**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](#_Toc510269804)

[1. About 4](#_Toc510269805)

[2. Support Policy 5](#_Toc510269806)

[3. Implementation Details 5](#_Toc510269807)

[4. Prerequisites 5](#_Toc510269808)

[4.1 Create AWS account 6](#_Toc510269809)

[4.2 Version 8.1 or Greater 6](#_Toc510269810)

[4.3 Accept the EULA 6](#_Toc510269811)

[4.4 Download GitHub Files 6](#_Toc510269812)

[4.5 Create a Bootstrap Bucket 6](#_Toc510269813)

[5. Launch the Template 8](#_Toc510269814)

[6. Deploy Jumphost 11](#_Toc510269815)

[7. Access the Jumphost 13](#_Toc510269816)

[8. Update the Firewalls 13](#_Toc510269817)

[9. Verify the Results 19](#_Toc510269818)

[10. Cleanup 21](#_Toc510269819)

[10.1 Delete the deployment 21](#_Toc510269820)

[11. Conclusion 21](#_Toc510269821)

[Appendix A 22](#_Toc510269822)

# Version History

|  |  |
| --- | --- |
| Version number | Comments |
| 1.0 | Initial Draft |
| 1.1 | Dual Stack |

# 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. A close up of a map

Description automatically generated

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.

# 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.

# 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.

# Prerequisites

Here are the prerequisites required to successfully launch this template:

## 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.

## 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.

## Accept the EULA

Accept the EULA for the VM-Series PAYG license bundle you plan to use.  
[VM-Series firewall Bundle 2](https://aws.amazon.com/marketplace/pp/B00PJ2V04O)  
[VM-Series firewall Bundle 1](https://aws.amazon.com/marketplace/pp/B00PJ2VDFA)

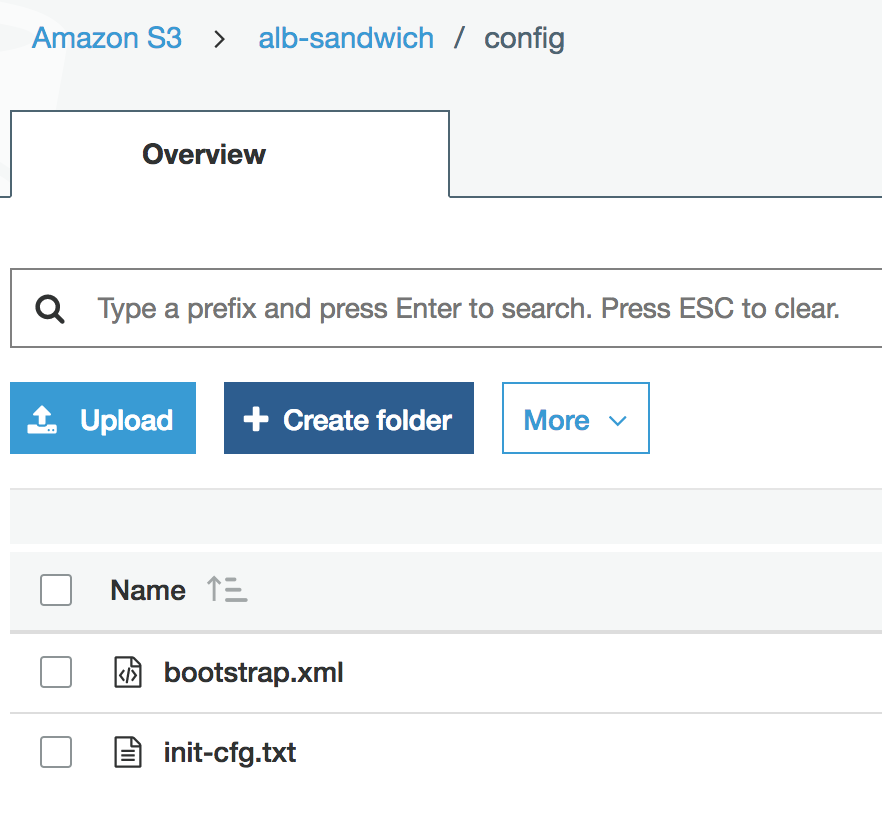
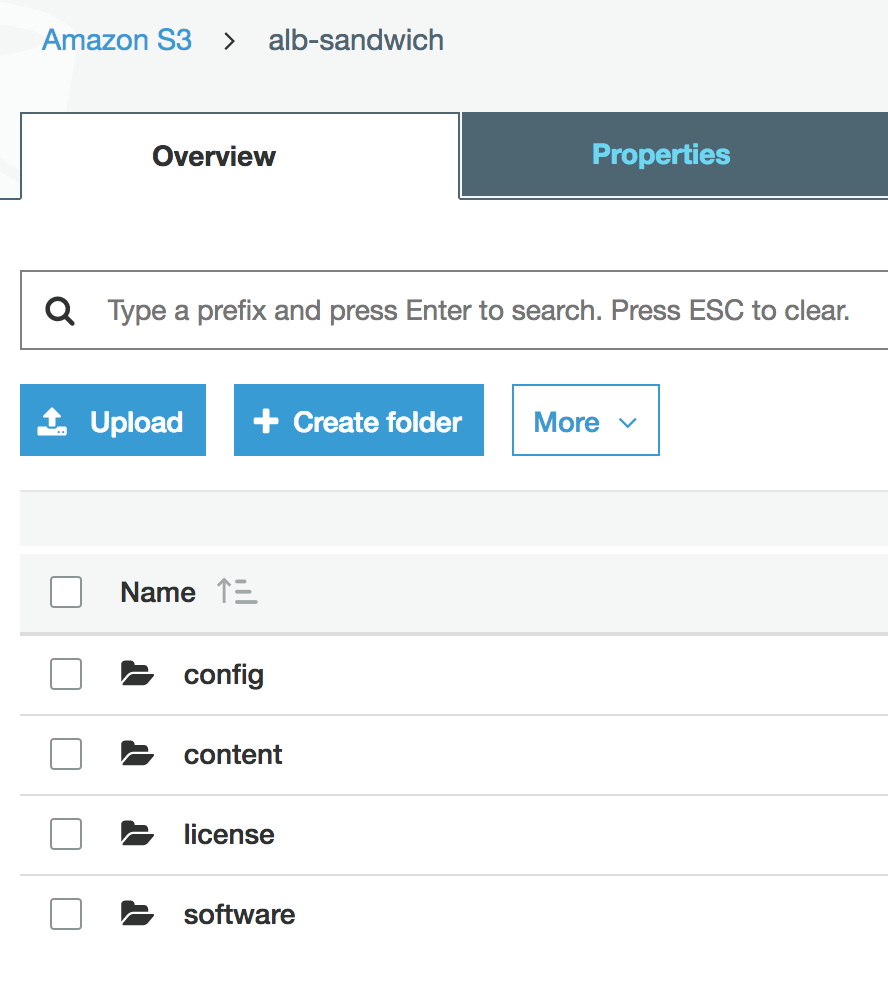
## Download GitHub Files

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

## 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.

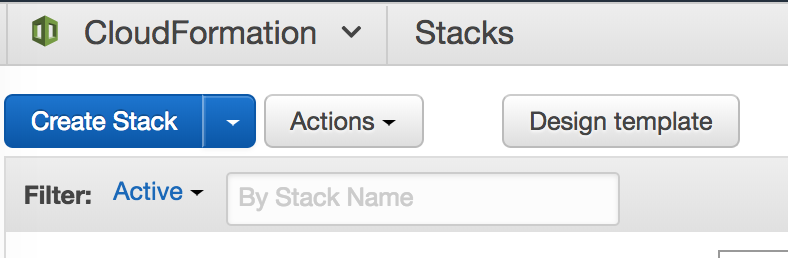
In the AWS S3 console, create bucket with config, content, license and software folders. Upload the init-cfg.txt file from the repository to the config folder. Additionally, upload the corresponding alb-\*lb.xml file as bootstrap.xml.



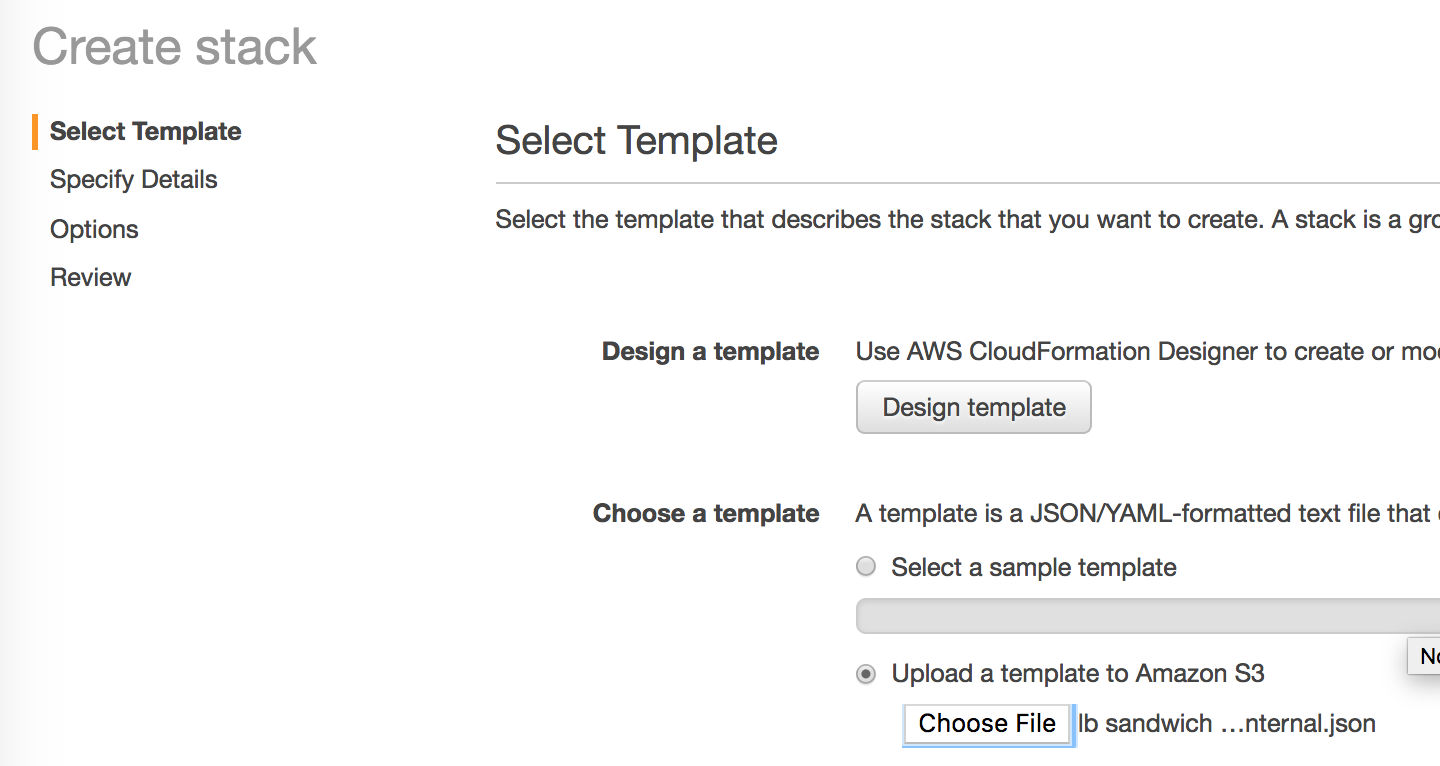
**NOTE: Please create the folders using the console. Creating folders locally on your machine and uploading them may not work as expected.**

# 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.

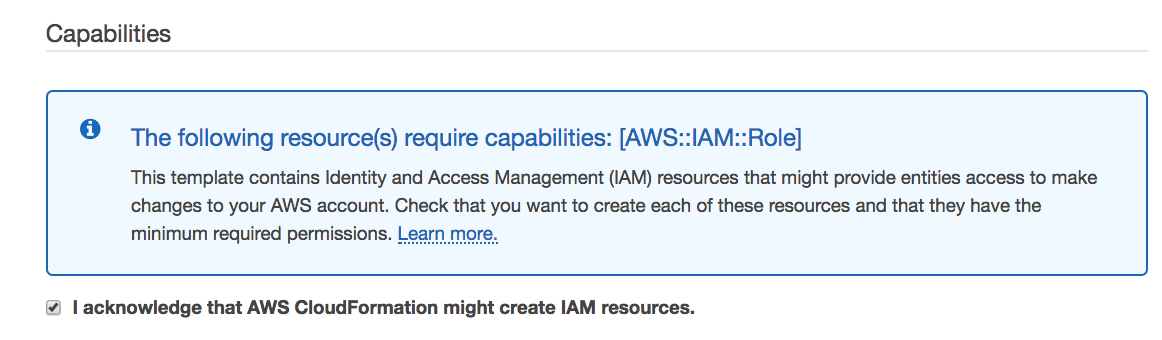
* Stack Name
* Select 2 Availability Zones
* Subnet Details for the VPC, Management, Untrust, Trust and Nat Gateway Subnets.
* Key Pair
* SSH From for Management Security lockdown
* Firewall AMI
* Firewall Instance Size
* Bootstrap Bucket Name previous created.
* Web Server Instance Size

A screenshot of a cell phone

Description automatically generated

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.



# Update the Firewalls

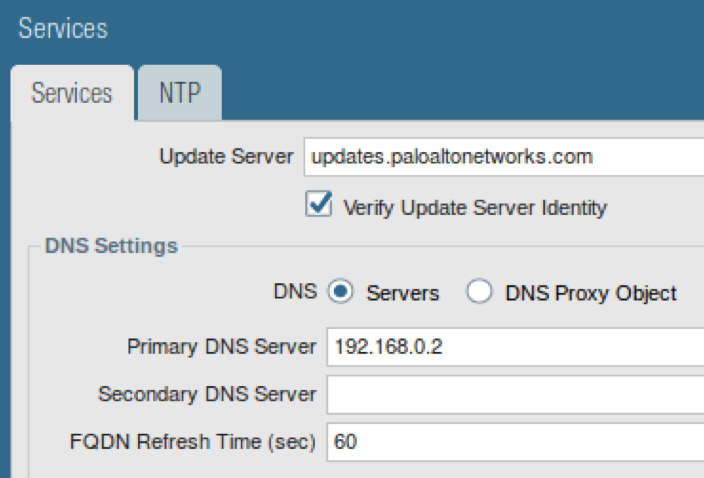
Using Firefox on the Jumphost, access the Management IPs of the Firewalls. This will be ETH1 on the AWS Firewall Instance Details.

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

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

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

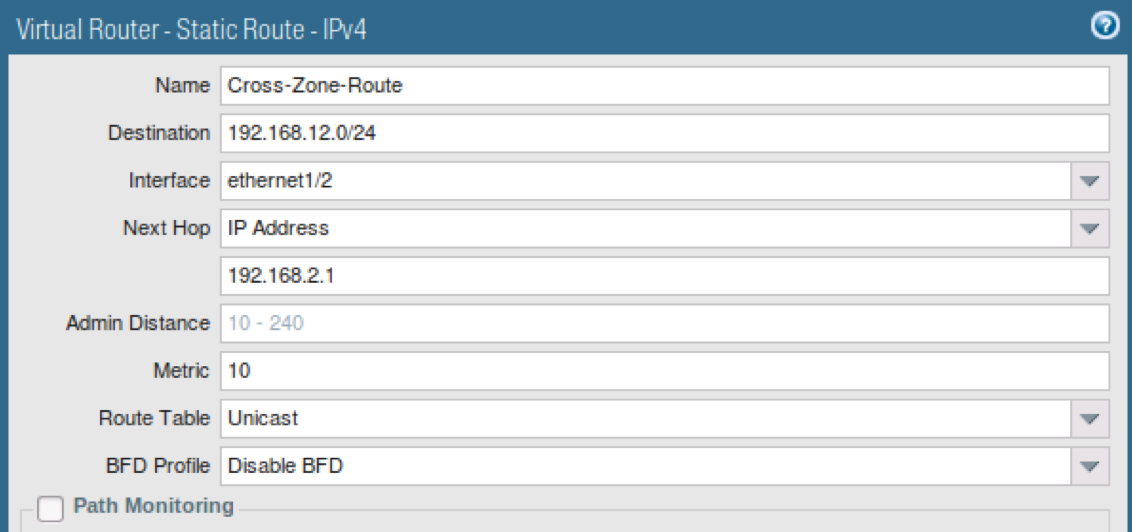
Access Network -> Virtual Routers and open the “default” Virtual Router.

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.

A screenshot of a social media post

Description automatically generatedA screenshot of a social media post

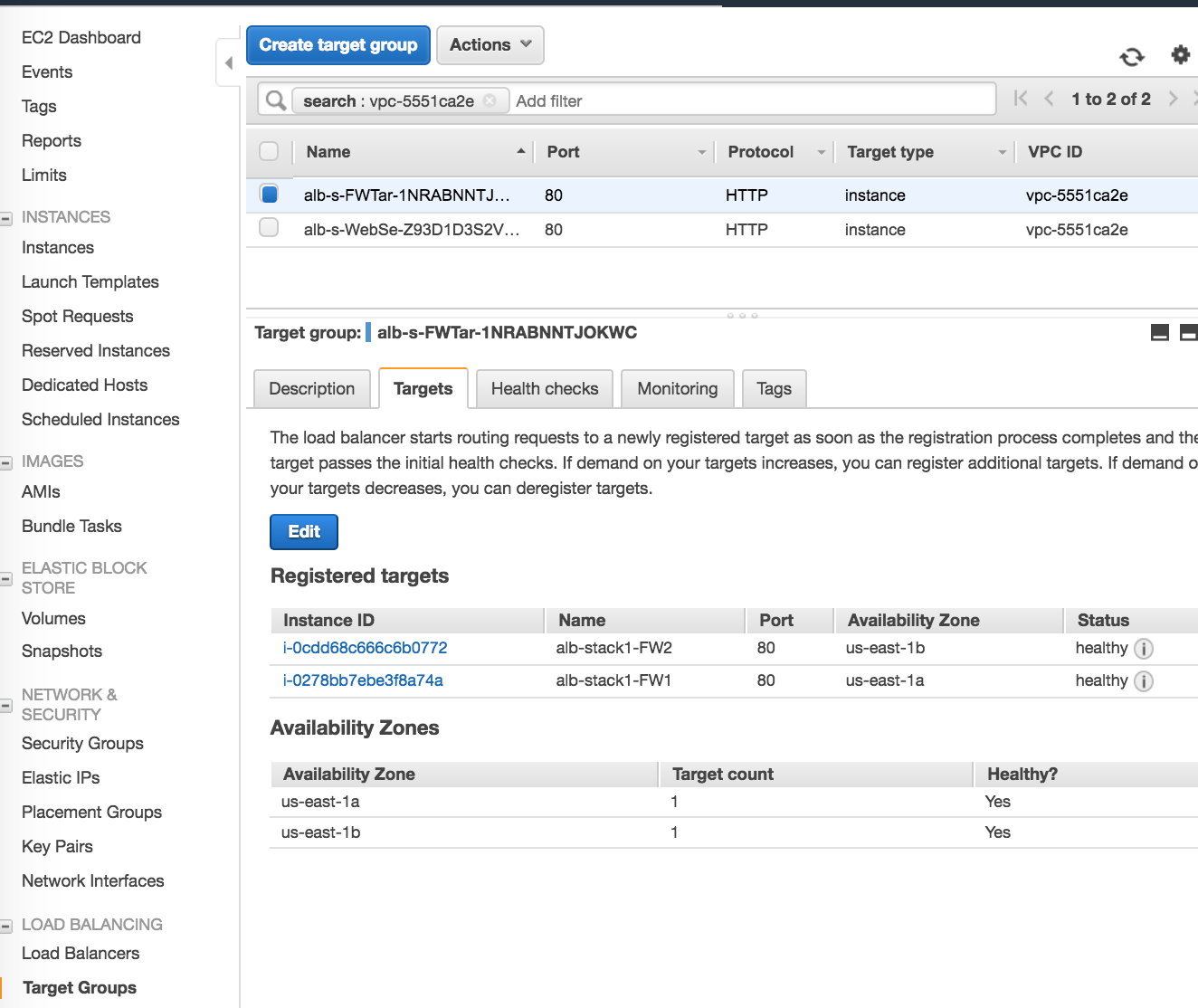
Description automatically generated

Commit the Policy.

Repeat Steps on the other Firewall.

# Verify the Results

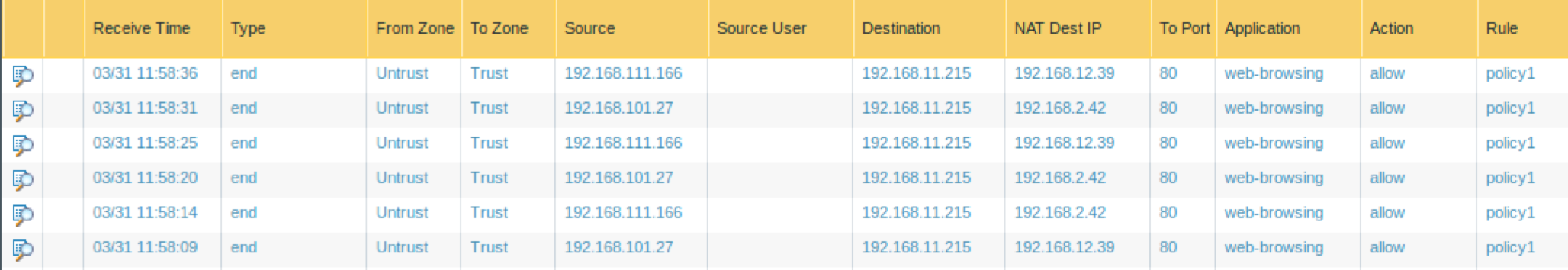
Review the Target Groups in EC2 to ensure the Targets are Healthy.



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



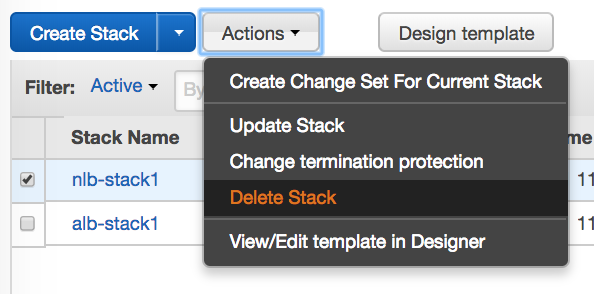
Review the Firewall Monitor to Ensure the Application is successfully resolving to web-browsing.



# Cleanup

## 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.

# 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