AWS ALB SandwichDeployment Guide

How to deploy a two-tiered application environment secured by the VM-Series firewall

http://www.paloaltonetworks.com
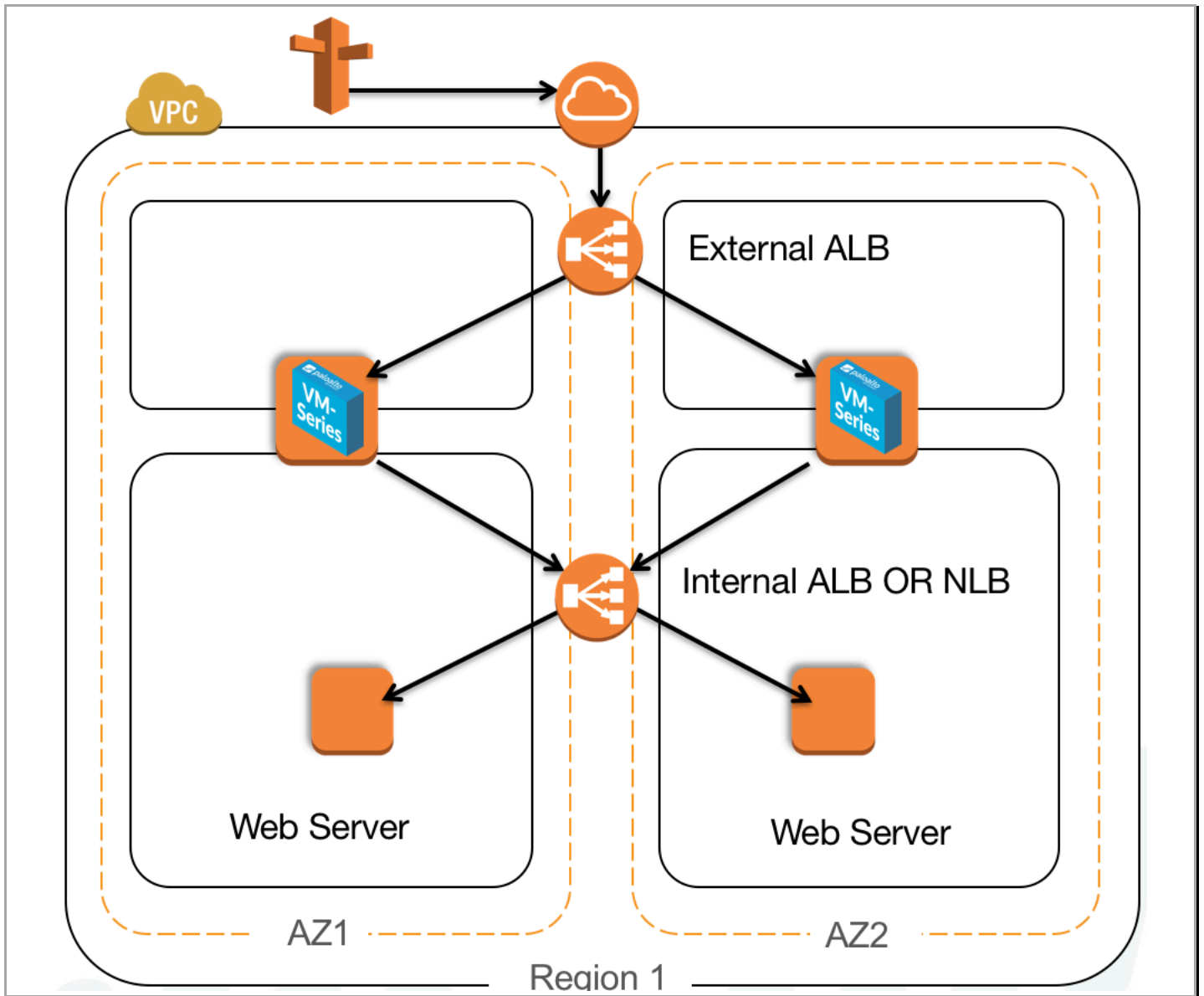
Table of Contents

Version History

Version number	Comments
1.0	Initial Draft

1. About

This CloudFormation template deploys a pair of VM-Series Firewalls and 2 Web Servers with an external Application Load Balancer and either an internal Application Load Balancer or Network Load Balancer depending on which CFT is chosen.

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	m4-xlarge
Jumphost	t2.medium

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 Jumphost 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 Jumphost.

Two template are provided. Both implement a ALB Externally with the Firewalls in the Target Group and the implementer has the choice of either an ALB or NLB in front of the Web Servers.

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 *.json 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.

Amazon S3 > alb-sandwich

Overview   Properties

Q Type a prefix and press Enter to search. Press ESC to clear.

⬆ Upload   ➕ Create folder   More ⌄

☐ Name ↑≡
☐ 📁 config
☐ 📁 content
☐ 📁 license
☐ 📁 software

Amazon S3 > alb-sandwich / config

Overview

Q Type a prefix and press Enter to search. Press ESC to clear.

⬆ Upload   ➕ Create folder   More ⌄

☐ Name ↑≡
☐ 📄 bootstrap.xml
☐ 📄 init-cfg.txt

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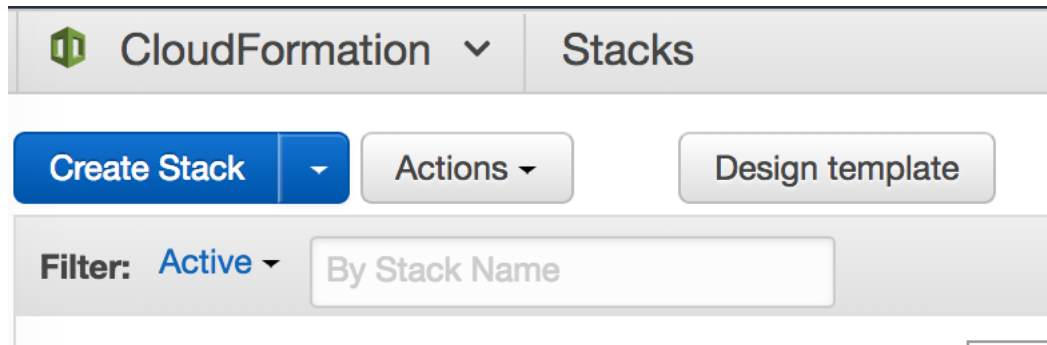
On the Select Template page, hit Choose File and select the appropriate template downloaded from GitHub Repository.
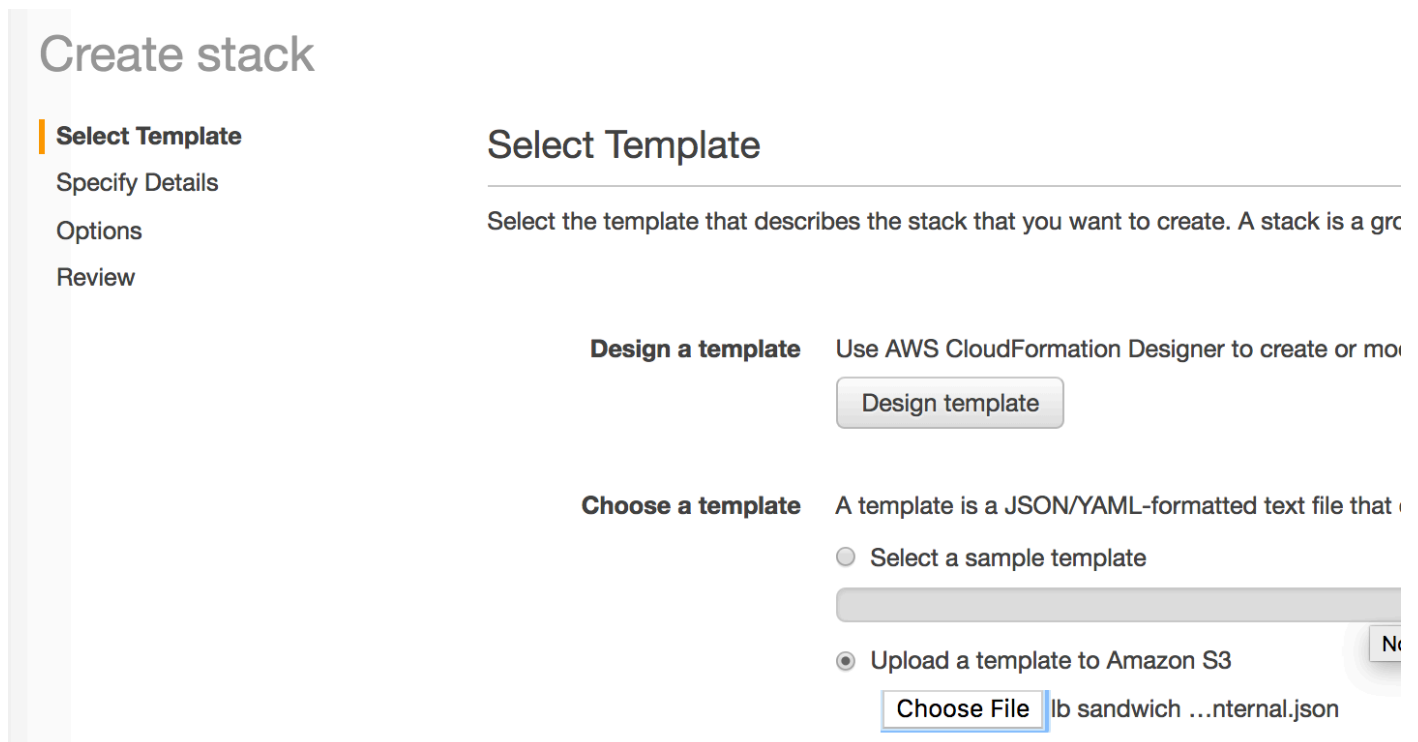
Specify the Details of the Stack.

- Stack Name
- VPC Name
- Select 2 Availability Zones
- Subnet Details for the VPC, Management, Untrust, Trust and Nat Gateway Subnets.
- Key Pair

- SSH From (Not Currently implemented as external access is not enabled for the firewall) Firewall License Type
- Firewall License Type. Choose Bundle 1 or Bundle 2 for PayGo, choose BYOL to provide a license either in the Bootstrap License folder or to license via the gui/panorama.
- Firewall Instance Size
- Bootstrap Bucket Name previous created.
- External and Internal Load Balancer Names
- Web Server Instance Size

Create stack

Select Template
Specify Details
Options
Review

Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. Learn more.

Stack name	alb-stack1

Parameters

VPC Configuration

VPC Name	alb-stack1-vpc	Name of the newly created VPC
Availability Zones	us-east-1a ✕ us-east-1b ✕	
	Select 2 AZs	
CIDR Block for the VPC	192.168.0.0/16	Enter the VPC CIDR that you want to use
Management Subnet CIDR Block	192.168.0.0/24, 192.168.10.0/24	
	Management subnet comma-delimited list of CIDR blocks	
Untrust Subnet CIDR Block	192.168.1.0/24, 192.168.11.0/24	Untrust subnet comma-delimited list of CIDR blocks
Trust Subnet CIDR Block	192.168.2.0/24, 192.168.12.0/24	Trust subnet comma-delimited list of CIDR blocks
NAT Gateway Subnet CIDR Block	192.168.101.0/24, 192.168.111.0/24	
	AWS NAT Gateway Comma-delimited list of CIDR blocks	
Key pair:	jason-mac	
	Amazon EC2 Key Pair	
SSH From:	0.0.0.0/0	
	Restrict SSH & HTTPS access to the Web Servers (by default can be accessed from anywhere)	

Firewall Configuration

FWLicenseType	Bundle1	Enter the license type for the Firewall
Firewall Instance Size	m4.xlarge	
	Enter the instance type and size for the VM-Series firewall	
Firewall Bootstrap Bucket	alb-sandwich	
	Enter the name S3 Bucket Name containing the Bootstrap files	

Load Balancer Configuration

External ALB Name	alb-ext1	Enter the name to associate with the NLB
Internal ALB Name	alb-int1	Enter the name to associate with the NLB

Web Server Configuration

Web Server Instance Size	t2.micro	WebServer EC2 instance type

Cancel   Previous   **Next**

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. Deploy Jumphost

This template will walk through the deployment of a Linux based instance with RDP access called Mint. You can also use Windows or SSH Tunneling to gain access to the Firewalls.

Access EC2 and hit Launch Instance. Select AWS Marketplace on the lefthand menu and Search for "Mint" and Select "Linux Mint Serena Desktop HVM"

Hit Continue from the Information Page.

Choose your Instance Type and hit the Configure Instance Details button. NOTE GUI based systems generally perform better with at least 2 vCPUs. T2.micro will work with the Free Tier.

On Step 3, update the following Parameters, accepting all other defaults.

- Network – Select your VPC created in via the template.
- Subnet – Add the Instance to either NATGW subnet.
- Auto-assign Public IP - Enable

Step 3: Configure Instance Details

No default VPC found. Select another VPC, or create a new default VPC.

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take adv pricing, assign an access management role to the instance, and more.

Number of instances ⓘ	1 Launch into Auto Scaling Group ⓘ
Purchasing option ⓘ	☐ Request Spot instances
Network ⓘ	vpc-5551ca2e | alb-stack1-vpc ⬍ C Create new VPC
	No default VPC found. Create a new default VPC.
Subnet ⓘ	subnet-5e0fc514 | alb-stack1-NATGWSubnetAz1 | u ⬍ Create new subnet
	249 IP Addresses available
Auto-assign Public IP ⓘ	Enable ⬍

Accept the defaults for Add Storage and Add Tags.

On the Configure Security Group page, choose the SGJumpbox group.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ○Create a **new** security group
◉Select an **existing** security group

	Security Group ID	Name	Description
☑	sg-82afa4f4	alb-stack1-sgJumpbox-JXNPKP0M03N5	SG for Jumpbox
☐	sg-22bab154	alb-stack1-sgWideOpen-1I34XY0F0K7MU	Wide open security group
☐	sg-0eaaa178	default	default VPC security group

Select Review and Launch and the Launch Button.

Specify the appropriate Key Pair, check the acknowledgement box and hit Launch Instance.

Select an existing key pair or create a new key pair   ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

```
Choose an existing key pair                                                            ⬍
```
Select a key pair
```
jason-mac                                                                             ⬍
```

☑ I acknowledge that I have access to the selected private key file (jason-mac.pem), and that without this file, I won't be able to log into my instance.
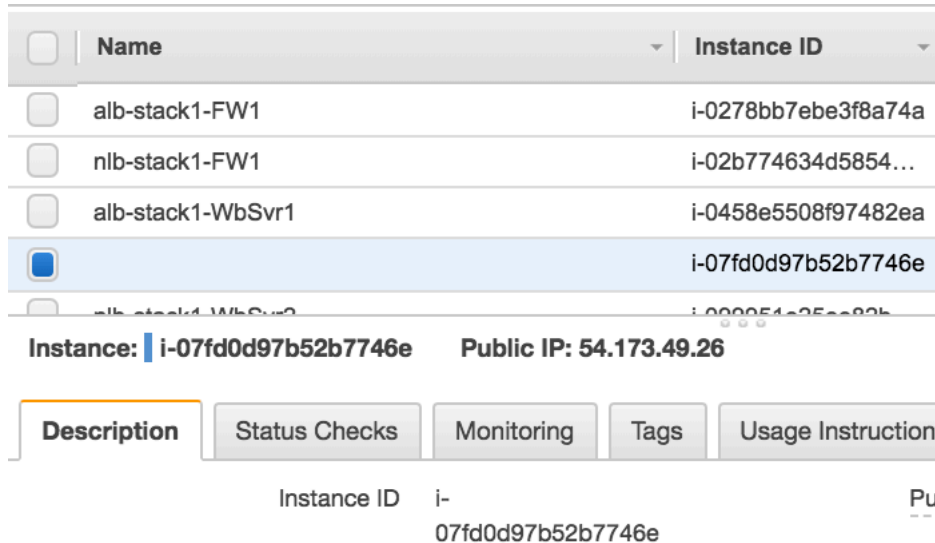
Cancel   **Launch Instances**

7. Access the Jumphost

Access EC2->Instance and Select the Jumphost.

Copy the Public IP to your RDP client.

Username – ec2-user

Password – Instance-ID copied from the Instance Details

	Name		Instance ID	
☐	alb-stack1-FW1		i-0278bb7ebe3f8a74a	
☐	nlb-stack1-FW1		i-02b774634d5854…	
☐	alb-stack1-WbSvr1		i-0458e5508f97482ea	
☑			i-07fd0d97b52b7746e	
☐	nlb-stack1-WbSvr2		i-092951a25aa82b…	

Instance: | i-07fd0d97b52b7746e   **Public IP: 54.173.49.26**

| Description | Status Checks | Monitoring | Tags | Usage Instruction |

Instance ID   i-07fd0d97b52b7746e   Pu

RDP to the Instance.

8. Update the Firewalls

Using Firefox on the Jumphost, 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.

Move to the Objects Tab.

Update the "AWS-NAT-UNTRUST" object with AWS ETH0 IP address of the firewall.

Name		Instance ID	Instance Type	Availabil
☐	alb-stack1-FW1	i-0278bb7ebe3f8a74a	m4.xlarge	us-east-1
☐	nlb-stack1-FW1	i-02b774634d5854	m4.xlarge	us-east-1

Instance: ▌ **i-0278bb7ebe3f8a74a (alb-stack1-FW1)   Private IP: 192.168.1.156**

| Description | Status Checks | Monitoring | Tags | Usage Instructions |

Instance ID   i-0278bb7ebe3f8a74a

Instance state   running

Network Interface eth0

Interface ID	eni-a8560c7f
VPC ID	vpc-5551ca2e
Attachment Owner	360174888430
Attachment Status	attached
Attachment Time	Sat Mar 31 11:59:48 GMT-500 2018
Delete on Terminate	false
Private IP Address	192.168.1.156
Private DNS Name	-
Elastic IP Address	-
Source/Dest. Check	false
Description	AWS FW1 E1/1
Security Groups	alb-stack1-sgWideOpen-1I34XY0F0K7MU

Public DNS (IPv4)   -

IPv4 Public IP   -

92-168-1-
ec2.intern
168.2.174
168.0.20,
168.1.156

5551ca2e

et-750bc

Platform   -   Network interfaces   eth0
                                                eth1
                                                eth2

IAM role   alb-stack1-
            BootstrapRole-   Source/dest. check   False

If using the ALB Internal Template. Update the "alb-fqdn" with the Internal ALB DNS Name.

If Using the NLB Internal template, use the dig command on the jumphost to resolve the NLB IPs.

```
ec2-user@LinuxMint ~ $ dig internal-alb-int1-2007287960.us-east-1.elb.amazonaws.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> internal-alb-int1-2007287960.us-east-1.elb.amazonaws.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62701
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;internal-alb-int1-2007287960.us-east-1.elb.amazonaws.com. IN A

;; ANSWER SECTION:
internal-alb-int1-2007287960.us-east-1.elb.amazonaws.com. 60 IN A 192.168.2.42
internal-alb-int1-2007287960.us-east-1.elb.amazonaws.com. 60 IN A 192.168.12.39

;; Query time: 3 msec
;; SERVER: 192.168.0.2#53(192.168.0.2)
;; WHEN: Sat Mar 31 13:44:29 EDT 2018
;; MSG SIZE  rcvd: 117

ec2-user@LinuxMint ~ $
```

Update the "alb-internal" object with IP in the corresponding Availability Zone.

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

Access the Static Routes and open the Cross-Zone-Route.

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	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

Path Monitoring

Commit the Policy.

Repeat Steps on the other Firewall.

9. Verify the Results

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

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

The following headers were sent to the server:

local IP: ip-192-168-2-181
HTTP_X_FORWARDED_FOR: 107.213.82.99, 192.168.12.149
HTTP_X_FORWARDED_PROTO: http
HTTP_X_FORWARDED_PORT: 80
HTTP_HOST: alb-ext1-1908835841.us-east-1.elb.amazonaws.com
HTTP_X_AMZN_TRACE_ID: Self=1-5abfd9d6-c911e66559948b51eafe99fd;Root=1-5abfd9d6-0da79be6042754c26fe1cc81
HTTP_UPGRADE_INSECURE_REQUESTS: 1
HTTP_USER_AGENT: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181 Safari/537.36
HTTP_ACCEPT: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
HTTP_ACCEPT_ENCODING: gzip, deflate
**HTTP_ACCEPT_LANGUAGE**: en-US,en;q=0.9

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

10. Cleanup

10.1 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.
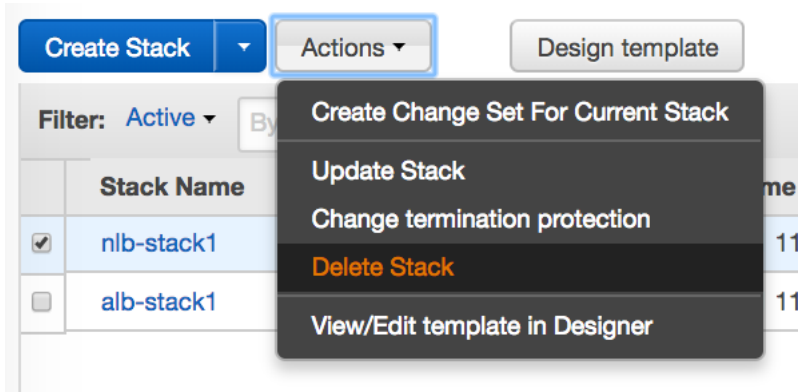
This should delete all the resources created via the template.

11. Conclusion

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

Appendix A