

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

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 Review and accept the EULA	6
4.3 Create and download an SSH keypair	11
4.4 Create a Bootstrap Bucket.....	12
4.5 Download Bootstrap Files and CFT from GitHub.....	14
4.6 Check Elastic IPs	19
5. Launch the Two-tier CFT	21
5.1 Create CloudFormation Stack.....	21
5.2 Review Resources Created by the Template	25
6. VM-Series Access and WebUI Review	28
6.1 Access VM-Series Firewall	28
6.2 Login and Dashboard Summary	29
6.3 Review Application Command Center (ACC)	30
6.4 Review Security Policies	32
6.5 Review The Monitor Tab	33
6.6 Review Object, Network and Device Tabs.....	34
7. Securing Applications	35
7.1 Verify Static Content on Web Server	35
7.2 Verify Dynamic Content on Web Server	36
7.3 SSH attack from the Web to the DB Server.....	37
7.4 SQL attack from the Web to the DB Server	39
7.5 Review Threat Protection Profile	40
8. Cleanup	41
8.1 Delete the Stack.....	41
8.2 Delete keys	42
9. Conclusion.....	44

Appendix A.....	45
Troubleshooting tips	45

Version History

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

1. About CFTs

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

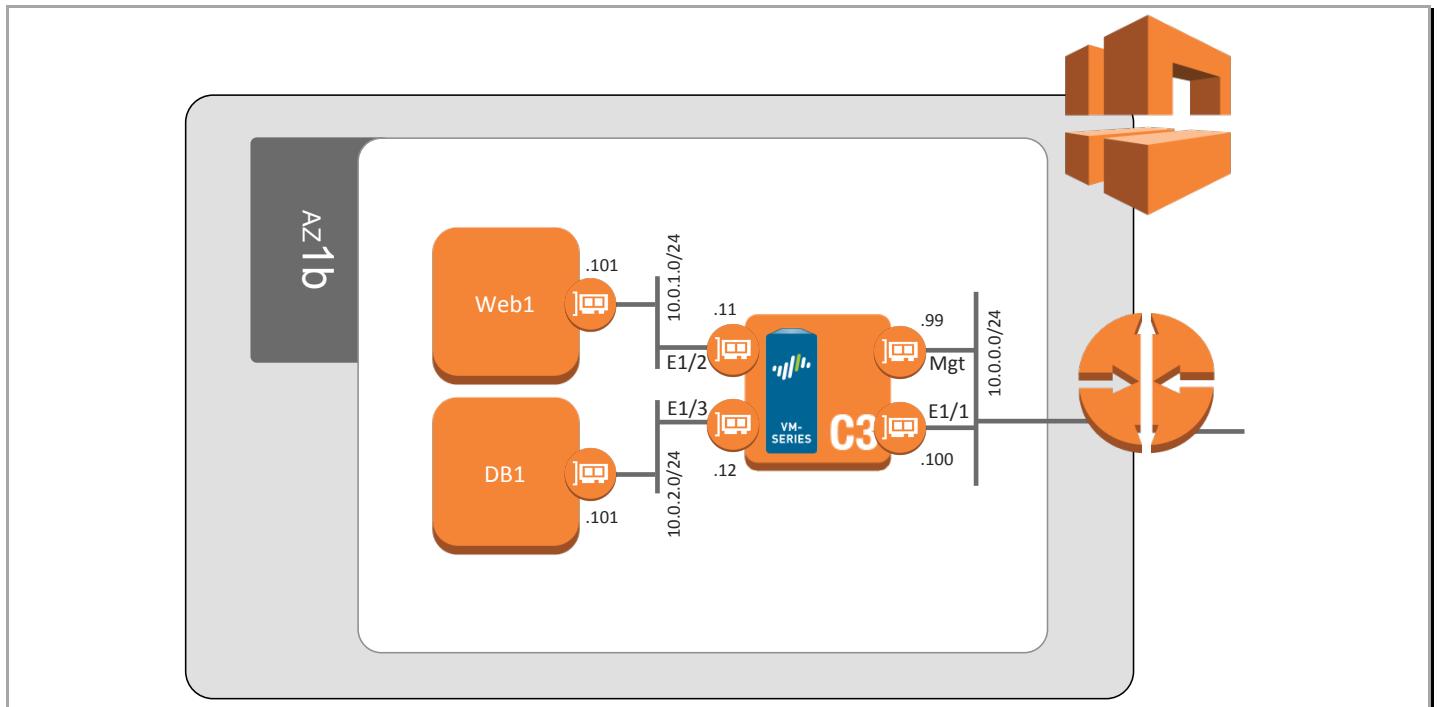
For more information on CFTs and sample CFTs refer to Amazon's documentation

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

There are also many sample templates available here

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/sample-templates-services-us-west-2.html>

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



2. Support Policy

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

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

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

3. Instances used

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

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

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

4. Prerequisites

Here are the prerequisites required to successfully launch this template.

4.1 Create an AWS account

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

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

4.2 Review and accept the EULA

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

Click on **AWS Marketplace**.

Palo Alto Networks AWS CFT Deployment Guide

The screenshot shows the AWS Management Console with the navigation pane open. The 'AWS services' section is visible, displaying various service categories and their sub-components. A red box highlights the 'AWS Marketplace' section on the right, which contains links for discovering, procuring, and deploying popular software products.

Search for Palo Alto Networks firewall

The screenshot shows the AWS Marketplace search results for 'Palo Alto Networks'. The search bar at the top has 'Palo Alto Networks' typed into it. Below the search bar, there are three search results: 'Palo Alto Networks', 'Palo Alto Networks firewall', and 'Palo Alto Networks firewall bundle 2'. The first result, 'Palo Alto Networks', is the main listing. It features a large image with the text 'PROTECT MISSION-CRITICAL APPLICATIONS' and 'VM-Series: Next-Generation Firewall for the Cloud'. It also includes a 'FREE TRIAL AVAILABLE' button and a note about infrastructure costs. Below this listing are 'Popular Categories' with icons and names: Operating Systems, Security, Networking, Storage, Business Intelligence, Databases, Dev Ops, View All Categories, and SaaS Subscriptions.

Palo Alto Networks AWS CFT Deployment Guide

Palo Alto Networks (3 results) showing 1 - 3

The screenshot shows the search results for "Palo Alto Networks" in the AWS Marketplace. The first result is highlighted with a red border:

VM-Series Next-Generation Firewall Bundle 2
★★★★★ (3) | Version PAN-OS 8.0.3 | Sold by Palo Alto Networks
Starting from \$1.28/hr or from \$4,500.00/yr (60% savings) for software + AWS usage fees
The VM-Series complements AWS Security Groups and Network ACLs, by uniquely classifying and controlling your AWS traffic based on the application identity, and applying Threat...
Linux/Unix, Other PAN-OS 8.0.3 - 64-bit Amazon Machine Image (AMI)

Below it are two more results:

VM-Series Next-Generation Firewall Bundle 1
★★★★★ (1) | Version PAN-OS 8.0.3 | Sold by Palo Alto Networks
Starting from \$0.86/hr or from \$3,000.00/yr (60% savings) for software + AWS usage fees
The VM-Series complements AWS Security Groups and Network ACLs, by uniquely classifying and controlling your AWS traffic based on the application identity, and applying Threat...
Linux/Unix, Other PAN-OS 8.0.3 - 64-bit Amazon Machine Image (AMI)

VM-Series Next-Generation Firewall (BYOL)
★★★★★ (1) | Version PAN-OS 8.0.3 | Sold by Palo Alto Networks
The VM-Series complements AWS Security Groups and Network ACLs by uniquely classifying and controlling your AWS traffic based on the application identity, and applying Threat...
Linux/Unix, Other PAN-OS 8.0.3 - 64-bit Amazon Machine Image (AMI)

At the bottom left, it says "showing 1 - 3".

Select VM-Series Next Generation Firewall Bundle 2

The screenshot shows the product page for the VM-Series Next-Generation Firewall Bundle 2. The main title is "VM-Series Next-Generation Firewall Bundle 2" with a "Free Trial" badge.

Sold by: Palo Alto Networks | See product video

15 Day Free Trial Available - The VM-Series complements AWS Security Groups and Network ACLs, by uniquely classifying and controlling your AWS traffic based on the application identity, and applying Threat Prevention policies to block known and unknown cyberattacks. With the VM-Series, you can quickly create a hybrid architecture that extends your existing datacenter onto AWS via an IPsec VPN tunnel. As your AWS deployment grows, application whitelisting and segmentation policies can be implemented to maintain compliance and improve your security posture by preventing cyberattacks from moving laterally from VPC-to-VPC... [Read more](#)

Customer Rating: ★★★★★ (3 Customer Reviews)

Latest Version: PAN-OS 8.0.3 ([Other available versions](#))

Operating System: Linux/Unix, Other PAN-OS 8.0.3

Delivery Method: 64-bit Amazon Machine Image (AMI) ([Read more](#))

Support: [See details below](#)

AWS Services Required: Amazon EC2, Amazon EBS

Highlights:

- Integration with AWS Auto Scaling and ELB enables continual protection of dynamic workloads.
- Optimized for performance of up to 4Gbps of firewall throughput and increased capacities using AWS Enhanced

Continue button (highlighted with a red box). A tooltip says: "You will have an opportunity to review your order before launching or being charged."

Pricing Information: Use the Region dropdown selector to see software and infrastructure pricing information for the chosen AWS region.

For Region: Asia Pacific (Mumbai)

Free Trial: Try one instance of this product for 15 days. There will be no hourly software... [Read More](#)

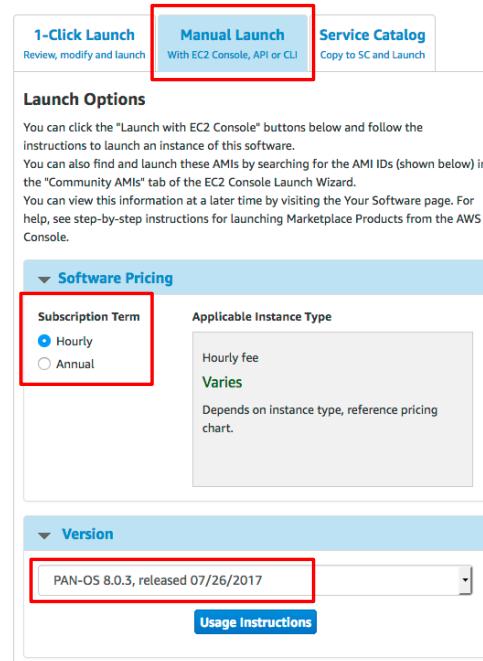
Additional Taxes May Apply

Click Continue.

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

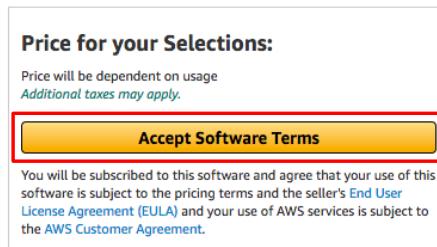
Palo Alto Networks AWS CFT Deployment Guide

Launch on EC2: VM-Series Next-Generation Firewall Bundle 2

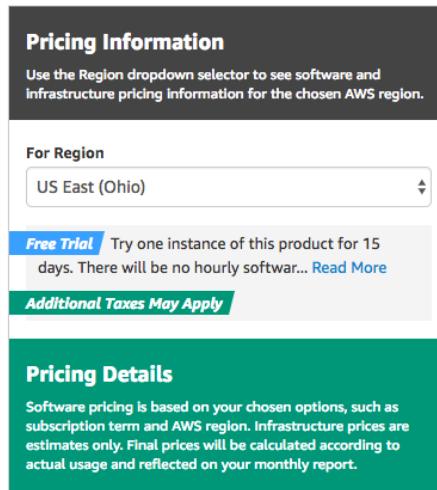


The screenshot shows the AWS Lambda console interface for launching a VM-Series Next-Generation Firewall Bundle 2. At the top, there are three buttons: '1-Click Launch' (Review, modify and launch), 'Manual Launch' (With EC2 Console, API or CLI), and 'Service Catalog' (Copy to SC and Launch). The 'Manual Launch' button is highlighted with a red box. Below these buttons is a section titled 'Launch Options' with instructions for launching instances via the EC2 Console or by searching for AMI IDs. Further down are sections for 'Software Pricing' (Subscription Term: Hourly selected, Annual option available) and 'Version' (PAN-OS 8.0.3, released 07/26/2017). A 'Usage Instructions' button is also present.

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



The screenshot shows the 'Price for your Selections' step in the AWS Lambda console. It displays a message stating that price will be dependent on usage and may include additional taxes. A large yellow 'Accept Software Terms' button is highlighted with a red box. Below the button, a note explains that users will be subscribed to the software and agree to the End User License Agreement (EULA) and AWS Customer Agreement.



The screenshot shows the 'Pricing Information' and 'Pricing Details' steps in the AWS Lambda console. The 'Pricing Information' step includes a dropdown for selecting a region ('For Region: US East (Ohio)'). It also features a 'Free Trial' offer to try one instance for 15 days and a note about additional taxes. The 'Pricing Details' step provides a detailed explanation of how software pricing is calculated based on chosen options like subscription term and AWS region.

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

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

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

The screenshot shows a 'Pricing Information' page. At the top, it says 'For Region' with a dropdown menu set to 'US East (N. Virginia)'. Below this, a note states 'Additional Taxes May Apply'. A green box labeled 'Pricing Details' contains a note about software pricing being based on chosen options like subscription term and region. It also mentions that final prices will be calculated according to actual usage. A table titled 'VM-Series Next-Generation Firewall Bundle 2 - Hourly' lists EC2 instance types and their corresponding software and total hourly rates. The table includes columns for EC2 Instance Type, Software /hr, EC2 /hr, and Total /hr.

EC2 Instance Type	Software /hr	EC2 /hr	Total /hr
m3.xlarge	\$1.28	\$0.266	\$1.546
m4.xlarge	\$1.28	\$0.20	\$1.48
m4.2xlarge	\$1.28	\$0.40	\$1.68
c3.4xlarge	\$1.28	\$0.84	\$2.12
c4.2xlarge	\$1.28	\$0.398	\$1.678
c4.Bxlarge	\$1.28	\$1.591	\$2.871
m4.4xlarge	\$1.28	\$0.80	\$2.08
c4.4xlarge	\$1.28	\$0.796	\$2.076
m3.2xlarge	\$1.28	\$0.532	\$1.812
c3.2xlarge	\$1.28	\$0.42	\$1.70
c3.8xlarge	\$1.28	\$1.68	\$2.96

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

You should see this screen:

A confirmation message box displays a green checkmark icon and the text: '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.' Below this, a message says 'Thank you! Your subscription will be completed in a few moments.'

Palo Alto Networks AWS CFT Deployment Guide

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

Dear AWS Marketplace Customer,

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

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

Details needed to launch the software, including AMI IDs, instructions, and recommended security settings can be found by visiting Your Software on AWS Marketplace:
https://aws.amazon.com/marketplace/library/ref=bill_email_2

Software Pricing and Other Charges

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

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

You can review pricing for this software here: https://aws.amazon.com/marketplace/pp/ref=bill_email_2?sku=8062ef0qy5osgjlx9qc6g.

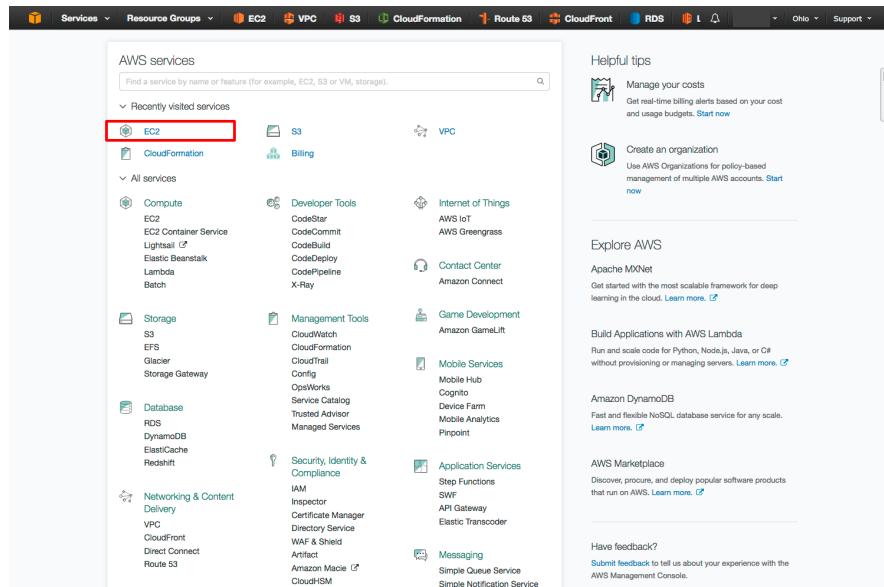
If you have questions, please contact us: https://aws.amazon.com/marketplace/help/contact-us/ref=bill_email_2

-- The AWS Marketplace Team

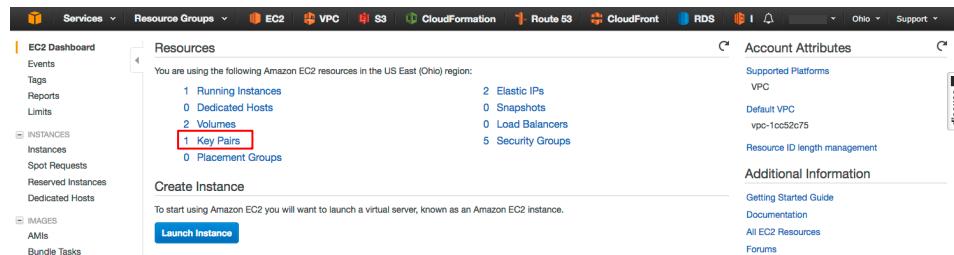
Continue with the next step.

4.3 Create and download an SSH Key Pair

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



Click Key Pairs



Palo Alto Networks AWS CFT Deployment Guide

Click **Create Key Pair**



Give it a name.

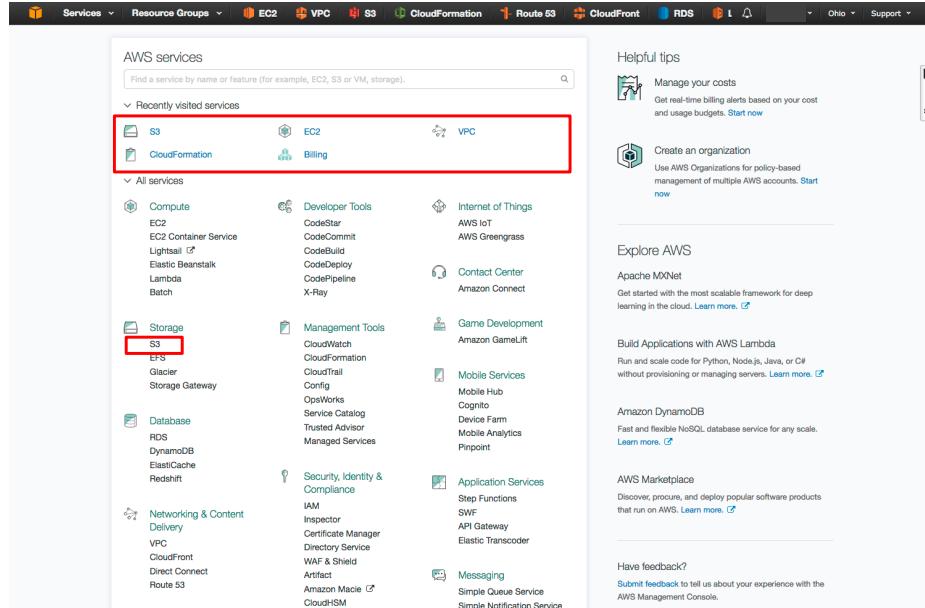


And click **Create**. When prompted save Key Pair you just created.

4.4 Create a Bootstrap Bucket

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

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



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

Click **Create Bucket**:

Palo Alto Networks AWS CFT Deployment Guide

The screenshot shows the Amazon S3 console interface. At the top, there's a navigation bar with various AWS services like EC2, VPC, S3, CloudFormation, Route 53, CloudFront, and RDS. Below the navigation bar, a banner reads "Identify optimal storage classes with S3 Analytics - Storage Class Analysis. Learn More >". The main area is titled "Amazon S3" and has a search bar labeled "Search for buckets". Below the search bar are three buttons: "+ Create bucket" (highlighted with a red box), "Delete bucket", and "Empty bucket". In the bottom right corner, it says "6 Buckets" and "2 Regions".

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

This is a screenshot of the "Create bucket" wizard, Step 1: Name and region. It shows a progress bar with four steps: 1. Name and region (highlighted with a red box), 2. Set properties, 3. Set permissions, and 4. Review. The "Name and region" section contains fields for "Bucket name" (set to "bootstrap-ngfw") and "Region" (set to "US East (Ohio)"). There's also a dropdown for "Copy settings from an existing bucket". At the bottom, there are "Create" and "Next" buttons, with "Create" highlighted with a red box.

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**.

This is a screenshot of the Amazon S3 bucket overview page for "bootstrap-ngfw". It features tabs for Overview, Properties, Permissions, and Management (which is selected). Below the tabs are buttons for Upload, + Create folder (highlighted with a red box), and More. A list of objects in the bucket is shown at the bottom.

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

This is a screenshot of the Amazon S3 bucket contents page for "bootstrap-ngfw". It lists four folders: config, content, license, and software. The "config" folder is highlighted with a red box. The table includes columns for Name, Last modified, Size, and Storage class. At the top right, it says "Viewing 1 to 4".

Name	Last modified	Size	Storage class
config	--	--	--
content	--	--	--
license	--	--	--
software	--	--	--

Palo Alto Networks AWS CFT Deployment Guide

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

4.5 Download Bootstrap Files and CFT from GitHub

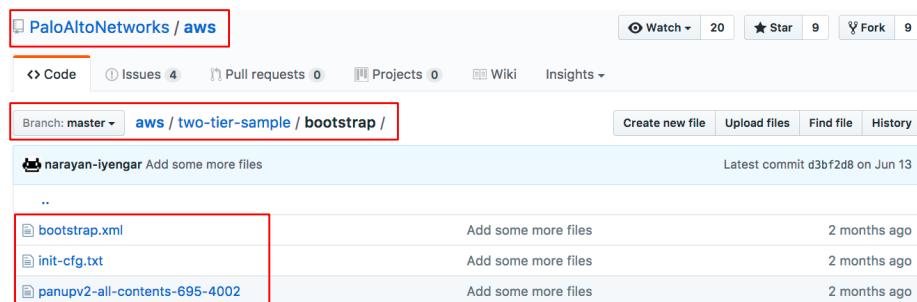
Download the following files and save them in a known location:

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

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

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

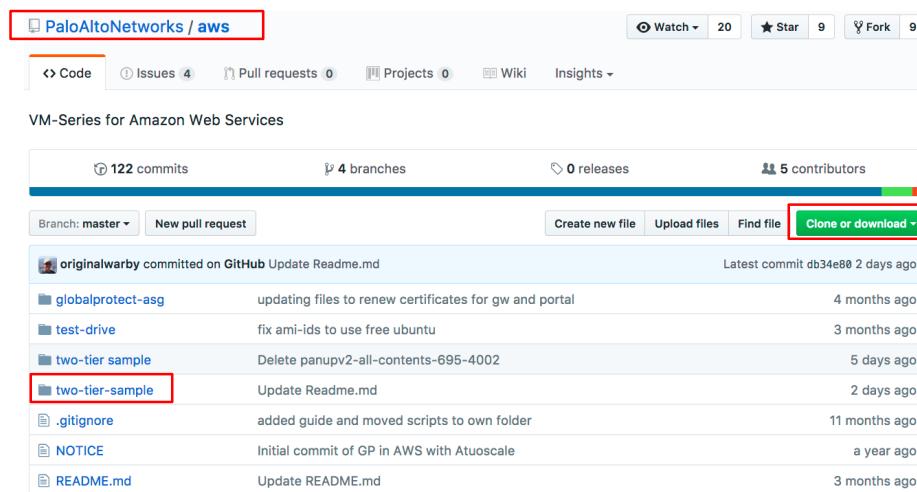
This is the GitHub location where you'll find the files:



The screenshot shows a GitHub repository page for the 'aws/two-tier-sample/bootstrap' branch. The sidebar on the left has a red box around 'PaloAltoNetworks / aws'. The main content area shows a list of files under the 'bootstrap' directory. Three files are listed: 'bootstrap.xml', 'init-cfg.txt', and 'panupv2-all-contents-695-4002'. The first two files have red boxes around them, highlighting them as the ones to download.

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

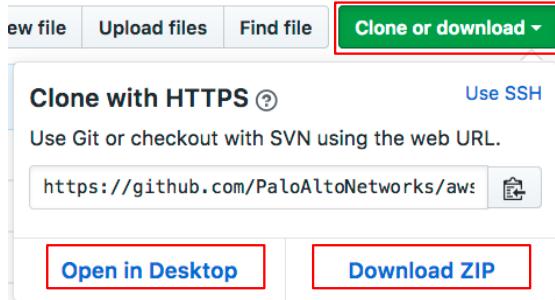
You could either Clone or Download the files from the master branch .../PaloAltoNetworks/aws/



The screenshot shows a GitHub repository page for the 'aws' repository. The sidebar on the left has a red box around 'PaloAltoNetworks / aws'. The main content area shows a summary of the repository: 122 commits, 4 branches, 0 releases, and 5 contributors. Below this, the 'two-tier-sample' folder is selected in the sidebar. A list of files in this folder is shown, including 'README.md', 'NOTICE', '.gitignore', 'two-tier sample', 'test-drive', 'globalprotect-asg', and '122 commits'. The 'Clone or download' button at the bottom right of the file list has a red box around it.

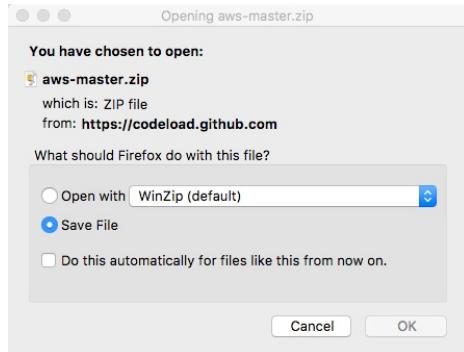
Click on **Clone or download**:

Palo Alto Networks AWS CFT Deployment Guide

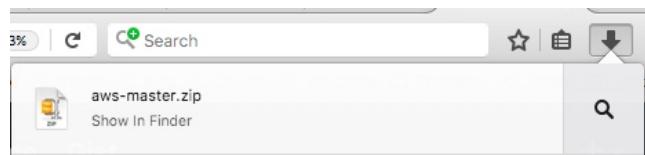


Choose the preferred method. **Open in Desktop** requires the GitHub desktop app which is available for Windows and macOS. The **Download ZIP** option just requires a app to unpack the zip file and it is the simpler approach to download the files. We'll walk through the two approaches on macOS.

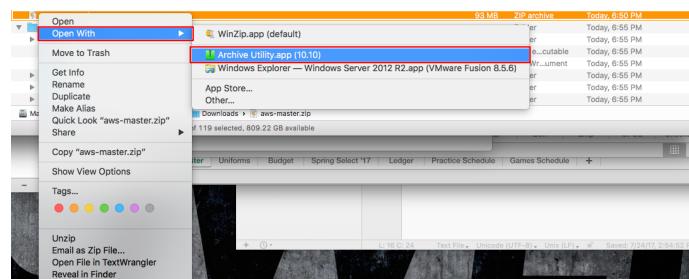
Download ZIP approach: Click on **Download ZIP** and select **Save File**.



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



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

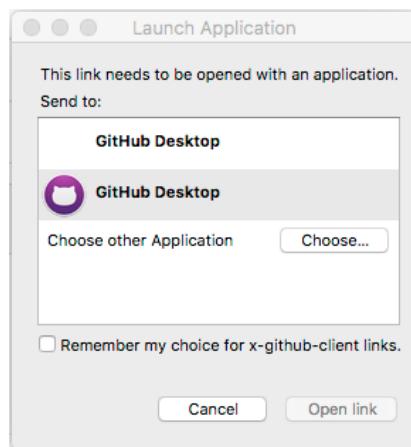


Palo Alto Networks AWS CFT Deployment Guide

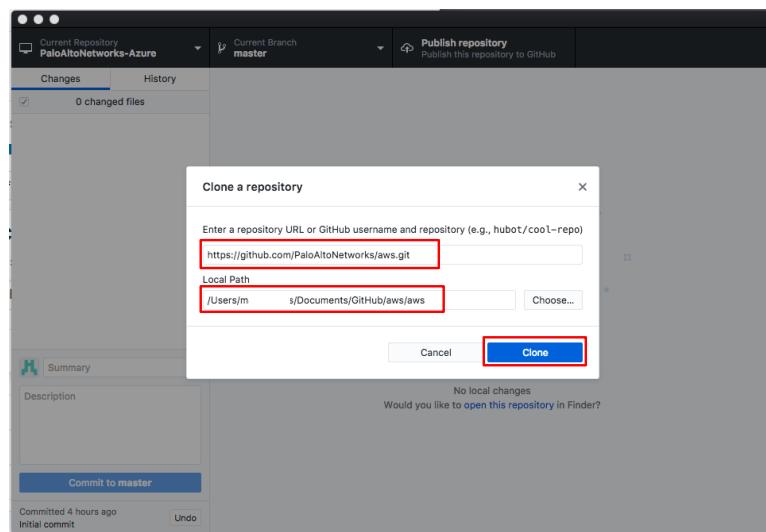
Remember the location of the extracted files and look at the directory structure where the specific files to upload are located at.

aws-master		--	Folder
globalprotect-asg		--	Folder
NOTICE		1 KB	Unix executable
README.md		1 KB	TextWr...ument
test-drive		--	Folder
two-tier sample		--	Folder
two-tier-sample		--	Folder
AWS_CFT_How_To_Guide-UTD.pdf		14.9 MB	PDF Document
bootstrap		--	Folder
bootstrap.xml		31 KB	TextWr...ument
init-cfg.txt		156 bytes	Plain Text
panupv2-all-contents-695-4002		38.3 MB	Unix executable
guess-sql-root-password.cgi		732 bytes	Document
pan-sample-cft.json		21 KB	JSON File
Readme.md		1 KB	TextWr...ument
sql-attack.html		606 bytes	HTML
ssh-to-db.cgi		652 bytes	Document
topology.png		49 KB	PNG Image

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

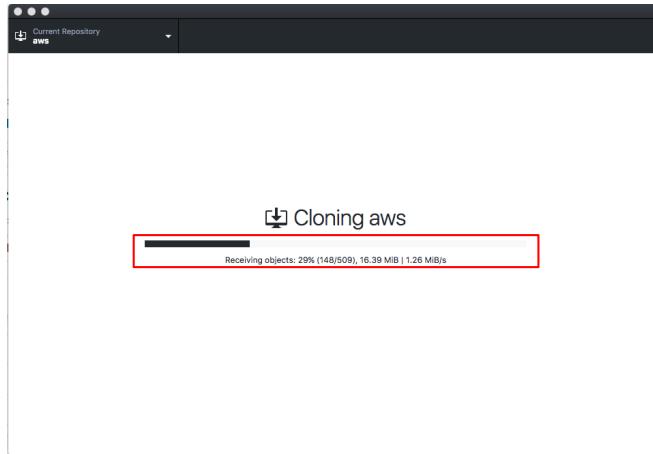


The repository is the master which is automatically filled in. Select the local path you wish to clone it to for future reference. Click on **Clone**.



Palo Alto Networks AWS CFT Deployment Guide

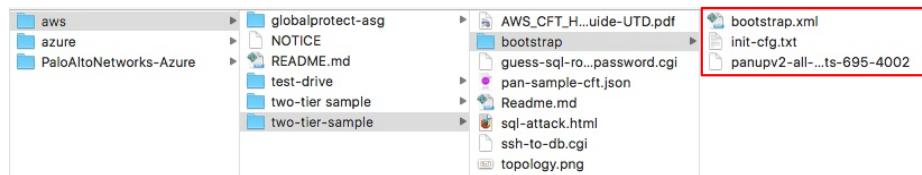
The cloning process takes just a couple of minutes.



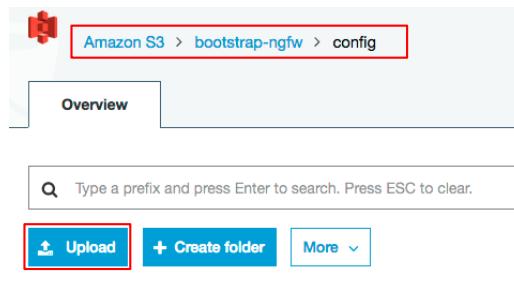
Once it is finished go to Current Repository and you'll see the new one just created.



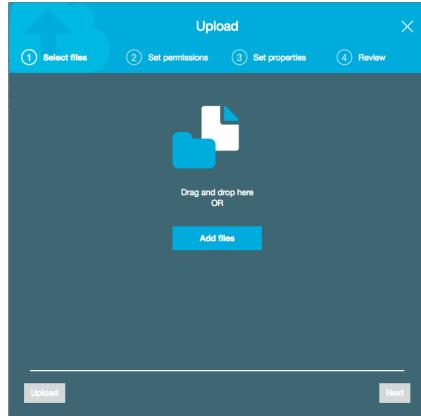
Go the location where the files were cloned to and verify they were copied.



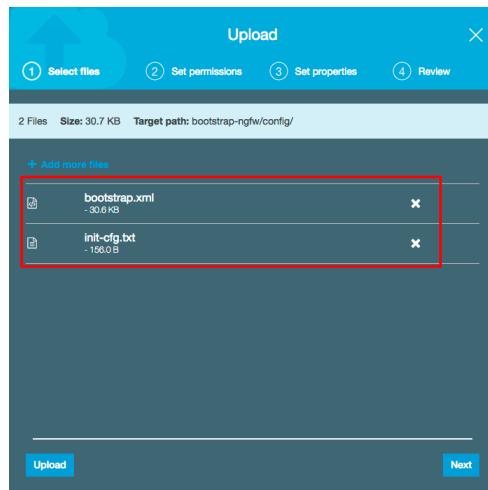
Go back to the AWS S3 console and select the **config** folder click **Upload**:



Palo Alto Networks AWS CFT Deployment Guide



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

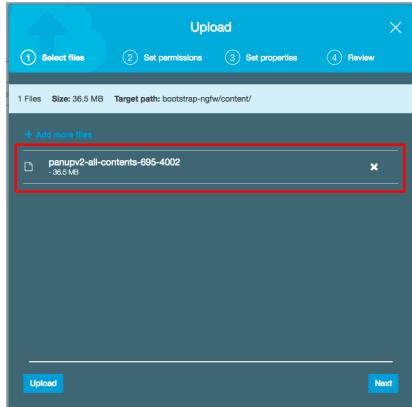


The two files should be listed under the folder:

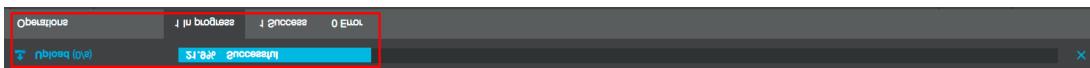
Name	Last modified	Size	Storage class
bootstrap.xml	Aug 14, 2017 6:22:13 PM	30.6 KB	Standard
init-cft.txt	Aug 14, 2017 6:22:13 PM	156.0 B	Standard

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

Palo Alto Networks AWS CFT Deployment Guide



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



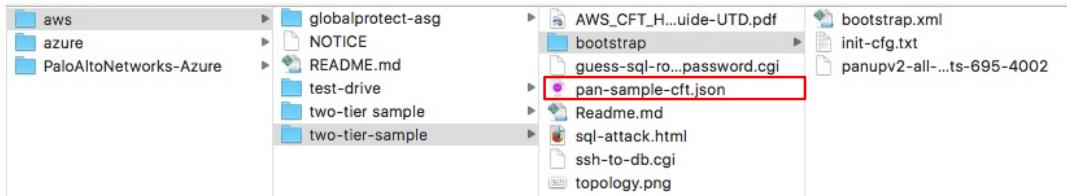
Once completed the file is listed under the folder content.

US East (Ohio)				
Viewing 1 to 1				
Name	Last modified	Size	Storage class	
panupv2-all-contents-695-4002	Aug 14, 2017 6:25:00 PM	36.5 MB	Standard	

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

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

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

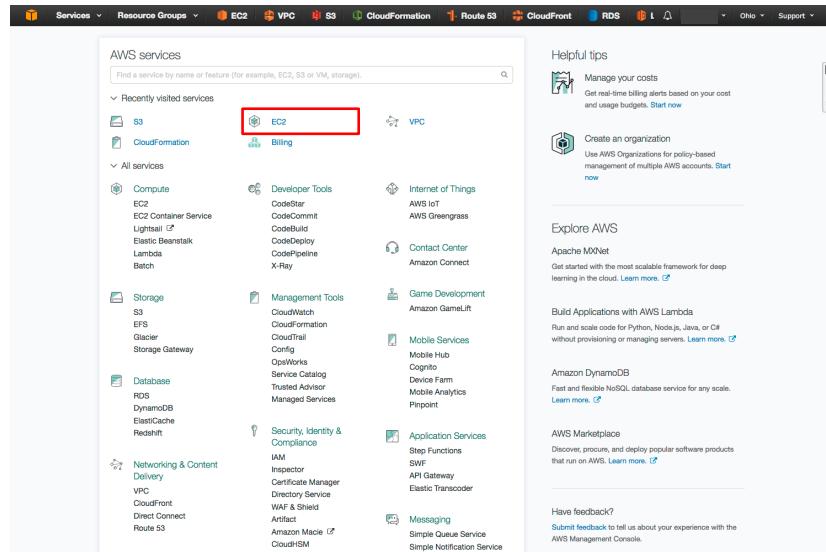


We'll use the CFT once other AWS infrastructure has been created.

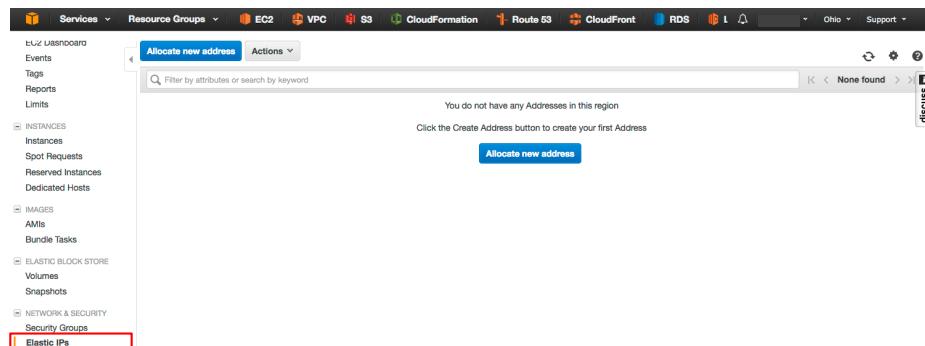
4.6 Check Elastic IPs

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

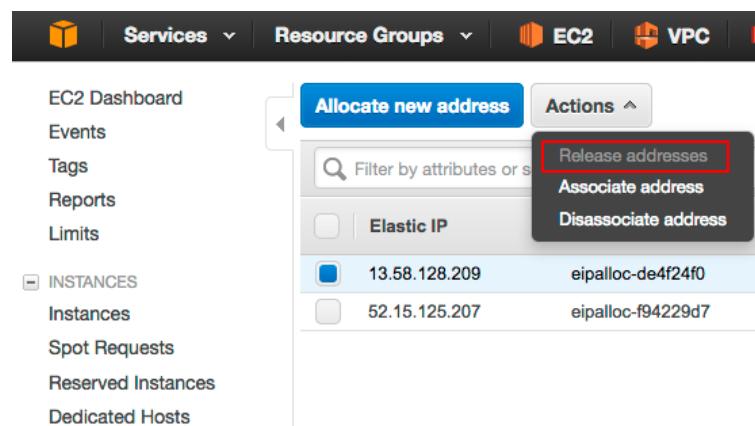
Palo Alto Networks AWS CFT Deployment Guide



And click on Elastic IPs:



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

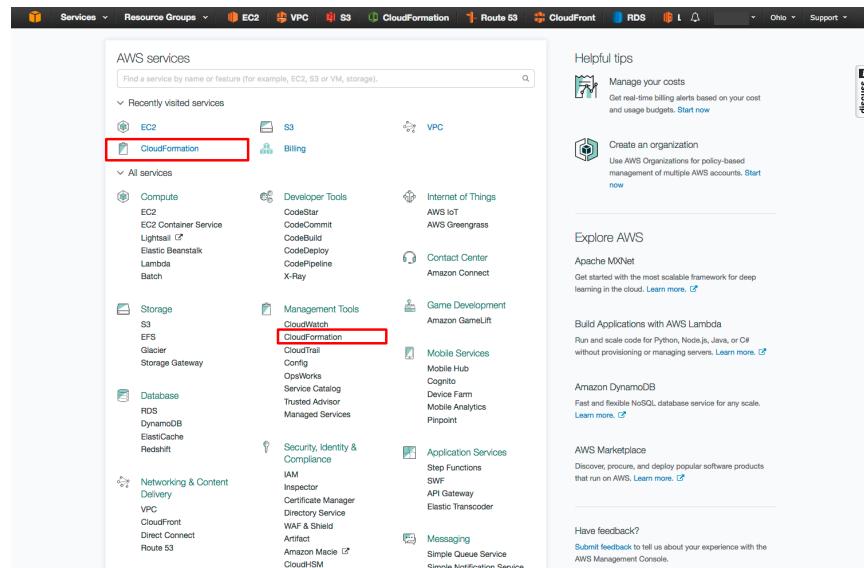


Palo Alto Networks AWS CFT Deployment Guide

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

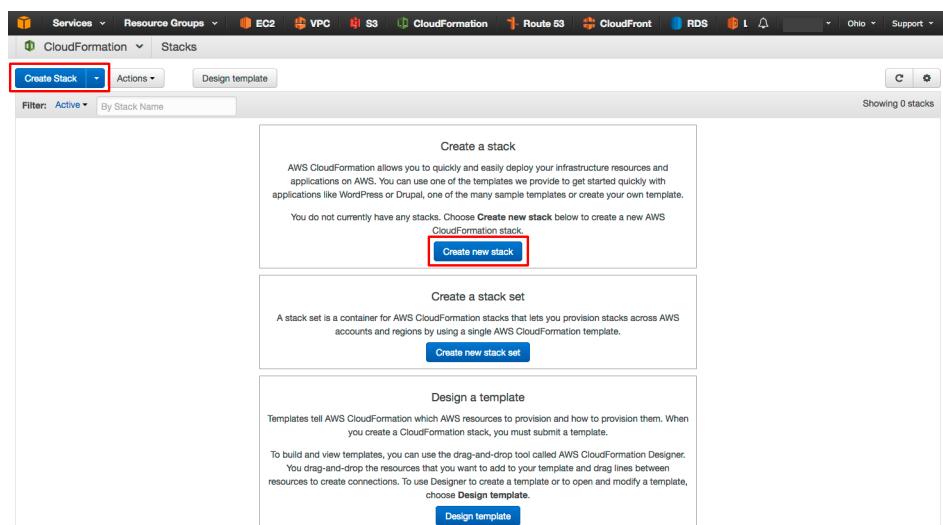
5. Launch the Two-tier CFT

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



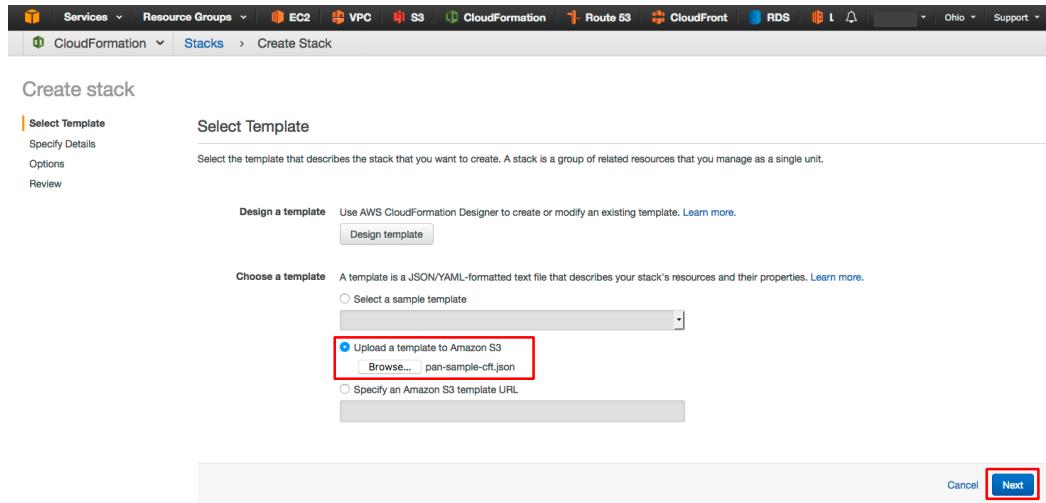
5.1 Create CloudFormation Stack

Click **Create Stack**:

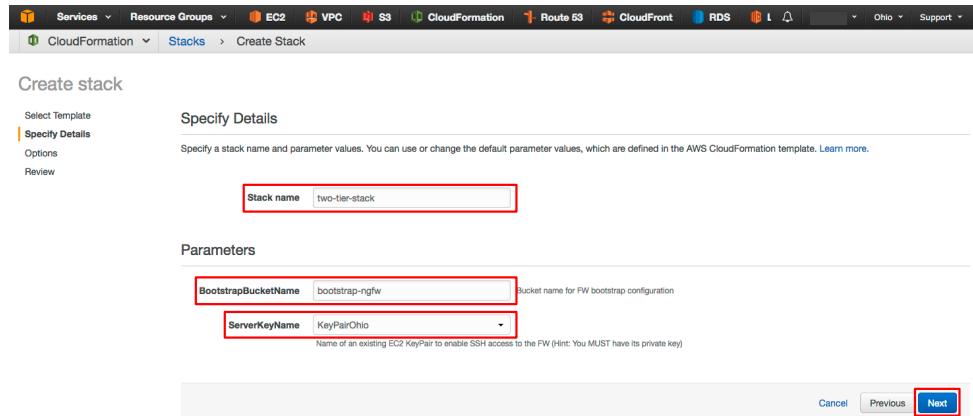


Palo Alto Networks AWS CFT Deployment Guide

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



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



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

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 50 unique key-value pairs for each stack. [Learn more.](#)

Key (127 characters maximum)	Value (255 characters maximum)
1 Env	Test

Permissions

You can choose an IAM role that CloudFormation uses to create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses the permissions defined in your account. [Learn more.](#)

IAM Role

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**.

Create stack

Select Template
Specify Details
Options
Review

Review

Template

Template URL: <https://s3.us-east-2.amazonaws.com/cf-templates-4em3j0uc5d-us-east-2/2017227EBA-pan-sample-cft.json>
Description: Install WordPress server, and database fronted by PANW Firewall (sample-cft).
Estimate cost: Link is not available

Details

Stack name: two-tier-stack
BootstrapBucketName: bootstrap-ngfw
ServerKeyName: KeyPairOhio

Options

Tags

Env Test

Advanced

Notification: None
Timeout: None
Rollback on failure: Yes

Capabilities

The following resource(s) require capabilities: [AWS::IAM::Role]
This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. [Learn more.](#)

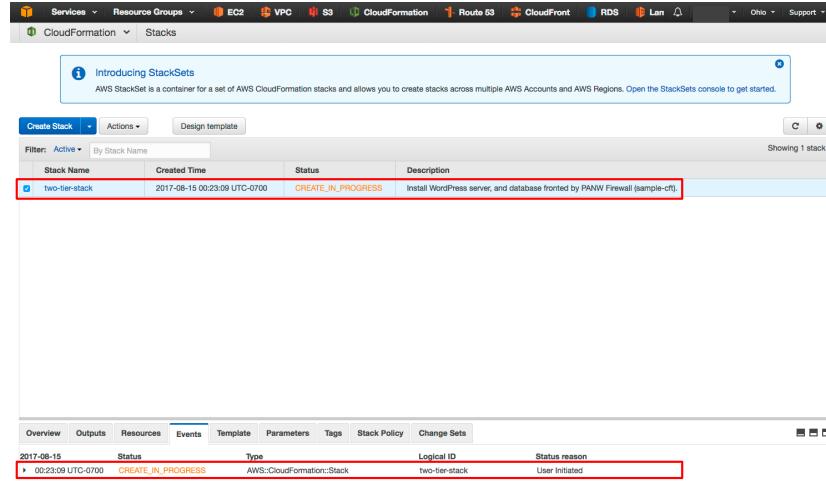
I acknowledge that AWS CloudFormation might create IAM resources.

Cancel Previous **Create**

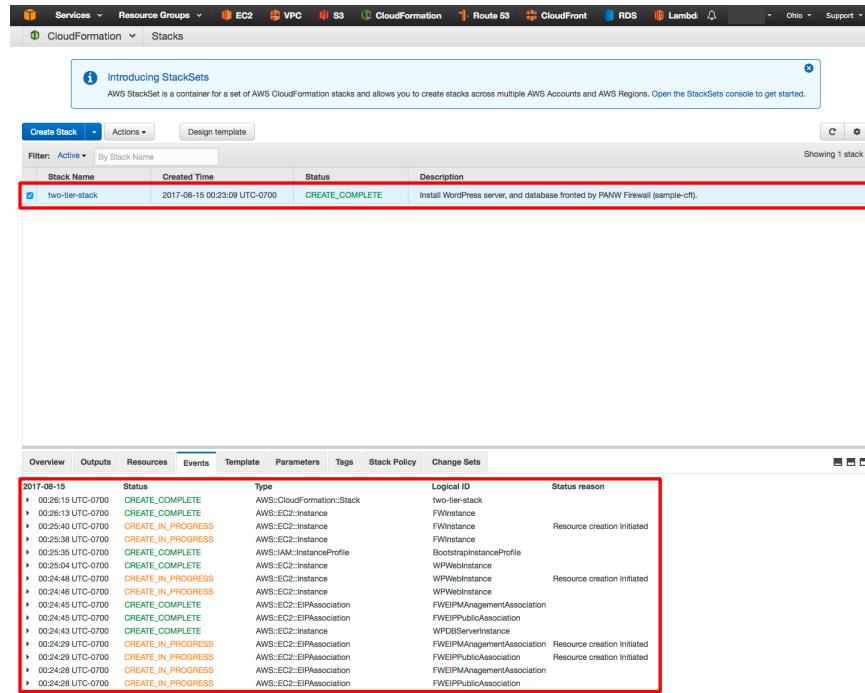
Once launched you should be able to monitor the stack creation progress in the next screen by clicking on the **Events** tab.

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

Palo Alto Networks AWS CFT Deployment Guide



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

Palo Alto Networks AWS CFT Deployment Guide

The screenshot shows the AWS CloudFormation console with the 'teststack' stack listed. The 'Events' tab is selected, showing the following log entries:

Time	Status	Type	Logical ID	Description
2016-02-25 10:00:34 UTC-0800	ROLLBACK_COMPLETE	AWS::CloudFormation::Stack	teststack	Install VM-Series helper, WordPress server, and database fronted by PANW BYOL Firewall (test-drive).
2016-02-25 10:21:14 UTC-0800	DELETE_IN_PROGRESS	AWS::IAM::AccessKey		
2016-02-25 10:21:08 UTC-0800	ROLLBACK_IN_PROGRESS	AWS::CloudFormation::Stack	teststack	
2016-02-25 10:21:07 UTC-0800	CREATE_FAILED	AWS::EC2::Instance	FWInstance	
2016-02-25 10:02:23 UTC-0800	CREATE_COMPLETE	AWS::EC2::Instance	WPWebInstance	
2016-02-25 10:02:23 UTC-0800	CREATE_COMPLETE	AWS::EC2::Instance	WPDBServerInstance	
2016-02-25 10:02:15 UTC-0800	CREATE_IN_PROGRESS	AWS::EC2::Instance	FWInstance	
2016-02-25 10:02:13 UTC-0800	CREATE_COMPLETE	AWS::EC2::EBSAssociation	EMI_EBSInAssociation	

A red box highlights the error message in the right-hand panel: "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=6kodw3bbmndea3o6i1ggq4km>".

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

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

The screenshot shows the AWS CloudFormation console with the 'teststack' stack listed. The 'Actions' dropdown is open, showing the 'Delete Stack' option highlighted with a red box.

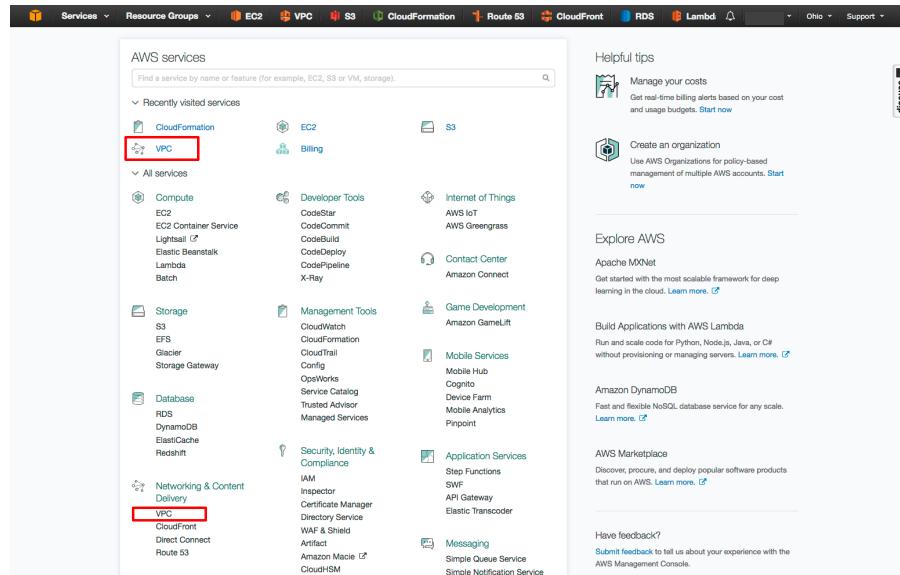
The 'Events' tab is selected, showing the following log entries:

Time	Status	Type	Logical ID	Status Reason
2016-02-23 12:48:50 UTC-0800	CREATE_COMPLETE	AWS::CloudFormation::Stack	teststack	
2016-02-23 13:02:19 UTC-0800	CREATE_COMPLETE	Custom::VMSeriesHelper	VMSeriesHelper	
2016-02-23 13:02:16 UTC-0800	CREATE_COMPLETE	Custom::VMSeriesHelper	VMSeriesHelper	
2016-02-23 13:02:15 UTC-0800	CREATE_IN_PROGRESS	Custom::VMSeriesHelper	VMSeriesHelper	Resource creation initiated
2016-02-23 12:51:10 UTC-0800	CREATE_IN_PROGRESS	Custom::VMSeriesHelper	VMSeriesHelper	
2016-02-23 12:51:06 UTC-0800	CREATE_COMPLETE	AWS::EC2::Instance	FWInstance	
2016-02-23 12:50:27 UTC-0800	CREATE_COMPLETE	AWS::EC2::Instance	WPWebInstance	

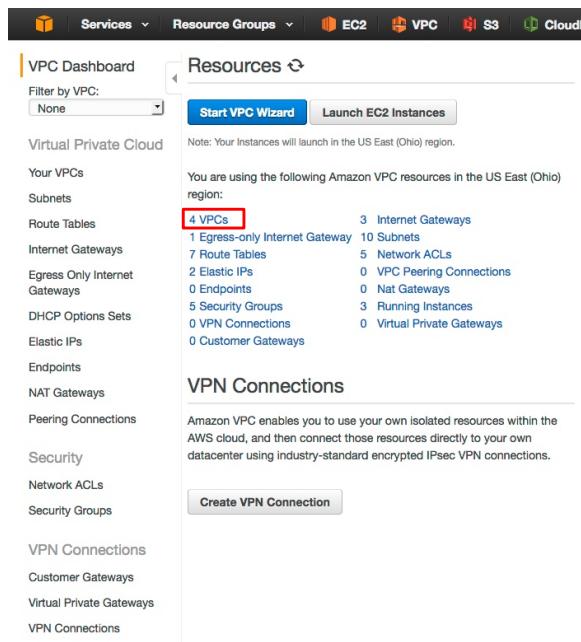
5.2 Review Resources Created by the Template

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

Palo Alto Networks AWS CFT Deployment Guide



Here you should see all VPCs created in your account:



Here is the sample VPC:

Palo Alto Networks AWS CFT Deployment Guide

The screenshot shows the AWS VPC Dashboard. On the left sidebar, under 'Virtual Private Cloud', the 'Subnets' option is selected. In the main content area, a table lists VPCs. One row is highlighted with a red border: 'PAN Sample CFT' (vpc-0620756f). The table includes columns for Name, VPC ID, State, IPv4 CIDR, IPv6 CIDR, DHCP options set, Route table, Network ACL, Tenancy, and Default V.

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

The screenshot shows the 'Create Subnet' section of the AWS Subnet Actions page. The 'Subnets' option is selected in the sidebar. A table lists three subnets for the 'PAN Sample CFT' VPC. The table columns include Name, Subnet ID, State, VPC, IPv4 CIDR, Available IPv4, IPv6 CIDR, Availability Zone, and Route Table. All three subnets belong to the same VPC and have the same route table assigned.

Route tables:

The screenshot shows the 'Create Route Table' section of the AWS Route Table Actions page. The 'Route Tables' option is selected in the sidebar. A table lists three route tables for the 'PAN Sample CFT' VPC. The table columns include Name, Route Table ID, Explicitly Associated, Main, and VPC. The first two route tables are marked as 'Main' and have 0 subnets explicitly associated. The third route table has 1 subnet explicitly associated.

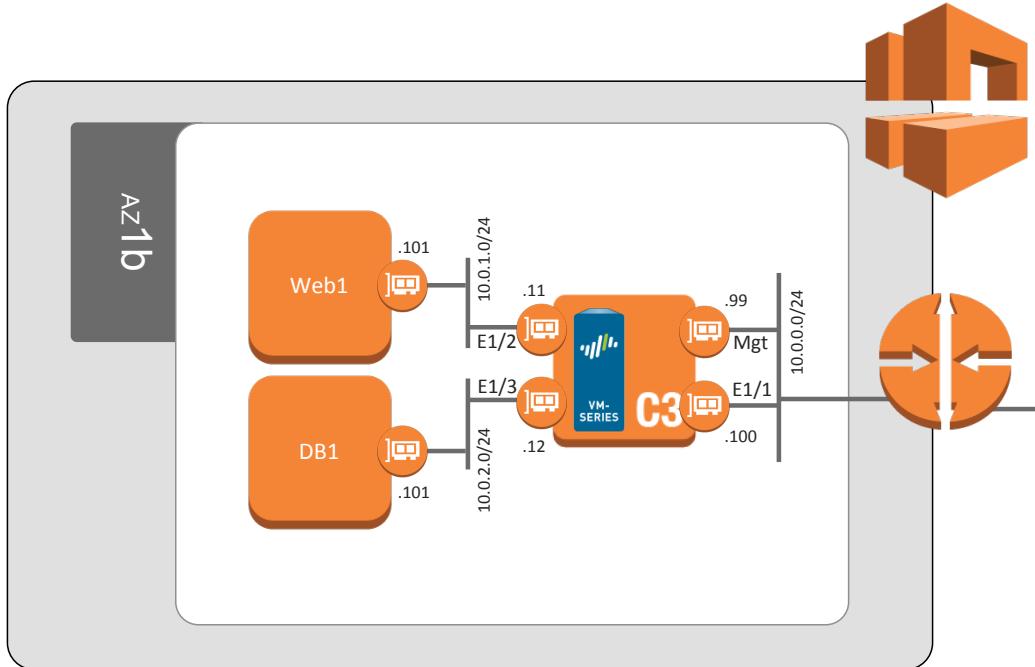
And Elastic IPs (EIPs):

Palo Alto Networks AWS CFT Deployment Guide

The screenshot shows the AWS VPC Dashboard. On the left, there's a sidebar with options like Virtual Private Cloud, Your VPCs, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, and Elastic IPs. The 'Elastic IPs' option is highlighted with a red box. The main area displays a table titled 'Allocate new address' with columns: Elastic IP, Allocation ID, Instance, Private IP address, Scope, Public DNS, and Network Interface ID. Two entries are listed:

Elastic IP	Allocation ID	Instance	Private IP address	Scope	Public DNS	Network Interface ID
52.15.125.207	eipalloc-f94229d7	i-0ca7f2c1f07c8e...	10.0.0.100	vpc	epassoc-af185fb1	eni-54adfc7c
13.58.128.209	eipalloc-de4f24f0	i-0ca7f2c1f07c8e...	10.0.0.99	vpc	epassoc-ef2661c1	eni-0faeff27

All of this matches the topology shown previously:



6. VM-Series Access and WebUI Review

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

6.1 Access VM-Series Firewall

Palo Alto Networks AWS CFT Deployment Guide

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

Key	Value	Description	Export Name
WordpressURL	http://82.15.125.207/wordpress	Wordpress server	
FirewallManagementURL	https://13.58.128.209	VM-Series management Interface URL	

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

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

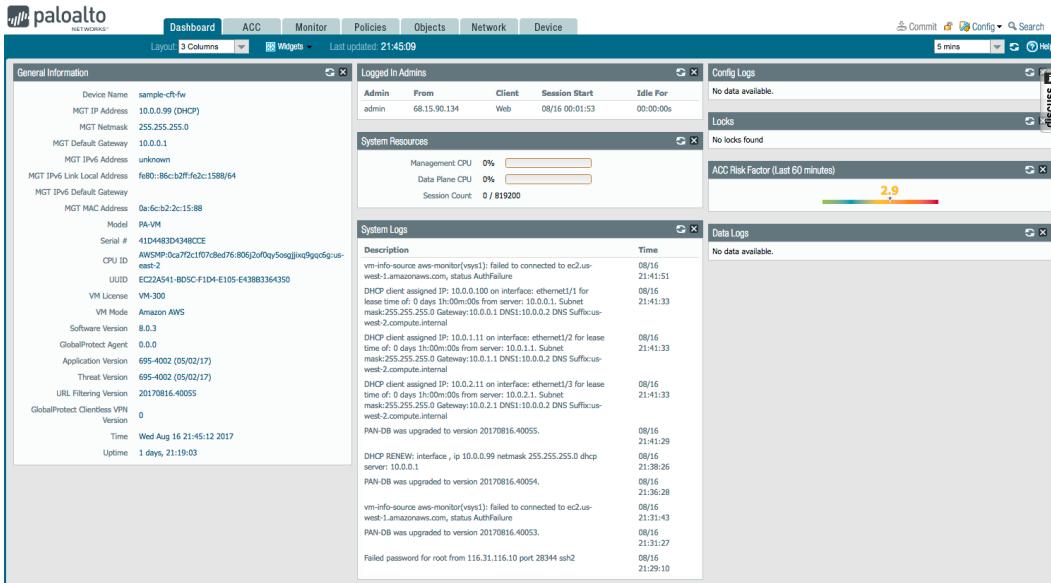
Note: If your browser gives you a certificate warning, you can safely acknowledge it and proceed.



6.2 Login and Dashboard Summary

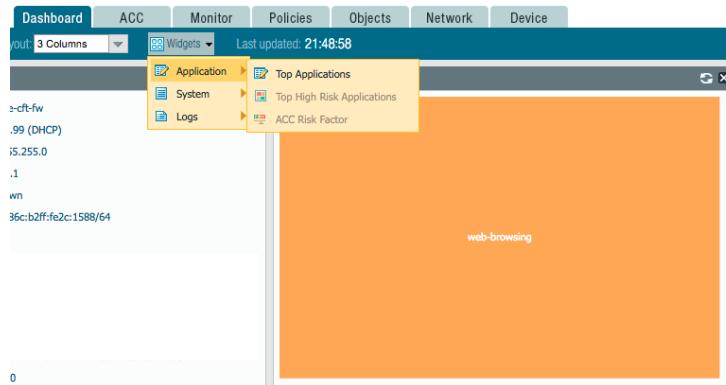
Palo Alto Networks AWS CFT Deployment Guide

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



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

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



6.3 Review Application Command Center (ACC)

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

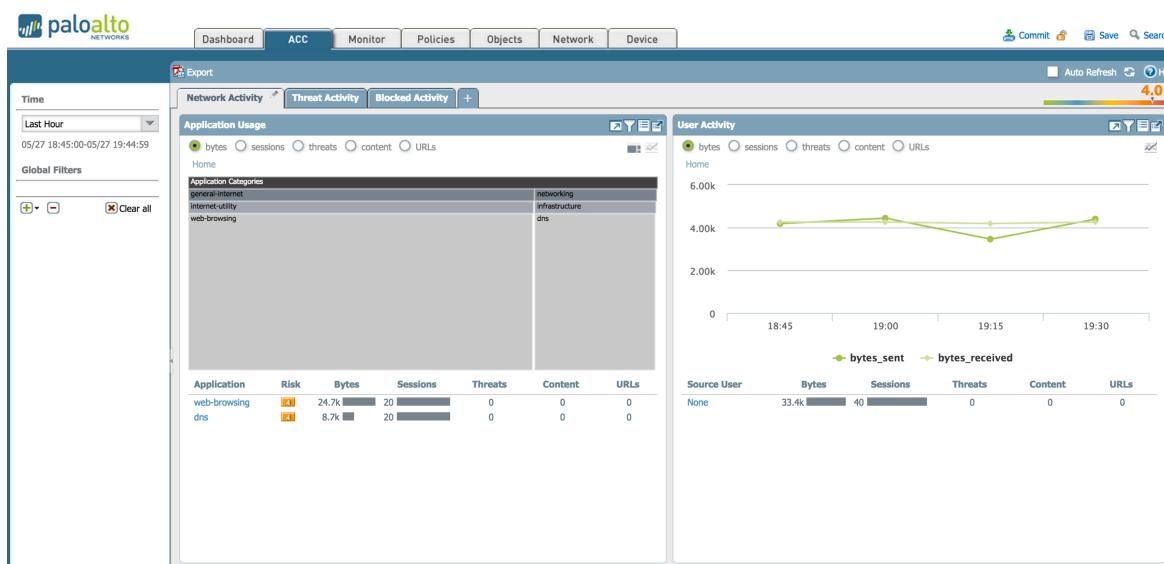
Palo Alto Networks AWS CFT Deployment Guide

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

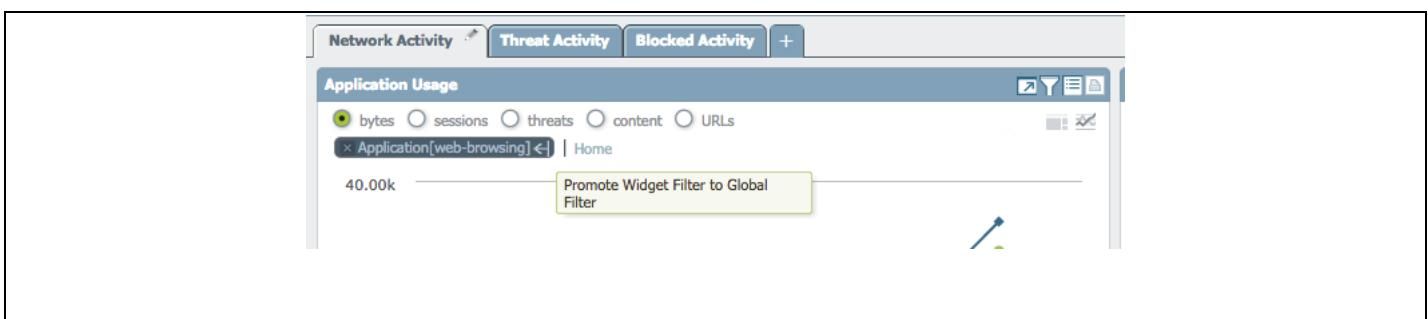
Select the **ACC** Tab.



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



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



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

6.4 Review Security Policies

The Policies tab is 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.

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	any	any	any	any	10.0.0.100	service-tcp-2...	dynamic-ip-and-port	address: 10.0.1.101		
2 DB SSH	none	any	any	any	any	10.0.0.100	service-tcp-2...	dynamic-ip-and-port	address: 10.0.2.101		
3 WordPress NAT	none	any	any	any	any	10.0.0.100	service-http	dynamic-ip-and-port	address: 10.0.1.101		
4 Outbound nat	none	any	any	any	any	any	any	dynamic-ip-and-port	port: 80		
		any	any	any	any	any	any	ethernet1/1	none		

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

Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options	
SSH inbound	none	universal	any	any	any	any	any	any	ssh	application-d...	Allow	none		
SSH 221-222 inbound	none	universal	any	any	any	any	any	any	ssh	service-tcp-2...	Allow	none		
Allow all ping	none	universal	any	any	any	any	any	any	ping	application-d...	Allow	none		
Web browsing	none	universal	any	any	any	any	any	any	web	application-d...	Allow	none		
Allow all outbound	none	universal	any	any	any	any	any	any	any	web-browsing	application-d...	Allow	none	
Web to DB	none	universal	any	any	any	any	any	any	mysql	application-d...	Deny	none		
Log default deny	none	universal	any	any	any	any	any	any	any	any	Deny	none		
intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow	none	none	
interzone-default	none	interzone	any	any	any	any	any	any	any	any	Deny	none	none	

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

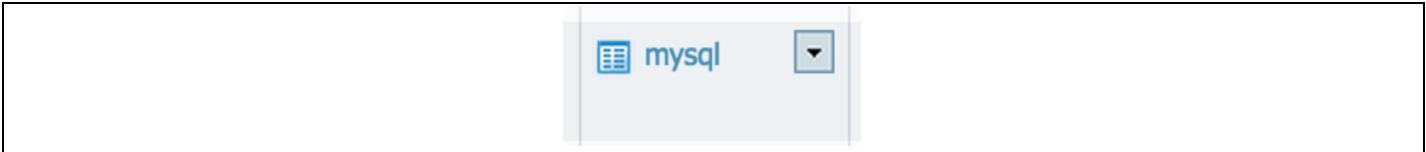
Application Service Action Profile

Columns

Adjust Columns

- Name
- Tags
- Type
- Source Zone
- Source Address
- Source User
- Source HIP Profile
- Destination Zone
- Destination Address
- Application
- Service
- URL Category
- Action
- Profile
- Options
- Description

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.

A screenshot of a software interface showing the "Application" details for MySQL. The "Name" is MySQL, "Description" is "MySQL is a multithreaded, multi-user, SQL Database Management System (DBMS) with more than six million installations", "Category" is business-systems, "Subcategory" is database, "Technology" is client-server, "Risk" is 2, and "Standard Ports" is tcp/3306. The "Characteristic" is Vulnerability and Widely used. The "Standard Ports" entry is highlighted with a red box.

6.5 Review The Monitor Tab

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

Click on the Monitor tab.



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

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

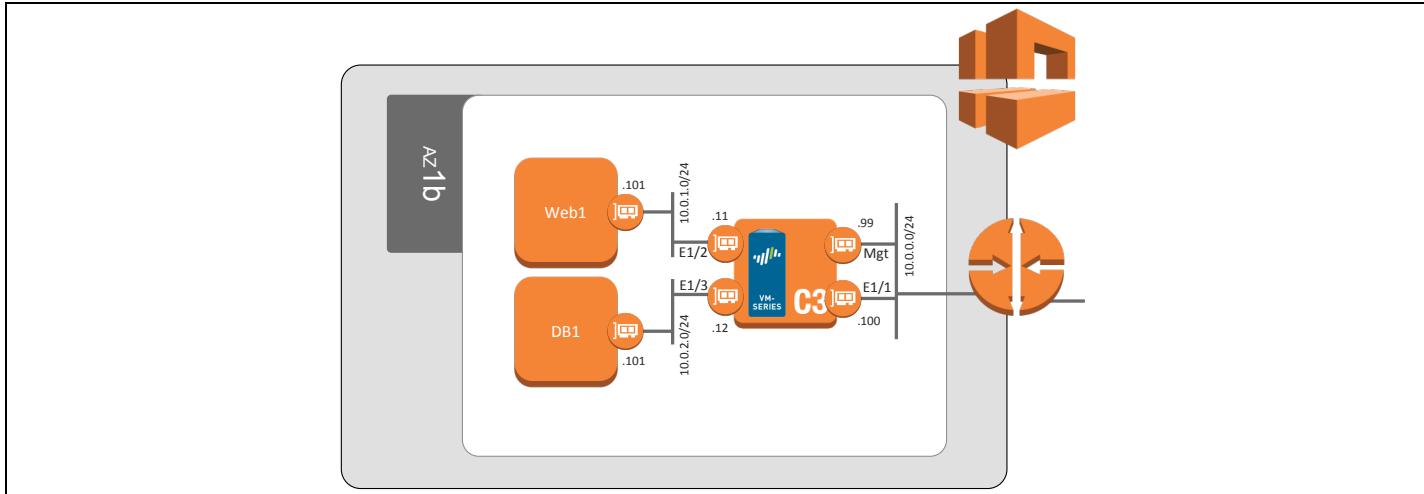
Palo Alto Networks AWS CFT Deployment Guide

The screenshot shows the Palo Alto Networks Network traffic log interface. The left sidebar contains a navigation tree with sections like Firewall, Threat, URL Filtering, Wildfire Submission, Data Filtering, IP Match, User-ID, File Configuration System, Alarms, Authentication, Unified, Policy Capture, App Summary, Change Monitor, Threat Monitor, Threat Map, Network Monitor, Traffic Map, Session Browser, and Reports. A red box highlights the 'Logs' section under 'Threat'. The main area displays a table of logs with the following columns: Receive Time, Type, From Zone, To Zone, Source, Destination, To Port, Application, Action, Rule, Session End Reason, and Bytes. The logs list various network events, such as drops from external sources to internal ports (e.g., 10.0.0.100) on specific ports (e.g., 5060, 23, 23389, 1433). The table has 14 columns and 18 rows of data.

6.6 Review Object, Network and Device Tabs

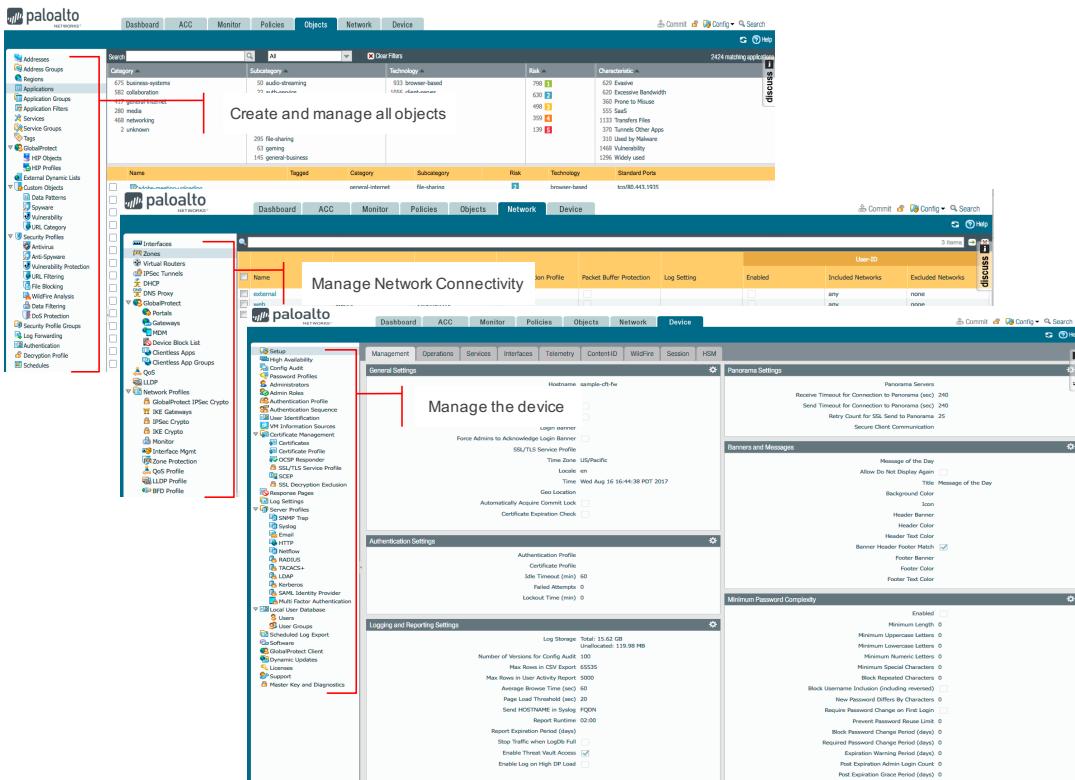
The Objects, Network, and Device tabs provide you with the various management capabilities. The Objects tab allows you to manage the building blocks for creating policies such as address objects, custom applications, and security profiles. The network tab allows you to create and manage interfaces, security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

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



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

Palo Alto Networks AWS CFT Deployment Guide



7. Securing Applications

In this activity, you will:

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

7.1 Verify Static Content on Web Server

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

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'. A filter dropdown is set to 'Active' and a search bar says 'By Stack Name'. Below this is a table with one row:

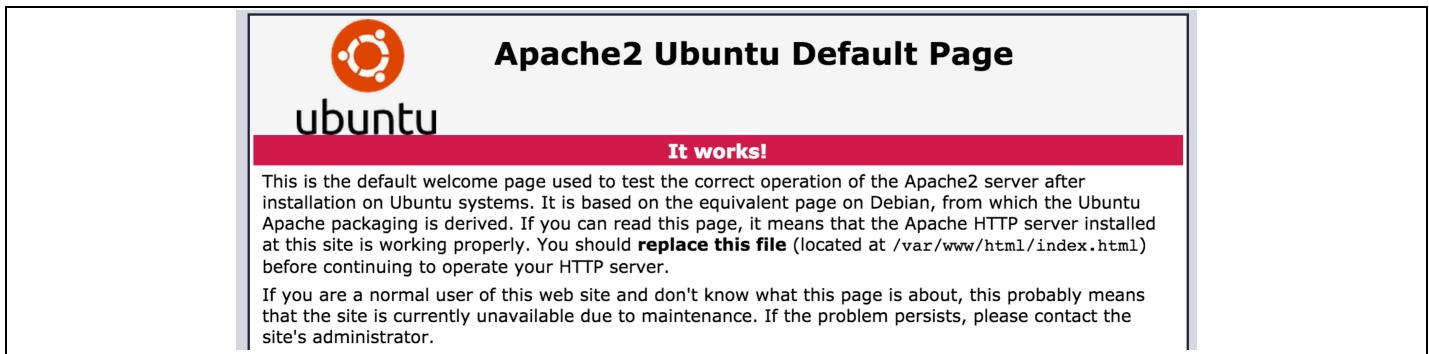
Stack Name	Created Time	Status	Description
two-tier-stack	2017-08-15 00:23:09 UTC-0700	CREATE_COMPLETE	Install WordPress server, and database fronted by PANW Firewall (sample-cft).

Below the table is a navigation bar with tabs: Overview, Outputs, Resources, Events, Template, Parameters, Tags, Stack Policy, and Change Sets. The 'Outputs' tab is selected. It displays two output items:

Key	Value	Description	Export Name
WordpressURL	http://52.15.125.207/wordpress	Wordpress server	
FirewallManagementURL	https://13.58.128.209	VM-Series management interface URL	

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

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



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

The screenshot shows the 'Monitor' tab of the Palo Alto Networks Firewall interface. The top navigation bar includes 'Dashboard', 'ACC', 'Monitor' (which is selected), 'Policies', 'Objects', 'Network', and 'Device'. On the right, there are 'Commit' and 'Manual' buttons. Below the navigation is a search bar and a table of traffic logs.

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
	08/16 20:53:35	start	external	web	68.15.90.134		10.0.0.100	80	web-browsing	allow	Web browsing	n/a	729
	08/16 20:53:33	end	external	web	68.15.90.134		10.0.0.100	80	web-browsing	allow	Web browsing	tcp-rst-from-client	4.0k

7.2 Verify Dynamic Content on Web Server

Palo Alto Networks AWS CFT Deployment Guide

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>

Overview	Outputs	Resources	Events	Template	Parameters	Tags	Stack Policy	Change Sets
Key	Value	Description						
WordpressURL	http://52.15.125.207/wordpress	Wordpress server						
FirewallManagementURL	https://13.58.128.209	VM-Series management interface URL						

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



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

Welcome

Welcome to the famous five-minute WordPress installation process! 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

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

Password uBe^aMV&0Bx#obLbOg
Strong Hide

Important: You will need this password to log in. Please store it in a secure location.

Your Email

Double-check your email address before continuing.

Search Engine Visibility Discourage search engines from indexing this site
It is up to search engines to honor this request.

7.3 SSH attack from the Web to the DB Server

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

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

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

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

The landing page is:



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

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	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
🔗	08/17 00:09:07	drop	web	db	10.0.1.101		10.0.2.101	22	not-applicable	deny	Log default deny	policy-deny	74
🔗	08/17 00:09:06	drop	web	db	10.0.1.101		10.0.2.101	22	not-applicable	deny	Log default deny	policy-deny	74

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

SSH from web server to DB server attempt launched.

RETURN TO ATTACK LAUNCH PAGE

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

7.4 SQL attack from the Web to the DB Server

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

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

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

LAUNCH BRUTE FORCE SQL ROOT PASSWORD GUESSING

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



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

The screenshot shows the same interface as the previous one, but the log table now contains three entries:

Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity
08/17 00:25:10	vulnerability	MySQL Authentication Brute Force Attempt	web	db	10.0.1.101		10.0.2.101	3306	mysql	alert	high
08/17 00:25:07	vulnerability	MySQL Login Authentication Failed	web	db	10.0.1.101		10.0.2.101	3306	mysql	reset-client	informational
08/17 00:24:53	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. If you generate multiple attacks consecutively, the severity of the attack increases. Return back to the web server attack page by clicking **RETURN TO ATTACK LAUNCH PAGE**.

Brute force MySQL root password attempt launched.

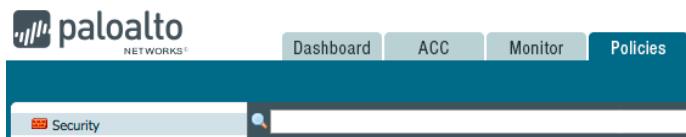
[RETURN TO ATTACK LAUNCH PAGE](#)

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

7.5 Review Threat Protection Profile

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

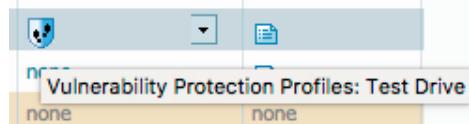
Return to the firewall management UI and click on the **Policies** tab and select **Security** on the left-hand pane.



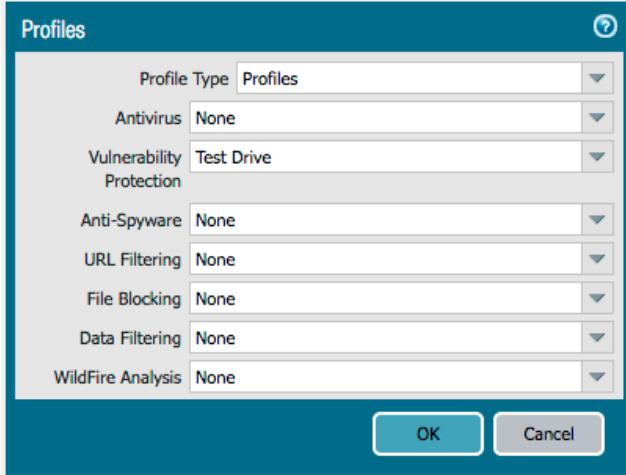
Go to the **Web to DB** rule.

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

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



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



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



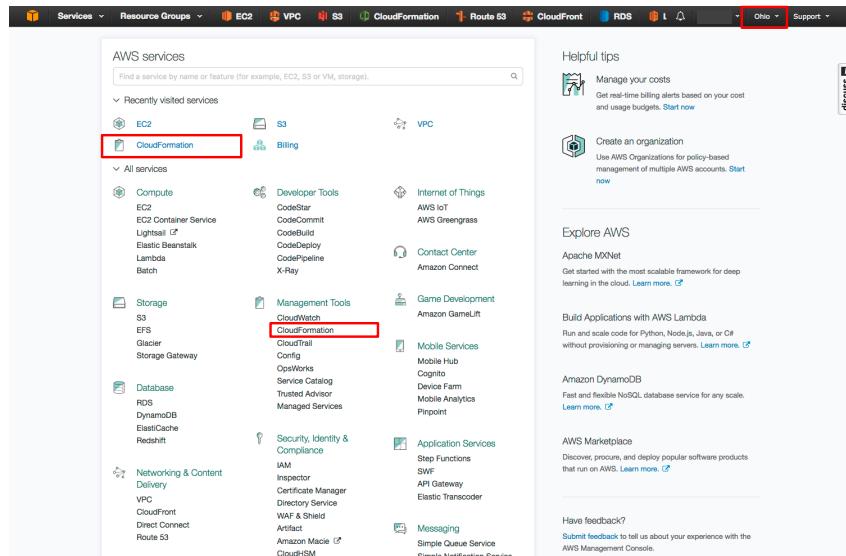
Now that you have completed the lab, it is time to erase the resources created through the template.

8. Cleanup

8.1 Delete the Stack

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

Palo Alto Networks AWS CFT Deployment Guide



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



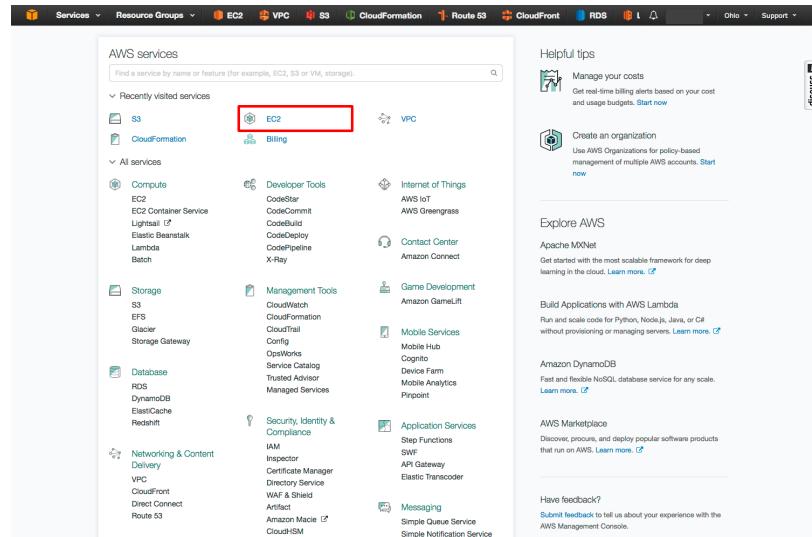
This should delete all the resources created via the template and release any Elastic IPs associated with the firewall.

8.2 Delete keys

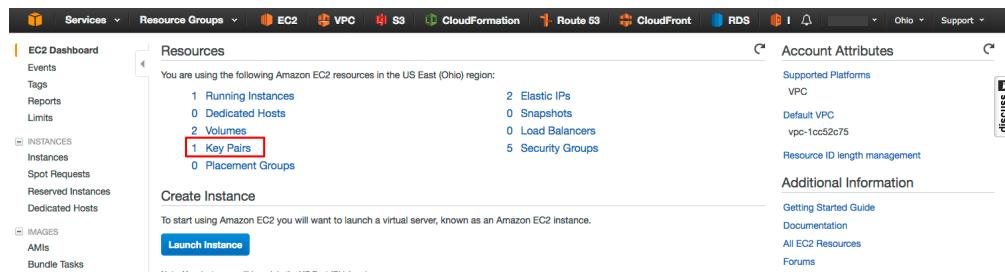
As part of the lab exercise, a key pair was manually created thus it must be manually removed.

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

Palo Alto Networks AWS CFT Deployment Guide



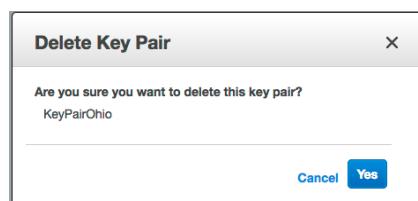
Click on **Key Pairs**:



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



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



Congratulations, you have successfully completed the lab.

9. Conclusion

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

Appendix A

Troubleshooting tips

1. Stack creation fails

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

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

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

2. EIP Exhaustion

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

Overview	Outputs	Resources	Events	Template	Parameters	Tags	Stack Policy	Change Sets
▶ 09:09:02 UTC-0600	CREATE_COMPLETE	AWS::EC2::NetworkAcl		aci0/c00002				
▶ 09:09:02 UTC-0600	CREATE_IN_PROGRESS	AWS::EC2::VPCHDCHPOptionsAssociation		dchpassoc1			Resource creation initiated	
▶ 09:09:02 UTC-0600	CREATE_IN_PROGRESS	AWS::EC2::RouteTable		rtb059a2460			Resource creation initiated	
09:09:02 UTC-0600	CREATE_FAILED	AWS::EC2::EIP		ManagementElasticIP			The maximum number of addresses has been reached.	
09:09:02 UTC-0600	CREATE_FAILED	AWS::EC2::EIP		PublicElasticIP			The maximum number of addresses has been reached.	
▶ 09:09:02 UTC-0600	CREATE_IN_PROGRESS	AWS::EC2::RouteTable		rtb049a2461			Resource creation initiated	
▶ 09:09:01 UTC-0600	CREATE_IN_PROGRESS	AWS::EC2::NetworkAcl		aci0/b65d6d2			Resource creation initiated	
09:09:01 UTC-0600	CREATE_IN_PROGRESS	AWS::EC2::VPCHDCHPOptionsAssociation		dchpassoc1			Resource creation initiated	
09:09:01 UTC-0600	CREATE_IN_PROGRESS	AWS::EC2::RouteTable		rtb059a2460				

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

3. Bootstrapping not working

If the VM-Series firewall is up and you are able to access the login page, but unable to login using the username/password: admin/paloalto, then chances are 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 4.4 are not corrupted.

b. Incorrect bootstrap bucket-name

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