

# VM-Series Integration with AWS Appliance Gateway

Beta

---

## Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

[www.paloaltonetworks.com/company/contact-support](http://www.paloaltonetworks.com/company/contact-support)

## About the Documentation

- To ensure you are viewing the most current version of this document, or to access related documentation, visit the Technical Documentation portal: [docs.paloaltonetworks.com](https://docs.paloaltonetworks.com).
- To search for a specific topic, go to our search page: [docs.paloaltonetworks.com/search.html](https://docs.paloaltonetworks.com/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](mailto:documentation@paloaltonetworks.com).

## Copyright

Palo Alto Networks, Inc.

[www.paloaltonetworks.com](http://www.paloaltonetworks.com)

© 2020-2020 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](http://www.paloaltonetworks.com/company/trademarks.html). All other marks mentioned herein may be trademarks of their respective companies.

## Last Revised

October 8, 2020

---

# Table of Contents

**VM-Series Firewall Integration with AWS Appliance Gateway..... 5**

- VM-Series Integration with AWS Appliance Gateway Overview..... 7
  - Transit Gateway Deployments.....7
  - Frequently Asked Questions.....9
- Deploy the VM-Series Firewall Behind an AGW..... 10
- Advanced Options for Manual Deployment.....14
- Launch the Security VPC Template..... 17
- Launch the Application Template.....22
- Known Issues..... 24



# VM-Series Firewall Integration with AWS Appliance Gateway

This document describes how to deploy the VM-Series firewall behind an Appliance gateway. You can deploy the VM-Series firewall manually or using CloudFormation templates.

- > [VM-Series Integration with AWS Appliance Gateway Overview](#)
- > [Deploy the VM-Series Firewall Behind an AGW](#)
- > [Advanced Options for Manual Deployment](#)
- > [Launch the Security VPC Template](#)
- > [Launch the Application Template](#)

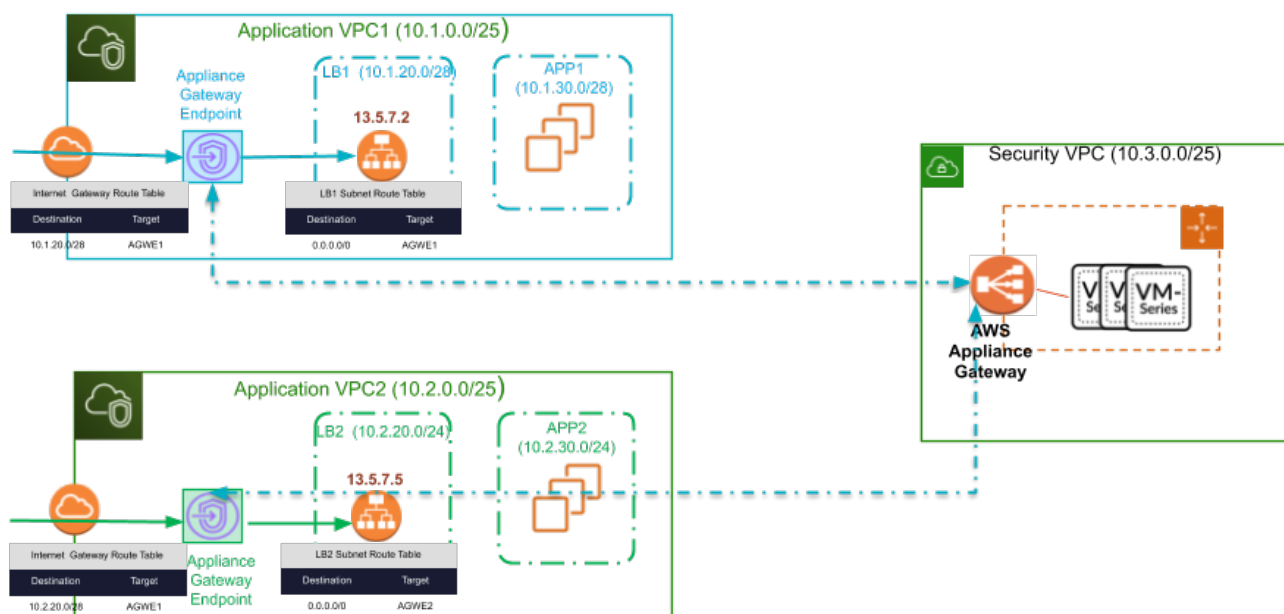


# VM-Series Integration with AWS Appliance Gateway

## Gateway Overview

We are excited to announce the beta availability of **VM-Series Integration with the AWS Appliance gateway**. With this support, you can now easily scale your VM-Series next-generation firewall to protect your AWS cloud applications from known and unknown threats.

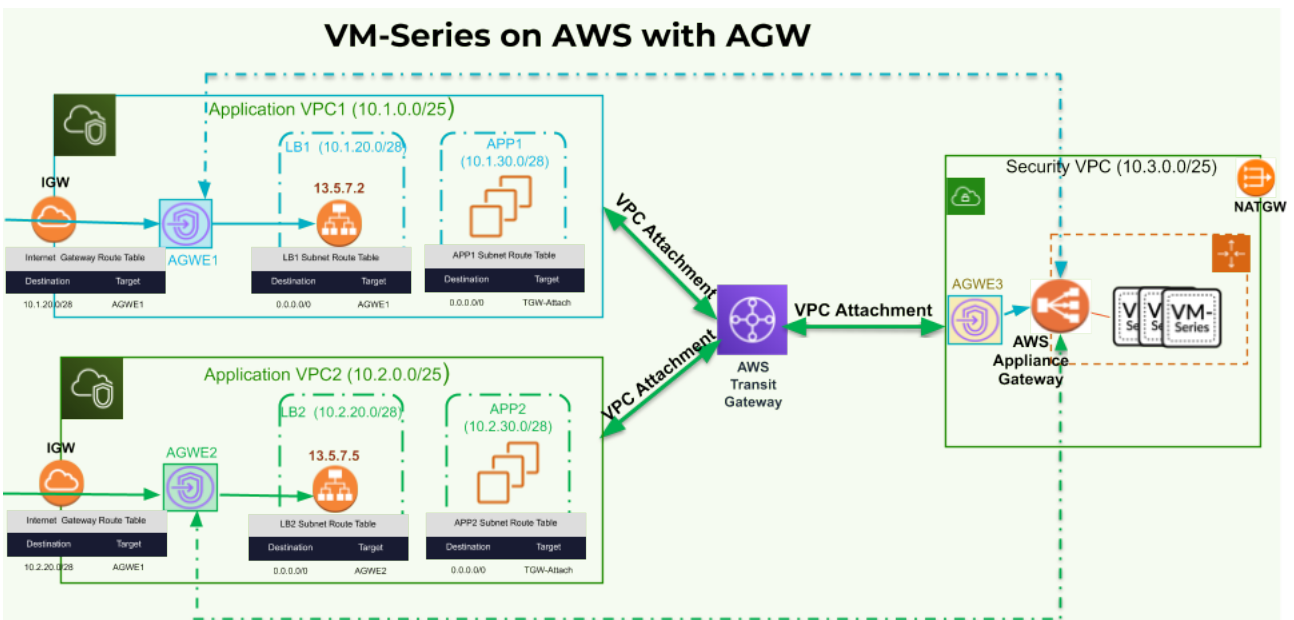
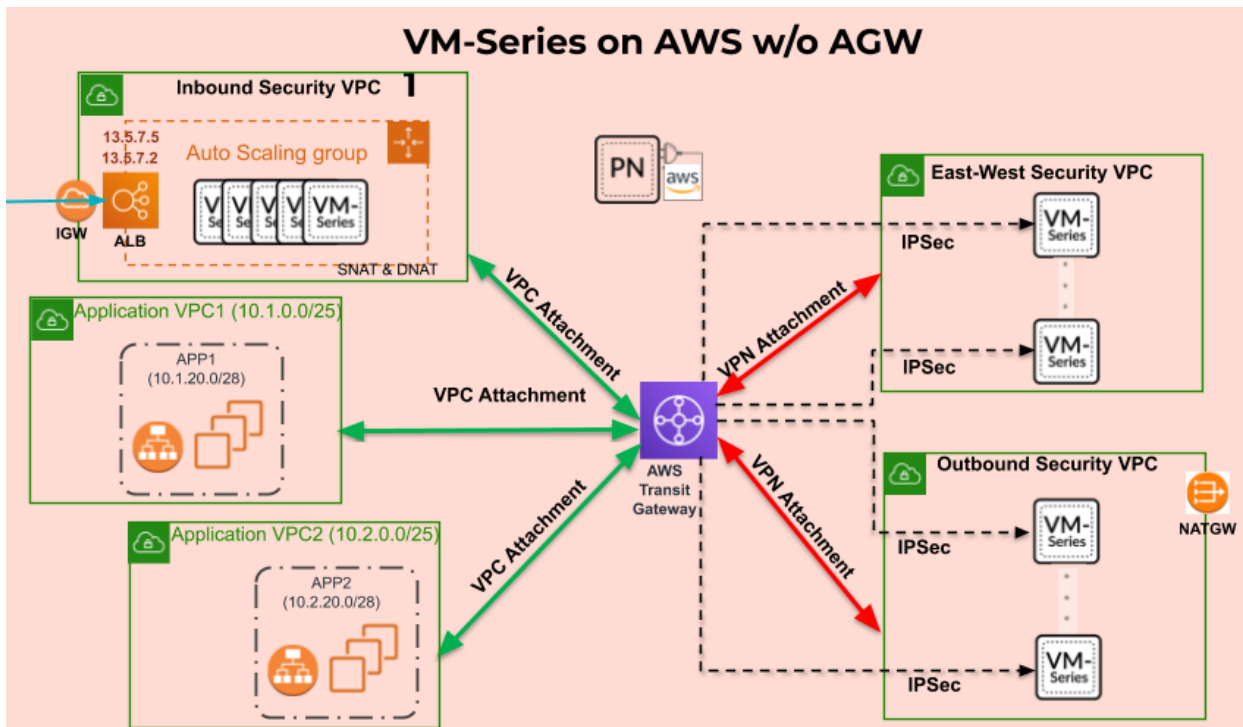
Appliance Gateway is a new AWS managed service that allows you to deploy a group of VM-Series firewalls and operate in a horizontally scalable and fault-tolerant manner. You can then expose the group of firewalls as a VPC endpoint service for traffic inspection and threat prevention. To protect your inbound traffic to your applications, you can create an Appliance gateway endpoint for that endpoint service in your application VPC. You can then add route rules in your application VPC route tables to redirect your VPC traffic to the Appliance gateway endpoint for inspection.



## Transit Gateway Deployments

With this integration, you can scale your VM-Series Next-generation firewall capabilities to dynamically match your outbound and east-west traffic using AWS native networking constructs and VPC attachments in your AWS transit gateway environments. Additionally, you can use this integration to simplify the VM-Series insertion at scale for your spoke VPC's inbound traffic.

The figure below shows you can use the AWS Appliance gateway integration with VM-Series to simplify your AWS Transit gateway environments. You can continue to use a centralized security VPC that has an AWS Appliance gateway to scale and load-balance traffic across a group of VM-Series firewalls. To protect the inbound traffic, you can now create AWS Appliance gateway endpoints (AGW1 and AGW2) in your spoke VPCs and add route rules in the spoke's Internet gateway and subnet route tables to protect all inbound traffic to your VPC. Similarly, you can now create an Appliance gateway endpoint (AGW3) in the centralized firewall VPC and then use route rules in your VPCs and transit gateways to redirect your outbound and east-west traffic to your security VPC for inspection.



The VM-Series integration with AWS Appliance Gateway offers the following benefits:

- **Simplified connectivity** - You can now use the AWS Appliance gateway to easily insert an auto-scaling VM-Series firewall pool in the outbound, east-west, and inbound traffic path of your applications.
- **Performance at scale** - Appliance gateway helps you scale your traffic across multiple VM-Series firewalls at higher throughput by using AWS native networking constructs and the transit gateway VPC attachments. You no longer need encrypted tunnels for east-west and outbound traffic inspection.
- **Transparent resiliency** - Appliance gateway helps you to scale and load balance your traffic across multiple VM-Series firewalls. With this integration, VM-Series and the Appliance gateway use the GENEVE encapsulation to keep your traffic packet headers and payload intact, providing complete visibility of the source's identity to your applications.



---

You can now use the **VM-Series with AWS Appliance Gateway** to improve your AWS environment's security posture. This integration scales out the VM-Series next-generation firewall capabilities at its maximum performance. It also centralizes your firewall and policy management while maintaining the source's identity for applications (a.k.a no SNAT).

We have whitelisted your AWS account for this beta. We will love to hear any feedback that you have. Please contact [vmseries-beta@paloaltonetworks.com](mailto:vmseries-beta@paloaltonetworks.com) for additional questions.

## Frequently Asked Questions

### 1. How do I get access to AWS Appliance Gateway?

Since you have enrolled in Amazon Web Services (AWS) Appliance gateway beta, AWS will whitelist your account to use the AWS Appliance gateway.



*When you enroll your AWS account for the beta, AWS will restrict all VPCs in your environment to have the maximum CIDR range of /25. This CIDR range will allow a maximum of 126 usable IPv4 addresses in the VPC (or a maximum of eight subnets of CIDR range of /28 within your VPC). The restriction will be static, per account. With the restricted account, you cannot resize your VPC even if you are not using it for AGW testing.*

### 2. Do I need a new version of VM-Series software for this beta?

Yes, You will need a new version of VM-Series software for this Beta. Palo Alto Networks will share the VM-Series private Beta Amazon Machine Image (AMI) to your account. You will use an authorization code with the AMI.

### 3. Can I deploy VM-Series firewalls in different AWS availability zones as targets of the AWS Appliance gateway?

Yes, You can enable one or more availability zones for your AWS appliance gateway. You can then register VM-Series firewalls deployed in different availability zones as targets of your AWS Appliance gateway.

### 4. What are the different options to test VM-Series integration AWS Appliance gateway integration during the beta?

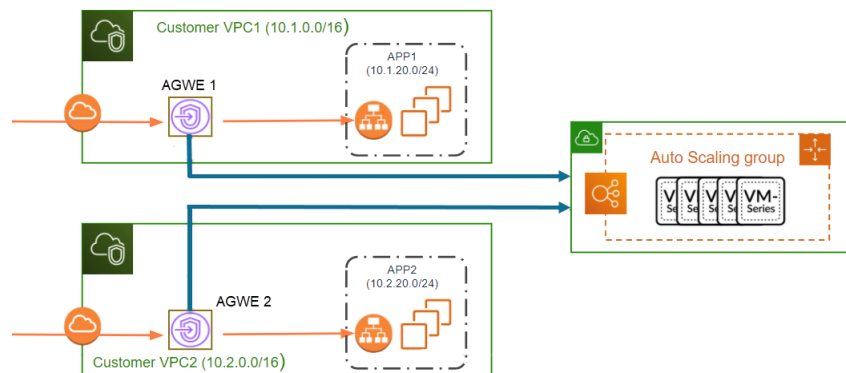
You have the following options:

1. You can test the integration of VM-Series with the AWS Appliance gateway manually.
2. You can test using the integration using the simple Terraform or Cloud formation templates. These templates will allow you to deploy two VM-Series in a single AWS availability zone as targets to your AWS Appliance gateway.
3. You can also use the VM-Series autoscaling cloud formation template. This template will allow you to deploy VM-Series in an autoscaling group and add them as the target of your Appliance gateway.

# Deploy the VM-Series Firewall Behind an AGW

You can now deploy the VM-Series firewall on AWS in an appliance gateway. In an appliance gateway deployment, the VM-Series firewall is deployed in a separate VPC and traffic moving through your application VPCs is redirected to the VM-Series firewall for inspection and policy enforcement. By placing your firewalls behind an appliance gateway and redirecting traffic to your security VPC, you no longer need to deploy firewalls between the source and destination.

In the simple North-South example below, traffic directed to your application is redirected to the security VPC containing the VM-Series firewall by an appliance gateway endpoint. After the firewall inspects the traffic and applies any applicable policy, the traffic is sent back to the appliance gateway endpoint and then onto the destination. When a single security zone is used, traffic is treated as intrazone and enters and exits the VM-Series firewall via a single interface.



Complete the following procedure to manually deploy your VM-Series firewall on AWS behind an appliance gateway.

## STEP 1 | Set up the security VPC. See the [AWS documentation](#) for more information about creating your security VPC.

- Create two subnets—one for management and one for data.
- Create two security groups—one for firewall management and one for data.
- The management subnet security groups should allow https and ssh for management access.
- Ensure that the security group(s) in your data VPC allows GENEVE-encapsulated packets (UDP port 6081).



*The target group of the appliance gateway cannot use HTTP for health checks because the VM-Series firewall does not allow access with an unsecured protocol. Instead, use another protocol such as HTTPS or TCP.*

## STEP 2 | Launch the VM-Series firewall.

1. On the EC2 Dashboard, click Launch Instance.
2. Select the VM-Series AMI. To get the AMI, see [Obtain the AMI](#).
3. Launch the VM-Series firewall on an EC2 instance.
  1. Choose the EC2 instance type for allocating the resources required for the firewall, and click Next. See [VM-Series System Requirements](#), for resource requirements.
  2. Select the security VPC.

3. Select the data subnet to attach to eth0.
4. Select Launch as an EBS-optimized instance.
5. Add another network interface for eth1 to act as the management interface after the interface swap. Swapping interfaces requires a minimum of two ENIs (eth0 and eth1).
  - Expand the Network Interfaces section and click Add Device to add another network interface.

Make sure that your VPC has more than one subnet so that you can add additional ENIs at launch.



*If you launch the firewall with only one ENI:*

- The interface swap command will cause the firewall to boot into maintenance mode.
- You must reboot the firewall when you add the second ENI.
- Expand the Advanced Details section and in the User data field enter **mgmt-interface-swap=enable** and **plugin-op-commands=aws-agw-inspect:enable** as text to perform the interface swap during launch.

User data ⓘ ☒ As text ☐ As file ☐ Input is already base64 encoded

```

drgname=agw-device-group
op-command=mode=mgmt-interface-swap:jumbo-frame
vm-series-auto-registration-pin-id=abcdefgh1234****
vm-series-auto-registration-pin-value=zyxwvut0987****
mgmt-interface-swap=enable
plugin-op-commands=aws-agw-inspect:enable
  
```

6. Accept the default Storage settings. The firewall uses volume type SSD (gp2).



*This key pair is required for first time access to the firewall. It is also required to access the firewall in maintenance mode.*

7. (Optional) Tagging. Add one or more tags to create your own metadata to identify and group the VM-Series firewall. For example, add a Name tag with a Value that helps you remember that the ENI interfaces have been swapped on this VM-Series firewall.
8. Select the data Security Group for eth0 (data interface). Enable traffic on UDP port 6081.
 

If you enable health checks to the firewall, you cannot use HTTP. Instead, use another protocol such as HTTPS or TCP.
9. If prompted, select an appropriate SSD option for your setup.
10. Select Review and Launch. Review that your selections are accurate and click Launch.
11. Select an existing key pair or create a new one, and acknowledge the key disclaimer.
12. Download and save the private key to a safe location; the file extension is `.pem`. You cannot regenerate this key, if lost.

It takes 5-7 minutes to launch the VM-Series firewall. You can view the progress on the EC2 Dashboard. When the process completes, the VM-Series firewall displays on the Instances page of the EC2 Dashboard.

**STEP 3 | Attach the management security group to eth1 (management interface). Allow ssh and https. See the [AWS Documentation](#) for more information.**

**STEP 4 | Create and assign an Elastic IP address (EIP) to the ENI used for management access (eth1) to the firewall.**

1. Select Elastic IPs and click Allocate New Address.
2. Select EC2-VPC and click Yes, Allocate.
3. Select the newly allocated EIP and click Associate Address.
4. Select the Network Interface and the Private IP address associated with the management interface and click Yes, Associate.

**STEP 5 | Configure a new administrative password for the firewall.**



*On the VM-Series firewall CLI, you must configure a unique administrative password before you can access the web interface of the firewall. To log in to the CLI, you require the private key that you used to launch the firewall.*

1. Use the EIP to SSH into the Command Line Interface (CLI) of the VM-Series firewall. You will need the private key that you used or created in [#ide203b126-ee2c-46d9-9caa-23f1a1023fcd/id89c6ac81-128f-488a-b01d-a473f93925da](#) above and using the user name admin to access the CLI.

If you are using PuTTY for SSH access, you must convert the .pem format to a .ppk format. See <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html>

2. Enter the following command to log in to the firewall:

```
ssh -i <private_key.pem> admin@<public-ip_address>
```

3. Configure a new password, using the following command and follow the onscreen prompts:

```
configure
```

```
set mgt-config users admin password
```

4. If you have a BYOL that needs to be activated, set the DNS server IP address so that the firewall can access the Palo Alto Networks licensing server. Enter the following command to set the DNS server IP address:

```
set deviceconfig system dns-setting servers primary <ip_address>
```

5. Commit your changes with the command:

```
commit
```

6. Terminate the SSH session.

## STEP 6 | Configure the dataplane network interface as a Layer 3 interface on the firewall.



*On the application servers within the VPC, define the dataplane network interface of the firewall as the default gateway.*

1. Using a secure connection (https) from your web browser, log in using the EIP address and password you assigned during initial configuration ([https://<Elastic\\_IP\\_address>](https://<Elastic_IP_address>)). You will see a certificate warning; that is okay. Continue to the web page.
2. Select Network > Interfaces > Ethernet.
3. Click the link for ethernet 1/1 and configure as follows:

- Interface Type: Layer3
- On the Config tab, assign the interface to the default router.
- On the Config tab, expand the Security Zone drop-down and select New Zone. Define a new zone and then click OK.
- On the IPv4 tab, select DHCP Client.

If using DHCP, select DHCP Client; the private IP address that you assigned to the ENI in the AWS management console will be automatically acquired.

- On the Advanced tab, create a management profile to allow health checks to be received by the firewall.
4. Click Commit. Verify that the link state for the interface is up.

## STEP 7 | Create security policies to allow/deny traffic.



*Because the VM-Series treats traffic as intrazone when deployed behind an appliance gateway, a default intrazone rule allows all traffic. It is a best practice to override the*

---


*default intrazone rule with a deny action for traffic that does not match any of your other security policy rules.*

1. Select Policies > Security on the web interface of the firewall.
2. Click Add, and specify the security zones, applications and logging options that you would like to execute to restrict and audit traffic traversing through the network.

**STEP 8** | Commit the changes on the firewall.

# Advanced Options for Manual Deployment

In addition to the procedures described above, you can configure the parameters necessary to deploy the VM-Series firewall behind an appliance gateway using the firewall CLI. Each op-command used in the user-data has an equivalent CLI command.

Operation Command	CLI Command	Description
mgmt-interface-swap=enable	set system setting mgmt-interface-swap enable yes	Swaps eth0 and eth1. Eth0 becomes a data interface and eth1 becomes the management interface.   <i>This command requires the firewall to reboot before taking effect.</i>
aws-agw-inspect:enable	request plugins vm_series aws agw inspect enable <yes/no>	Enables the VM-Series firewall to properly process traffic behind an appliance gateway.
aws-agw-associate-agwe:vpce-<vpce-id>@ethernet<subinterface>	request plugins vm_series aws agw associate vpc-endpoint <vpce-id> interface <subinterface>	Associates a VPC endpoint with an interface or subinterface on the firewall. The specified interface is assigned to a security zone.
—	request plugins vm_series aws agw disassociate vpc-endpoint <vpce-id> interface <subinterface>	Disassociates a VPC endpoint with an interface or subinterface on the firewall. The specified interface is assigned to a security zone.
—	show plugins vm_series aws agw	Displays the operating state of the firewall as it relates to your appliance gateway deployment. It does not display the firewall configuration.  For example, if you configure an association to an interface that does not exist, that association is configured but not part of the operating state. Therefore, it is not displayed.



If you associate VPC endpoints to subinterfaces via user data while bootstrapping and your `bootstrap.xml` file does not include the subinterface configuration, you can configure the subinterfaces after the firewall boots up.

If your deployment includes multiple VPCs but no transit gateway, you might encounter an issue with overlapping CIDRs. To avoid this issue, you can separate the traffic from each VPC by associating a VPC endpoint with a subinterface with a different security zone on your VM-Series firewall.

Complete the following procedure to create a subinterface in a different and associate it with a VPC endpoint.

### STEP 1 | Log in to the VM-Series firewall web interface.

### STEP 2 | Create the subinterface.

1. Select Network > Interface.
2. Highlight ethernet1/1 and click Add Subinterface.
3. Enter a numerical suffix (1 to 9,999) to identify the subinterface.
4. Enter a VLAN Tag (1 to 4,094) for the subinterface. This field is required but the VLAN is not used.
5. Select a Virtual Router.
6. Select a Security Zone.
7. Click OK.

The screenshot shows the 'Layer3 Subinterface' configuration window. The 'Interface Name' field is set to 'ethernet1/1' and the 'Tag' field is set to '1'. The 'Comment' field is empty. The 'Tag' field is set to '10'. The 'Netflow Profile' is set to 'None'. The 'Config' tab is selected, showing the 'Assign Interface To' section with 'Virtual Router' set to 'default' and 'Security Zone' set to 'agw'. The 'OK' button is highlighted in blue.

8. Repeat this command for each VPC endpoint.

### STEP 3 | Associate the subinterface with a VPC endpoint.

1. Execute the following command.  

```
request plugins vm_series aws agw associate vpc-endpoint <vpce-id>
interface <subinterface>
```

For example:

```
request plugins vm_series aws agw associate vpc-endpoint
vpce-02c4e6g8ha97h7e39 interface ethernet1/1.4
```



You can locate the VPC endpoint ID in the AWS console.

2. Repeat this command for each subinterface and VPC endpoint association.

### STEP 4 | Verify your subinterface to VPC endpoint associations.

```
show plugins vm_series aws agw
```

---

```
AGW enabled:      True
Overlay Routing:  False
```

```
-----
VPC endpoint      Interface
-----
vpce-0aeb1a919bd4ae609  ethernet1/1.1
vpce-0294375bfe413f04a  ethernet1/1.2
```

**STEP 5** **[(Optional)]** If necessary, you can use the following command to disassociate a VPC endpoint from a subinterface.


```
request plugins vm_series aws agw disassociate vpc-endpoint <vpce-id>
interface <subinterface>
```



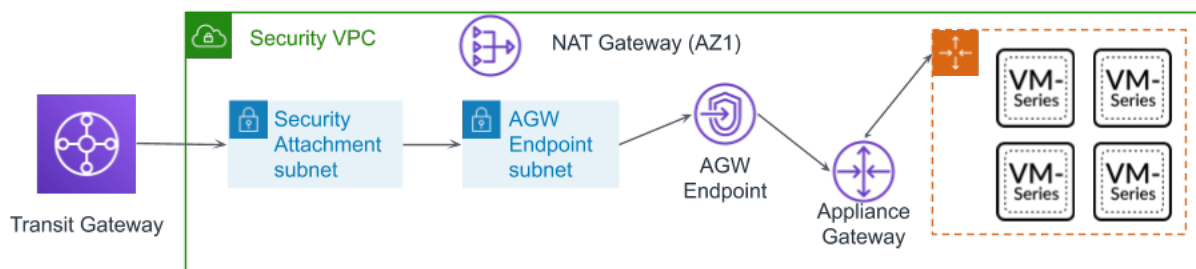
# Launch the Security VPC Template

The Palo Alto Networks auto scaling template for AWS help you deploy and configure the VM-Series firewall behind an appliance gateway to protect applications deployed in AWS. The template leverage AWS scalability features to independently and automatically scale VM-Series firewalls deployed in AWS to meet surges in application workload resource demand.

This version of the solution provides a security VPC template and an application template. The security VPC template deploys the VM-Series firewall auto scaling group, an appliance gateway, an appliance gateway endpoint, appliance gateway endpoint subnet, security attachment subnet, and a NAT gateway for each availability zone.

 *The template does not deploy a transit gateway. You must configure the transit gateway manually.*

*The beta supports only one availability zone.*




This workflow describes how to deploy the security VPC template.

## STEP 1 | Ensure that you have the following before you begin.

- Obtain the auth code for a bundle that supports the number of firewalls that might be required for your deployment. You must save this auth code in a text file named `authcodes` (no extensions), and put the `authcodes` file in the `/license` folder of the bootstrap package.
- Download the files required to launch the [VM-Series Appliance Gateway](#) template from the GitHub repository.
- Create a [Transit Gateway](#). This transit gateway connects your security and application VPCs. Take note of the transit gateway ID; you will need it later when deploying the template.

Ensure that Default route table association and Default route table propagation are disabled.

 *The target group of the appliance gateway cannot use HTTP for health checks because the VM-Series firewall does not allow access with an unsecured protocol. Instead use HTTPS or TCP.*

## STEP 2 | Deploy Panorama running 10.0.2 and configure the following.

Panorama must allow AWS public IP addresses. The VM-Series firewall accesses Panorama using the external IP address of the NAT gateway created by the template.

## STEP 3 | Configure the template.

1. Log in to the Panorama web interface.
2. Select Panorama > Templates and click Add.
  1. Enter a descriptive Name.

- 
2. Click OK.
  3. Configure the virtual router.
    1. Select Network > Virtual Routers.
    2. Ensure that you have selected the template you create above from the Template drop-down.
    3. Click Add.
    4. Name the virtual router using the following format: VR-<tempstackname>.
    5. Enable ECMP on the virtual router.
    6. Click OK.
  4. Configure the interface and create the zone.
    1. Select Network > Interfaces and click Add Interface.
    2. Select Slot 1.
    3. Set Interface Type to Layer 3.
    4. On the Config tab, select New Zone from the Security Zone drop-down. In the Zone dialog, define a Name for new zone, for example Internet, and then click OK.
    5. In the Virtual Router drop-down, select virtual router your created above.
    6. Select IPv4 and click DHCP Client.
    7. Click OK.
  5. Configure the DNS server and FQDN refresh time.
    1. Select Device > Setup > Services and click the Edit icon.
    2. Set the Primary DNS Server to 169.254.169.253. This is the AWS DNS address.
    3. Set the Minimum FQDN Refresh Time to 60 seconds.
    4. Click OK.
  6. Commit your changes. This is required before proceeding to the next step.
  7. Create an administrator.
    1. Select Device > Administrators.
    2. Enter **pandemo** as the Name.
    3. Set the Password to **demopassword** and Confirm.
    4. Click OK.
  8. Commit your changes.

#### **STEP 4 | Create the Device Group.**

1. Select Panorama > Device Groups.
2. Ensure that you have selected the device group you create above from the Device Group drop-down.
3. Click Add.
4. Enter a descriptive Name.
5. Click OK.
6. Add an allow all security pre-rule.
  1. Select Policies > Security > Pre Rules and click Add.
  2. Enter a descriptive Name.
  3. Under Source, User, Destination, Application, and Service/URL Category, select any.
  4. Under Actions, select Allow.
  5. Click OK.
7. Commit your changes.

#### **STEP 5 | Add the license deactivation API key for the firewall to Panorama.**

1. Log in to the Customer Support Portal.

2. Select Assets > Licensing API.
3. Copy the API key.
4. Use the CLI to install the API key copied in the previous step.

```
request license api-key set key <key>
```

#### STEP 6 | Modify the `init-cfg.txt` file and upload it to the `/config` folder.

Because you use Panorama to bootstrap the VM-Series firewalls, your `init-cfg.txt` file should be modified as follows. No `bootstrap.xml` file is needed.

Ensure that you use the device group and template names you created above in the `init-cfg.txt` file.

```
type=dhcp-client
ip-address=
default-gateway=
netmask=
ipv6-address=
ipv6-default-gateway=
hostname=
vm-auth-key=
panorama-server=
panorama-server-2=
tplname=
dgroup=
dhcp-send-hostname=yes
dhcp-send-client-id=yes
dhcp-accept-server-hostname=yesdhcp-accept-server-domain=yes
plugin-op-commands=aws-agw-inspect:enable
```

Your `init-cfg.txt` file must include `plugin-op-commands=aws-agw-inspect:enable`. This is required when deploying the VM-Series firewall behind an appliance gateway.

You must add the device certificate auto-registration PIN to the `init-cfg.txt` file to automatically install a [device certificate](#) when your VM-Series firewall instance is deployed.

#### STEP 7 | Add the license auth code in the `/license` folder of the bootstrap package.

1. Use a text editor to create a new text file named `authcodes` (no extension).
2. Add the authcode for your BYOL licenses to this file, and save. The authcode must represent a bundle, and it must support the number of firewalls that might be required for your deployment. If you use individual authcodes instead of a bundle, the firewall only retrieves the license key for the first authcode in the file.

#### STEP 8 | Upload Lambda code for the firewall template (`panw-aws.zip`) and the Application template (`app.zip`) to an S3 bucket. You can use the same S3 bucket that you use for bootstrapping.

If the Application stack is managed by a different account than the firewall, use the Application account to create another s3 bucket in the same AWS region as the firewall template and copy `app.zip` to that s3 bucket.

#### STEP 9 | Select the firewall template.

1. In the AWS Management Console, select CloudFormation > Create Stack.
2. Select Upload a template to Amazon S3, to choose the application template to deploy the resources that the template launches within the same VPC as the firewalls, or 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 10 | Enter a descriptive Name for your stack. The name must be 28 characters or less.**

**STEP 11 | Configure the parameters for the VPC.**

1. Enter one (1) for the number of availability zones and select the us-west-2a from the availability zone drop-down.
2. 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 version and the BYOL or PAYG licensing option you opted to use. See [Get the Amazon Machine Image IDs](#) for more information.
3. 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.
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 AWS 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 12 | Specify the name of the Amazon S3 bucket(s).**

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 fails, and you cannot log in to the firewall. Health checks for the load balancers also fail.
2. Enter the name of the S3 bucket that contains the panw-aws.zip file. As mentioned earlier you can use one S3 bucket for the Bootstrap and Lambda code.

**STEP 13 | Specify the keys for enabling API access to the firewall and Panorama.**

1. Enter the key that the firewall must use to authenticate API calls. The default key is based on the sample file and you should only use it 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. For a production deployment, you should create a separate login just for the API call and generate an associated key.

**STEP 14 | Add your AWS account number(s). You must provide the account number used to deploy any VPC that is connected to your appliance gateway. Add these values as a comma-separated list. You can add additional account numbers after deploying the template.**

To locate your account number, click your AWS username in the top right of the AWS console and select My Security Credentials.

**STEP 15 | Enter the maximum and minimum VM-Series firewalls for your auto scaling group.**

**STEP 16 | Enter the transit gateway ID. The transit gateway ID is required to secure east-west and outbound traffic. If you do not enter a transit gateway ID, the template assumes that only inbound traffic should be inspected by firewalls behind the appliance gateway.**

**STEP 17 | Enter the CIDR for the security VPC. The CIDR must be /25.**

---

**STEP 18 | 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.

**STEP 19 | Verify that the template has launched all required resources.**

---

# Launch the Application Template

Complete the following procedure to launch the application template.

## **STEP 1 | Create an S3 bucket from which you will launch the application template.**

- If this is a cross-account deployment, create a new bucket.
- If there is one account you can create a new bucket or use the S3 bucket you created earlier (you can use one bucket for everything).

## **STEP 2 | Upload the app.zip file into the S3 bucket.**

## **STEP 3 | Select the application launch template you want you launch.**

1. In the AWS Management Console, select CloudFormation > CreateStack
2. Select Upload a template to Amazon S3, to choose the application template to deploy the resources that the template launches within the same VPC as the firewalls, or 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 4 | Select the two Availability Zones that your setup will span in Select list of AZ. You must choose us-west-2a as the first AZ This template makes use of only one AZ but two are required to deploy the ALB.**

## **STEP 5 | Enter a descriptive VPC Name.**

## **STEP 6 | Configure the parameters for Lambda.**

1. Enter the S3 bucket name where app.zip is stored.
2. Enter the name of the zip file name.

## **STEP 7 | Select the EC2 instance type for the Ubuntu web server launched by this template.**

## **STEP 8 | Enter your Amazon EC2 key pair.**

## **STEP 9 | Enter the name of the service configuration (Service Name) for the AGW endpoint in the security VPC.**

1. Select DynamoDB from the Services drop-down in the AWS console.
2. Select Tables and locate your security VPC table.
3. Click the Items tab and copy the Service Name.
4. Paste the Service Name into the template configuration parameters.

## **STEP 10 | Enter the transit gateway ID. This is the same transit gateway you created before deploying the firewall template.**

## **STEP 11 | Review the template settings and launch the template.**

## **STEP 12 | After the application has been deployed, you must add a route to the transit gate route table to enable east-west and outbound traffic inspection.**

1. Log in to the AWS VPC console.
2. Select Transit Gateway Route Tables and choose your transit gateway route table. This route table is created by the template and is called <app-stack-name>-<region>-PANWAppAttRt.

- 
3. Select Routes and click Create static route.
  4. Enter 0.0.0.0/0 in the CIDR field.
  5. From the Choose attachment drop-down, select the VM-Series firewall VPC attachment.
  6. Click Create static route.

**STEP 13** |(Optional) **Create a bastion host (also called a jump box) to access the web server created by the application template.**

1. Create a public-facing [subnet](#) in your application VPC.
2. Add a route to this subnet from your IP address to the internet gateway.
3. Create a new EC2 instance in the public subnet with a public IP address.
4. Create a security group for this EC2 instance that allows SSH from your IP address.

---

# Known Issues

The following list describes known issues in the VM-Series firewall in AWS appliance gateway beta.

Bug ID	Description
PLUG-6264	<p>You can not use <code>op-command-modes=mgmt-interface-swap</code> along with <code>plugin-op-cmd</code> in the <code>init-cfg.txt</code> file.</p> <p><b>Workaround:</b> Use <code>mgmt-interface-swap=enable</code> in the AWS user-data field.</p>