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

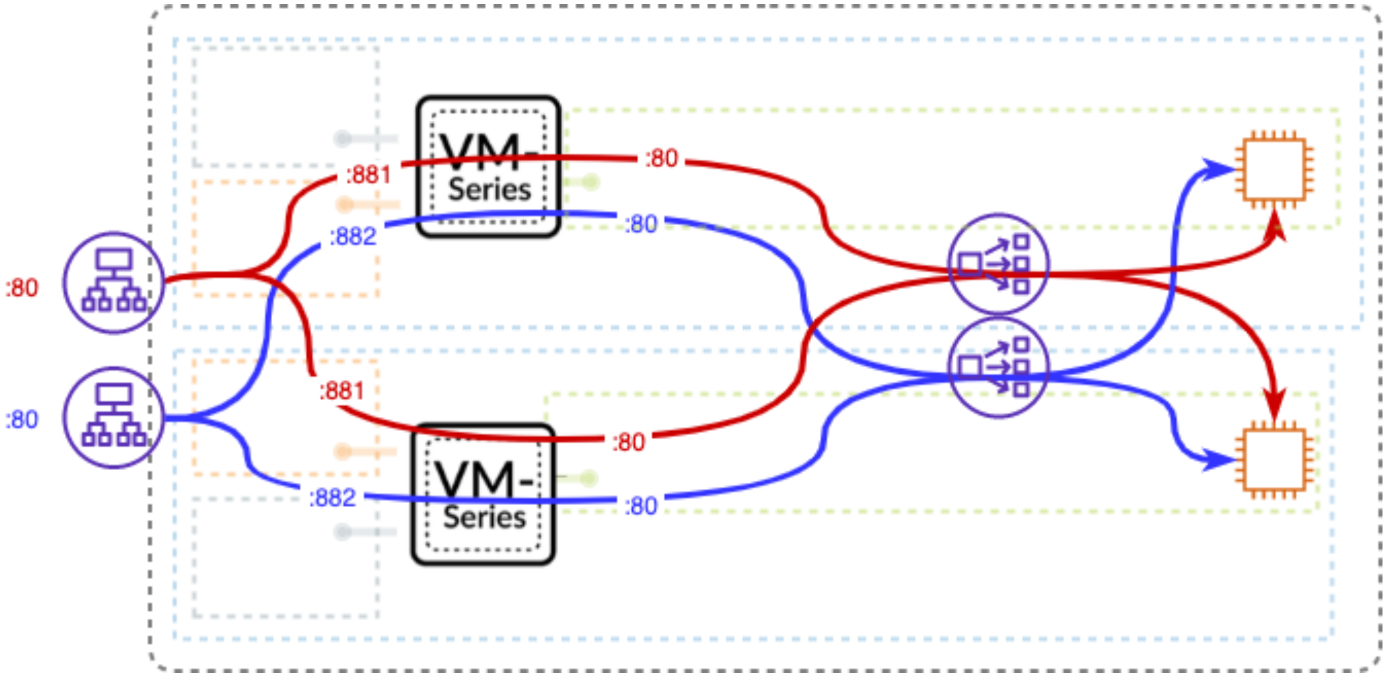
Version History

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 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 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

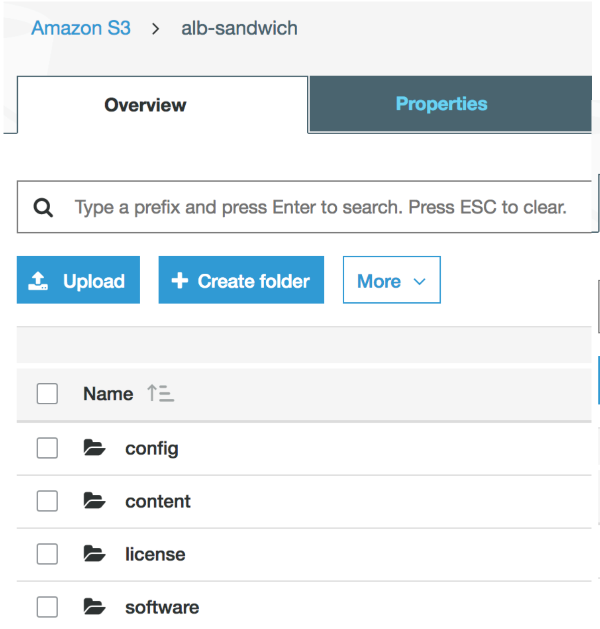
4.4 Download GitHub Files

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

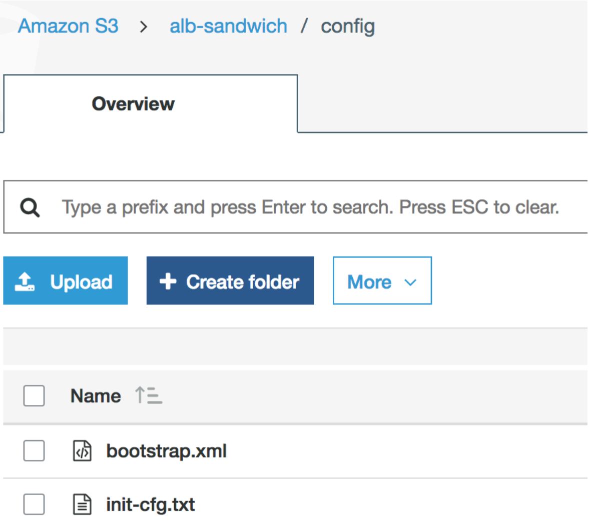
4.5 Create a Bootstrap Bucket

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.



□ config
□ content
□ license
□ software

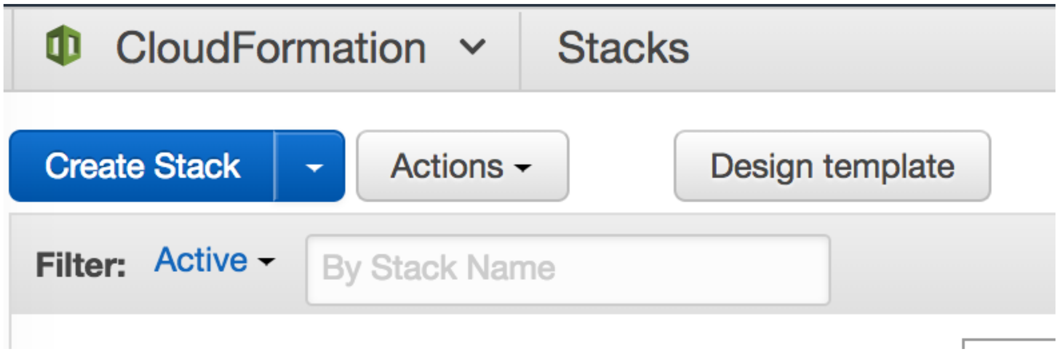

Amazon S3 > alb-sandwich / config
Overview
Type a prefix and press Enter to search. Press ESC to clear.
Upload
Create folder
More
Name

□ bootstrap.xml
□ init-cfg.txt

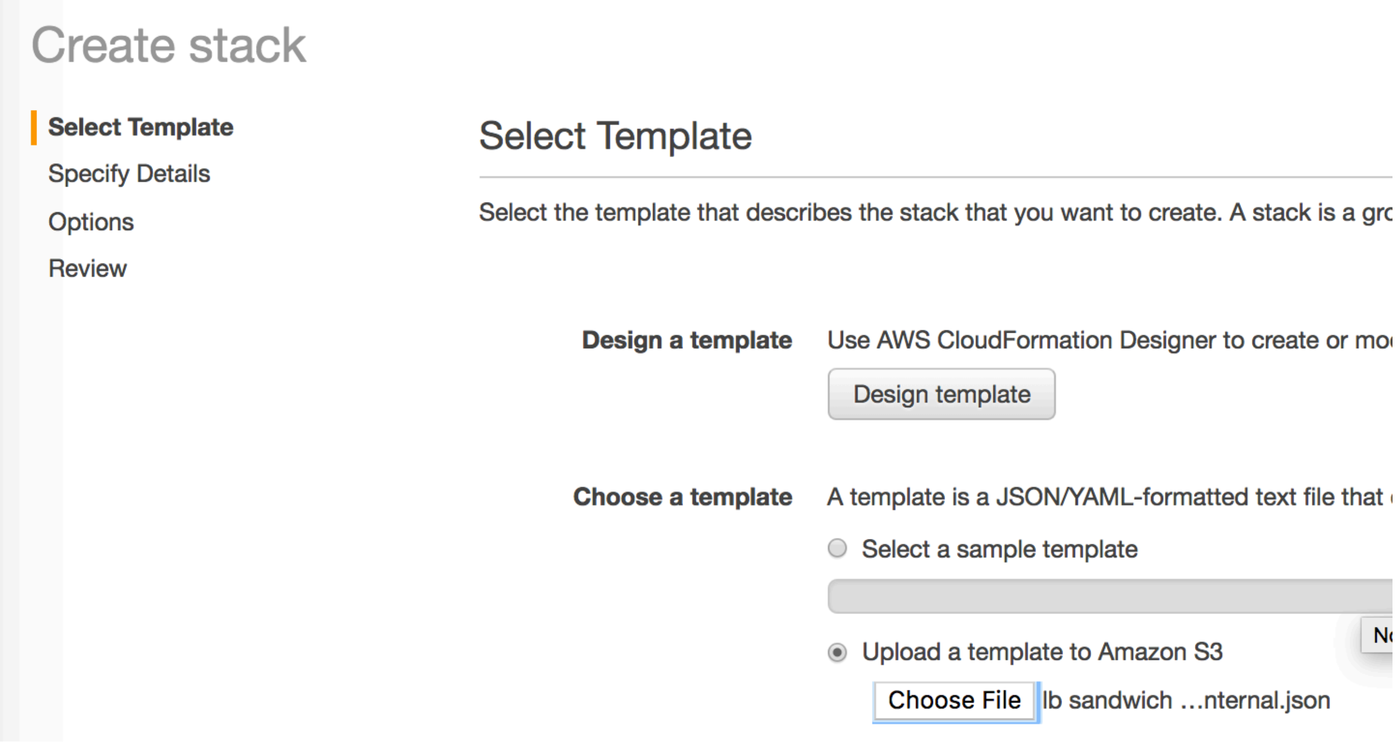
NOTE: Please create the folders using the console. Creating folders locally on your machine and uploading them may not work as expected.

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.



Select Template

Select the template that describes the stack that you want to create. A stack is a grc

Design a template: Use AWS CloudFormation Designer to create or mo

Choose a template: A template is a JSON/YAML-formatted text file that

○ Select a sample template

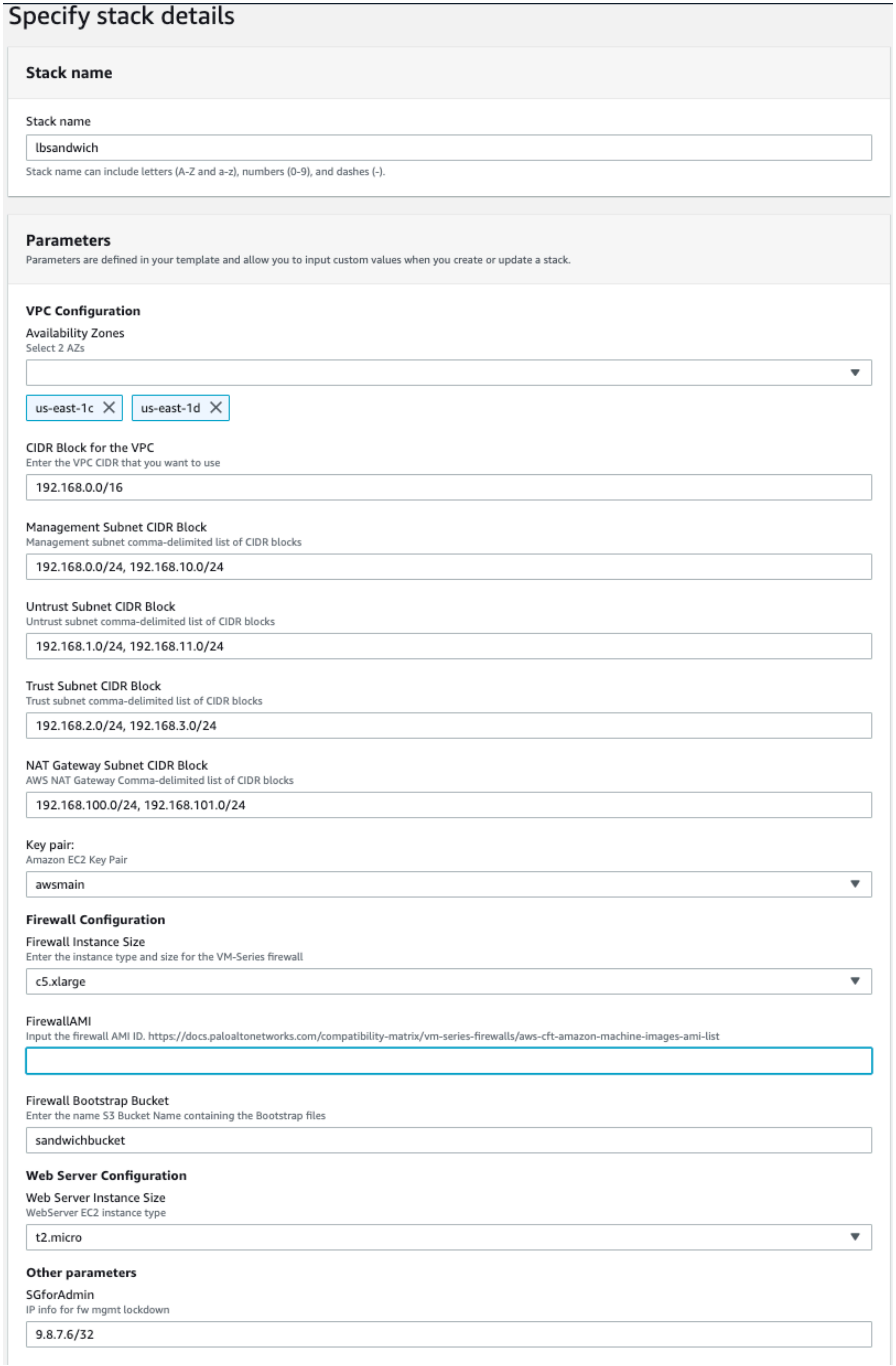
● Upload a template to Amazon S3

lb sandwich ...nternal.json

Specify the Details of the Stack.

- Stack Name
- Select 2 Availability Zones
- 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



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

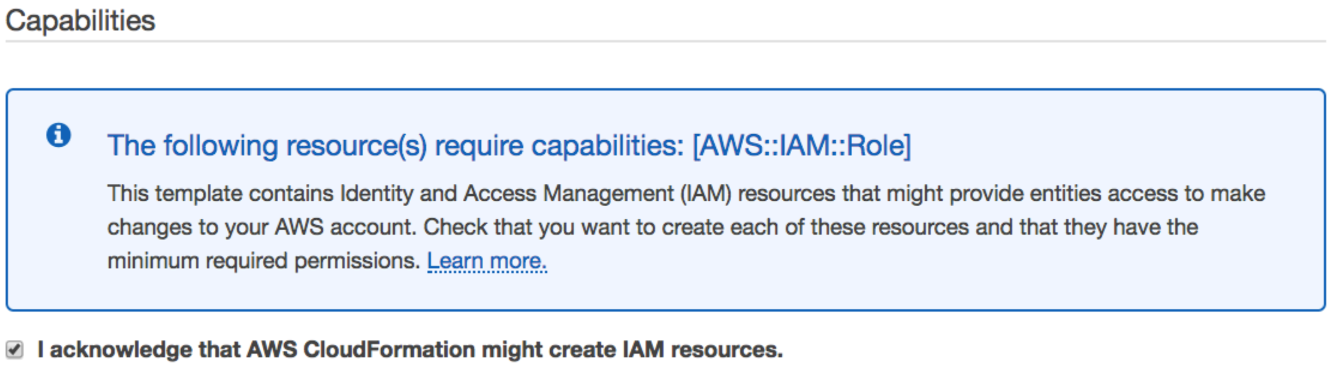
Other parameters

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

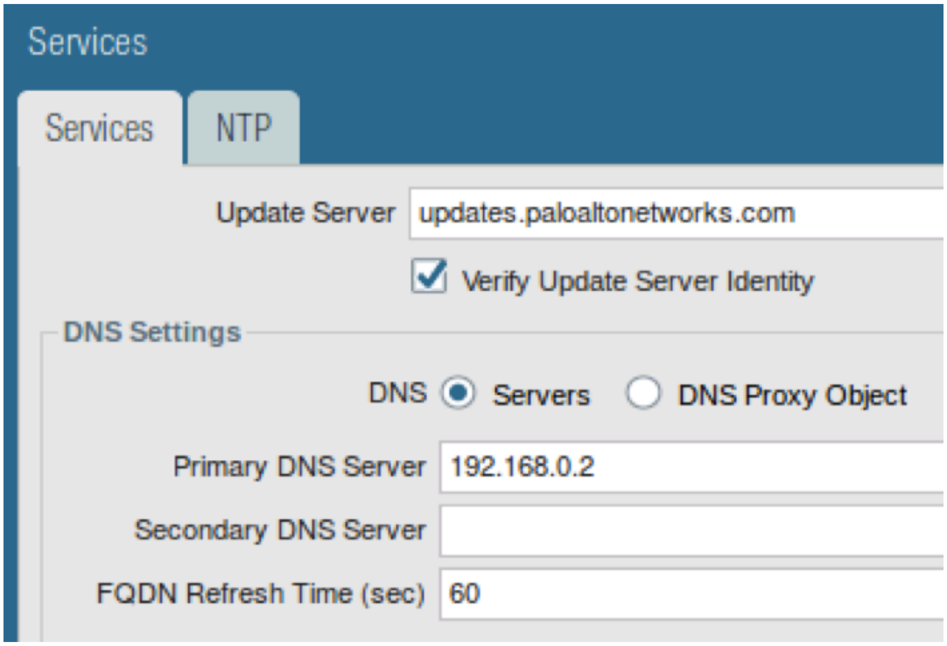
Using Firefox on the Jumphost, access the Management IPs of the Firewalls. This will be ETH1 on the AWS Firewall Instance Details.

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.



Update Server: updates.paloaltonetworks.com

☑ Verify Update Server Identity

DNS ● Servers ○ DNS Proxy Object

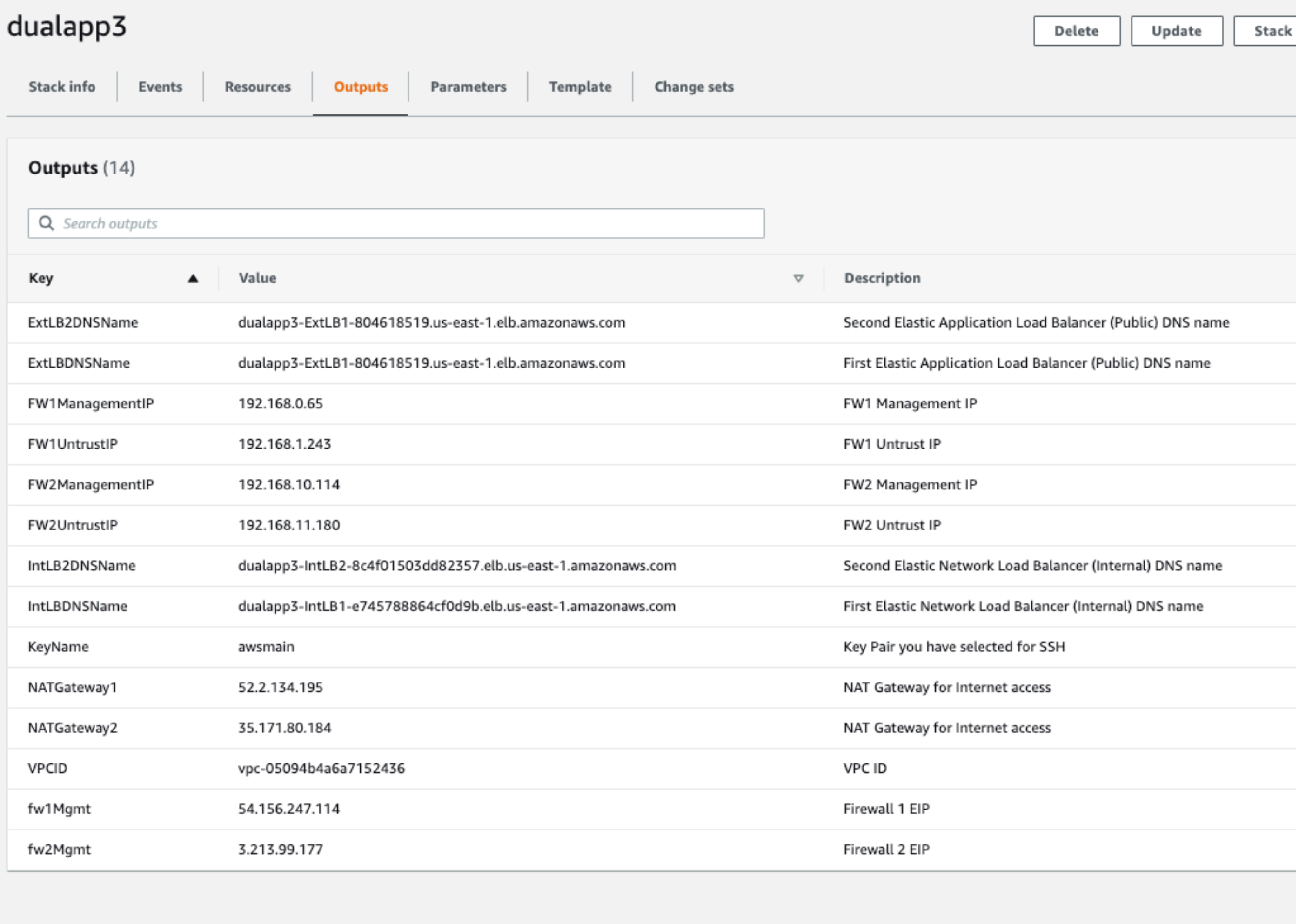
Primary DNS Server: 192.168.0.2

Secondary DNS Server:

FQDN Refresh Time (sec): 60

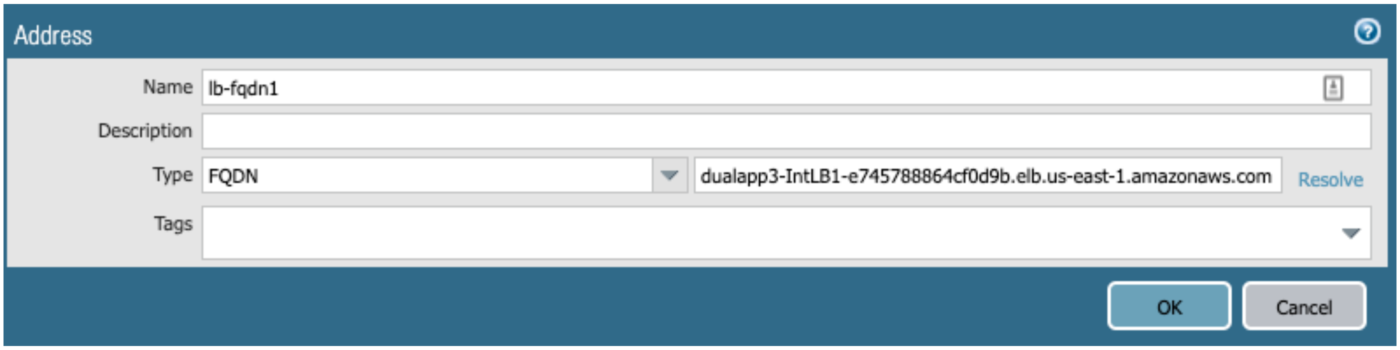
Move to the Objects Tab.

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



Outputs (14)

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



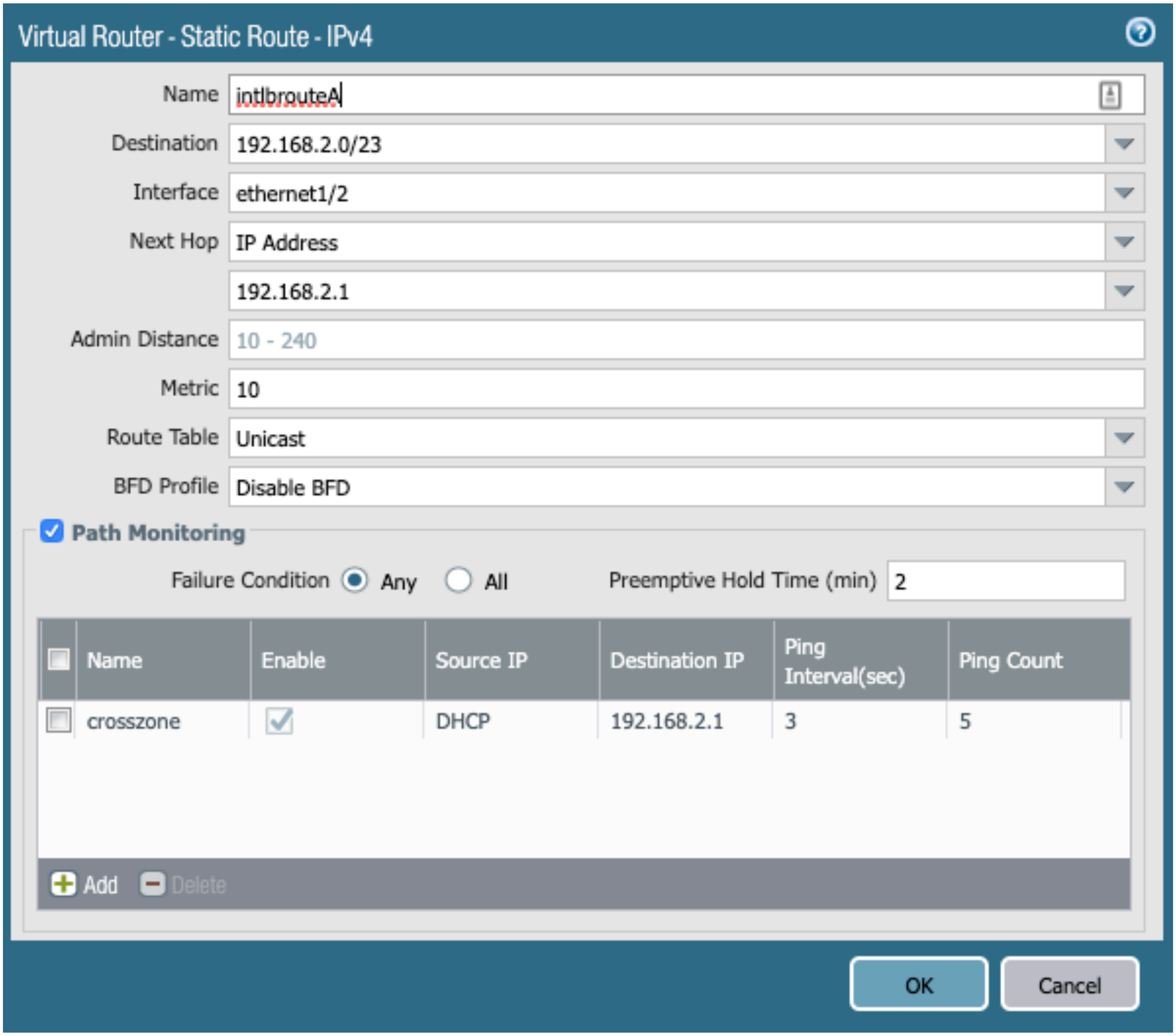
Name	lb-fqdn1
Description	
Type	FQDN dualapp3-IntLB1-e745788864cf0d9b.elb.us-east-1.amazonaws.com
Tags	

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.



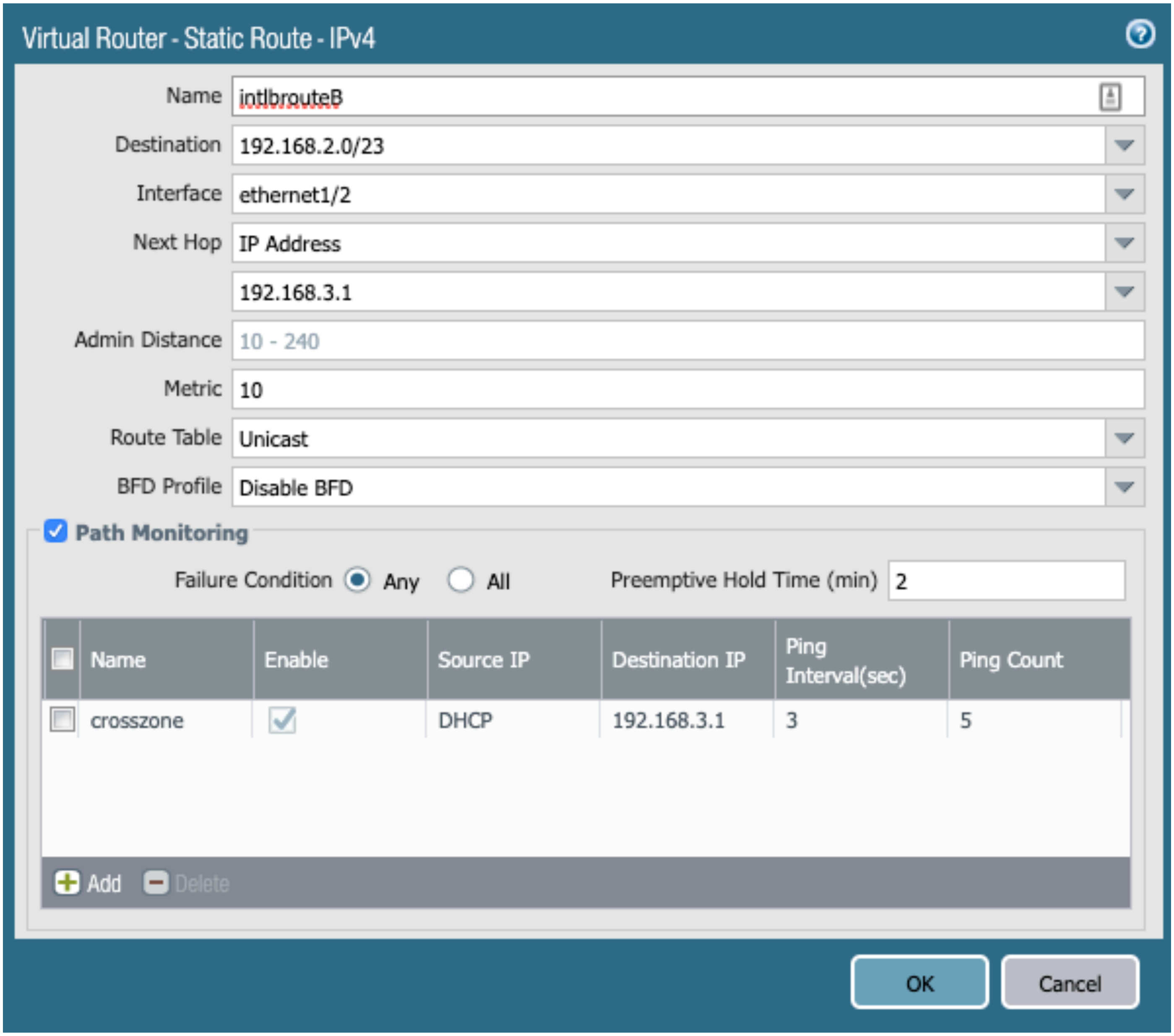
Virtual Router - Static Route - IPv4

Name	intlbrouteA
Destination	192.168.2.0/23
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

Failure Condition ● Any ○ All Preemptive Hold Time (min) 2

□	Name	Enable	Source IP	Destination IP	Ping Interval(sec)	Ping Count
□	crosszone	☑	DHCP	192.168.2.1	3	5



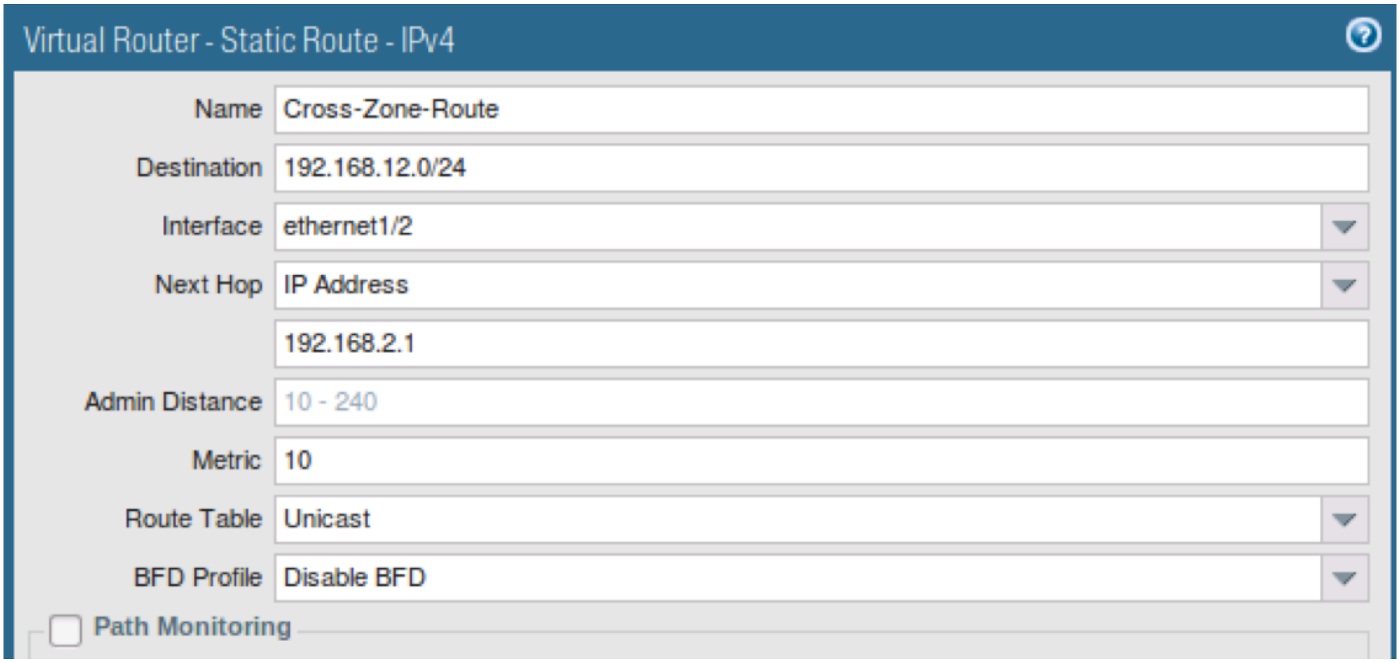
Virtual Router - Static Route - IPv4

Name	intlbrouteB
Destination	192.168.2.0/23
Interface	ethernet1/2
Next Hop	IP Address
	192.168.3.1
Admin Distance	10 - 240
Metric	10
Route Table	Unicast
BFD Profile	Disable BFD

☑ Path Monitoring

Failure Condition ● Any ○ All   Preemptive Hold Time (min) 2

□	Name	Enable	Source IP	Destination IP	Ping Interval(sec)	Ping Count
□	crosszone	☑	DHCP	192.168.3.1	3	5



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

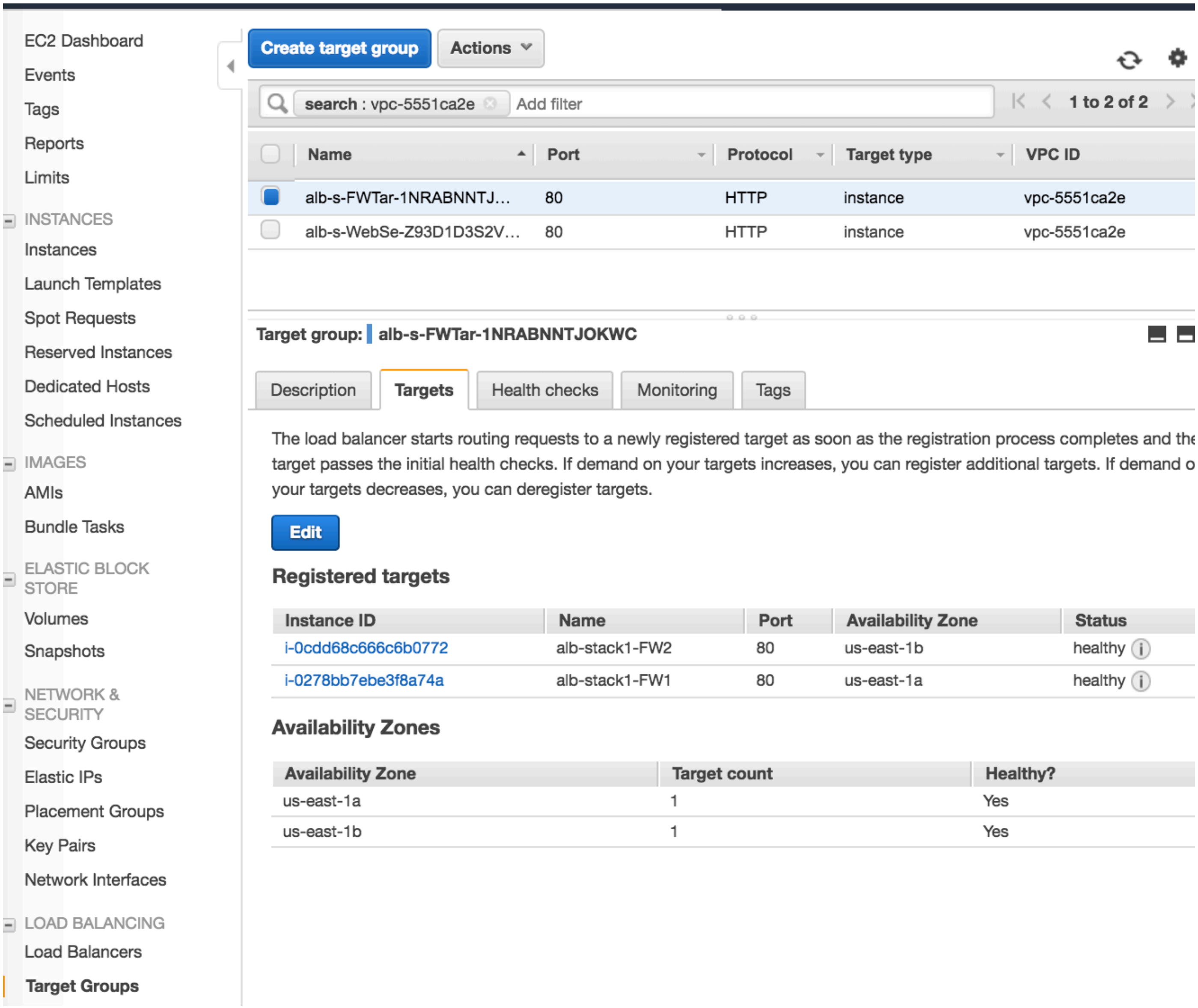
□ Path Monitoring

Commit the Policy.

Repeat Steps on the other Firewall.

7. Verify the Results

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



	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

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 o your targets decreases, you can deregister targets.

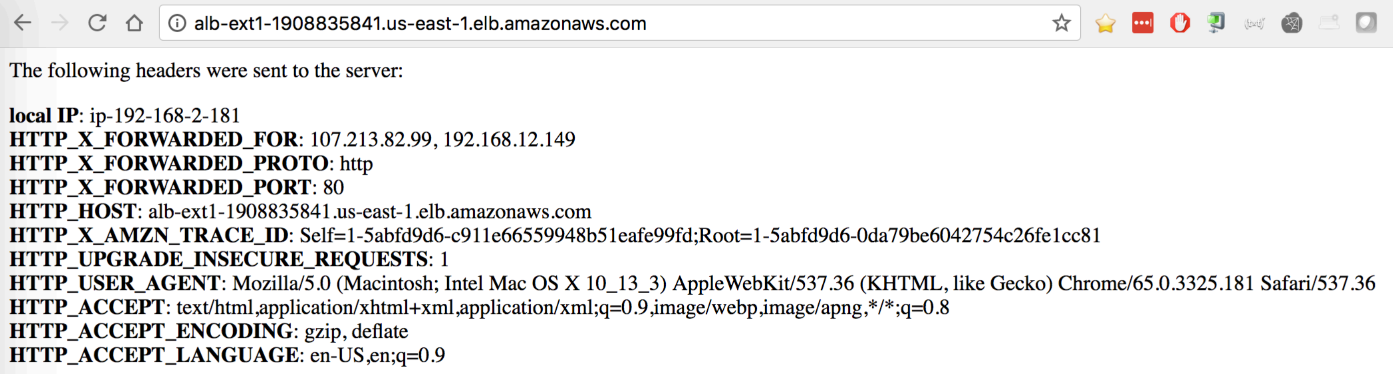
Registered targets

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

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

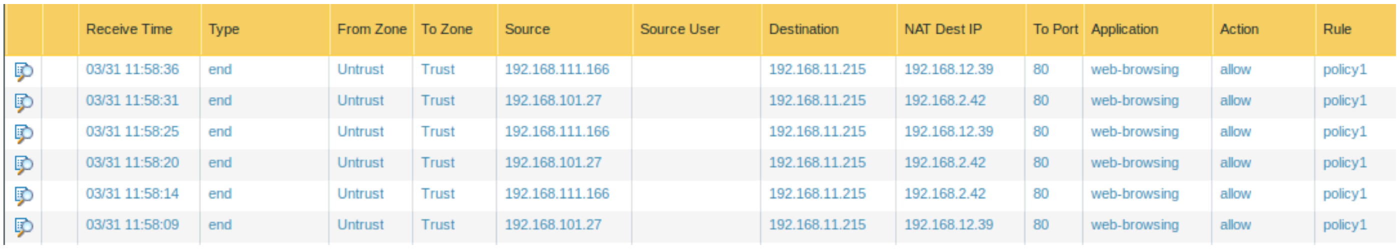


alb-ext1-1908835841.us-east-1.elb.amazonaws.com

```
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.

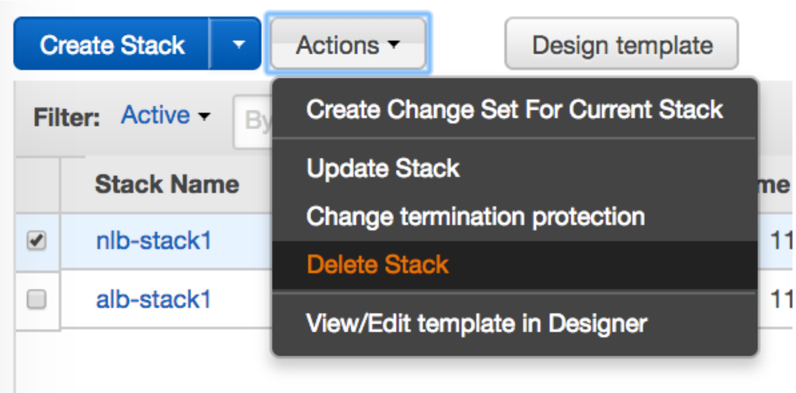


		Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	NAT Dest IP	To Port	Application	Action	Rule
		03/31 11:58:36	end	Untrust	Trust	192.168.111.166		192.168.11.215	192.168.12.39	80	web-browsing	allow	policy1
		03/31 11:58:31	end	Untrust	Trust	192.168.101.27		192.168.11.215	192.168.2.42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

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 webservers 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