

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.

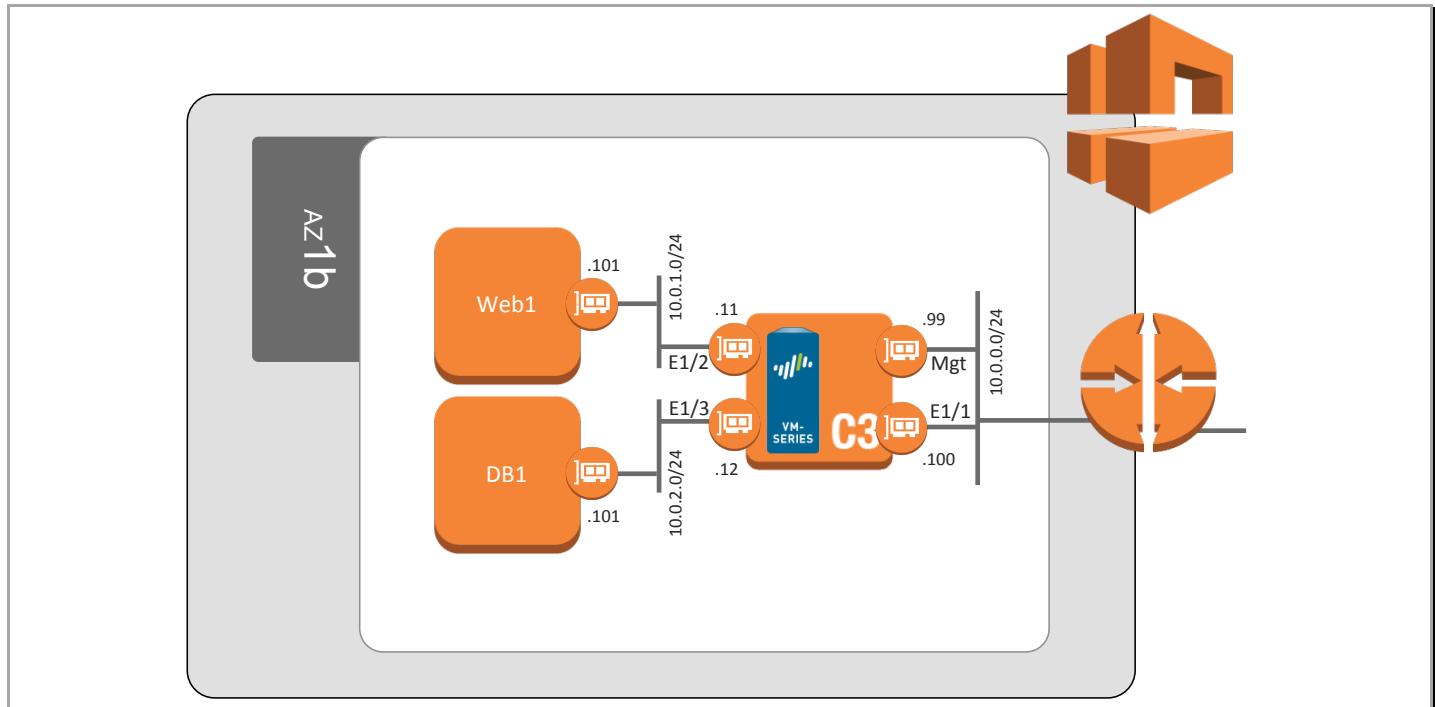
For more information on CFTs and sample CFTs refer to Amazon's documentation

<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' tab selected. The 'Amazon Web Services' section is expanded, displaying various services under categories like Compute, Storage & Content Delivery, Database, Networking, Developer Tools, Management Tools, Security & Identity, Analytics, and Application Services. On the right side, there is a 'Resource Groups' section with a 'Create a Group' button and a 'Tag Editor' button. Below that is an 'Additional Resources' section with links to 'Getting Started', 'AWS Console Mobile App', 'AWS Marketplace' (which is highlighted with a red box), and 'AWS re:Invent Announcements'. At the bottom right, there is a 'Service Health' section with a green checkmark and the text 'All services operating normally.' The URL in the address bar is <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 firewall", and "palo alto alot". To the right of the search bar, there are buttons for "GO" and "Y". At the bottom of the search results page, there is a promotional banner for "CLOUD PROTEC HYBRID CLOUD BACKUP AND DR" with a "FREE 30 DAY TRIAL" button. On the left side, a sidebar titled "Shop All Categories" lists various software categories: Desktop Apps, Software Infrastructure, Application Development, Application Servers, Application Stacks, Big Data, Databases & Caching, Network Infrastructure, Operating Systems, Security, and Developer Tools.

Select VM-Series Next Generation Firewall Bundle 2

The screenshot shows a product listing for the "VM-Series Next-Generation Firewall Bundle 2" from Palo Alto Networks. The listing includes the following details:
- **Image:** A logo for "paloaltonetworks" with the text "Free Trial" below it.
- **Title:** "VM-Series Next-Generation Firewall Bundle 2"
- **Rating:** ★★★★ (1) | Version PAN-OS 7.0.1 | Sold by [Palo Alto Networks](#)
- **Price:** \$1.28/hr or \$4,500/yr (60% savings) for software + AWS usage fees
- **Description:** 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, ...
- **Notes:** Linux/Unix, Other PAN-OS 7.0.1 | 64-bit Amazon Machine Image (AMI)

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 to 'Amazon Web Services Home', 'Your Account | Help | Sell on AWS Marketplace', and a search bar. Below the header, the product 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 visible. A promotional message about a '15 Day Free Trial Available' is present, followed by a link to 'Read more'. On the left side, there's a vertical list of product details: Customer Rating (4 stars), 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)), Support (See details below), AWS Services Required (Amazon EC2, Amazon EBS), and Highlights (Bundle 2 includes everything you need to protect your AWS environment). On the right side, there's a 'Continue' button highlighted with a red box, and a note stating 'You will have an opportunity to review your order before launching or being charged.' Below the 'Continue' button is a 'Pricing Details' section with a dropdown menu set to 'US West (Oregon)'. Under 'Hourly Fees', it says 'Total hourly fees will vary by instance type and EC2 region.' and 'Fees: Hourly' with a toggle switch set to 'Hourly'. It also mentions 'Software annual pricing savings over hourly: 60%'.

Click Continue.

The screenshot shows the AWS Marketplace interface. 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 displays a product listing for 'VM-Series Next-Generation Firewall Bundle 2'. It features two launch options: '1-Click Launch' and 'Manual Launch'. The 'Manual Launch' option is highlighted with a red border. Below these options is a note: 'Click "Accept Software Terms" to gain access to this software'. A detailed description follows: 'Once you accept these terms, you will have access to this software in any supported region. You can then launch the AMIs listed below directly from the EC2 console, EC2 APIs, or with other AWS management tools.' A 'Software Pricing' section is shown, with 'Hourly' selected as the subscription term. The 'Applicable Instance Type' section indicates a 'Software fee' that 'Varies' and depends on instance type, referencing a pricing chart. A blue 'Usage Instructions' button is located at the bottom of this section. To the right, a 'Price for your selections:' box contains a note: 'Price will be dependent on usage' and a large yellow 'Accept Software Terms' button. A detailed legal note is provided: 'You will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's End User License Agreement (EULA) [link] and your use of AWS services is subject to the AWS Customer Agreement [link]'. Below this is a 'Pricing Details' section with a 'For region' dropdown set to 'US West (Oregon)'. A note states 'Your Free Trial has expired'. Under 'Hourly Fees', it says 'Total hourly fees will vary by instance type and EC2 region.' A table at the bottom shows EC2 Instance Type, Software, EC2, and Total columns.

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

You should see this screen:

This screenshot shows a confirmation message: 'Thank you! Your subscription will be completed in a few moments.' Above this message is a green box containing a 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.'

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.

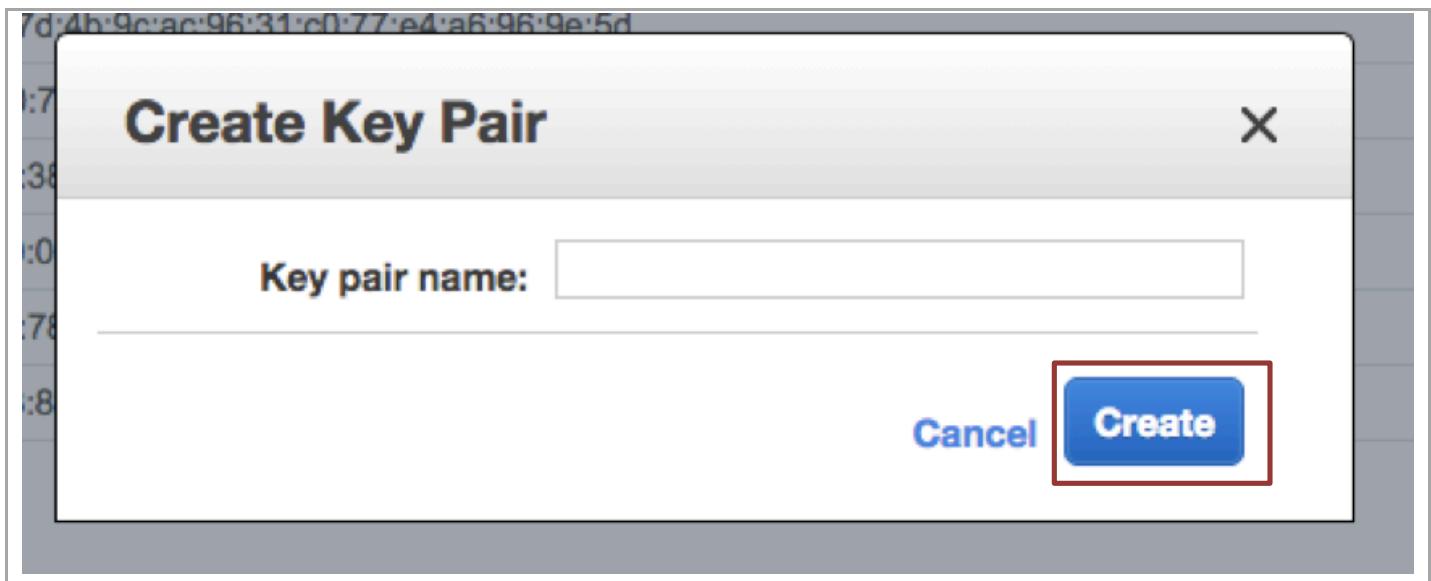
Click KeyPairs

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

Click Create Key Pair

The screenshot shows the Key Pairs list page. The 'Create Key Pair' button at the top left 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 Services page. The top navigation bar includes links for AWS, Services, EC2, VPC, CloudFormation, and Edit. Below the navigation is a section titled "Amazon Web Services" with several categories:

- 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, highlighted with a red box), 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).
- 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).

Click **Create Bucket**:

The screenshot shows the S3 service page. The top navigation bar includes links for AWS, Services, S3, EC2, and VPC. Below the navigation is a main area with two buttons: "Create Bucket" (highlighted with a red box) and "Actions".

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

Create a Bucket - Select a Bucket Name and Region Cancel 

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

Bucket Name: [Set Up Logging >](#)

Region: ▼

[Create](#) [Cancel](#)

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

Upload Create Folder Actions ▾

All Buckets / [sample-cft-bootstrap1](#)

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

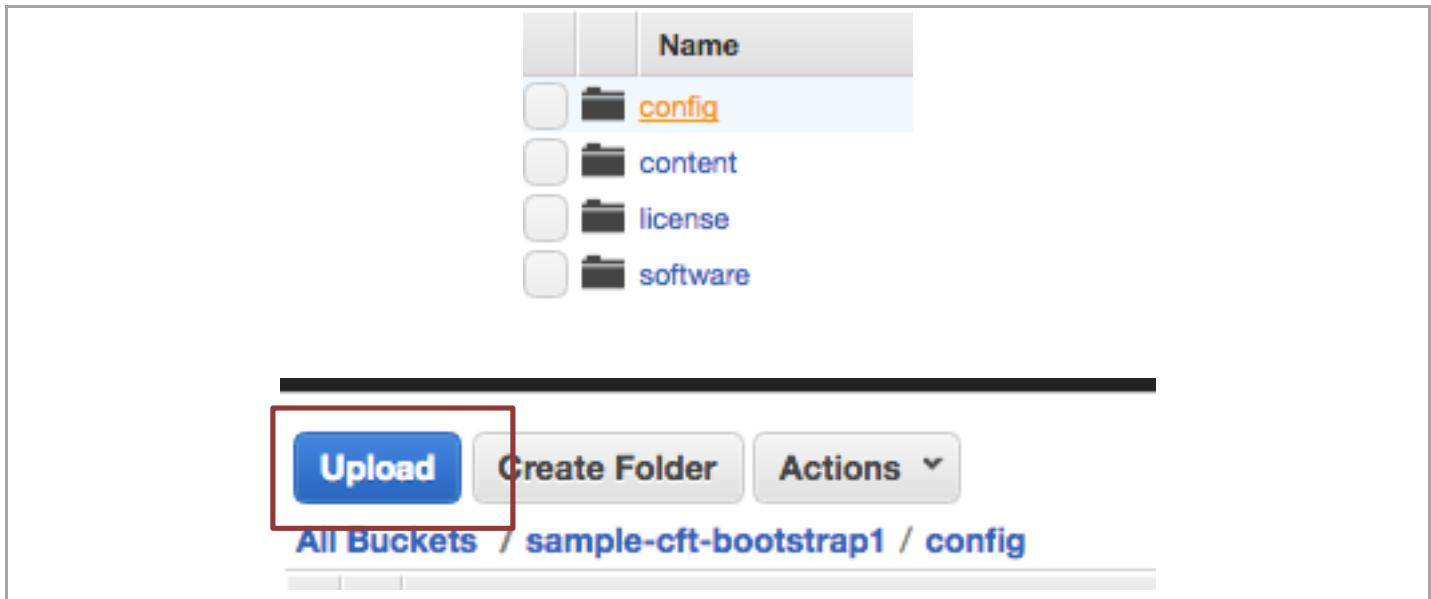
Download the following files and save them in a known location:

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

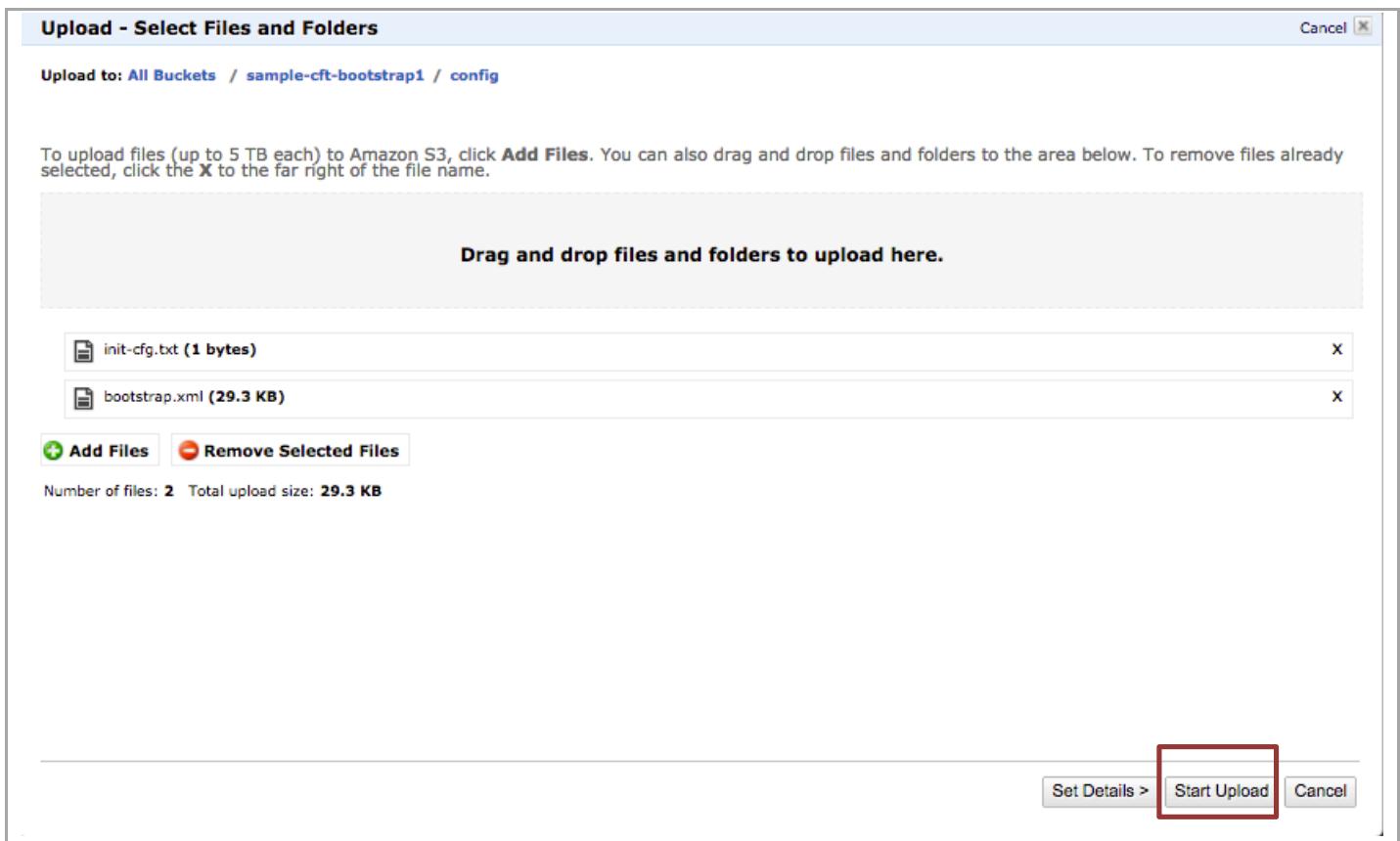
[https://raw.githubusercontent.com/PaloAltoNetworks/aws/master/two-tier sample/bootstrap/init-cfg.txt](https://raw.githubusercontent.com/PaloAltoNetworks/aws/master/two-tier%20sample/bootstrap/init-cfg.txt)

[https://github.com/PaloAltoNetworks/aws/blob/master/two-tier sample/bootstrap/panupv2-all-contents-695-4002](https://github.com/PaloAltoNetworks/aws/blob/master/two-tier%20sample/bootstrap/panupv2-all-contents-695-4002)

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

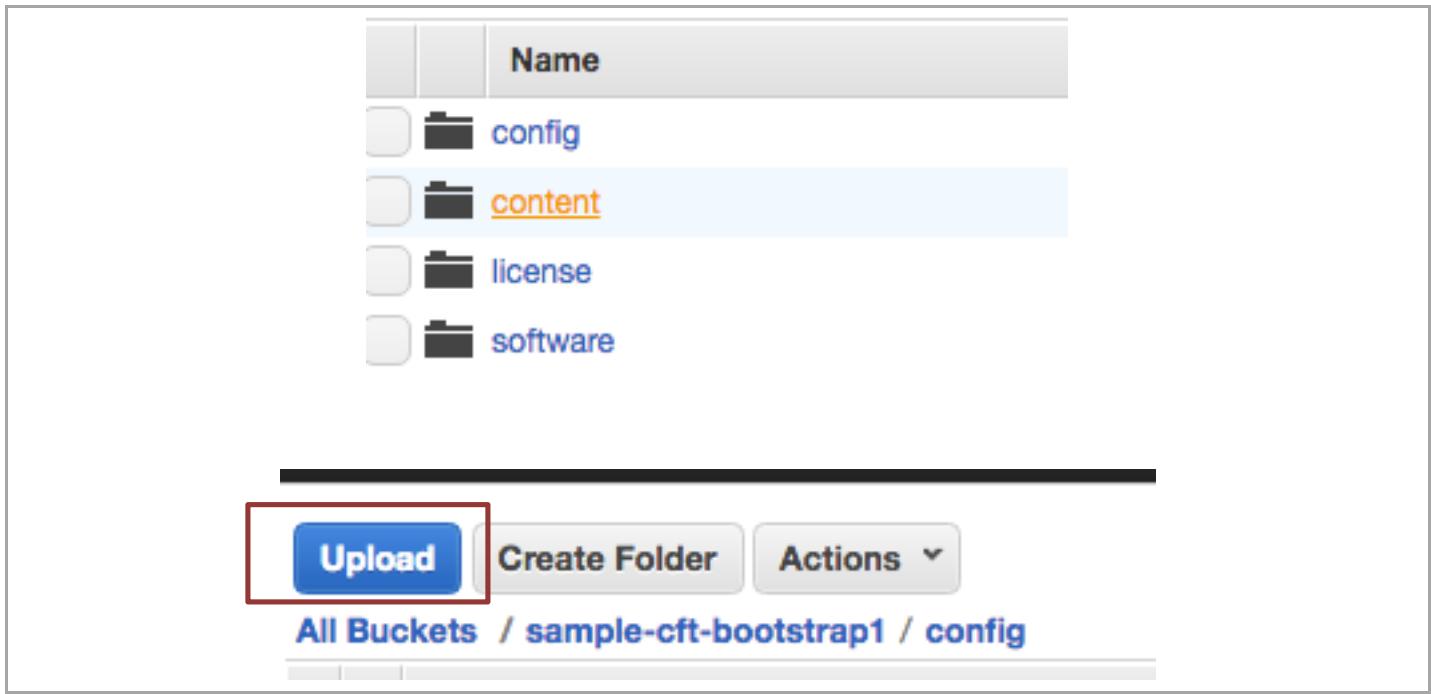


Select **Add Files** and select the two files (bootstrap.xml and init-cft.txt) downloaded previously and click **Start Upload**:



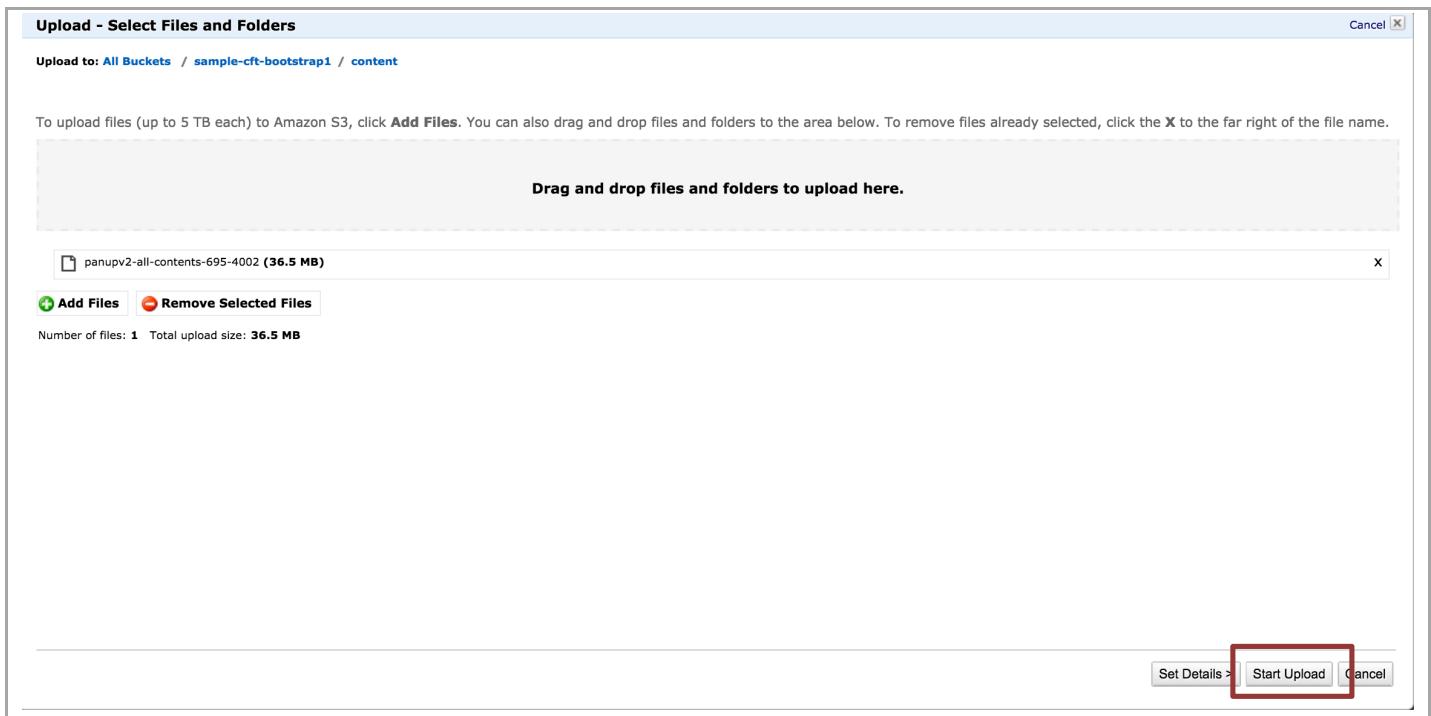
Palo Alto Networks AWS CFT Deployment Guide

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



The screenshot shows the AWS S3 console interface. On the left, there's a sidebar with a tree view of folders: 'config', 'content' (which is selected and highlighted in orange), 'license', and 'software'. Below the sidebar is a large, empty black rectangular area. At the bottom, there's a navigation bar with three buttons: 'Upload' (highlighted with a red box), 'Create Folder', and 'Actions'. Below the navigation bar, the path 'All Buckets / sample-cft-bootstrap1 / config' is displayed.

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



The screenshot shows the 'Upload - Select Files and Folders' dialog box. At the top, it says 'Upload to: All Buckets / sample-cft-bootstrap1 / content'. Below that, there's a large text area with the placeholder 'Drag and drop files and folders to upload here.' In this area, there's a single file listed: 'panupv2-all-contents-600-3449 (36.5 MB)'. At the bottom of the dialog, there are two buttons: 'Add Files' and 'Remove Selected Files'. Below these buttons, it says 'Number of files: 1 Total upload size: 36.5 MB'. At the very bottom right, there are three buttons: 'Set Details', 'Start Upload' (highlighted with a red box), and 'Cancel'.

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.

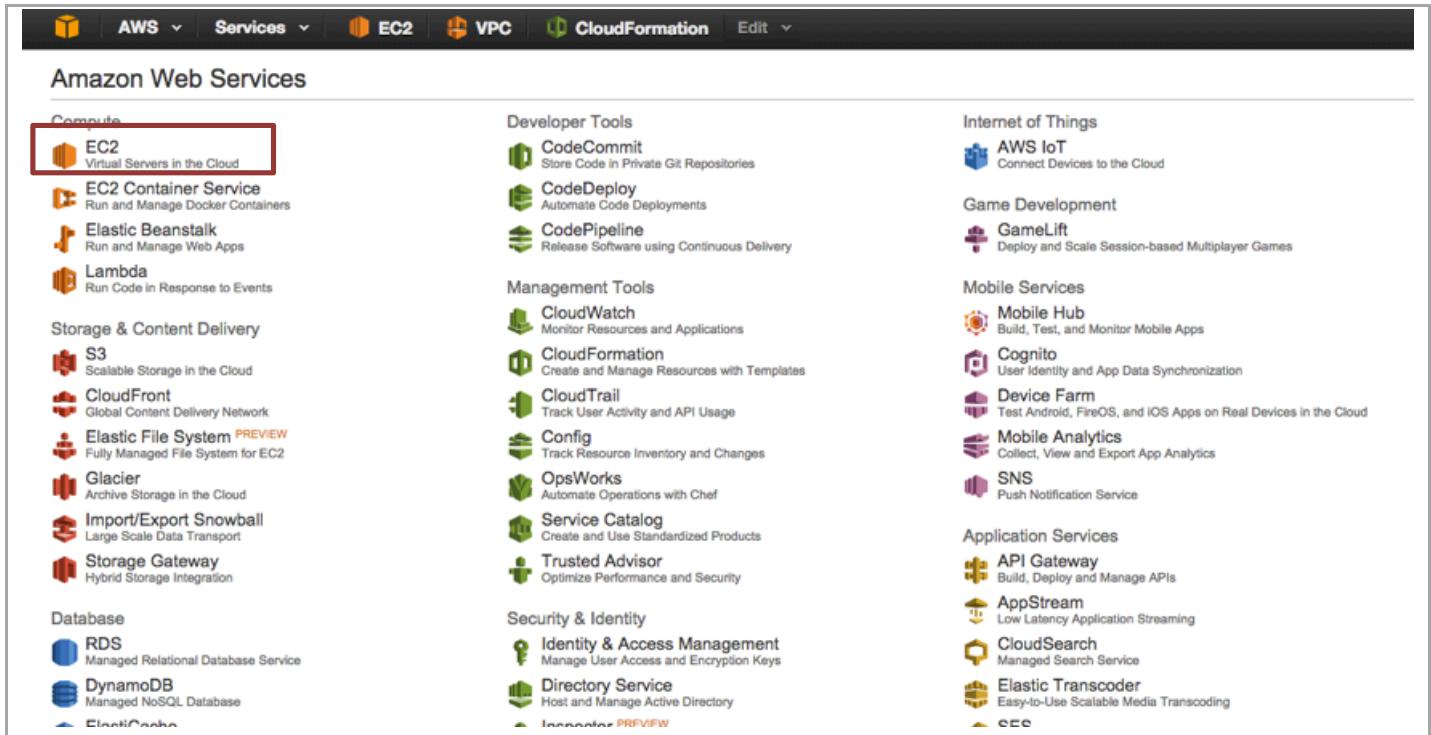
4.6 Download the Template

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**:



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 'INSTANCES' section, there is a link labeled 'Elastic IPs'. This link is highlighted with a red box. The main content area displays a table of allocated elastic IP addresses. The columns include 'Allocation ID', 'Instance', 'Private IP Address', 'Scope', and 'Public DNS'. Two entries are listed: one for instance 'eipalloc-b4f702d3' with private IP '52.10.248.59' and another for instance 'eipalloc-3fff0a58' with private IP '52.36.170.123'. The 'Actions' button at the top right of the table has a dropdown menu with options: 'Allocate New Address', 'Actions', 'Release Addresses', 'Associate Address', and 'Disassociate Address'. The 'Release Addresses' option is highlighted with a red box.

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. The left sidebar includes links for 'EC2 Dashboard', 'Events', 'Tags', 'Reports', 'Limits', 'INSTANCES' (with 'Instances', 'Spot Requests', 'Reserved Instances', 'Scheduled Instances', and 'Dedicated Hosts'), and 'IMAGES' (with 'AMIs'). The 'Elastic IPs' link is also present in the sidebar. The main area shows a table of allocated elastic IP addresses. One entry, '52.10.248.59', is selected and highlighted with a red box. The 'Actions' button has a dropdown menu with five options: 'Allocate New Address', 'Actions', 'Release Addresses' (which is highlighted with a red box), 'Associate Address', and 'Disassociate Address'. The table lists two entries: '52.10.248.59' (selected) and '52.36.170.123'.

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 menu with 'CloudFormation' selected. The page lists various AWS services under categories like Amazon Web Services, Management Tools, and Application Services. The 'CloudFormation' icon is highlighted with a red box.

Amazon Web Services

- Compute
 - EC2** Virtual Servers in the Cloud
 - EC2 Container Service** Run and Manage Docker Containers
 - Elastic Beanstalk** Run and Manage Web Apps
 - Lambda** Run Code in Response to Events
- Storage & Content Delivery
 - S3** Scalable Storage in the Cloud
 - CloudFront** Global Content Delivery Network
 - Elastic File System** PREVIEW Fully Managed File System for EC2
 - Glacier** Archive Storage in the Cloud
 - Import/Export Snowball** Large Scale Data Transport
 - Storage Gateway** Hybrid Storage Integration
- Database
 - RDS** Managed Relational Database Service
 - DynamoDB** Managed NoSQL Database
 - ElastiCache** In-Memory Cache
 - Redshift** Fast, Simple, Cost-Effective Data Warehousing
 - DMS** PREVIEW Managed Database Migration Service
- Networking
 - VPC** Isolated Cloud Resources
 - Direct Connect** Dedicated Network Connection to AWS
 - Route 53**

Management Tools

- CloudWatch** Monitor Resources and Applications
- CloudFormation** Create and Manage Resources with Templates **(highlighted)**
- CodeCommit** Store Code in Private Git Repositories
- CodeDeploy** Automate Code Deployments
- CodePipeline** Release Software using Continuous Delivery
- Config** Track Resource Inventory and Changes
- OpsWorks** Automate Operations with Chef
- Service Catalog** Creates and Use Standardized Products
- Trusted Advisor** Optimize Performance and Security

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

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

Click **Create Stack**:

The screenshot shows the AWS CloudFormation stacks page. The 'Create Stack' button is highlighted with a red box.

Actions

- Create Stack** **(highlighted)**
- Actions ▾
- Design template

Filter: Active ▾ By Name:

Select “Choose File” and select the template downloaded in [Section 4.6](#) into the box and click **Next:**

Palo Alto Networks AWS CFT Deployment Guide

The screenshot shows the 'Create stack' wizard in the AWS CloudFormation console. The 'Select Template' step is active. It provides three options: 'Design a template' (using CloudFormation Designer), 'Choose a template' (uploading a JSON template or specifying an S3 URL), and 'Specify Details' (which is currently selected). A sample template is shown as a placeholder. The 'Upload a template to Amazon S3' section is expanded, showing a file named 'pan-sample-cft-V4.json' selected. The 'Next' button at the bottom right is highlighted with a red box.

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

The screenshot shows the 'Specify Details' wizard in the AWS CloudFormation console. Under the 'Parameters' section, two fields are populated: 'BootstrapBucketName' set to 'bootstrap-bucket' and 'ServerKeyName' set to 'aws-keypair-virginia'. Both fields have descriptive placeholder text below them. The 'Next' button at the bottom right is highlighted with a red box.

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 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, adding up to 10 unique key-value pairs. A table shows one tag entry: 'Key' is 'Group' and 'Value' is 'Word Press Demo'. Below this is an 'Advanced' section where you can set notification options and a stack policy. At the bottom right are 'Cancel', 'Previous', and a blue 'Next' button, which is highlighted with a red box.

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' is <https://s3-us-west-2.amazonaws.com/sample-cft/pan-sample-cft-V1.json>, 'Description' is 'Instal VM-Series helper, WordPress server, and database fronted by PANW BYOL Firewall (sample-cft)', and 'Estimate cost' is 'Cost'. The 'Stack details' section shows 'Stack name' as 'teststack', 'FWInstancePassword' as '*****', 'ServerKeyName' as 'aws-keypair', and 'Create IAM resources' as 'No'. The 'Options' section includes 'Tags' (none provided) and 'Advanced' settings for 'Notification' (Timeout: none, Rollback on failure: Yes). The 'Capabilities' section contains a note about IAM requirements and a checkbox for acknowledging the creation of IAM resources. At the bottom right are 'Cancel', 'Previous', and a blue 'Create' button, which is highlighted with a red box.

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' status. The status cell is highlighted with a red box. The table has columns for 'Stack Name', 'Created Time', 'Status', and 'Description'. The 'Description' column states: 'Install VM-Series helper, WordPress server, and database fronted by PANW BYOL Firewall (test-drive.)'. Below the table, there are tabs for 'Overview', 'Outputs', 'Resources', 'Events' (which is selected), 'Template', 'Parameters', 'Tags', and 'Stack Policy'. Under the 'Events' tab, it shows the creation event: 'Status' is 'CREATE_IN_PROGRESS', 'Type' is 'AWS::CloudFormation::Stack', 'Logical ID' is 'teststack', and 'Status Reason' is 'User Initiated'. There are also icons for copy, refresh, and delete.

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

This screenshot shows the 'Events' tab for the 'teststack' stack. The table header includes 'Stack Name', 'Created Time', 'Status' (which is highlighted with a red box), and 'Description'. The 'teststack' row shows a status of 'CREATE_COMPLETE'. The 'Description' column states: 'Install VM-Series helper, WordPress server, and database fronted by PANW BYOL Firewall (test-drive.)'. Below this, the 'Events' tab is selected and shows a detailed list of events. The first event is 'Status' is 'CREATE_COMPLETE', 'Type' is 'AWS::CloudFormation::Stack', 'Logical ID' is 'teststack', and 'Status Reason' is 'Resource creation initiated'. This is followed by several other events for creating resources like 'VMSeriesHelper', 'FWInstance', etc., each with a status of 'CREATE_COMPLETE'. The table has columns for 'Created Time', 'Status', 'Type', 'Logical ID', and 'Status Reason'.

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 10:00:34 UTC-0800	DELETE_IN_PROGRESS	AWS::IAM::AccessKey		
2016-02-25 10:00:34 UTC-0800	ROLLBACK_IN_PROGRESS	AWS::CloudFormation::Stack		
2016-02-25 10:00:34 UTC-0800	CREATE_FAILED	AWS::EC2::Instance	FWInstance	
2016-02-25 10:00:34 UTC-0800	CREATE_COMPLETE	AWS::EC2::Instance	WPWebInstance	
2016-02-25 10:00:34 UTC-0800	CREATE_COMPLETE	AWS::EC2::Instance	WPDBServerInstance	
2016-02-25 10:00:34 UTC-0800	CREATE_IN_PROGRESS	AWS::EC2::Instance	FWInstance	
2016-02-25 10:00:34 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 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	

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 Calendaring 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, a sidebar lists various VPC-related resources: Your VPCs, Subnets, Route Tables, Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, NAT Gateways, Peering Connections, Security, Network ACLs, Security Groups, VPN Connections, Customer Gateways, Virtual Private Gateways, and VPN Connections. The "Your VPCs" section is expanded, showing 3 VPCs, 7 Subnets, 4 Network ACLs, 0 VPC Peering Connections, 0 Nat Gateways, 4 Running Instances, 0 Virtual Private Gateways, 3 Internet Gateways, 6 Route Tables, 3 Elastic IPs, 0 Endpoints, 5 Security Groups, 0 VPN Connections, and 0 Customer Gateways. A "Start VPC Wizard" button is located at the top right, and a "Launch EC2 Instances" button is also present. A note below the buttons states: "Note: Your Instances will launch in the US West (Oregon) region." A "Create VPN Connection" button is located in the bottom right corner of the main content area.

VPC Dashboard

Filter by VPC:
None

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

NAT Gateways

Peering Connections

Security

Network ACLs

Security Groups

VPN Connections

Customer Gateways

Virtual Private Gateways

VPN Connections

Resources ↗

Note: Your Instances will launch in the US West (Oregon) region.

You are using the following Amazon VPC resources in the US West (Oregon) region:

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

Start VPC Wizard Launch EC2 Instances

VPN Connections

Create VPN Connection

Palo Alto Networks AWS CFT Deployment Guide

Here is the sample VPC:

The screenshot shows the AWS VPC Dashboard. On the left sidebar, under 'Virtual Private Cloud', 'Your VPCs' is selected and highlighted with a red box. The main content area displays a table for the 'PAN Sample CFT' VPC. The table columns include Name, VPC ID, State, VPC CIDR, DHCP options set, Route table, Network ACL, Tenancy, and Default VPC. The entry shows 'PAN Sample CFT' with 'vpc-e2a95c86 (10.0.0.0/16)' as the VPC CIDR.

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

The screenshot shows the AWS Subnet Dashboard. On the left sidebar, under 'Virtual Private Cloud', 'Subnets' is selected and highlighted with a red box. The main content area displays a table for the 'PAN Sample CFT' VPC. The table columns include Name, Subnet ID, State, VPC, CIDR, Available IPs, Availability Zone, Route Table, Network ACL, and Default Subnet. Three subnets are listed: 'subnet-d9e01fb' (available), 'subnet-dee01fba' (available), and 'subnet-dde01fb9' (available).

Route tables:

The screenshot shows the AWS Route Table Dashboard. On the left sidebar, under 'Virtual Private Cloud', 'Route Tables' is selected and highlighted with a red box. The main content area displays a table for the 'PAN Sample CFT' VPC. The table columns include Name, Route Table ID, Explicitly Associated, Main, and VPC. Three route tables are listed: 'rtb-4318d127' (0 Subnets, Yes, associated with VPC), 'rtb-5d18d139' (1 Subnet, No, associated with VPC), and 'rtb-5e18d13a' (0 Subnets, No, associated with VPC).

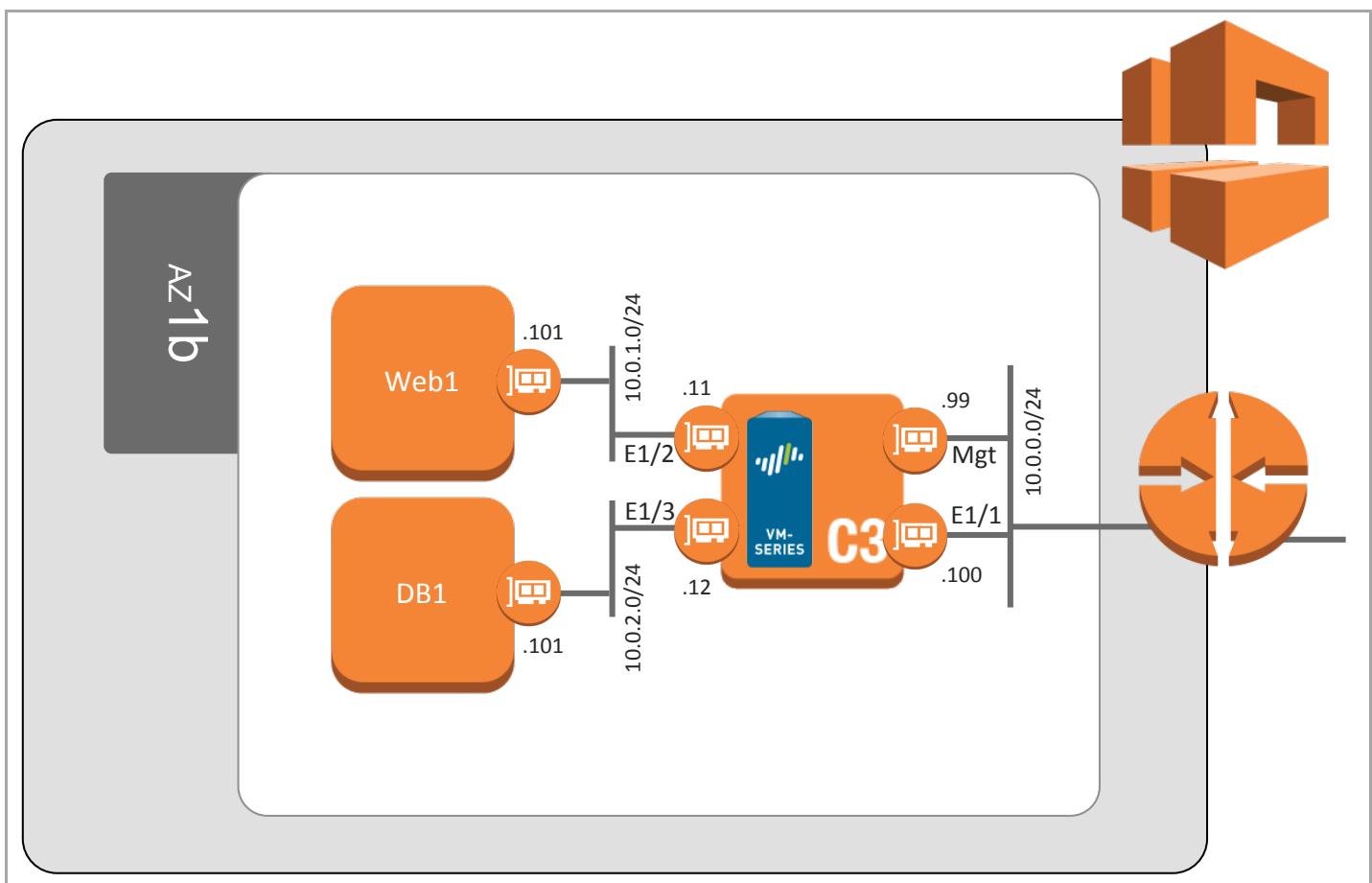
And **Elastic IPs (EIPs)**:

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, Subnets, Route Tables, Internet Gateways, DHCP Options Sets, and Elastic IPs. The 'Elastic IPs' option is highlighted with a red box. The main area displays a table of VPC addresses. Two entries are listed:

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

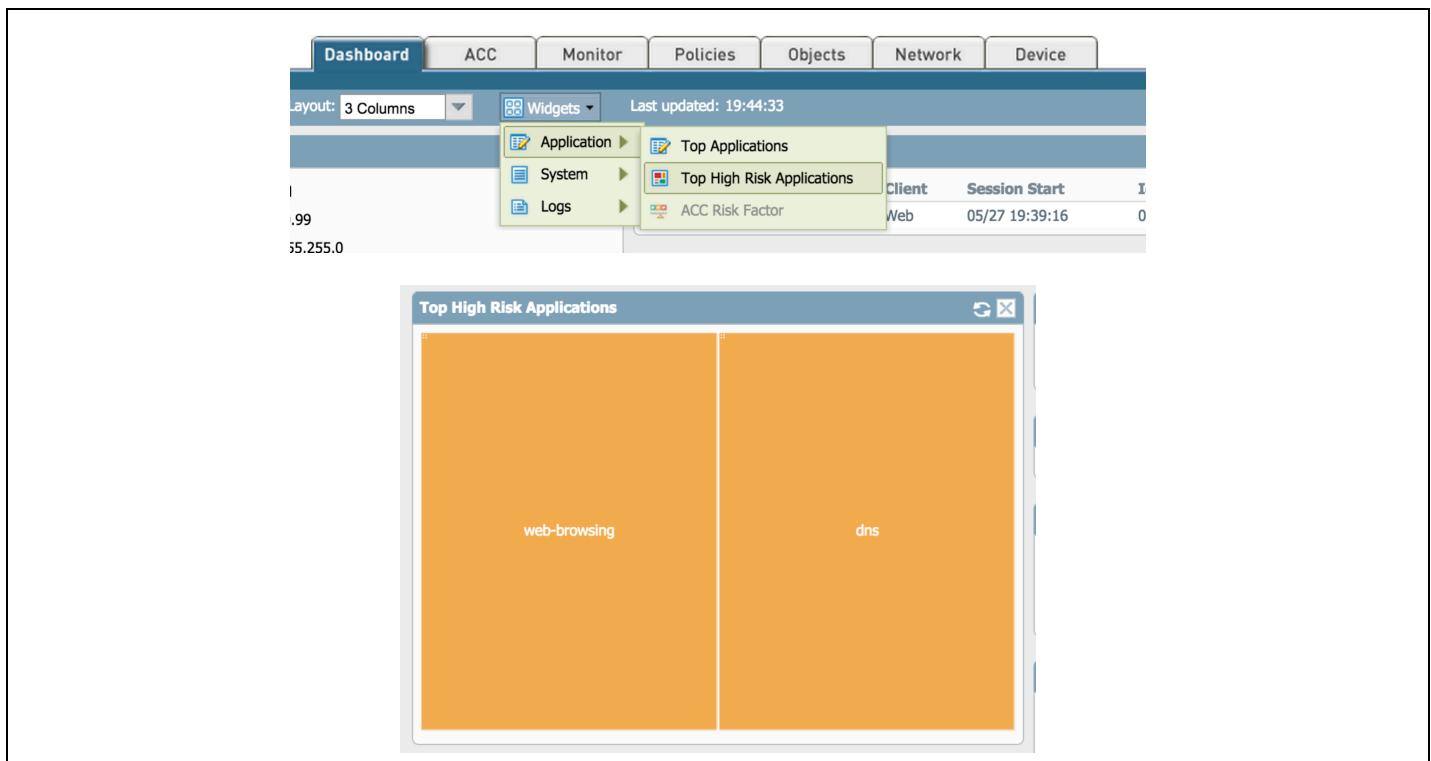


Upon login, you will see the dashboard for the VM-Series. The dashboard provides a visual summary of the device status. It is widget-based and can be customized to fulfill your specific requirements.

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. The main area is divided into several widgets: 'General Information' (listing device details like name, IP, MAC, and software version), 'Logged In Admins' (showing one admin session from 199.167.52.5), 'Config Logs' (empty), 'Locks' (empty), 'ACC Risk Factor (Last 60 minutes)' (a gauge showing 4.0), 'System Resources' (CPU and Session Count metrics), 'Data Logs' (empty), and 'System Logs' (a table of log entries with columns for Description and Time).

[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)

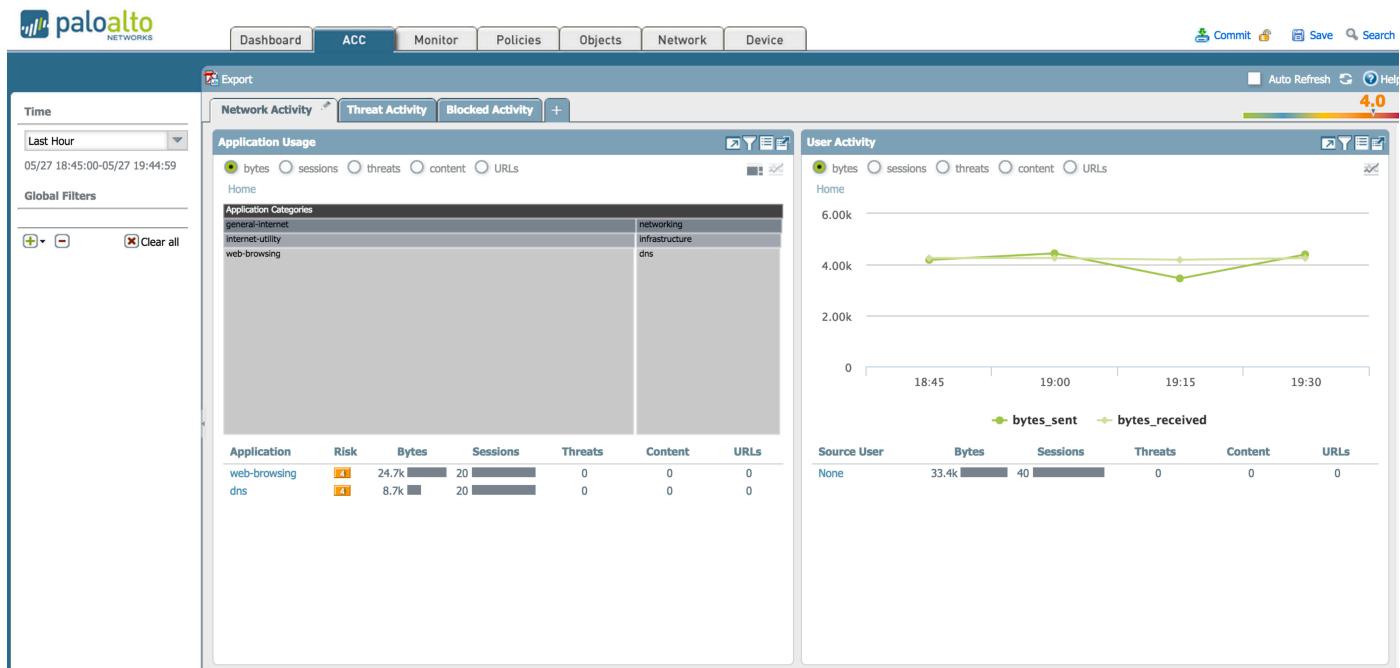
The ACC provides you with a widget-based summary of the applications, the content within, and who the user is over a given time period [default is 1 hour]. With the ACC, you can see the contextual linkage between the application and the content, which allows you to make more informed security decisions.

Select the **ACC** Tab.

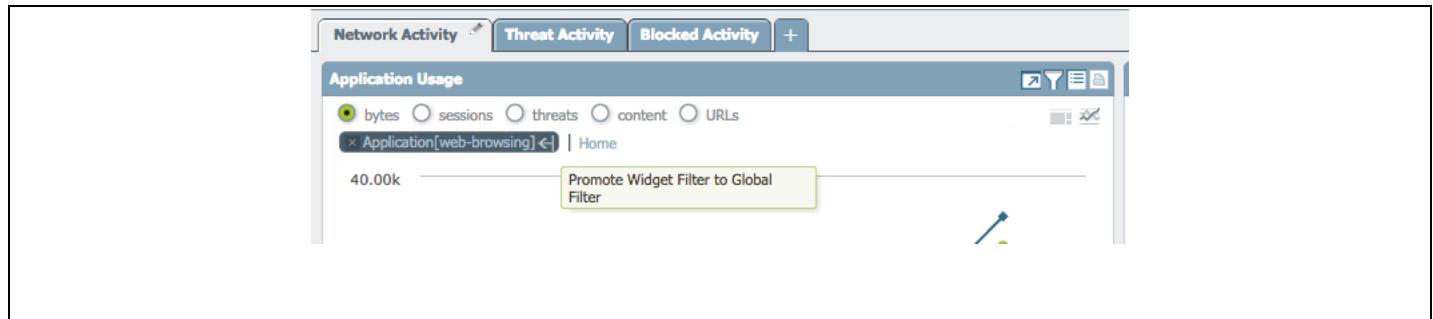


The default ACC view will show you the network, threat and blocked activity in 3 separate tabs for the past hour. As shown in the image below, the time frame and each tab can be customized to display the relevant application, threat, and user activity depending upon the user role. Additional tabs can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

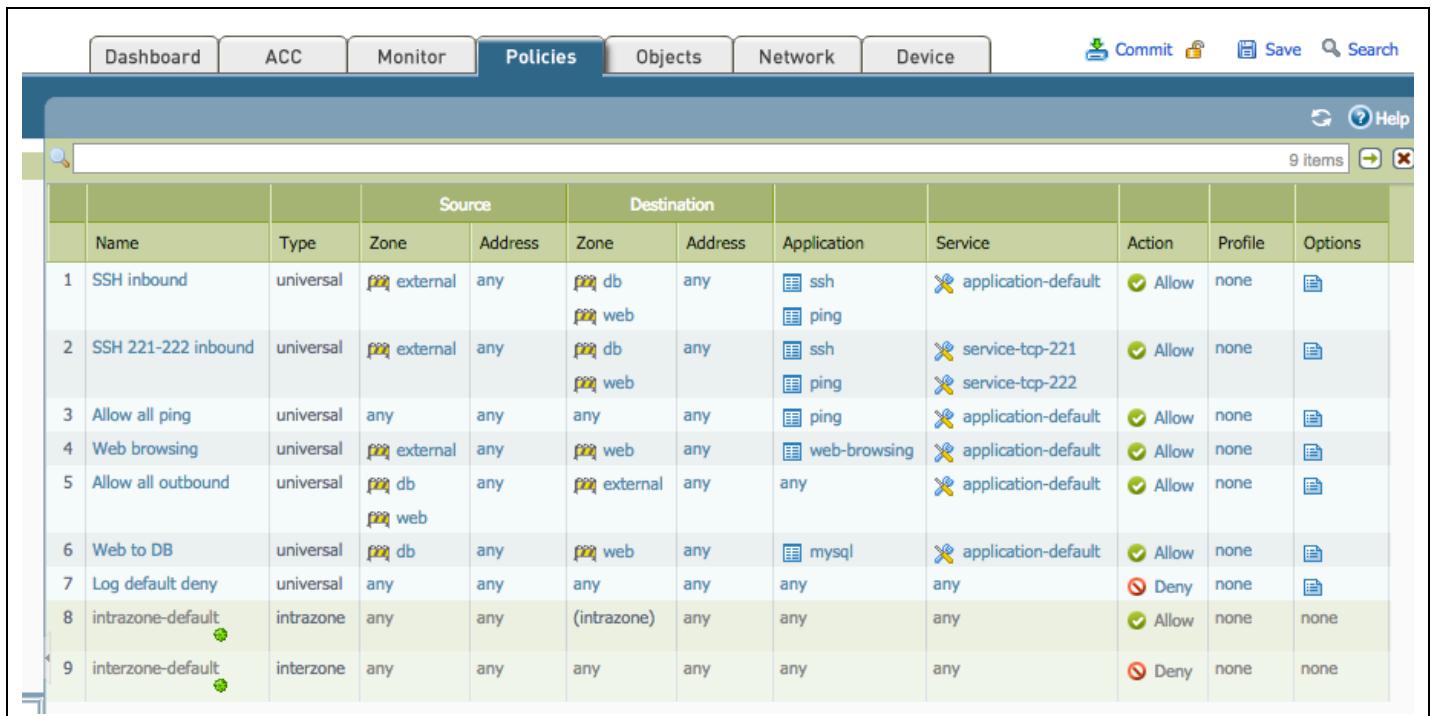


[Optional] Scroll through the information displayed in the **Network Activity** Tab. Customize one of the tabs, create/add a new tab.

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.

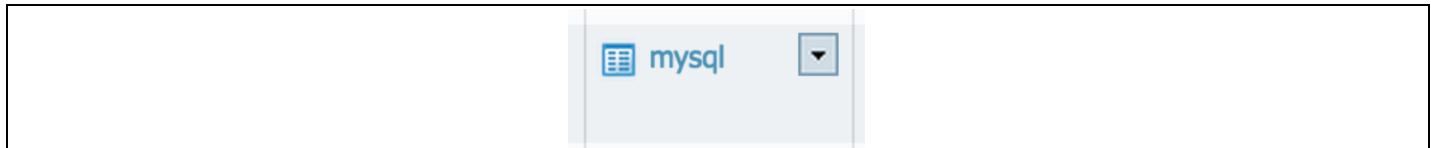
Select the **Policies** tab.



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	none
9	interzone-default	interzone	any	any	any	any	any	any	Deny	none	none

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



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

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

Palo Alto Networks AWS CFT Deployment Guide

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

Task 4 – Review PAN-OS WebUI – Monitor tab

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

Click on the Monitor tab.



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

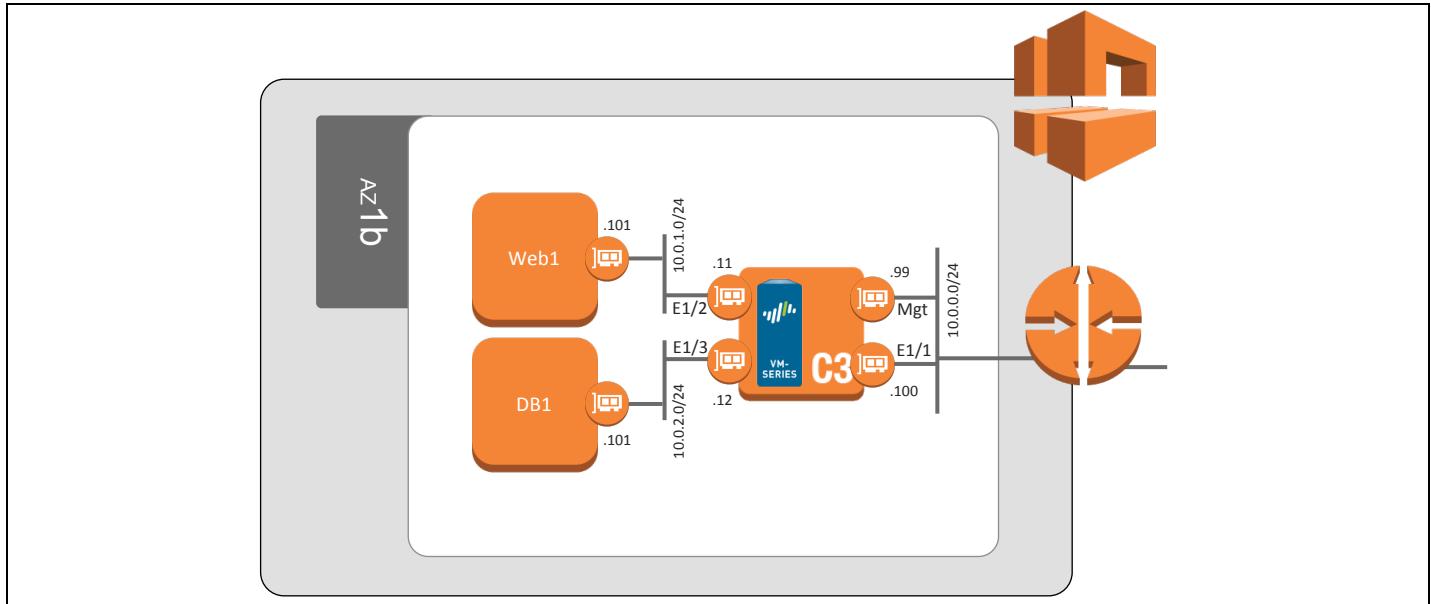
Note: Your firewall is new and doesn't have any data yet so any reports you create at this point will likely be blank. You can return to this step at the end of the lab and create new reports.

Receive Time	Severity	Type	Name	Ingress IF	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action
05/12 11:20:45	high	spyware	Trojan-Licenses.Rophom	ethern...	TAP-138	TAP-138				3208	web-browsing	ale
05/12 11:20:45	high	spyware	ZeroAccess.Gen Command and Control Traffic	ethern...	TAP-138	TAP-138				1111	unknown-udp	ale
05/12 11:20:45	high	spyware	ZeroAccess.Gen Command and Control Traffic	ethern...	TAP-138	TAP-138				1111	unknown-udp	ale
05/12 11:20:36	critical	spyware	ZeroAccess.Gen Command and Control Traffic	ethern...	TAP-138	TAP-138				1111	unknown-udp	ale
05/12 11:20:34	critical	spyware	ZeroAccess.Gen Command and Control Traffic	ethern...	TAP-138	TAP-138				1111	unknown-udp	ale
05/12 11:20:32	critical	spyware	ZeroAccess.Gen Command and Control Traffic	ethern...	TAP-138	TAP-138				1111	unknown-udp	ale
05/12 11:20:30	critical	spyware	ZeroAccess.Gen Command and Control Traffic	ethern...	TAP-138	TAP-138				1111	unknown-udp	ale
05/12 11:20:28	critical	spyware	ZeroAccess.Gen Command and Control Traffic	ethern...	TAP-138	TAP-138				21	ftp	ale
05/12 11:20:25	high	vulnerability	FTP: login Brute-force attempt	ethern...	TAP-138	TAP-138				5060	sp	ale
05/12 11:20:24	critical	spyware	ZeroAccess.Gen Command and Control Traffic	ethern...	TAP-138	TAP-138				1111	unknown-udp	ale
05/12 11:20:23	high	vulnerability	FTP: login Brute-force attempt	ethern...	TAP-138	TAP-138				21	ftp	ale
05/12 11:20:22	high	vulnerability	FTP: login Brute-force attempt	ethern...	TAP-138	TAP-138				21	ftp	ale
05/12 11:20:20	high	vulnerability	FTP: login Brute-force attempt	ethern...	TAP-138	TAP-138				1111	unknown-udp	ale
05/12 11:20:18	high	vulnerability	FTP: login Brute-force attempt	ethern...	TAP-138	TAP-138				21	ftp	ale
05/12 11:20:16	high	vulnerability	FTP: login Brute-force attempt	ethern...	TAP-138	TAP-138				21	ftp	ale
05/12 11:20:15	critical	spyware	ZeroAccess.Gen Command and Control Traffic	ethern...	TAP-138	TAP-138				1111	unknown-udp	ale
05/12 11:20:13	critical	spyware	ZeroAccess.Gen Command and Control Traffic	ethern...	TAP-138	TAP-138				1111	unknown-udp	ale
05/12 11:20:11	critical	spyware	ZeroAccess.Gen Command and Control Traffic	ethern...	TAP-138	TAP-138				1111	unknown-udp	ale
05/12 11:20:09	critical	spyware	ZeroAccess.Gen Command and Control Traffic	ethern...	TAP-138	TAP-138				1111	unknown-udp	ale
05/12 11:20:07	critical	spyware	ZeroAccess.Gen Command and Control Traffic	ethern...	TAP-138	TAP-138				1111	unknown-udp	ale
05/12 11:20:05	critical	spyware	ZeroAccess.Gen Command and Control Traffic	ethern...	TAP-138	TAP-138				1111	unknown-udp	ale
05/12 11:20:03	critical	spyware	ZeroAccess.Gen Command and Control Traffic	ethern...	TAP-138	TAP-138				1111	unknown-udp	ale
05/12 11:20:01	critical	spyware	ZeroAccess.Gen Command and Control Traffic	ethern...	TAP-138	TAP-138				1111	unknown-udp	ale
05/12 11:19:58	critical	spyware	ZeroAccess.Gen Command and Control Traffic	ethern...	TAP-138	TAP-138				1111	unknown-udp	ale
05/12 11:19:56	critical	spyware	ZeroAccess.Gen Command and Control Traffic	ethern...	TAP-138	TAP-138				1111	unknown-udp	ale
05/12 11:19:54	critical	spyware	ZeroAccess.Gen Command and Control Traffic	ethern...	TAP-138	TAP-138				1111	unknown-udp	ale
05/12 11:19:37	low	spyware	Servicelous.sundaydd User-Agent Traffic	ethern...	TAP-138	TAP-138				5060	sp	ale
05/12 11:19:29	high	vulnerability	FTP: login Brute-force attempt	ethern...	TAP-138	TAP-138				21	ftp	ale

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 figure consists of three vertically stacked screenshots of the Palo Alto Networks Management Console interface:

- Screenshot 1 (Top): Create and manage all objects**
- Screenshot 2 (Middle): Manage network connectivity**
- Screenshot 3 (Bottom): Manage the device**

Screenshot 1: Create and manage all objects

This screenshot shows the Objects page. The left sidebar includes sections like Addresses, Groups, Applications, Services, and Security Profiles. The main pane displays a search results table for "2014 matching applications". A red box highlights the title "Create and manage all objects".

Name	Category	Subcategory	Risk	Technology	Standard Ports
22-explore	212 business-systems	213 collaboration	120	ip-protocol	tcp/22
2410-reddwarf	210 general-internet	211 general	120	ip-protocol	tcp/2410
433-networking	213 networking	2 unknown	120	ip-protocol	tcp/433
1023-general-business	212 business-systems	213 collaboration	120	ip-protocol	tcp/1023

Screenshot 2: Manage network connectivity

This screenshot shows the Network > Interfaces page. The left sidebar lists various interface types. The main pane displays a table of interfaces (universe, TestZone1, trust, virtual-wire, virtual-wire, virtual-wire, layer3, layer3) with columns for User ID, Included Networks, and Excluded Networks. A red box highlights the title "Manage network connectivity".

Name	Type	User ID	Included Networks	Excluded Networks
universe	layer2	any	any	none
TestZone1	layer2	any	any	none
trust	virtual-wire	any	any	none
virtual-wire	virtual-wire	any	any	none
virtual-wire	virtual-wire	any	any	none
layer3	layer3	any	any	none
layer3	layer3	any	any	none
layer3	ethernet/L3	any	any	none

Screenshot 3: Manage the device

This screenshot shows the Device > Setup page. The left sidebar lists various configuration categories. The main pane is divided into several sections: General Settings (SSL/TLS Service Profile, Time Zone, Locale, Time, Geo Location), Authentication Settings (Authentication Profile, Certificate Profile, Idle Timeout, Failed Attempts, Lockout Time), Logging and Reporting Settings (Log Storage, Number of Versions for Config Audit, Max Rows in CSV Export, Average Browse Time, Page Load Threshold, Send HOSTNAME in Syslog, Report Expiration Period, Stop Traffic when LogDB Full, Enable Log on High DP Load), and Minimum Password Complexity (Enabled, Minimum Length, Minimum Uppercase Letters, Minimum Lowercase Letters, Minimum Numeric Letters, Minimum Special Characters, Block Repeated Characters). A red box highlights the title "Manage the device".

Activity 2 – Safely Enable Applications

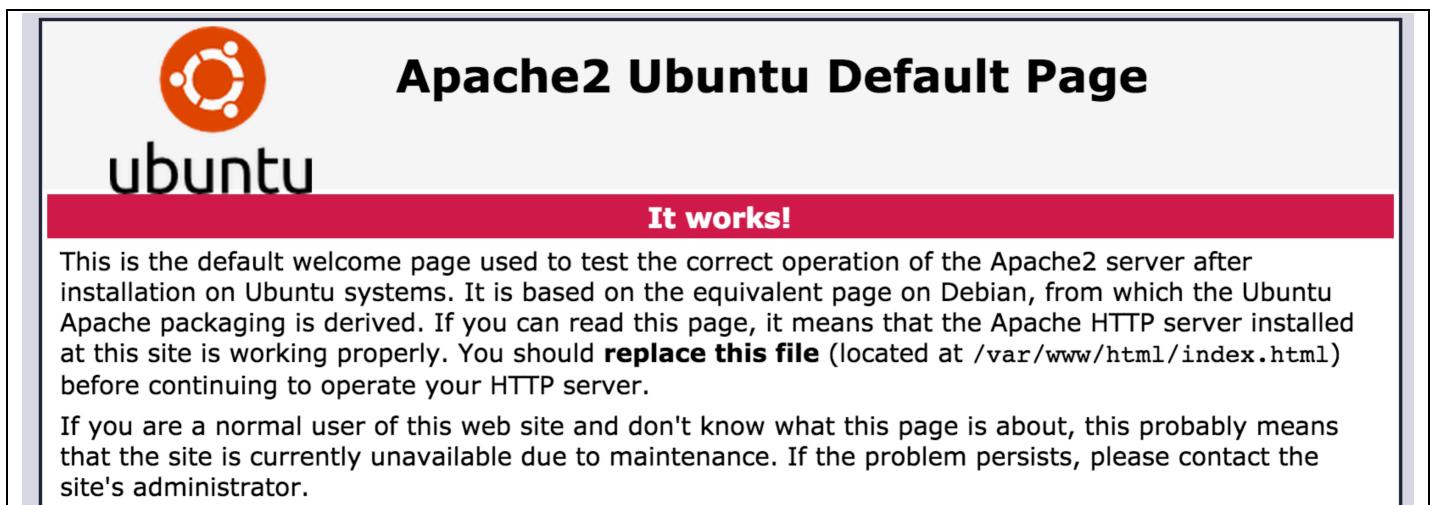
In this activity, you will:

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

Task 1 – Verify Static Content on Web Server

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

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



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

	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.

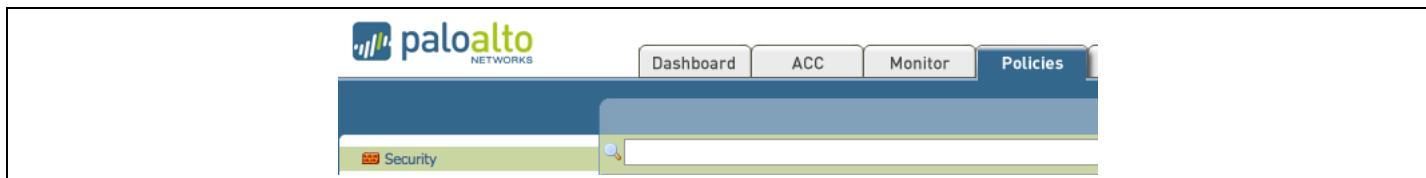
The screenshot shows a table of firewall logs. The columns are: Receive Time, Type, From Zone, To Zone, Source, Destination, To Port, Application, Action, and Rule. The 'Action' column for all rows is highlighted with a yellow box. The logs show multiple 'drop' events from 'web' to 'db' ports over port 3306.

	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.

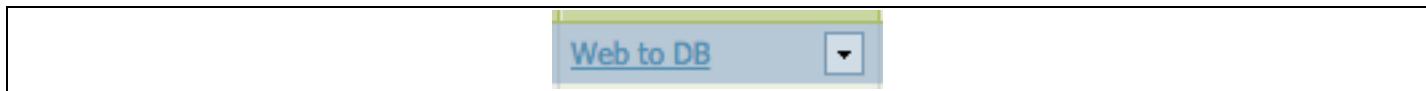


Scroll down to the **Web to DB** rule (rule 6) and note the Source and Destination zones.

	Name	Type	Zone	Source	Destination	Address	Zone	Address	Application	Service	Action
6	Web to DB	universal	db	any	web	any			mysql		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**.

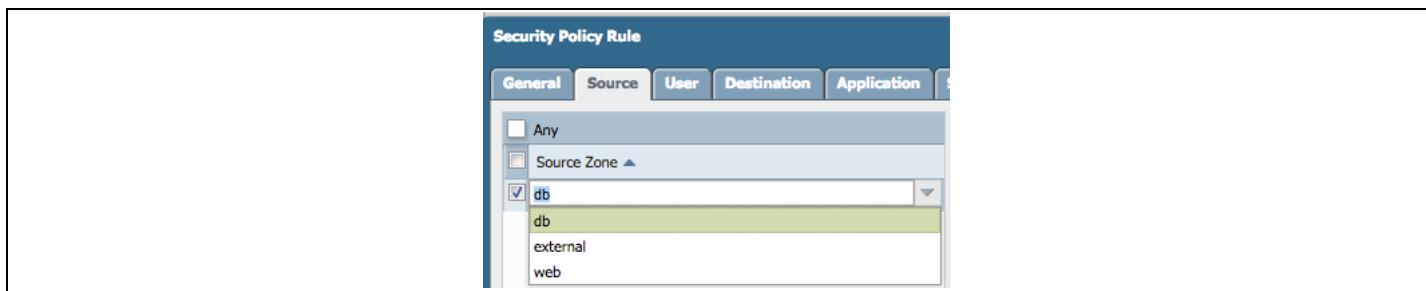
Click on the **Web to DB** rule



Click on the **Source**



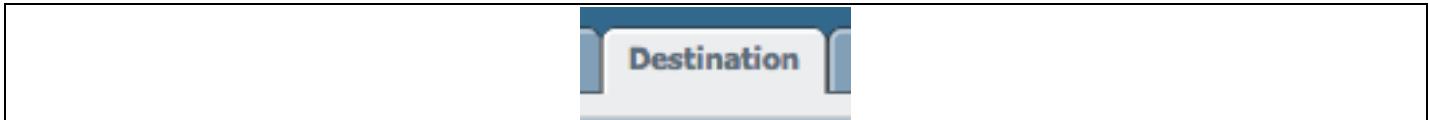
Click on **db** to bring up the pull down menu and change the selection to **web**



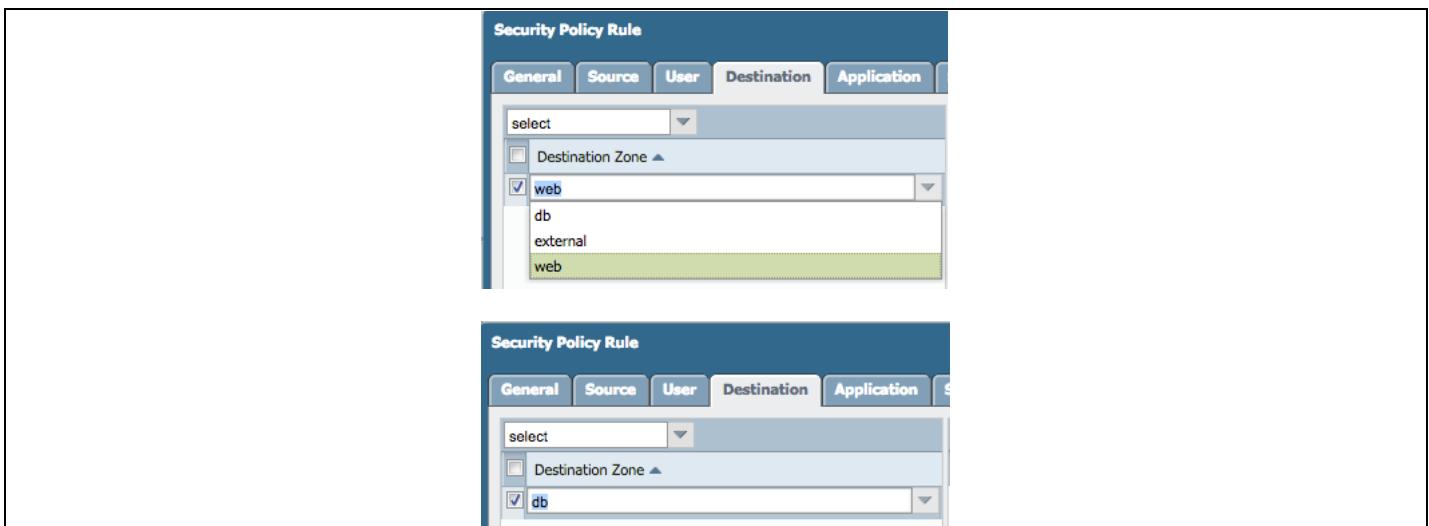
Palo Alto Networks AWS CFT Deployment Guide



Click on Destination



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



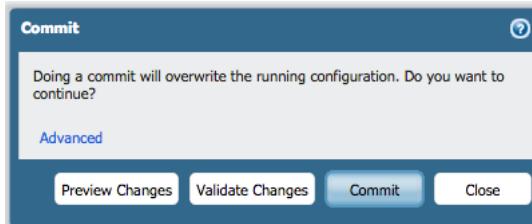
Verify your security rule now resembles the snapshot below. This rule should allow traffic from the web zone to the db zone.

			Source		Destination					
	Name	Type	Zone	Address	Zone	Address	Application	Service	Action	
6	Web to DB	universal	<input type="checkbox"/> web	any	<input type="checkbox"/> db	any	<input type="checkbox"/> mysql	<input type="checkbox"/> application-d...	<input checked="" type="checkbox"/> Allow	

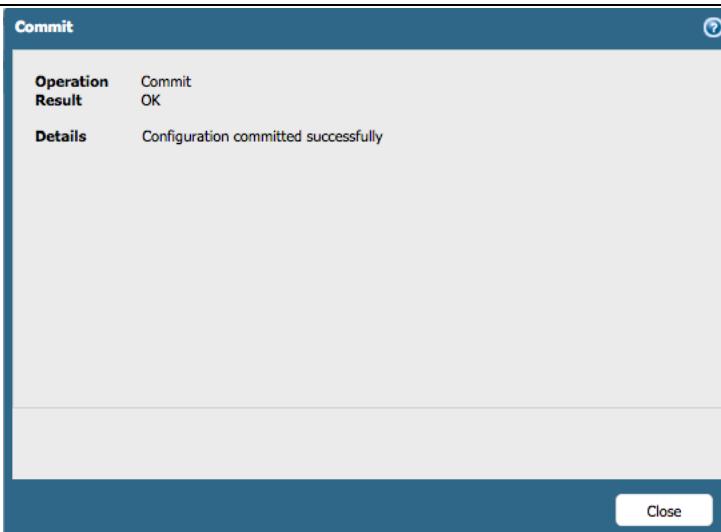
Click on **Commit** in the upper right.



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

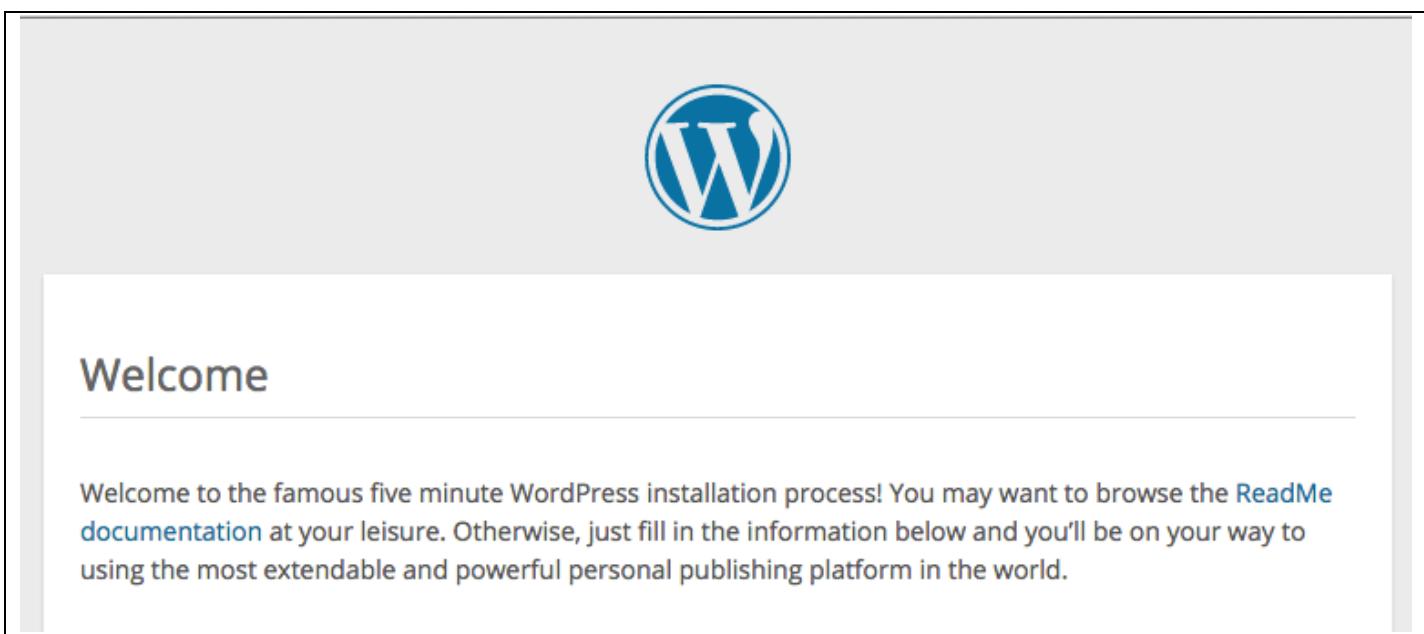


Verify the commit was successful and then click **Close**.



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.

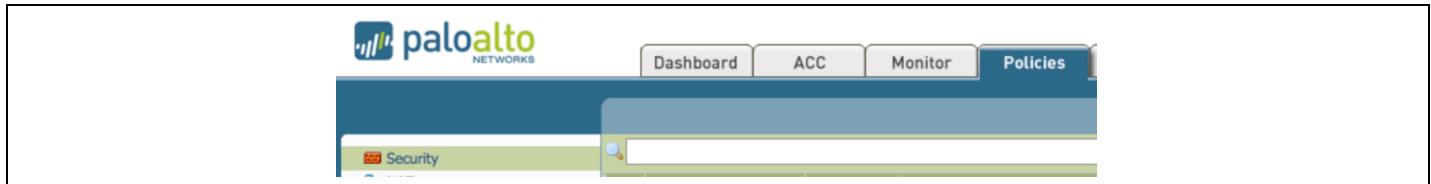
Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule
05/28 16:26:02	drop	web	db	10.0.1.101	10.0.2.101	22	not-applicable	deny	Log default deny
05/28 16:25:30	drop	web	db	10.0.1.101	10.0.2.101	22	not-applicable	deny	Log default deny

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.

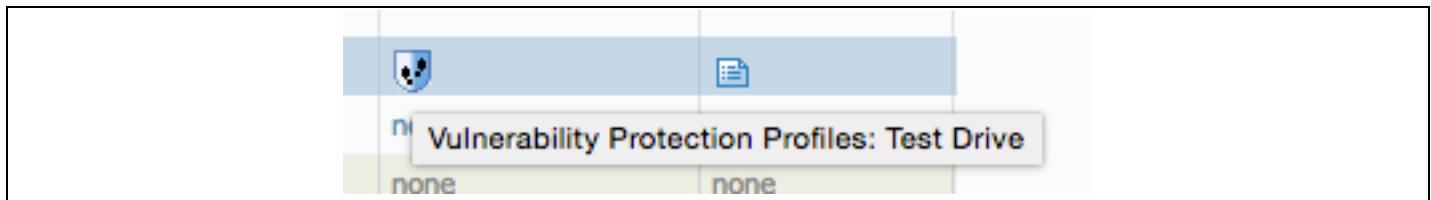
Palo Alto Networks AWS CFT Deployment Guide

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

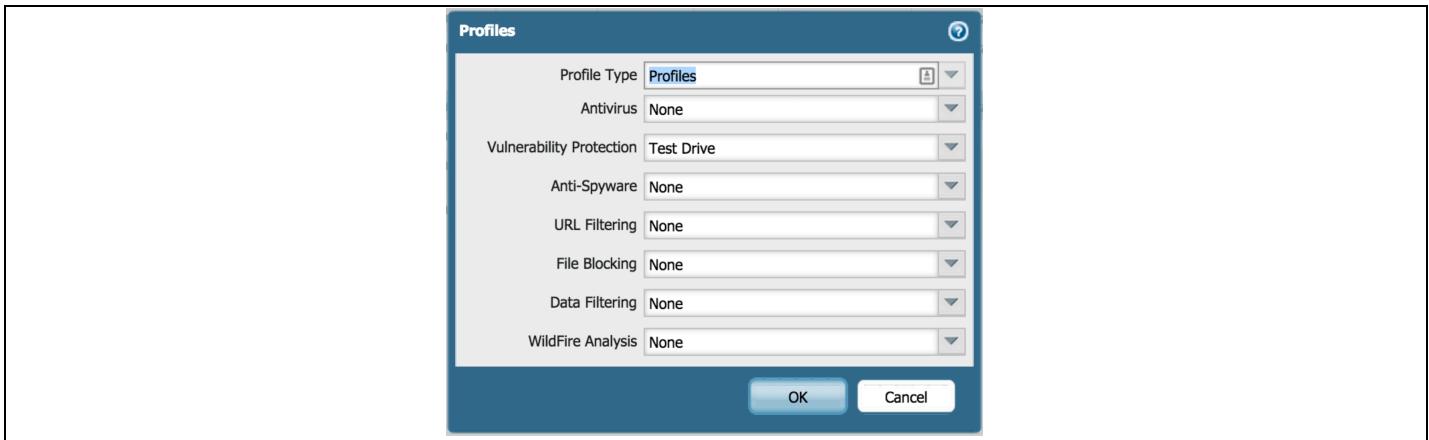


For the **Web to DB** rule, hover over the icon in the **Profile** column and note the **Test Drive** vulnerability profile in use.

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		
7 Log default deny	none	universal	any	any	any	any	any	any	any	any	Deny	none	
8 Intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow	none	none
9 interzone-default	none	interzone	any	any	any	any	any	any	any	any	Deny	none	none



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



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



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

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

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

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

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

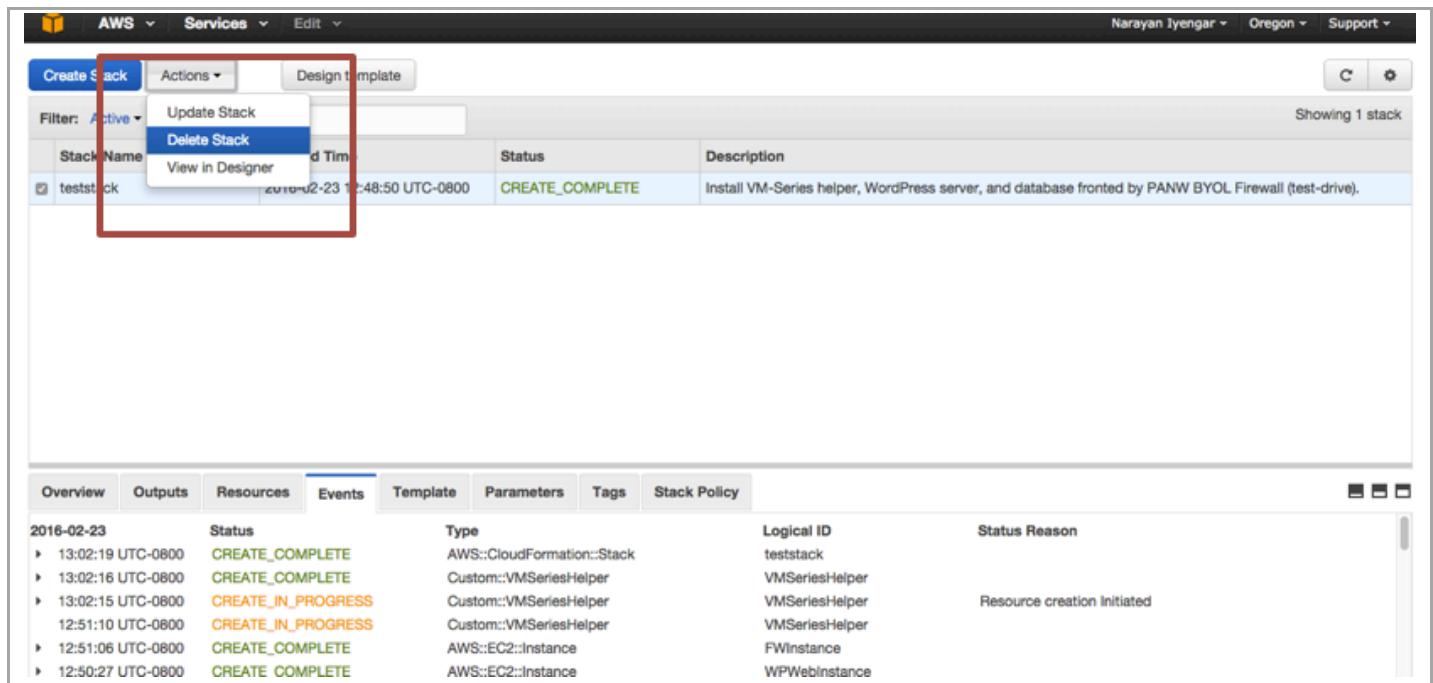
9.1 Delete the Stack

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

The screenshot shows the AWS CloudFormation service page. The 'CloudFormation' icon is highlighted with a red box. The URL at the bottom is <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', and user information ('Narayan Iyengar - Oregon - Support'). Below the navigation is a table for managing stacks. A red box highlights the 'Actions' dropdown menu for the stack named 'teststack'. The 'Delete Stack' option is selected. The table has columns for 'Stack Name', 'Last Updated', 'Status', and 'Description'. The 'teststack' row shows a status of 'CREATE_COMPLETE' with a description of 'Install VM-Series helper, WordPress server, and database fronted by PANW BYOL Firewall (test-drive)'. Below the table, there are tabs for 'Overview', 'Outputs', 'Resources', 'Events', 'Template', 'Parameters', 'Tags', and 'Stack Policy'. The 'Events' tab is selected, displaying a log of events for the stack creation on 2016-02-23.

Stack Name	Last Updated	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).

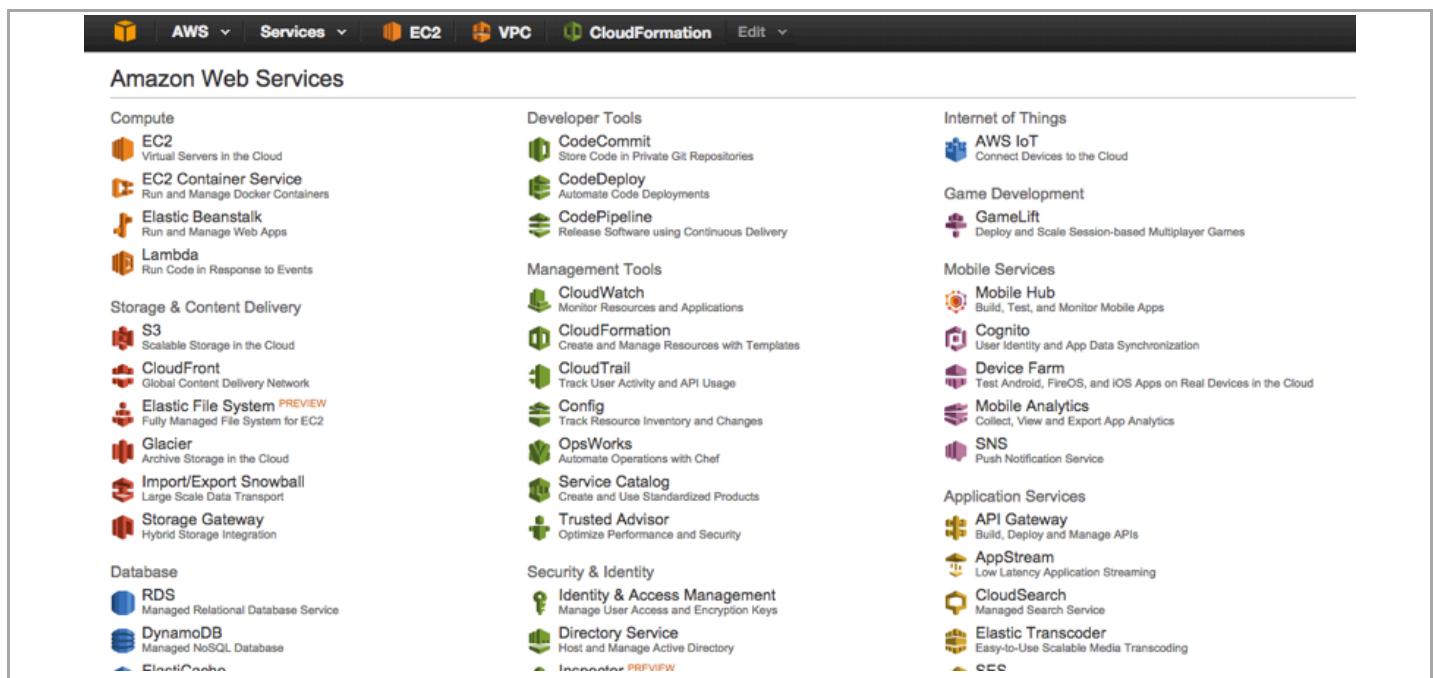
Events (2016-02-23)

Date	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 Services console. The 'EC2' service is selected in the top navigation bar. The main page is titled 'Amazon Web Services' and lists various services under different categories:

- 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).
- 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.

Palo Alto Networks AWS CFT Deployment Guide

Click on **Key Pairs**:

The screenshot shows the AWS EC2 Dashboard. On the left, there's a sidebar with links like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, and Images. The main area is titled "Resources" and displays statistics for the US West (Oregon) region: 0 Running Instances, 0 Dedicated Hosts, 17 Volumes, 11 Key Pairs, 0 Placement Groups, 0 Elastic IPs, 0 Snapshots, 1 Load Balancers, and 5 Security Groups. Below this, there's 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" section of the EC2 dashboard. A red box highlights the "Delete" button. The table lists three key pairs: VMSH-test123, VMSH-foobar, and VMSH-blah, each with its corresponding fingerprint.

Key pair name	Fingerprint
VMSH-test123	79:29:5e:dc:81:61:0a:97:a1:5b:73:34:1a:30:2b:4f:1b:78:8f:97
VMSH-foobar	f0:3b:5d:cc:ba:2e:6f:54:c1:d4:19:a8:f4:b3:9c:19:c9:dc:eb:86
VMSH-blah	35:0e:06:b5:08:b1:02:2d:e5:a9:32:d4:97:55:f1:20:47:a3:bc:03

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

The screenshot shows a confirmation dialog box 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
2016-08-12								
▶ 13:32:37 UTC-0700	Status	AWS::CloudFormation::Stack	Type	test	Logical ID		Status reason	
▶ 13:32:23 UTC-0700	DELETE_IN_PROGRESS	AWS::CloudFormation::Stack		test			User Initiated	
▶ 13:32:15 UTC-0700	ROLLBACK_IN_PROGRESS						The following resource(s) failed to create: [NewWebSubnet, route2, NewPublicSubnet, subnetacl1, route1, BootstrapRole, FWPrivateNetworkInterface, WPDBServerInstance]. . Rollback requested by user.	
▶ 13:32:14 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::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					ac10/c00002	
▶ 09:09:02 UTC-0600	CREATE_IN_PROGRESS	AWS::EC2::VPDHCPOptionsAssociation					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					ac1b765d6d2	Resource creation initiated
09:09:01 UTC-0600	CREATE_IN_PROGRESS	AWS::EC2::VPDHCPOptionsAssociation					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 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.