

Auto Scale Template for VM-Series Firewall on AWS (Version 2.0)

Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal www.paloaltonetworks.com/documentation.
- To search for a specific topic, go to our search page www.paloaltonetworks.com/documentation/document-search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.

www.paloaltonetworks.com

© - Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

Table of Contents

Auto Scaling Template for VM-Series Firewall on AWS (Version 2.0)..... 4

 Auto Scale VM-Series Firewalls with the Amazon ELB Service.....5

 VM-Series Auto Scaling Template for AWS Version 2.0..... 7

 Launch the VM-Series Auto Scaling Template for AWS (v2.0)..... 11

 Launch the VM-Series Firewall Template..... 11

 Launch the Application Template..... 16

 Enable Traffic to the ELB Service..... 20

 Beta Known Issues..... 23

Palo Alto Networks delivers CloudFormation Templates to deploy an auto-scaling tier of VM-Series firewalls using several AWS services such as Lambda, auto scaling groups, Elastic Load Balancing (ELB), S3, and SNS, and the VM-Series automation capabilities including the PAN-OS API, native integration with AWS CloudWatch, and bootstrapping.

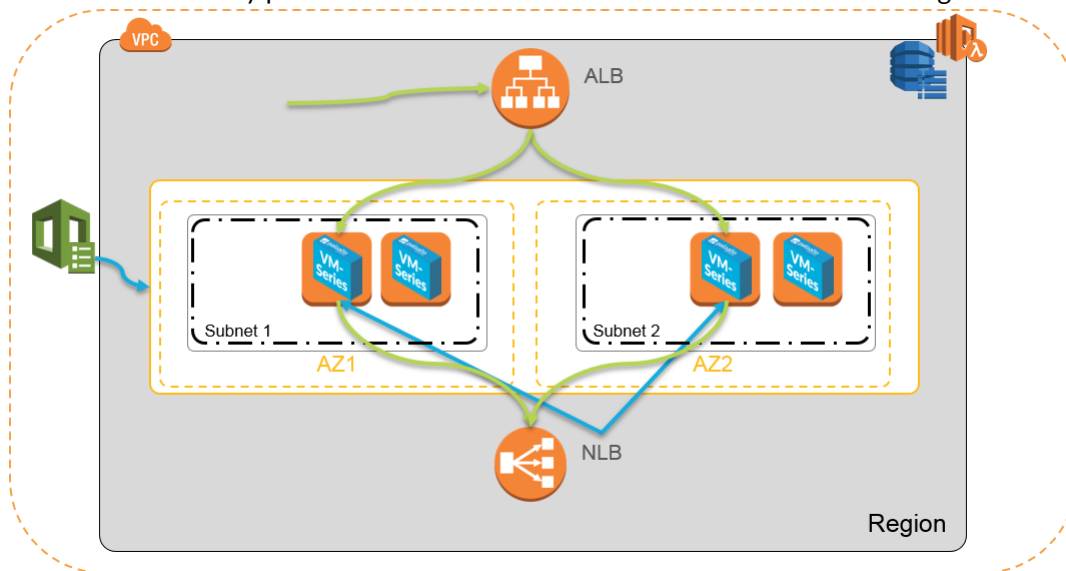
- [Auto Scale VM-Series Firewalls with the Amazon ELB Service](#)
- [VM-Series Auto Scaling Template for AWS Version 2.0](#)
- [Launch the VM-Series Auto Scaling Template for AWS \(v2.0\)](#)
- [Beta Known Issues](#)

Auto Scale VM-Series Firewalls with the Amazon ELB Service

The auto scaling template allows you to leverage the AWS scalability features designed to manage sudden surges in demand for application workload resources by simultaneously scaling the VM-Series firewalls with changing workloads.

To help you manage increased application scale, version 2.0 of the template provides two templates that with the network load balancer (instead of the application or classic load balancers included in earlier versions) as the internal load balancer and includes support for multi-VPC deployments within a single AWS account and cross-account deployments.

- **Firewall Template**—The firewall template deploys an application load balancer and VM-Series firewalls within auto scaling groups across two Availability Zones (AZs). This internet-facing application load balancer distributes traffic that enters the VPC across the pool of VM-Series firewalls. The VM-Series firewall automatically publishes custom PAN-OS metrics that enable auto scaling.



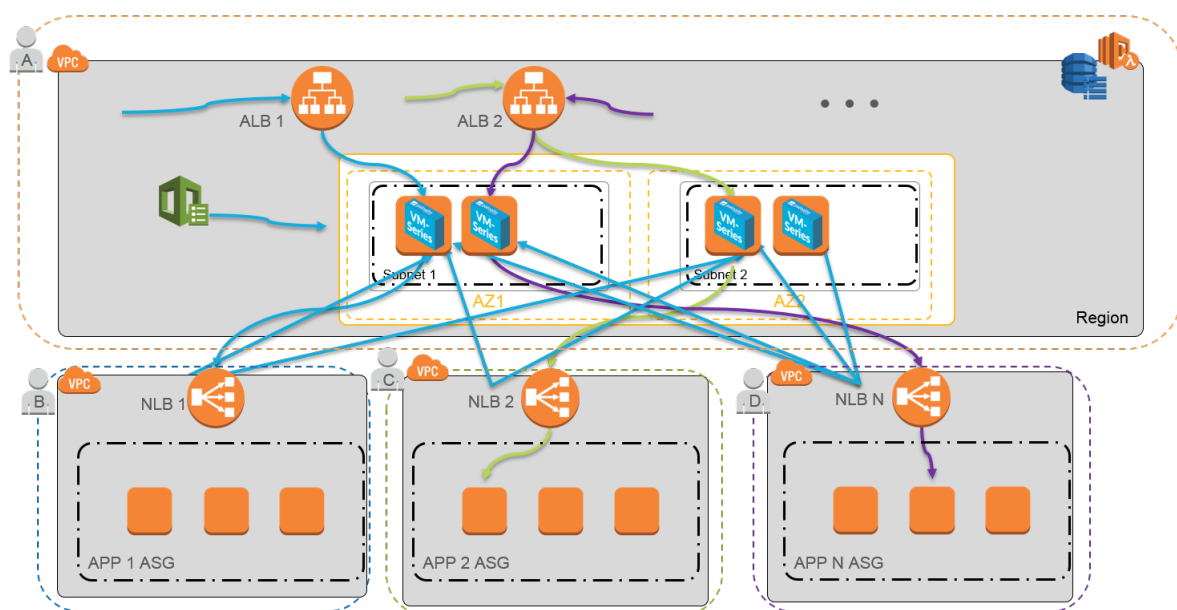
The network load balancer (NLB) depicted in the image is deployed by the network template below.

Palo Alto Networks officially supports the firewall template, and with a valid support entitlement, you can request assistance from Palo Alto Networks Technical Support.

- **Application Template**—The application template deploys a network load balancer and two auto scaling groups with a web server in each.

The application template is community supported.

Together these templates allow you to deploy a load balancer sandwich topology with an internet-facing application load balancer and an internal network load balancer. The application load balancer is accessible from the internet and distributes traffic that enters the VPC across a pool of VM-Series firewalls. The firewalls then route traffic using NAT policy to the internal network load balancer, which distributes traffic to an auto scaling tier of web servers. The VM-Series firewalls are enabled to publish custom PAN-OS metrics to AWS CloudWatch where you can monitor the health and resource load on the VM-Series firewalls and then use that information to trigger a scale in or scale out event in the respective auto scaling group.



- [VM-Series Auto Scaling Template for AWS Version 2.0](#)
- [Launch the VM-Series Auto Scaling Template for AWS \(v2.0\)](#)
- [Beta Known Issues](#)

VM-Series Auto Scaling Template for AWS

Version 2.0

The items in this checklist are actions and choices you must make for implementing this solution.

Planning Checklist for Version 2.0

<input type="checkbox"/> Verify the requirements for deploying the VM-Series Auto Scaling template.	<p>Version 2.0 of the auto scaling template deploys VM-Series firewalls running PAN-OS 8.0. This version requires AWS Lambda and S3 Signature versions 2 or 4.</p> <p>You will need to look up the list of supported regions and the AMI IDs.</p>
<input type="checkbox"/> Assign the appropriate permissions for the IAM user role.	<p>The user who deploys the VM-Series Auto Scaling template must either have administrative privileges or have the permissions listed in the iam-policy.json to launch this solution successfully. Copy and paste the permissions from this file in to a new IAM policy and then attach the policy to a new or existing IAM role.</p> <p>For a cross-account deployment, to access resources that are in a different AWS accounts, the IAM role for the user who deploys the application template must have full SQS access permissions and a trust relationship that authorizes them to write to the SQS queue that belongs to the firewall template.</p>
<input type="checkbox"/> Collect the details required for a cross-account deployment.	<p>For a deployment where the firewall template and the application template are in different accounts, the account that hosts the firewall template resources is the trusting account and the other AWS account(s) that hold the application template resources are the trusted accounts. To launch the application template in a cross-account deployment, you need the following information:</p> <ul style="list-style-type: none">• Cross- account Role Amazon Resource Name (ARN) of the account in which you are deploying the application template.• External ID, which you defined when creating the IAM role that grants full SQS access to the trusting account.• The 10-digit account number for every AWS account in which you plan to launch the application template. Because the account that hosts the firewall template resources serves as a trusting account, and it owns the resources that the users of the application template need, you need to list the account number for each trusted account that can access the firewall resources.
<input type="checkbox"/> Create a support account on the Palo Alto Networks Support portal, if you don't already have one.	<p>With VM-Series Auto Scaling template version 2.0, you can opt for the BYOL or PAYG (bundle 1 or bundle 2) licenses.</p> <ul style="list-style-type: none">• For BYOL, you must register an auth code to your Palo Alto Networks support account prior to launching the VM-Series Auto Scaling template and add the auth-code to the <code>/license</code> folder in the bootstrap package. See Launch the VM-Series Auto Scaling Template for AWS (v2.0) for details.

Planning Checklist for Version 2.0

- ❑ (For PAYG only) Review and accept the End User License Agreement (EULA).

Required, if you are launching a VM-Series firewall in an AWS account for the first time.

- For PAYG, you must register the VM-Series firewalls to activate your support entitlement.

In the AWS Marketplace, search for Palo Alto Networks, and select the bundle you plan to use. The VM-Series Auto Scaling template will fail to deploy if you have not accepted the EULA for the bundle you plan to use.

- For example, search for VM-Series Next Generation Firewall Bundle 2.

The screenshot shows the AWS Marketplace page for the Palo Alto Networks VM-Series Next-Generation Firewall Bundle 2. The page includes a 'Continue' button, a 'Pricing Information' section with a region dropdown set to 'Asia Pacific (Mumbai)', and a 'Pricing Details' section. A green banner at the bottom states: 'Software and AWS hourly usage fees apply when the instance is running. These fees will appear on your monthly bill. Please refresh this page later to enable launch with ec2 console.'

- Click Continue, and select Manual Launch. Review the agreement and click Accept Software Terms to accept the EULA.

Thank you! Your subscription will be completed in a few moments.

You can now close the browser.

- ❑ Decide whether you plan to use the public S3 buckets or your private S3 bucket for AWS Lambda, Python scripts, and templates.




Palo Alto Networks recommends using the bootstrap files in the public

Palo Alto Networks provides public S3 buckets in all AWS regions included in the [supported regions](#) list. These S3 buckets include all the templates, AWS Lambda code, and the bootstrap files that you need.


The naming convention for the S3 bucket is `panw-aws-autoscale-v20-<region_name>`. For example, the bucket in the AWS Oregon region is `panw-aws-autoscale-v20-us-west-2`.

If you plan to use your private S3 bucket, you must download and copy the templates, AWS Lambda code, and the bootstrap files to your private S3 bucket. You can place all the required files for both the firewall template and the application template in one S3 bucket or place them in separate S3 buckets.

Planning Checklist for Version 2.0

<p>S3 bucket only for evaluating this solution. For a production deployment, you must create a private S3 bucket for the bootstrap package.</p>	
<p>❑ Download the templates, AWS Lambda code, and the bootstrap files.</p> <p> Do not mix and match files across VM-Series Auto Scaling template versions.</p>	<ul style="list-style-type: none"> • Get the files for deploying the firewall template (application load balancer and the VM-Series firewalls) from the following GitHub repository at: https://github.com/PaloAltoNetworks/aws-elb-autoscaling/tree/master/Version-2.0 <ul style="list-style-type: none"> • Templates and Lambda code: <ul style="list-style-type: none"> • panw-aws.zip • firewall.template • Bootstrap files: <ul style="list-style-type: none"> • init-cfg.txt • bootstrap.xml <p>The bootstrap.xml file bundled with this solution is designed to help you get started, and is provided for testing and evaluation only. For a production deployment, you must modify the bootstrap.xml prior to launch.</p> • iam-policy: The user who deploys the VM-Series Auto Scaling template must either have administrative privileges or have the permissions listed in this file to successfully launch this solution. • Get the files for deploying the NLB and the web servers from the following GitHub repository at: https://github.com/PaloAltoNetworks/pan_nlb_v1 <ul style="list-style-type: none"> • Templates: <ul style="list-style-type: none"> • pan_aws_nlb.template • pan_aws_nlb_vpc.template • pan_nlb_lambda.template • Lambda code and Python scripts.
<p>❑ Customize the bootstrap.xml file</p>	<p>To ensure that your production environment is secure, you must customize the bootstrap.xml file with a unique administrative username and password.</p>

Planning Checklist for Version 2.0

for your production environment.	<p>The default username and password is pandemo/demopassword. You can also use this opportunity to create an optimal firewall configuration with interfaces, zones, and security policy rules that meet your application security needs.</p>
<p>❑ Decide whether you want to use Panorama for centralized logging, reporting, and firewall management.</p>	<p>Panorama is an option for administrative ease. It is not required to manage the auto scaling tier of VM-Series firewalls deployed in this solution.</p> <p>If you want to use Panorama, you can either use a Panorama virtual appliance on AWS or on vCloud Air, or use the M-Series appliance or a Panorama virtual appliance on a VMware ESXi server inside your corporate network.</p> <p>To successfully register the firewalls with Panorama, you must collect the following details:</p> <ul style="list-style-type: none"> • API key for Panorama—So that AWS Lambda can make API requests to Panorama, you must provide an API key when you launch the VM-Series Auto Scaling template. As a best practice, in a production deployment, create a separate administrative account just for the API call and generate an associated API key. • Panorama IP address—You must include the IP address in the configuration (init-cfg.txt) file. The firewalls must be able to access this IP address from the VPC; to ensure a secure connection, use a direct connect link or an IPsec tunnel. • VM auth key—Allows Panorama to authenticate the firewalls so that it can add each firewall as a managed device. You must include this key in the configuration (init-cfg.txt) file. <p>The vm auth key is required for the lifetime of the deployment. Without a valid key in the connection request, the VM-Series firewall will be unable to register with Panorama. For details on the key, see Generate VM Auth Key.</p> <ul style="list-style-type: none"> • Template name and the device group name to which to assign the firewalls —You must first add a template and create a device group on Panorama, and then include the template name and the device group name in the configuration (init-cfg.txt) file. <p> <i>In order to reduce the cost and scale limits of using Elastic IP addresses, the firewalls do not have public IPs. The best practice for managing the firewalls is to use Panorama. If you are not using Panorama to manage the firewalls, you must deploy a jump server (a bastion host with an EIP address) that attaches to the Untrust subnet within the VPC to enable SSH and/or HTTPS access to the VM-Series firewalls. By default, this solution includes an AWS NAT gateway that the firewalls use to initiate outbound requests for retrieving updates, connecting to Panorama, and publishing metrics to AWS CloudWatch.</i></p>
Get started	Launch the VM-Series Auto Scaling Template for AWS (v2.0)

Launch the VM-Series Auto Scaling Template for AWS (v2.0)

You can choose to deploy the firewall template in one VPC and the application template within the same VPC or across VPCs. To secure your applications that belong to another AWS account, the application template gives you the flexibility to deploy the network load balancer and web servers in a cross-account deployment.

- [Launch the VM-Series Firewall Template](#)
- [Launch the Application Template](#)
- (Required only if you deploy more than one NLB) [Enable Traffic to the ELB Service](#)

Launch the VM-Series Firewall Template

This workflow tells you how to deploy the application load balancer and the VM-Series firewalls using the firewall template.



This firewall template includes an AWS NAT gateway that the firewalls use to initiate outbound requests for retrieving updates, connecting to Panorama, and publishing metrics to AWS CloudWatch. If you are not using Panorama to manage the firewalls, you must deploy a jump server (a bastion host with an EIP address) that attaches to the Untrust subnet within the VPC to enable SSH and/or HTTPS access to the VM-Series firewalls. This jump server is required because the management interface on the VM-Series firewalls has a private IP address only.

STEP 1 | Reviewed the checklist for [VM-Series Auto Scaling Template for AWS Version 2.0](#).

Make sure that you have completed the following tasks:

- (For PAYG only) Reviewed and accepted the EULA for the PAYG bundle you plan to use.
- (For BYOL only) Obtained the auth code. You will need to enter this auth code in the /license folder of the [bootstrap package](#).
- Downloaded the files required to launch the VM-Series Auto Scaling template from the [GitHub repository](#).

STEP 2 | (Optional) Modify the init-cfg.txt file.

For more details read about the [bootstrapping process](#) and the [init-cfg.txt](#) file.

If you're using Panorama to manage the firewalls, complete the following tasks:

1. [Generate the VM-auth key on Panorama](#). The firewalls must include a valid key in the connection request to Panorama. Set the lifetime for the key to 8760 hours (1 year).
2. Open the init-cfg.txt file with a text editor, such as Notepad. Make sure that you do not alter the format as this will cause a failure in deploying the VM-Series Auto Scaling template. Add the following information as name-value pairs:
 - IP addresses for the primary Panorama and optionally a secondary Panorama. Enter:
`panorama-server=`
`panorama-server-2=`
 - Specify the template stack name and the device group to which you want to assign the firewall. Enter:

tplstackname=

dgname=

- VM auth key. Enter:

vm-auth-key=

3. Verify that you have not deleted the command for swapping the management interface (mgmt) and the dataplane interface (ethernet 1/1) on the VM-Series firewall on AWS. For example, the file must include name-value pairs for the items in bold:

op-command-modes=mgmt-interface-swap

vm-auth-key=755036225328715

panorama-server=10.5.107.20

panorama-server-2=10.5.107.21

tplname=FINANCE_TG4

dgname=finance_dg



The vm auth key and Panorama IP address above are example values. You need to enter the values that match your setup.

4. Save and close the file.

STEP 3 | (For BYOL only) Add the license auth code in the /license folder of the bootstrap package. For more information see [prepare the bootstrap package](#).

1. Create a new .txt file with a text editor, such as Notepad.
2. Add the authcode for your BYOL licenses. The auth code must support the number of firewalls that may be required for your deployment. You must use an auth code bundle instead of individual auth codes so that the firewall can simultaneously fetch all license keys associated with a firewall. If you use individual auth codes instead of a bundle, the firewall will retrieve only the license key for the first auth code included in the file.

STEP 4 | Change the default credentials for the VM-Series firewall administrator account defined in the bootstrap.xml file.

Required for using the VM-Series Auto Scaling template in a production environment.

The bootstrap.xml file provided in the GitHub repository is provided for testing and evaluation only. For a production deployment, you must [customize the bootstrap.xml](#) prior to launch.

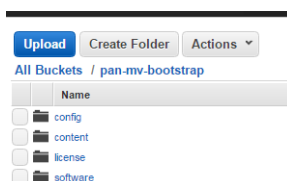
STEP 5 | Prepare the Amazon Simple Storage (S3) buckets for launching the VM-Series Auto Scaling template to a production environment.



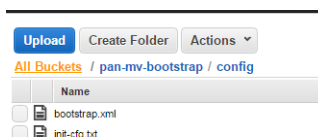
Make sure to create the S3 buckets in the same region in which you plan to deploy the template; the bootstrapping files hosted in the public S3 bucket are provided only to make it easier for you to evaluate the template.

1. Create a new S3 bucket for the bootstrap files.
 1. Sign in to the AWS Management Console and open the S3 console.
 2. Click Create Bucket.
 3. Enter a Bucket Name and a Region, and click Create. The bucket must be at the S3 root level. If you nest the bucket, bootstrapping will fail because you cannot specify a path to the location of the bootstrap files.
2. Upload the bootstrap files to the S3 bucket.

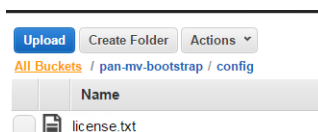
1. Click the name of bucket and then click Create folder.
2. Create the following folder structure for bootstrapping.



3. Click the link to open the config folder.
4. Select Actions > Upload and Add Files, browse to select the init-cfg.txt file and bootstrap.xml file, and click Open.
5. Click Start Upload to add the files to the config folder. The folder can contain only two files: init-cfg.txt and the bootstrap.xml.



6. (For BYOL only) Click the link to open the license folder and upload the txt file with the auth code required for licensing the VM-Series firewalls.



3. Upload the AWS Lambda code (panw-aws.zip file) to the S3 bucket.
1. Click the bucket name.
 2. Click Add Files to select the panw-aws.zip file, click Open.
 3. Click Start Upload to add the zip file to the S3 bucket.

<input type="checkbox"/>	Name	Last modified	Size	Storage class
<input type="checkbox"/>	config	--	--	--
<input type="checkbox"/>	content	--	--	--
<input type="checkbox"/>	license	--	--	--
<input type="checkbox"/>	software	--	--	--
<input type="checkbox"/>	panw-aws.zip	Dec 4, 2017 12:10:50 PM GMT-0800	162.1 KB	Standard

STEP 6 | Select the firewall template.

1. In the AWS Management Console, select CloudFormation > Create Stack.
2. Select Upload a template to Amazon S3, choose the firewall.template that you downloaded previously, and click Open and Next.
3. Specify the Stack name. The stack name allows you to uniquely identify all the resources that this template deploys.

STEP 7 | Configure the parameters for the VPC.

1. Enter the parameters for the VPC Configuration as follows:
 1. Enter a VPCName. The default CIDR is 192.168.0.0/16.
 2. Select the two Availability Zones that your setup will span in Select two AZs.

STEP 8 | Select your preferences for the VM-Series firewalls.

1. [Look up the AMI ID](#) for the VM-Series firewall and enter it. Make sure that the AMI ID matches the AWS region, PAN-OS-8.0 version and the BYOL or PAYG licensing option you have opted to use.
2. Select the EC2 Key pair (from the drop-down) for launching the firewall. To log in to the firewalls, you must provide the name of this key pair and the private key associated with it.
3. If you want to restrict access to the firewall, specify the IP address block or IP addresses that can SSH in to the firewall. Verify your IP address before configuring it on the VM-Series Auto Scaling template to make sure that you do not lock yourself out.
4. Select Yes if you want to Enable Debug Log. Enabling the debug log generates more verbose logs that help with troubleshooting issues with the deployment. These logs are generated using the stack name and are saved in CloudWatch.

By default, the template uses CPU utilization as the scaling parameter for the VM-Series firewalls. [Custom PAN-OS metrics](#) are automatically published to the CloudWatch namespace that matches the stack name you specified earlier.

STEP 9 | Specify the name of the Amazon S3 bucket(s).



You can use one S3 bucket the bootstrap package and the zip file.

1. Enter the name of the S3 bucket that contains the bootstrap package.
If the bootstrap bucket is not set up properly or if you enter the bucket name incorrectly, the bootstrap process will fail and you will not be able to log in to the firewall. Health checks for the load balancers will also fail.
2. Enter the name of the S3 bucket that contains the panw-aws.zip file.

STEP 10 | Specify the keys for enabling API access to the firewall and Panorama.

1. Enter the key that the firewall will use to authenticate API calls. The default key is based on the sample bootstrap.xml file and should only be used for testing and evaluation. For a production deployment, you must create a separate PAN-OS login just for the API call and generate an associated key.
2. Enter the API Key to allow AWS Lambda to make API calls to Panorama, if you are using Panorama for centralized management. For a production deployment, you should create a separate login just for the API call and generate an associated key.
3. Copy and paste the license deactivation API key for your account. This key is required to successfully deactivate licenses on your firewalls when a scale-in event occurs. To get this key:
 1. Log in to the Customer Support Portal.
 2. From the Go To drop-down, select License API.
 3. Copy the API key.

STEP 11 | Enter the name for the application load balancer.

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

Parameters

VPC Configuration

VPCName Name of the newly created VPC

Select two AZs:
Enter two Availability Zones

VM-Series firewall Instance configuration

The Ami Id of the PAN FW Image: Link to Ami Id lookup table: <https://www.paloaltonetworks.com/documentation/global/compatibility-matrix/vm-series-firewalls/aws-oft-amazon-machine-images-ami-list>

Key pair: Amazon EC2 Key Pair

SSH From: Restrict SSH access to the VM-Series firewall (by default can be accessed from anywhere)

Enable Debug Log: Enable/Disable debug. Default is disabled

S3 Bucket details

Bootstrap bucket for VM-Series firewalls Enter the name of the Bootstrap S3 bucket for the VM-Series firewall

S3 Bucket Name for templates and Lambda Code: VM-Series firewall Lambda/Scripts/CFT template S3 Bucket or your own in the same region

VM-Series API Key

API Key for Firewall: API Key associated to username/password of the VM-Series Firewall. By default it is pandemo/demopassword

API Key for Panorama: API Key associated to username/password of the Panorama.

API Key for Delicensing Firewall: Key used to de-license the PAN FW

Load Balancer configuration

Name of External Application Load Balancer: Enter the name of the external Application Load Balancer

STEP 12 | (Optional) Apply tags to identify the resources associated with the VM-Series Auto Scaling template.

Add a name-value pair to identify and categorize the resources in this stack.

STEP 13 | Review the template settings and launch the template.

1. Select I acknowledge that this template might cause AWS CloudFormation to create IAM resources.
2. Click Create to launch the template. The CREATE_IN_PROGRESS event displays.
3. On successful deployment the status updates to CREATE_COMPLETE.

In each AZ, the VM-Series Auto Scaling template will launch an ASG that includes one VM-Series firewall behind the application load balancer. The firewalls will be bootstrapped with a basic Security policy rule.

STEP 14 | Verify that the template has launched all required resources.

1. On the EC2 Dashboard, select Load Balancers and find the application load balancer name you entered in the template.
2. Get the DNS name for the application load balancer, and enter it into a web browser. For example:
`http://public-elb-123456789.us-east-1.elb.amazonaws.com/`
The web page will display to indicate that you have successfully launched the CloudFormation template.
3. On the EC2 Dashboard, select Auto Scaling Groups. Verify that in each AZ, you have one ASG for the VM-Series firewalls with the one firewall in each ASG. The ASG name prefix includes the stack name.
4. Log in to the VM-Series firewall. You must deploy a jump server or use Panorama to access the user interface on the firewall.



- *It may take up to 20 minutes for the firewalls to boot up and be available to handle traffic.*
- *When you are finished with testing or a production deployment, the only way to ensure charges stop occurring is to completely delete the stack. Shutting down instances, or changing the ASG maximum to 0, is not sufficient as the CFT might automatically deploy new ASGs.*



Launch the Application Template

The application template allows you to complete the sandwich topology and is provided so that you can evaluate the auto scaling solution. The template deploys a network load balancer and a pair of web servers behind the auto scaling group of VM-Series firewalls, which you deployed using the firewall template. The web servers in this template have a public IP address for direct outbound access so that they can get software updates. So, use this to evaluate the solution, but build your own template to deploy to production.

When launching the application template, you must select the template based on whether you want to deploy the application template within the same VPC (`panw_aws_nlb.template`) in which you deployed the firewall template or in a separate VPC (`panw_aws_nlb_vpc.template`). For a separate VPC, the template provides supports for cross-account deployments. A cross-account deployment requires you to create a IAM role and enable permissions and trust relationship between the trusting AWS account and the trusted AWS account, and the account information is required as input when launching the template.

STEP 1 | (Required only for a cross-account deployment) Create the IAM role. Refer to [AWS documentation](#).

This role grants access to a user who belongs to a different AWS account. This user requires permissions to access the Simple Queue Service (SQS) resource in the firewall template. The firewall uses this queue to learn about each network load balancer that you deploy so that it can create NAT policy to send traffic to the web servers that are behind the network load balancer.

- For Account ID, type the AWS account ID of the account into which you are deploying the application template. Specifying that account ID allows you grant access to the resources in your account that hosts the firewall template resources.
- Select Require external ID and enter a value that is a shared secret. Specifying an external ID allows the user to assume the role only if the request includes the correct value.
- Choose Permissions to allow Amazon SQS Full Access.

Review

Provide the required information below and review this role before you create it.

Role name*

Maximum 64 characters. Use alphanumeric and '+=, @-_' characters.

Role description

Maximum 1000 characters. Use alphanumeric and '+=, @-_' characters.

Trusted entities The account 123456678890

Policies  AmazonSQSFullAccess [↗](#)

STEP 2 | Use the Palo Alto Networks public S3 bucket or prepare the your private (S3) bucket for launching the application template.

1. Create a zip file with all the files in the [GitHub repository](#), excluding the three .template files, named nlb.zip in the screenshot below.
2. Upload the zip file to the S3 bucket you created earlier or to a new bucket.

Amazon S3 > mvbootstrap

Overview Properties Permissions Management

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

[Upload](#) [Create folder](#) [More](#) US East (Ohio)

Viewing 1 to 7

<input type="checkbox"/>	Name ↑	Last modified ↑	Size ↑	Storage class ↑
<input type="checkbox"/>	config	--	--	--
<input type="checkbox"/>	content	--	--	--
<input type="checkbox"/>	license	--	--	--
<input type="checkbox"/>	software	--	--	--
<input type="checkbox"/>	nlb.zip	Dec 3, 2017 4:09:11 PM GMT-0800	78.2 KB	Standard
<input type="checkbox"/>	pan_nlb_lambda.template	Dec 3, 2017 4:37:20 PM GMT-0800	17.1 KB	Standard
<input type="checkbox"/>	panfw-aws.zip	Dec 3, 2017 4:02:23 PM GMT-0800	162.0 KB	Standard

3. Copy the pan_nlb_lambda template into the same bucket to which you copied the nlb.zip file.

STEP 3 | Get the Simple Queue Service URL from the AWS management console. You need this URL to enable the firewalls to learn about the network load balancer once it is deployed. The firewalls automatically create a NAT policy rule to send traffic to the network load balancer.

1. On the AWS Management console, select Simple Queue Service in the Application Integration section.
2. Find the Network Load Balancer queue for the firewall stack you deployed and copy the URL.

<input checked="" type="checkbox"/>	MV-Dec3-NetworkLoadBalancerQueue-1EX54C9C36I7G	Standard	N/A
<input type="checkbox"/>	arkOFwSTK22-LambdaENIQueue-1I3ZHTAOYYPKJ	Standard	N/A
<input type="checkbox"/>	arkOFwSTK22-NetworkLoadBalancerQueue-18V5Q5WMIUDR	Standard	N/A
<input type="checkbox"/>	rkc_test_nlbQueue	Standard	N/A
<input type="checkbox"/>	vrp12o2-az2-11L0LLSSUFE3O	Standard	N/A

1 SQS Queue selected

Details	Permissions	Redrive Policy	Monitoring	Tags	Encryption
---------	-------------	----------------	------------	------	------------

Name: MV-Dec3-NetworkLoadBalancerQueue-1EX54C9C36I7G

URL: <https://sqs.us-east-2.amazonaws.com/680518198024/MV-Dec3-NetworkLoadBalancerQueue-1EX54C9C36I7G>

ARN: [arn:aws:sqs:us-east-2:680518198024:MV-Dec3-NetworkLoadBalancerQueue-1EX54C9C36I7G](#)

STEP 4 | Select the application template to launch.

1. In the AWS Management Console, select CloudFormation > Create Stack.
2. Select Upload a template to Amazon S3, to choose the panw_aws_nlb.template to deploy the resources that the template will launch within the same VPC as the firewalls, or the panw_aws_nlb_vpc.template to deploy the resources in to a different VPC. Click Open and Next.
3. Specify the Stack name. The stack name allows you to uniquely identify all the resources that are deployed using this template.

STEP 5 | Configure the parameters for the VPC and network load balancer.

1. Select the two Availability Zones that your setup will span in Select list of AZ. If you are deploying within the same VPC make sure to select the same Availability Zones that you selected for the firewall template.
2. Enter a CIDR Block for the VPC. The default CIDR is 192.168.0.0/16.
3. Enter a name for the network load balancer in 11 characters or less. Using a longer name results in a failure to launch the the template.

STEP 6 | Configure the parameters for Lambda.

1. Enter the S3 bucket name where nlb.zip and the pan_nlb_lambda.template is stored.
2. Enter the name of the pan_nlb_lambda.template and the zip file name.
3. Paste the SQS URL that you copied earlier.
4. (Optional) Modify the backend table name, to your preference.

STEP 7 | Modify the web server EC2 instance type to meet your deployment needs.

STEP 8 | Configure the other parameters requires to launch the stack.

1. Select the EC2 Key pair (from the drop-down) for launching the firewall. To log in to the web servers, you must provide the name of this key pair and the private key associated with it.
2. If you want to restrict access to the web servers, specify the IP address block or IP addresses that can SSH in to the web servers.
3. Select SameAccount true if you are deploying this application template within the same AWS account as the firewall template; select false for a cross-account deployment.

For a cross-account deployment, enter the Amazon Resource Number (ARN) for the CrossAccountRole and ExternalId that you defined in [\(Required only for a cross-account deployment\) Create the IAM role. Refer to AWS documentation](#). You can get the ARN from Support > Support Center on the AWS Management Console.

4. Enter the name of the VPC in which you want to deploy the network template resources.

STEP 9 | Review the template settings and launch the template.

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

Parameters

VPC Section

Select list of AZ:
Enter the list of Availability Zones (Based on Number of AZs above)

CIDR Block for the VPC: Enter the VPC CIDR that you want to use

NLB Section

NLBName Enter the name to associate with the NLB

Lambda Section

S3BucketName Enter the name S3 Bucket Name which contains the template and lambda code

NestedLambdaTemplateName Enter the name of the S3 object which contains the lambda template

LambdaZipFileName Enter the name of the S3 object which contains the lambda function code

QueueURL Enter the URL of the Queue to send NLB updates to

TableName Enter the name of the backend DB Table

Application Section

Instance Type of Web Servers behind ILB: WebServer EC2 Instance type

Access Section

Key pair: Amazon EC2 Key Pair

SSH From: Restrict SSH access to the VM-Series firewall (by default can be accessed from anywhere)

Other parameters

CrossAccountRole Enter the ARN of the role to be used.

ExternalId The external ID associated with the Cross Account Role

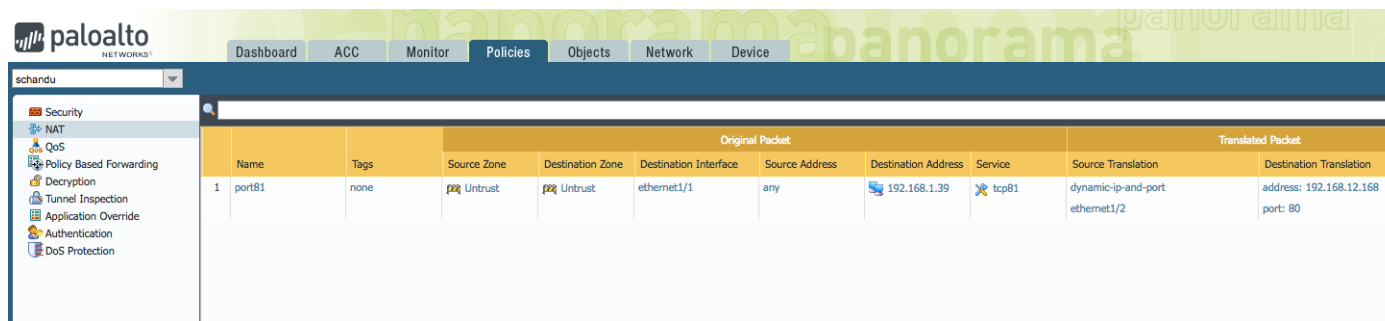
NLBSubnetipBlocks Management subnet comma-delimited list of CIDR blocks

SameAccount Flag to indicate if the NLB will be deployed into the same account or a different one

VPC Name: Name of the newly created VPC

STEP 10 | Verify that the firewall has a NAT policy rule to the IP address of the network load balancer.

When you deploy the application template to launch another instance of a network load balancer and pair of web servers, the firewall learns about the port allocated for the next network load balancer instance and creates another NAT policy rule. So, if you deploy the application template three times, the firewall will have three NAT policy rules for ports 81, 82, and 83.



STEP 11 | If you have launched the application template more than once, you need to [Enable Traffic to the ELB Service](#).

Enable Traffic to the ELB Service

If you add a second or additional network load balancers in your deployment, you must complete additional configuration so that the application load balancer, the VM-Series firewalls auto scaling groups, and the web servers can report as healthy and traffic is load balanced across all your AWS resources.

STEP 1 | [Create a target group](#). The application load balancer sends requests to registered targets using the port and protocol that you specify for the servers in the target group.

Increment the port by 1 starting at 81 for every additional network load balancer you deploy, after the first. So, the second network LB will be port 82, and the third port 83. On the AWS management console, you can verify the ports allocated for each network balancer on the DynamoDB Table that matches the application template name.

Create target group

Your load balancer routes requests to the targets in a target group using the protocol and port that you specify, and perfoi

Target group name ⓘ

Ohio-TG82

Protocol ⓘ

HTTP

Port ⓘ

82

Target type ⓘ

instance

VPC ⓘ

vpc-2cbf4b44 (192.168.0.0/16) | MV-VPC3

Health check settings

Protocol ⓘ

HTTP

Path ⓘ

/Ohio-TG82/index.html

▶ Advanced health check settings

STEP 2 | [Edit the listener rules](#) on the application load balancer to route requests to the target web servers.

1. On the AWS management console, select Load Balancers in the Load Balancing section, and select the application load balancer that matches your stack name.
2. Select View/edit rules to modify the rules for the listener.
3. Select Insert rule and add a path-based route to forward traffic to the target group you defined above as follows:

Rules for: MM-Dec3-ALB HTTP 80		
1	ARN	IF ✓ Path is /Ohio-TG85/*
		THEN Forward to Ohio-TG85
2	ARN	IF ✓ Path is /Ohio-TG84/*
		THEN Forward to Ohio-TG84
3	ARN	IF ✓ Path is /Ohio-TG83/*
		THEN Forward to Ohio-TG83
4	ARN	IF ✓ Path is /Ohio-TG82/*
		THEN Forward to Ohio-TG82
last	HTTP 80: default action <i>This rule cannot be moved or deleted</i>	IF ✓ Requests otherwise not routed
		THEN Forward to arkOF-Publi-4TR49F6X3F5Y

STEP 3 | Attach the target group to both VM-Series firewalls auto scaling groups.

1. Select Auto Scaling Groups in the Auto Scaling section and select an auto scaling group that matches the stack name.
2. Select Details > Edit and select the new target group from the Target Groups drop-down.

Auto Scaling Group: arkOFwJTK2-arl-DF-P-bli-4TR49.6A. ASG-us-1

Details Activity History Scaling Policies Instances Monitoring Notifications Tags Scheduled Actions Lif

Launch Configuration arkOFwJTK2-arl-F-F-Jun-41.14TF6X3F5Y_AS-1

Launch Template

Launch Template Version

Load Balancers

Target Groups arkOF-Publi-4TR49.6X3F5Y x Ohio-TG82 x

Desired 1

Min 1

Max 5

Health Check Type EC2

Health Check Grace Period 900

Termination Policies Default x

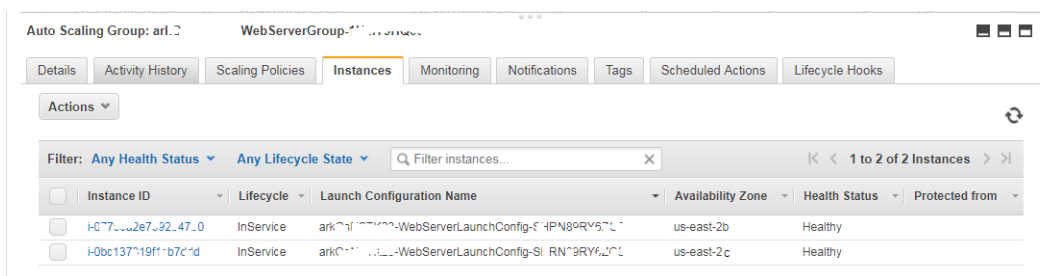
Creation Time Mon Dec 04 18:15:04 GMT-800 2017

STEP 4 | Log in to each web server that was deployed by the application template, create a new directory with the target group name and copy the index.html file into the directory. Until until you set up the path to the index.html file, the health check for this web server reports as unhealthy.

```
sudo su
cd/var/www/html
mkdir <target-groupname>
cp index.html <target-groupname>
```

STEP 5 | Verify that the health status of the web servers.

Select Auto Scaling Groups, and use the application stack name to find the webserver auto scaling group to verify that the web servers are reporting healthy.



Beta Known Issues

The following table includes known issues in the auto scaling template 2.0 beta 2 release.

Issue ID	Description
HYPI-166	In a cross account deployment, when you deploy the firewall template in a VPC and use the application template in two or or more VPCs, the target web servers report as unhealthy even after you add the target groups to the application load balancer.
HYPI-165	Launching two instances of the application template stack at the same time may cause a delay in updating DynamoDB with the correct number of network load balancers that have been deployed. If you need to launch the application template multiple times for more network load balancer instances, launch the application template with a time gap of a few minutes to ensure that DynamoDB is updated properly.
HYPI-161	<p>When you deploy the firewall template and the application template in different VPCs across different accounts, on occasion the firewalls are not ready for traffic. Although the template reports a success, the firewalls maybe in the initializing state.</p> <p>Workaround: After 20 minutes, verify the status of the firewalls on the DynamoDB table. If the firewalls are still reported as initializing (INIT state), delete the stack and deploy the firewall template again.</p>
HYPI-158(Added in beta 2)	Panorama fails to remove firewalls from the managed devices list when a scale-in event happens and one or more instances of the VM-Series firewall are deleted within an autoscaling group.
HYPI-157	When a scale-in event happens and one or more instances of the VM-Series firewall are deleted, the licenses are not released back to the available license pool. This issue pertains to BYOL licenses only and it occurs occasionally.
HYPI-156	<p>The NLB template fails to deploy when the stack name is more than 11 characters.</p> <p>Workaround: Enter 11 characters or less for the template name.</p>
HYPI-155	<p>The firewall template launches a single auto scaling group instead of two in Singapore (ap-southeast-1)region when you use the public S3 bucket, panw-aws-autoscale-v20-ap-southeast-1.</p> <p>Workaround: Create a private S3 bucket and copy the files required for deploying the template.</p>
HYPI-154	<p>Using the pan_aws_nlb_vpc. template to deploy the NLB template in a separate VPC in the Canada region fails when you use the public S3 bucket, panw-aws-autoscale-v20-ca-central-1.</p> <p>Workaround: Create a private S3 bucket and copy the files required for deploying the template.</p>
HYPI-121	You cannot deploy the auto scaling template in Sao Paulo (sa-east-1). This is because some of the resources that the template requires are not available there.