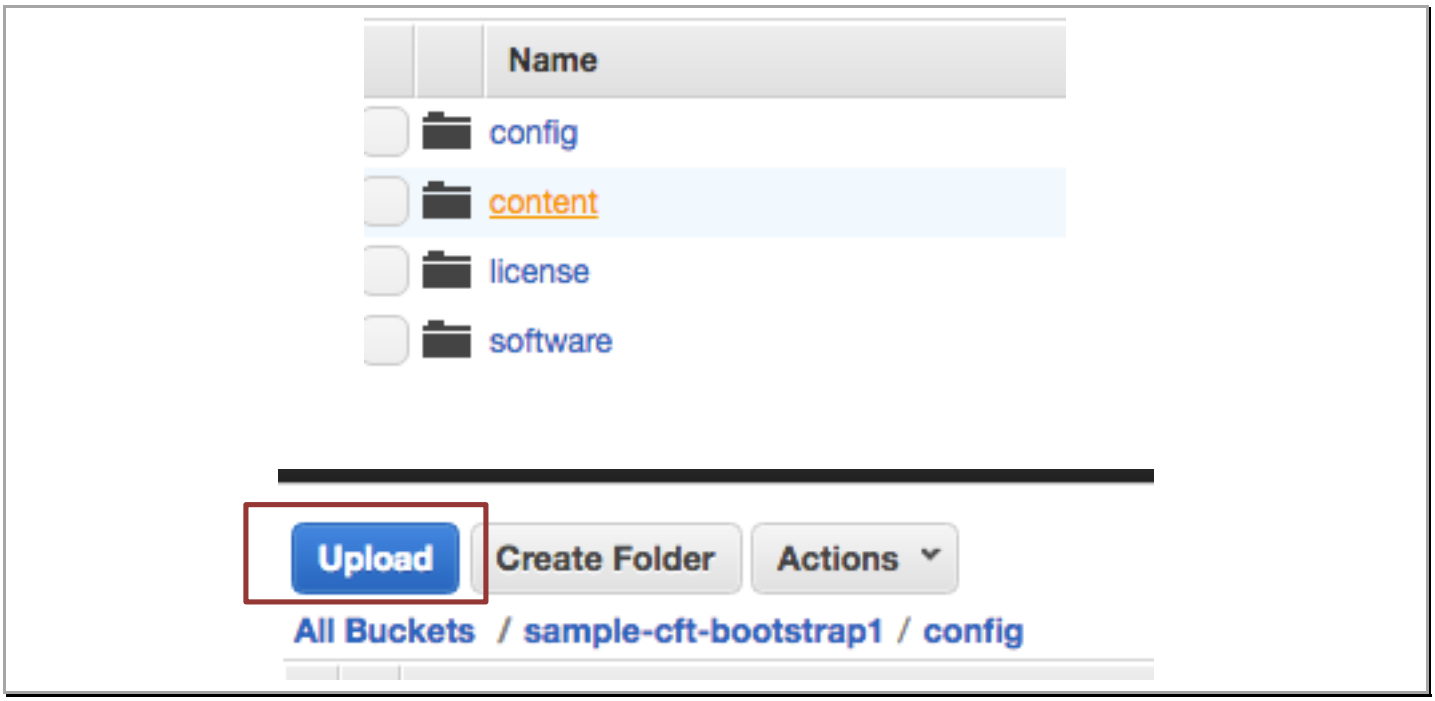
Now click on the **config** folder in the **S3** console and click **Upload:**



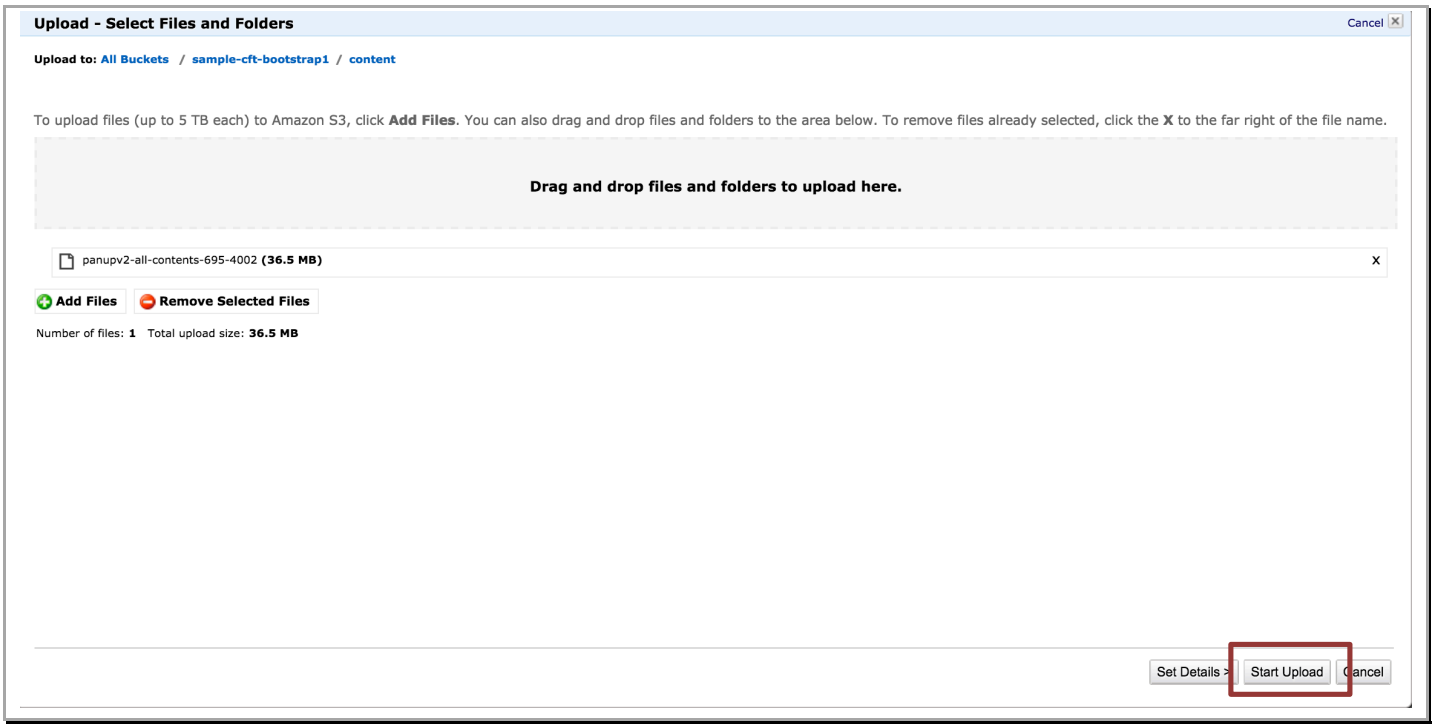
Select **Add Files** and select the two files (bootstrap.xml and init-cft.txt) downloaded previously and click **Start Upload**:



Now click on the **content** folder ins the **S3** console and click **Upload**:



Select **Add Files** and select the file (panupv2-all-contents-600-3449) downloaded previously and click **Start Upload**:



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.

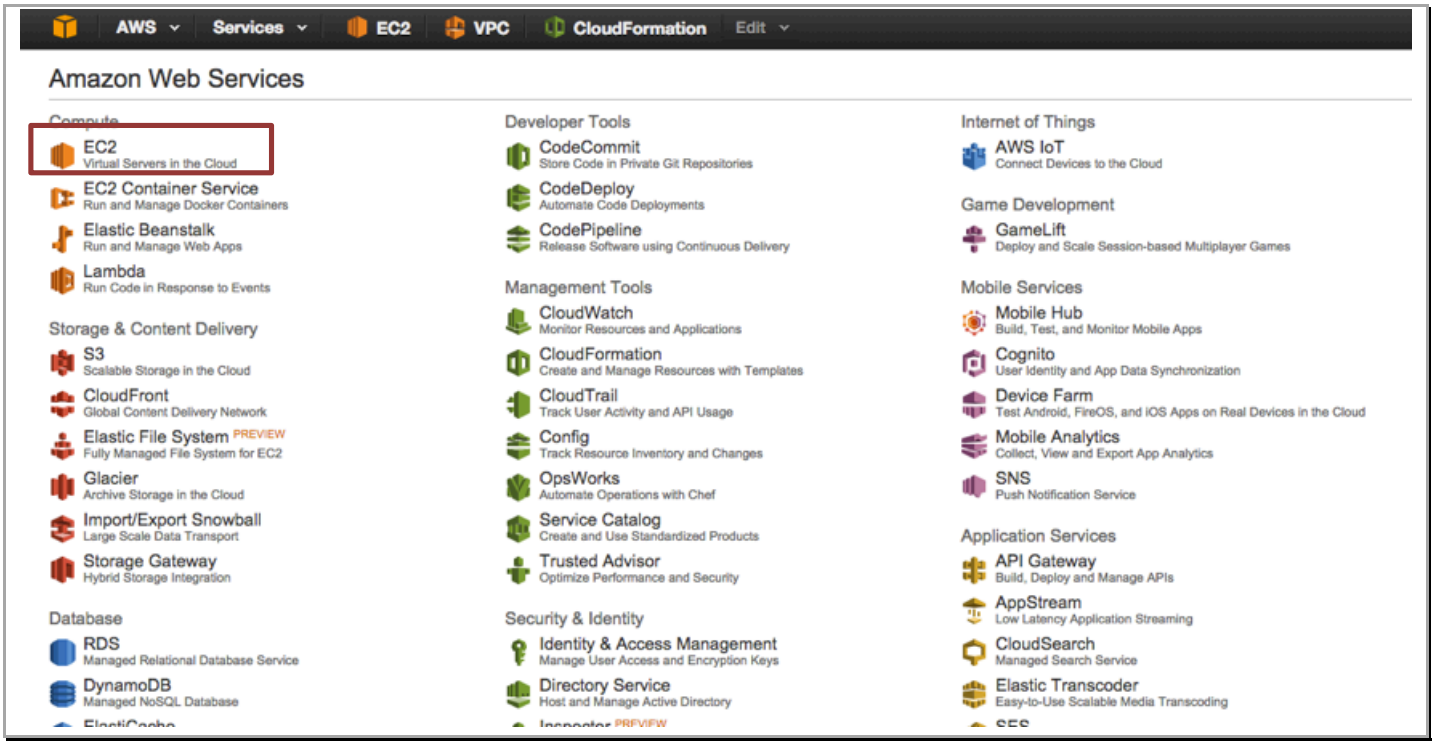
4.6 Download the Template

Download and save the CloudFormation template and save in a known location:

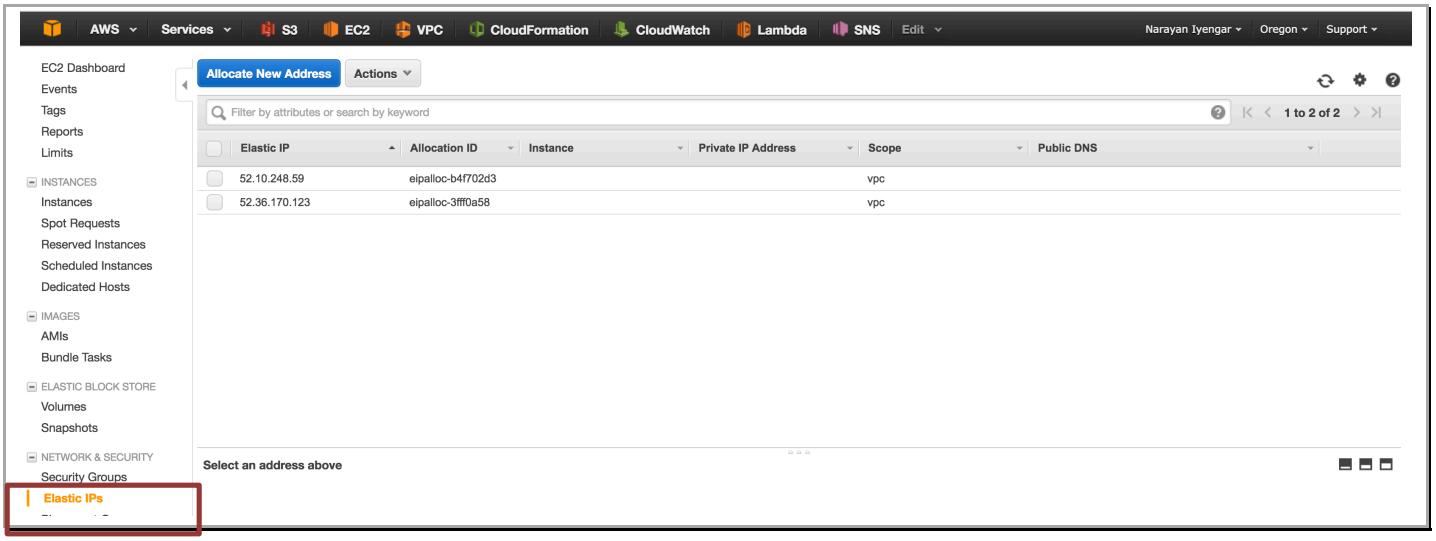
https://raw.githubusercontent.com/PaloAltoNetworks/aws/master/two-tier sample/pan-sample-cft.json

4.7 Check Elastic IPs

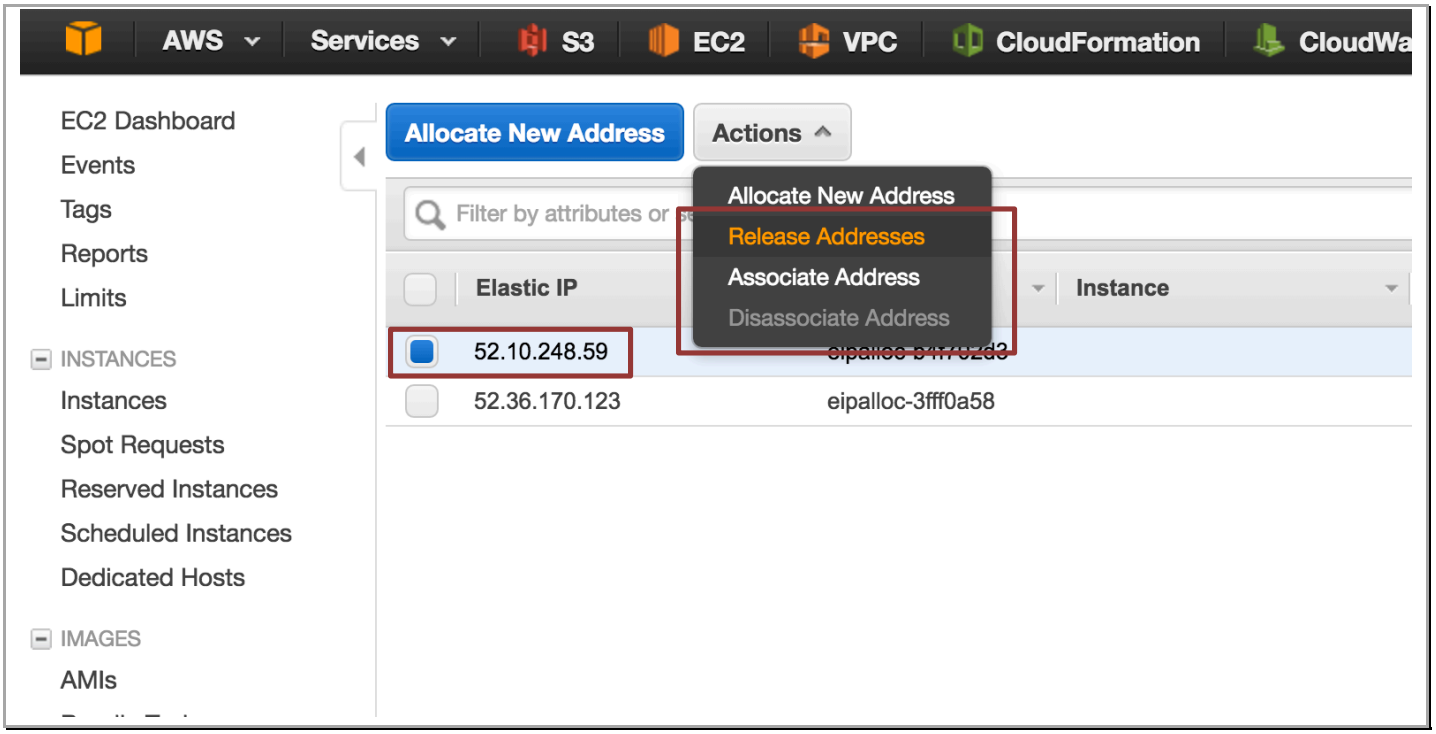
By default, each AWS account has a 5 elastic IP (EIP) limit per region unless a limit increase has been requested (via an AWS support ticket). In order to launch this template, you will need two EIPs. To check any allocated or associated EIPs, on the AWS console click on **EC2:**



And click on Elastic IPs:



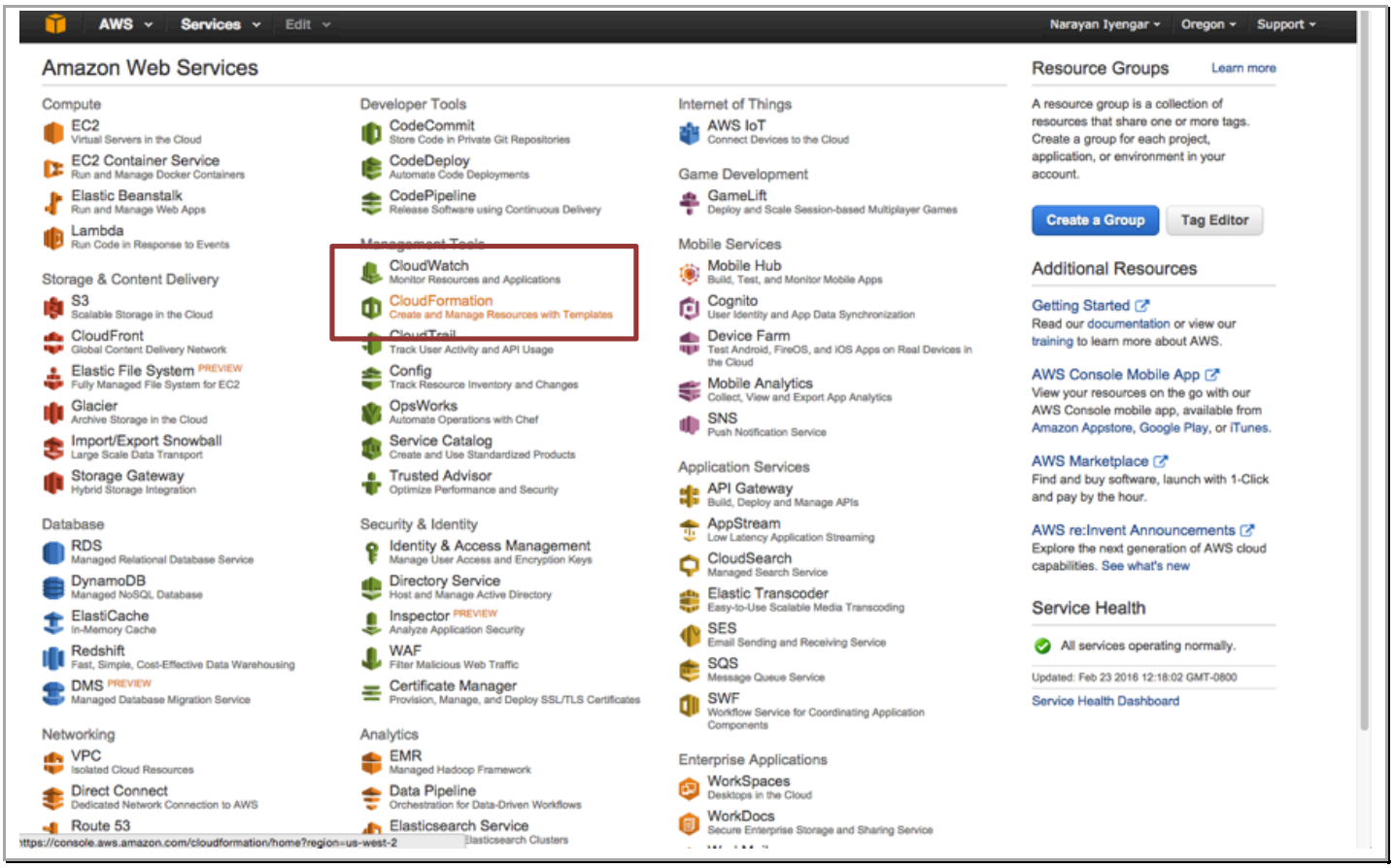
If there are no EIPs allocated, proceed to Section 4. If there are more than 3 EIPs allocated and you have not requested an EIP limit increase, the template launch will fail. You can either release an EIP or request a limit increase via an AWS support ticket. In order to release an allocated EIP, simply click on the EIP and click **Actions**, **Release Addresses**



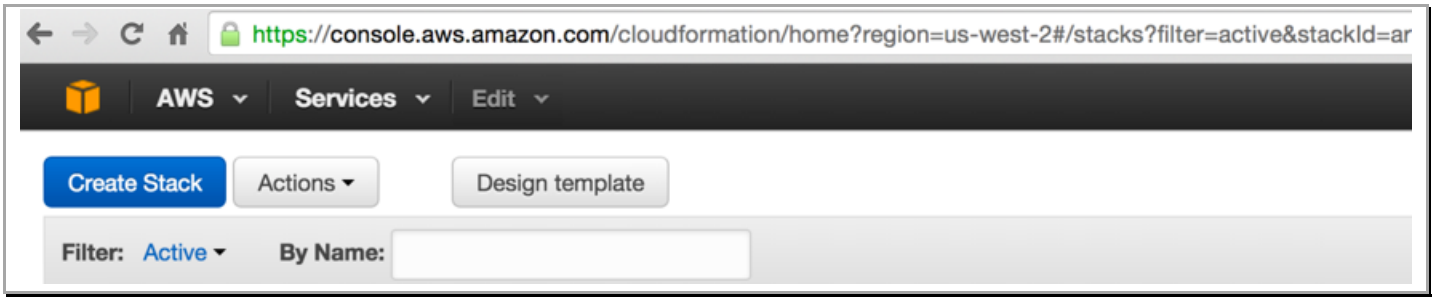
If the EIP is associated with an instance, you will need to disassociate the address first and then release the address. If you are relying on the address for other work, please be aware that disassociating the address and releasing the address could cause work disruption.

5. Launch The CFT

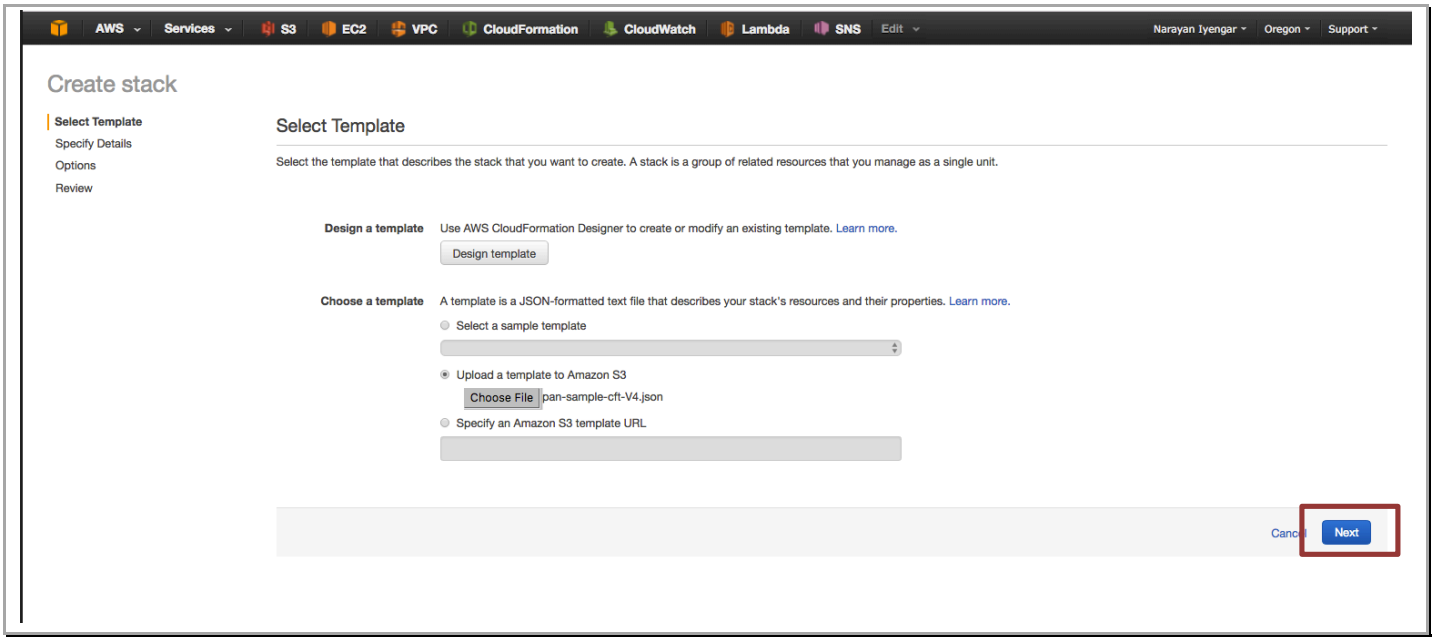
Login in to the AWS console https://console.aws.amazon.com and click on **CloudFormation**



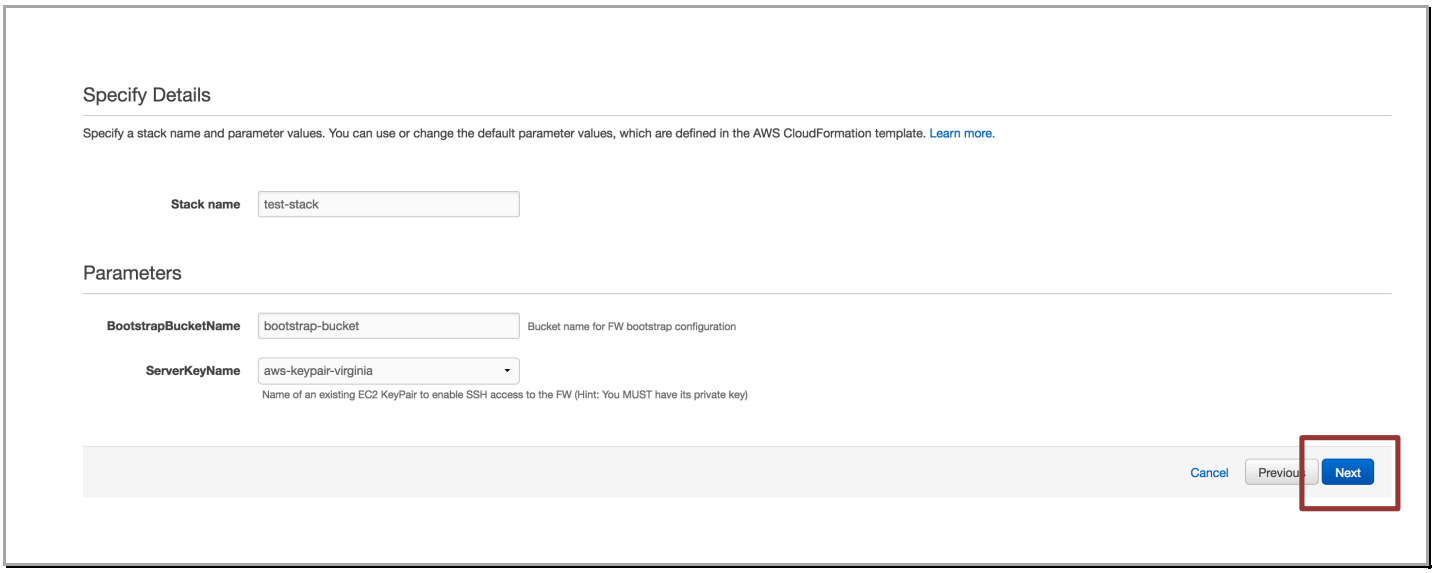
Click **Create Stack**:



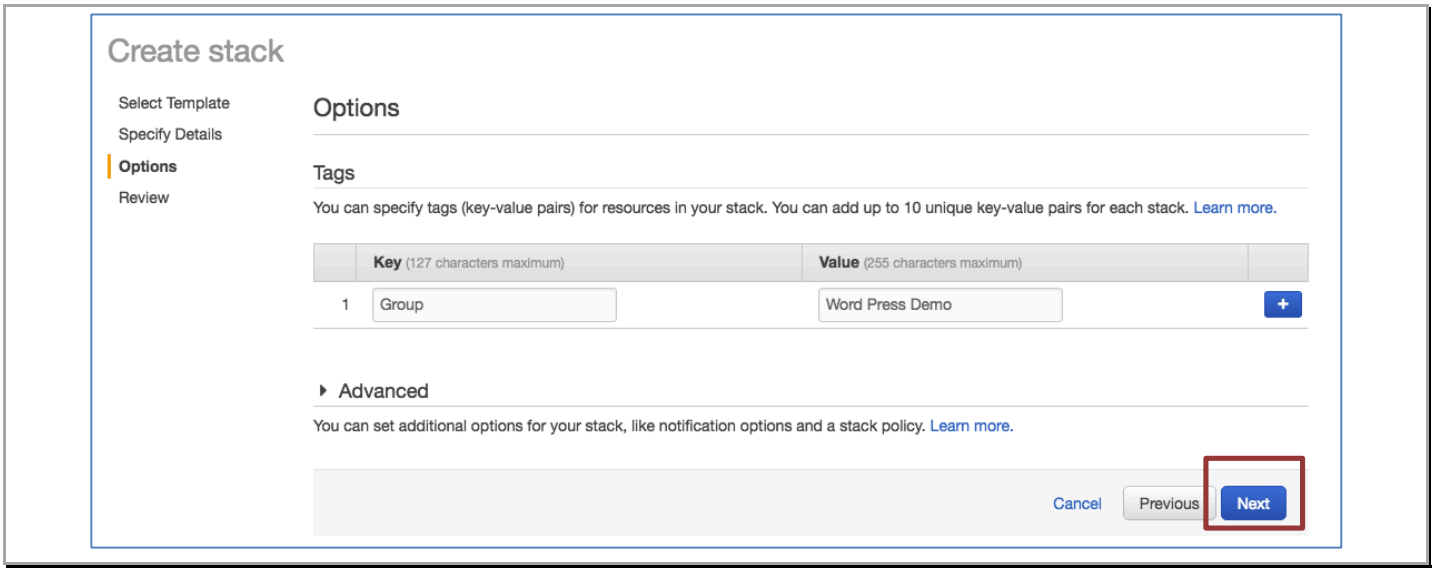
Select "**Choose File**" and select the template downloaded in Section 4.6 into the box and click **Next**:



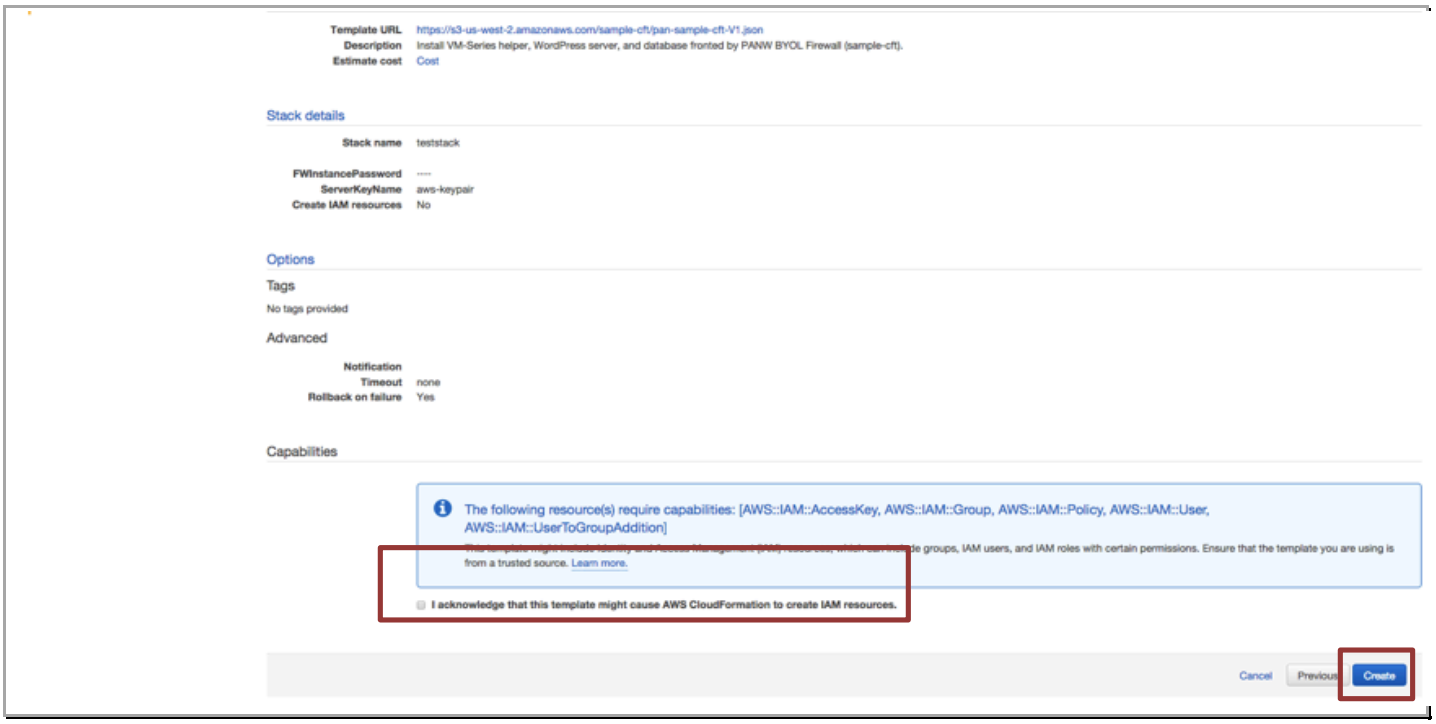
In the next screen specify a "**Stack Name**". This can be anything. In the **Parameters** section, specify the bucket name of the bootstrapping bucket that was created in section 3.5 and select a **Serverkey** for which you have the private key. Refer to section 2.4 on how to generate a keypair. Once satisfied, click **Next**.



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

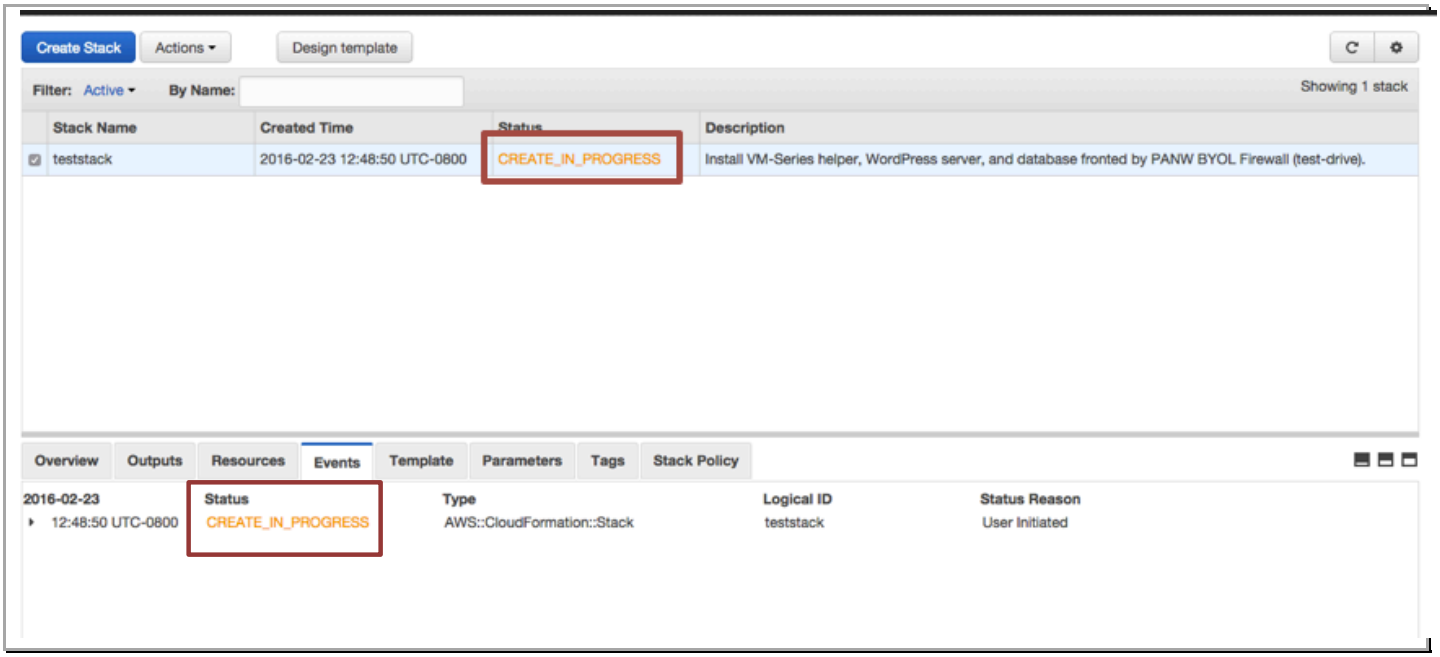


Next, review and check acknowledge at the bottom and click **Create**.

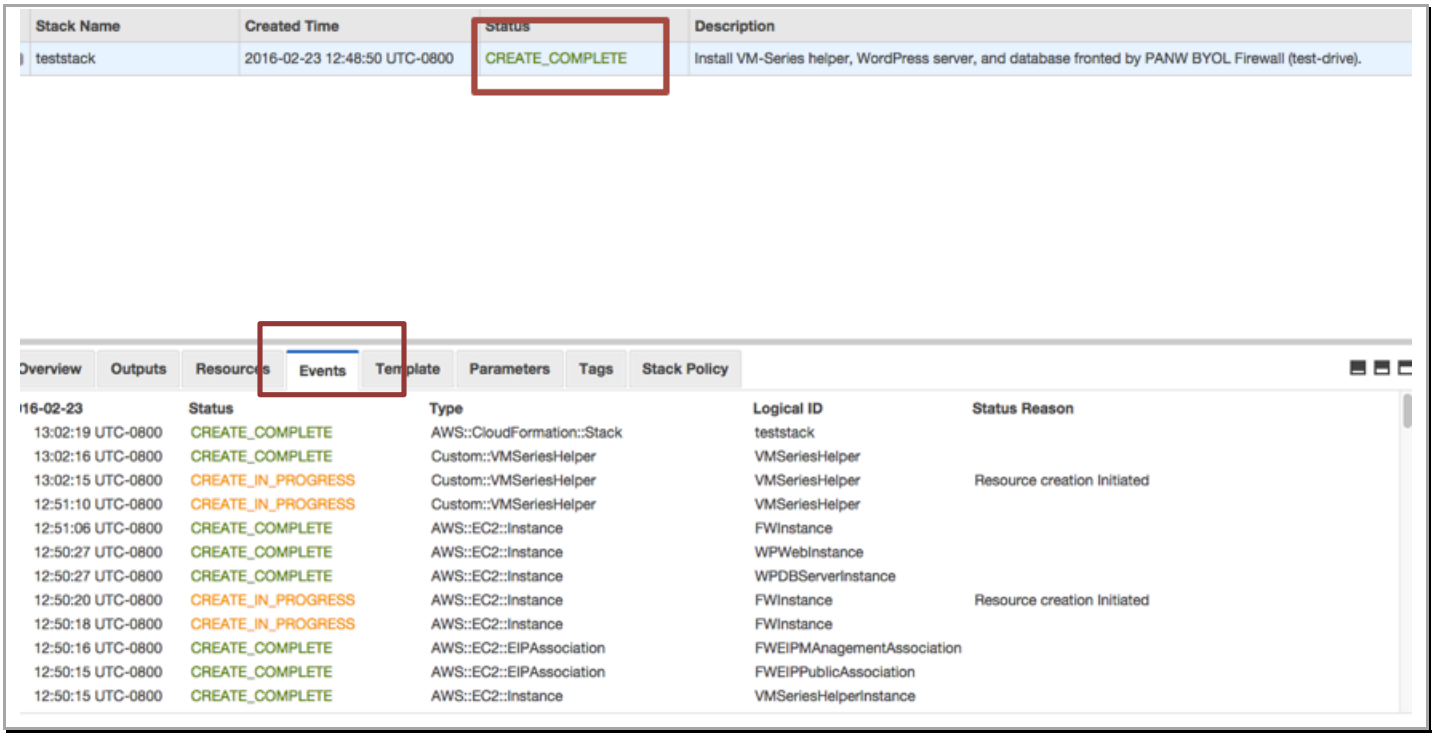


Once launched you should be able to monitor the stack creation progress in the next screen by clicking on the **Events** tab.

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

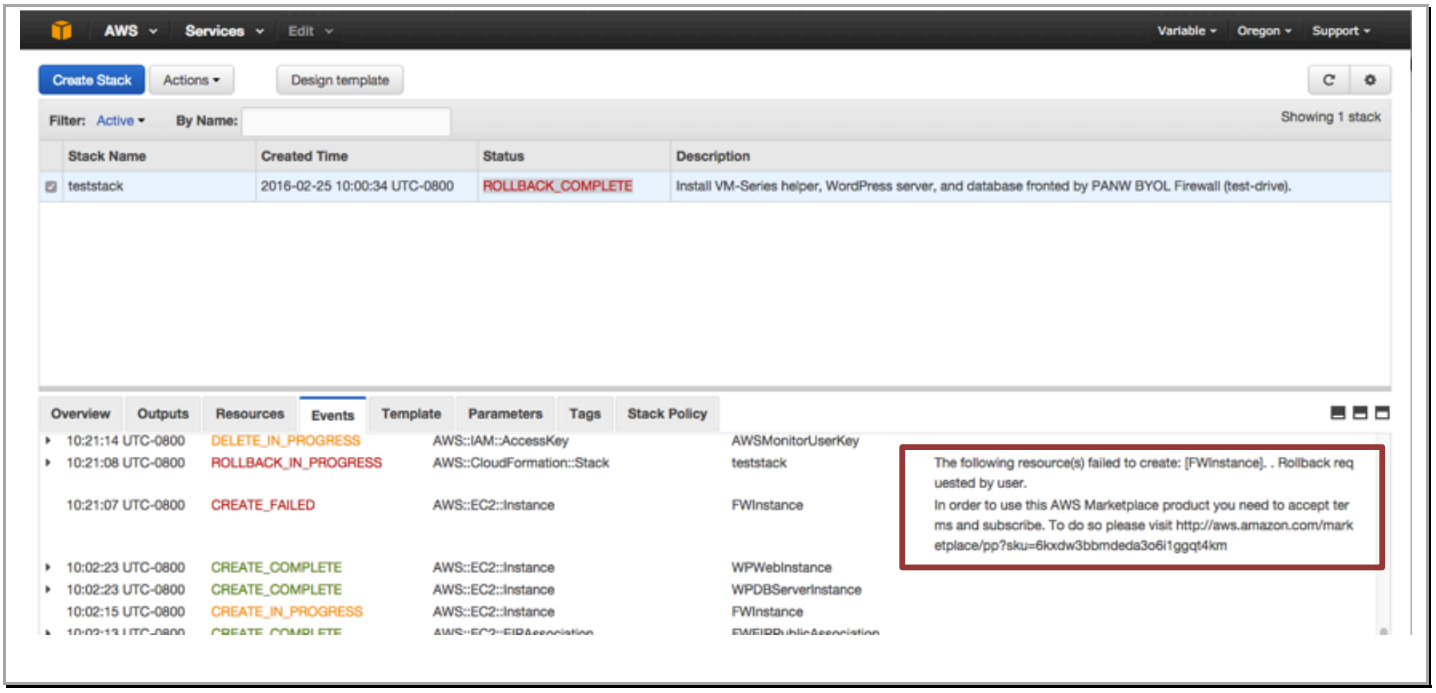


If the CFT was successfully launched, you should see an event as below:



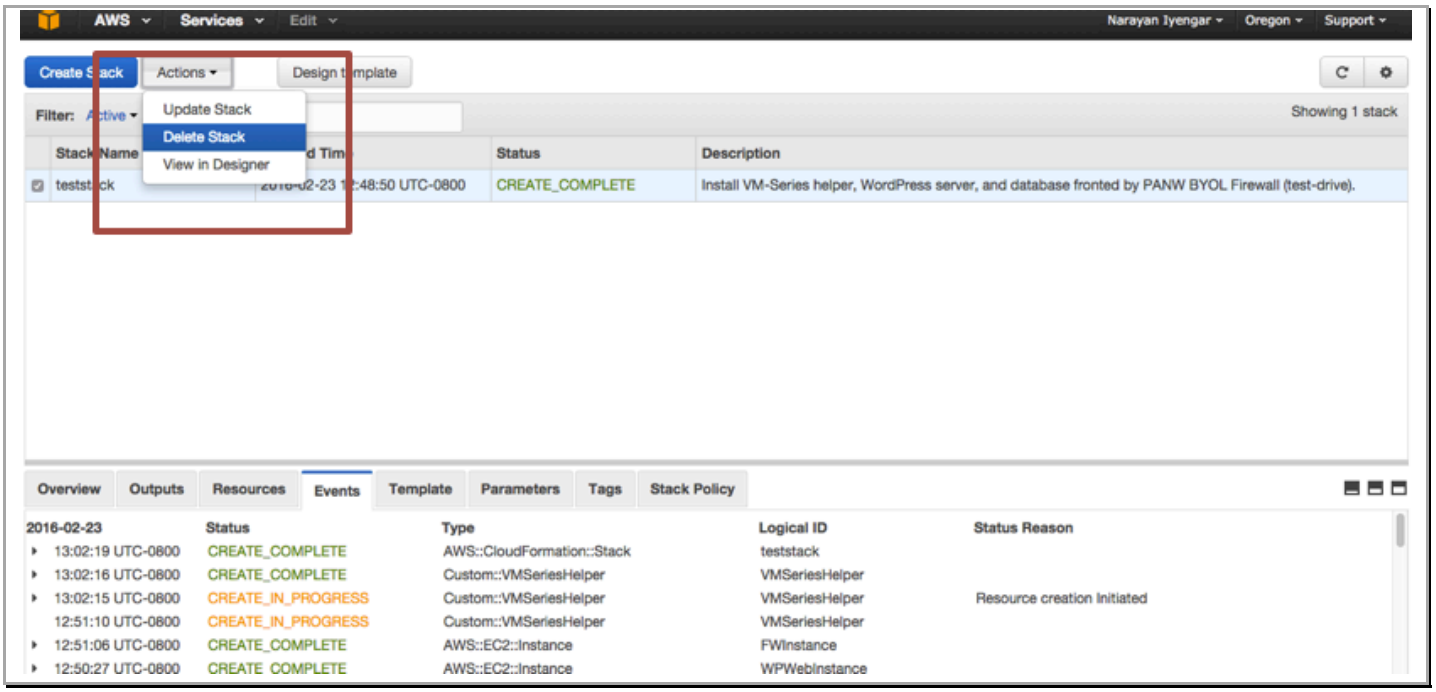
If there were any errors during the creation of the stack, you will need to drill down to the specific event in the **Events** tab and **Outputs** tab to debug and then create a new stack after fixing any errors.

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



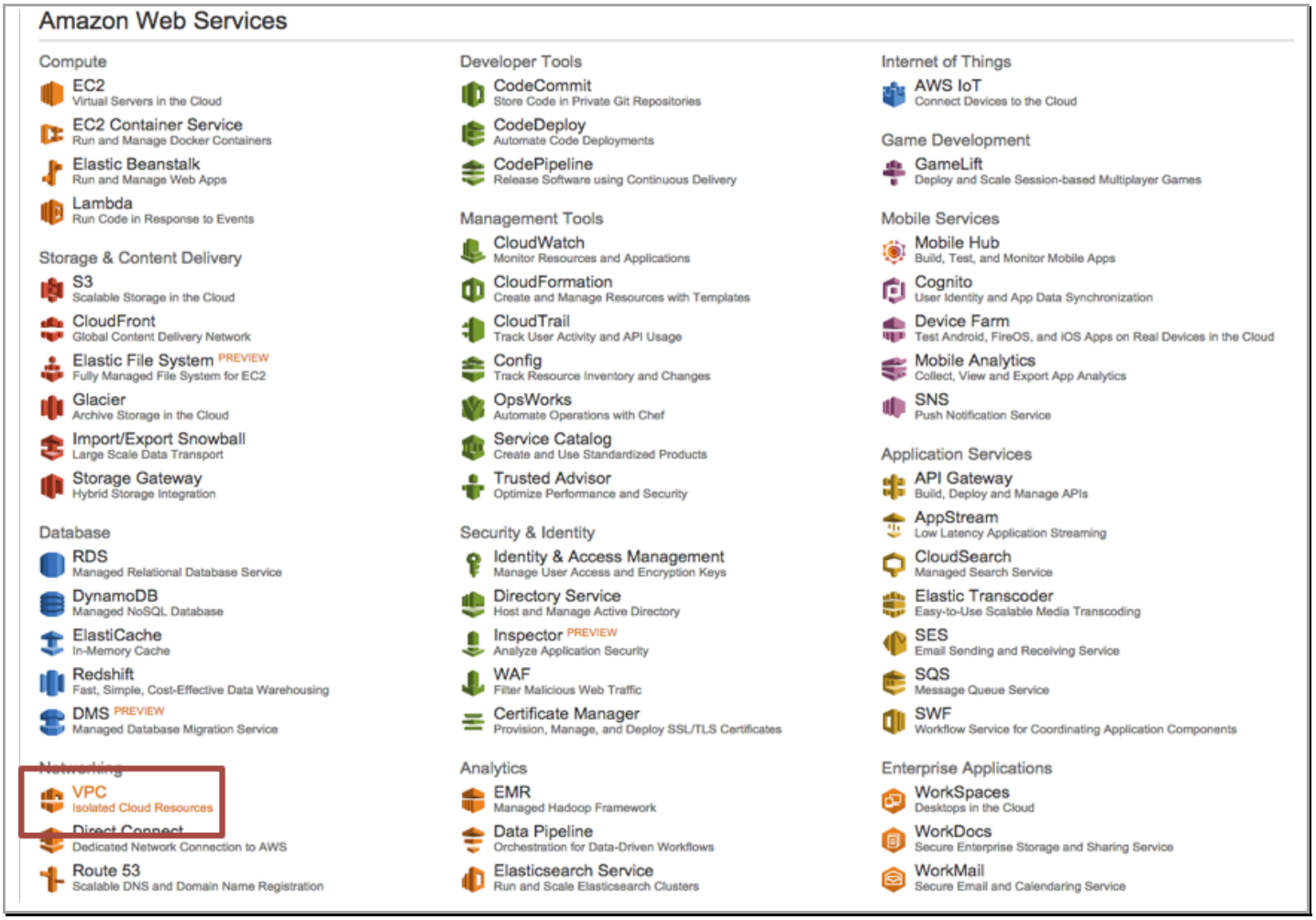
Refer to section 2.3 to review and accept the EULA for the VM-Series NGFW

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

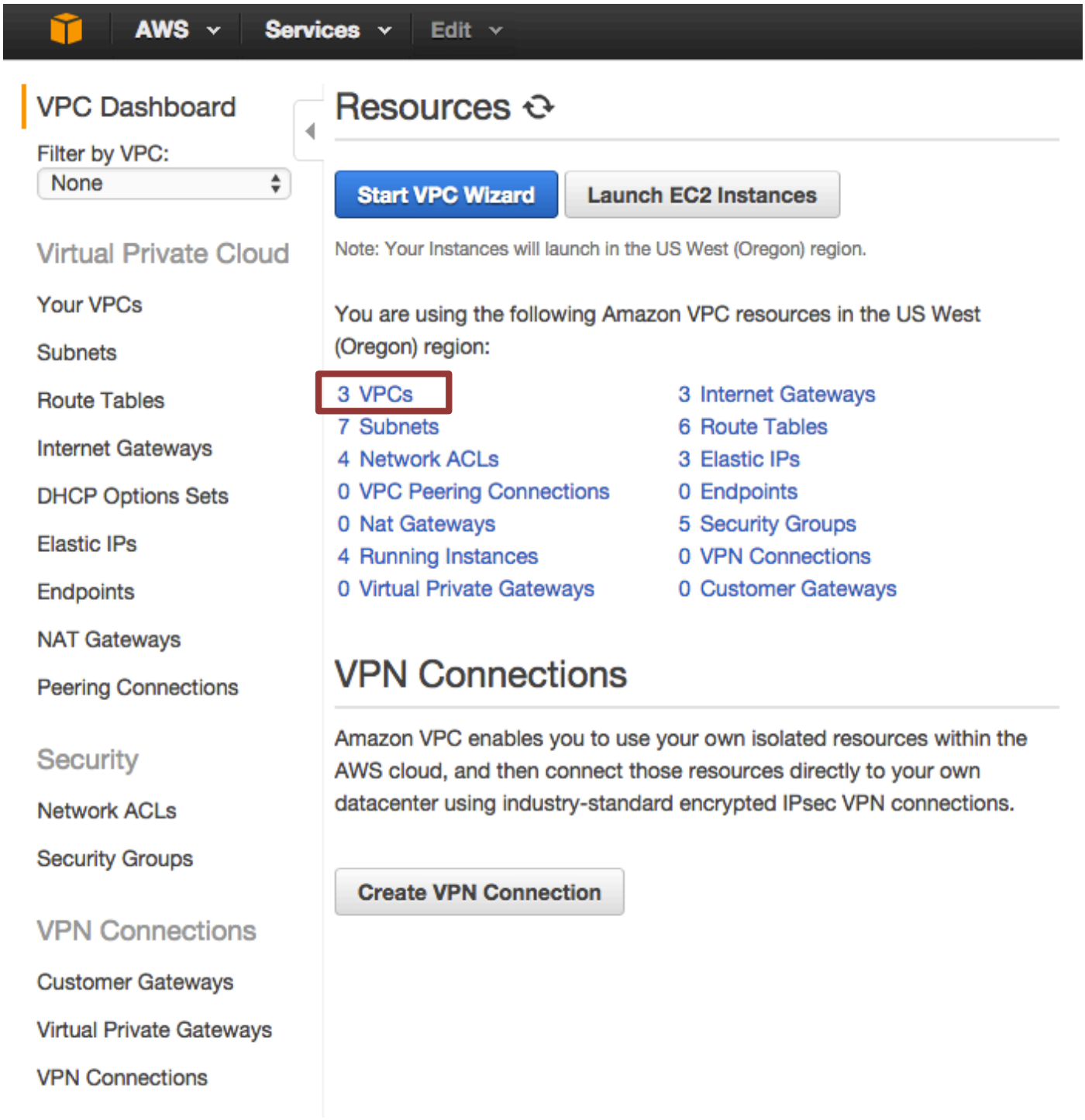


6. Review what was created

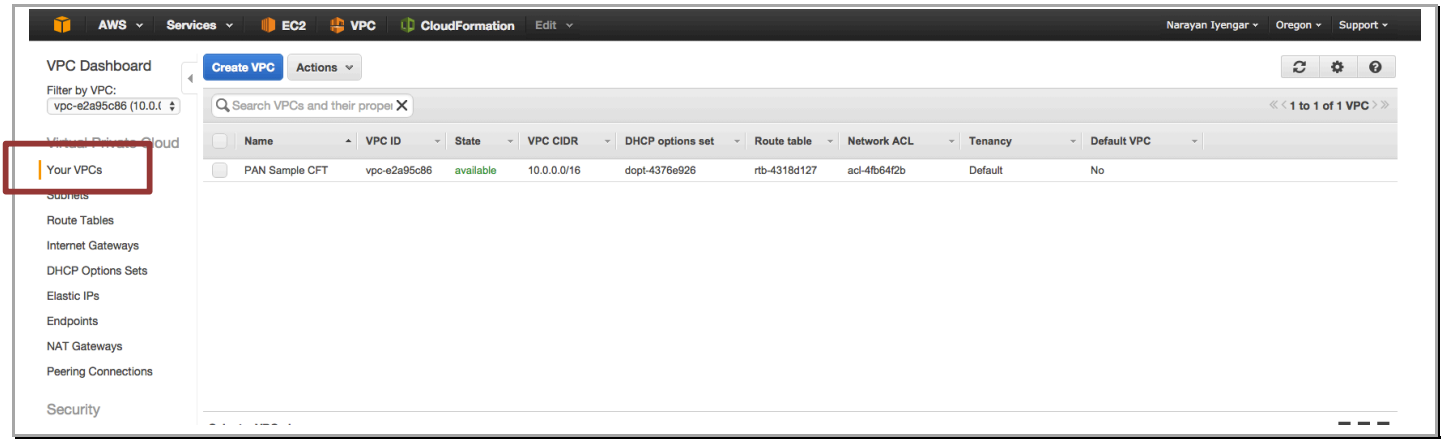
Let's review what the CFT has launched. The newly created VPC can be accessed via:


Amazon Web Services
Compute
EC2
Virtual Servers in the Cloud
EC2 Container Service
Run and Manage Docker Containers
Elastic Beanstalk
Run and Manage Web Apps
Lambda
Run Code in Response to Events
Storage & Content Delivery
S3
Scalable Storage in the Cloud
CloudFront
Global Content Delivery Network
Elastic File System PREVIEW
Fully Managed File System for EC2
Glacier
Archive Storage in the Cloud
Import/Export Snowball
Large Scale Data Transport
Storage Gateway
Hybrid Storage Integration
Database
RDS
Managed Relational Database Service
DynamoDB
Managed NoSQL Database
ElastiCache
In-Memory Cache
Redshift
Fast, Simple, Cost-Effective Data Warehousing
DMS PREVIEW
Managed Database Migration Service
VPC
Isolated Cloud Resources
Direct Connect
Dedicated Network Connection to AWS
Route 53
Scalable DNS and Domain Name Registration
Developer Tools
CodeCommit
Store Code in Private Git Repositories
CodeDeploy
Automate Code Deployments
CodePipeline
Release Software using Continuous Delivery
Management Tools
CloudWatch
Monitor Resources and Applications
CloudFormation
Create and Manage Resources with Templates
CloudTrail
Track User Activity and API Usage
Config
Track Resource Inventory and Changes
OpsWorks
Automate Operations with Chef
Service Catalog
Create and Use Standardized Products
Trusted Advisor
Optimize Performance and Security
Security & Identity
Identity & Access Management
Manage User Access and Encryption Keys
Directory Service
Host and Manage Active Directory
Inspector PREVIEW
Analyze Application Security
WAF
Filter Malicious Web Traffic
Certificate Manager
Provision, Manage, and Deploy SSL/TLS Certificates
Analytics
EMR
Managed Hadoop Framework
Data Pipeline
Orchestration for Data-Driven Workflows
Elasticsearch Service
Run and Scale Elasticsearch Clusters
Internet of Things
AWS IoT
Connect Devices to the Cloud
Game Development
GameLift
Deploy and Scale Session-based Multiplayer Games
Mobile Services
Mobile Hub
Build, Test, and Monitor Mobile Apps
Cognito
User Identity and App Data Synchronization
Device Farm
Test Android, FireOS, and iOS Apps on Real Devices in the Cloud
Mobile Analytics
Collect, View and Export App Analytics
SNS
Push Notification Service
Application Services
API Gateway
Build, Deploy and Manage APIs
AppStream
Low Latency Application Streaming
CloudSearch
Managed Search Service
Elastic Transcoder
Easy-to-Use Scalable Media Transcoding
SES
Email Sending and Receiving Service
SQS
Message Queue Service
SWF
Workflow Service for Coordinating Application Components
Enterprise Applications
WorkSpaces
Desktops in the Cloud
WorkDocs
Secure Enterprise Storage and Sharing Service
WorkMail
Secure Email and Calendaring Service

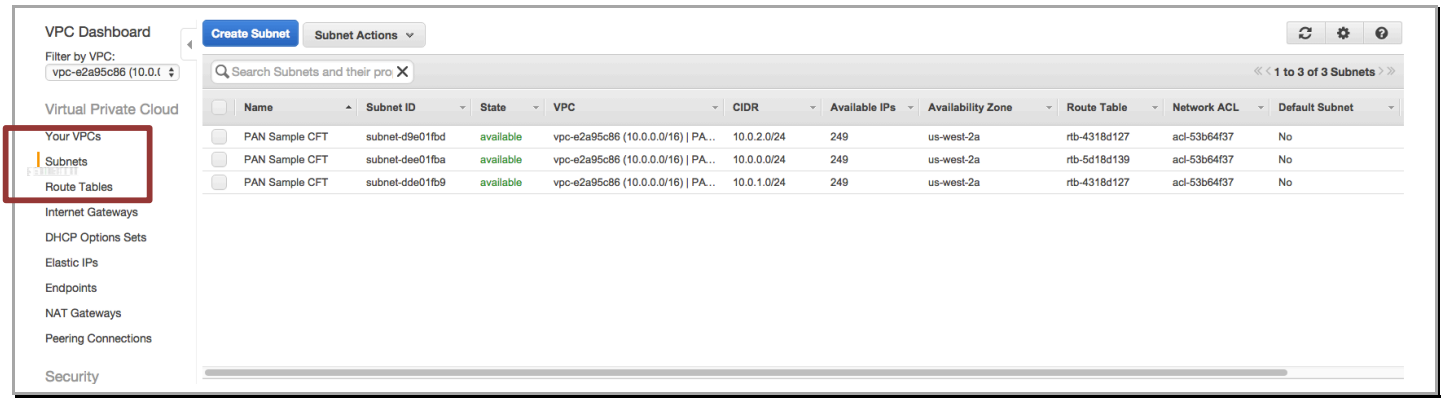
Here you should see all VPCs created in your account:



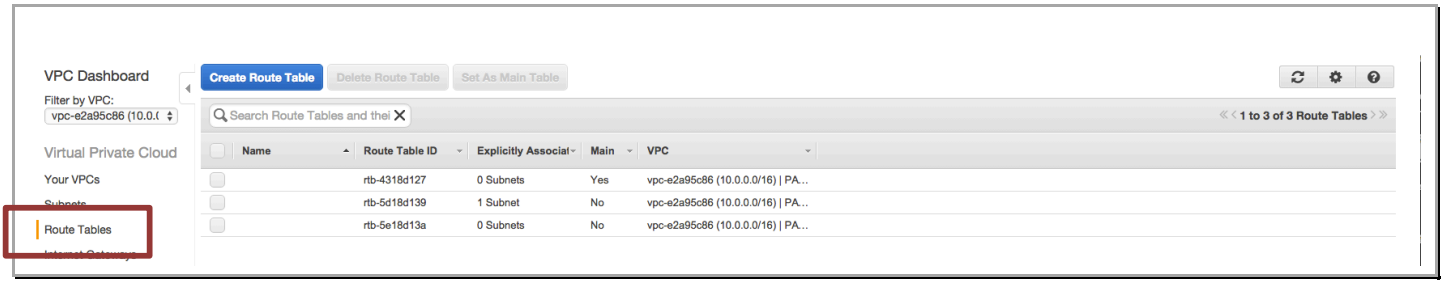
Here is the sample **VPC**:



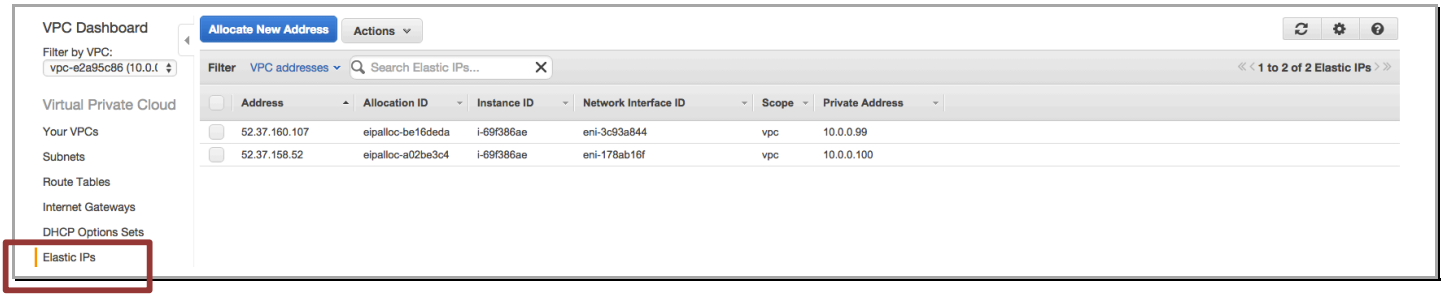
On the left you can review **subnets**:



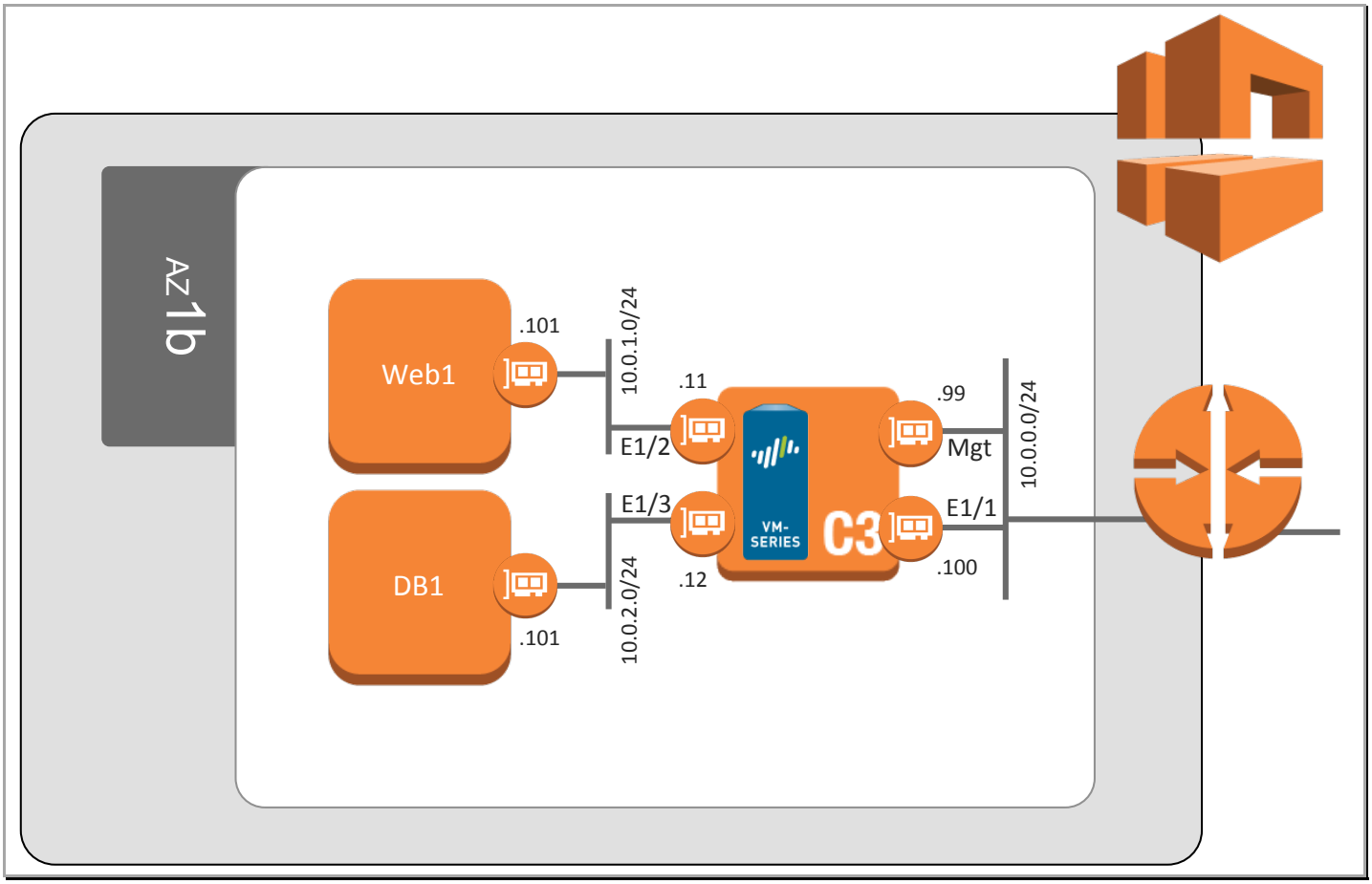
Route tables:



And **Elastic IPs (EIPs)**:



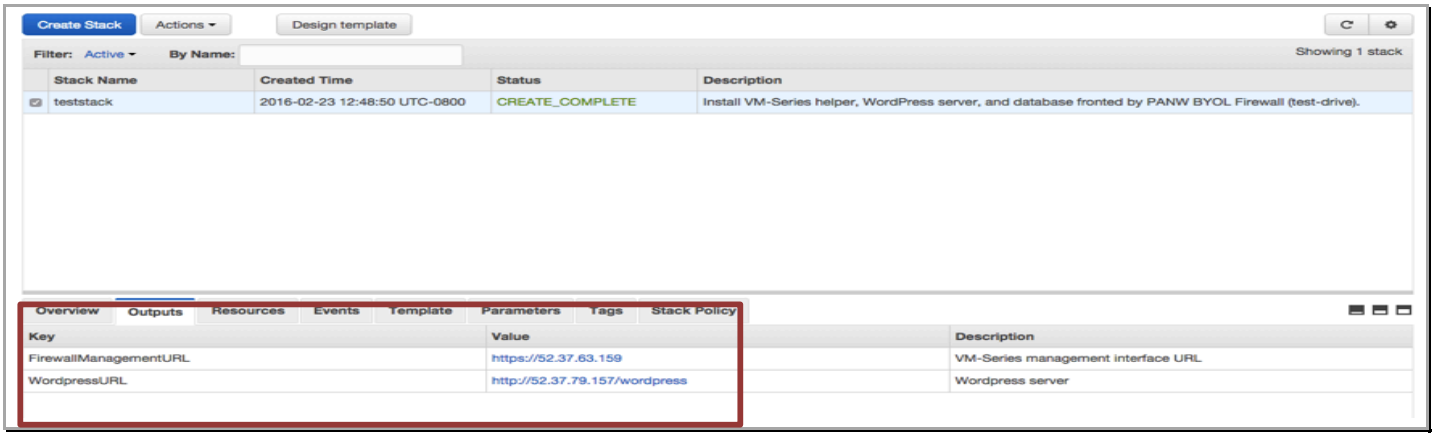
All of this matches the topology shown previously:



7. Access the VM-Series Firewall

NOTE: 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.

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



You should now be able to login to the firewall using the **username: admin** and password: **paloalto**

8. Review the VM-Series WebUI

In this activity, you will:

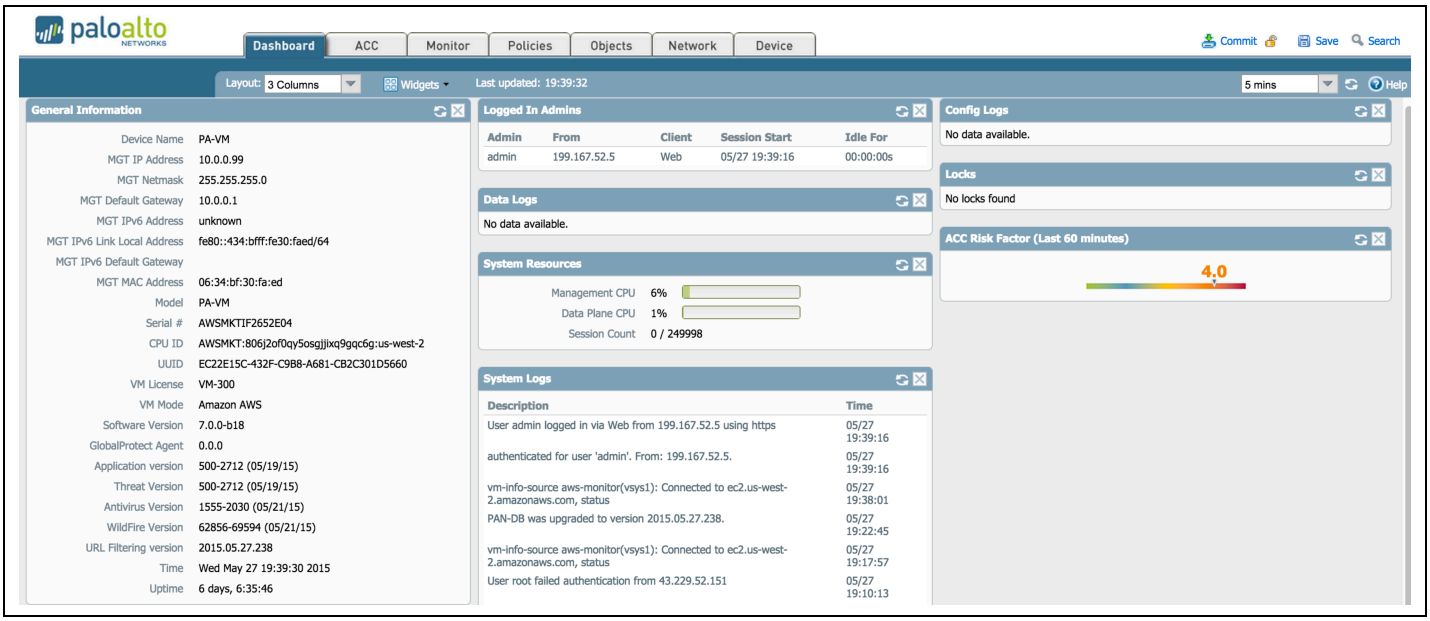
- Login to the VM-Series firewall
- Review key portions of the firewall configurations

Task 1 – Login and Dashboard summary

Using the browser of your choice, connect to the management interface of the new firewall using the first URL in the outputs tab and login with the username ***admin*** and the password ***paloalto***.

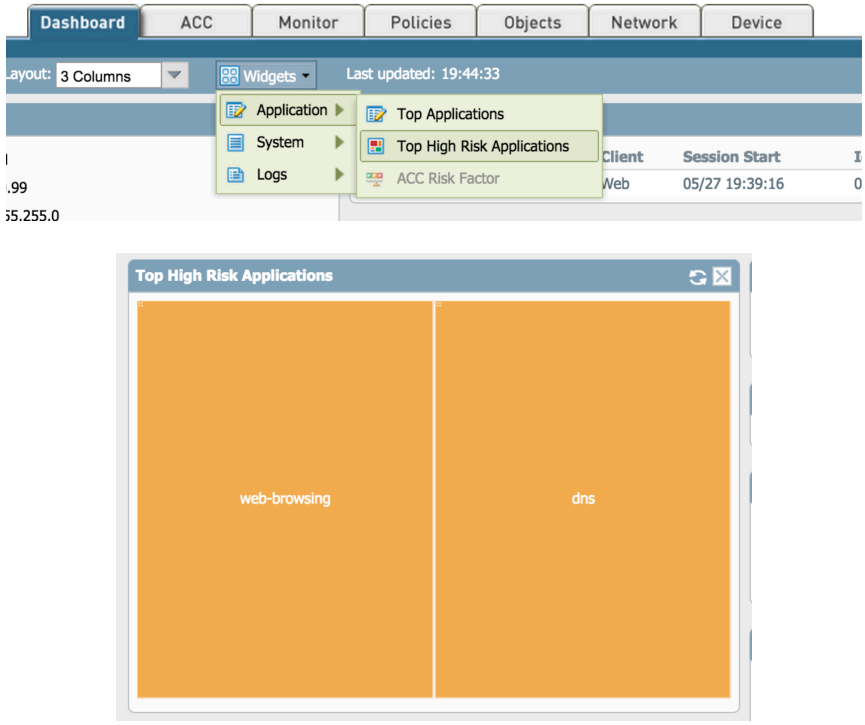
Note: If your browser gives you a certificate warning, you can safely acknowledge it and proceed.

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.

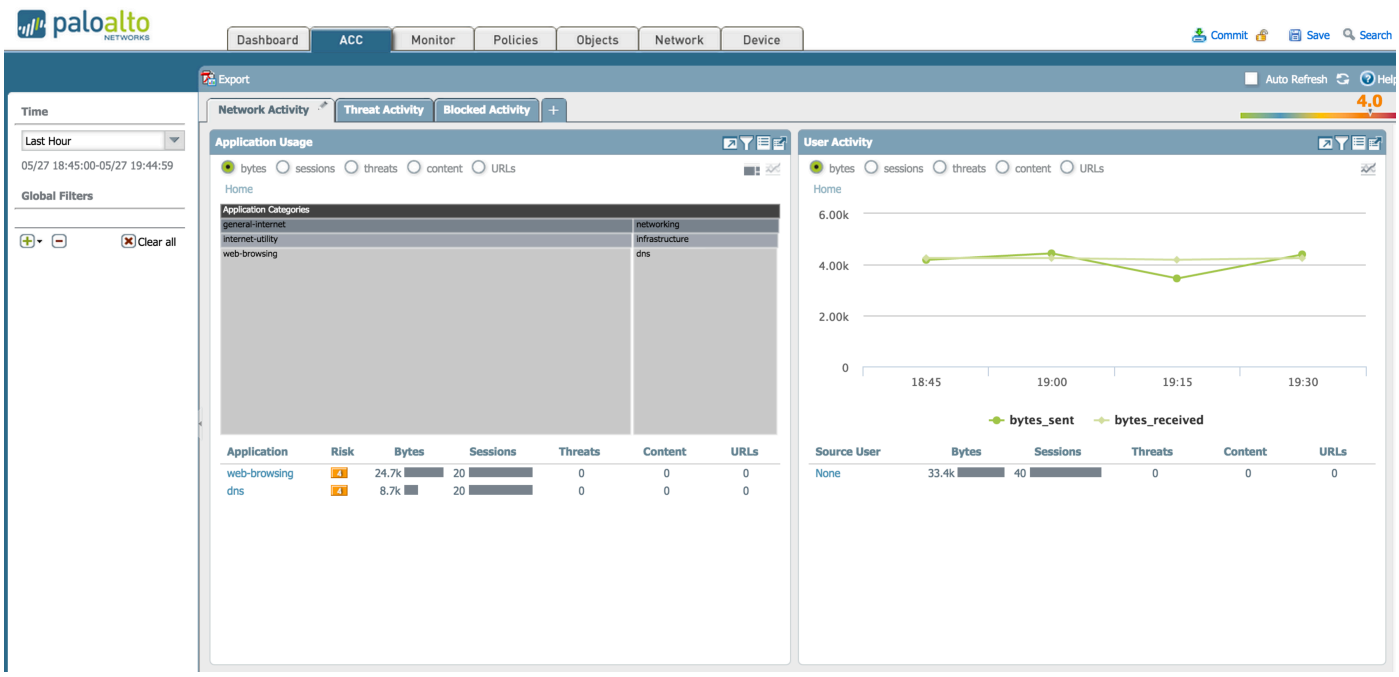


Task 2 – Review PAN-OS WebUI – Application Command Center (ACC)

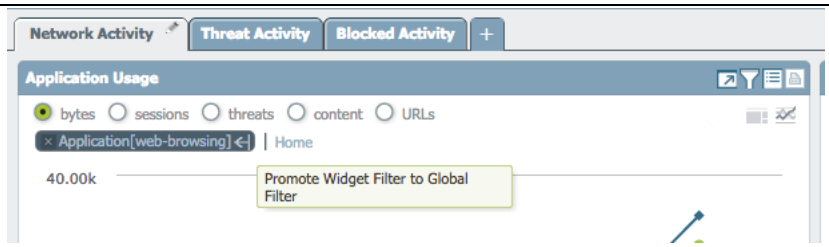
The ACC provides you with a widget-based summary of the applications, the content within, and who the user is over a given time period [default is 1 hour]. With the ACC, you can see the contextual linkage between the application and the content, which allows you to make more informed security decisions.

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.

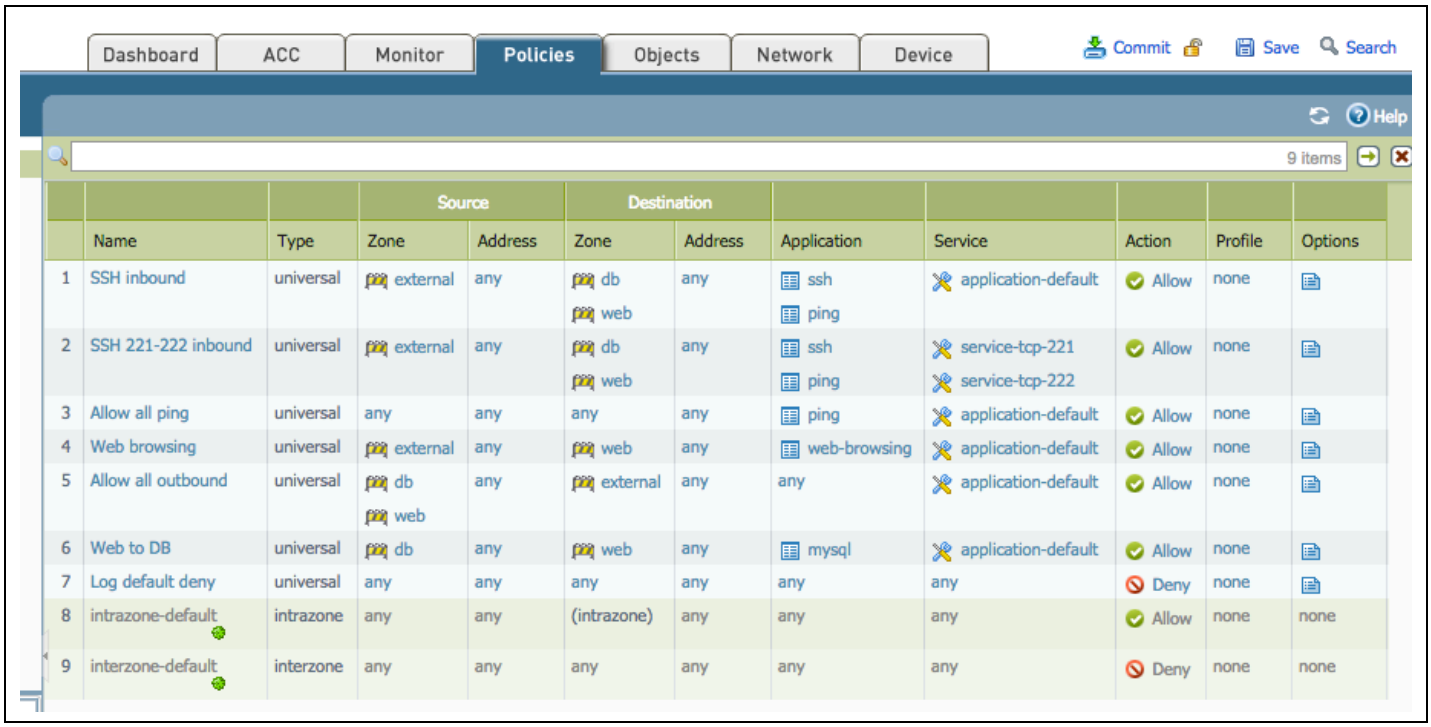


[Optional] Scroll through the information displayed in the ***Network Activity*** Tab. Customize one of the tabs, create/add a new tab.

Task 3 – Review PAN-OS WebUI – Security Policies

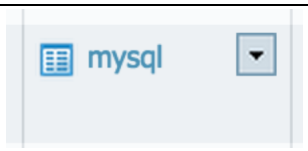
The Policies tab is a where you will define all of your policies. The default view will be your security policies, all of which can be based on the application, the content within, and the user. As shown along the left side of the image, additional policies can be defined for actions such as NAT, Decryption,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

Select the ***Policies*** tab.



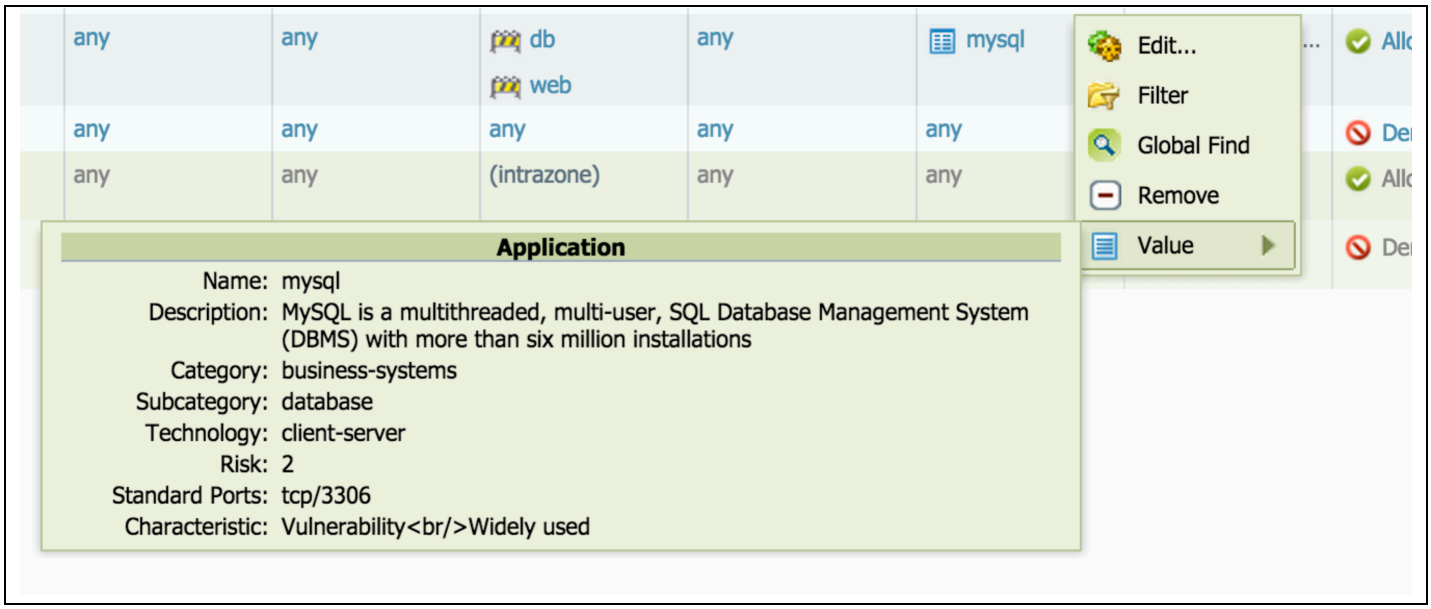
			Source		Destination						
	Name	Type	Zone	Address	Zone	Address	Application	Service	Action	Profile	Options
1	SSH inbound	universal	external	any	db web	any	ssh ping	application-default	Allow	none	
2	SSH 221-222 inbound	universal	external	any	db web	any	ssh ping	service-tcp-221 service-tcp-222	Allow	none	
3	Allow all ping	universal	any	any	any	any	ping	application-default	Allow	none	
4	Web browsing	universal	external	any	web	any	web-browsing	application-default	Allow	none	
5	Allow all outbound	universal	db web	any	external	any	any	application-default	Allow	none	
6	Web to DB	universal	db	any	web	any	mysql	application-default	Allow	none	
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

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.


any
any
db
web
any
mysql
any
any
any
any
any
any
any
(intrazone)
any
any
Edit...
Filter
Global Find
Remove
Value
Application
Name: mysql
Description: MySQL is a multithreaded, multi-user, SQL Database Management System (DBMS) with more than six million installations
Category: business-systems
Subcategory: database
Technology: client-server
Risk: 2
Standard Ports: tcp/3306
Characteristic: Vulnerability
Widely used

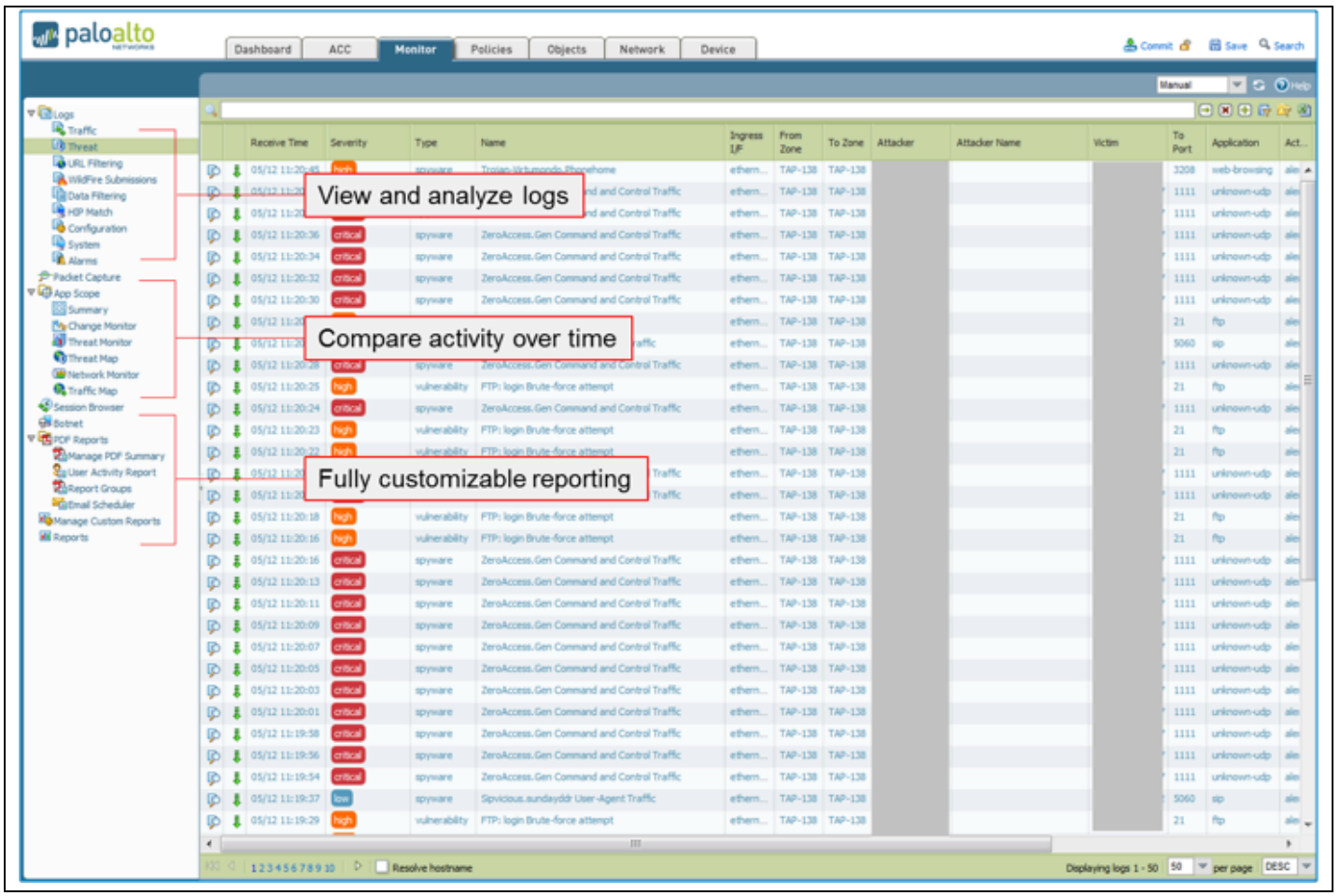
Task 4 – Review PAN-OS WebUI – Monitor tab

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.

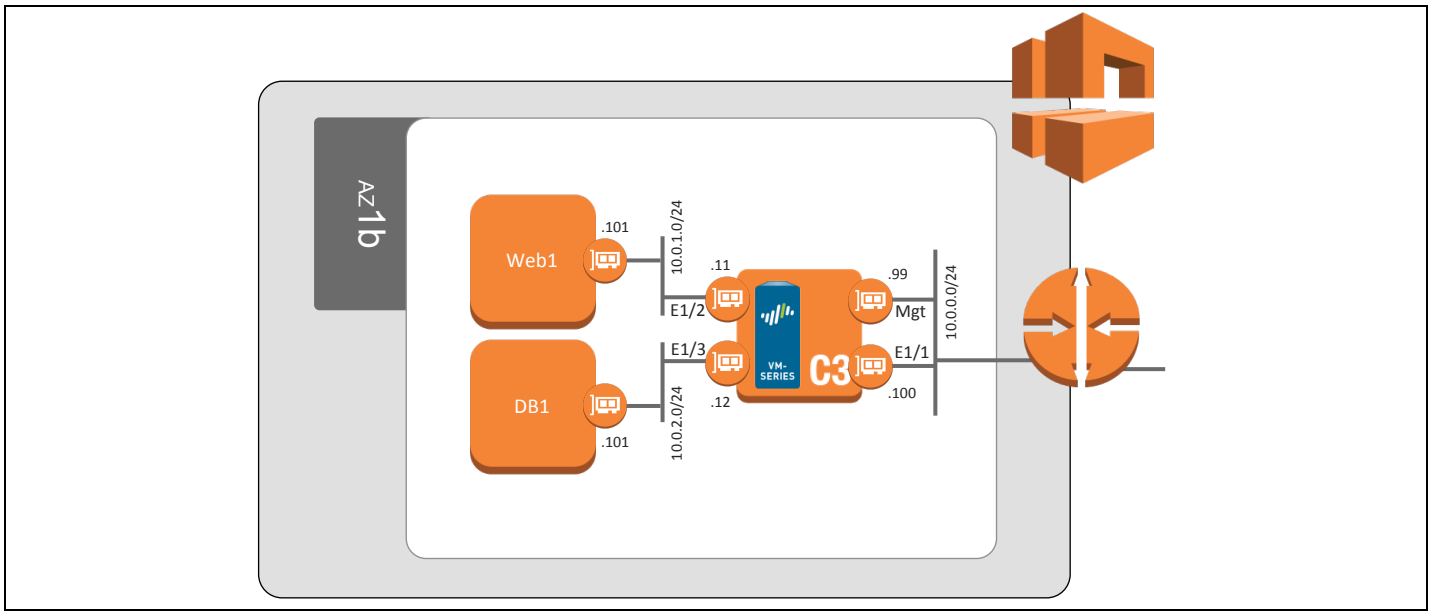
Note: Your firewall is new and doesn't have any data yet so any reports you create at this point will likely be blank. You can return to this step at the end of the lab and create new reports.



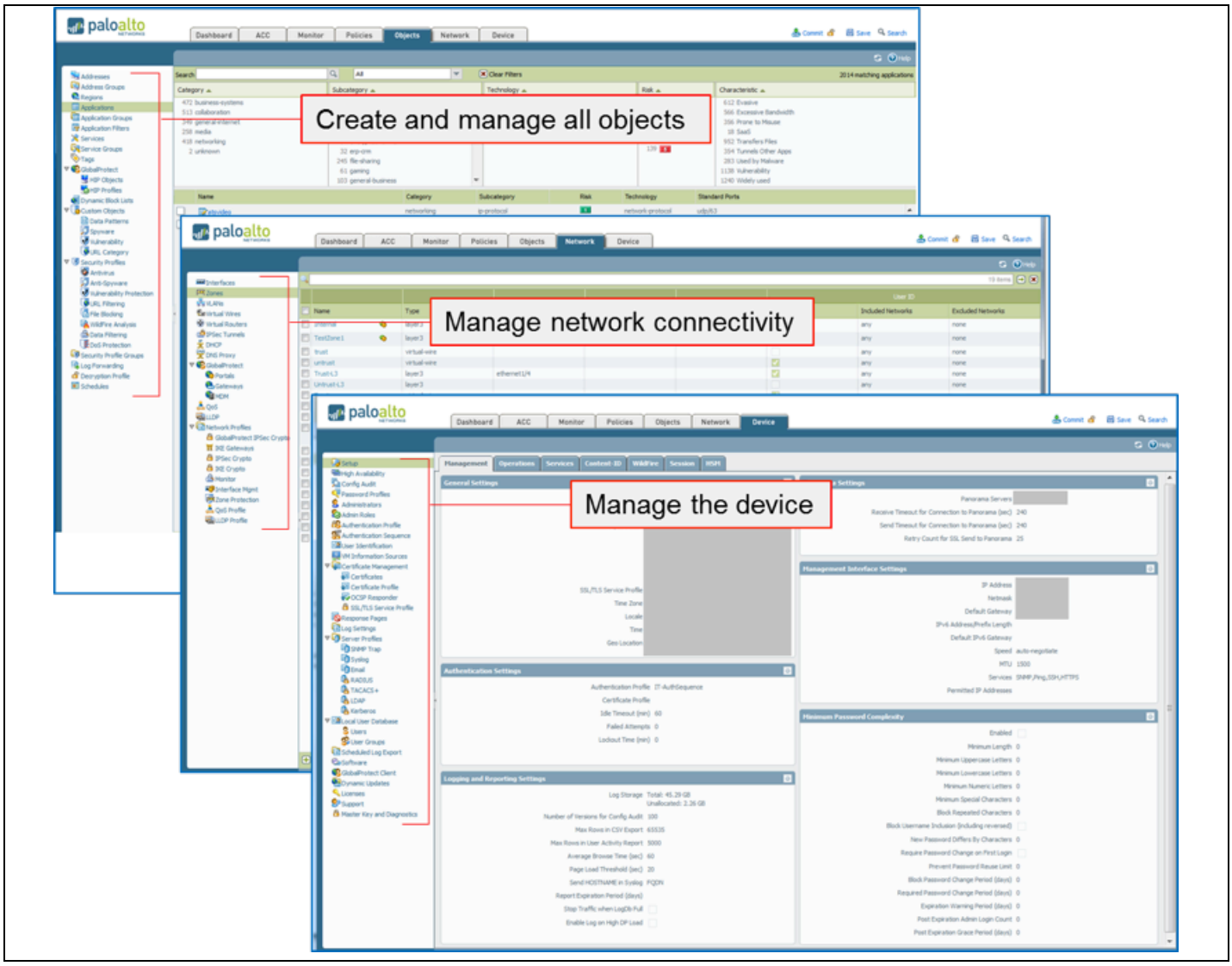
Task 5 – Review the WebUI – Object, Network, Device Tabs

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, etc are managed.


Create and manage all objects
Manage network connectivity
Manage the device

Activity 2 – Safely Enable Applications

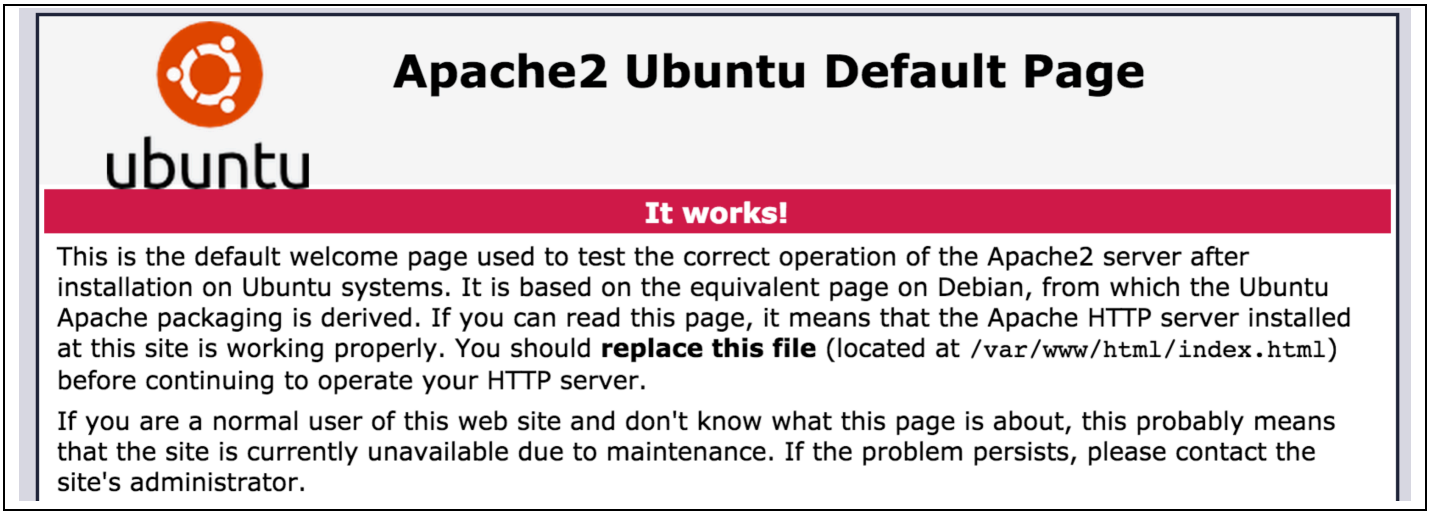
In this activity, you will:

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

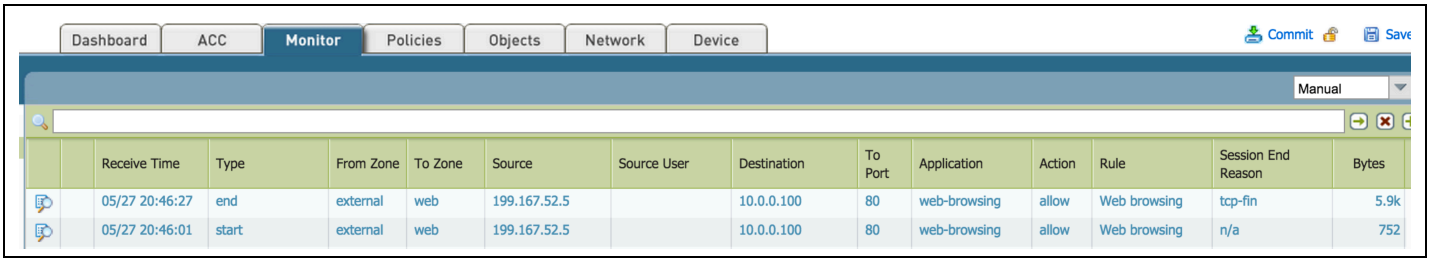
Task 1 – Verify Static Content on Web Server

Using the second URL in the outputs tab in section 7, open a browser tab and browse to the URL http://<<Web Server IP>>/

Note: If your email included ***/wordpress*** in the URL, remove the ***wordpress*** portion for this step.



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

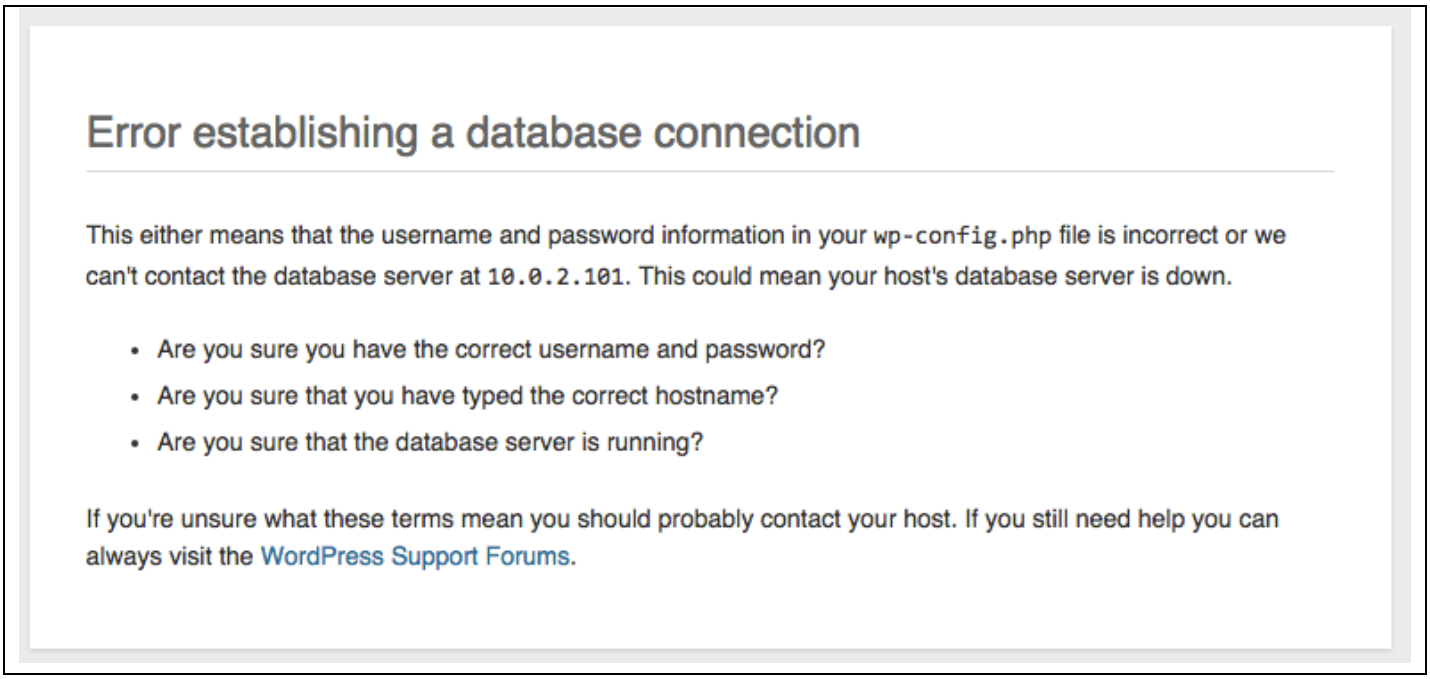


Task 2 – Verify Dynamic Content on Web Server

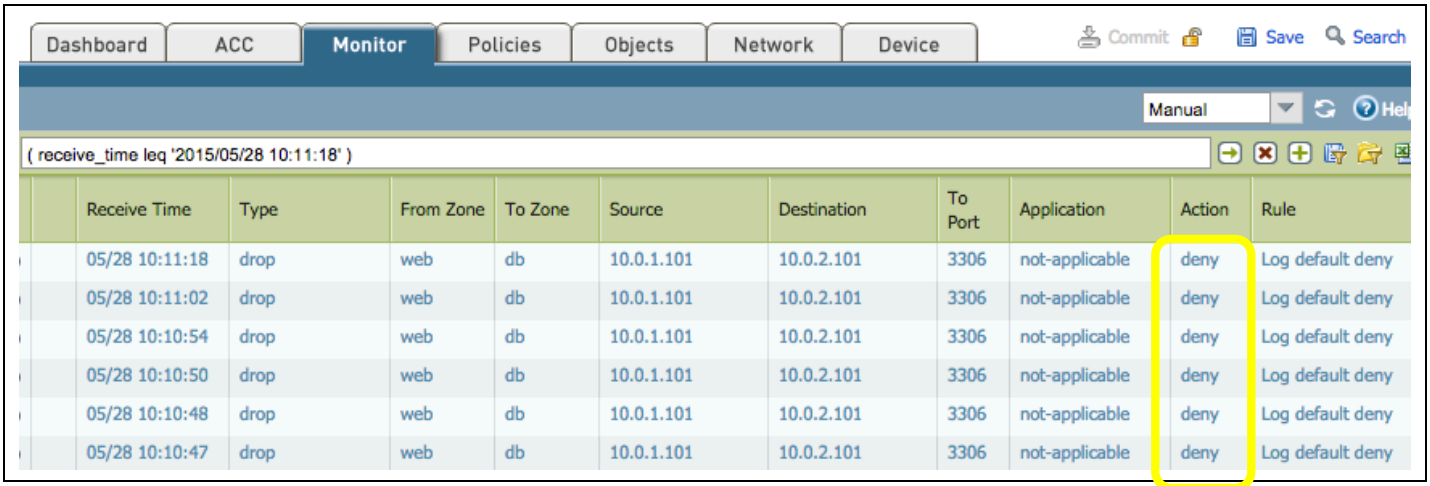
In this task, you will generate a WordPress content request from your web browser that will trigger a database query to the MySQL server. Like many web-based applications, WordPress uses a backend database to create, store, and retrieve dynamic content. You will use the WordPress application to show 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

Note: this will eventually time out but it will take a while. You can proceed with the next step without waiting for the timeout.



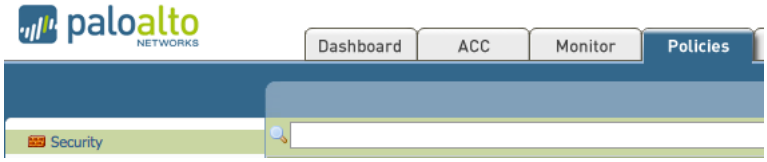
Return to the firewall ***Monitor*** tab and check the firewall logs to troubleshoot the problem.



As you can see, the MySQL traffic (TCP port 3306) is being blocked between the ***web*** zone and the ***db*** zone. Let's look at the security policy to determine the cause.

Task 3 – Allow MySQL on the VM-Series Firewall

Click on the ***Policies*** tab and then click on ***Security*** on the left hand pane if not there already.



Scroll down to the ***Web to DB*** rule (rule 6) and note the Source and Destination zones.

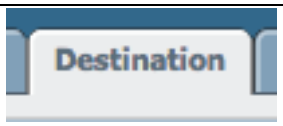
As you can see, *the Source and Destination zones are reversed* and need to be corrected. The Source zone should be ***web*** and the destination zone should be ***db***.

Click on the ***Web to DB*** rule

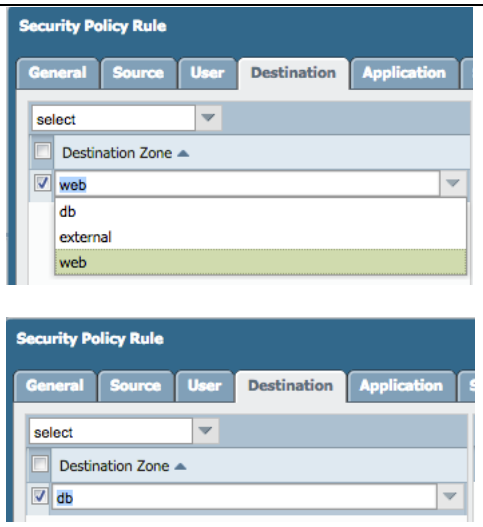
Click on the ***Source***

Click on ***db*** to bring up the pull down menu and change the selection to ***web***

Click on Destination



Click on ***web*** to bring up the pull down menu and change the selection to ***db***

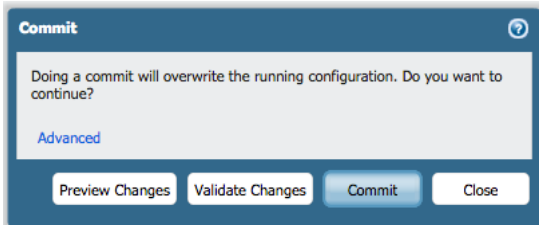


Verify your security rule now resembles the snapshot below. This rule should allow traffic *from* the web zone *to* the db zone.

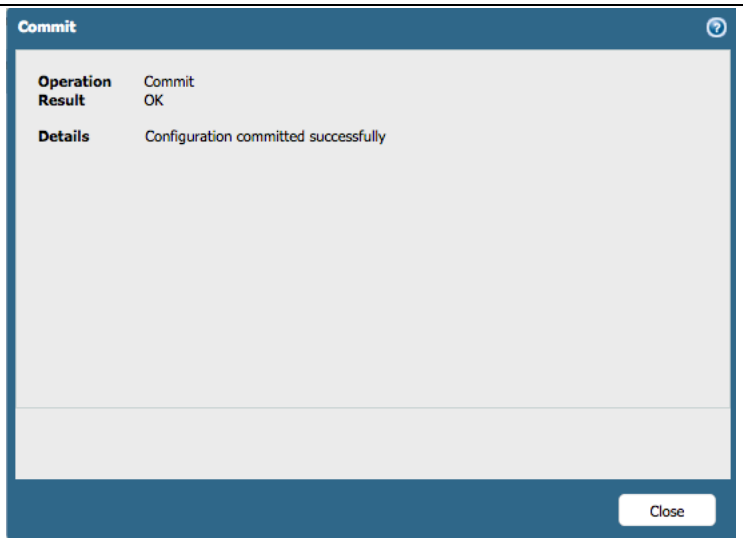
			Source		Destination				
	Name	Type	Zone	Address	Zone	Address	Application	Service	Action
6	Web to DB	universal	web	any	db	any	mysql	application-d...	Allow

Click on ***Commit*** in the upper right.

Click on ***Commit*** in the new dialog window.

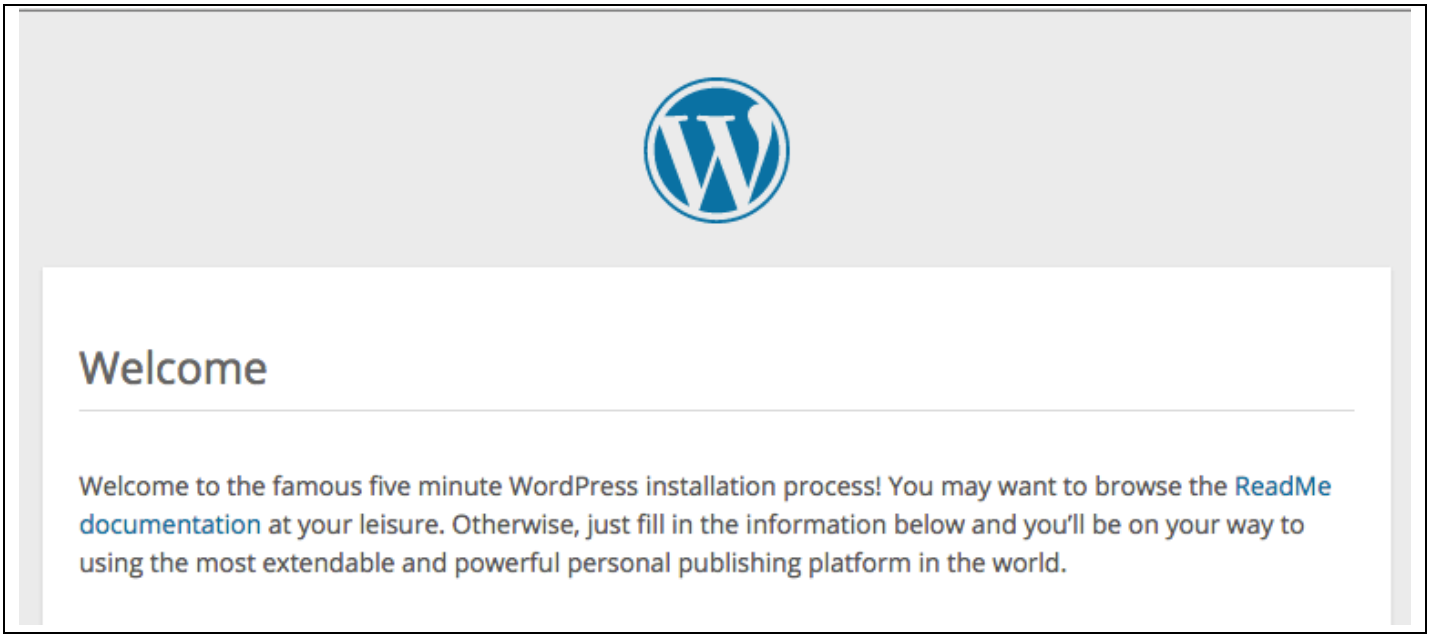


Verify the commit was successful and then click ***Close***.



Task 4 – Re-verify Dynamic Content on Web Server

Return to your WordPress browser tab and click refresh. You should see the initial WordPress welcome screen.



Note: You don't need to actually configure the new WordPress server for the purpose of the test drive. In its initial, un-configured state, it will generate the traffic we need to test the VM-Series firewall.

Return to the firewall traffic log and note the successful traffic. You should be able to see the initial web request, the subsequent MySQL request, and the additional web traffic.

Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule
05/28 10:49:12	start	external	web	199.167.55.50	10.0.0.100	80	web-browsing	allow	Web browsing
05/28 10:49:12	start	external	web	199.167.55.50	10.0.0.100	80	web-browsing	allow	Web browsing
05/28 10:49:12	start	external	web	199.167.55.50	10.0.0.100	80	web-browsing	allow	Web browsing
05/28 10:49:12	start	external	web	199.167.55.50	10.0.0.100	80	web-browsing	allow	Web browsing
05/28 10:49:12	start	external	web	199.167.55.50	10.0.0.100	80	web-browsing	allow	Web browsing
05/28 10:49:12	start	web	db	10.0.1.101	10.0.2.101	3306	mysql	allow	Web to DB
05/28 10:49:12	start	external	web	199.167.55.50	10.0.0.100	80	web-browsing	allow	Web browsing

End of Activity 2

Activity 3 – Safe Application Enablement

In this activity, you will:

- Generate two simulated east/west (web tier to database tier) attacks
- Monitor the firewall logs to see the results of the attacks

Task 1 – Attempt to SSH from the web server to the DB server

This task will simulate a compromised web server that is being used to attack the database. 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.

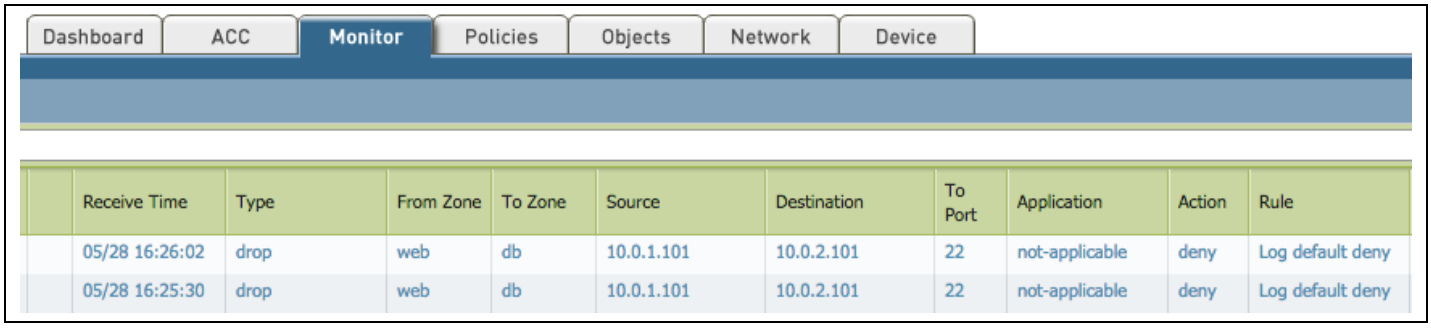
Because the Palo Alto Networks VM-Series firewall has visibility of traffic between the web and database server (east/west traffic), it can detect and automatically block the attacker's attempt to compromise other resources.

Browse to the SQL attack web page at http://<<Web Server IP>>/sql-attack.html

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.

LAUNCH WEB TO DB SSH ATTEMPT

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.

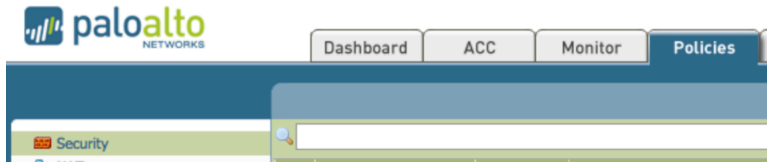


Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule
05/28 16:26:02	drop	web	db	10.0.1.101	10.0.2.101	22	not-applicable	deny	Log default deny
05/28 16:25:30	drop	web	db	10.0.1.101	10.0.2.101	22	not-applicable	deny	Log default deny

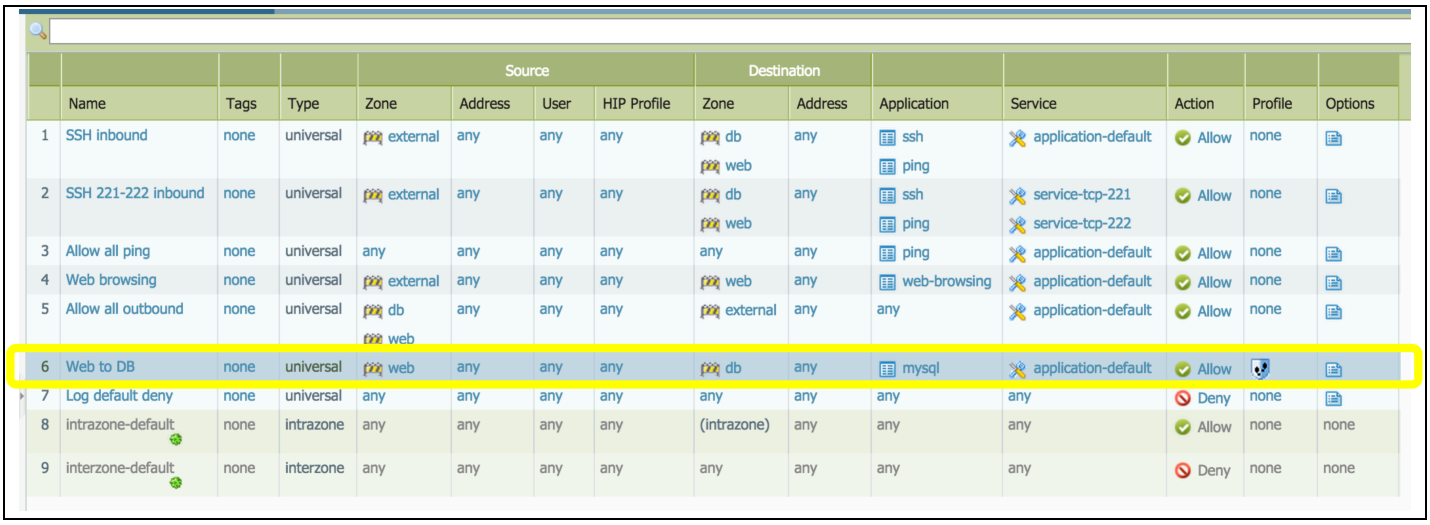
Task 2 – Review the threat protection profile

In this task, we will look at the Vulnerability Protection profile. 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.

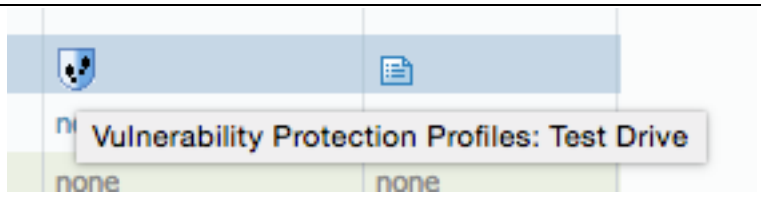
Return to the firewall management interface and click on the Policies tab and make sure your are in Security in the left hand pane.



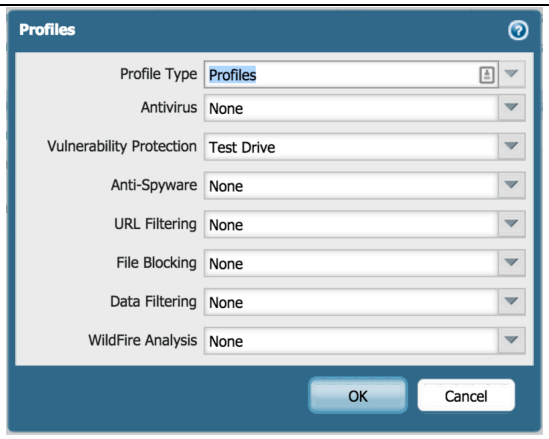
For the ***Web to DB*** rule, hover over the icon in the ***Profile*** column and note the ***Test Drive*** vulnerability profile in use.



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



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.

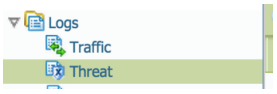
Task 3 – Trigger the SQL brute force attack and review logs

For this task, 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.

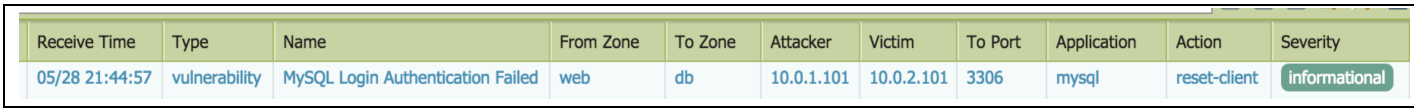
Open a new browser tab and browse to the URL ***http://<<Web Server IP>>/sql-attack.html***

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

Return to the firewall and click the ***Monitor*** tab and then click on ***Threats*** in the left hand pane under ***Logs***.



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



Receive Time	Type	Name	From Zone	To Zone	Attacker	Victim	To Port	Application	Action	Severity
05/28 21:44:57	vulnerability	MySQL Login Authentication Failed	web	db	10.0.1.101	10.0.2.101	3306	mysql	reset-client	informational

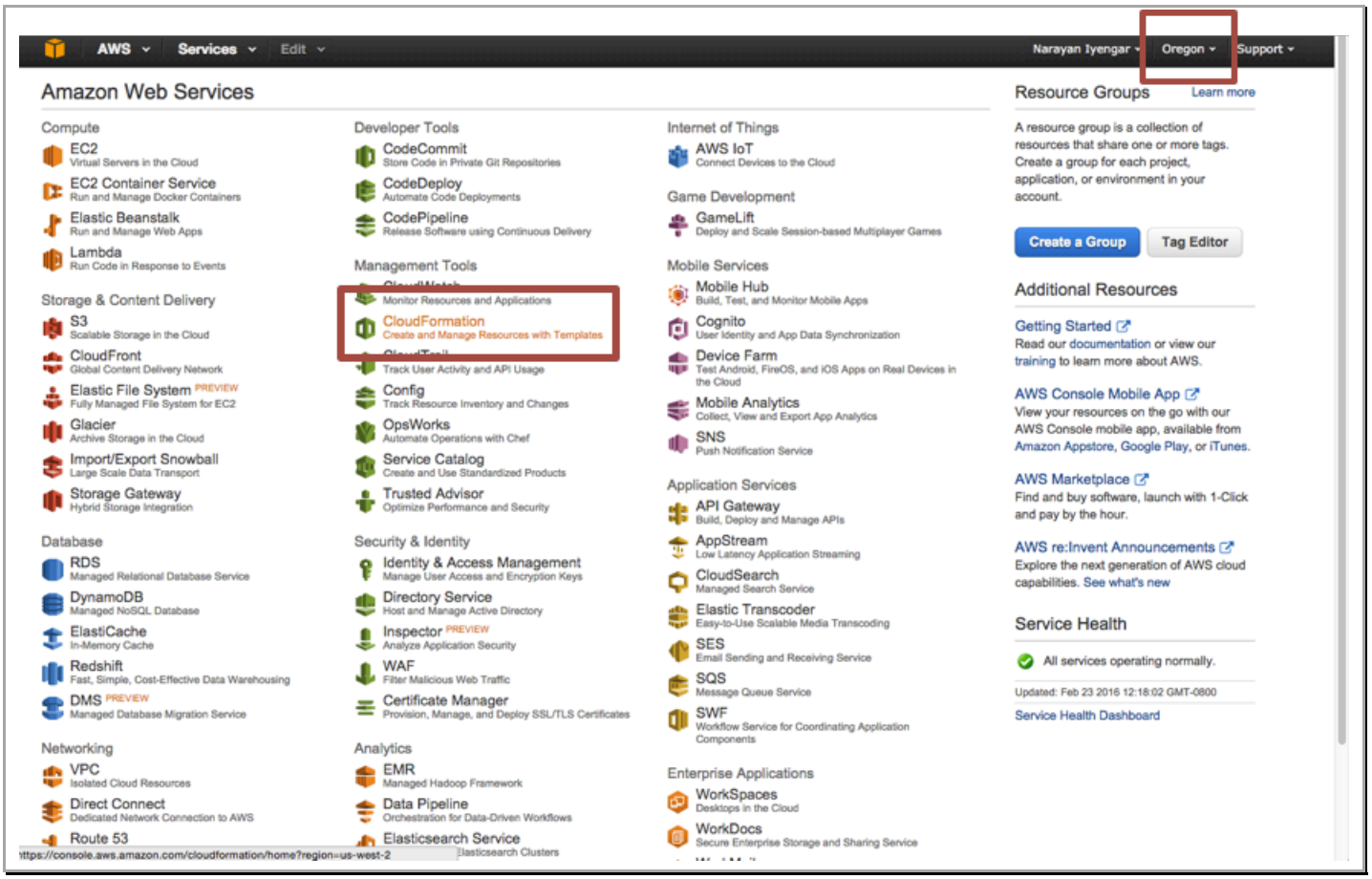
Note: The CGI script you launched in Step 2 attempted to login to the MySQL database multiple times with an incorrect password. The VM-Series firewall saw this activity and using the vulnerability profile, reset the connection and logged the activity.

End of Activity 3

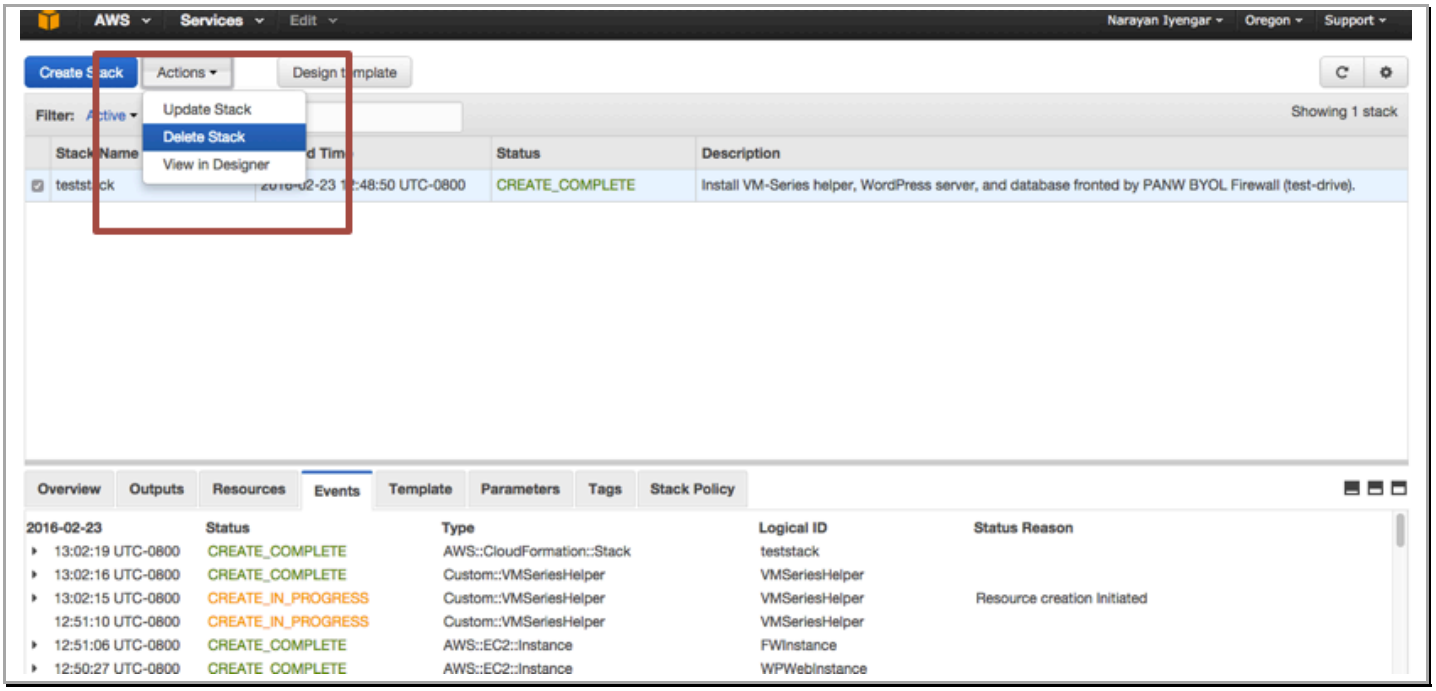
9. Cleanup

9.1 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**:



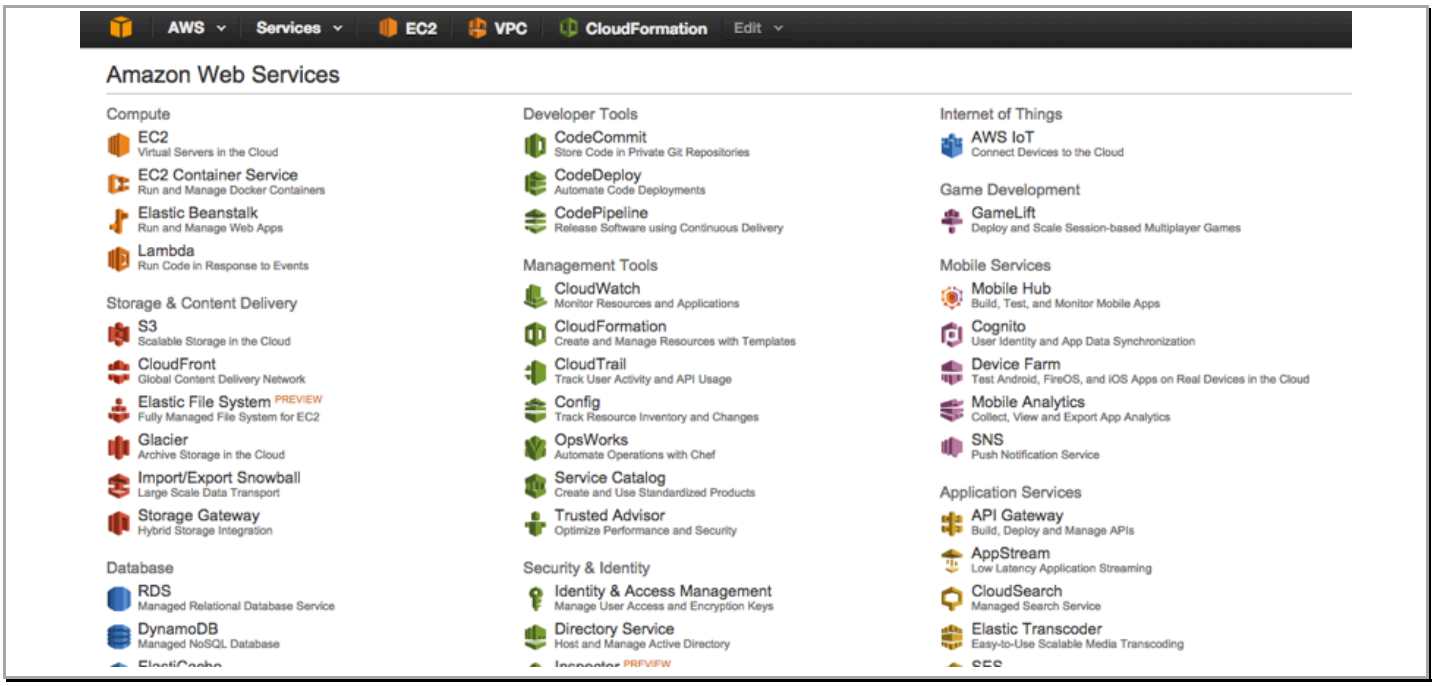
Under **Actions**, click **Delete Stack:**



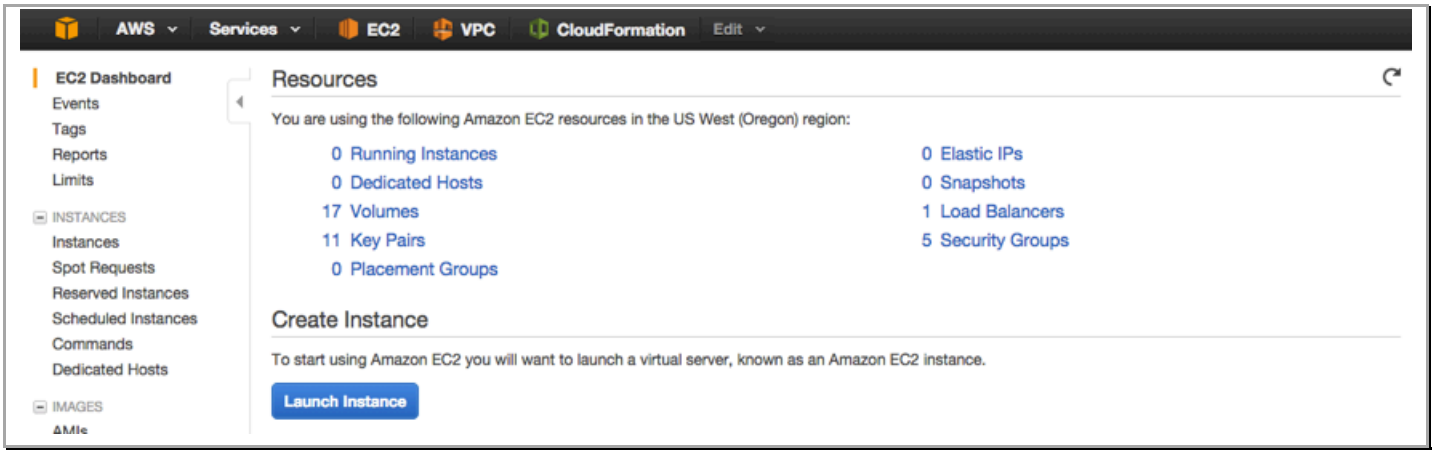
This should delete all the resources created via the template and release any Elastic IPs associated with the firewall.

9.2 Delete keys

As part of the template certain keys are created to access the VM-Series firewall. These keys need to be manually deleted. To do that, go to the **EC2** console:

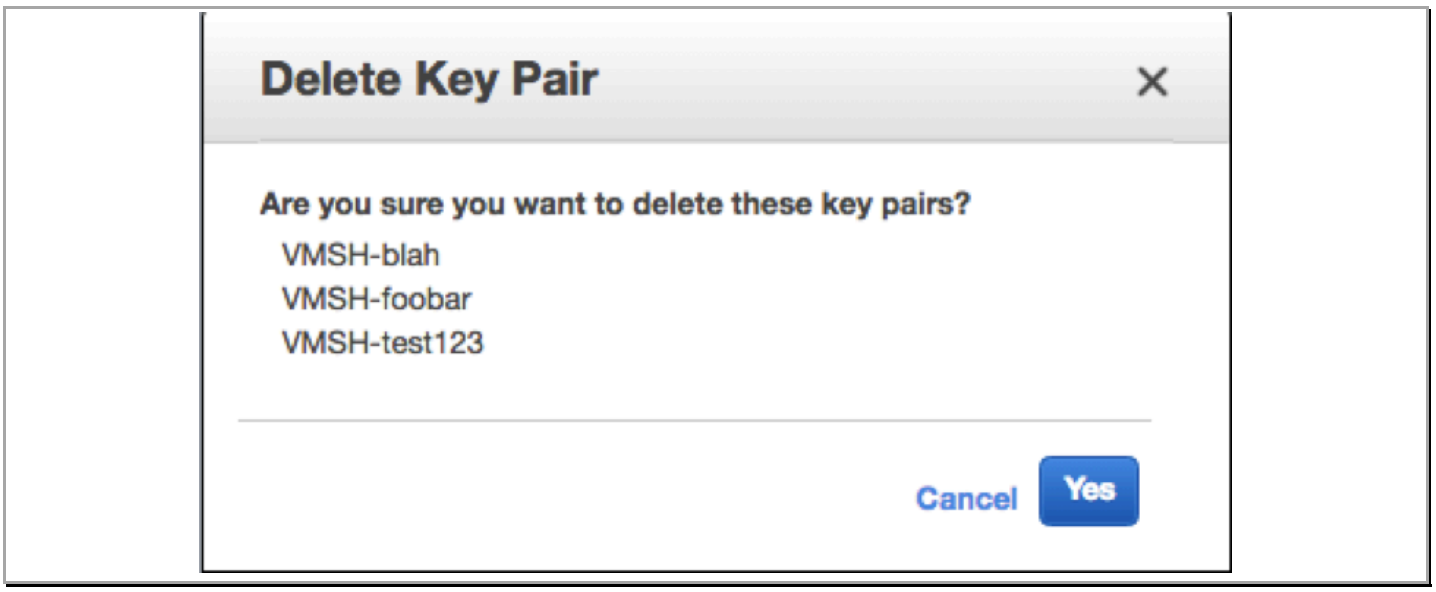


Click on **Key Pairs**:



Select all keys that start with **VMSH** and click **Delete:**

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



10. Conclusion

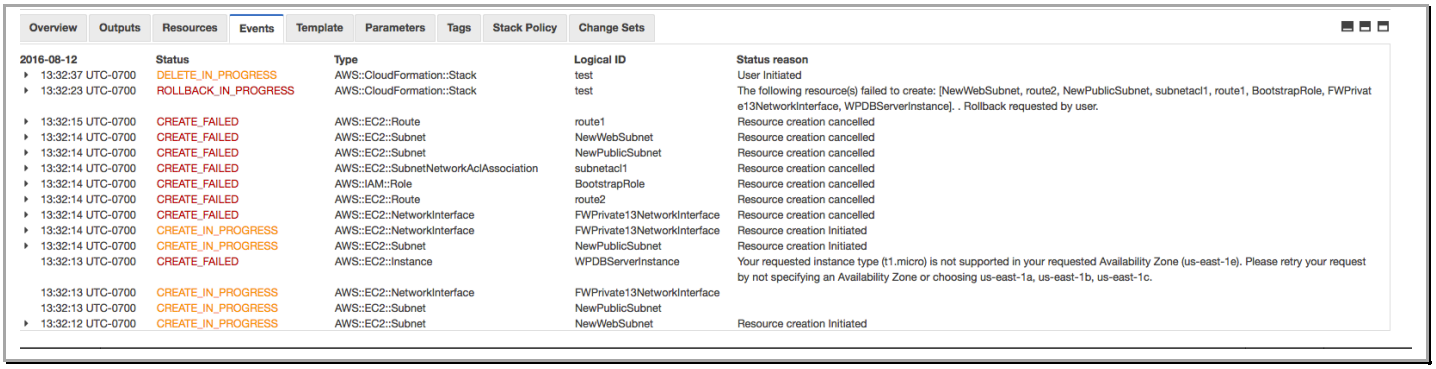
You have successfully deployed a sample CFT in AWS and demonstrated how the next generation VM-Series firewall can not only secure traffic inbound into your VPC, but within the VPC itself.

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:



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.

If you encounter this error, please refer to Section 3.6 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 3.5 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 3.5 is mentioned when launching the template.