

# 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>

# Table of Contents

---

<b>Version History.....</b>	<b>3</b>
<b>1. About CFTs.....</b>	<b>4</b>
<b>2. Support Policy .....</b>	<b>4</b>
<b>3. Instances used.....</b>	<b>5</b>
<b>4. Prerequisites .....</b>	<b>5</b>
4.1 Create an AWS account.....	5
4.2 Add a credit card to your AWS account.....	5
4.3 Review and accept the EULA.....	5
4.4 Create and download an SSH keypair.....	8
4.5 Create a Bootstrap Bucket.....	10
4.6 Download the Template .....	15
4.7 Check Elastic IPs .....	15
<b>5. Launch The CFT.....</b>	<b>17</b>
<b>6. Review what was created .....</b>	<b>22</b>
<b>7. Access the firewall .....</b>	<b>25</b>
<b>8. Access the Webserver .....</b>	<b>28</b>
<b>9. Launch some attacks.....</b>	<b>30</b>
9.1 SSH from Web Server to DB Server .....	30
9.2 SQL Brute force attack .....	31
<b>10. Cleanup.....</b>	<b>33</b>
10.1 Delete the Stack .....	33
10.2 Delete keys.....	34
<b>11. Conclusion .....</b>	<b>36</b>
<b>Appendix A .....</b>	<b>37</b>
Troubleshooting tips .....	37

## Version History

Version number	Comments
1.0	Initial GitHub check-in
1.1	Update links in doc to point to GitHub

# 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.

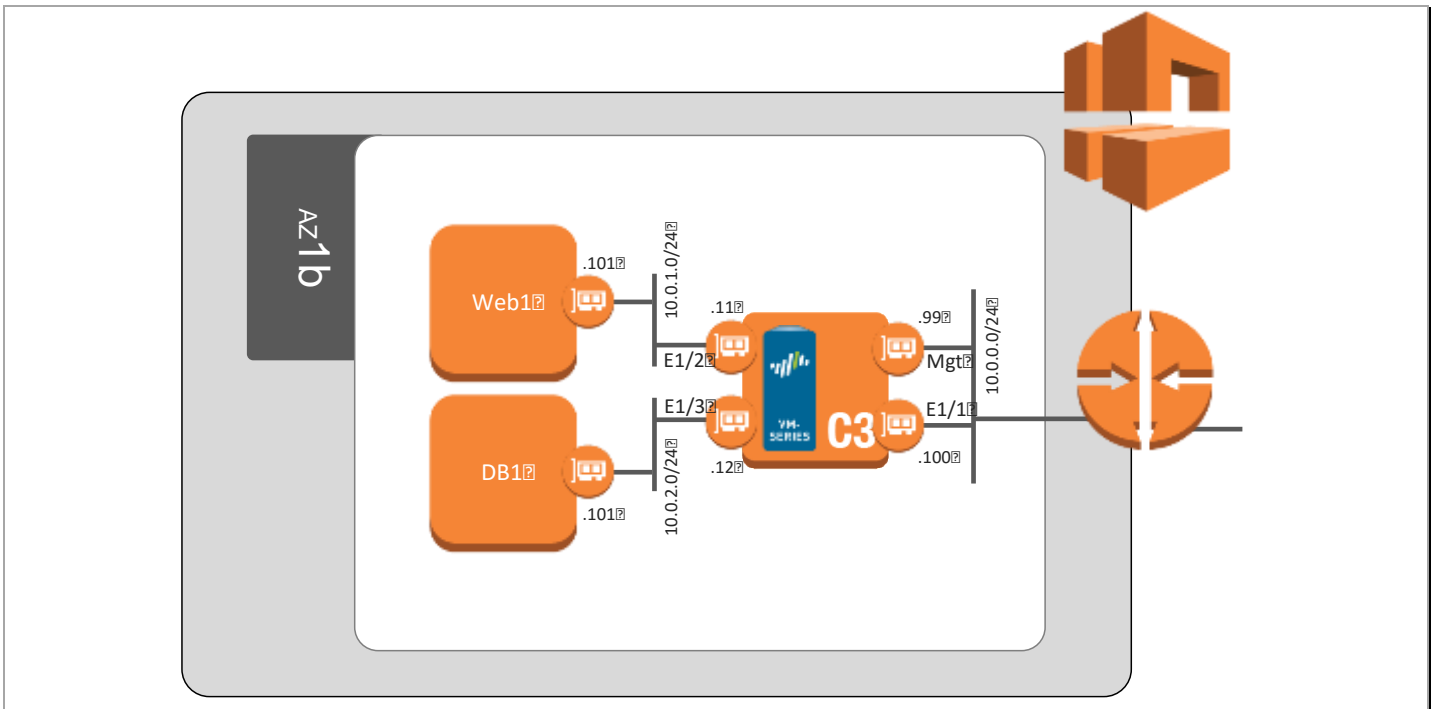
For more information on CFTs and sample CFTs refer to Amazon's documentation

<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>

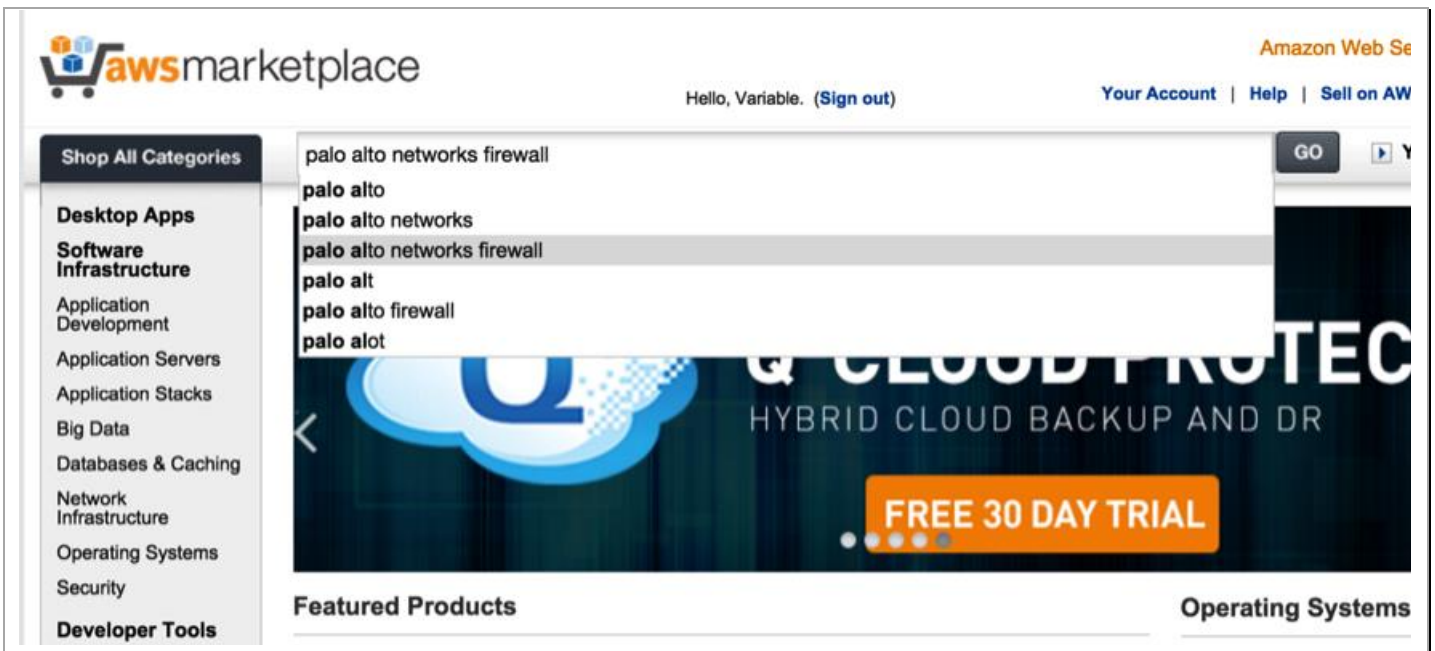
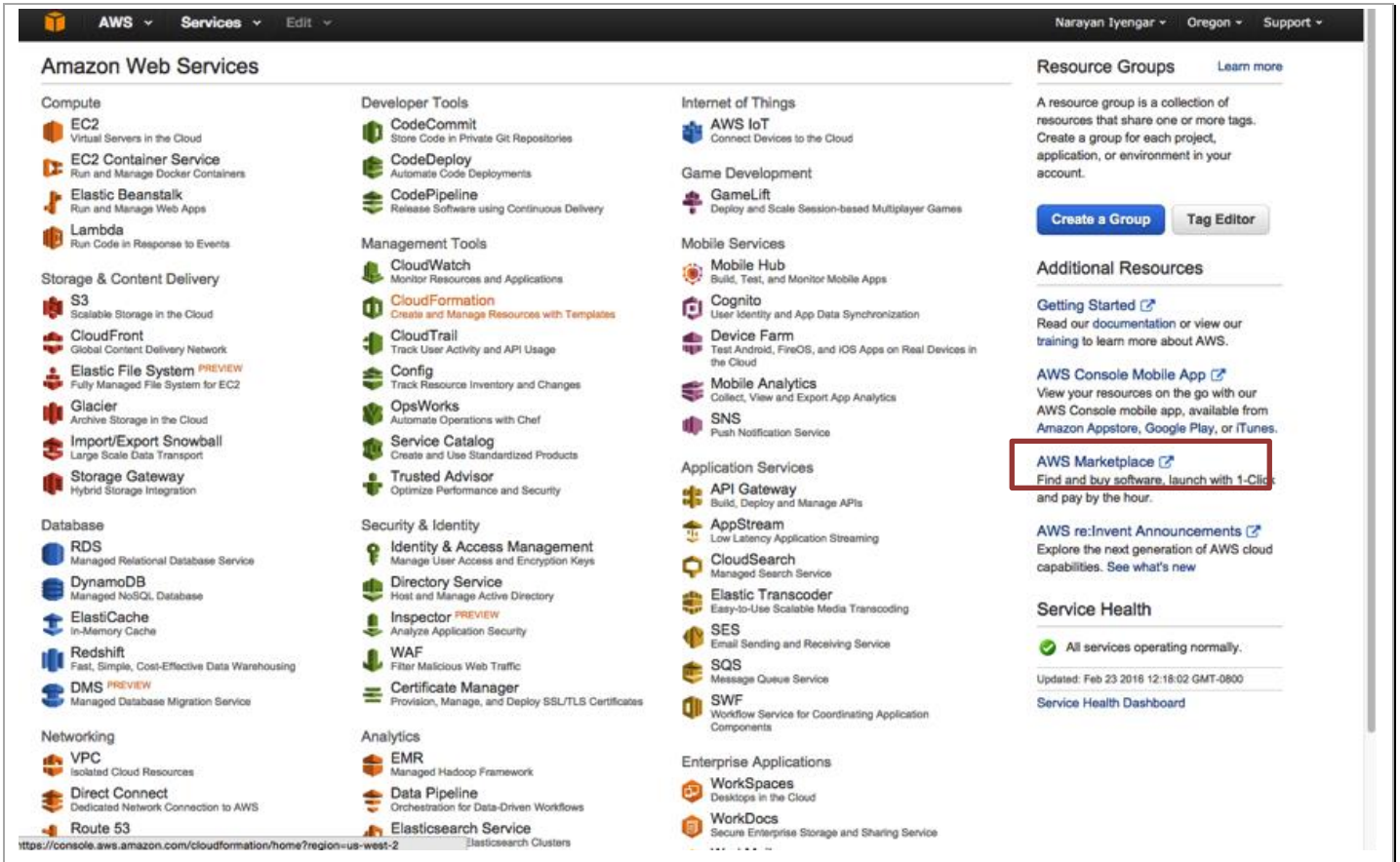
If creating a new account, you may receive a phone call from AWS for verification purposes.

#### 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.

## Palo Alto Networks AWS CFT Deployment Guide


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




## Select VM-Series Next Generation Firewall Bundle 2

**palo alto networks firewall (3 results)** showing 1 - 3

---



**VM-Series Next-Generation Firewall Bundle 2**  
★★★★★ (1) | Version PAN-OS 7.0.1 | Sold by [Palo Alto Networks](#)  
**\$1.28/hr or \$4,500/yr (60% savings) for software + AWS usage fees**  
The VM-Series for AWS Bundle 2 includes a VM-300 next-generation firewall license, subscriptions for Threat Prevention (includes IPS, AV, malware prevention), WildFire, ...  
Linux/Unix, Other PAN-OS 7.0.1 | 64-bit Amazon Machine Image (AMI)




Amazon Web Services Home

Sign in or Create a new account

Your Account | Help | Sell on AWS Marketplace

Shop All Categories ▾ Search AWS Marketplace **GO** ▶ Your Software

---



**VM-Series Next-Generation Firewall Bundle 2**  
Sold by: [Palo Alto Networks](#)

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

---

**Customer Rating** ★★★★★ (1 Customer Review)

**Latest Version** PAN-OS 7.0.1

**Operating System** Linux/Unix, Other PAN-OS 7.0.1

**Delivery Method** 64-bit Amazon Machine Image (AMI) ([Learn more](#))

**Support** [See details below](#)

**AWS Services Required** Amazon EC2, Amazon EBS

**Highlights**

- Bundle 2 includes everything you need to protect your AWS environment. It includes: a VM-Series 300 firewall license, subscriptions for Threat Prevention, WildFire, URL Filtering,

**Continue**

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

**Pricing Details**

For region  
**US West (Oregon)**

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

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

Click **Continue**.



**Launch on EC2:**

## VM-Series Next-Generation Firewall Bundle 2

**1-Click Launch**  
Review, modify, and launch

**Manual Launch**  
With EC2 Console, APIs or CLI

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

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

**Software Pricing**

**Subscription Term**

☒ Hourly
☐ Annual

**Applicable Instance Type**

**Software fee**  
Varies  
Depends on instance type, reference pricing chart.

**Usage Instructions**

Select a Version

**Price for your selections:**  
Price will be dependent on usage

**Accept Software Terms**

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

**Pricing Details**

For region  
US West (Oregon)

**Your Free Trial has expired**

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

EC2 Instance Type	Software	EC2	Total

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

You should see this screen:

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

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

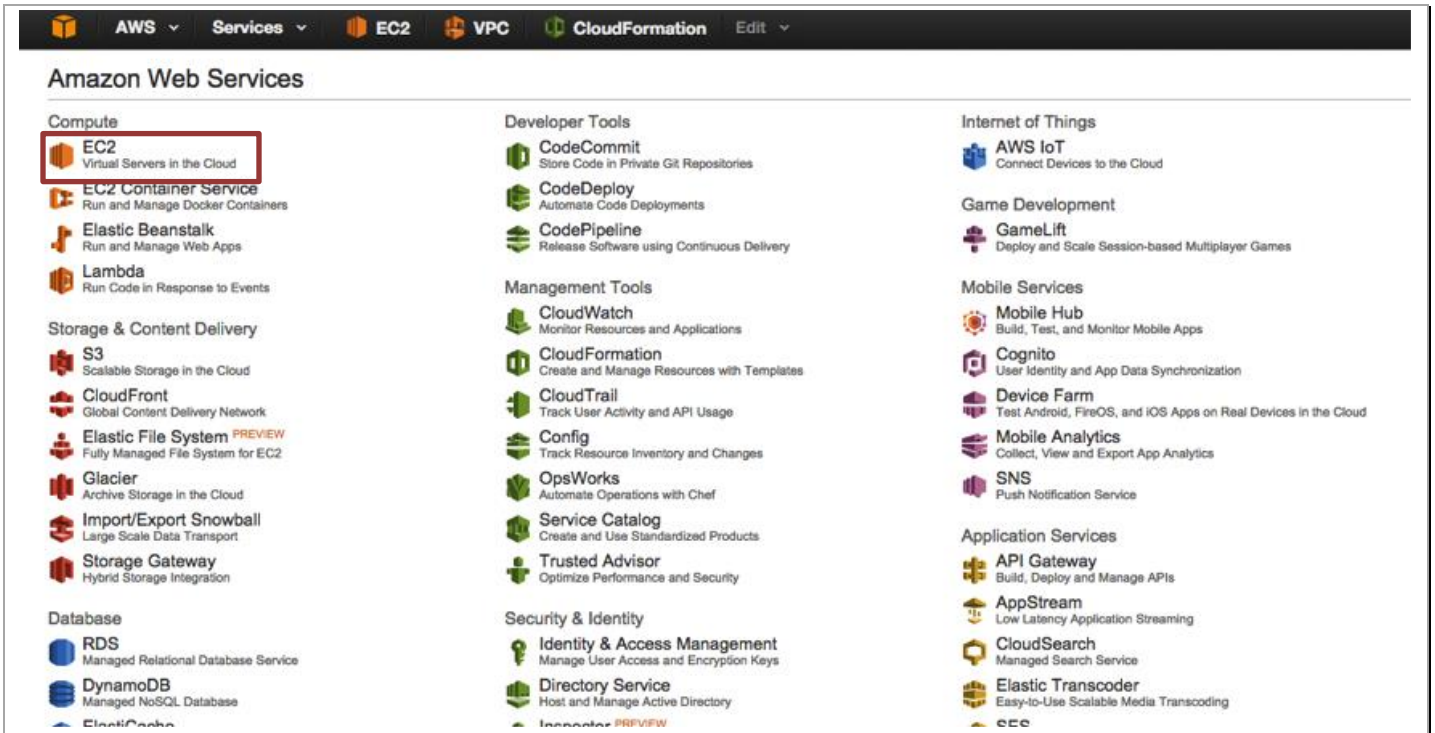
You can now close the browser tab or window and continue with the next step.

## 4.4 Create and download an SSH keypair

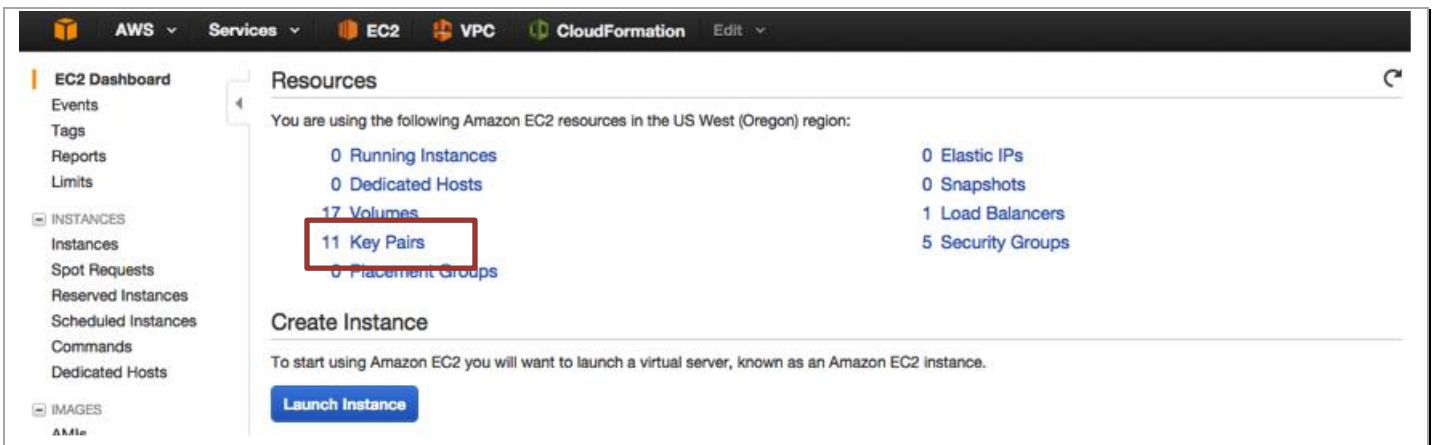
Sign into the AWS console <https://www.amazon.com> and click on **EC2**



## Palo Alto Networks AWS CFT Deployment Guide



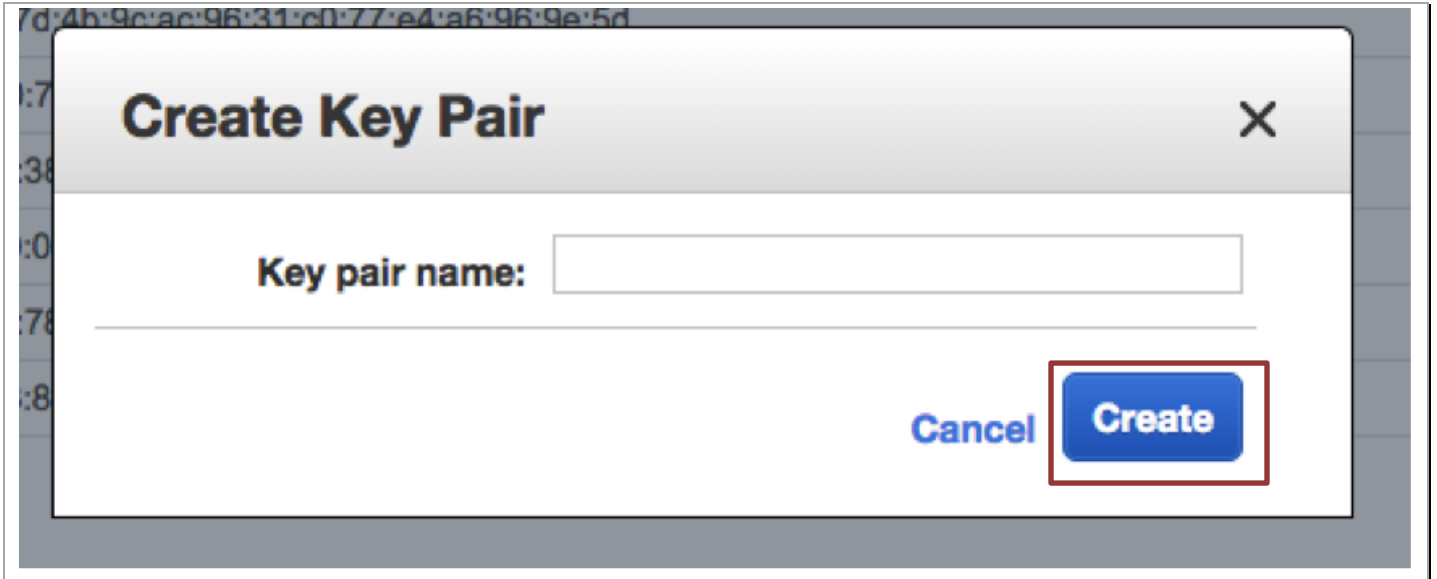
Click **KeyPairs**



Click **Create Key Pair**



Give it a name



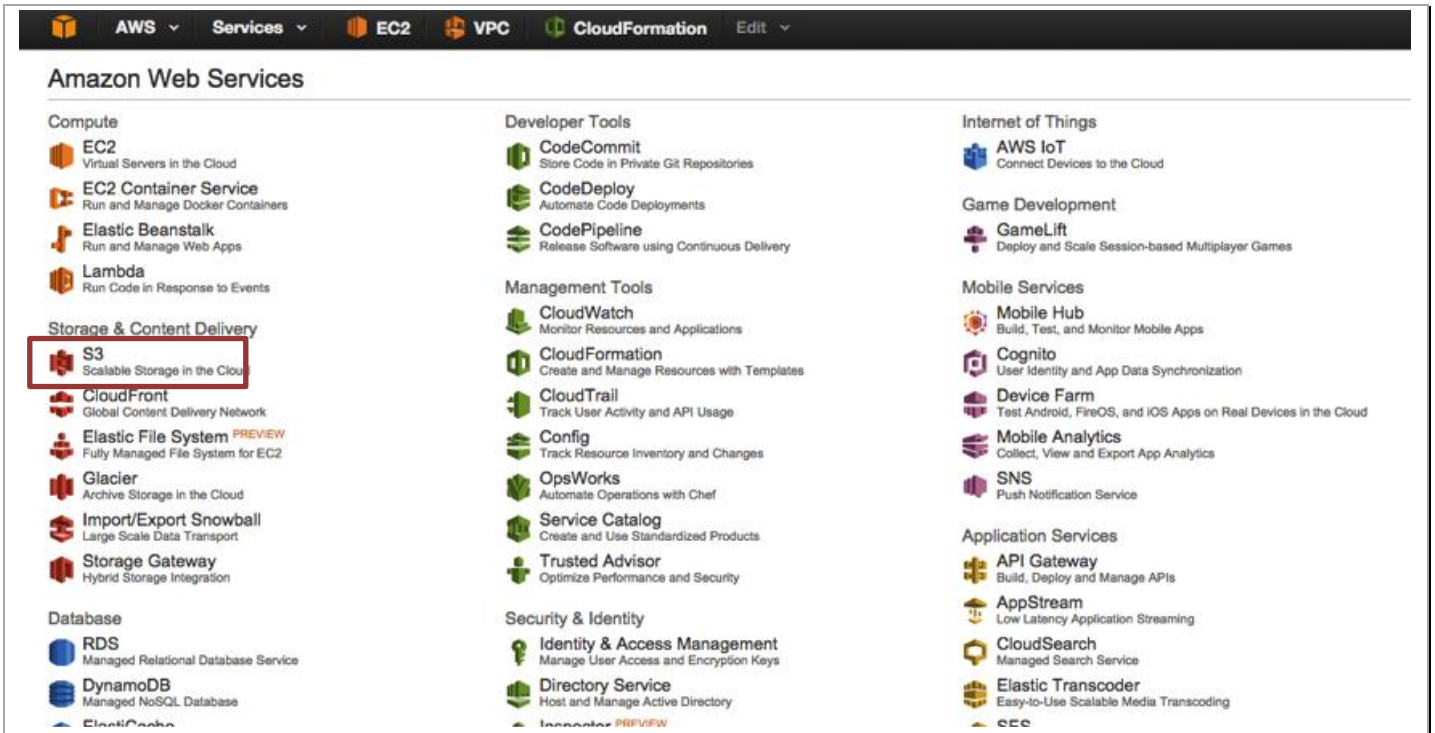
And click **Create**. This should now prompt you to save the just generated private key. Save the key.

## 4.5 Create a Bootstrap Bucket

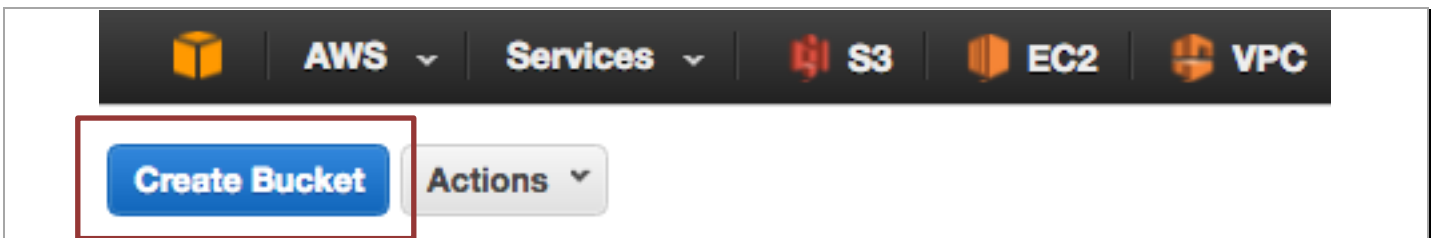
Bootstrapping is a feature of the VM-Series firewall that allows you to load a pre-defined configuration into the firewall during boot-up. This ensures that the firewall is configured and ready at initial boot-up, thereby removing the need for manual configuration. The bootstrapping feature also enables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

## Palo Alto Networks AWS CFT Deployment Guide



Click **Create Bucket**:



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

Create a Bucket - Select a Bucket Name and Region

Cancel

A bucket is a container for objects stored in Amazon S3. When creating a bucket, you can choose a Region to optimize for latency, minimize costs, or address regulatory requirements. For more information regarding bucket naming conventions, please visit the [Amazon S3 documentation](#).

**Bucket Name:**

**Region:**

Set Up Logging >

Create

Cancel

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**:

Upload

Create Folder

Actions

All Buckets / sample-cft-bootstrap1

	Name
<input type="checkbox"/>	config
<input type="checkbox"/>	content
<input type="checkbox"/>	license
<input type="checkbox"/>	software

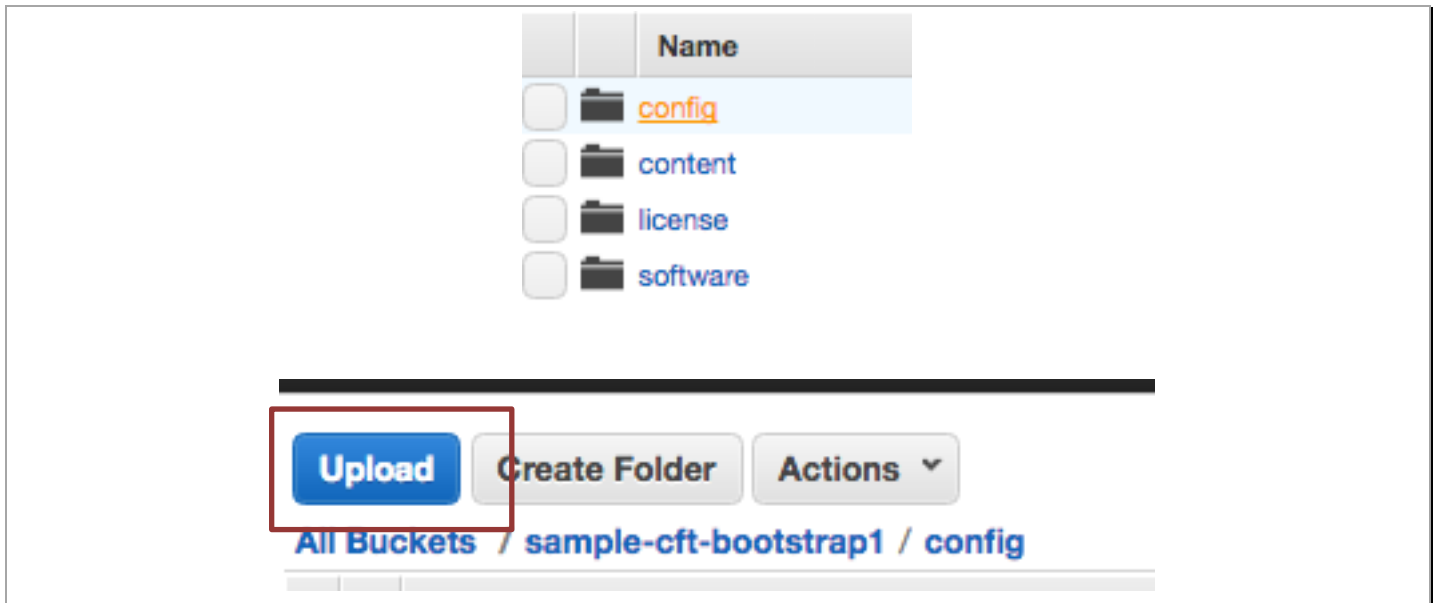
Download the following files and save them in a known location:

<https://raw.githubusercontent.com/PaloAltoNetworks/aws/master/two-tier%20sample/bootstrap/bootstrap.xml>

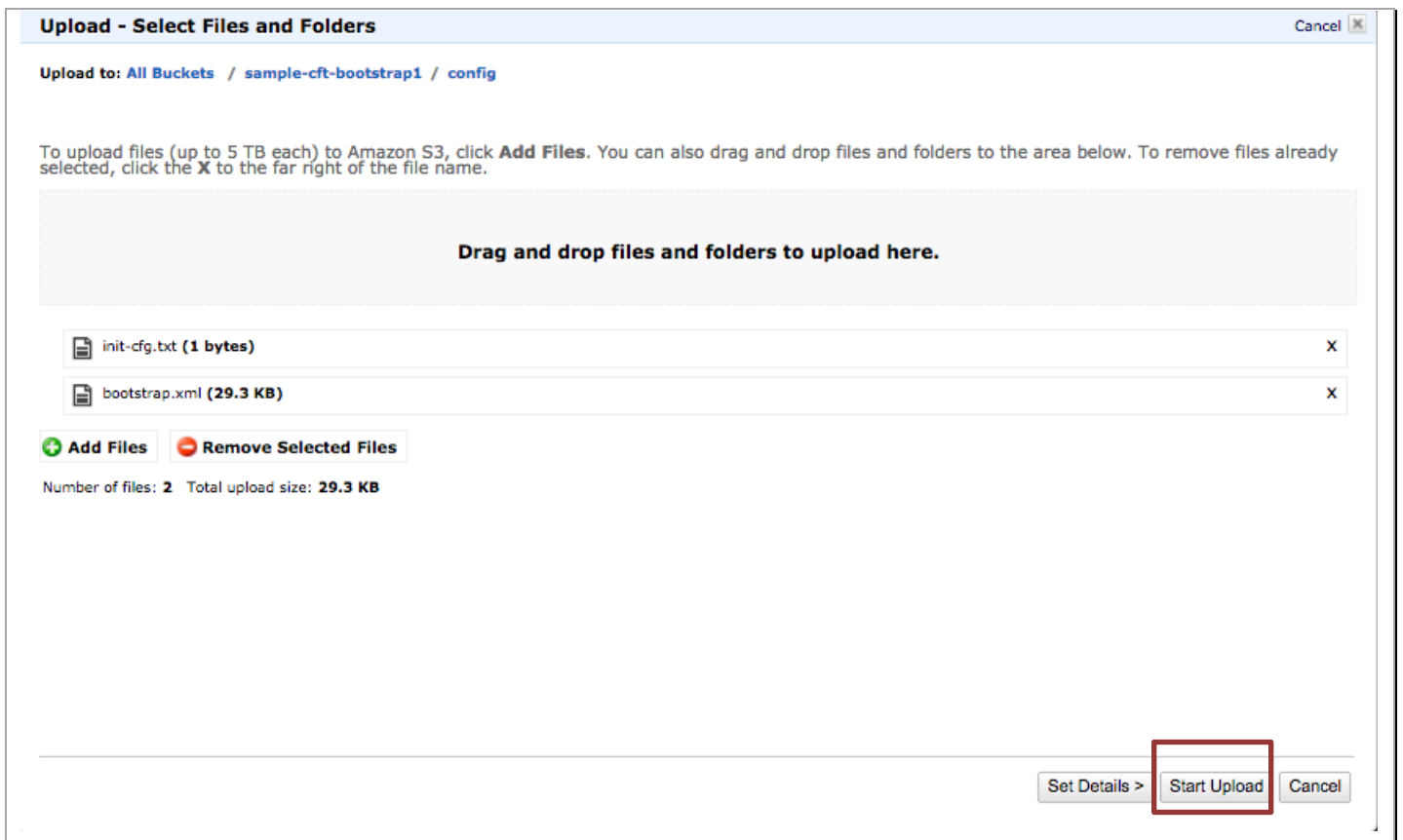
<https://raw.githubusercontent.com/PaloAltoNetworks/aws/master/two-tier%20sample/bootstrap/init-cfg.txt>

<https://github.com/PaloAltoNetworks/aws/raw/master/two-tier%20sample/bootstrap/panupv2-all-contents-600-3449>

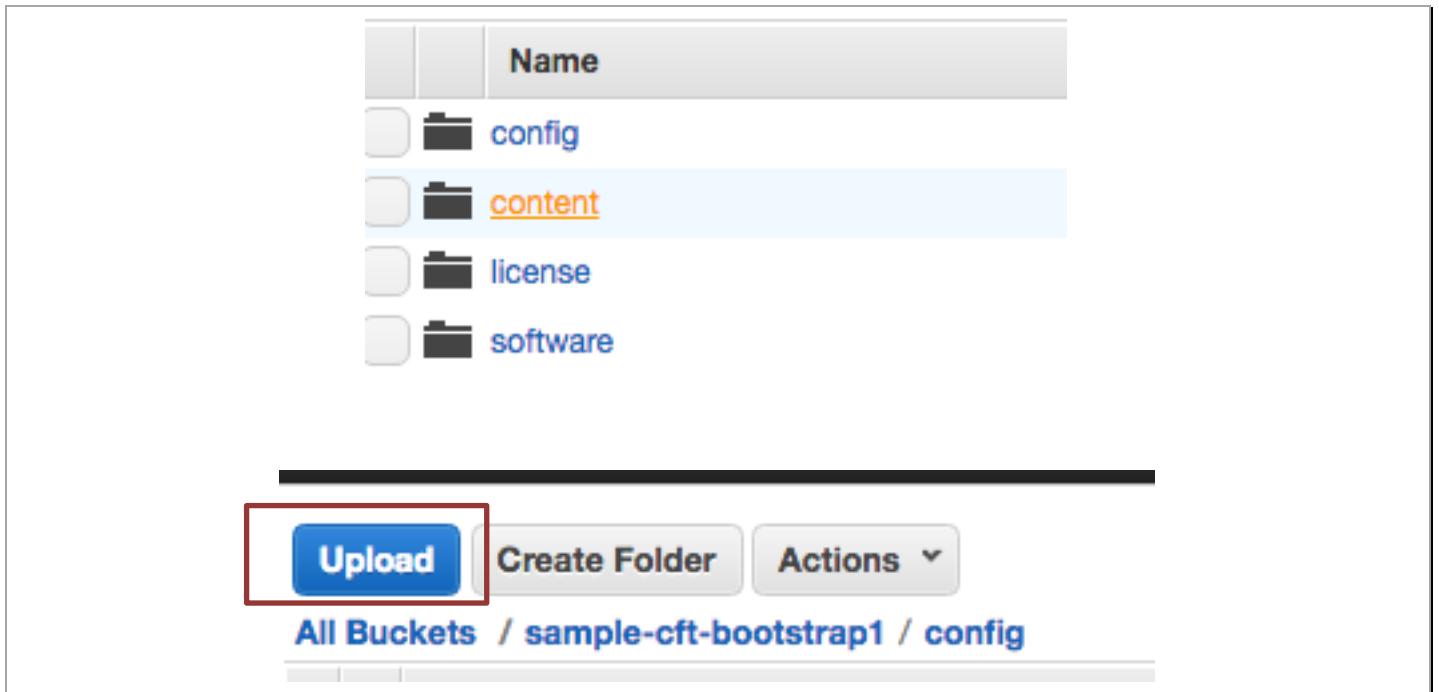
Now click on the **config** folder in the **S3** console and click **Upload**:



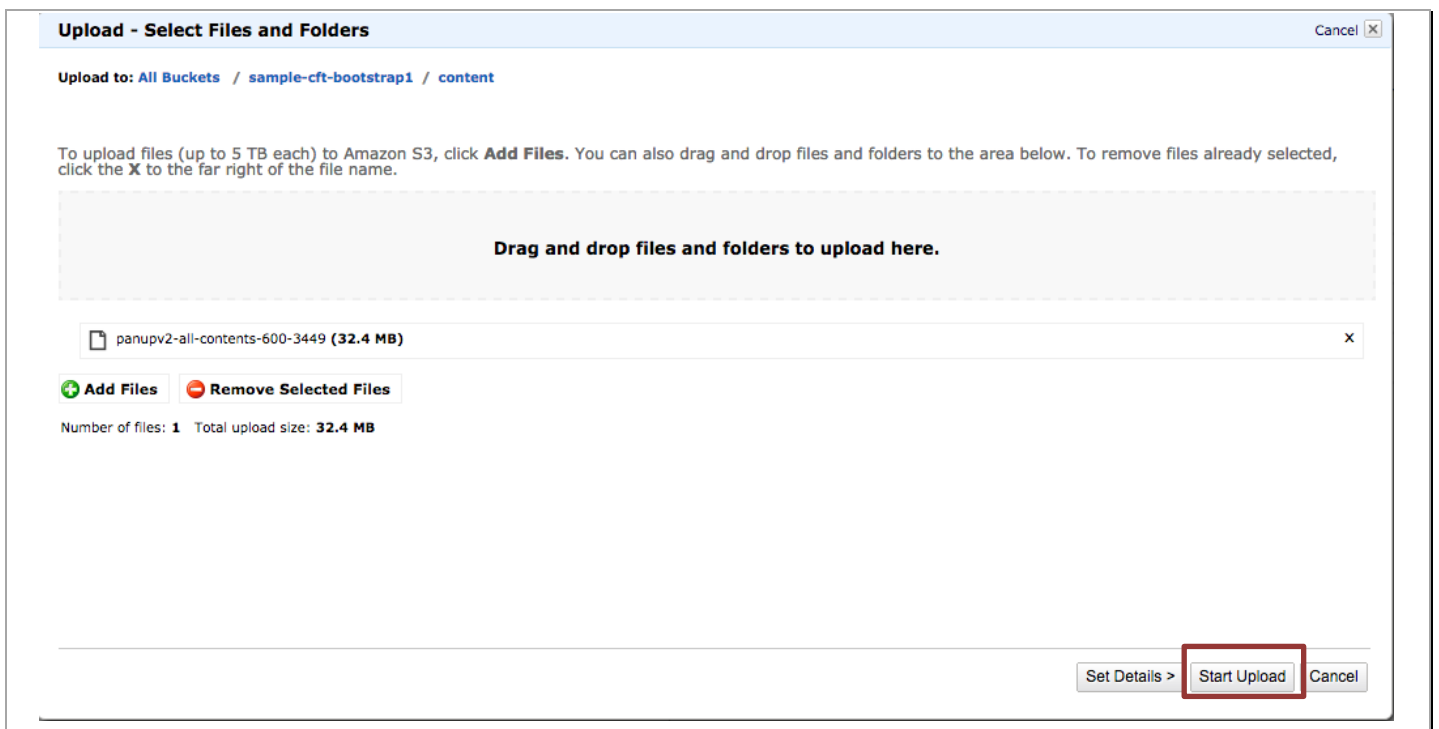
Select **Add Files** and select the two files (bootstrap.xml and init-cft.txt) downloaded previously and click **Start Upload**:



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.

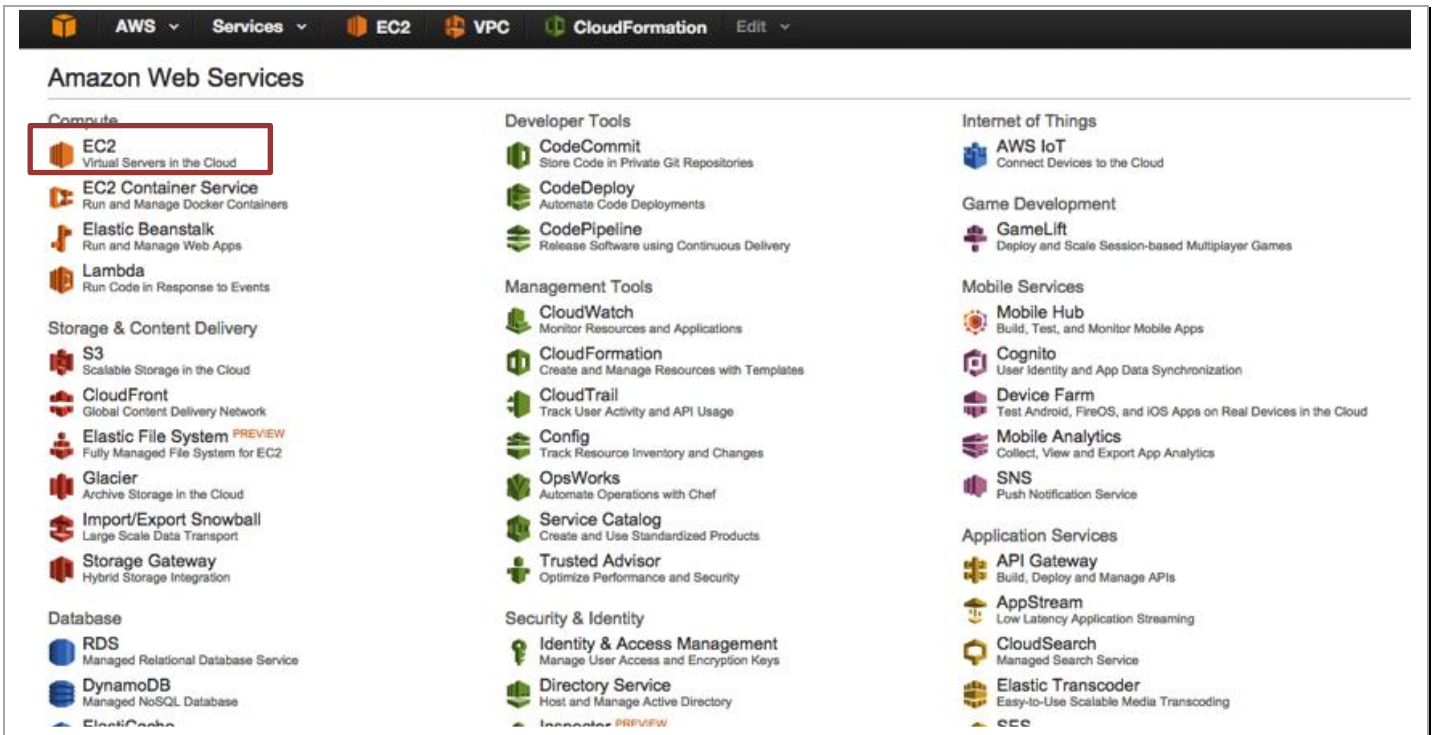
## 4.6 Download the Template

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

<https://raw.githubusercontent.com/PaloAltoNetworks/aws/master/two-tier%20sample/pan-sample-cft-V4.json>

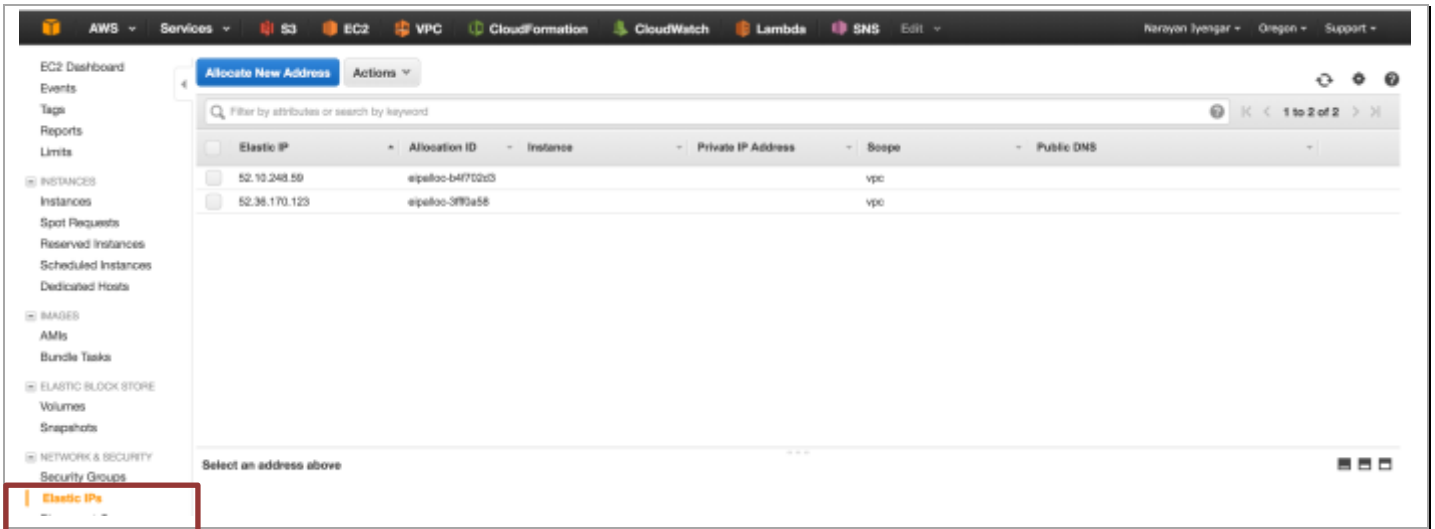
## 4.7 Check Elastic IPs

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**:

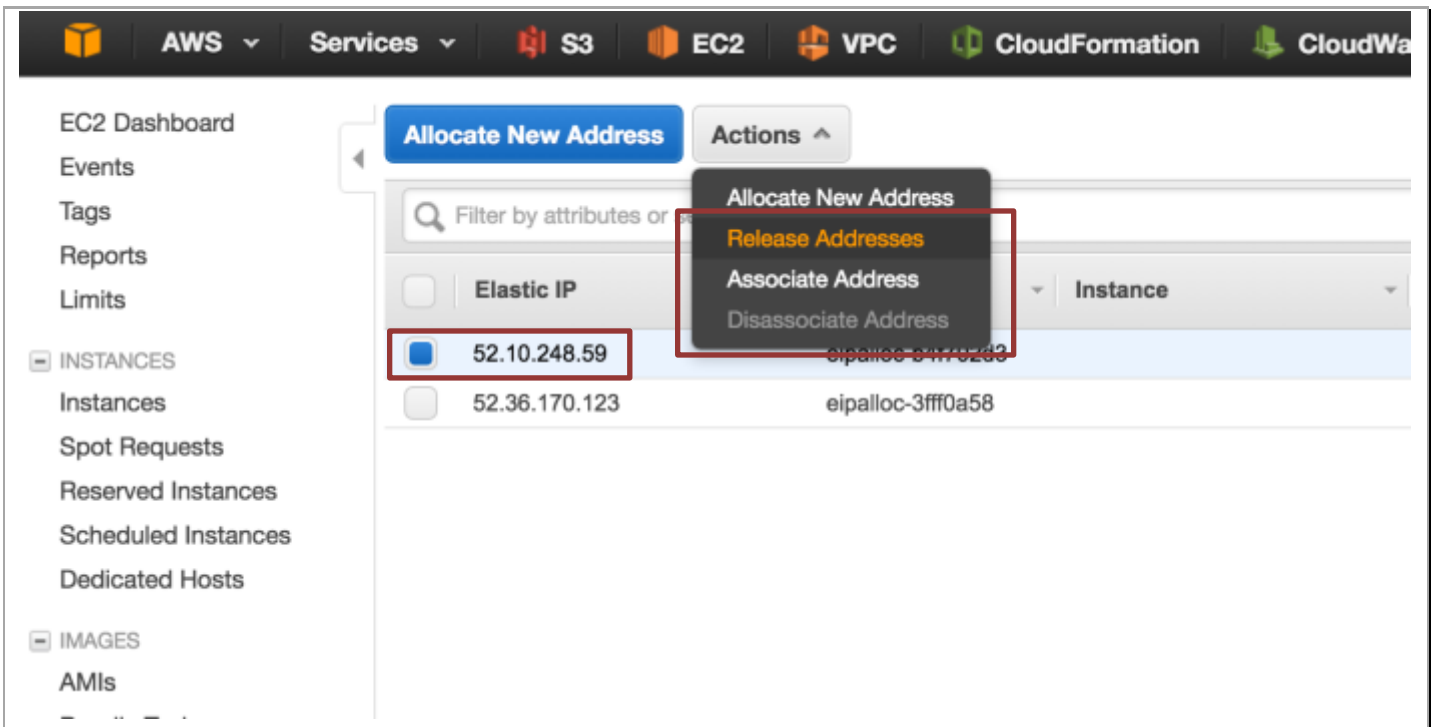


And click on Elastic IPs:

## Palo Alto Networks AWS CFT Deployment Guide



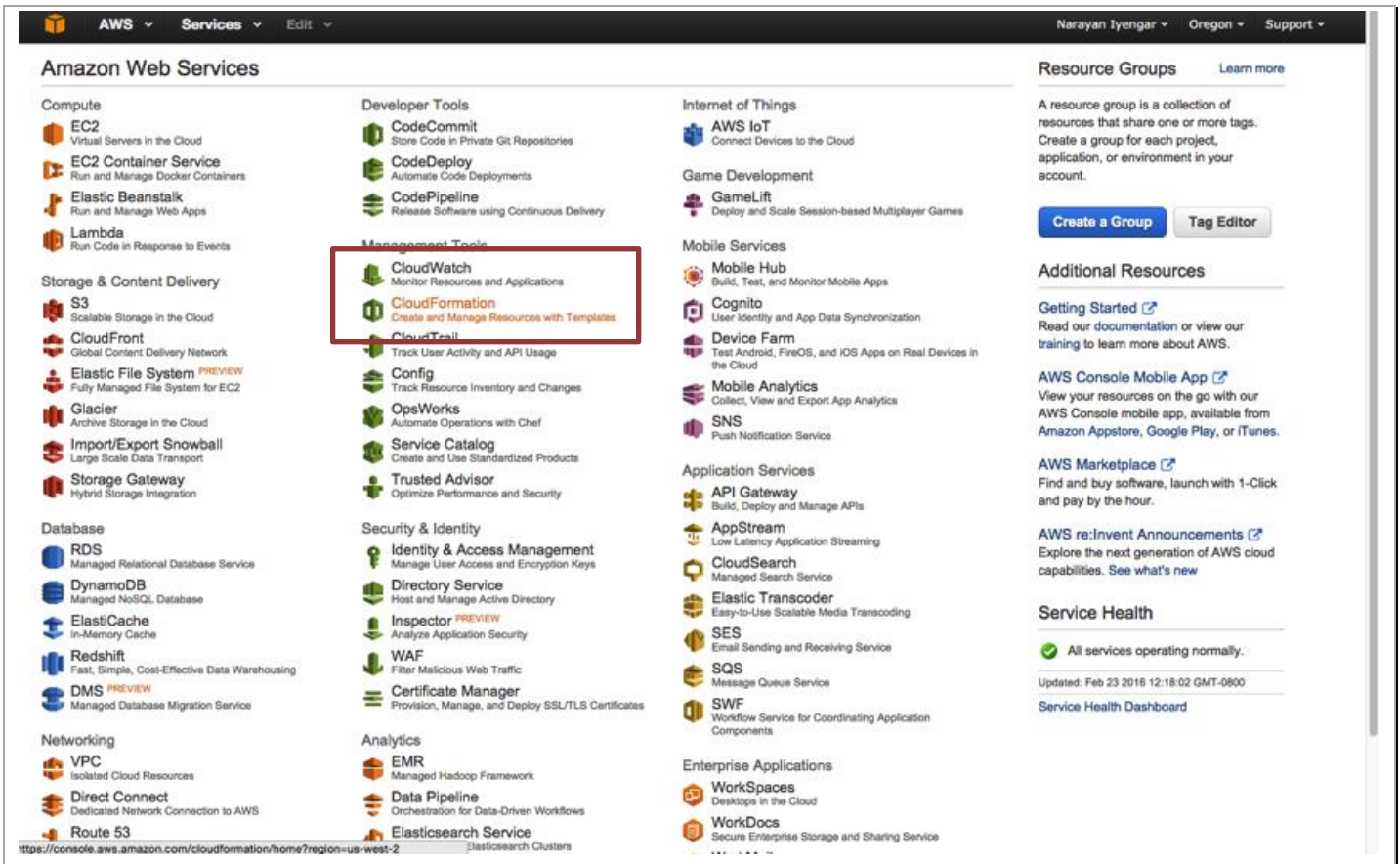
If there are no EIPs allocated, proceed to [Section 4](#). If there are more than 3 EIPs allocated and you have not requested an EIP limit increase, the template launch will fail. You can either release an EIP or request a limit increase via an AWS support ticket. In order to release an allocated EIP,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



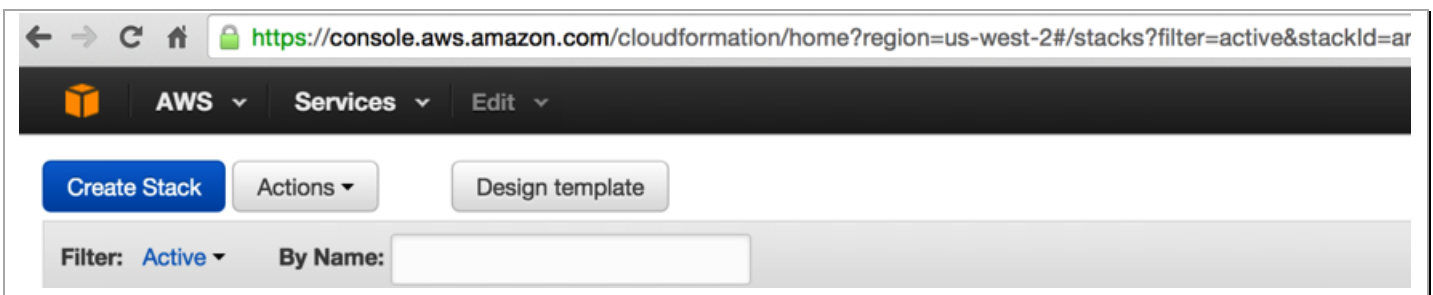
If the EIP is associated with an instance, you will need to disassociate the address first and then release the address. If you are relying on the address for other work, please be aware that disassociating the address and releasing the address could cause work disruption.

## 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**:

## Palo Alto Networks AWS CFT Deployment Guide

The screenshot shows the AWS CloudFormation console's 'Create stack' wizard. The 'Select Template' step is active. On the left, a sidebar lists the steps: 'Select Template', 'Specify Details', 'Options', and 'Review'. The main content area has a heading 'Select Template' and a sub-heading 'Select the template that describes the stack that you want to create. A stack is a group of related resources that you manage as a single unit.' Below this, there are two sections: 'Design a template' with a 'Design template' button, and 'Choose a template' with three radio button options: 'Select a sample template', 'Upload a template to Amazon S3' (which is selected), and 'Specify an Amazon S3 template URL'. Under 'Upload a template to Amazon S3', there is a 'Choose File' button and a text input field containing 'pan-sample-cft-V4.json'. At the bottom right, there are 'Cancel' and 'Next' buttons, with the 'Next' button highlighted by a red rectangle.

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**.

The screenshot shows the 'Specify Details' step of the AWS CloudFormation 'Create stack' wizard. The 'Stack name' field is filled with 'test-stack'. Below this is the 'Parameters' section. It contains two fields: 'BootstrapBucketName' with the value 'bootstrap-bucket' and a description 'Bucket name for FW bootstrap configuration', and 'ServerKeyName' with a dropdown menu showing 'aws-keypair-virginia' and a description 'Name of an existing EC2 KeyPair to enable SSH access to the FW (Note: You MUST have its private key)'. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons, with the 'Next' button highlighted by a red rectangle.

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.

## Palo Alto Networks AWS CFT Deployment Guide

**Create stack**

Select Template  
Specify Details  
**Options**  
Review

**Options**

**Tags**

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

	Key (127 characters maximum)	Value (255 characters maximum)	
1	Group	Word Press Demo	+

► **Advanced**

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

Cancel Previous **Next**

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

Template URL: <https://s3-us-west-2.amazonaws.com/sample-cft/pan-sample-cft-v1.json>  
Description: Install VM-Series helper, WordPress server, and database fronted by PANW BYOL Firewall (sample-cft).  
Estimate cost: [Cost](#)

**Stack details**

Stack name: teststack

FWInstancePassword: ----  
ServerKeyName: aws-keypair  
Create IAM resources: No

**Options**

**Tags**

No tags provided

**Advanced**

Notification: none  
Timeout: none  
Rollback on failure: Yes

**Capabilities**

**ⓘ** The following resource(s) require capabilities: [AWS::IAM::AccessKey, AWS::IAM::Group, AWS::IAM::Policy, AWS::IAM::User, AWS::IAM::UserToGroupAddition]  
This template requests capabilities and Access Keys, which require that you create groups, IAM users, and IAM roles with certain permissions. Ensure that the template you are using is from a trusted source. [Learn more.](#)

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

Cancel Previous **Create**

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

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

## Palo Alto Networks AWS CFT Deployment Guide

The screenshot shows the AWS CloudFormation console. At the top, there are buttons for 'Create Stack', 'Actions', and 'Design template'. Below these, there's a filter section with 'Filter: Active' and 'By Name:'. A table lists the stacks, with 'teststack' selected. The 'Status' column for 'teststack' is highlighted with a red box and shows 'CREATE\_IN\_PROGRESS'. Below the table, there are tabs for 'Overview', 'Outputs', 'Resources', 'Events', 'Template', 'Parameters', 'Tags', and 'Stack Policy'. The 'Events' tab is selected, showing a list of events for the stack 'teststack'. The first event is highlighted with a red box and shows 'Status: CREATE\_IN\_PROGRESS'.

Stack Name	Created Time	Status	Description
teststack	2016-02-23 12:48:50 UTC-0800	CREATE_IN_PROGRESS	Install VM-Series helper, WordPress server, and database fronted by PANW BYOL Firewall (test-drive).

Overview	Outputs	Resources	Events	Template	Parameters	Tags	Stack Policy
2016-02-23			Status: CREATE_IN_PROGRESS	Type: AWS::CloudFormation::Stack	Logical ID: teststack	Status Reason: User Initiated	

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

The screenshot shows the AWS CloudFormation console. At the top, there are buttons for 'Create Stack', 'Actions', and 'Design template'. Below these, there's a filter section with 'Filter: Active' and 'By Name:'. A table lists the stacks, with 'teststack' selected. The 'Status' column for 'teststack' is highlighted with a red box and shows 'CREATE\_COMPLETE'. Below the table, there are tabs for 'Overview', 'Outputs', 'Resources', 'Events', 'Template', 'Parameters', 'Tags', and 'Stack Policy'. The 'Events' tab is selected, showing a list of events for the stack 'teststack'. The first event is highlighted with a red box and shows 'Status: CREATE\_COMPLETE'.

Stack Name	Created Time	Status	Description
teststack	2016-02-23 12:48:50 UTC-0800	CREATE_COMPLETE	Install VM-Series helper, WordPress server, and database fronted by PANW BYOL Firewall (test-drive).

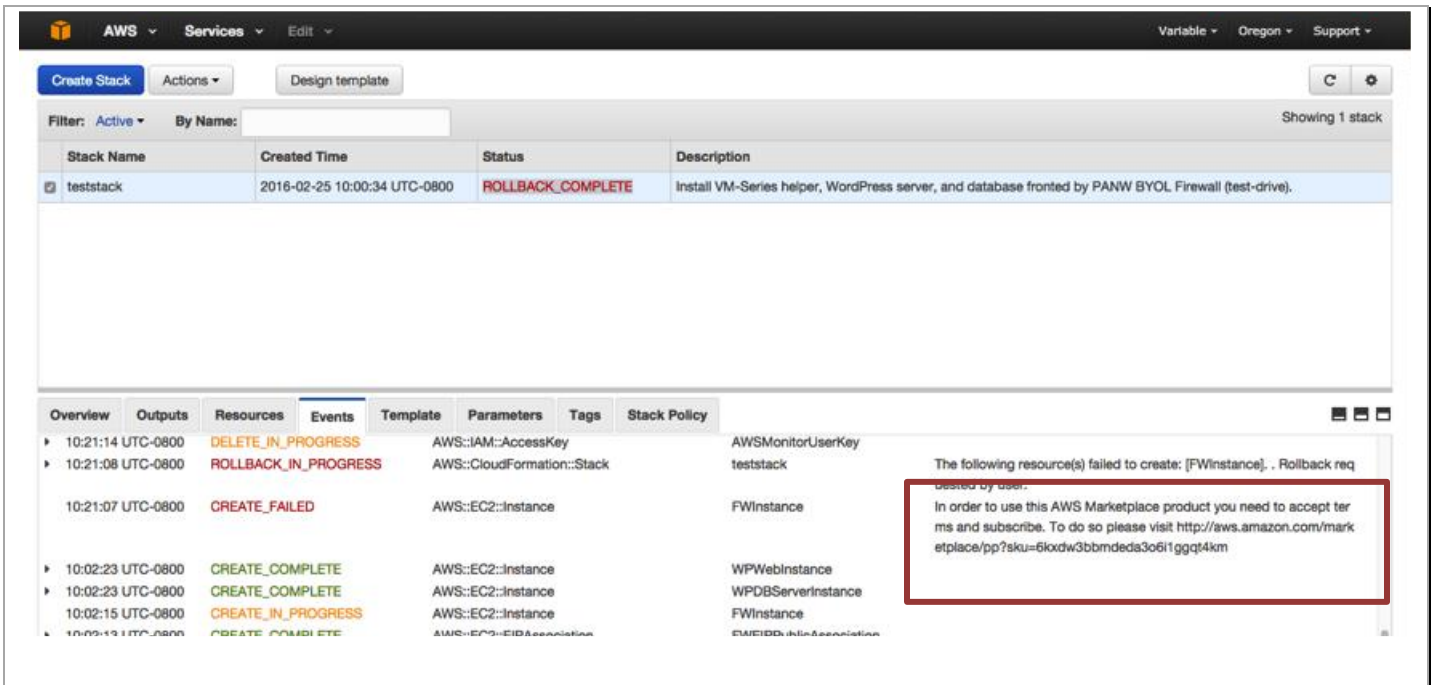
Overview	Outputs	Resources	Events	Template	Parameters	Tags	Stack Policy
16-02-23			Status: CREATE_COMPLETE	Type: AWS::CloudFormation::Stack	Logical ID: teststack	Status Reason: Resource creation Initiated	

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.



## Palo Alto Networks AWS CFT Deployment Guide

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



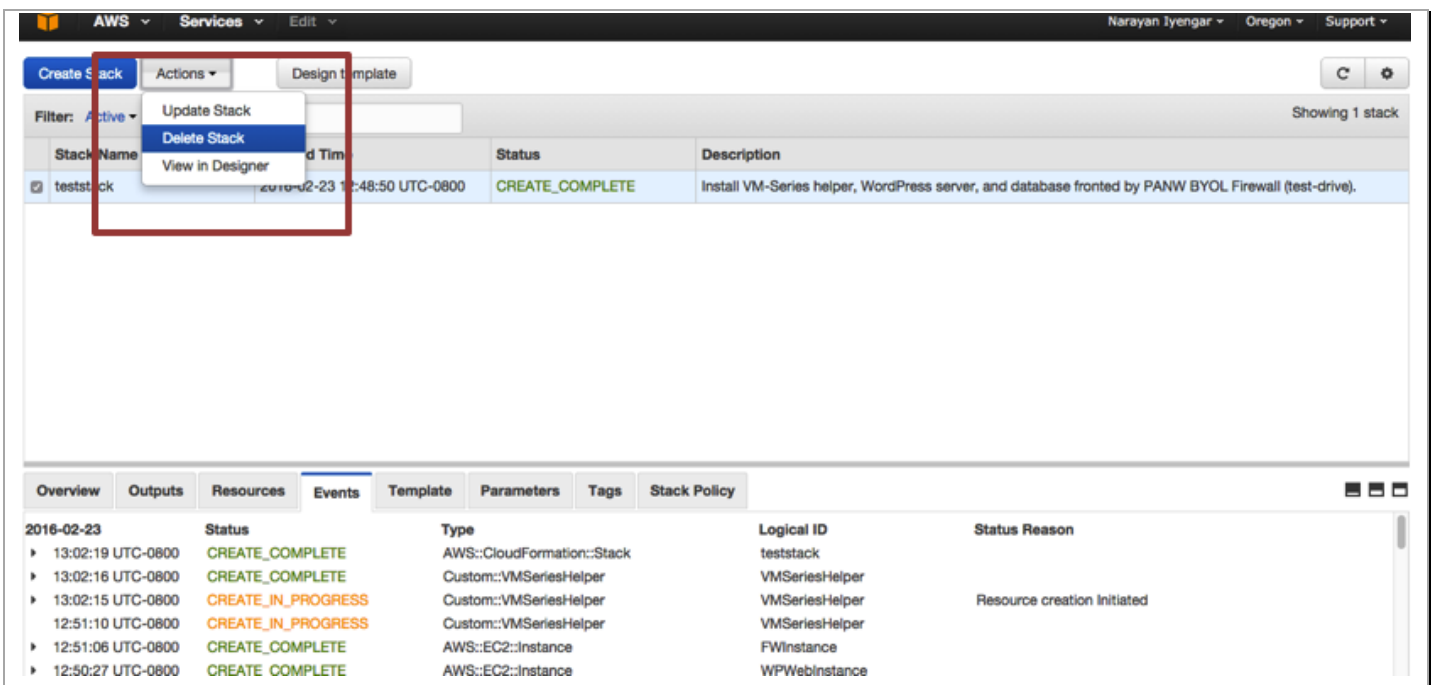
The screenshot shows the AWS CloudFormation console. The stack 'teststack' is in a 'ROLLBACK\_COMPLETE' state. The 'Events' tab is selected, showing a list of events. A red box highlights an error message: 'The following resource(s) failed to create: [FWInstance]. Rollback requested by user. In order to use this AWS Marketplace product you need to accept terms and subscribe. To do so please visit <http://aws.amazon.com/marketplace/pp?sku=6kxdw3bbmdeda3o6i1ggq4km>'.

Stack Name	Created Time	Status	Description
teststack	2016-02-25 10:00:34 UTC-0800	ROLLBACK_COMPLETE	Install VM-Series helper, WordPress server, and database fronted by PANW BYOL Firewall (test-drive).

Event ID	Timestamp	Type	Resource	Status
10:21:14 UTC-0800	DELETE_IN_PROGRESS	AWS::IAM::AccessKey	AWSMonitorUserKey	
10:21:08 UTC-0800	ROLLBACK_IN_PROGRESS	AWS::CloudFormation::Stack	teststack	
10:21:07 UTC-0800	CREATE_FAILED	AWS::EC2::Instance	FWInstance	
10:02:23 UTC-0800	CREATE_COMPLETE	AWS::EC2::Instance	WPWebInstance	
10:02:23 UTC-0800	CREATE_COMPLETE	AWS::EC2::Instance	WPDBServerInstance	
10:02:15 UTC-0800	CREATE_IN_PROGRESS	AWS::EC2::Instance	FWInstance	
10:02:13 UTC-0800	CREATE_COMPLETE	AWS::EC2::EIPAssociation	FWEIPAssociation	

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.



The screenshot shows the AWS CloudFormation console. The stack 'teststack' is in a 'CREATE\_COMPLETE' state. The 'Actions' menu is open, showing options: 'Update Stack', 'Delete Stack', and 'View in Designer'. The 'Delete Stack' option is highlighted.

Stack Name	Created Time	Status	Description
teststack	2016-02-23 12:48:50 UTC-0800	CREATE_COMPLETE	Install VM-Series helper, WordPress server, and database fronted by PANW BYOL Firewall (test-drive).

Timestamp	Status	Type	Logical ID	Status Reason
13:02:19 UTC-0800	CREATE_COMPLETE	AWS::CloudFormation::Stack	teststack	
13:02:16 UTC-0800	CREATE_COMPLETE	Custom::VMSeriesHelper	VMSeriesHelper	
13:02:15 UTC-0800	CREATE_IN_PROGRESS	Custom::VMSeriesHelper	VMSeriesHelper	Resource creation initiated
12:51:10 UTC-0800	CREATE_IN_PROGRESS	Custom::VMSeriesHelper	VMSeriesHelper	
12:51:06 UTC-0800	CREATE_COMPLETE	AWS::EC2::Instance	FWInstance	
12:50:27 UTC-0800	CREATE_COMPLETE	AWS::EC2::Instance	WPWebInstance	

## 6. Review what was created

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

The screenshot displays the Amazon Web Services console with various services organized into categories. The 'Networking' category is highlighted with a red box, showing the following services:

- VPC** (Isolated Cloud Resources)
- Direct Connect** (Dedicated Network Connection to AWS)
- Route 53** (Scalable DNS and Domain Name Registration)

Other categories and services visible include:

- Compute:** EC2, EC2 Container Service, Elastic Beanstalk, Lambda
- Storage & Content Delivery:** S3, CloudFront, Elastic File System (PREVIEW), Glacier, Import/Export Snowball, Storage Gateway
- Database:** RDS, DynamoDB, ElastiCache, Redshift, DMS (PREVIEW)
- Developer Tools:** CodeCommit, CodeDeploy, CodePipeline
- Management Tools:** CloudWatch, CloudFormation, CloudTrail, Config, OpsWorks, Service Catalog, Trusted Advisor
- Security & Identity:** Identity & Access Management, Directory Service, Inspector (PREVIEW), WAF, Certificate Manager
- Analytics:** EMR, Data Pipeline, Elasticsearch Service
- Internet of Things:** AWS IoT
- Game Development:** GameLift
- Mobile Services:** Mobile Hub, Cognito, Device Farm, Mobile Analytics, SNS
- Application Services:** API Gateway, AppStream, CloudSearch, Elastic Transcoder, SES, SQS, SWF
- Enterprise Applications:** WorkSpaces, WorkDocs, WorkMail

Here you should see all VPCs created in your account:

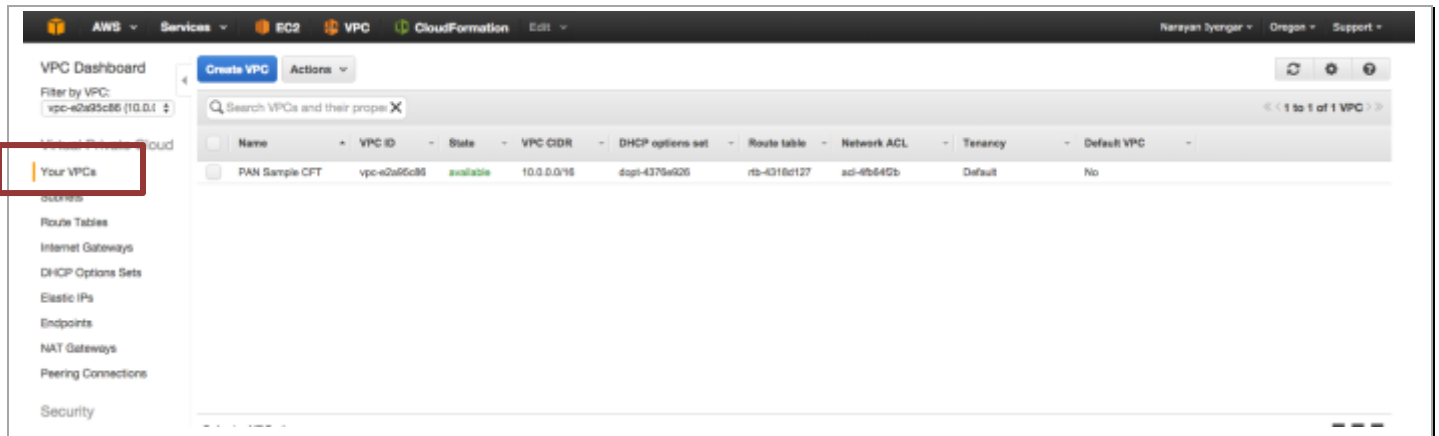
The screenshot shows the AWS VPC Dashboard. The top navigation bar includes the AWS logo, 'AWS' dropdown, 'Services' dropdown, and 'Edit' dropdown. The left sidebar contains a 'VPC Dashboard' section with a 'Filter by VPC:' dropdown set to 'None'. Below this is a list of VPC-related services: Virtual Private Cloud, Your VPCs, Subnets, Route Tables, Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, NAT Gateways, Peering Connections, Security, Network ACLs, Security Groups, VPN Connections, Customer Gateways, Virtual Private Gateways, and VPN Connections. The main content area is titled 'Resources' and features two buttons: 'Start VPC Wizard' and 'Launch EC2 Instances'. A note states: 'Note: Your Instances will launch in the US West (Oregon) region.' Below this, a message says: 'You are using the following Amazon VPC resources in the US West (Oregon) region:'. A table of resources follows, with '3 VPCs' highlighted by a red box. The resources are:

3 VPCs	3 Internet Gateways
7 Subnets	6 Route Tables
4 Network ACLs	3 Elastic IPs
0 VPC Peering Connections	0 Endpoints
0 Nat Gateways	5 Security Groups
4 Running Instances	0 VPN Connections
0 Virtual Private Gateways	0 Customer Gateways

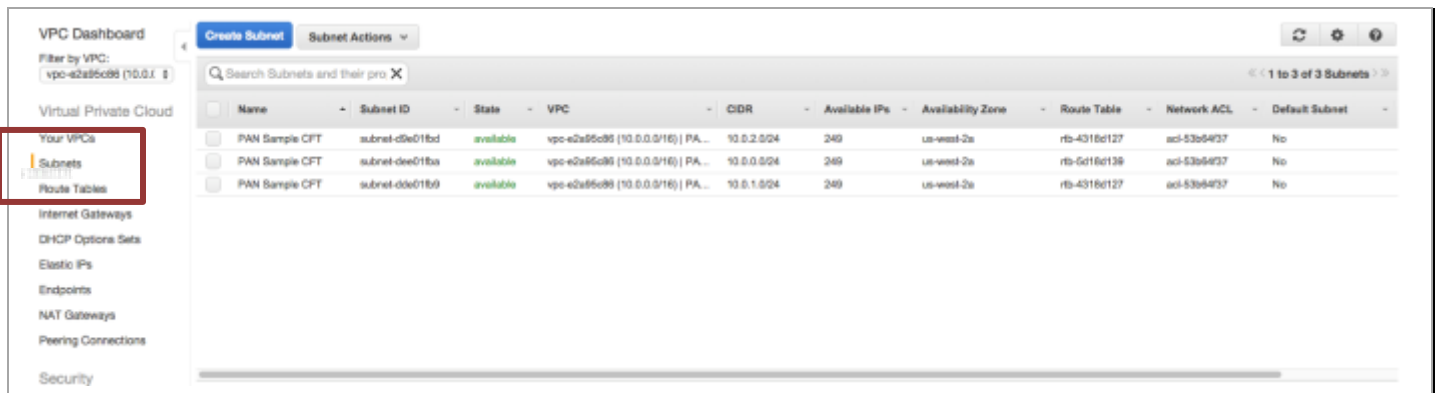
Below the resource list is a section titled 'VPN Connections' with a description: 'Amazon VPC enables you to use your own isolated resources within the AWS cloud, and then connect those resources directly to your own datacenter using industry-standard encrypted IPsec VPN connections.' and a 'Create VPN Connection' button.

## Palo Alto Networks AWS CFT Deployment Guide

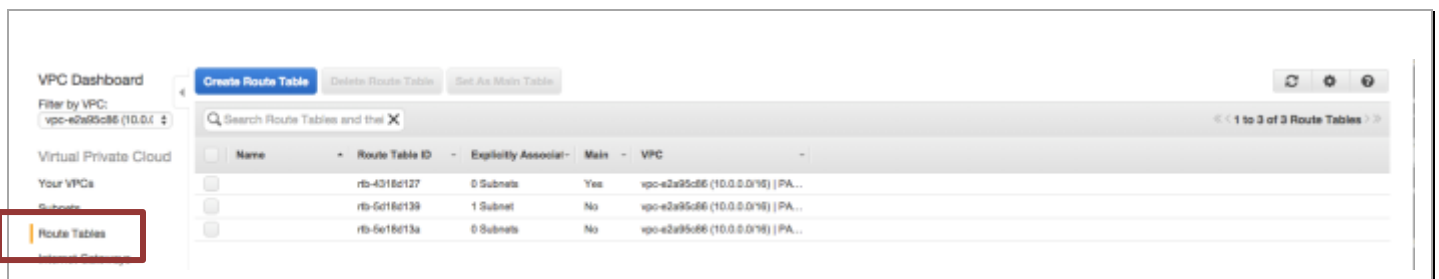
Here is the sample **VPC**:



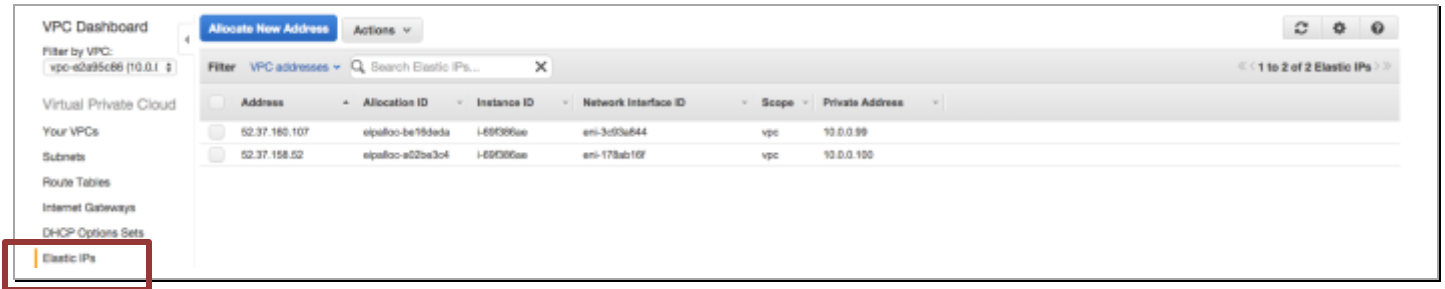
On the left you can review **subnets**:



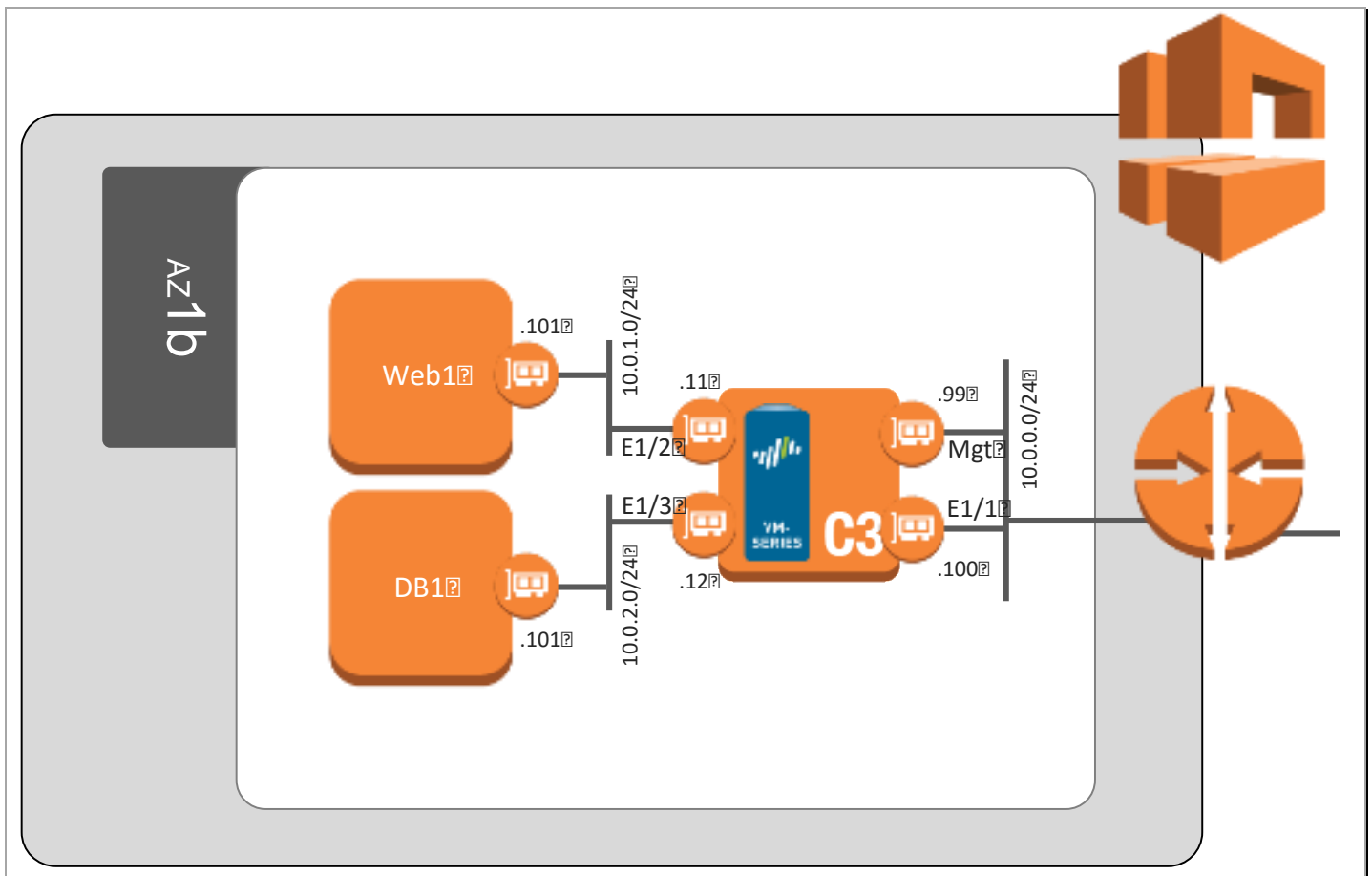
**Route tables:**



And **Elastic IPs (EIPs)**:



All of this matches the topology shown previously:



## 7. Access the 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:

## Palo Alto Networks AWS CFT Deployment Guide

Stack Name: teststack, Created Time: 2016-02-23 12:48:50 UTC-0800, Status: CREATE\_COMPLETE, Description: Install VM-Series helper, WordPress server, and database fronted by PANW BYOL Firewall (test-drive).

Key	Value	Description
FirewallManagementURL	https://52.37.63.159	VM-Series management interface URL
WordpressURL	http://52.37.79.157/wordpress	Wordpress server

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

General Information:

- Device Name: PA-VM
- MGT IP Address: 10.0.0.99
- MGT Netmask: 255.255.255.0
- MGT Default Gateway: 10.0.0.1
- MGT IPv6 Address: unknown
- MGT IPv6 Link Local Address: fe80::56:5ff:fedc:839b/64
- MGT IPv6 Default Gateway: unknown
- MGT MAC Address: 02:56:05:dc:83:9b
- Model: PA-VM
- Serial #: AWSMKTJF71E8730
- CPU ID: AWSMKT:6lodw3bbmdeda3o61ggq4km:us-west-2
- UUID: EC26D787-4347-60A3-1B61-D0CA98F6950C
- VM License: VM-300
- VM Mode: Amazon AWS
- Software Version: 7.0.1
- GlobalProtect Agent: 0.0.0
- Application version: 561-3150 (02/19/16)
- Threat Version: 561-3150 (02/19/16)
- URL Filtering version: 0000.00.00.000
- Time: Tue Feb 23 13:41:09 2016
- Uptime: 0 days, 0:49:58

System Resources:

- Management CPU: 2%
- Data Plane CPU: 1%
- Session Count: 0 / 249998

System Logs:

Description	Time
User admin logged in via Web from 199.167.55.50 using https	02/23 13:40:17
authenticated for user 'admin'. From: 199.167.55.50.	02/23 13:40:17
vm-info-source aws-monitor(vsys1): Connected to ec2.us-west-2.amazonaws.com, status	02/23 13:21:25
Content update job succeeded for user admin	02/23 13:03:11
Config installed	02/23 13:03:11
Wildfire package upgraded from version <unknown version> to 0 by admin	02/23 13:02:34
Threat detection package upgraded from version 0 to 561-3150 by admin	02/23 13:02:34
Application Identification package upgraded from version 497-2688 to 561-3150 by admin	02/23 13:02:34
Correlation object 6001 added	02/23 13:02:27
Correlation object 6006 added	02/23 13:02:27

Config Logs:

Command	Path	Admin	Time
commit		admin	02/23 13:00:12
set	vsys vsys1 rulebase nat rules Outbound nat	admin	02/23 13:00:09
set	vsys vsys1 rulebase nat rules WordPress NAT	admin	02/23 13:00:09
set	vsys vsys1 rulebase nat rules DB SSH	admin	02/23 13:00:09
set	vsys vsys1 rulebase nat rules Web SSH	admin	02/23 13:00:08
set	vsys vsys1 rulebase security rules Log default deny	admin	02/23 13:00:08
set	vsys vsys1 rulebase security rules Web to DB	admin	02/23 13:00:07
set	vsys vsys1 rulebase security rules Allow all outbound	admin	02/23 13:00:07
set	vsys vsys1 rulebase security rules Web browsing	admin	02/23 13:00:07
set	vsys vsys1 rulebase security rules Allow all ping	admin	02/23 13:00:06

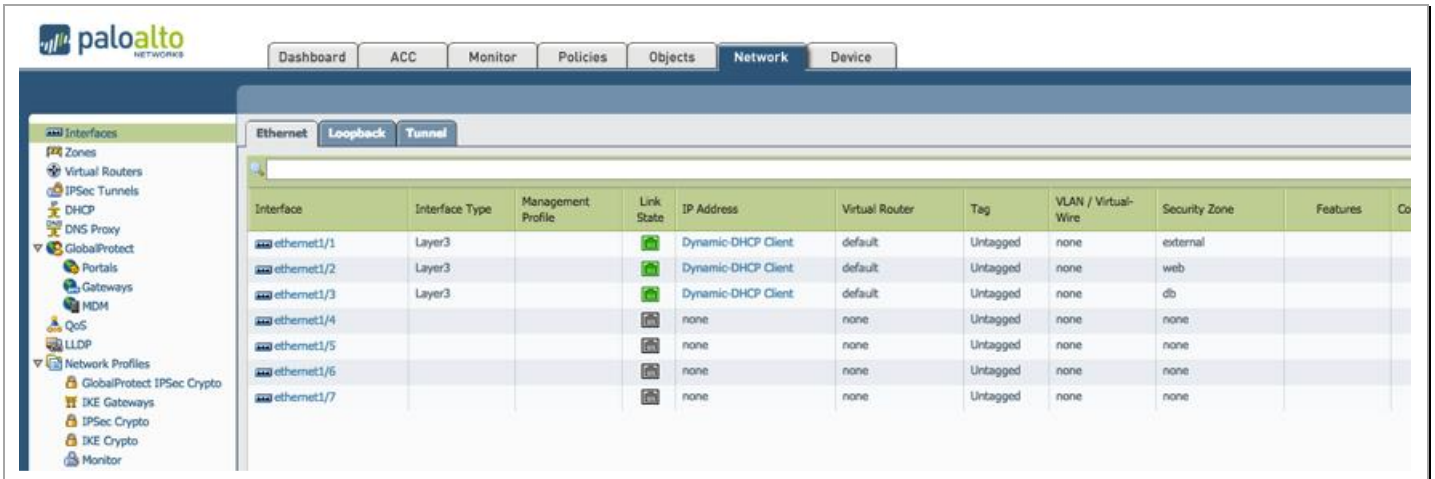
Locks: No locks found

ACC Risk Factor (Last 60 minutes): 4.0

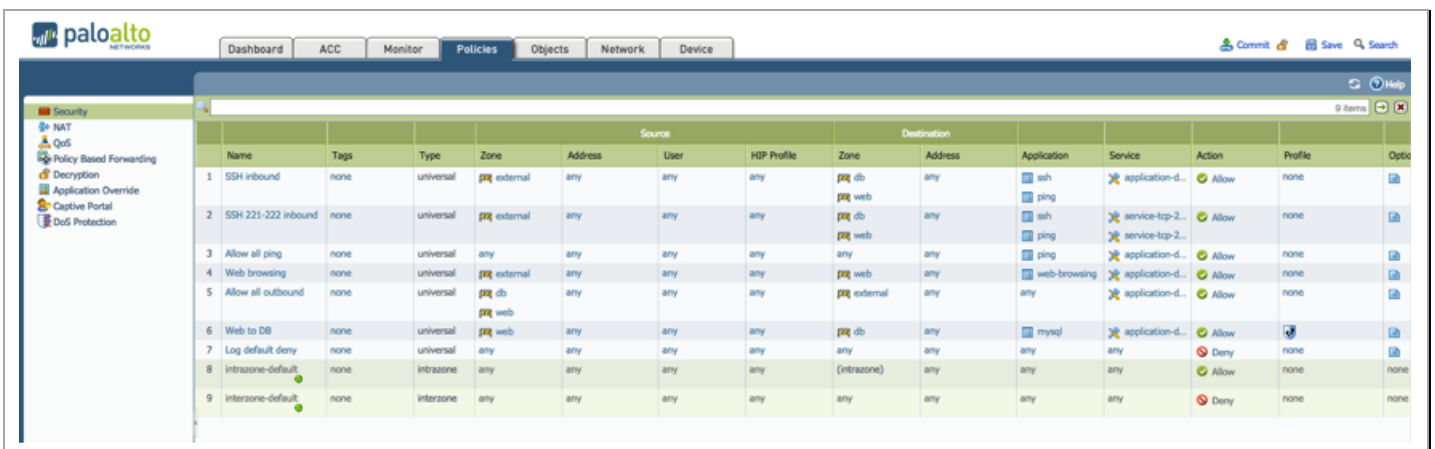
Here are the interfaces to zone mappings:



## Palo Alto Networks AWS CFT Deployment Guide



In the policies tab you can review the security policies:



These policies are defined to allow ssh access on ports 221 and 222 to the web and db server respectively (for troubleshooting purposes), secures N/S traffic and E/W traffic between zones.

And the NAT policies allow for ssh access to the web and db servers as well as directing web traffic to the web server only. There is also a rule for source NAT from web and db servers to the outside world.

paloalto

networks

Dashboard

ACC

Monitor

Policies

Objects

Network

Device

Commit

Save

Search

Security

NAT

QoS

Policy Based Forwarding

Decryption

Application Override

Captive Portal

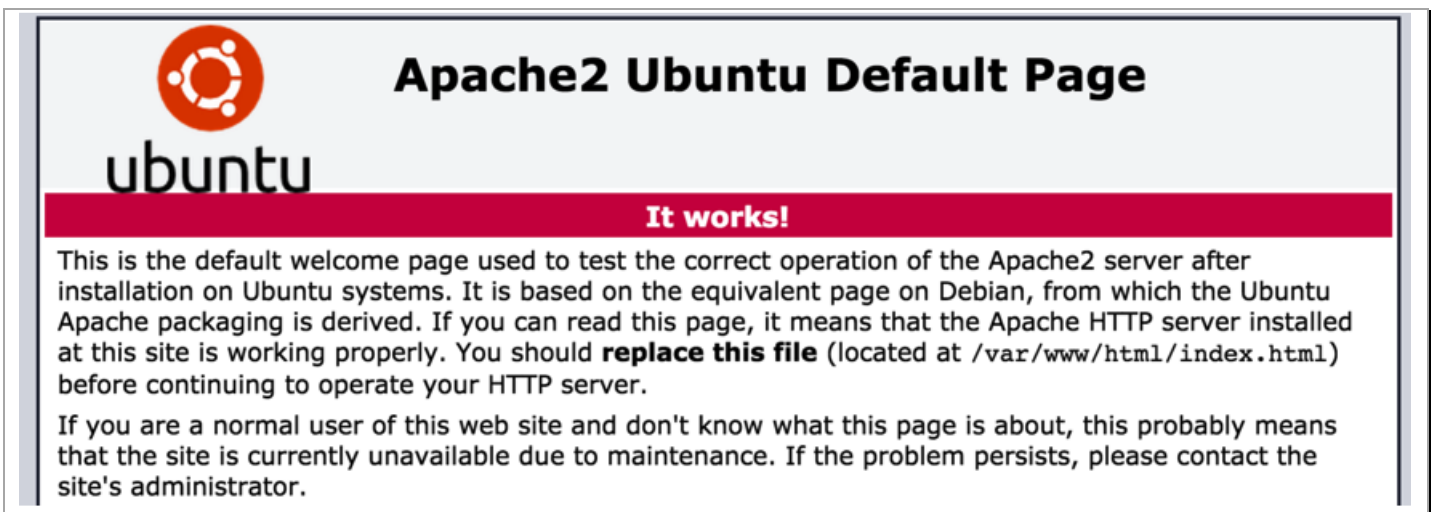
DoS Protection

4 items

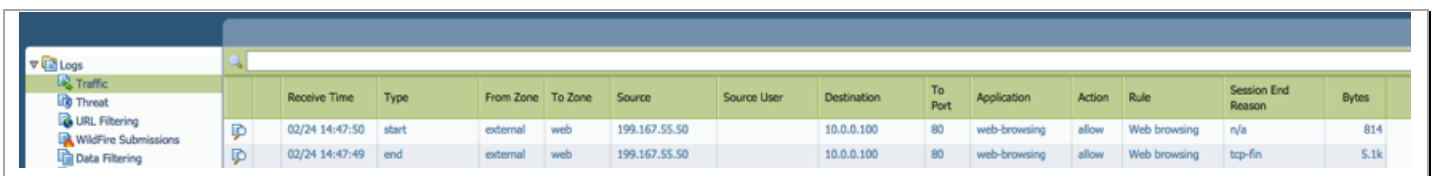
	Original Packet							Translated Packet		
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	Web SSH	none	external	external	any	any	10.0.0.100	service-tcp-2...	dynamic-ip-and-port ethernet1/2	address: 10.0.1.101 port: 22
2	DB SSH	none	external	external	any	any	10.0.0.100	service-tcp-2...	dynamic-ip-and-port ethernet1/3	address: 10.0.2.101 port: 22
3	WordPress NAT	none	external	external	any	any	10.0.0.100	service-http	dynamic-ip-and-port ethernet1/2	address: 10.0.1.101 port: 80
4	Outbound nat	none	db	external	any	any	any	any	dynamic-ip-and-port ethernet1/1	none

## 8. Access the Webserver

Using the second URL in the output tab access the static content of the webserver so in a web browser just type <http://<webserver-IP>> and you should see:



Check firewall logs to verify that the traffic is passing through the firewall:

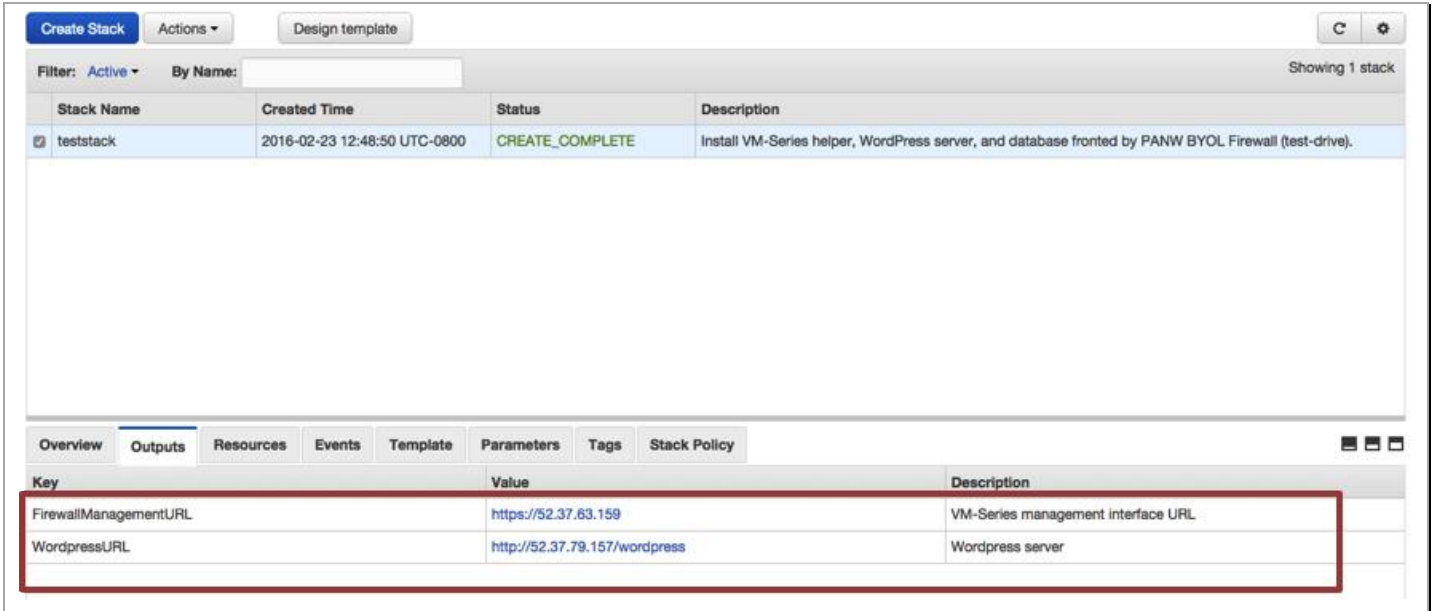


The screenshot shows the Palo Alto Networks Firewall Logs interface. The 'Logs' tab is selected, and a table lists log entries. The table columns include Receive Time, Type, From Zone, To Zone, Source, Source User, Destination, To Port, Application, Action, Rule, Session End Reason, and Bytes.

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
02/24 14:47:50	start	external	web	199.167.55.50		10.0.0.100	80	web-browsing	allow	Web browsing	n/a	814
02/24 14:47:49	end	external	web	199.167.55.50		10.0.0.100	80	web-browsing	allow	Web browsing	tcp-fin	5.1k

Now let us verify we pass east-West traffic through the firewall. In the browser, head to the wordpress server (<http://<webserver-IP/wordpress>>), this should be the second link in the AWS console **Outputs** tab:

## Palo Alto Networks AWS CFT Deployment Guide

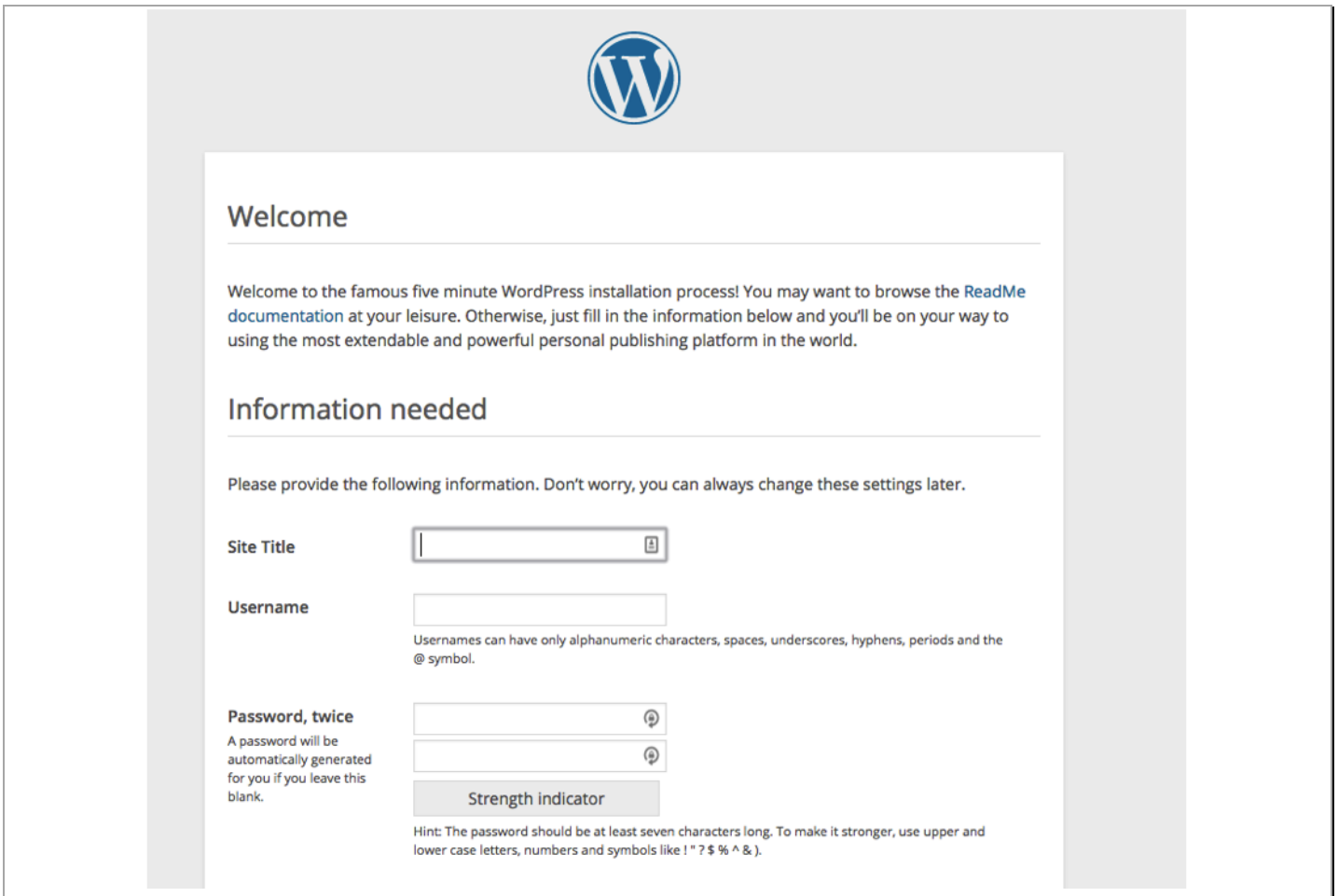


Stack Name	Created Time	Status	Description
teststack	2016-02-23 12:48:50 UTC-0800	CREATE_COMPLETE	Install VM-Series helper, WordPress server, and database fronted by PANW BYOL Firewall (test-drive).

Key	Value	Description
FirewallManagementURL	<a href="https://52.37.63.159">https://52.37.63.159</a>	VM-Series management interface URL
WordpressURL	<a href="http://52.37.79.157/wordpress">http://52.37.79.157/wordpress</a>	Wordpress server

And you should see the WordPress welcome screen:



### Welcome

Welcome to the famous five minute WordPress installation process! You may want to browse the [ReadMe documentation](#) at your leisure. Otherwise, just fill in the information below and you'll be on your way to using the most extendable and powerful personal publishing platform in the world.

### Information needed

Please provide the following information. Don't worry, you can always change these settings later.

**Site Title**

**Username**   
Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods and the @ symbol.

**Password, twice**  
A password will be automatically generated for you if you leave this blank.

**Strength indicator**

Hint: The password should be at least seven characters long. To make it stronger, use upper and lower case letters, numbers and symbols like ! " ? \$ % ^ & ).

**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.

Now, head back to the firewall and verify that the traffic did indeed go through the firewall from web to db :

02/24 14:51:49	start	web	db	10.0.1.101	10.0.2.101	3306	mysql	allow	Web to DB	n/a	375
02/24 14:51:48	start	web	db	10.0.1.101	10.0.2.101	3306	mysql	allow	Web to DB	n/a	375
02/24 14:51:48	start	external	web	199.167.55.50	10.0.0.100	80	web-browsing	allow	Web browsing	n/a	705

You have now successfully deployed a cloud formation template with a VM-Series firewall in AWS.

## 9. Launch some attacks

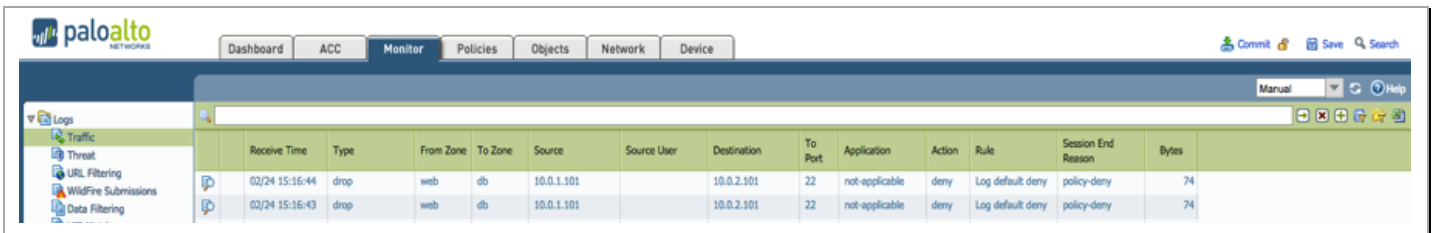
### 9.1 SSH from Web Server to DB Server

Let's 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.

Go to <http://<webserver-IP>/sql-attack.html> and simulate a web to db ssh attempt by clicking on the **LAUNCH WEB TO DB SSH ATTEMPT**.

**LAUNCH WEB TO DB SSH ATTEMPT**

This launches a CGI script that attempts to ssh as root to the db server from the web server. Now return to the firewall's monitor tab to note the failed traffic:



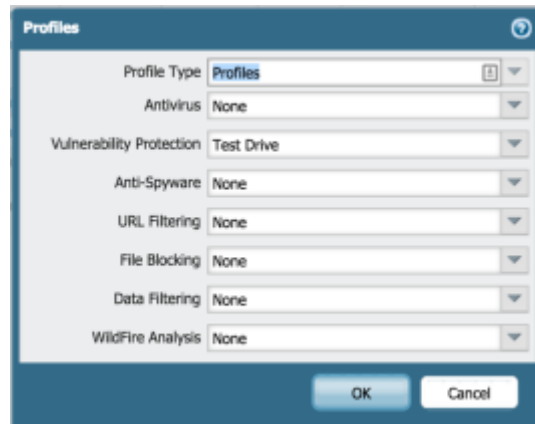
Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
02/24 15:16:44	drop	web	db	10.0.1.101		10.0.2.101	22	not-applicable	deny	Log default deny	policy-deny	74
02/24 15:16:43	drop	web	db	10.0.1.101		10.0.2.101	22	not-applicable	deny	Log default deny	policy-deny	74

## 9.2 SQL Brute force attack

On the firewall's security policies tab, under Security, Rule 6, you will notice that the web to db traffic is protected further by a vulnerability profile:

	Name	Tags	Type	Source				Destination				Action	Profile	Options
				Zone	Address	User	HIP Profile	Zone	Address	Application	Service			
1	SSH inbound	none	universal	external	any	any	any	db	any	ssh	application-default	Allow	none	
2	SSH 221-222 inbound	none	universal	external	any	any	any	db	any	ssh	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	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



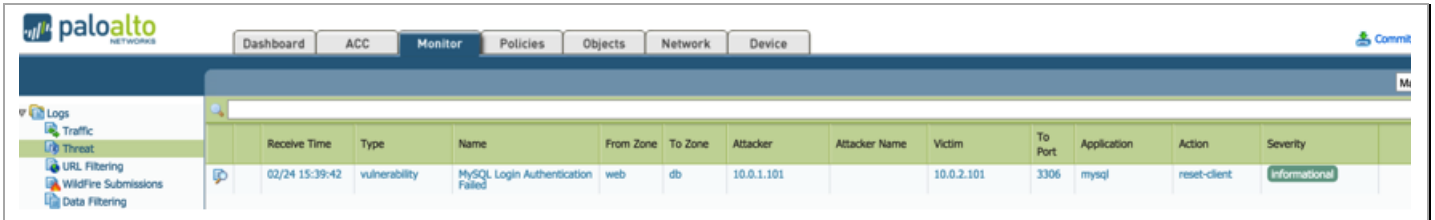
Note the Vulnerability Protection profile. This is a custom profile created just for this lab. It is part of the default vulnerability protection profile but is called out separately for the purpose of this demo environment.

Let's finally trigger the attack. Head back to the sql-attack.html page at <https://<webserver-IP>/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

This 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. Now return to the firewall and click the Monitor tab and then click on Threats in the left hand pane under Logs and notice the new vulnerability log message regarding the failed MySQL events:



The screenshot shows the Palo Alto Networks VM-Series firewall interface. The 'Monitor' tab is selected, and the 'Threats' section is expanded in the left-hand pane. A table displays a single log entry for a vulnerability event.

Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity
02/24 15:39:42	vulnerability	MySQL Login Authentication Failed	web	db	10.0.1.101		10.0.2.101	3306	mysql	reset-client	Informational

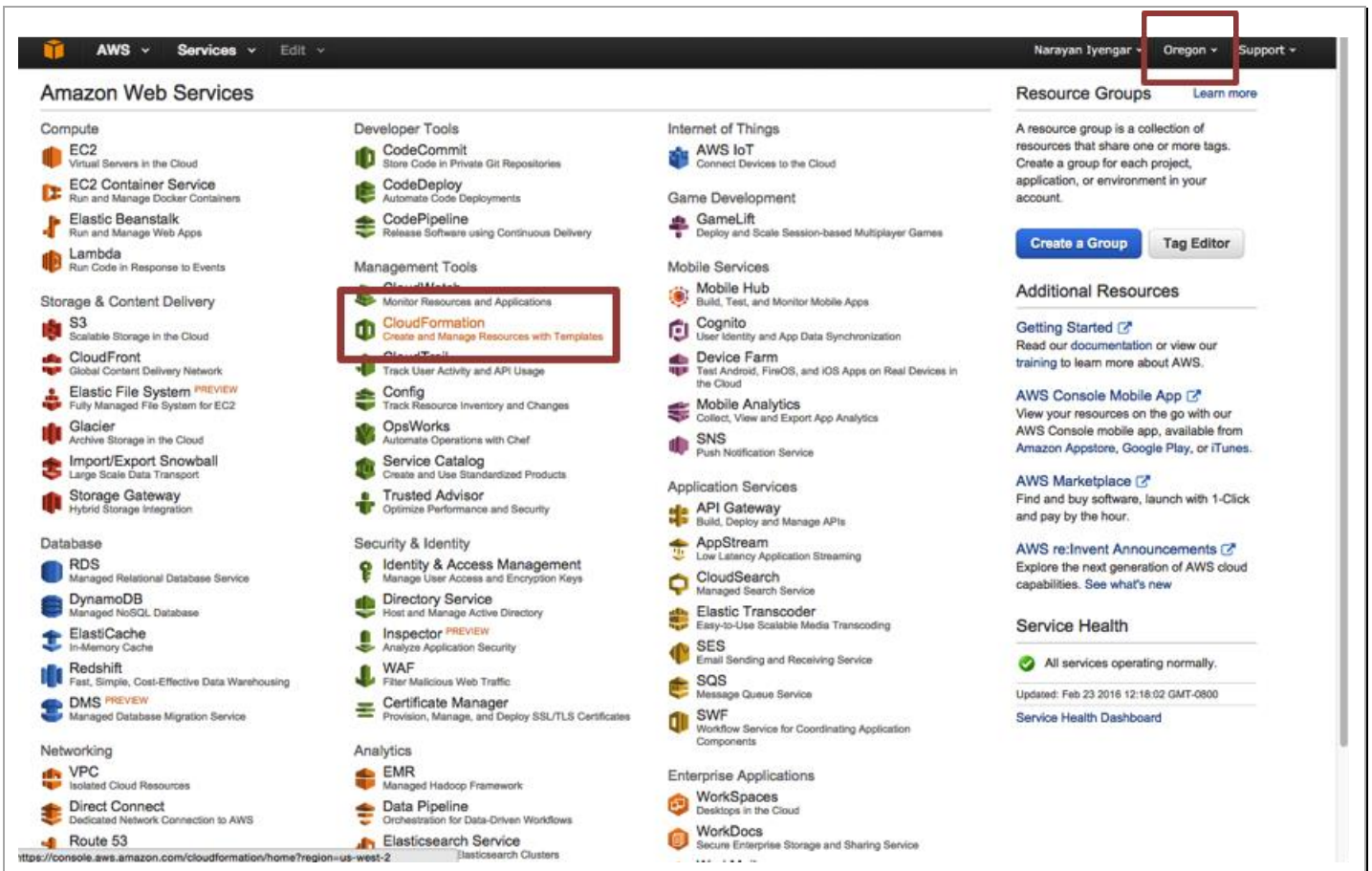
The CGI script you launched above attempted to login to the MySQL database multiple times with an incorrect password. The VM-Series firewall saw this activity and using the vulnerability profile, reset the connection and logged the activity.



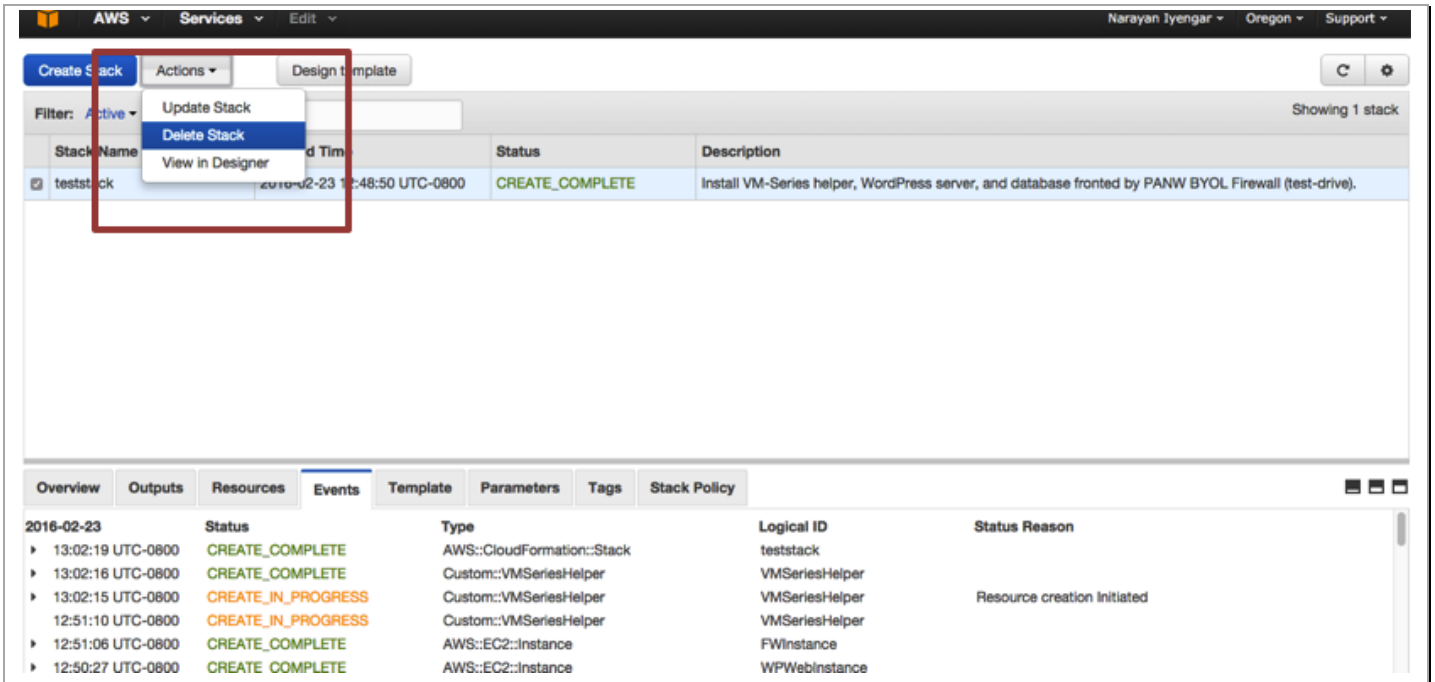
# 10. Cleanup

## 10.1 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**:



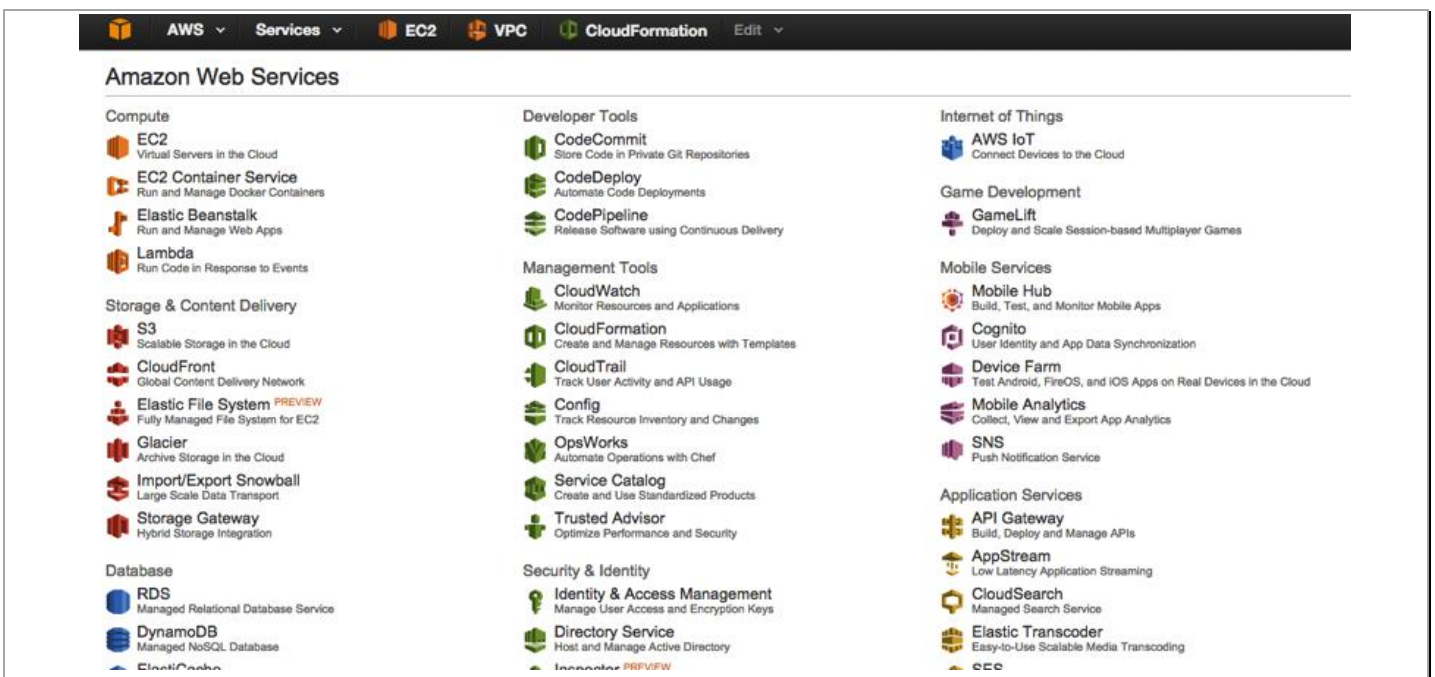
Under **Actions**, click **Delete Stack**:



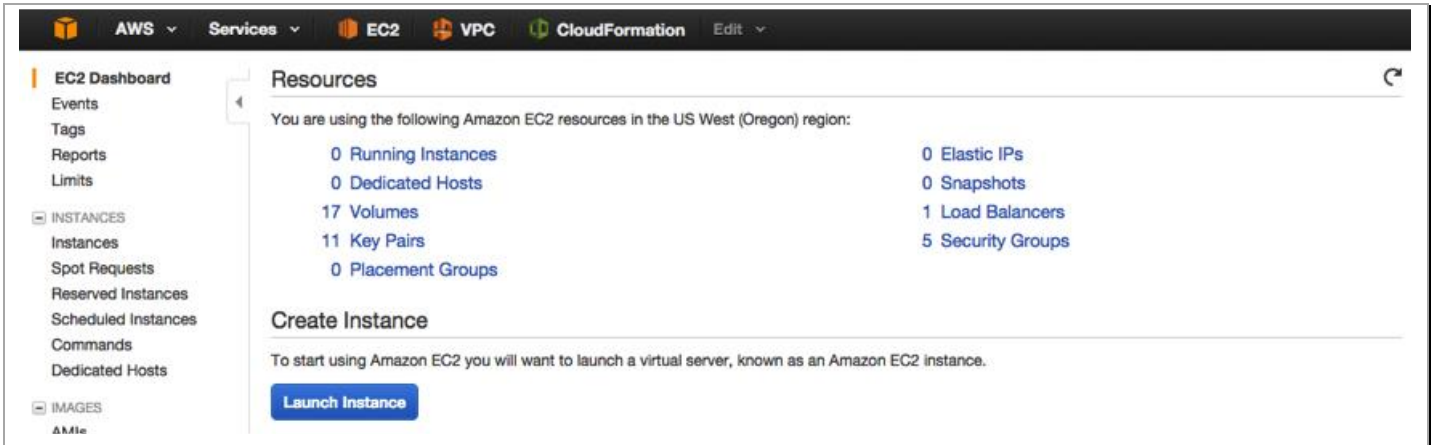
This should delete all the resources created via the template and release any Elastic IPs associated with the firewall.

## 10.2 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:



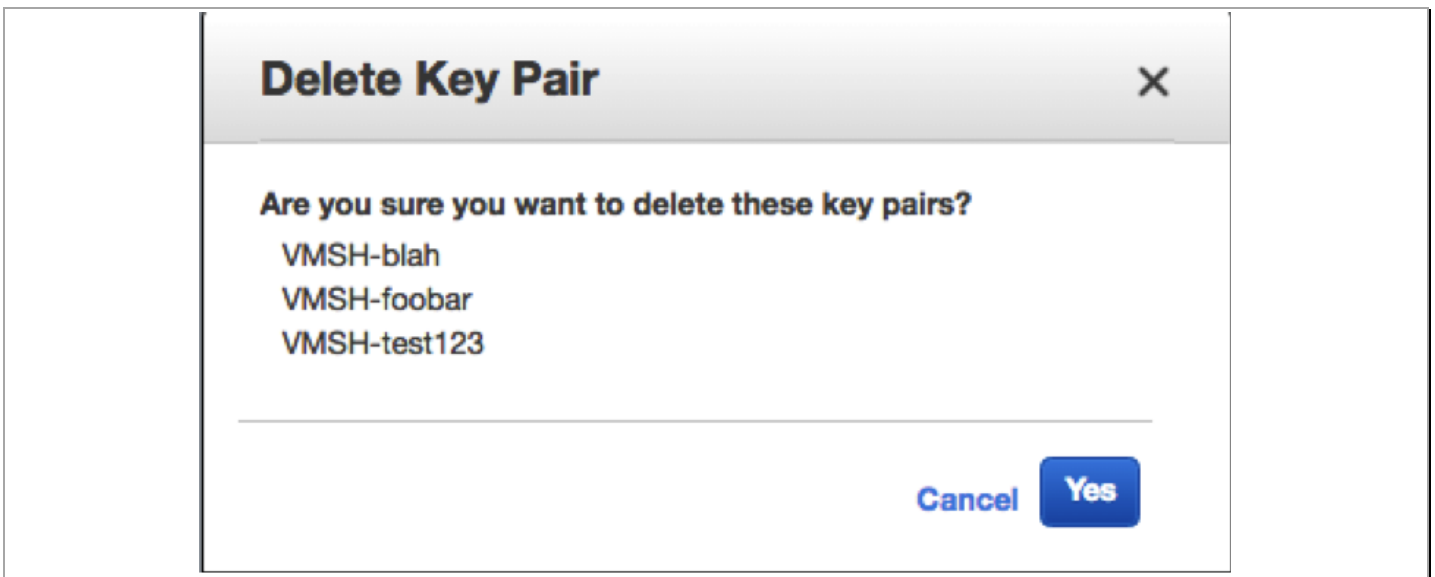
Click on **Key Pairs**:



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



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



## 11. 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:

Overview	Outputs	Resources	Events	Template	Parameters	Tags	Stack Policy	Change Sets
2016-08-12								
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, subnetac1, route1, BootstrapRole, FWPPrivate13NetworkInterface, WPDGServerInstance]. 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::SubnetNetworkAssociation	subnetac1			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	WPDGServerInstance			Your requested instance type (t1.micro) is not supported in your requested Availability Zone (us-east-1a). 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.

Overview	Outputs	Resources	Events	Template	Parameters	Tags	Stack Policy	Change Sets
09-09-02 UTC-0600								
09-09-02 UTC-0600		CREATE_COMPLETE		AWS::EC2::NetworkInterface	actb0608d4			Resource creation initiated
09-09-02 UTC-0600		CREATE_IN_PROGRESS		AWS::EC2::VPCHCPOptionsAssociation	dchpassoc1			Resource creation initiated
09-09-02 UTC-0600		CREATE_IN_PROGRESS		AWS::EC2::RouteTable	rtb009a2460			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::NetworkInterface	actb765dbd2			Resource creation initiated
09-09-01 UTC-0600		CREATE_IN_PROGRESS		AWS::EC2::VPCHCPOptionsAssociation	dchpassoc1			Resource creation initiated
09-09-01 UTC-0600		CREATE_IN_PROGRESS		AWS::EC2::RouteTable	rtb009a2460			Resource creation initiated

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 bootstrapping 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.