

AWS ALB Sandwich



AWS ALB Sandwich Deployment Guide

Deploying the VM-Series and an AWS ALB sandwich for multi-AZ high availability and manual scale

<http://www.paloaltonetworks.com>

Table of Contents

Version History	3
1. About	4
2. Support Policy	5
3. Implementation Details	5
4. Prerequisites	6
4.1 Create AWS account	6
4.2 Version 8.1 or Greater	6
4.3 Accept the EULA	6
4.4 Download GitHub Files	6
4.5 Create a Bootstrap Bucket	6
5. Launch the Template	8
6. Deploy Jumphost	Error! Bookmark not defined.
7. Access the Jumphost	Error! Bookmark not defined.
8. Update the Firewalls	12
9. Verify the Results	18
10. Cleanup	20
10.1 Delete the deployment	20
11. Conclusion	20
Appendix A	21

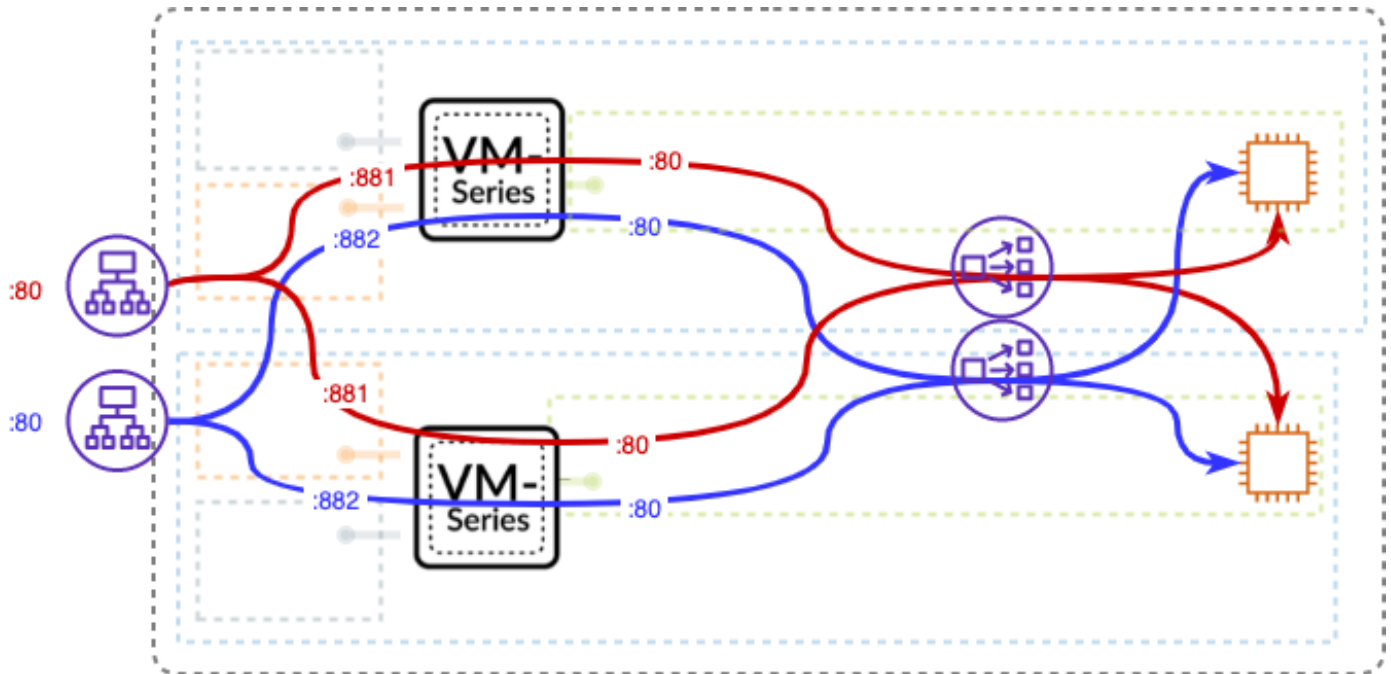
Version History

Version number	Comments
1.0	Initial Draft
1.1	Dual Stack

1. About

Customers are looking for different ways to ensure inbound high availability and scale for their AWS deployments. Several options exist including traditional two device HA in active passive mode, or Auto Scaling the VM-Series.

This ALB sandwich CloudFormation Template deploys a pair of VM-Series Firewalls and 2 Web Servers with 1 or 2 external Application Load Balancers and 1 or 2 internal Network Load Balancers.



The ALB sandwich with the VM-Series is an elegant and simplified way to manually scale VM-Series deployments to address planned or projected traffic increases while also delivering multi-Availability Zone HA.

- Manual scale: the ALB sandwich allows you to add, via script, or manual process, additional VM-Series firewalls can be added to the deployment to address planned/projected inbound traffic increases.
- Multi-availability zone high availability: two VM-Series firewalls deployed in separate Availability Zones with traffic being distributed by the AWS load balancers enables a cloud-centric approach to resiliency and availability.

The ALB sandwich is dependent on PAN-OS 8.1 or greater as it uses the new FQDN object for NAT rules to automatically update the IP addresses.

2. Support Policy

This template 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/>) or sites other than our official Downloads page on <https://support.paloaltonetworks.com> are provided under the best effort policy.

3. Implementation Details

When using this sample CFT the following machine types are used by default, this can be changed:

Instance name	Machine Type
Web Server	t2-micro
VM Series Firewall	d5-xlarge

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

External access to the firewalls is obtained through the use of a Jumpbox created separately. Since no inbound access is enabled to the firewall management interfaces or web servers, the Security Groups are intentionally wide open. There is a sgJumpbox Security Group provided for access to the Jumpbox.

Two templates are provided. One template deploys a single application stack and the other deploys 2 application stacks to show NAT flow through the firewalls.

4. Prerequisites

Here are the prerequisites required to successfully launch this template:

4.1 Create AWS account

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

4.2 Version 8.1 or Greater

When utilizing the an internal ALB, version 8.1 or greater is required for use of the FQDN NAT destination feature.

4.3 Accept the EULA

Accept the EULA for the VM-Series PAYG license bundle you plan to use.

[VM-Series firewall Bundle 2](#)

[VM-Series firewall Bundle 1](#)

4.4 Download GitHub Files

Download *.yml files, *.xml and init-cfg.txt files from Github to a local directory.

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 the AWS S3 console, create bucket with config, content, license and software folders. Upload the init-cfg.txt file from the repository to the config folder. Additionally, upload the corresponding alb-*lb.xml file as bootstrap.xml.

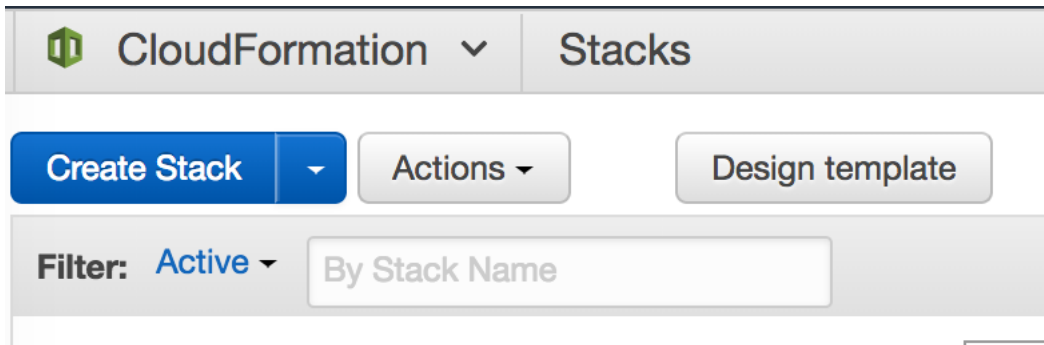
AWS ALB Sandwich Deployment Guide

The screenshot displays the AWS S3 console interface. The top navigation bar shows 'Amazon S3 > alb-sandwich'. Below this, there are two tabs: 'Overview' and 'Properties', with 'Properties' being the active tab. A search bar is present with the placeholder text 'Type a prefix and press Enter to search. Press ESC to clear.' Below the search bar, there are three buttons: 'Upload', 'Create folder', and 'More'. The main content area shows a list of objects in the 'alb-sandwich' bucket. The list has a header row with a checkbox and the text 'Name ↑'. Below this, there are four entries: 'config', 'content', 'license', and 'software', each with a folder icon. To the right, there is a separate panel showing the 'config' folder's contents. The top navigation bar for this panel shows 'Amazon S3 > alb-sandwich / config'. Below this, there are two tabs: 'Overview' and 'Properties', with 'Overview' being the active tab. A search bar is present with the placeholder text 'Type a prefix and press Enter to search. Press ESC to clear.' Below the search bar, there are three buttons: 'Upload', 'Create folder', and 'More'. The main content area shows a list of objects in the 'config' folder. The list has a header row with a checkbox and the text 'Name ↑'. Below this, there are two entries: 'bootstrap.xml' and 'init-cfg.txt', each with a document icon.

NOTE: Please create the folders using the console. Creating folders locally on your machine and uploading them may not work as expected.

5. Launch the Template

Log in to the AWS Console, access CloudFormation and hit the Create Stack Button.



On the Select Template page, hit Choose File and select the appropriate template downloaded from GitHub Repository.

Create stack

Prerequisite - Prepare template

Prepare template
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

☒ Template is ready
 ☐ Use a sample template
 ☐ Create template in Designer

Specify template

A template is a JSON or YAML file that describes your stack's resources and properties.

Template source
Selecting a template generates an Amazon S3 URL where it will be stored.

☐ Amazon S3 URL
 ☒ Upload a template file

Upload a template file

LbSandwichdualappNlbInternal.yml

JSON or YAML formatted file

S3 URL: <https://s3-external-1.amazonaws.com/cf-templates-1j98zfnc7hzy-us-east-1/2020093fMd-LbSandwichdualappNlbInternal.yml>

Specify the Details of the Stack.

- Stack Name
- Select 2 Availability Zones

AWS ALB Sandwich Deployment Guide

- Subnet Details for the VPC, Management, Untrust, Trust and Nat Gateway Subnets.
- Key Pair
- SSH From for Management Security lockdown
- Firewall AMI
- Firewall Instance Size
- Bootstrap Bucket Name previous created.
- Web Server Instance Size

AWS ALB Sandwich Deployment Guide

Specify stack details

Stack name

Stack name

lbsandwich

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

VPC Configuration

Availability Zones

Select 2 AZs

us-east-1c ✕

us-east-1d ✕

CIDR Block for the VPC

Enter the VPC CIDR that you want to use

192.168.0.0/16

Management Subnet CIDR Block

Management subnet comma-delimited list of CIDR blocks

192.168.0.0/24, 192.168.10.0/24

Untrust Subnet CIDR Block

Untrust subnet comma-delimited list of CIDR blocks

192.168.1.0/24, 192.168.11.0/24

Trust Subnet CIDR Block

Trust subnet comma-delimited list of CIDR blocks

192.168.2.0/24, 192.168.3.0/24

NAT Gateway Subnet CIDR Block

AWS NAT Gateway Comma-delimited list of CIDR blocks

192.168.100.0/24, 192.168.101.0/24

Key pair:

Amazon EC2 Key Pair

awsmain

Firewall Configuration

Firewall Instance Size

Enter the instance type and size for the VM-Series firewall

c5.xlarge

FirewallAMI

Input the firewall AMI ID. <https://docs.paloaltonetworks.com/compatibility-matrix/vm-series-firewalls/aws-cft-amazon-machine-images-ami-list>

Firewall Bootstrap Bucket

Enter the name S3 Bucket Name containing the Bootstrap files

sandwichbucket

Web Server Configuration

Web Server Instance Size

WebServer EC2 Instance type

t2.micro

Other parameters

SGforAdmin

IP info for fw mgmt lockdown

9.8.7.6/32

Click Next to move through the Options Page and optionally specify Tags.

On the Review Page, Check the “I acknowledge that AWS CloudFormation might create IAM resources.” Box and click Create.

Capabilities



The following resource(s) require capabilities: [AWS::IAM::Role]

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

☒ **I acknowledge that AWS CloudFormation might create IAM resources.**

6. Update the Firewalls

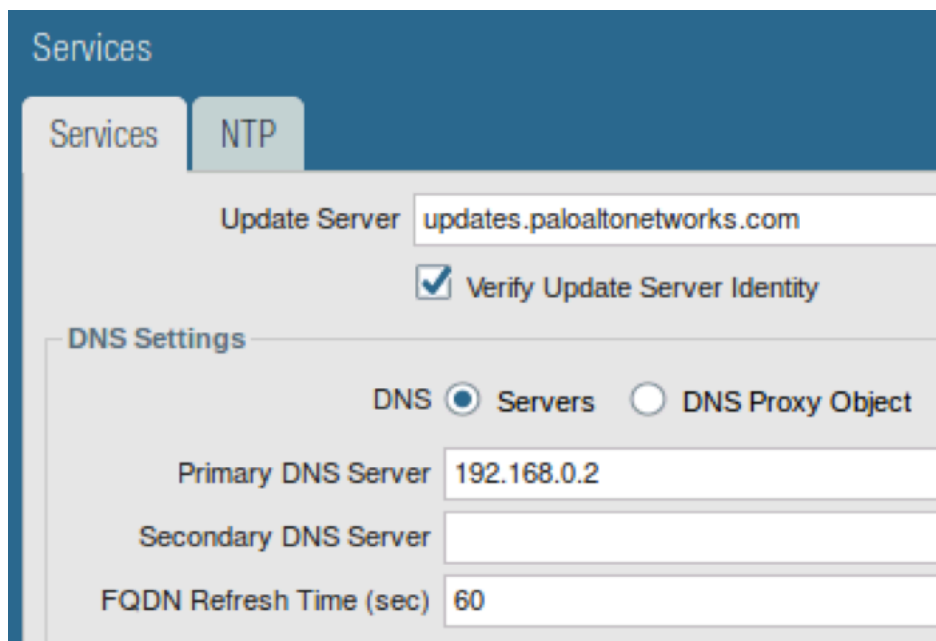
Using Firefox on the Jump host, access the Management IPs of the Firewalls. This will be ETH1 on the AWS Firewall Instance Details.

Username: pandemo Password: demopassword

Until PAN-94864 is resolved you will need to update the DNS server of the firewall.

Access Device -> Setup -> Services and hit the Gear Icon.

Set the Primary DNS server to the #.#.0.2 of the VPC's subnet.



The screenshot shows the 'Services' configuration page in the Palo Alto Networks management interface. The 'NTP' tab is selected. Under 'Update Server', the text 'updates.paloaltonetworks.com' is entered, and the checkbox 'Verify Update Server Identity' is checked. The 'DNS Settings' section has 'DNS Servers' selected with a radio button. The 'Primary DNS Server' field contains '192.168.0.2'. The 'Secondary DNS Server' field is empty. The 'FQDN Refresh Time (sec)' field contains '60'.

Move to the Objects Tab.

AWS ALB Sandwich Deployment Guide

Update the inside Load Balancer FQDN objects lb-fqdn1 and lb-fqdn2. These names are available on the Outputs tab of the CFT.

dualapp3

Delete

Update

Stack

Stack info

Events

Resources

Outputs

Parameters

Template

Change sets

Outputs (14)

Q Search outputs

Key	Value	Description
ExtLB2DNSName	dualapp3-ExtLB1-804618519.us-east-1.elb.amazonaws.com	Second Elastic Application Load Balancer (Public) DNS name
ExtLBDNSName	dualapp3-ExtLB1-804618519.us-east-1.elb.amazonaws.com	First Elastic Application Load Balancer (Public) DNS name
FW1ManagementIP	192.168.0.65	FW1 Management IP
FW1UntrustIP	192.168.1.243	FW1 Untrust IP
FW2ManagementIP	192.168.10.114	FW2 Management IP
FW2UntrustIP	192.168.11.180	FW2 Untrust IP
IntLB2DNSName	dualapp3-IntLB2-8c4f01503dd82357.elb.us-east-1.amazonaws.com	Second Elastic Network Load Balancer (Internal) DNS name
IntLBDNSName	dualapp3-IntLB1-e745788864cf0d9b.elb.us-east-1.amazonaws.com	First Elastic Network Load Balancer (Internal) DNS name
KeyName	awsmain	Key Pair you have selected for SSH
NATGateway1	52.2.134.195	NAT Gateway for Internet access
NATGateway2	35.171.80.184	NAT Gateway for Internet access
VPCID	vpc-05094b4a6a7152436	VPC ID
fw1Mgmt	54.156.247.114	Firewall 1 EIP
fw2Mgmt	3.213.99.177	Firewall 2 EIP

Address

Name

lb-fqdn1

Description

Type

FQDN

dualapp3-IntLB1-e745788864cf0d9b.elb.us-east-1.amazonaws.com

Resolve

Tags

OK

Cancel

AWS ALB Sandwich Deployment Guide

If subnets other than those suggested are utilized, update the following to match your Trust subnets.

Access Network -> Virtual Routers and open the “default” Virtual Router.

Access the Static Routes and open the introuteA.

Ensure the Trust Subnet in the opposing Availability Zone is correct in the Destination, the Interface is Ethernet1/2 and pointing the Trust Subnet’s #.#.#.1 IP address.

Virtual Router - Static Route - IPv4

Name

Destination

Interface

Next Hop

IP Address

Admin Distance

Metric

Route Table

BFD Profile

☒ Path Monitoring

Failure Condition
☒ Any
☐ All

Preemptive Hold Time (min)

<input type="checkbox"/>	Name	Enable	Source IP	Destination IP	Ping Interval(sec)	Ping Count
<input type="checkbox"/>	crosszone	<input checked="" type="checkbox"/>	DHCP	192.168.2.1	3	5

+ Add
- Delete

OK

Cancel

Virtual Router - Static Route - IPv4

Name

Destination

Interface

Next Hop

IP Address

Admin Distance

Metric

Route Table

BFD Profile

☒ Path Monitoring

Failure Condition
☒ Any
☐ All

Preemptive Hold Time (min)

<input type="checkbox"/>	Name	Enable	Source IP	Destination IP	Ping Interval(sec)	Ping Count
<input type="checkbox"/>	crosszone	<input checked="" type="checkbox"/>	DHCP	192.168.3.1	3	5

+ Add
- Delete

OK

Cancel

Virtual Router - Static Route - IPv4

Name	Cross-Zone-Route
Destination	192.168.12.0/24
Interface	ethernet1/2
Next Hop	IP Address
	192.168.2.1
Admin Distance	10 - 240
Metric	10
Route Table	Unicast
BFD Profile	Disable BFD
<input type="checkbox"/> Path Monitoring	

Commit the Policy.

Repeat Steps on the other Firewall.

7. Verify the Results

Review the Target Groups in EC2 to ensure the Targets are Healthy.

EC2 Dashboard

Events

Tags

Reports

Limits

INSTANCES

Instances

Launch Templates

Spot Requests

Reserved Instances

Dedicated Hosts

Scheduled Instances

IMAGES

AMIs

Bundle Tasks

ELASTIC BLOCK STORE

Volumes

Snapshots

NETWORK & SECURITY

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

LOAD BALANCING

Load Balancers

Target Groups

Create target group Actions

search : vpc-5551ca2e Add filter

Name	Port	Protocol	Target type	VPC ID
alb-s-FWTar-1NRABNNTJ...	80	HTTP	instance	vpc-5551ca2e
alb-s-WebSe-Z93D1D3S2V...	80	HTTP	instance	vpc-5551ca2e

Target group: alb-s-FWTar-1NRABNNTJOKWC

Description Targets Health checks Monitoring Tags

The load balancer starts routing requests to a newly registered target as soon as the registration process completes and the target passes the initial health checks. If demand on your targets increases, you can register additional targets. If demand on your targets decreases, you can deregister targets.

Edit

Registered targets

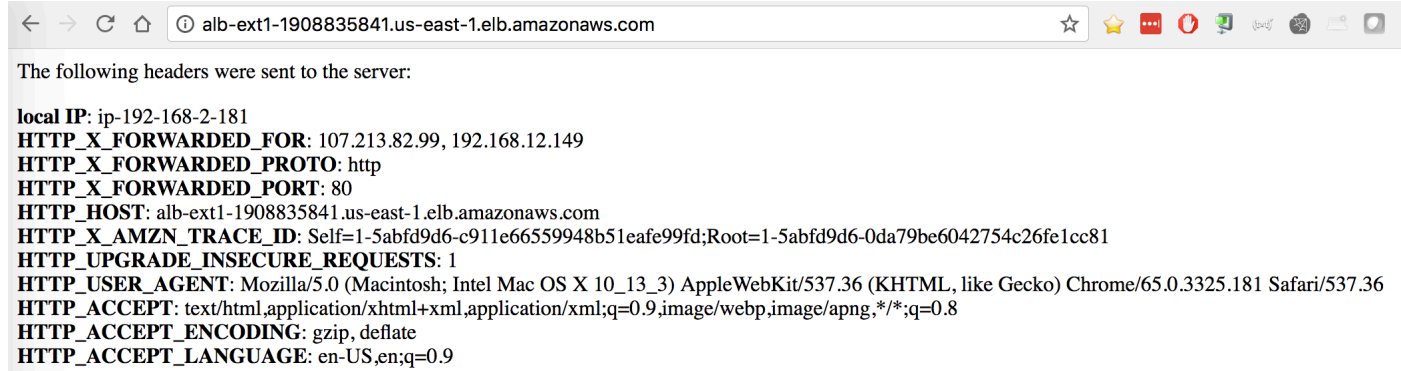
Instance ID	Name	Port	Availability Zone	Status
i-0cdd68c666c6b0772	alb-stack1-FW2	80	us-east-1b	healthy ⓘ
i-0278bb7ebe3f8a74a	alb-stack1-FW1	80	us-east-1a	healthy ⓘ

Availability Zones

Availability Zone	Target count	Healthy?
us-east-1a	1	Yes
us-east-1b	1	Yes

AWS ALB Sandwich Deployment Guide

Access the DNS Name of the External Load Balancer from a browser.



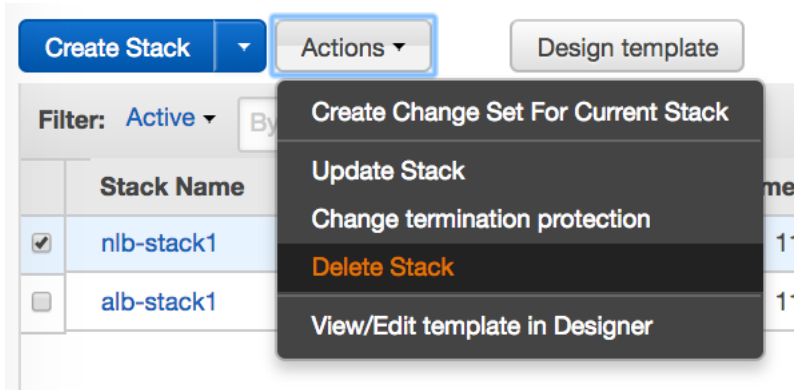
Review the Firewall Monitor to Ensure the Application is successfully resolving to web-browsing.

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	NAT Dest IP	To Port	Application	Action	Rule
	03/31 11:58:36	end	Untrust	Trust	192.168.111.166		192.168.11.215	192.168.12.39	80	web-browsing	allow	policy1
	03/31 11:58:31	end	Untrust	Trust	192.168.101.27		192.168.11.215	192.168.2.42	80	web-browsing	allow	policy1
	03/31 11:58:25	end	Untrust	Trust	192.168.111.166		192.168.11.215	192.168.12.39	80	web-browsing	allow	policy1
	03/31 11:58:20	end	Untrust	Trust	192.168.101.27		192.168.11.215	192.168.2.42	80	web-browsing	allow	policy1
	03/31 11:58:14	end	Untrust	Trust	192.168.111.166		192.168.11.215	192.168.2.42	80	web-browsing	allow	policy1
	03/31 11:58:09	end	Untrust	Trust	192.168.101.27		192.168.11.215	192.168.12.39	80	web-browsing	allow	policy1

8. Cleanup

8.1 Delete the deployment

Once done with the template, clean-up the environment by first deleting the Jumphost in EC2. Once the Jumphost has entered a Terminated state, delete the Stack in CloudFormation.



This should delete all the resources created via the template.

9. Conclusion

You have successfully deployed a CloudFormation Template with 2 Firewalls and two webserver behind a load balancer sandwich. In the case of an ALB internally, you are utilizing the new FQDN NAT destination feature of PAN-OS 8.1.

Appendix A