
# 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



Last Update: May 2016

# Table of Contents

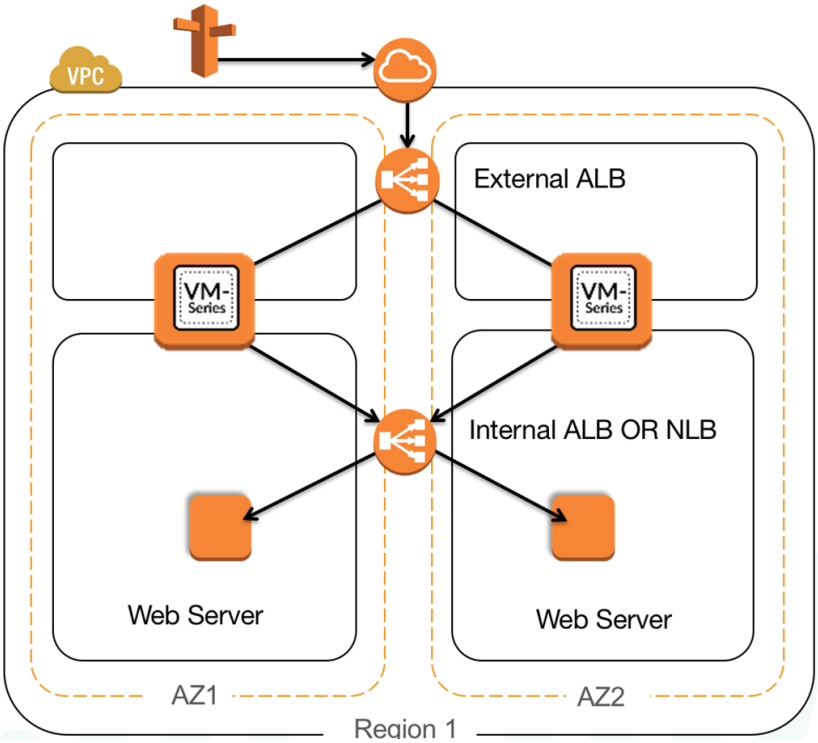
# Version History

| Version number | Comments |
|---|---|
| **1.0** | Initial Draft |
| | |

# 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 an external Application Load Balancer and either an internal Application Load Balancer or Network Load Balancer depending on which CFT is chosen.




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 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 | 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 templates 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

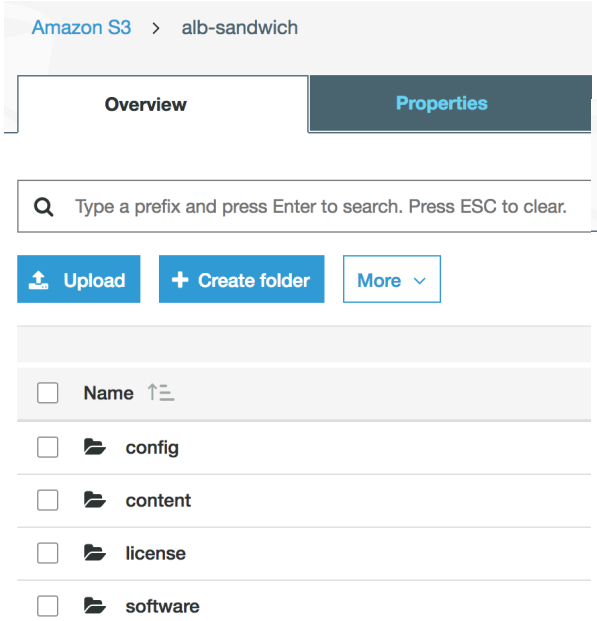
## 4.4 Download GitHub Files

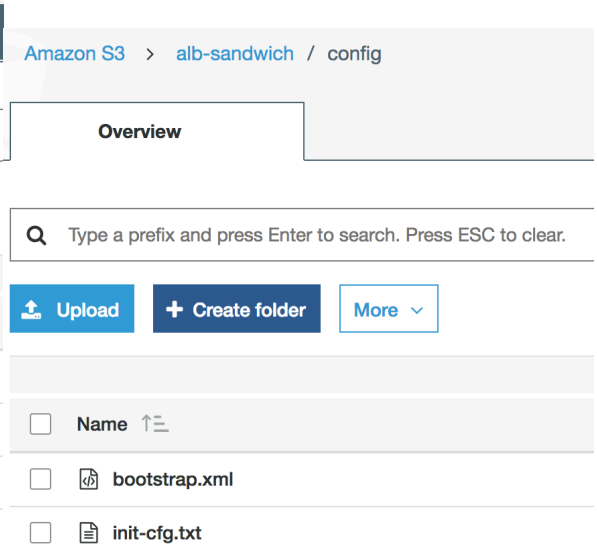
Download *.json files, *.xml and init-cfg.txt files from Github to a local directory.

## 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.

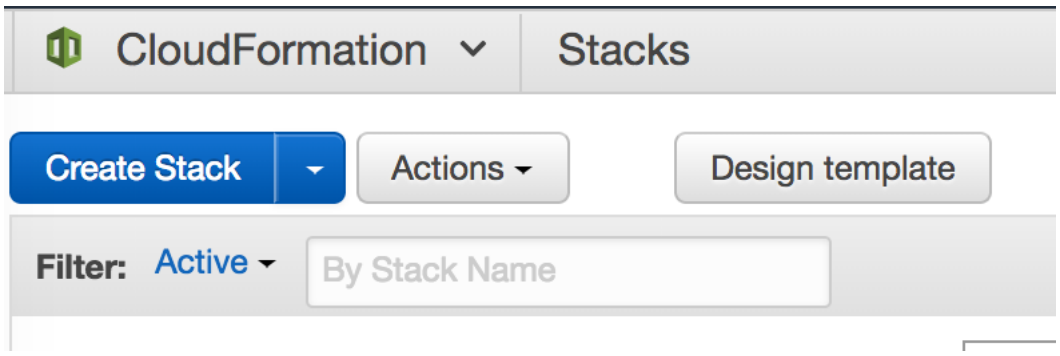


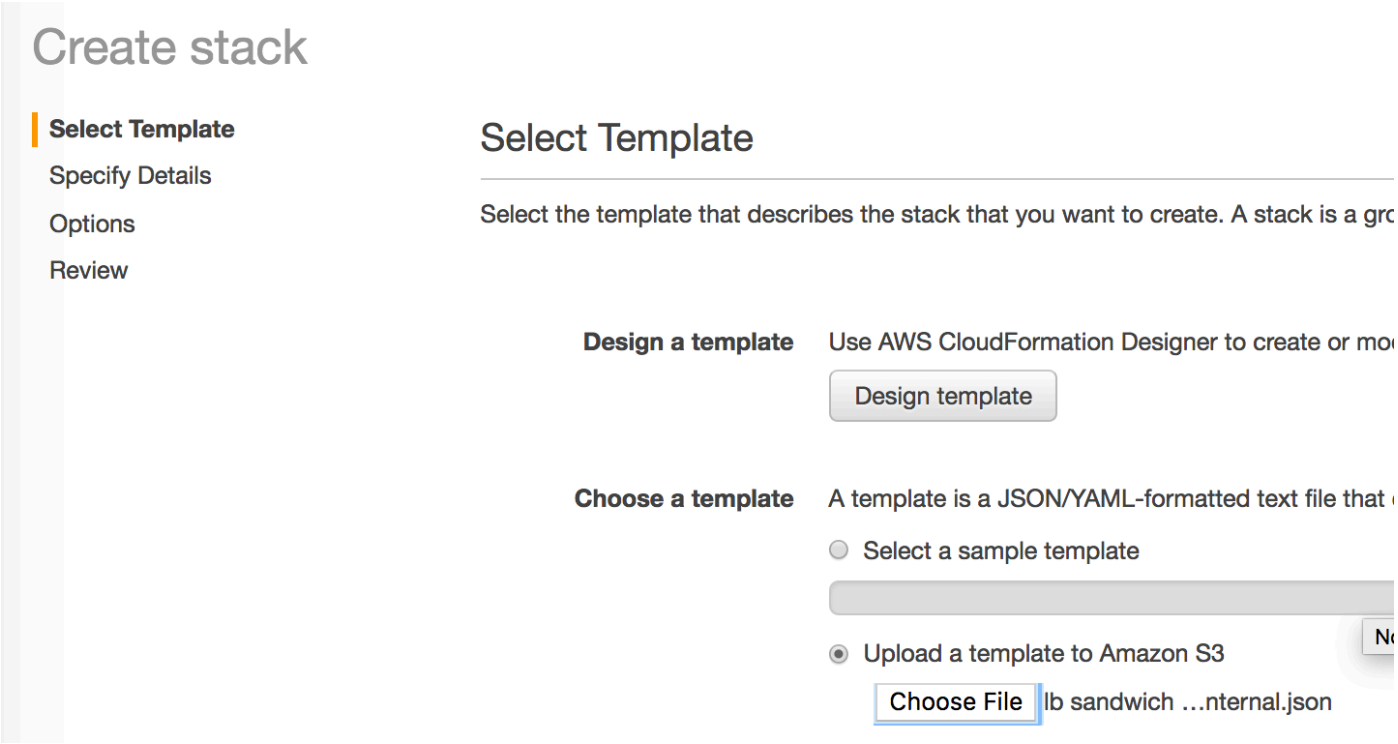

**NOTE: Please create the folders using the console. Creating folders locally on your machine and uploading them may not work as expected.**

# 5. Launch the Template

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



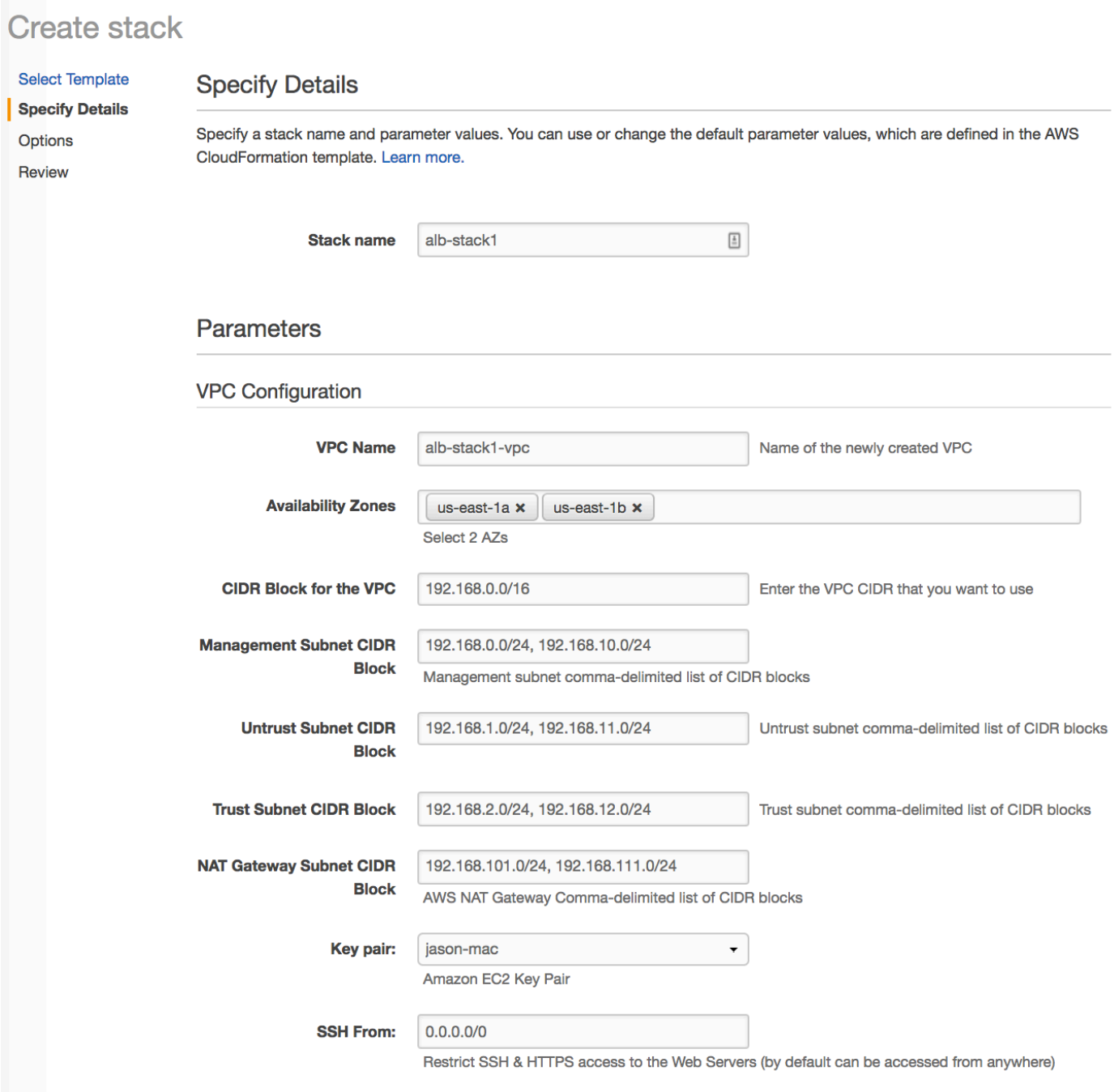

On the Select Template page, hit Choose File and select the appropriate template downloaded from GitHub Repository.




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. 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



Firewall Configuration

| | | |
|---|---|---|
| **FWLicenseType** | Bundle1 | Enter the license type for the Firewall |
| **Firewall Instance Size** | m4.xlarge<br>Enter the instance type and size for the VM-Series firewall | |
| **Firewall Bootstrap Bucket** | alb-sandwich<br>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.

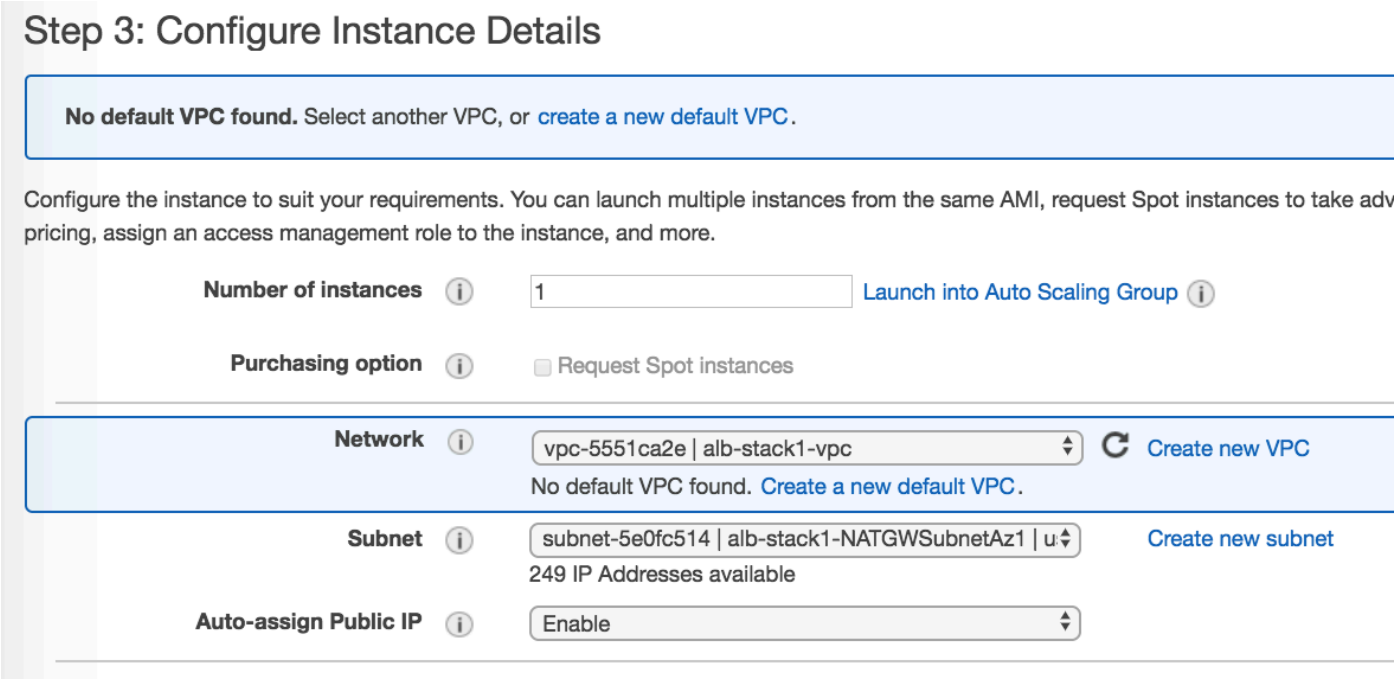
Access EC2 and hit Launch Instance. Select AWS Marketplace on the lefthand menu and Search for “Mint” and Select “Linux Mint Serena Desktop HVM”

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




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**

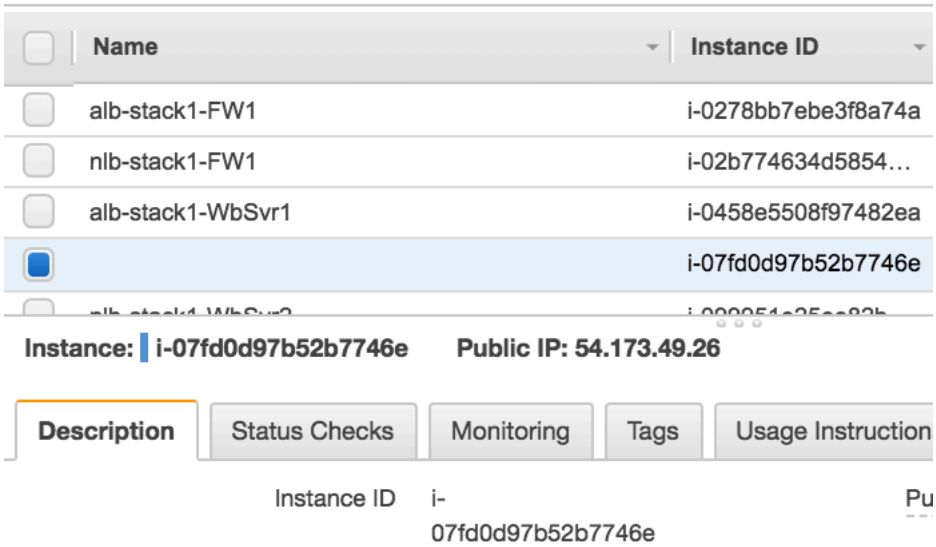
# 7. Access the Jumphost

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




RDP to the Instance.

# 8. Update the Firewalls

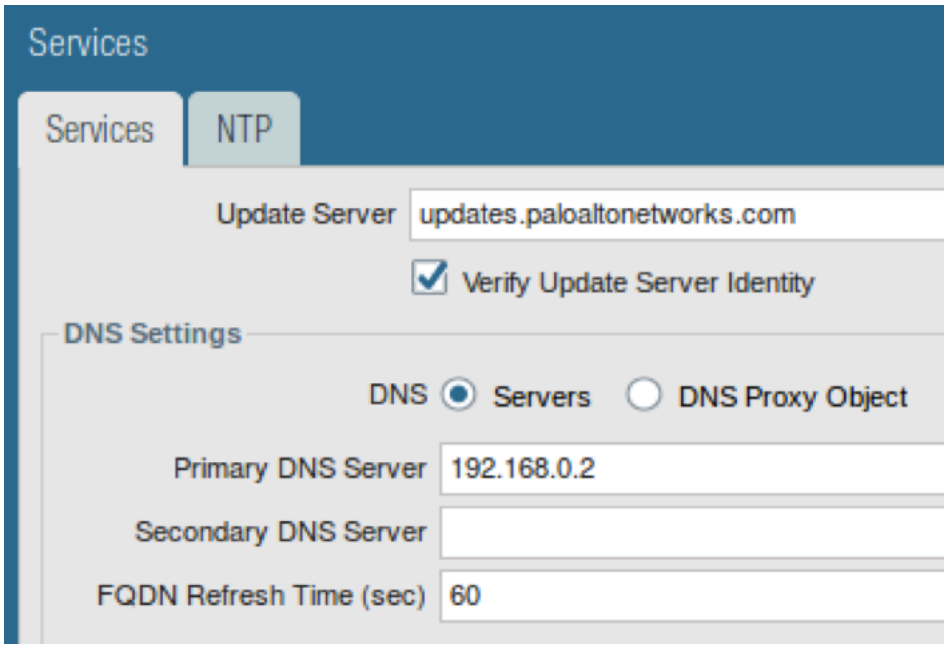
Using Firefox on the Jumphost, access the Management IPs of the Firewalls. This will be ETH1 on the AWS Firewall Instance Details.

Username: pandemo Password:demopassword

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

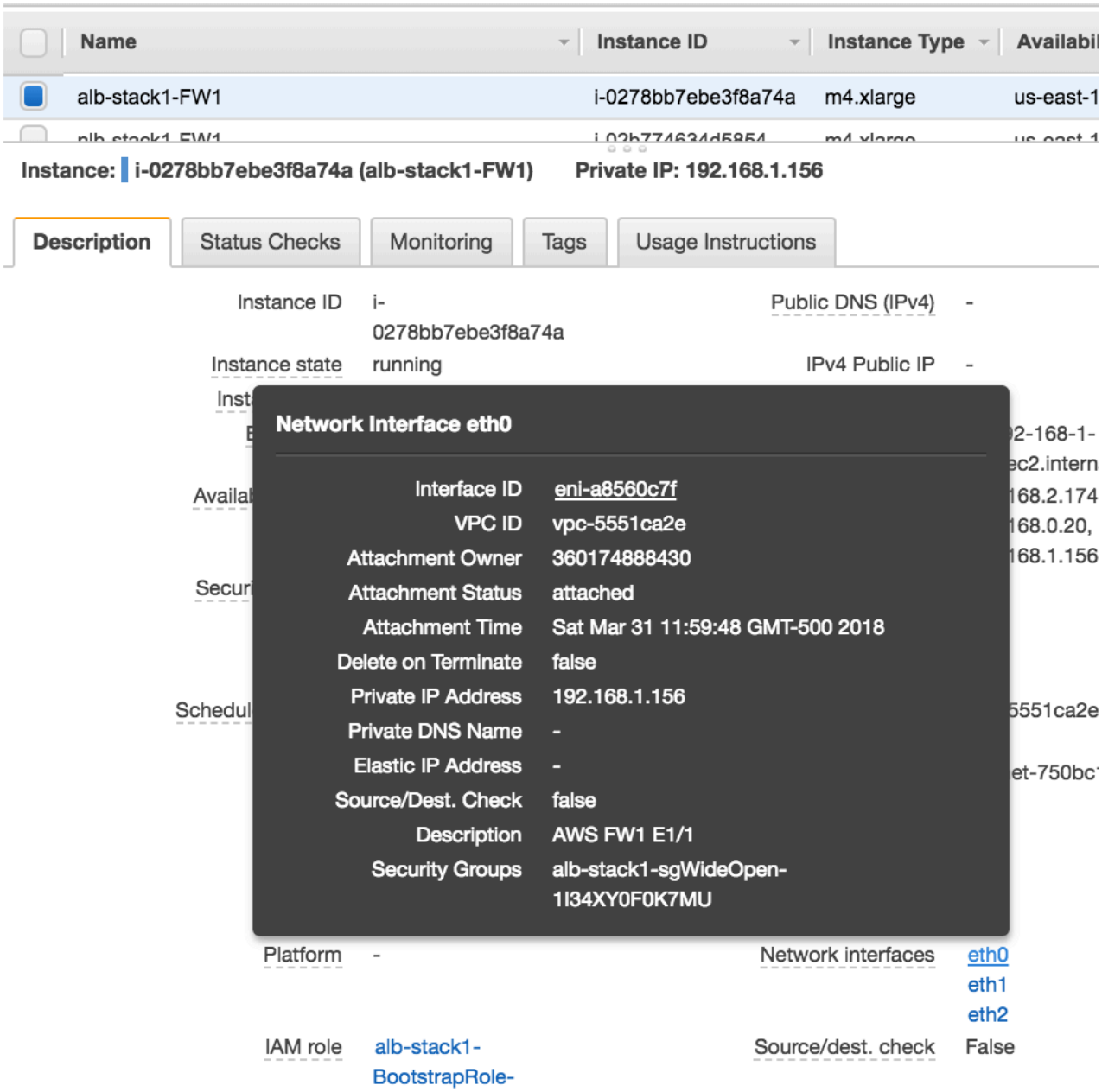
Access Device -> Setup -> Services and hit the Gear Icon.

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

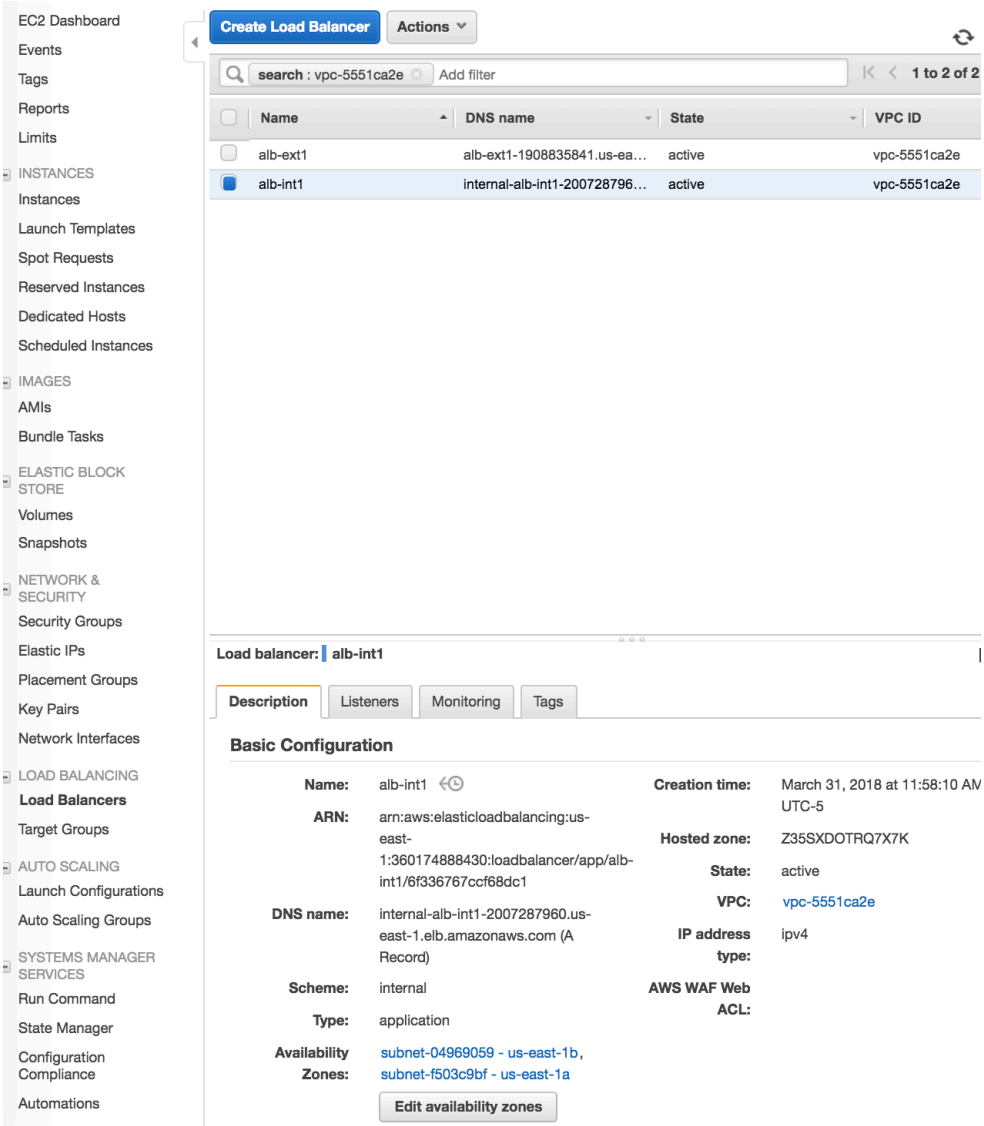


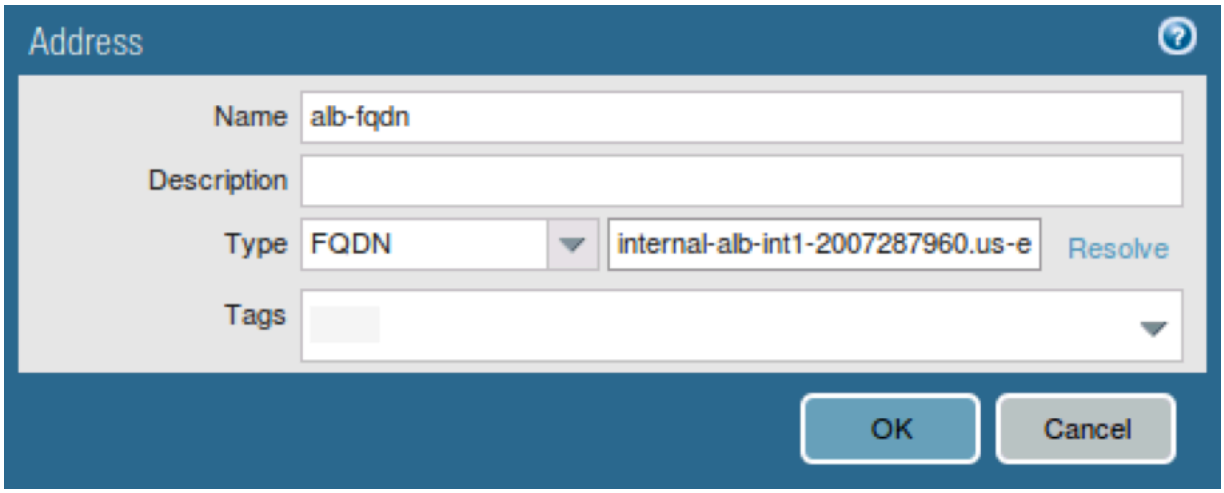

Move to the Objects Tab.

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




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

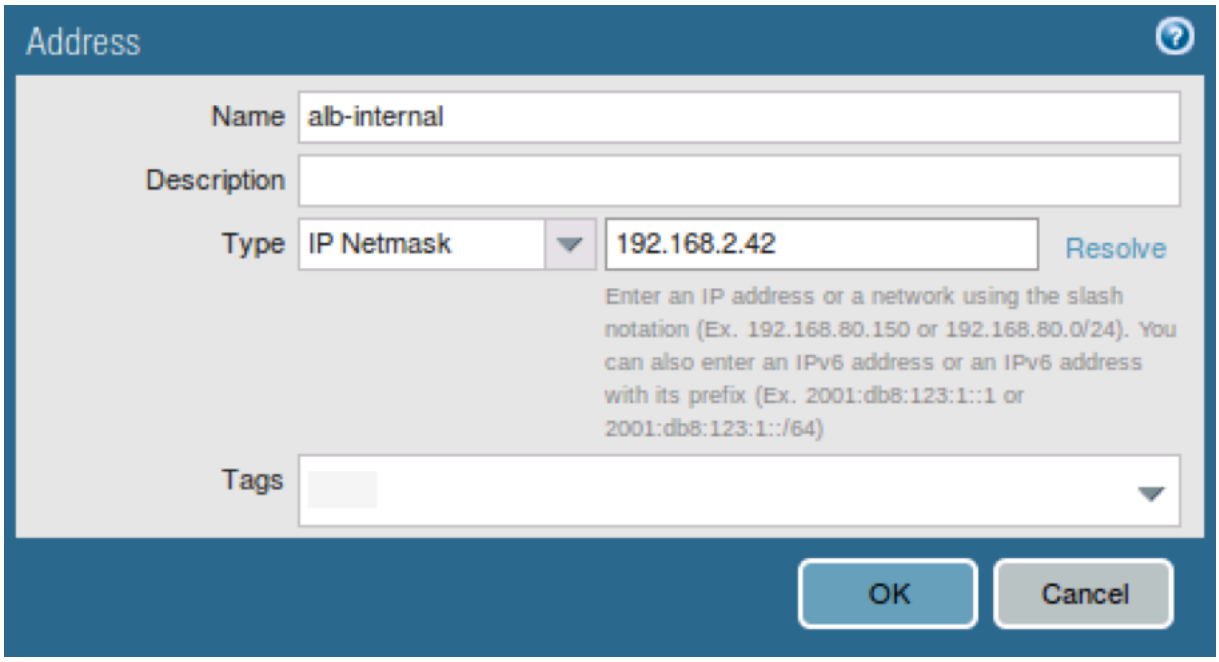

EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Launch Templates
Spot Requests
Reserved Instances
Dedicated Hosts
Scheduled Instances
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
LOAD BALANCING
Load Balancers
Target Groups
AUTO SCALING
Launch Configurations
Auto Scaling Groups
SYSTEMS MANAGER SERVICES
Run Command
State Manager
Configuration Compliance
Automations
Create Load Balancer
Actions
search : vpc-5551ca2e
Add filter
1 to 2 of 2
Name
DNS name
State
VPC ID
alb-ext1
alb-ext1-1908835841.us-ea...
active
vpc-5551ca2e
alb-int1
internal-alb-int1-200728796...
active
vpc-5551ca2e
Load balancer: alb-int1
Description
Listeners
Monitoring
Tags
Basic Configuration
Name: alb-int1
ARN: arn:aws:elasticloadbalancing:us-east-1:360174888430:loadbalancer/app/alb-int1/6f336767ccf68dc1
DNS name: internal-alb-int1-2007287960.us-east-1.elb.amazonaws.com (A Record)
Scheme: internal
Type: application
Availability Zones: subnet-04969059 - us-east-1b, subnet-f503c9bf - us-east-1a
Edit availability zones
Creation time: March 31, 2018 at 11:58:10 AM UTC-5
Hosted zone: Z35SXDOTRQ7X7K
State: active
VPC: vpc-5551ca2e
IP address type: ipv4
AWS WAF Web ACL:


Address
Name
alb-fqdn
Description
Type
FQDN
internal-alb-int1-2007287960.us-e
Resolve
Tags
OK
Cancel

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 ~ $
```

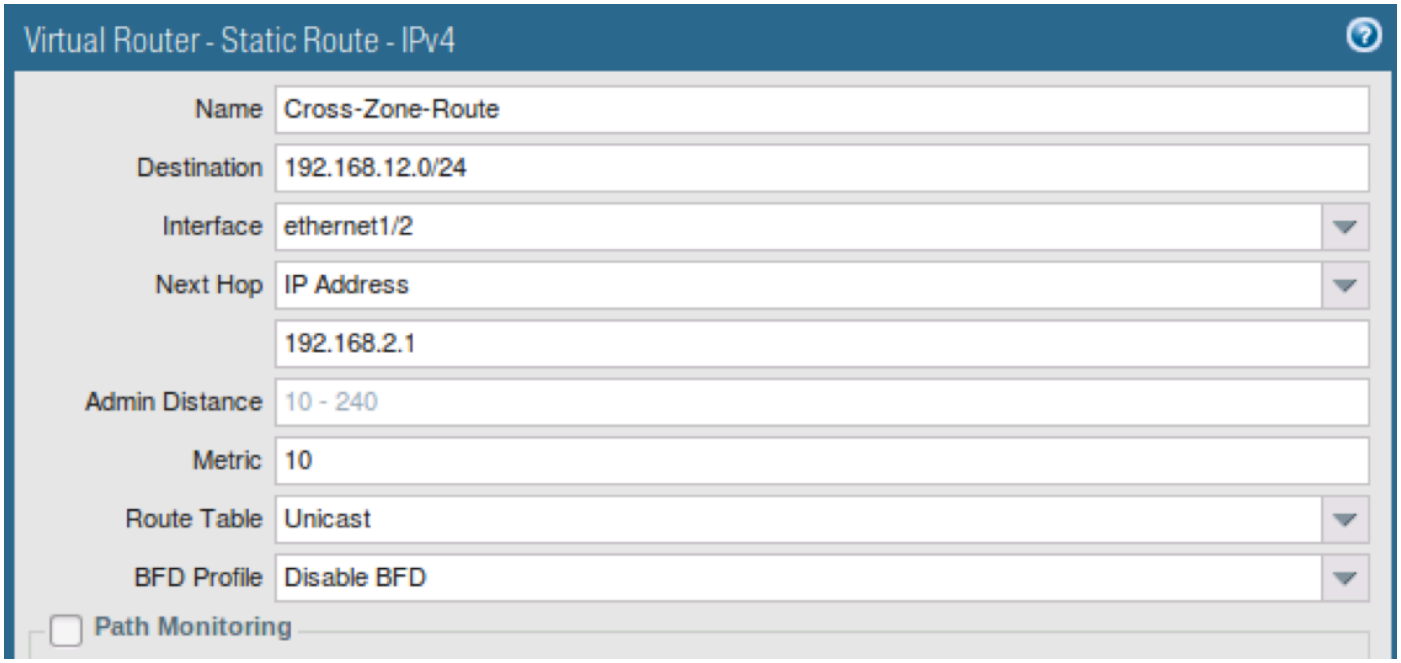
Update the “alb-internal” object with IP in the corresponding Availability Zone.




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.




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.

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 | 1 to 2 of 2

| 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 o your targets decreases, you can deregister targets.

Edit

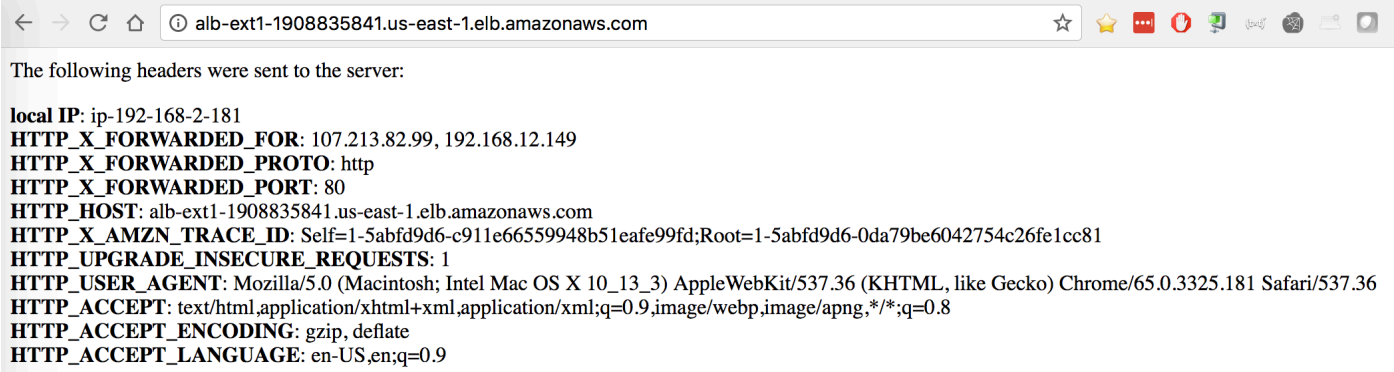
**Registered targets**

| 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 |

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



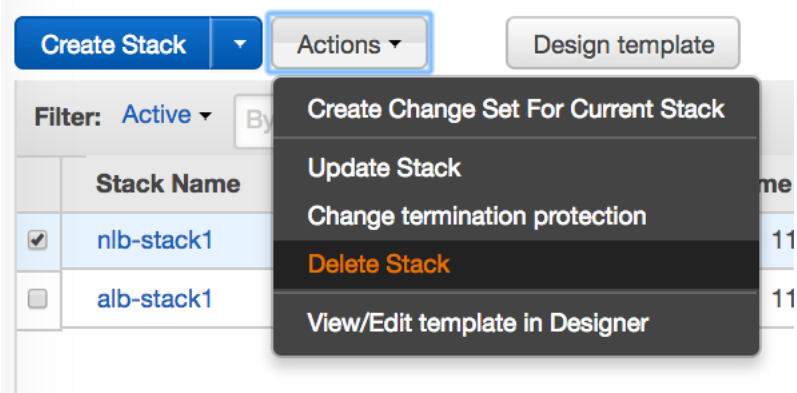

Review the Firewall Monitor to Ensure the Application is successfully resolving to web-browsing.

| | | 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 |

# 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 PAN-OS 8.1.

# Appendix A