

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

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

Version History

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

1. About CFTs

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

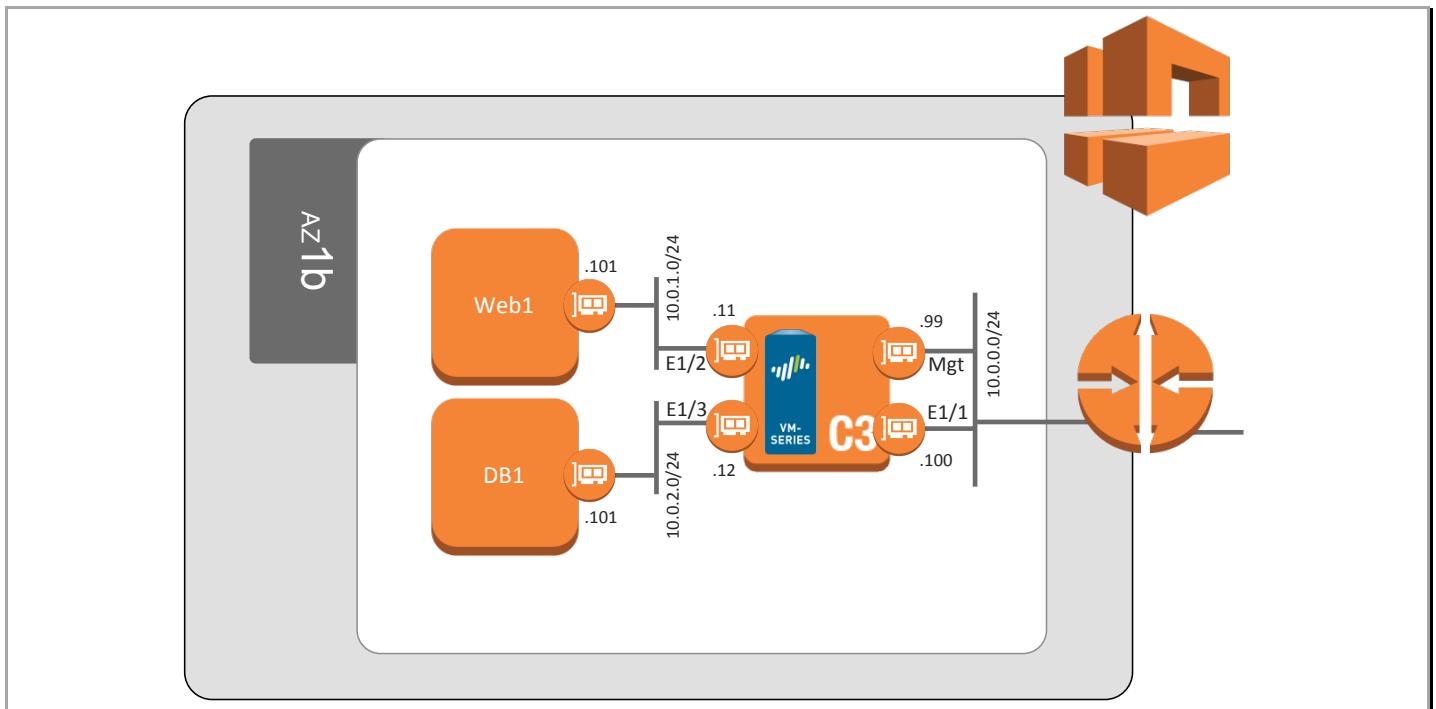
For more information on CFTs and sample CFTs refer to Amazon's documentation

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

There are also many sample templates available here

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

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



2. Support Policy

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

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

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

3. Instances used

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

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

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

4. Prerequisites

Here are the prerequisites required to successfully launch this template.

4.1 Create an AWS account

If you do not have an AWS account already, go to <https://aws.amazon.com/console/> and create an account.

4.2 Add a credit card to your AWS account

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

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

4.3 Review and accept the EULA

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

Palo Alto Networks AWS CFT Deployment Guide

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

The screenshot shows the AWS Management Console with the 'Services' menu selected. The 'Amazon Web Services' section is expanded, displaying various service categories and their sub-services. On the right side, there is a sidebar titled 'Resource Groups' with a 'Create a Group' button and a 'Tag Editor' button. Below that is an 'Additional Resources' section containing links to 'Getting Started', 'AWS Console Mobile App', 'AWS Marketplace' (which is highlighted with a red border), 'AWS re:Invent Announcements', and 'Service Health'. At the bottom of the sidebar, it says 'All services operating normally.' and 'Updated: Feb 23 2016 12:18:02 GMT-0800'. The URL in the address bar is <https://console.aws.amazon.com/cloudformation/home?region=us-west-2>.

Amazon Web Services

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

Narayan Iyengar - Oregon - Support

Resource Groups Learn more

A resource group is a collection of resources that share one or more tags. Create a group for each project, application, or environment in your account.

Create a Group Tag Editor

Additional Resources

Getting Started Read our documentation or view our training to learn more about AWS.

AWS Console Mobile App View your resources on the go with our AWS Console mobile app, available from Amazon Appstore, Google Play, or iTunes.

AWS Marketplace Find and buy software, launch with 1-Click and pay by the hour.

AWS re:Invent Announcements Explore the next generation of AWS cloud capabilities. See what's new

Service Health

All services operating normally.

Updated: Feb 23 2016 12:18:02 GMT-0800

Service Health Dashboard

<https://console.aws.amazon.com/cloudformation/home?region=us-west-2>

Palo Alto Networks AWS CFT Deployment Guide

The screenshot shows the AWS Marketplace search interface. In the search bar at the top right, the query "palo alto networks firewall" is entered. Below the search bar, a dropdown menu lists several suggestions: "palo alto networks firewall", "palo alto", "palo alto networks", "palo alto networks firewall", "palo alt", "palo alto firewall", and "palo alot". To the right of the search bar are buttons for "GO" and "Your Account | Help | Sell on AW". On the left, a sidebar titled "Shop All Categories" lists various software categories. At the bottom, there's a "Featured Products" section with a "HYBRID CLOUD BACKUP AND DR" advertisement for "Q CLOUD PRO TEC" featuring a "FREE 30 DAY TRIAL".

Select VM-Series Next Generation Firewall Bundle 2

The screenshot shows the product details for the "VM-Series Next-Generation Firewall Bundle 2" from Palo Alto Networks. The product has a rating of ★★★★☆ (1) and is sold by Palo Alto Networks. It costs \$1.28/hr or \$4,500/yr (60% savings) for software + AWS usage fees. The description states: "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, ...". A note indicates it's for Linux/Unix, Other PAN-OS 7.0.1 | 64-bit Amazon Machine Image (AMI). A "Free Trial" button is visible on the left.

Palo Alto Networks AWS CFT Deployment Guide

The screenshot shows the AWS Marketplace product page for the VM-Series Next-Generation Firewall Bundle 2. At the top, there's a navigation bar with links for 'Amazon Web Services Home', 'Your Account | Help | Sell on AWS Marketplace', 'Sign in or Create a new account', and a search bar. Below the header, there's a category dropdown 'Shop All Categories ▾' and a search field 'Search AWS Marketplace' with a 'GO' button. The main title 'VM-Series Next-Generation Firewall Bundle 2' is displayed in orange, along with the seller information 'Sold by: Palo Alto Networks'. The Palo Alto Networks logo is shown next to the seller name. A promotional message states '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 ...' followed by a 'Read more' link. On the left, there's a vertical sidebar with sections for 'Customer Rating' (4.5 stars, 1 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), and '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). On the right, there's a 'Continue' button in a yellow box, a note about reviewing the order before launching, and a 'Pricing Details' section with a dropdown for 'For region' set to 'US West (Oregon)', 'Hourly Fees' (total fees will vary by instance type and EC2 region), and a toggle switch for 'Fees: Hourly' (switch is off, labeled 'Annual').

Click Continue.

The screenshot shows the AWS Marketplace interface for the VM-Series Next-Generation Firewall Bundle 2. At the top, there's a navigation bar with links to 'Amazon Web Services Home', 'Your Account', 'Help', and 'Sell on AWS Marketplace'. Below the navigation is a search bar labeled 'Search AWS Marketplace' and a 'GO' button. A 'Shop All Categories' dropdown is also present.

The main content area features a product title 'VM-Series Next-Generation Firewall Bundle 2' and two launch options: '1-Click Launch' and 'Manual Launch'. The 'Manual Launch' option is highlighted with a red box. Below it, a note says 'Click "Accept Software Terms" to gain access to this software'. A large yellow 'Accept Software Terms' button is positioned next to a detailed note about the software's usage and licensing.

On the left, there's a 'Software Pricing' section with a 'Subscription Term' dropdown (set to 'Hourly') and an 'Applicable Instance Type' section showing 'Software fee' as 'Varies' and noting it depends on instance type. A blue 'Usage Instructions' button is located below these sections.

On the right, there's a 'Price for your selections:' section with a note that price will be dependent on usage. It includes a 'Pricing Details' section with a dropdown for 'For region' set to 'US West (Oregon)' and a note about a free trial expiring. Below this is a table showing 'Hourly Fees' for different EC2 instance types.

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

You should see this screen:

This screenshot shows a confirmation message in a green-bordered box: '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.'

You can now proceed to the next step.

4.4 Create and download an SSH keypair

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

The screenshot shows the AWS Services dashboard. The EC2 icon is highlighted with a red box. Other services listed include VPC, CloudFormation, Lambda, S3, CloudFront, Elastic File System, Glacier, Import/Export Snowball, Storage Gateway, RDS, DynamoDB, and ElastiCache.

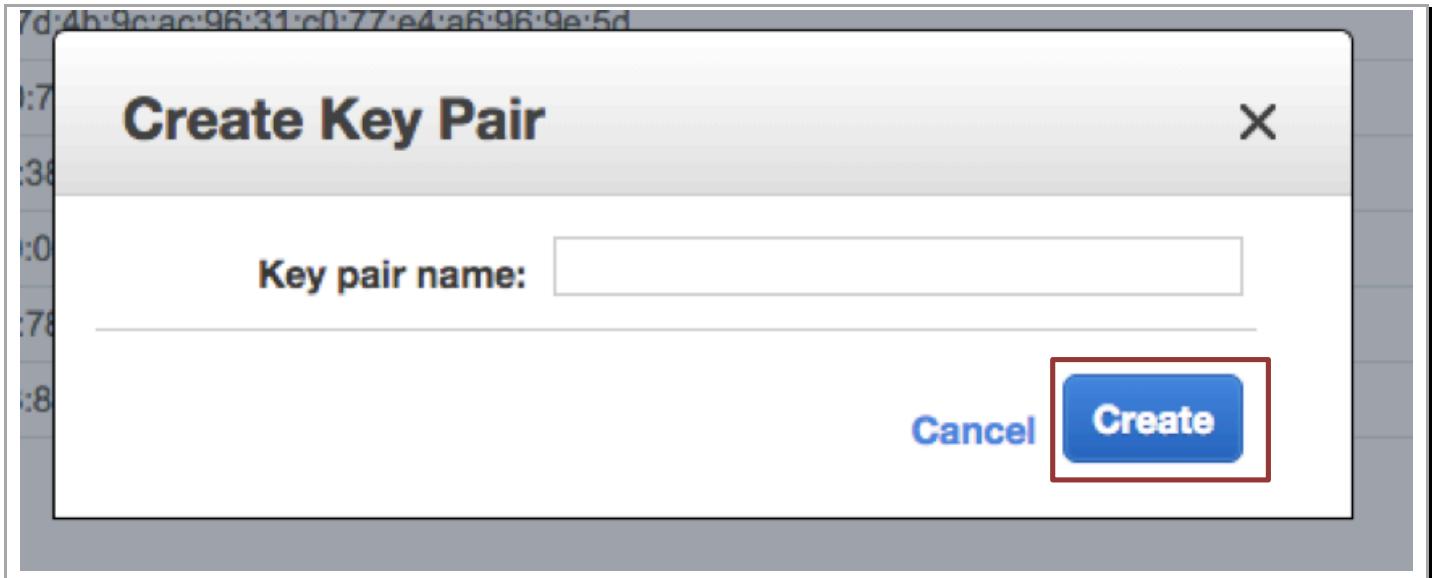
Click KeyPairs

The screenshot shows the EC2 Dashboard. The 'Key Pairs' section is highlighted with a red box. It displays 11 Key Pairs.

Click Create Key Pair

The screenshot shows the EC2 Key Pairs page. The 'Create Key Pair' button is highlighted with a red box.

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**

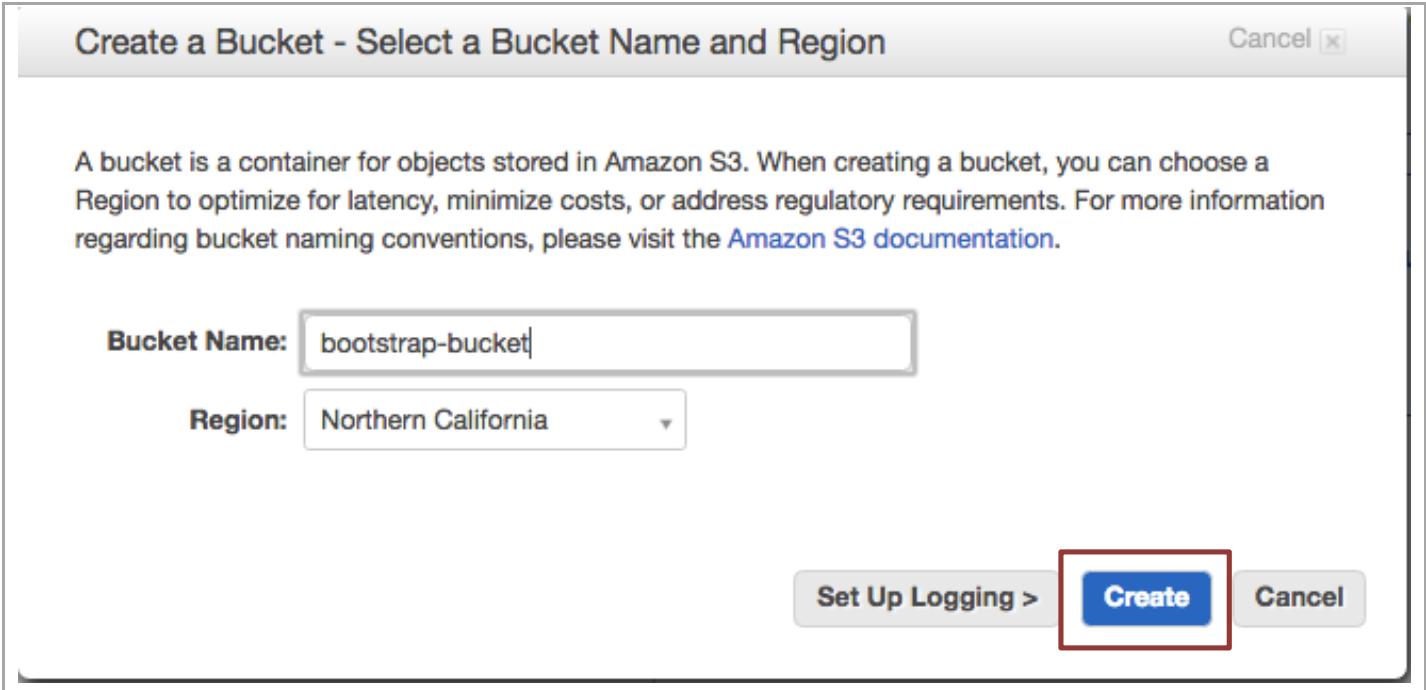
Palo Alto Networks AWS CFT Deployment Guide

The screenshot shows the AWS Management Console with the Services menu open. The 'Amazon Web Services' section is selected. The services listed under 'Storage & Content Delivery' include S3 (Scalable Storage in the Cloud), CloudFront (Global Content Delivery Network), Elastic File System (PREVIEW), Glacier, Import/Export Snowball, Storage Gateway, and others. The 'S3' service is highlighted with a red box. Other sections like Compute, Developer Tools, Internet of Things, Game Development, Mobile Services, Application Services, and various management tools are also visible.

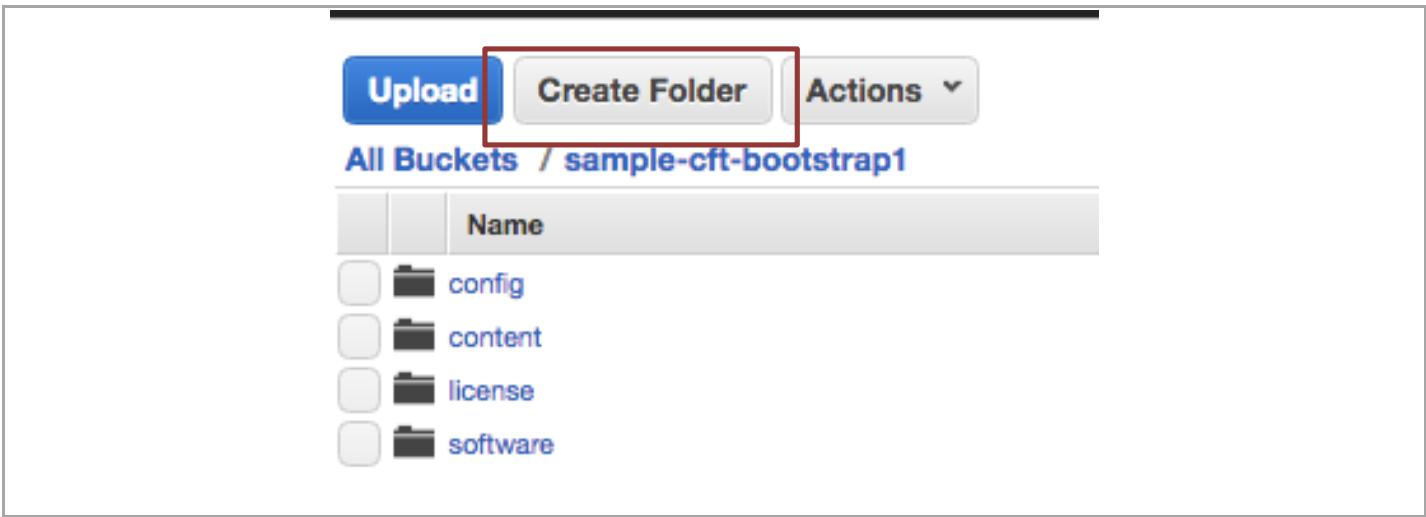
Click **Create Bucket**:

The screenshot shows the AWS S3 service page. The top navigation bar includes the AWS logo, Services dropdown, and links for S3, EC2, and VPC. A large blue 'Create Bucket' button is prominently displayed, with a red box highlighting it. Below the button is an 'Actions' dropdown menu.

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



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



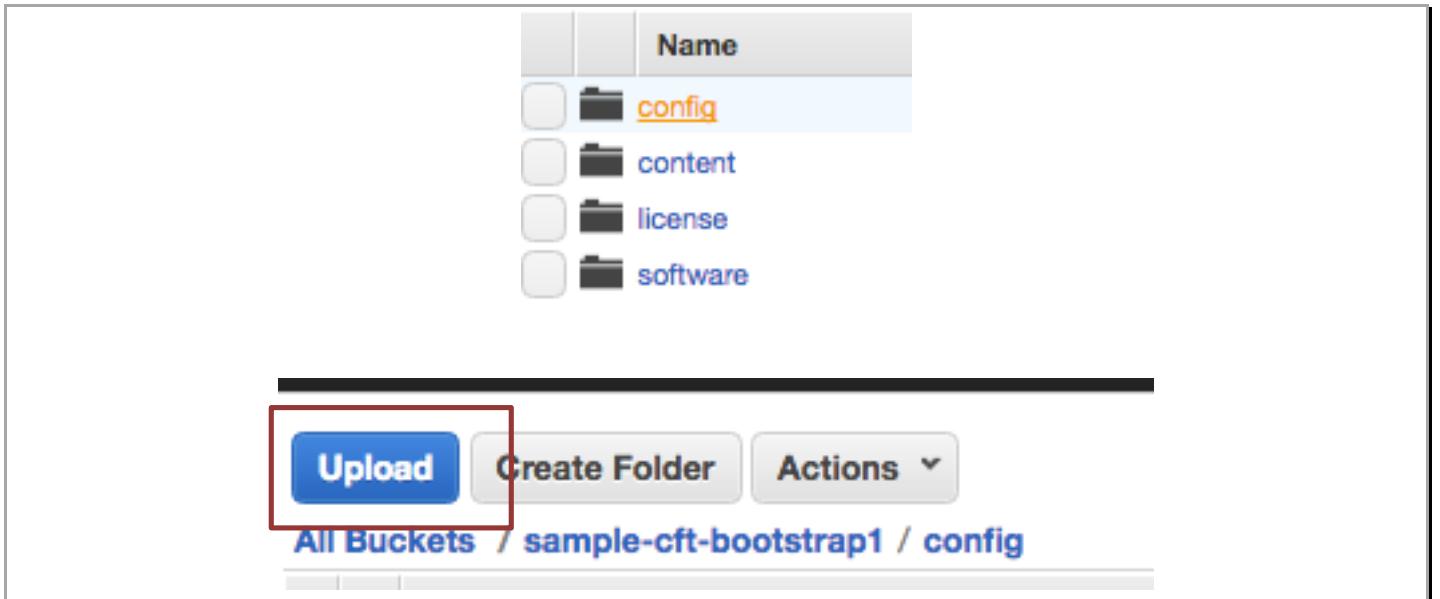
Download the following files and save them in a known location:

[https://raw.githubusercontent.com/PaloAltoNetworks/aws/master/two-tier sample/bootstrap/bootstrap.xml](https://raw.githubusercontent.com/PaloAltoNetworks/aws/master/two-tier%20sample/bootstrap/bootstrap.xml)

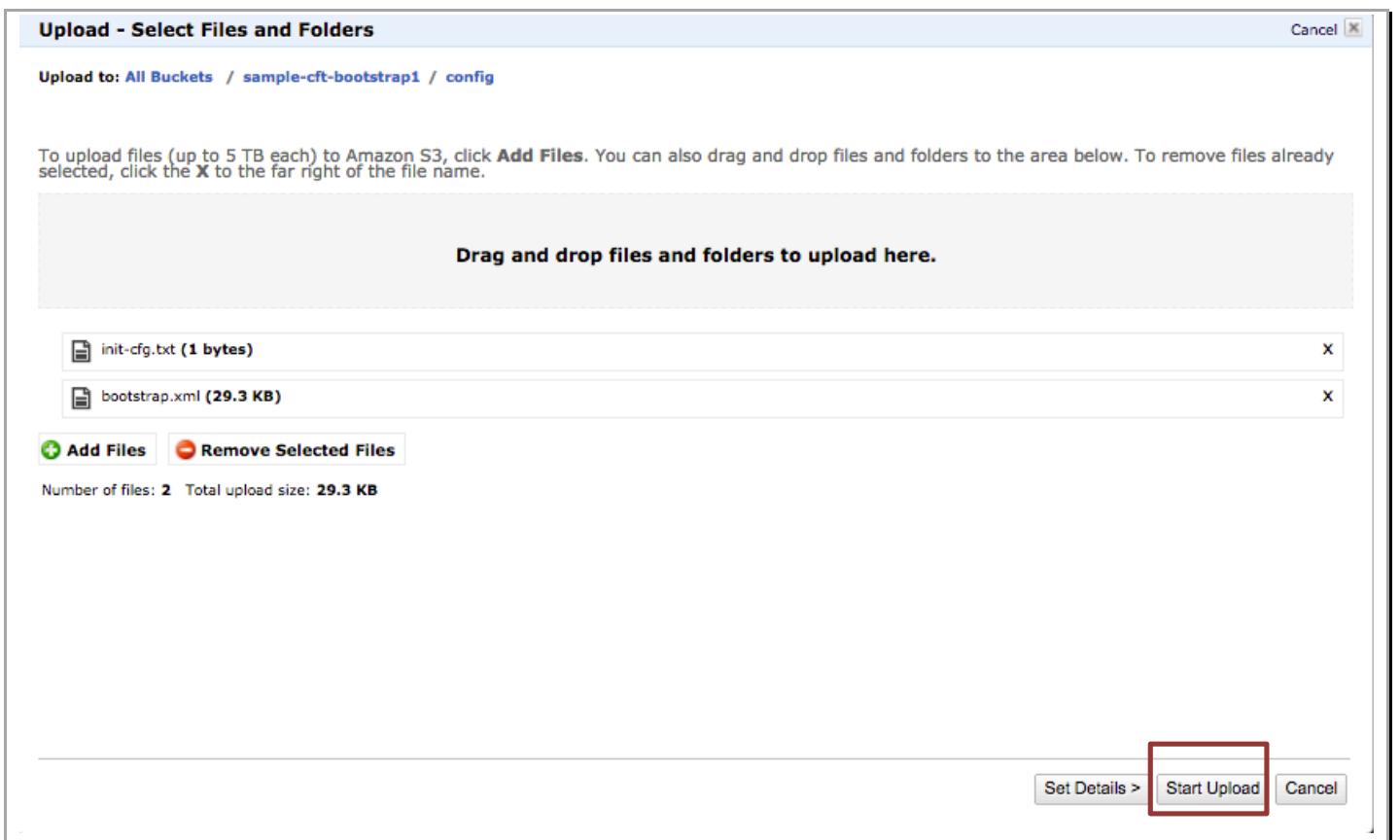
[https://raw.githubusercontent.com/PaloAltoNetworks/aws/master/two-tier sample/bootstrap/init-cfg.txt](https://raw.githubusercontent.com/PaloAltoNetworks/aws/master/two-tier%20sample/bootstrap/init-cfg.txt)

[https://github.com/PaloAltoNetworks/aws/raw/master/two-tier sample/bootstrap/panupv2-all-contents-600-3449](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**:

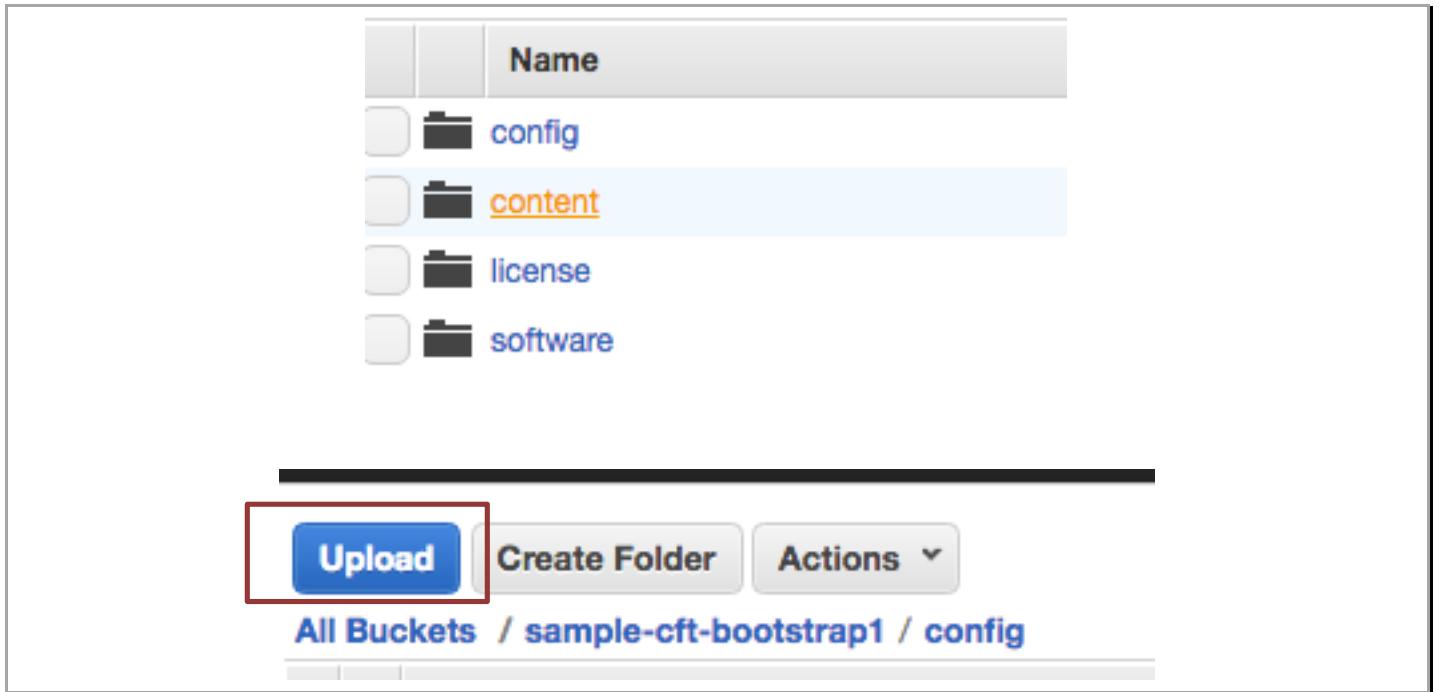


Select **Add Files** and select the two files (bootstrap.xml and init-cft.txt) downloaded previously and click **Start Upload**:

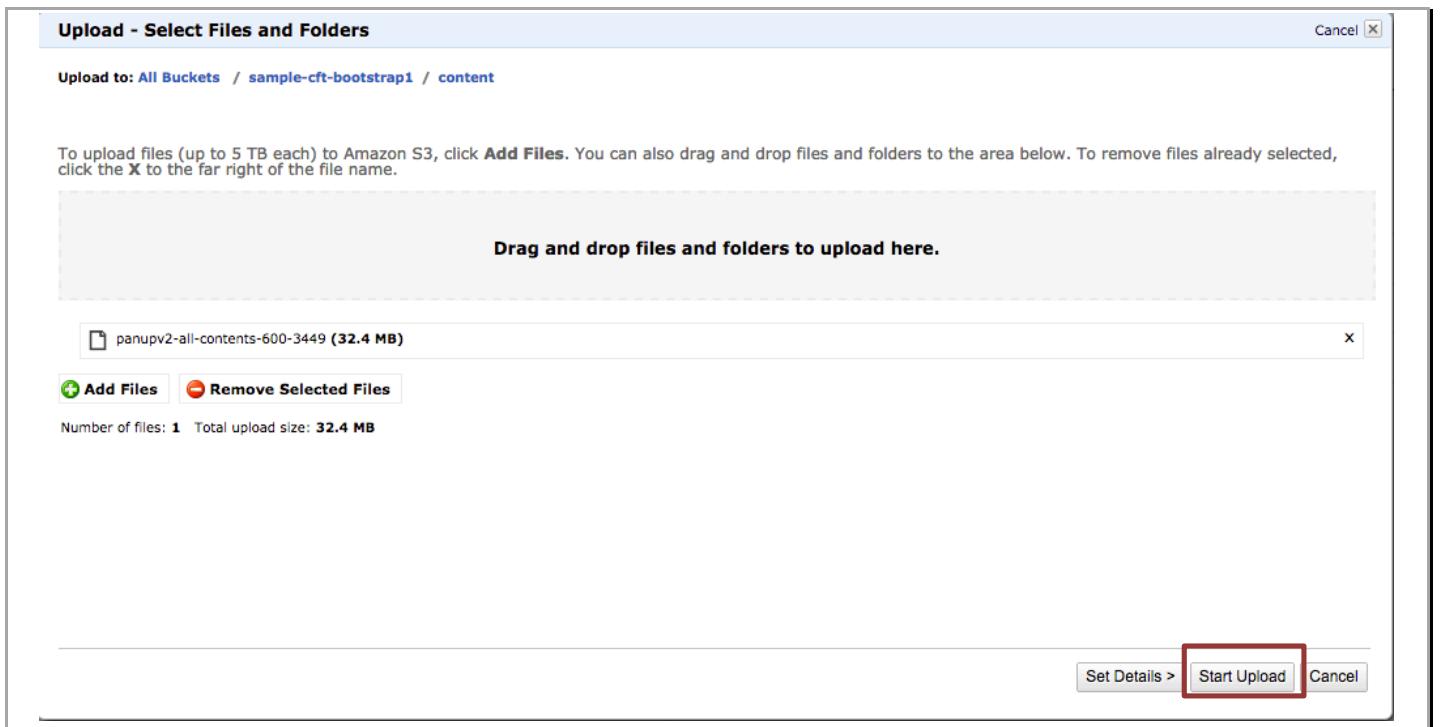


Palo Alto Networks AWS CFT Deployment Guide

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



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



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

4.6 Download the Template

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

[https://raw.githubusercontent.com/PaloAltoNetworks/aws/master/two-tier sample/pan-sample-cft.json](https://raw.githubusercontent.com/PaloAltoNetworks/aws/master/two-tier%20sample/pan-sample-cft.json)

4.7 Check Elastic IPs

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

The screenshot shows the AWS Management Console interface. At the top, there's a navigation bar with icons for AWS, Services, EC2 (which is highlighted with a red box), VPC, CloudFormation, and Edit. Below the navigation bar, the page title is "Amazon Web Services". The main content area is organized into several sections: "Compute" (with EC2, Container Service, Beanstalk, Lambda), "Storage & Content Delivery" (with S3, CloudFront, Elastic File System, Glacier, Import/Export Snowball, Storage Gateway), "Database" (with RDS, DynamoDB, ElastiCache), "Developer Tools" (with CodeCommit, CodeDeploy, CodePipeline), "Management Tools" (with CloudWatch, CloudFormation, CloudTrail, Config, OpsWorks, Service Catalog, Trusted Advisor), "Security & Identity" (with Identity & Access Management, Directory Service), and "Internet of Things" (with AWS IoT). On the right side, there are additional sections: "Game Development" (with GameLift), "Mobile Services" (with Mobile Hub, Cognito, Device Farm, Mobile Analytics, SNS), and "Application Services" (with API Gateway, AppStream, CloudSearch, Elastic Transcoder). Each service item includes a small icon and a brief description.

And click on Elastic IPs:

Palo Alto Networks AWS CFT Deployment Guide

The screenshot shows the AWS EC2 Dashboard. In the left sidebar, under the 'Elastic IP' section, there is a link labeled 'Elastic IPs' which is highlighted with a red box. The main content area displays a table of allocated elastic IP addresses:

Elastic IP	Allocation ID	Instance	Private IP Address	Scope	Public DNS
52.10.248.59	eipalloc-b4f702d3			vpc	
52.36.170.123	eipalloc-3fff0a58			vpc	

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**

The screenshot shows the AWS EC2 Dashboard with the 'Allocate New Address' button highlighted. In the main content area, an EIP address '52.10.248.59' is selected, and a context menu is open over it. The menu options are: 'Allocate New Address', 'Release Addresses' (which is highlighted with a red box), 'Associate Address', and 'Disassociate Address'. The main table below shows two entries:

Elastic IP	Allocation ID	Instance
52.10.248.59	eipalloc-b4f702d3	
52.36.170.123	eipalloc-3fff0a58	

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**

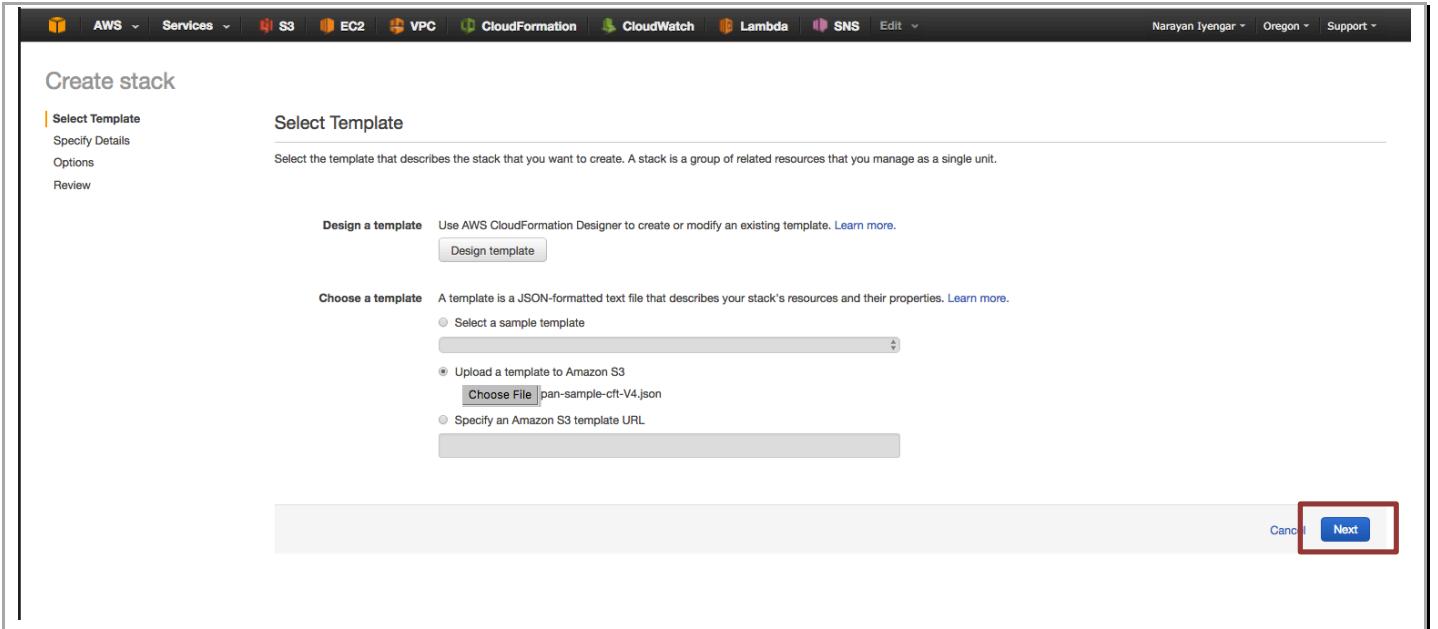
The screenshot shows the AWS Services dashboard. The 'CloudFormation' icon under 'Management Tools' is highlighted with a red box. Other visible services include CloudWatch, Config, OpsWorks, Service Catalog, Trusted Advisor, Identity & Access Management, Directory Service, Inspector, WAF, Certificate Manager, EMR, Data Pipeline, Elasticsearch Service, API Gateway, AppStream, CloudSearch, Elastic Transcoder, SES, SQS, SWF, WorkSpaces, and WorkDocs.

Click **Create Stack**:

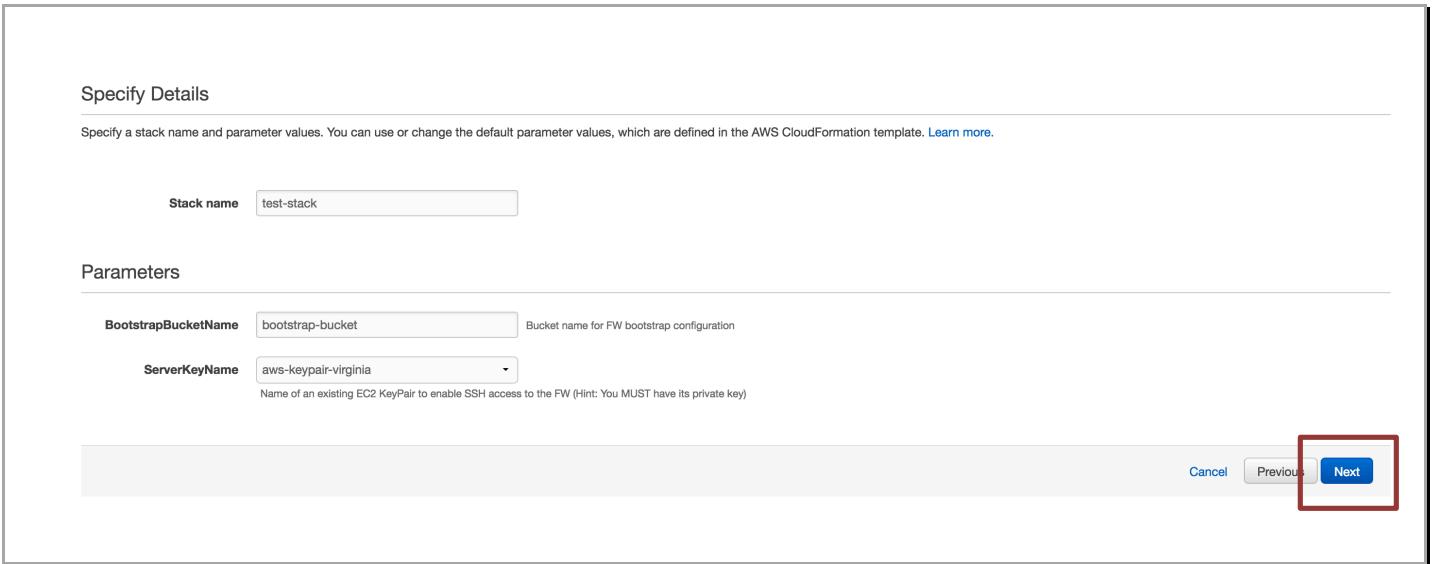
The screenshot shows the 'Create Stack' page. At the top, there are buttons for 'Create Stack', 'Actions', and 'Design template'. Below that, there are filters: 'Filter: Active' and 'By Name:'. The URL in the address bar is <https://console.aws.amazon.com/cloudformation/home?region=us-west-2#/stacks?filter=active&stackId=ar>.

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



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



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

Palo Alto Networks AWS CFT Deployment Guide

The screenshot shows the 'Create stack' wizard at the 'Options' step. On the left, a vertical navigation bar lists 'Select Template', 'Specify Details', 'Options' (which is selected and highlighted in orange), and 'Review'. The main area is titled 'Options' and contains a 'Tags' section. It says you can specify tags for resources in your stack, with a note that you can add up to 10 unique key-value pairs. A table shows one tag entry: 'Key' (Group) and 'Value' (Word Press Demo). Below this is an 'Advanced' section with a note about setting notification options and stack policies. At the bottom right are 'Cancel', 'Previous', and a large blue 'Next' button.

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

The screenshot shows the 'Create stack' wizard at the 'Review' step. It displays the template details: 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)), and Estimate cost (Cost). The 'Stack details' section shows the stack name 'teststack' and other parameters like FWInstancePassword, ServerKeyName, and Create IAM resources. The 'Options' section includes 'Tags' (No tags provided) and 'Advanced' settings for Notification (Timeout: none, Rollback on failure: Yes). The 'Capabilities' section contains a note about required IAM capabilities and a checkbox for acknowledging potential IAM resource creation. At the bottom right are 'Cancel', 'Previous', and a large blue 'Create' button.

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 that is a search bar with 'Filter: Active' and 'By Name:'. A table lists one stack: 'teststack' was created on '2016-02-23 12:48:50 UTC-0800' and is currently in the 'CREATE_IN_PROGRESS' state. The status cell is highlighted with a red box. The 'Description' column indicates it's for 'Install VM-Series helper, WordPress server, and database fronted by PANW BYOL Firewall (test-drive)'. Below the table, tabs for 'Overview', 'Outputs', 'Resources', 'Events' (which is selected), 'Template', 'Parameters', 'Tags', and 'Stack Policy' are visible. Under the 'Events' tab, a single event is listed: 'Status' is 'CREATE_IN_PROGRESS', 'Type' is 'AWS::CloudFormation::Stack', 'Logical ID' is 'teststack', and 'Status Reason' is 'User Initiated'. The entire screenshot is enclosed in a black border.

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

The screenshot shows the AWS CloudFormation console. The 'Events' tab is selected, indicated by a red box around its tab header. The table lists several events: 13:02:19 UTC-0800: CREATE_COMPLETE (Type: AWS::CloudFormation::Stack, Logical ID: teststack). Subsequent rows show various resources being created: VMSeriesHelper (Custom::VMSeriesHelper), FWInstance (AWS::EC2::Instance), WPWebInstance (AWS::EC2::Instance), WPDBServerInstance (AWS::EC2::Instance), FWInstance (AWS::EC2::Instance), FWInstance (AWS::EC2::Instance), FWEIPManagementAssociation (AWS::EC2::EIPAssociation), FWEIPPublicAssociation (AWS::EC2::EIPAssociation), and VMSeriesHelperInstance (AWS::EC2::Instance). All events have a status of 'CREATE_COMPLETE'. The entire screenshot is enclosed in a black border.

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 selected. The 'Events' tab is active, displaying 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	AWSMonitorUserKey	
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 10:02:14 UTC-0800	CREATE_COMPLETE	AWS::EC2::EIPAssociation	EIPFWInstanceAssociation	

A red box highlights the 'Delete Stack' option in the 'Actions' dropdown menu for the 'teststack' stack.

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 with the 'teststack' stack selected. The 'Events' tab is active, displaying the following log entries:

Time	Status	Type	Logical ID	Status Reason
2016-02-23 13:02:19 UTC-0800	CREATE_COMPLETE	AWS::CloudFormation::Stack	teststack	
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	

6. Review what was created

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

Palo Alto Networks AWS CFT Deployment Guide

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

Here you should see all VPCs created in your account:

The screenshot shows the AWS VPC Dashboard. At the top, there's a navigation bar with icons for Home, AWS, Services, and Edit. Below the navigation bar, the title "VPC Dashboard" is displayed, followed by a "Filter by VPC:" dropdown set to "None". On the left side, there's a sidebar with links for "Virtual Private Cloud" (Your VPCs, Subnets, Route Tables, Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, NAT Gateways, Peering Connections) and "Security" (Network ACLs, Security Groups). Under "VPN Connections", there are links for Customer Gateways, Virtual Private Gateways, and VPN Connections. In the main content area, the title "Resources" is shown with a refresh icon. Below it are two buttons: "Start VPC Wizard" (blue) and "Launch EC2 Instances" (grey). A note states: "Note: Your Instances will launch in the US West (Oregon) region." Below this, a section says: "You are using the following Amazon VPC resources in the US West (Oregon) region:". A table lists the following counts:

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

VPN Connections

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.

[Create VPN Connection](#)

Palo Alto Networks AWS CFT Deployment Guide

Here is the sample VPC:

The screenshot shows the AWS VPC Dashboard. A red box highlights the 'Your VPCs' section on the left sidebar. The main table displays one VPC entry:

Name	VPC ID	State	VPC CIDR	DHCP options set	Route table	Network ACL	Tenancy	Default VPC
PAN Sample CFT	vpc-e2a95c86	available	10.0.0.0/16	dopt-4376e926	rtb-4318d127	acl-4fb64f2b	Default	No

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

The screenshot shows the AWS Subnet Dashboard. A red box highlights the 'Subnets' section on the left sidebar. The main table displays three subnet entries:

Name	Subnet ID	State	VPC	CIDR	Available IPs	Availability Zone	Route Table	Network ACL	Default Subnet
PAN Sample CFT	subnet-d9e01fb0	available	vpc-e2a95c86 (10.0.0.0/16) PA...	10.0.2.0/24	249	us-west-2a	rtb-4318d127	acl-53b64f37	No
PAN Sample CFT	subnet-dee01fba	available	vpc-e2a95c86 (10.0.0.0/16) PA...	10.0.0.0/24	249	us-west-2a	rtb-5d18d139	acl-53b64f37	No
PAN Sample CFT	subnet-dde01fb9	available	vpc-e2a95c86 (10.0.0.0/16) PA...	10.0.1.0/24	249	us-west-2a	rtb-4318d127	acl-53b64f37	No

Route tables:

The screenshot shows the AWS Route Table Dashboard. A red box highlights the 'Route Tables' section on the left sidebar. The main table displays three route table entries:

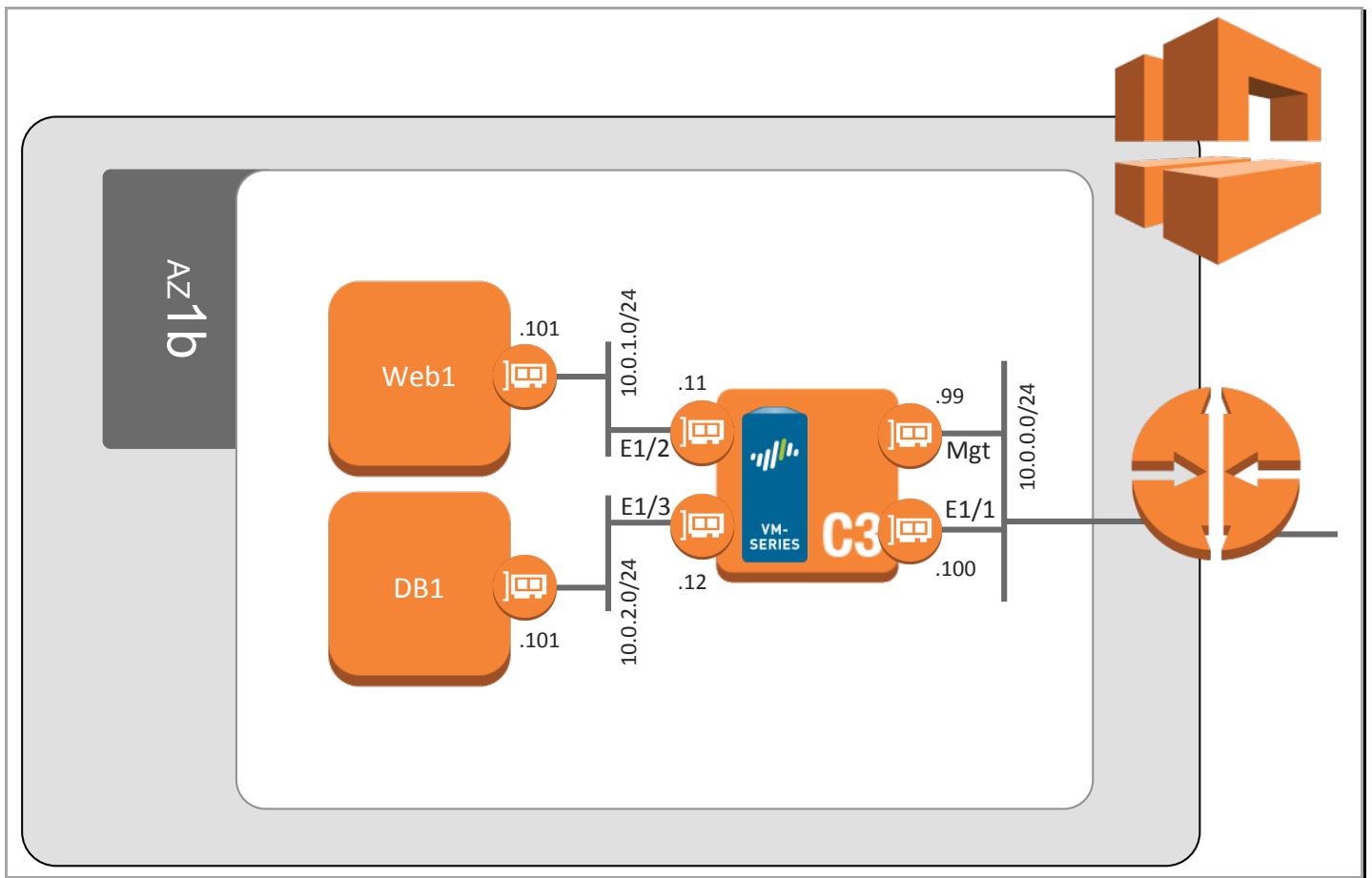
Name	Route Table ID	Explicitly Associated	Main	VPC
rtb-4318d127	0 Subnets	Yes	vpc-e2a95c86 (10.0.0.0/16) PA...	
rtb-5d18d139	1 Subnet	No	vpc-e2a95c86 (10.0.0.0/16) PA...	
rtb-5e18d13a	0 Subnets	No	vpc-e2a95c86 (10.0.0.0/16) PA...	

And **Elastic IPs (EIPs)**:

Palo Alto Networks AWS CFT Deployment Guide

Address	Allocation ID	Instance ID	Network Interface ID	Scope	Private Address
52.37.160.107	eipalloc-be16deda	i-69f386ae	eni-3c93a844	vpc	10.0.0.99
52.37.158.52	eipalloc-a02be3c4	i-69f386ae	eni-178ab16f	vpc	10.0.0.100

All of this matches the topology shown previously:



7. Access the VM-Series Firewall

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

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

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**

8. Review the VM-Series WebUI

In this activity, you will:

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

Task 1 – Login and Dashboard summary

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

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

Palo Alto Networks AWS CFT Deployment Guide

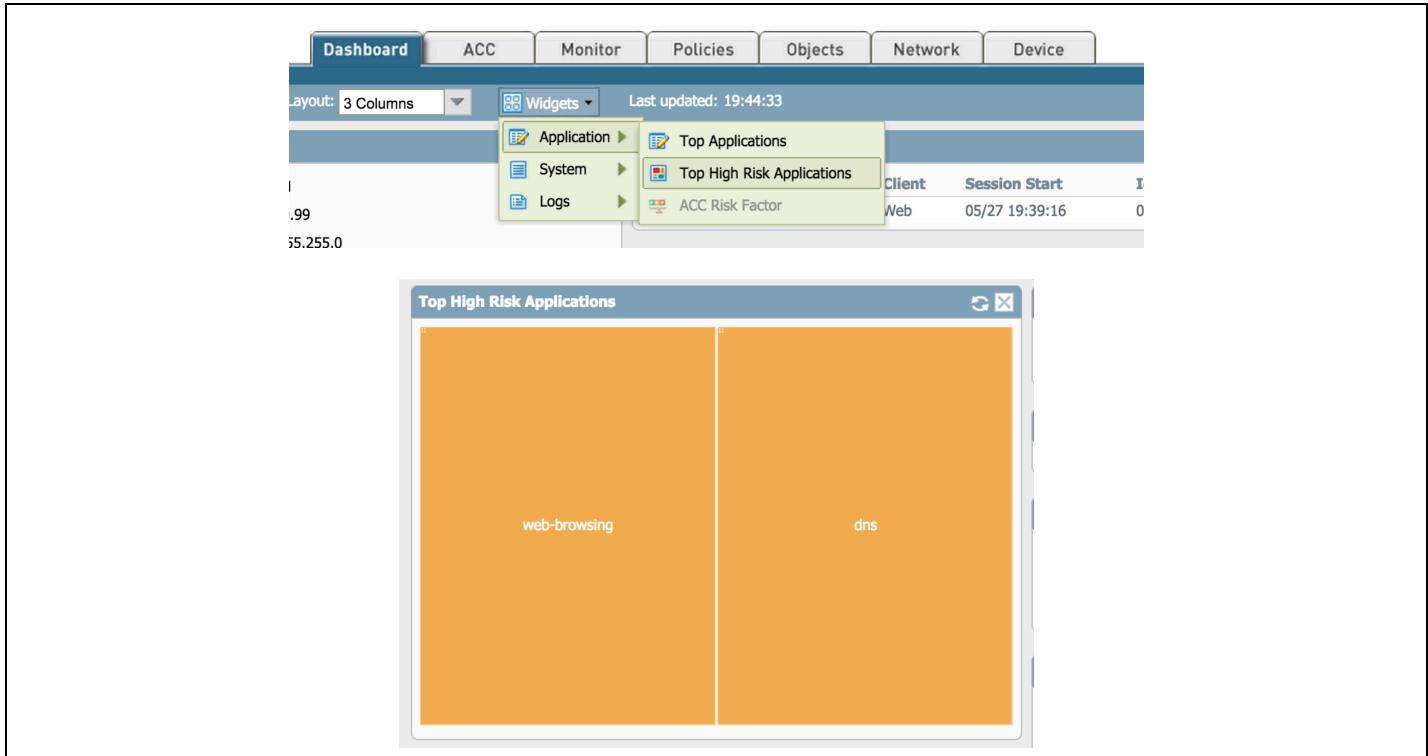


Upon login, you will see the dashboard for the VM-Series. The dashboard provides a visual summary of the device status. It is widget-based and can be customized to fulfill your specific requirements.

A screenshot of the Palo Alto Networks VM-Series dashboard. The top navigation bar includes tabs for Dashboard, ACC, Monitor, Policies, Objects, Network, and Device. On the far right are buttons for Commit, Save, and Help. The main area contains several widgets: 1) General Information: displays device details like Device Name (PA-VM), MGT IP Address (10.0.0.99), and CPU ID (AWSMKT:806j2ofoqy5osgljxq9gqc6g:us-west-2). 2) Logged In Admins: shows one admin session from IP 199.167.52.5 via Web at 05/27 19:39:16. 3) Data Logs: indicates 'No data available.' 4) System Resources: shows Management CPU at 6%, Data Plane CPU at 1%, and Session Count at 0 / 249998. 5) Config Logs: states 'No data available.' 6) Locks: states 'No locks found.' 7) ACC Risk Factor (Last 60 minutes): shows a value of 4.0 on a color-coded scale. 8) System Logs: lists various log entries such as user authentication and system upgrades.

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

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



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

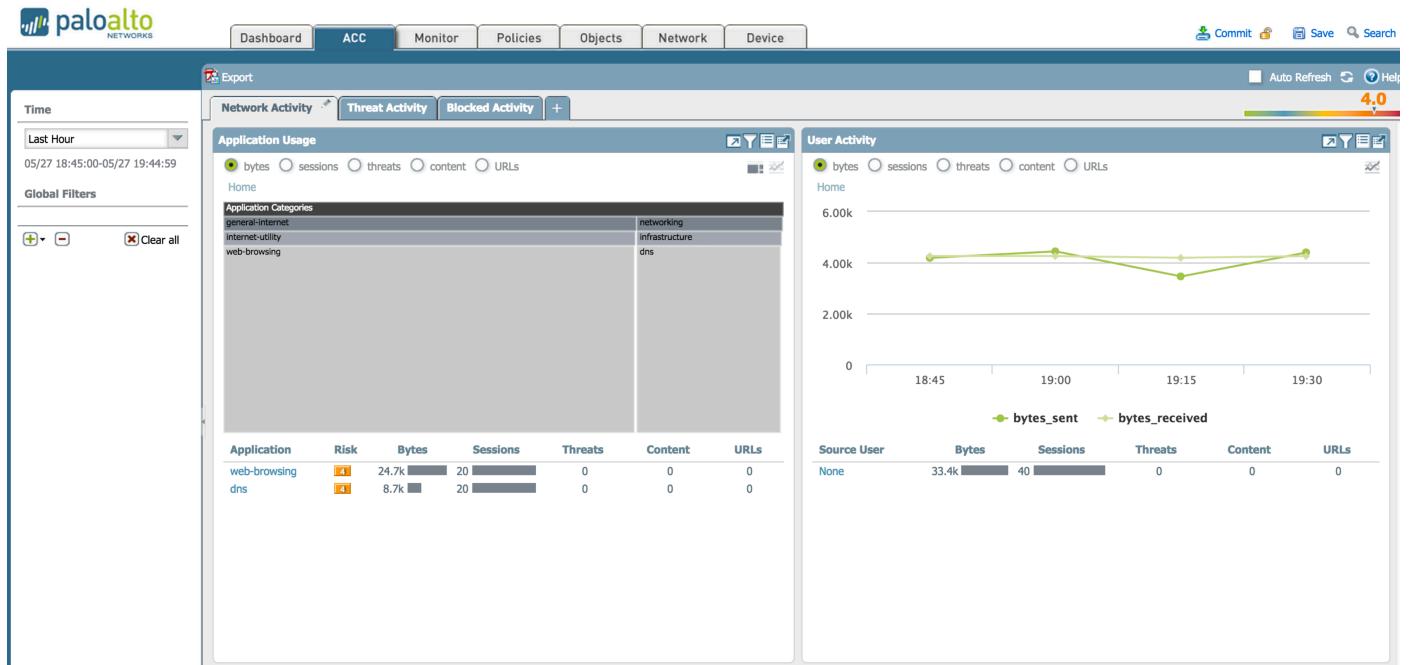
The ACC provides you with a widget-based summary of the applications, the content within, and who the user is over a given time period [default is 1 hour]. With the ACC, you can see the contextual linkage between the application and the content, which allows you to make more informed security decisions.

Select the **ACC** Tab.

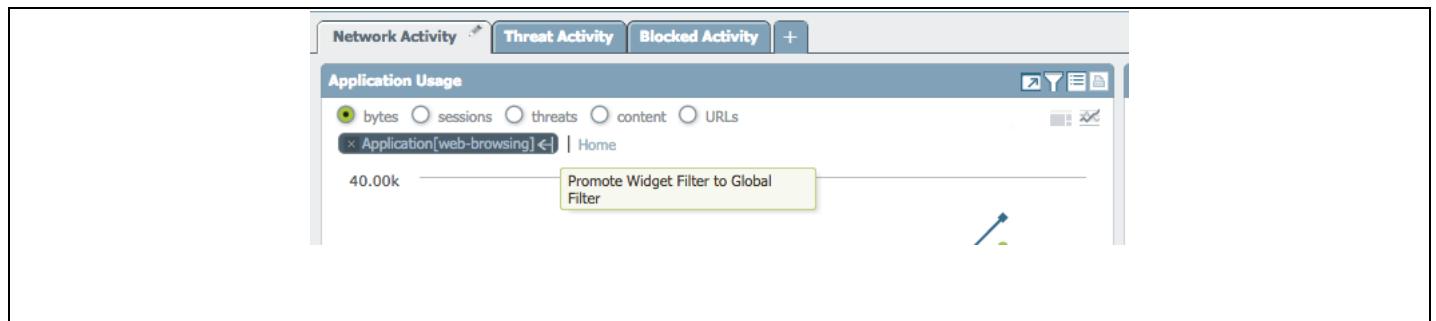


The default ACC view will show you the network, threat and blocked activity in 3 separate tabs for the past hour. As shown in the image below, the time frame and each tab can be customized to display the relevant application, threat, and user activity depending upon the user role. Additional tabs can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

Palo Alto Networks AWS CFT Deployment Guide



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

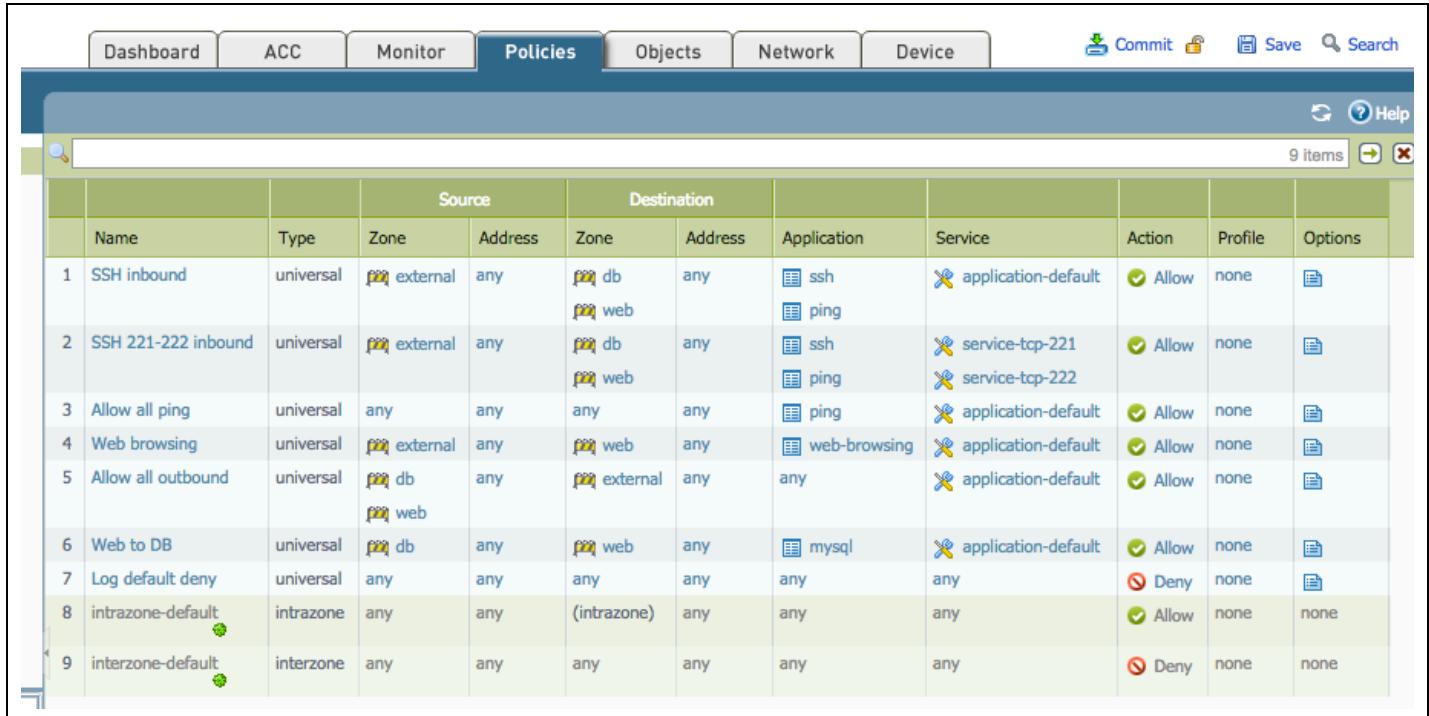


[Optional] Scroll through the information displayed in the **Network Activity** Tab. Customize one of the tabs, create/add a new tab.

Task 3 – Review PAN-OS WebUI – Security Policies

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

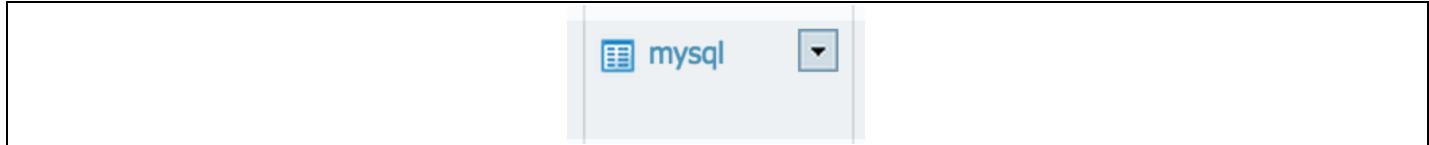
Select the **Policies** tab.



The screenshot shows the PAN-OS WebUI interface with the 'Policies' tab selected. The main area displays a table of security rules:

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

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



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

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

Palo Alto Networks AWS CFT Deployment Guide

The screenshot shows a network configuration interface with a table and a context menu.

Table Data:

any	any	db web	any	mysql	...	Allocated
any	any	any	any	any	...	Deleted
any	any	(intrazone)	any	any	...	Allocated

Context Menu (MySQL row):

- Edit...
- Filter
- Global Find
- Remove
- Value ►

Application Details (MySQL row):

Name: mysql
Description: MySQL is a multithreaded, multi-user, SQL Database Management System (DBMS) with more than six million installations
Category: business-systems
Subcategory: database
Technology: client-server
Risk: 2
Standard Ports: tcp/3306
Characteristic: Vulnerability
Widely used

Task 4 – Review PAN-OS WebUI – Monitor tab

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

Click on the Monitor tab.



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

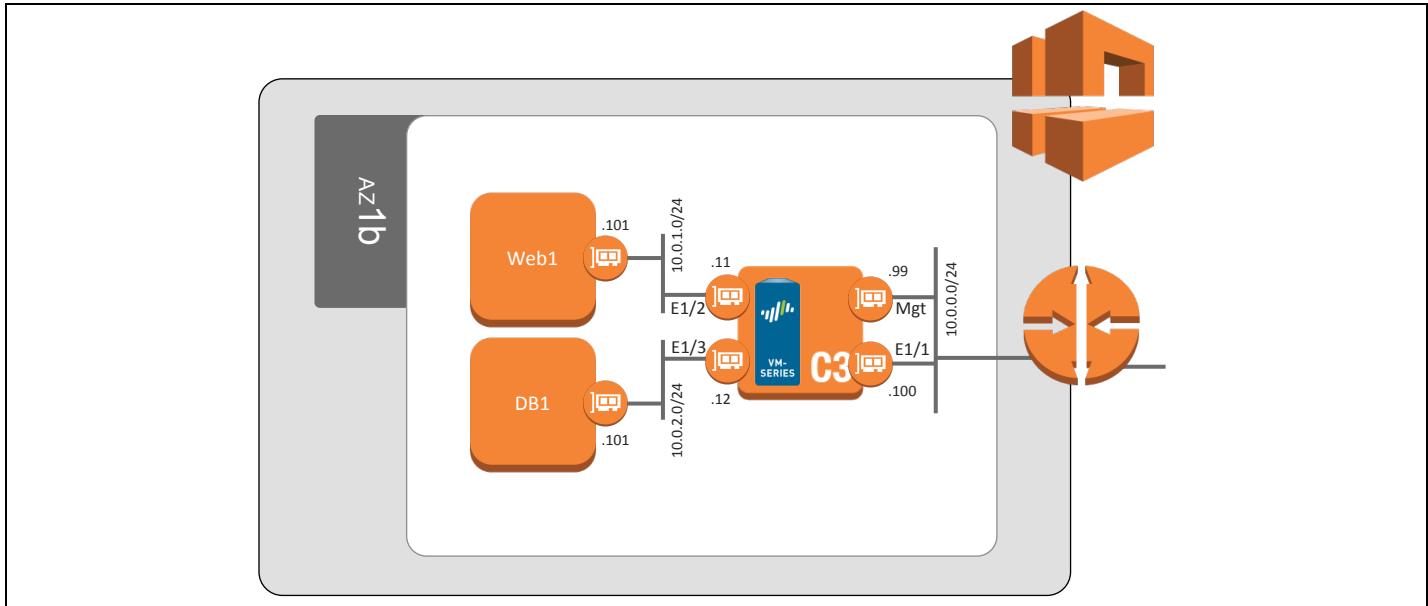
Note: Your firewall is new and doesn't have any data yet so any reports you create at this point will likely be blank. You can return to this step at the end of the lab and create new reports.

A detailed screenshot of the PAN-OS WebUI Monitor tab. The left sidebar shows a tree view of monitoring categories: Threat, Traffic, URL Filtering, Wildfire Submissions, Data Filtering, H2P Match, Configuration, System, Alarms, Packet Capture, App Scope, Summary, Change Monitor, Threat Monitor, Threat Map, Network Monitor, Traffic Map, Session Browser, Botnet, PDF Reports, Manage PDF Summary, User Activity Report, Report Groups, eMail Scheduler, Manage Custom Reports, and Reports. Three specific sections are highlighted with red boxes: "View and analyze logs" (over a log entry for a threat), "Compare activity over time" (over a log entry for a vulnerability), and "Fully customizable reporting" (over a log entry for a vulnerability). The main content area displays a table of logs with columns: Receive Time, Severity, Type, Name, Ingress I/F, From Zone, To Zone, Attacker, Attacker Name, Victim, To Port, Application, and Act... The table lists numerous log entries from May 12, 2018, at 11:20:45 to 11:29:54, detailing various threats and vulnerabilities.

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

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

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



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

Palo Alto Networks AWS CFT Deployment Guide

The image displays three screenshots of the Palo Alto Networks Management Console interface, each with a red box highlighting a specific feature:

- Create and manage all objects**: This screenshot shows the "Objects" tab, specifically the "Applications" section. It lists various application categories and their characteristics, such as "472 business-systems", "566 excessive bandwidth", and "1394 used by Malware". A red box highlights the search and filter functionality.
- Manage network connectivity**: This screenshot shows the "Network" tab, specifically the "Interfaces" section. It lists network interfaces like "Teradue1", "trust", "untrust", "trust-L3", and "untrust-L3", categorized by type (layer 2, layer 3) and technology (virtual-wire, ethernet/L4). A red box highlights the interface configuration table.
- Manage the device**: This screenshot shows the "Device" tab, specifically the "Management" section. It includes tabs for "General Settings", "Authentication Settings", "Logging and Reporting Settings", and "Management Interface Settings". A red box highlights the "General Settings" panel, which contains configuration for Panorama servers, SSL/TLS service profiles, and management interface settings.

Activity 2 – Safely Enable Applications

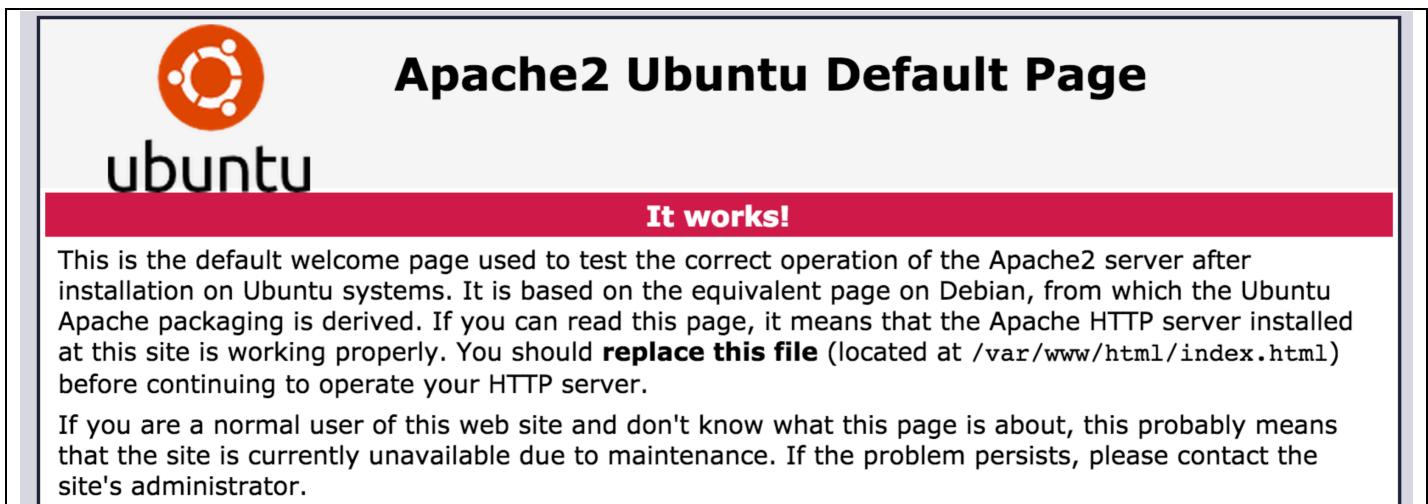
In this activity, you will:

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

Task 1 – Verify Static Content on Web Server

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

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



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

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
	05/27 20:46:27	end	external	web	199.167.52.5		10.0.0.100	80	web-browsing	allow	Web browsing	tcp-fin	5.9k
	05/27 20:46:01	start	external	web	199.167.52.5		10.0.0.100	80	web-browsing	allow	Web browsing	n/a	752

Task 2 – Verify Dynamic Content on Web Server

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

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

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

WordPress Support Forums.'"/>

Error establishing a database connection

This either means that the username and password information in your wp-config.php file is incorrect or we can't contact the database server at 10.0.2.101. This could mean your host's database server is down.

- Are you sure you have the correct username and password?
- Are you sure that you have typed the correct hostname?
- Are you sure that the database server is running?

If you're unsure what these terms mean you should probably contact your host. If you still need help you can always visit the [WordPress Support Forums](#).

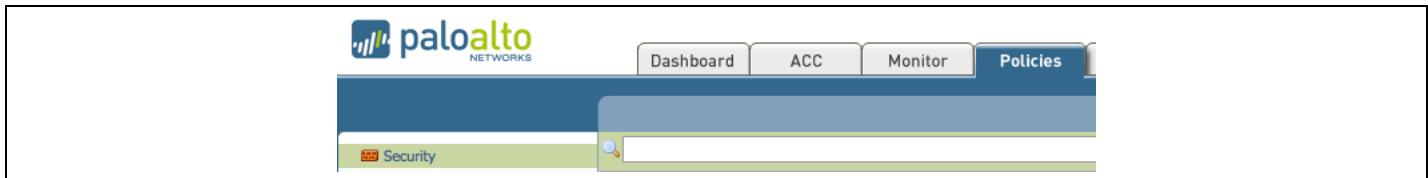
Return to the firewall **Monitor** tab and check the firewall logs to troubleshoot the problem.

Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule
05/28 10:11:18	drop	web	db	10.0.1.101	10.0.2.101	3306	not-applicable	deny	Log default deny
05/28 10:11:02	drop	web	db	10.0.1.101	10.0.2.101	3306	not-applicable	deny	Log default deny
05/28 10:10:54	drop	web	db	10.0.1.101	10.0.2.101	3306	not-applicable	deny	Log default deny
05/28 10:10:50	drop	web	db	10.0.1.101	10.0.2.101	3306	not-applicable	deny	Log default deny
05/28 10:10:48	drop	web	db	10.0.1.101	10.0.2.101	3306	not-applicable	deny	Log default deny
05/28 10:10:47	drop	web	db	10.0.1.101	10.0.2.101	3306	not-applicable	deny	Log default deny

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

Task 3 – Allow MySQL on the VM-Series Firewall

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

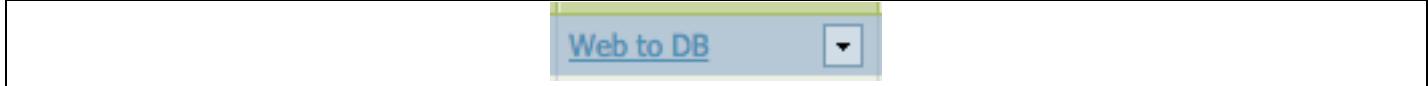


Scroll down to the **Web to DB** rule (rule 6) and note the Source and Destination zones.

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

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

Click on the **Web to DB** rule



Click on the **Source**



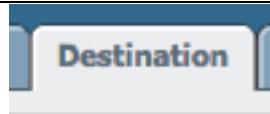
Click on **db** to bring up the pull down menu and change the selection to **web**



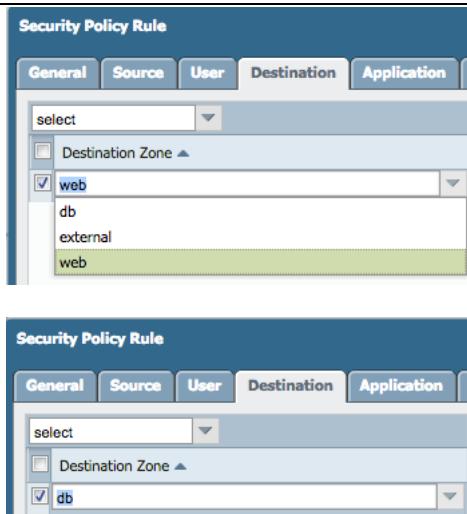
Palo Alto Networks AWS CFT Deployment Guide



Click on Destination



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



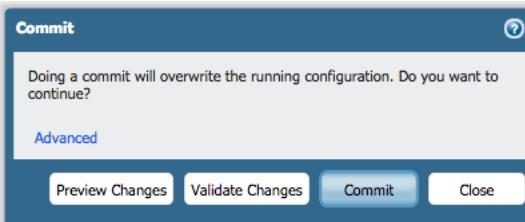
Verify your security rule now resembles the snapshot below. This rule should allow traffic *from* the web zone to the db zone.

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

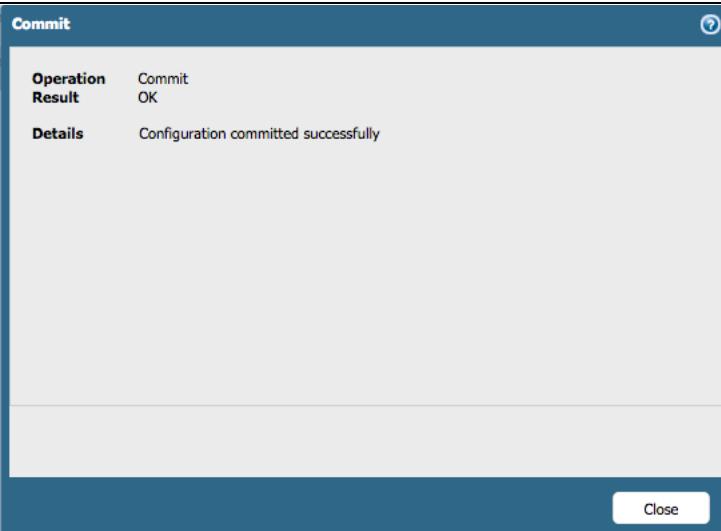
Click on **Commit** in the upper right.



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

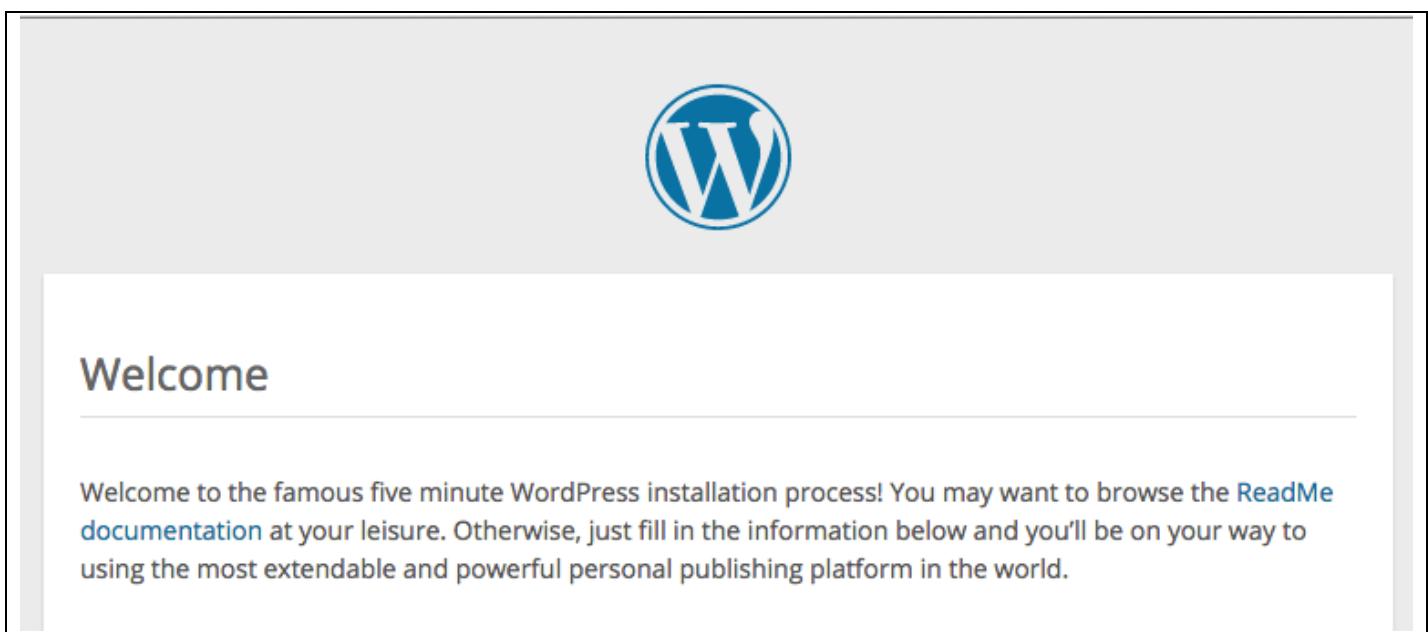


Verify the commit was successful and then click **Close**.



Task 4 – Re-verify Dynamic Content on Web Server

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



Palo Alto Networks AWS CFT Deployment Guide

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

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

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

End of Activity 2

Activity 3 – Safe Application Enablement

In this activity, you will:

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

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

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

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

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

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

LAUNCH WEB TO DB SSH ATTEMPT

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

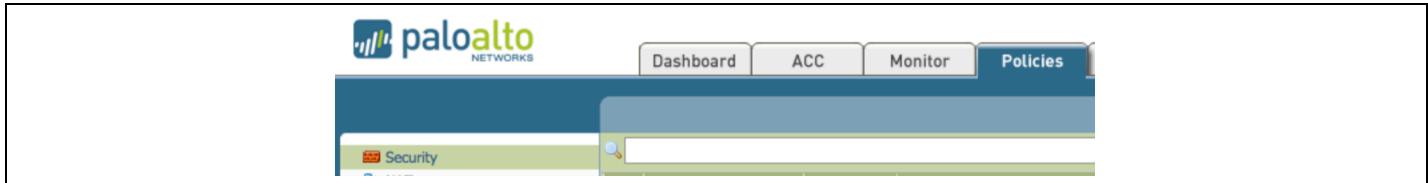
	Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule
	05/28 16:26:02	drop	web	db	10.0.1.101	10.0.2.101	22	not-applicable	deny	Log default deny
	05/28 16:25:30	drop	web	db	10.0.1.101	10.0.2.101	22	not-applicable	deny	Log default deny

Task 2 – Review the threat protection profile

In this task, we will look at the Vulnerability Protection profile. This profile is used to prevent exploits of vulnerabilities – in the case MySQL. There are many other components of Palo Alto Networks threat protection that are beyond the scope of this lab and are not included in the firewall configuration.

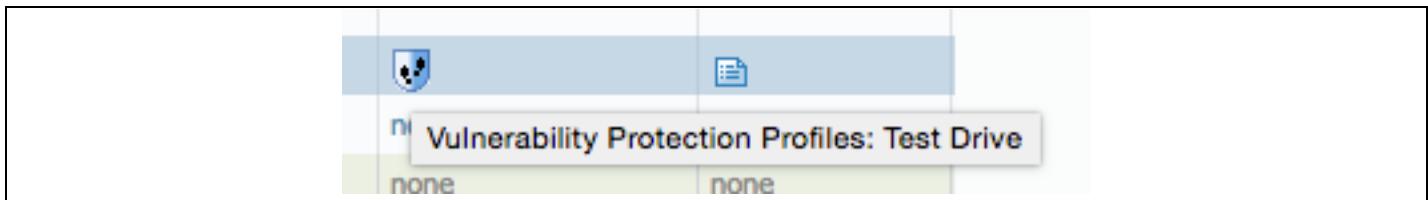
Palo Alto Networks AWS CFT Deployment Guide

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

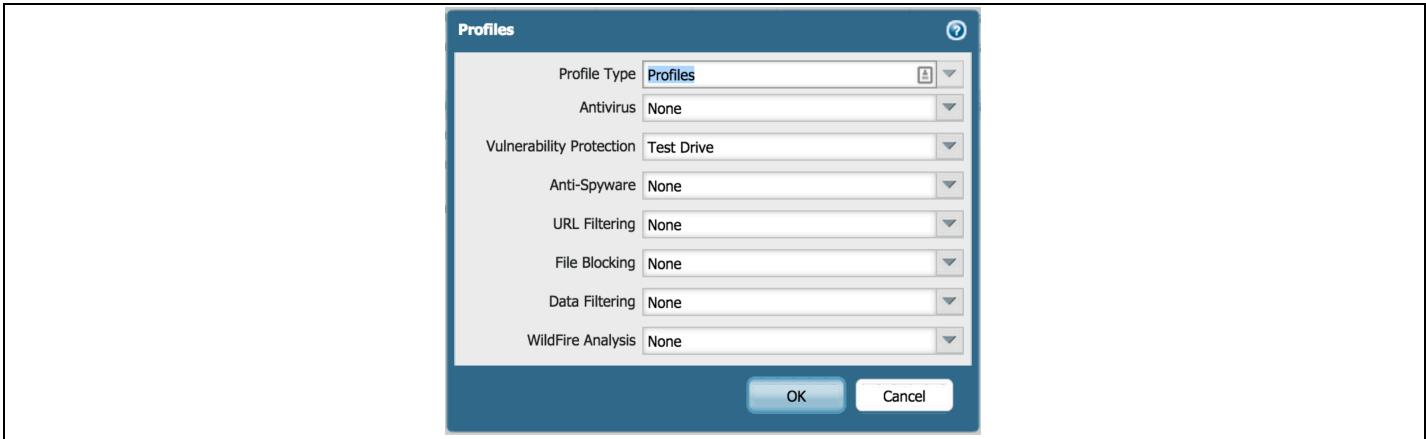


For the **Web to DB** rule, hover over the icon in the **Profile** column and note the **Test Drive** vulnerability profile in use.

Name	Tags	Type	Source				Destination				Service	Action	Profile	Options
			Zone	Address	User	HIP Profile	Zone	Address	Application					
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	Allow	none		
3 Allow all ping	none	universal	any	any	any	any	any	any	ping	service-tcp-222	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	Test Drive		
7 Log default deny	none	universal	any	any	any	any	any	any	any	any	Deny	none		
8 intrazone-default	none	intrazone	any	any	any	(intrazone)	any	any	any	any	Allow	none	none	
9 interzone-default	none	interzone	any	any	any	any	any	any	any	any	Deny	none	none	



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



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



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

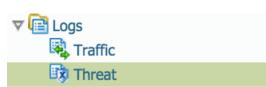
For this task, you will launch some scripted attacks on the SQL server and use the pre-configured threat protection to show and block those attacks on the VM-Series firewall. As noted above, these are simple, scripted attacks and blocking configurations – there are many other threat protection features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

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

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

LAUNCH BRUTE FORCE SQL ROOT PASSWORD GUESSING

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



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

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

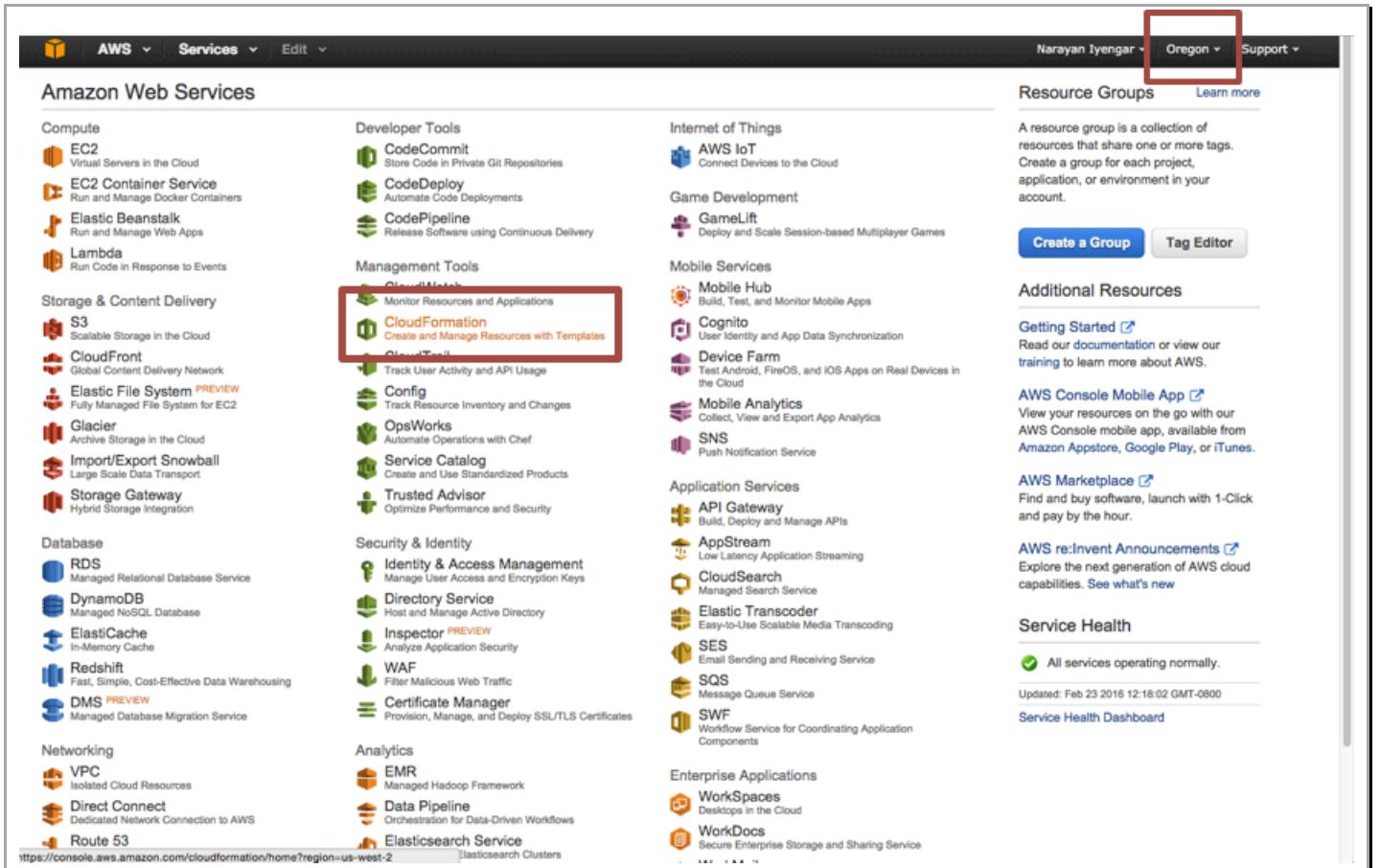
Note: The CGI script you launched in Step 2 attempted to login to the MySQL database multiple times with an incorrect password. The VM-Series firewall saw this activity and using the vulnerability profile, reset the connection and logged the activity.

End of Activity 3

9. Cleanup

9.1 Delete the Stack

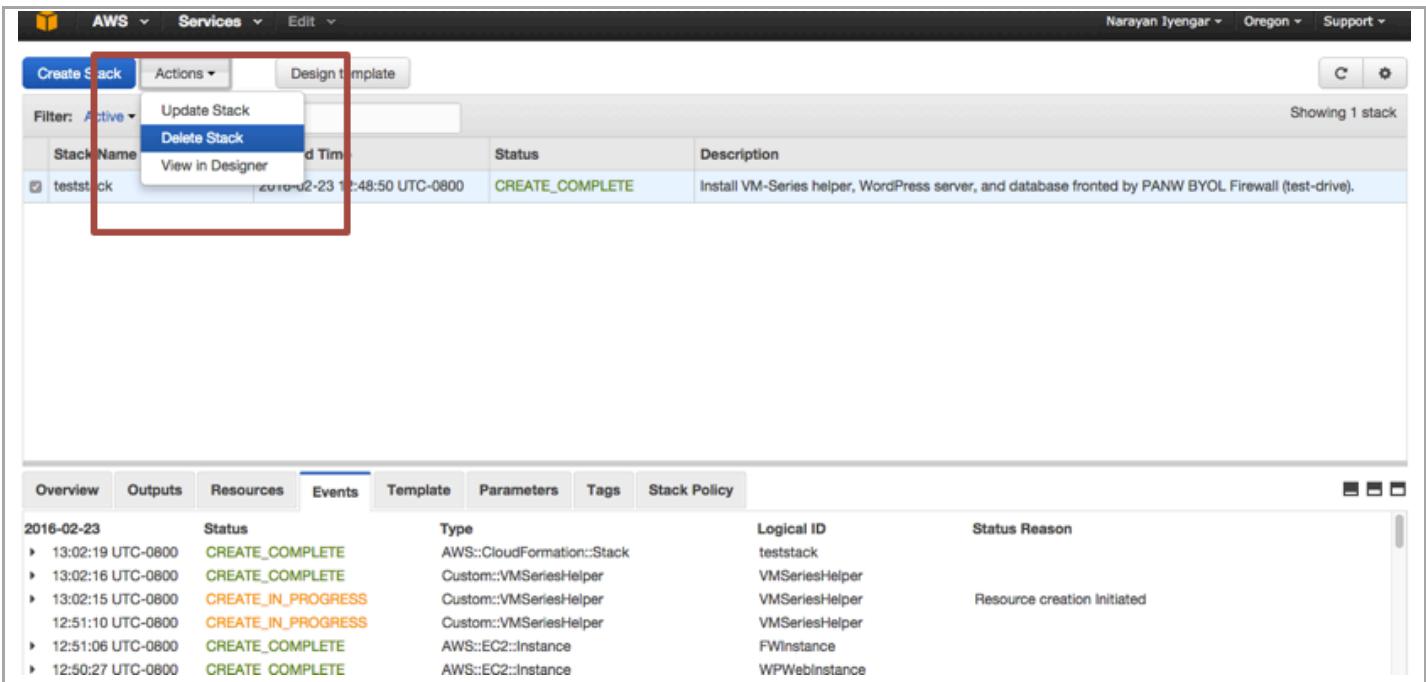
Once done with the template, feel free to play around with various things. If done, cleanup as follows. In the AWS management console, click on **CloudFormation**:



The screenshot shows the AWS Management Console interface. The top navigation bar includes 'AWS', 'Services' (with a dropdown), 'Edit', and user information ('Narayan Iyengar - Oregon - Support'). A red box highlights the 'Oregon' region selection. Below the navigation is a 'Resource Groups' section with a 'Create a Group' button and a 'Tag Editor' button. To the right is an 'Additional Resources' section with links for 'Getting Started', 'AWS Console Mobile App', 'AWS Marketplace', 'AWS re:Invent Announcements', and 'Service Health'. The main content area is titled 'Amazon Web Services' and lists various services under categories: Compute, Storage & Content Delivery, Database, Networking, Developer Tools, Game Development, Internet of Things, Mobile Services, Application Services, Security & Identity, Analytics, and Enterprise Applications. The 'CloudFormation' service is highlighted with a red box. At the bottom left is the URL 'https://console.aws.amazon.com/cloudformation/home?region=us-west-2'.

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

Palo Alto Networks AWS CFT Deployment Guide



The screenshot shows the AWS CloudFormation console. At the top, there's a navigation bar with 'AWS Services Edit'. On the right, it shows 'Narayan Iyengar - Oregon - Support'. Below the navigation is a table with one row for a stack named 'teststack'. The 'Actions' column for this stack has a dropdown menu open, with 'Delete Stack' highlighted. The table columns are 'Stack Name', 'Last Updated Time', 'Status', and 'Description'. The status for 'teststack' is 'CREATE_COMPLETE' with a description of 'Install VM-Series helper, WordPress server, and database fronted by PANW BYOL Firewall (test-drive)'. Below the table is a tab navigation bar with 'Overview', 'Outputs', 'Resources', 'Events', 'Template', 'Parameters', 'Tags', and 'Stack Policy'. Under the 'Events' tab, there's a table showing creation events for the stack, including entries for EC2 instances and VMSeriesHelper resources.

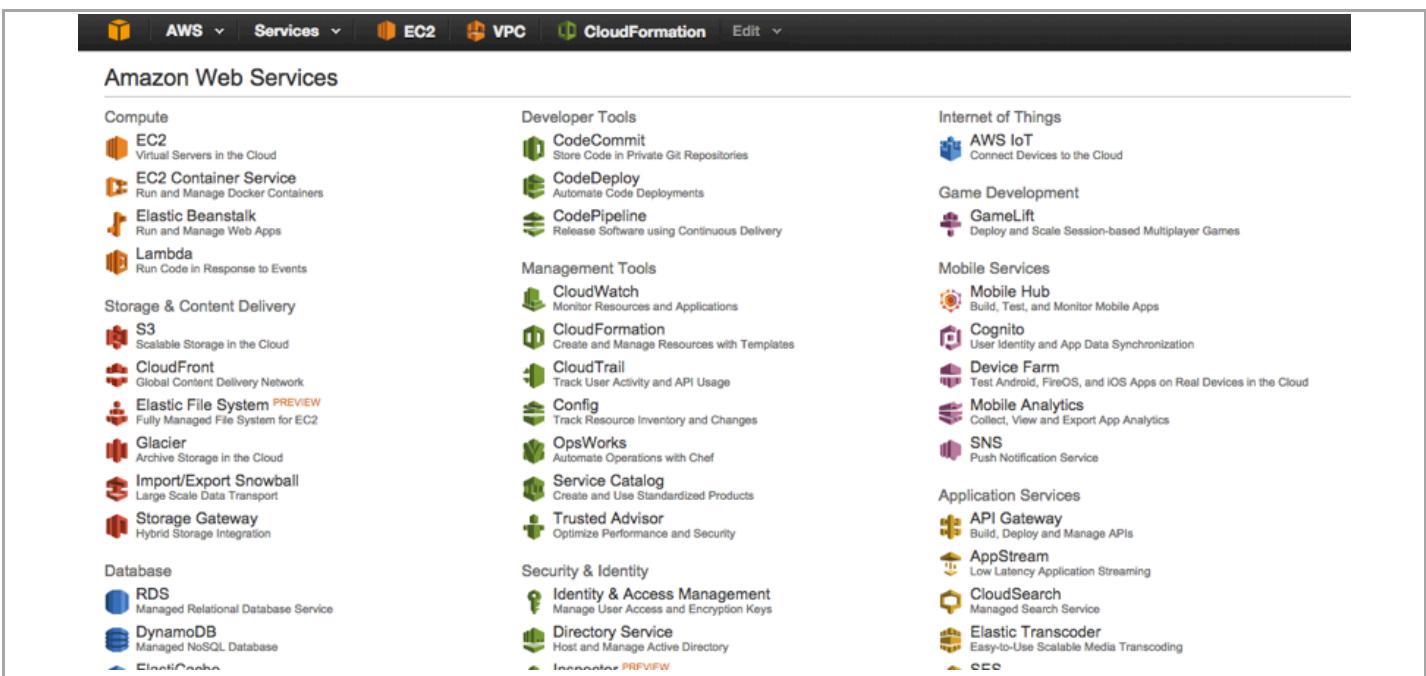
Stack Name	Last Updated Time	Status	Description
teststack	2016-02-23 12:48:50 UTC-0800	CREATE_COMPLETE	Install VM-Series helper, WordPress server, and database fronted by PANW BYOL Firewall (test-drive).

Event Time	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	

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

9.2 Delete keys

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



The screenshot shows the AWS Management Console homepage. At the top, there's a navigation bar with 'AWS Services Edit'. Below the navigation is a section titled 'Amazon Web Services' with a grid of service icons and names. The services are categorized as follows:

- Compute**: EC2 (Virtual Servers in the Cloud), EC2 Container Service (Run and Manage Docker Containers), Elastic Beanstalk (Run and Manage Web Apps), Lambda (Run Code in Response to Events).
- Storage & Content Delivery**: S3 (Scalable Storage in the Cloud), CloudFront (Global Content Delivery Network), Elastic File System (Fully Managed File System for EC2), Glacier (Archive Storage in the Cloud), Import/Export Snowball (Large Scale Data Transport), Storage Gateway (Hybrid Storage Integration).
- Database**: RDS (Managed Relational Database Service), DynamoDB (Managed NoSQL Database), ElastiCache.
- Developer Tools**: CodeCommit (Store Code in Private Git Repositories), CodeDeploy (Automate Code Deployments), CodePipeline (Release Software using Continuous Delivery).
- Management Tools**: CloudWatch (Monitor Resources and Applications), CloudFormation (Create and Manage Resources with Templates), CloudTrail (Track User Activity and API Usage), Config (Track Resource Inventory and Changes), OpsWorks (Automate Operations with Chef), Service Catalog (Create and Use Standardized Products), Trusted Advisor (Optimize Performance and Security).
- Security & Identity**: Identity & Access Management (Manage User Access and Encryption Keys), Directory Service (Host and Manage Active Directory), Inspector (PRIVACY).
- Internet of Things**: AWS IoT (Connect Devices to the Cloud).
- Game Development**: GameLift (Deploy and Scale Session-based Multiplayer Games).
- Mobile Services**: Mobile Hub (Build, Test, and Monitor Mobile Apps), Cognito (User Identity and App Data Synchronization), Device Farm (Test Android, FireOS, and iOS Apps on Real Devices in the Cloud), Mobile Analytics (Collect, View and Export App Analytics), SNS (Push Notification Service).
- Application Services**: API Gateway (Build, Deploy and Manage APIs), AppStream (Low Latency Application Streaming), CloudSearch (Managed Search Service), Elastic Transcoder (Easy-to-Use Scalable Media Transcoding), SES (Simple Email Service).

Palo Alto Networks AWS CFT Deployment Guide

Click on **Key Pairs**:

The screenshot shows the AWS EC2 Dashboard. On the left sidebar, under the 'INSTANCES' section, 'Key Pairs' is listed. In the main content area, there is a summary of resources: 0 Running Instances, 0 Dedicated Hosts, 17 Volumes, 11 Key Pairs, and 0 Placement Groups. Below this, there is a 'Create Instance' section with a 'Launch Instance' button.

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

The screenshot shows the 'Key Pairs' page in the AWS EC2 service. Three key pairs are listed: 'VMSH-test123', 'VMSH-foobar', and 'VMSH-blah'. The 'Delete' button is highlighted with a red box.

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

The screenshot shows a confirmation dialog titled 'Delete Key Pair'. It asks 'Are you sure you want to delete these key pairs?' and lists the three selected key pairs: 'VMSH-blah', 'VMSH-foobar', and 'VMSH-test123'. At the bottom right are 'Cancel' and 'Yes' buttons, with 'Yes' being highlighted.

10. Conclusion

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

Appendix A

Troubleshooting tips

1. Stack creation fails

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

Overview	Outputs	Resources	Events	Template	Parameters	Tags	Stack Policy	Change Sets
2016-09-12	Status			Type	Logical ID		Status reason	
▶ 13:32:37 UTC-0700	DELETE_IN_PROGRESS	AWS::CloudFormation::Stack		test	test		User Initiated	
▶ 13:32:23 UTC-0700	ROLLBACK_IN_PROGRESS	AWS::CloudFormation::Stack					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			ac10760d042			
▶ 09:09:02 UTC-0600	CREATE_IN_PROGRESS	AWS::EC2::VPCDHCPOptionsAssociation			dchpassoc1		Resource creation initiated	
▶ 09:09:02 UTC-0600	CREATE_IN_PROGRESS	AWS::EC2::RouteTable			rb059a2460		Resource creation initiated	
09:09:02 UTC-0600	CREATE_FAILED	AWS::EC2::EIP					The maximum number of addresses has been reached.	
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_IN_PROGRESS	AWS::EC2::RouteTable			rb049a2461		Resource creation initiated	
▶ 09:09:01 UTC-0600	CREATE_IN_PROGRESS	AWS::EC2::NetworkAcl			ac1b765d6d2		Resource creation initiated	
09:09:01 UTC-0600	CREATE_IN_PROGRESS	AWS::EC2::VPCDHCPOptionsAssociation			dchpassoc1			
09:09:01 UTC-0600	CREATE_IN_PROGRESS	AWS::EC2::RouteTable			rb059a2460			

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.