VM-Series Deployment Guide

Version 8.0

paloaltonetworks.com/documentation

techDOCS

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

Last Revised

May 6, 2019

Table of Contents

About the VM-Series Firewall

The Palo Alto Networks VM-Series firewall is the virtualized form of the Palo Alto Networks next-generation firewall. It is positioned for use in a virtualized or cloud environment where it can protect and secure east-west and north-south traffic.

VM-Series Models

The VM-Series firewall is available in the following models—VM-50, VM-100, VM-200, VM-300, VM-500, VM-700 and VM-1000-HV.

All models can be deployed as guest virtual machines on VMware ESXi and vCloud Air, Citrix NetScaler SDX, KVM and KVM in OpenStack, and Microsoft Hyper-V. In the public cloud environments—Amazon Web Services, Azure—all models except the VM-50 are supported; on VMware NSX, only the VM-100, VM-200, VM-300, VM-500, and VM-1000-HV firewalls are supported. The software package (*.xva*, *.ova*, or *.vhdx* file) that is used to deploy the VM-Series firewall is common across all models. For information, see VM-Series Deployments.

When you apply the capacity license on the VM-Series firewall, the model number and the associated capacities are implemented on the firewall. Capacity is defined in terms of the number of sessions, rules, security zones, address objects, IPSec VPN tunnels, and SSL VPN tunnels that the VM-Series firewall is optimized to handle. To make sure that you purchase the correct model for your network requirements, use the following table to understand the maximum capacity for each model and the capacity differences by model:

Model	Sessions	Security Rules	Dynamic IP Addresses	Security Zones	IPSec VPN Tunnels	SSL VPN Tunnels
VM-50	50,000	250	1,000	15	250	250
VM-100 VM-200	250,000	1,500	2,500	40	1,000	500
VM-300 VM-1000-HV	800,000	10,000	100,000	40	2,000	2,000
VM-500	2,000,000	10,000	100,000	200	4,000	6,000
VM-700	10,000,000	20,000	100,000	200	8,000	12,000

To compare the different VM-Series firewall models, see the Palo Alto Networks Firewall comparison tool. You can also review general information About the VM-Series Firewall.

- VM-Series System Requirements
- CPU Oversubscription

VM-Series System Requirements

Each instance of the VM-Series firewall requires a minimum resource allocation—number of CPUs, memory, and disk space, on its host server. Use the table below to verify that you allocate the necessary hardware resources for your VM-Series model.

When upgrading to 8.0 or the VM-Series model license, you may be required to allocate additional hardware resources before completing your upgrade.

VM-Series Model	Supported Hypervisors	Supported vCPUs	Minimum Memory	Minimum Hard Drive
VM-50	ESXi, KVM, Hyper-V	2	4.5GB	32GB (60GB at boot)
VM-100 VM-200	ESXi, KVM, Hyper-V, AWS, Azure, NSX, SDX	2	6.5GB	60GB
VM-300 VM-1000-HV	ESXi, KVM, Hyper-V, AWS, Azure, NSX, SDX	2, 4	9GB	60GB
VM-500	ESXi, KVM, Hyper-V, AWS, Azure, NSX	2, 4, 8	16GB	60GB
VM-700	ESXi, KVM, Hyper-V, AWS, Azure	2, 4, 8, 16	56GB	60GB

To achieve the best performance, all of the needed cores should be available on a single CPU socket.

For operation, the VM-50 firewall requires minimum 32GB of hard drive space. However, because the VM-Series base image is common to all models, you must allocate 60GB of hard drive space until you license the VM-50.

The number of vCPUs assigned to the management plane and those assigned to the dataplane differs depending on the total number of vCPUs assigned to the VM-Series firewall. If you assign more vCPUs than those officially supported by the license, any additional vCPUs are assigned to the management plane.

Total vCPUs	Management Plane vCPUs	Dataplane vCPUs
2	1	1
4	2	2
8	2	6
16	4	12

CPU Oversubscription

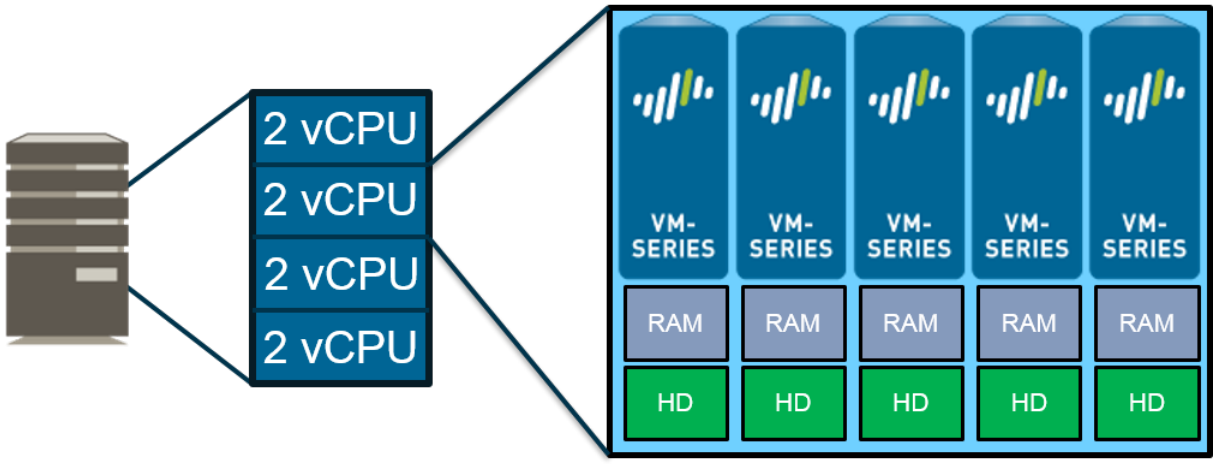
The VM-Series firewall supports CPU oversubscription on all models. CPU oversubscription allows you deploy a higher density of VM-Series firewalls on hypervisors running on x86 architecture. You can deploy two (2:1) to five (5:1) VM-Series firewalls per required allocation of CPUs. When planning your deployment, use the following formula to calculate the number of VM-Series firewalls your hardware can support.

(Total CPUs x Oversub Ratio)/CPUs per firewall = total number of VM-Series firewalls

For example, at a 5:1 ratio, a host machine with 16 physical CPU and at least 180GB of memory (40 × 4.5GB) can support up to 40 instances to the VM-50. Each VM-50 requires two vCPUs and five VM-50s can be associated to each pair of vCPUs.

(16 CPUs x 5)/2 = 40 VM-50 firewalls

Beyond meeting the minimum VM-Series System Requirements, no additional configuration is required to take advantage of oversubscription. Deploy VM-Series firewalls normally and resource oversubscription occurs automatically. When planning your deployment, consider other functions, such as virtual switches, and guest machines on the host that require hardware resources of their own.

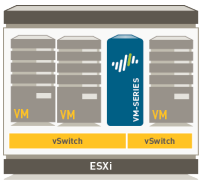


VM-Series Deployments

The VM-Series firewall can be deployed on the following platforms:

- **VM-Series for VMware vSphere Hypervisor (ESXi) and vCloud Air**

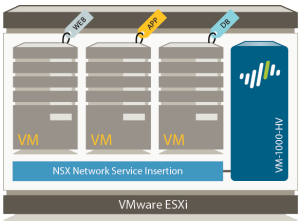
  You can deploy any VM-Series model as a guest virtual machine on VMware ESXi; ideal for cloud or networks where virtual form factor is required.



  For details, see Set Up a VM-Series Firewall on an ESXi Server and Set Up the VM-Series Firewall on vCloud Air.

- **VM-Series for VMware NSX**

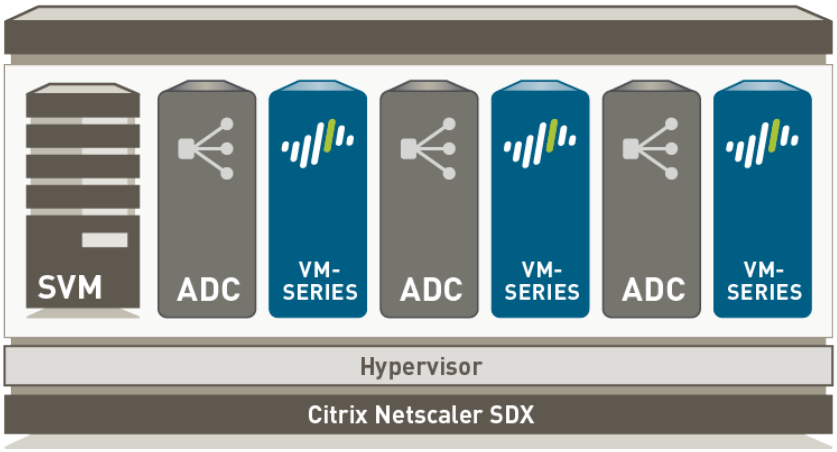
  The VM-100, VM-200, VM-300, VM-500, or VM-1000-HV is deployed as a network introspection service with VMware NSX, and Panorama. This deployment is ideal for east-west traffic inspection, and it also can secure north-south traffic.



  For details, see Set Up the VM-Series Firewall on VMware NSX

- **VM-Series for Citrix SDX**

  VM-100, VM-200, VM-300, or VM-1000-HV is deployed as guest virtual machine on Citrix NetScaler SDX; consolidates ADC and security services for multi-tenant and Citrix XenApp/XenDesktop deployments.



  For details, see Set Up a VM-Series Firewall on the Citrix SDX Server

- **VM-Series for Amazon Web Services (AWS)**

  You can deploy any VM-Series model, except the VM-50, on EC2 instances on the AWS Cloud.

For details, see Set Up the VM-Series Firewall on AWS.

- **VM-Series for Kernel Virtualization Module (KVM)**

  You can deploy any VM-Series model on a Linux server that is running the KVM hypervisor. For details, see Set Up the VM-Series Firewall on KVM.

- **VM-Series for Microsoft Hyper-V**

  You can deploy any VM-Series model on a Windows Server 2012 R2 server with the Hyper-V role add-on enabled or a standalone Hyper-V 2012 R2 server. For details, see Set Up the VM-Series Firewall on Hyper-V.

- **VM-Series for Microsoft Azure**

  You can deploy any VM-Series model, except the VM-50, on the Azure VNet.

  For details, see Set up the VM-Series Firewall on Azure.

- **VM-Series for OpenStack**

  You can deploy any VM-Series model on KVM in your OpenStack environment. For details, see Set Up the VM-Series Firewall on OpenStack.

VM-Series in High Availability

High availability (HA) is a configuration in which two firewalls are placed in a group and their configuration is synchronized to prevent a single point of failure on your network. A heartbeat connection between the firewall peers ensures seamless failover in the event that a peer goes down. Setting up the firewalls in a two-device cluster provides redundancy and allows you to ensure business continuity. In an HA configuration on the VM-Series firewalls, both peers must be deployed on the same type of hypervisor, have identical hardware resources (such as CPU cores/network interfaces) assigned to them, and have the set same of licenses/subscriptions. For general information about HA on Palo Alto Networks firewalls, see High Availability.

The VM-Series firewalls support stateful active/passive or active/active high availability with session and configuration synchronization. The active/active deployment is supported in virtual wire and Layer 3 deployments, and is recommended only if each firewall needs its own routing instances and you require full, real-time redundancy out of both firewalls all the time. To configure the VM-Series firewall as an HA pair, see Configure Active/Passive HA and Configure Active/Active HA.

If you are deploying the VM-Series firewall in the public cloud, such as on the Amazon Web Services (AWS) or Azure, the traditional HA architecture may not be as relevant because of the innate differences in how resource or region redundancy is built into the cloud infrastructure as compared to a private data center. So, to take advantage of native cloud services and build a resilient architecture that maximizes uptime, see

- AWS— Auto Scale VM-Series Firewalls with the Amazon ELB to deploy multiple firewalls across two or more Availability Zones within a VPC.

  The VM-Series firewall on the Amazon Web Services (AWS) cloud also supports traditional active/passive HA configuration, if you need it, see High Availability for VM-Series Firewall on AWS.
- Azure— VM-Series and Azure Application Gateway Template Parameters.

Features/ Links Supported	ESX	KVM	SDX	AWS	NSX	Hyper-V	Azure
Active/Passive HA	Yes	Yes	Yes	Yes	No	Yes	No
Active/Active HA	Yes	Yes	Yes	No	No	Yes	No
HA 1	Yes	Yes	Yes	Yes	No	Yes	No
HA2—(session synchronization and keepalive)	Yes	Yes	Yes	Yes	No	Yes	No
HA3	Yes	Yes	Yes	No	No	Yes	No

Upgrade the VM-Series Firewall

- Upgrade the PAN-OS Software Version (Standalone Version)
- Upgrade the PAN-OS Software Version (VM-Series for NSX)
- Upgrade the VM-Series Model
- Upgrade the VM-Series Model in an HA Pair

For instructions on installing your VM-Series firewall, see VM-Series Deployments.

Upgrade the PAN-OS Software Version (Standalone Version)

Now that the VM-Series firewall has network connectivity and the base PAN-OS software is installed, consider upgrading to the latest version of PAN-OS. Use the following instructions for firewalls that are not deployed in a high availability (HA) configuration. For firewalls deployed in HA, refer to the PAN-OS 8.0 New Features Guide.To minimize downtime for your users, perform upgrades during non-business hours.

STEP 1 | Verify that enough hardware resources are available to the VM-Series firewall. Refer to the VM-Series System Requirements to see the new resource requirements for each VM-Series model. Allocate additional hardware resources before continuing the upgrade process. The process for assigning additional hardware resources differs on each hypervisor.

STEP 2 | From the web interface, navigate to **Device** > **Licenses** and make sure you have the correct VM-Series firewall license and that the license is activated.

On the VM-Series firewall standalone version, navigate to **Device** > **Support** and make sure that you have activated the support license.

STEP 3 | (Required for a firewall that is in production) Save a backup of the current configuration file.

1. Select **Device** > **Setup** > **Operations** and click **Export named configuration snapshot**.
2. Select the XML file that contains your running configuration (for example, **running-config.xml**) and click **OK** to export the configuration file.
3. Save the exported file to a location external to the firewall. You can use this backup to restore the configuration if you have problems with the upgrade.

STEP 4 | Check the Release Notes to verify the Content Release version required for the PAN-OS version. The firewalls you plan to upgrade must be running the Content Release version required for the PAN-OS version.

1. Select **Device** > **Dynamic Updates**.
2. Check the **Applications and Threats** or **Applications** section to determine what update is currently running.
3. If the firewall is not running the required update or later, click **Check Now** to retrieve a list of available updates.
4. Locate the desired update and click **Download**.
5. After the download completes, click **Install**.

STEP 5 | Upgrade the PAN-OS version on the VM-Series firewall.

1. Select **Device** > **Software**.
2. Click **Refresh** to view the latest software release and also review the **Release Notes** to view a description of the changes in a release and to view the migration path to install the software.
3. Click **Download** to retrieve the software then click **Install**.

STEP 6 | If you are upgrading from PAN-OS 7.1 to PAN-OS 8.0, transition your VM-Series firewall from a 40GB hard disk to a 60GB hard disk.

1. On your hypervisor, attach a new 60GB hard drive to the VM-Series firewall. This new disk must be 60GB. The firewall will return an error if another value is assigned.
2. Access the firewall CLI.
3. Use the following CLI command to create a new disk partition to copy the data from the original system disk to the new system disk.

```
> request system

clone-system-disk target sdb
```

4. Return to your hypervisor and power off the VM-Series firewall.
5. Remove the original system disk.
6. Power on the VM-Series firewall.

Upgrade the PAN-OS Software Version (VM-Series for NSX)

Choose the upgrade method that best suits your deployment.

- Upgrade the VM-Series for NSX During a Maintenance Window—use this option to upgrade the VM-Series firewall during a maintenance window without changing the OVF URL in the service definition.
- Upgrade the VM-Series for NSX Without Disrupting Traffic—use this option to upgrade the VM-Series firewall without disrupting service to the guest VMs or changing the OVF URL in the service definition.
- Upgrade the VM-Series for NSX by Changing the OVF URL—use this option to upgrade the VM-Series firewall by changing the OVF URL in the service definition.
- Migrate Panorama 7.1 Configuration to Panorama 8.0 Configuration—this procedure describes migrating your operations-centric configuration to a security-centric configuration.

Upgrade the VM-Series for NSX During a Maintenance Window

For the VM-Series Firewall NSX edition, use Panorama to upgrade the software version on the firewalls. Complete this procedure during a maintenance window because it will disrupt traffic flowing through the firewall.

STEP 1 | Allocate additional hardware resources to your VM-Series firewall.

Verify that enough hardware resources are available to the VM-Series firewall. Refer to the VM-Series System Requirements to see the new resource requirements for each VM-Series model. Allocate additional hardware resources before continuing the upgrade process. The process for assigning additional hardware resources differs on each hypervisor.

STEP 2 | Save a backup of the current configuration file on each managed firewall that you plan to upgrade.

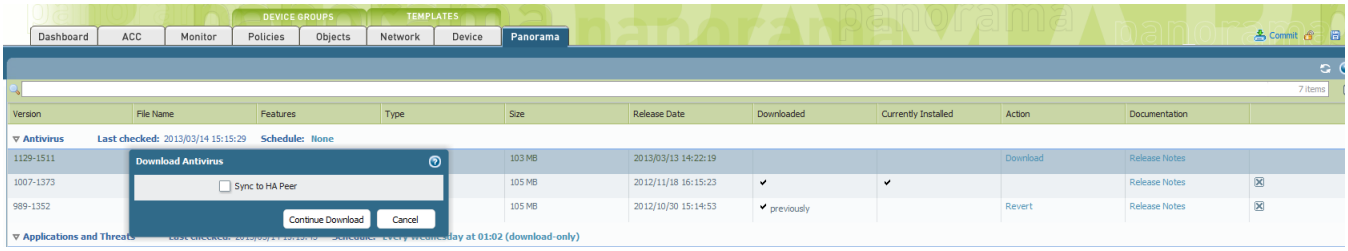
Although the firewall will automatically create a backup of the configuration, it is a best practice to create a backup prior to upgrade and store it externally.

1. Select **Device** > **Setup** > **Operations** and click **Export Panorama and devices config bundle**. This option is used to manually generate and export the latest version of the configuration backup of Panorama and of each managed device.
2. Save the exported file to a location external to the firewall. You can use this backup to restore the configuration if you have problems with the upgrade.

STEP 3 | Check the Release Notes to verify the Content Release version required for the PAN-OS version.

The firewalls you plan to upgrade must be running the Content Release version required for the PAN-OS version.

1. Select **Panorama** > **Device Deployment** > **Dynamic Updates**.
2. Check for the latest updates. Click Check Now (located in the lower left-hand corner of the window) to check for the latest updates. The link in the Action column indicates whether an update is available. If a version is available, the **Download** link displays.



3. Click **Download** to download a selected version. After successful download, the link in the **Action** column changes from **Download** to **Install**.
4. Click **Install** and select the devices on which you want to install the update. When the installation completes, a check mark displays in the **Currently Installed** column.

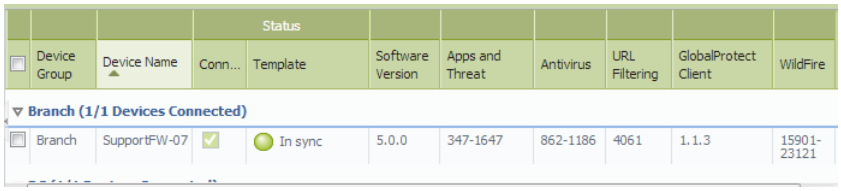
STEP 4 | Deploy software updates to selected firewalls.

If your firewalls are configured in HA, make sure to clear the Group HA Peers check box and upgrade one HA peer at a time.

1. Select **Panorama** > **Device Deployment** > **Software**.
2. Check for the latest updates. Click **Check Now** (located in the lower left-hand corner of the window) to check for the latest updates. The link in the **Action** column indicates whether an update is available.
3. Review the **File Name** and click **Download**. Verify that the software versions that you download match the firewall models deployed on your network. After successful download, the link in the **Action** column changes from **Download** to **Install**.
4. Click **Install** and select the devices on which you want to install the software version.
5. Select **Reboot device after install**, and click **OK**.
6. If you have devices configured in HA, clear the **Group HA Peers** check box and upgrade one HA peer at a time.

STEP 5 | Verify the software and Content Release version running on each managed device.

1. Select **Panorama** > **Managed Devices**.
2. Locate the device(s) and review the content and software versions on the table.



Upgrade the VM-Series for NSX Without Disrupting Traffic

Use the following procedure to upgrade the PAN-OS version of the VM-Series firewalls in your VMware NSX environment. This procedure allows you to perform the PAN-OS upgrade without disrupting traffic by migrating VMs to different ESXi hosts.

STEP 1 | Save a backup of the current configuration file on each managed firewall that you plan to upgrade.

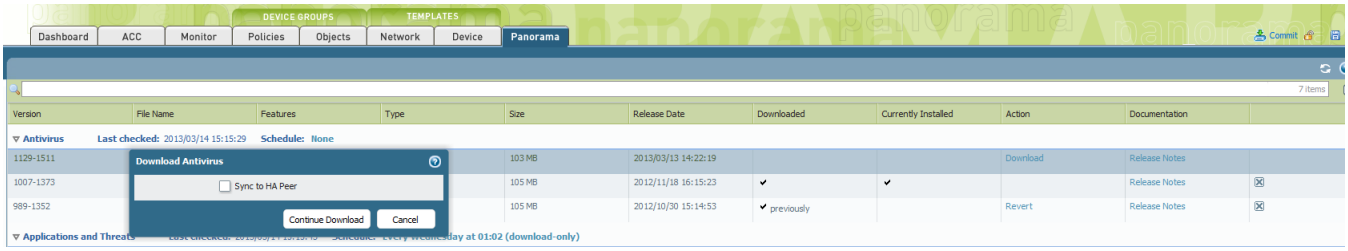
Although the firewall will automatically create a backup of the configuration, it is a best practice to create a backup prior to upgrade and store it externally.

1. Select **Device** > **Setup** > **Operations** and click **Export Panorama and devices config bundle**. This option is used to manually generate and export the latest version of the configuration backup of Panorama and of each managed device.
2. Save the exported file to a location external to the firewall. You can use this backup to restore the configuration if you have problems with the upgrade.

STEP 2 | Check the Release Notes to verify the Content Release version required for the PAN-OS version.

The firewalls you plan to upgrade must be running the Content Release version required for the PAN-OS version.

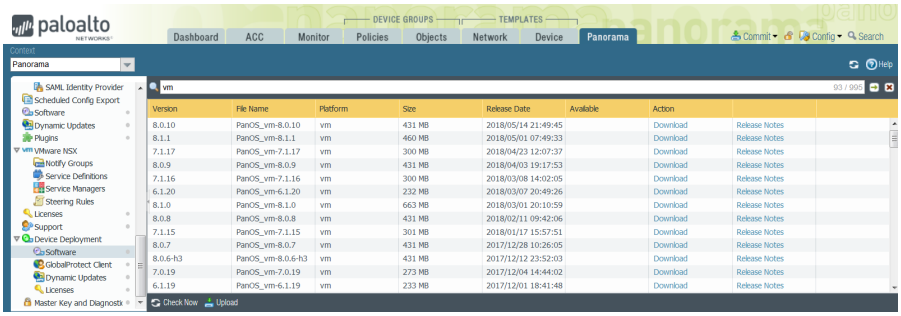
1. Select **Panorama** > **Device Deployment** > **Dynamic Updates**.
2. Check for the latest updates. Click Check Now (located in the lower left-hand corner of the window) to check for the latest updates. The link in the Action column indicates whether an update is available. If a version is available, the **Download** link displays.



3. Click **Download** to download a selected version. After successful download, the link in the **Action** column changes from **Download** to **Install**.
4. Click **Install** and select the devices on which you want to install the update. When the installation completes, a check mark displays in the **Currently Installed** column.

STEP 3 | Download the PAN-OS image to all VM-Series firewalls in the cluster.

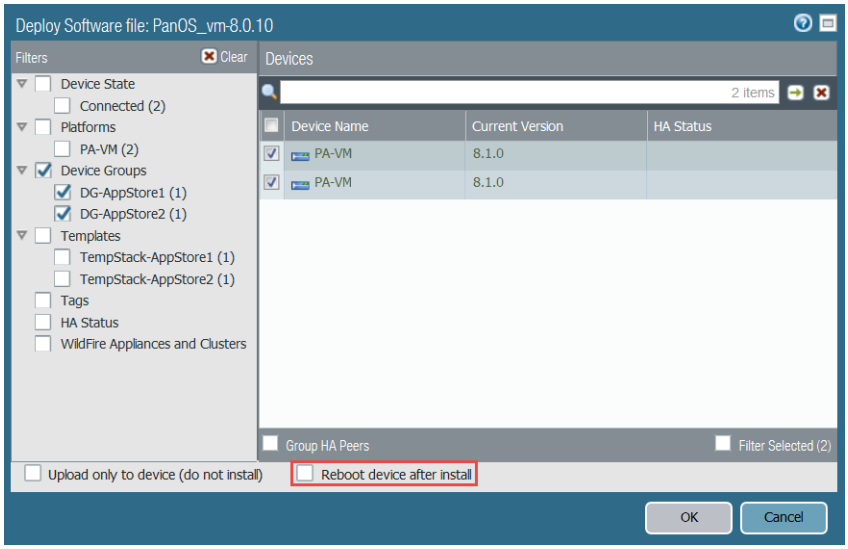
1. Login to Panorama.
2. Select **Panorama** > **Device Deployment** > **Software**.
3. Click **Refresh** to view the latest software release and also review the **Release Notes** to view a description of the changes in a release and to view the migration path to install the software.



4. Click **Download** to retrieve the software then click **Install**.

   Do not reboot the VM-Series firewalls after installing the new software image.

5. Select the managed devices to be upgraded.
6. Clear the **Reboot device after install** check box.



7. Click **OK**.

STEP 4 | Upgrade the VM-Series firewall on the first ESXi host in the cluster.

1. Login to vCenter.
2. Select **Hosts and Clusters**.
3. Right-click the host and select **Maintenance Mode** > **Enter Maintenance Mode**.
4. Migrate (automatically or manually) all VMs, except the VM-Series firewall, off of the host.
5. Power off the VM-Series firewall. This should happen automatically upon entering maintenance mode on the host.
6. (Optional) Assign additional CPUs or memory to the VM-Series firewall before continuing with the upgrade process.

   Verify that enough hardware resources are available to the VM-Series firewall. Refer to the VM-Series System Requirements to see the new resource requirements for each VM-Series model.
7. Right-click the host and select **Maintenance Mode** > **Exit Maintenance Mode**. Exiting maintenance mode causes the NSX ESX Agent Manager (EAM) to power on the VM-Series firewall. The firewall reboots with the new PAN-OS version.
8. Migrate (automatically or manually) all VMs back to the original host.

STEP 5 | Repeat this process for each VM-Series firewall on each ESXi host.

STEP 6 | Verify the software and Content Release version running on each managed device.

1. Select **Panorama** > **Managed Devices**.
2. Locate the device(s) and review the content and software versions on the table.

Upgrade the VM-Series for NSX by Changing the OVF URL

You can upgrade the PAN-OS version of your VM-Series firewall for NSX by changing the OVF URL in the service definition. If you do not change the OVF URL, any firewalls deployed in the future will be running the currently installed version of PAN-OS and require an additional upgrade. Changing the service definition requires you to redeploy the firewalls, which causes a disruption of service. Therefore, Palo Alto Networks recommends that you perform this upgrade during a maintenance window.

STEP 1 | Save a backup of the current configuration file of the firewalls that you plan to upgrade.

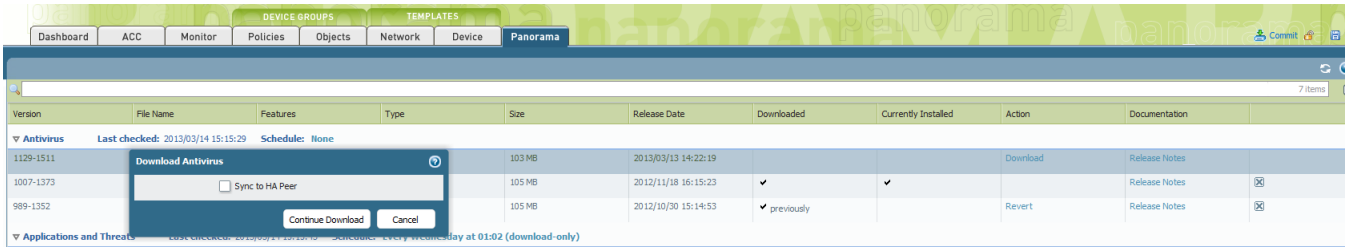
Although the firewall will automatically create a backup of the configuration, create a backup prior to upgrade and store it externally.

1. Select **Device** > **Setup** > **Operations** and click **Export Panorama and devices config bundle**. This option is used to manually generate and export the latest version of the configuration backup of Panorama and of each managed device.
2. Save the exported file to a location external to the firewall. You can use this backup to restore the configuration if you have problems with the upgrade.

STEP 2 | Check the Release Notes to verify the minimum Content Release.

The firewalls you plan to upgrade must be running the Content Release version required for the PAN-OS version.

1. Select **Panorama** > **Device Deployment** > **Dynamic Updates**.
2. Check for the latest updates. Click Check Now (located in the lower left-hand corner of the window) to check for the latest updates. The link in the Action column indicates whether an update is available. If a version is available, the **Download** link displays.



3. Click **Download** to download a selected version. After successful download, the link in the **Action** column changes from **Download** to **Install**.
4. Click **Install** and select the devices on which you want to install the update. When the installation completes, a check mark displays in the **Currently Installed** column.

STEP 3 | Download the PAN-OS 8.0 base image file.

1. Register your VM-Series firewall and obtain the OVA file from the Palo Alto Networks Customer Support web site.

Select the ovf file that matches the VM-Series model you plan to deploy. For the VM-200, use vm100.ovf. For the VM-1000-HV, use vm300.ovf.

2. Unzip the image file to extract and save the .ovf, mf, and .vmdk files to a directory accessible to NSX Manager. Place all three files in the same directory. These files are used to deploy each instance of the firewall.

   If needed, modify the security settings on the server so that you can download the file types. For example, on the IIS server modify the Mime Types configuration; on an Apache server edit the .htaccess file.

STEP 4 | Add the new OVF URL to your service definition configuration.

1. Select **Panorama** > **VMware NSX** > **Service Definitions**, and select the service definition you want to edit.
2. In **VM-Series OVF URL**, add the location of the web server that hosts the new ovf file. Both http and https are supported protocols. For example, enter https://acme.com/software/PA-VM-NSX.8.0.0.ovf.

   You can use the same ovf version or different versions across service definitions. Using different ovf versions across service definitions allows you to vary the PAN-OS version on the VM-Series firewalls in different ESXi clusters

   .
3. Click **OK**.
4. Select **Commit** > **Commit to Panorama** > **Commit**.

   Changing the OVF URL and committing it to Panorama triggers a configuration mismatch on NSX Manager. In vCenter, you must resolve the mismatch to redeploy the firewalls tied to the service definition.

STEP 5 | Manually deactivate the VM-Series for NSX license. Complete this task through the Panorama CLI or web interface.

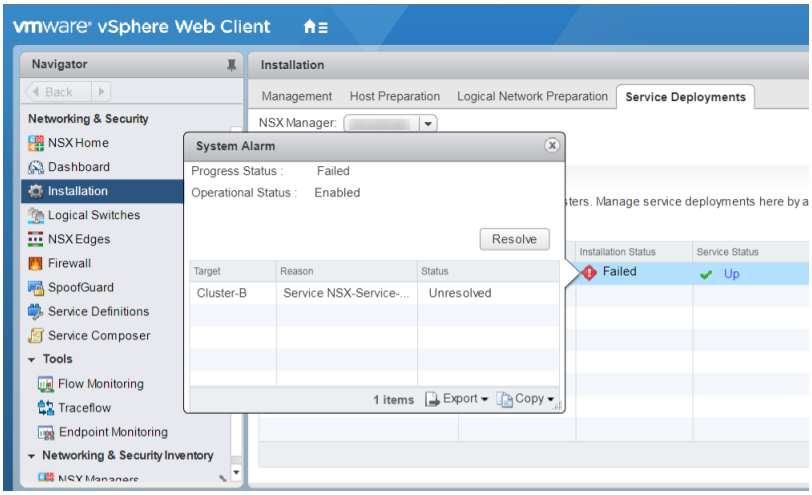
- Use the **`request license deactivate key features <name> mode manual`** CLI command Deactivate a Feature License or Subscription Using the CLI.
- To Deactivate the VM-Series for NSX license, choose **Complete Manually** (instead of **Continue**) and follow the steps to manually deactivate the license.

STEP 6 | Redeploy the firewalls. Redeploying your firewalls will interrupt any traffic moving across the firewalls.

1. Log in to vSphere.
2. Select **Network & Security** > **Installation** > **Service Deployments**.
3. Click the **Failed** icon in the Installation Status column to display the System Alarm window.
4. Click **Resolve**. Clicking Resolve redeploys the firewalls with the new ovf.

   Redeploying your firewalls will interrupt traffic that is redirected to the firewalls.



STEP 7 | Verify that your firewalls have redeployed successfully.

1. Select **Network & Security** > **Installation** > **Service Deployments**.
2. Verify that the Installation Status now displays Successful.

Upgrade the VM-Series Model

The licensing process for the VM-Series firewall uses the UUID and the CPU ID to generate a unique serial number for each VM-Series firewall. Hence, when you generate a license, the license is mapped to a specific instance of the VM-Series firewall and cannot be modified.

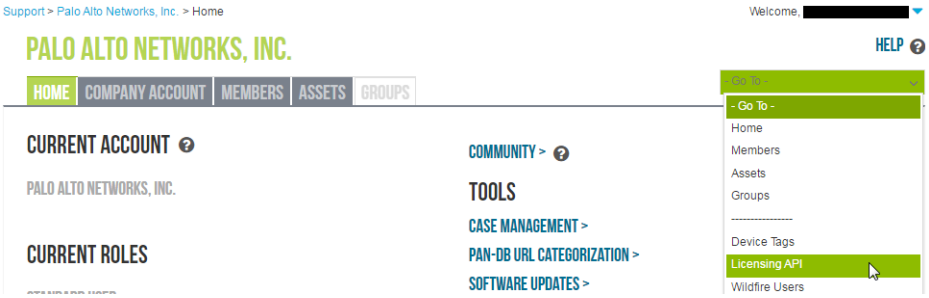
Use the instructions in this section, if you are:

- Migrating from an evaluation license to a production license.
- Upgrading the model to allow for increased capacity. For example you want to upgrade from the VM-100 to the VM-300 model.

A capacity upgrade restarts some critical processes on the firewall. An HA configuration is recommended to minimize service disruption; to upgrade the capacity on a HA pair, see Upgrade the VM-Series Model in an HA Pair.

STEP 1 | Retrieve the license deactivation API key from the Customer Support Portal.

1. Log in to the Customer Support Portal.
2. From the Go To drop-down, select **License API**.
3. Copy the API key.



Make sure that you are using the same account that you used to register the initial license.

STEP 2 | On the firewall, use the CLI to install the API key copied in the previous step.

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

STEP 3 | Enable the firewall to **Verify Update Server identity** on **Device** > **Setup** > **Service**.

STEP 4 | **Commit** your changes.

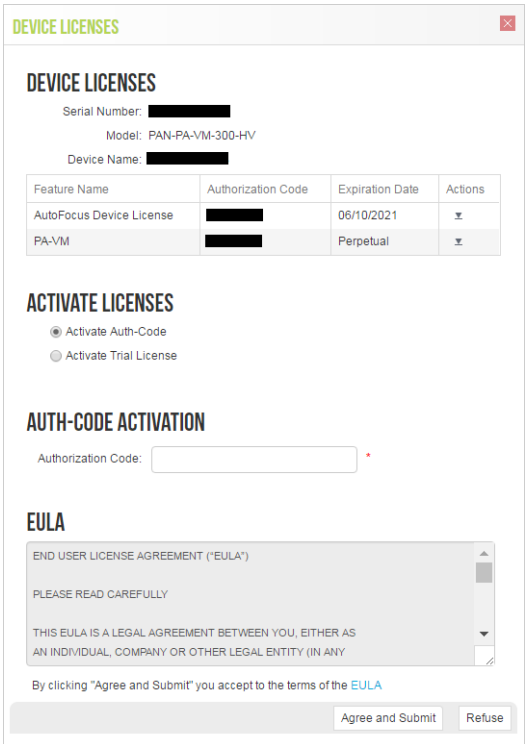
STEP 5 | Continue to the next step if you are upgrading capacity. If you are migrating your license, do the following

1. Register the VM-Series Firewall.
2. Retrieve the license keys on the firewall. See Activate the License.
3. Go to the last step to verify that your firewall is licensed successfully.

STEP 6 | Upgrade the license on the Customer Support portal.

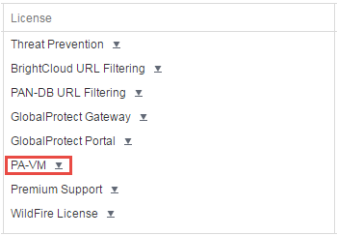
Skip this step if you are upgrading the capacity with an authorization code.

1. Log in to the Palo Alto Networks Customer Support portal.
2. Select **Assets** > **Devices** and search for your firewall by the serial number.
3. Select the Action icon to open the Device Licenses window.
4. Select **Activate Upgrade License** and enter the authorization code for the higher capacity VM.



5. Select **Agree and Submit**.
6. (Optional) If your VM-Series firewall does not have direct internet access, download the capacity upgrade license key.

1. Select **Assets** > **Devices** and search for your firewall by the serial number.
2. Under the License column, select the download icon next to PA-VM to download the license key.
3. Save the license key to a location the VM-Series firewall can access.



STEP 7 | Allocate additional hardware resources to your VM-Series firewall.

Before initiating the capacity upgrade, you must verify that enough hardware resources are available to the VM-Series firewall to support the new capacity. The process for assigning additional hardware resources differs on each hypervisor.

To check the hardware requirements for your new VM-Series model, see VM-Series Models.

Although the capacity upgrade does not require a reboot of the VM-Series firewall, you need to power down the virtual machine to change the hardware allocation.

STEP 8 | Upgrade the capacity.

Select **Device** > **Licenses** > **Upgrade Capacity** and then activate your licenses and subscriptions in one of the following ways:

- **Retrieve license keys from license server**—Use this option if you activated your license on the Customer Support portal.
- **Manually upload license key**—Use this option if your firewall does not have connectivity to the Palo Alto Networks Customer Support web site. In this case, you must download a license key file from the support site on an Internet connected computer and then upload to the firewall.
- **Use an authorization code**—Use this option to upgrade the VM-Series capacity using an authorization code for licenses that have not been previously activated on the support portal. When prompted, enter the **Authorization Code** and then click **OK**.

STEP 9 | Verify that your firewall is licensed successfully.

On the **Device** > **Licenses** page, verify that the license was successfully activated.

Upgrade the VM-Series Model in an HA Pair

Upgrading the VM-Series firewall allows you to increase the capacity on the firewall. Capacity is defined in terms of the number of sessions, rules, security zones, address objects, IPSec VPN tunnels, and SSL VPN tunnels that the VM-Series firewall is optimized to handle. When you apply a new capacity license on the VM-Series firewall, the model number and the associated capacities are implemented on the firewall.

This process is similar to that of upgrading a pair of hardware-based firewalls that are in an HA configuration. During the capacity upgrade process, session synchronization continues, if you have it enabled. To avoid downtime when upgrading firewalls that are in a high availability (HA) configuration, update one HA peer at a time.

Do not make configuration change to the firewalls during the upgrade process. During the upgrade process, configuration sync is automatically disabled when a capacity mismatch is detected and is then re-enabled when both HA peers have matching capacity licenses.

If the firewalls in the HA pair have different major software versions (such as 7.1 and 8.0) and different capacities, both devices will enter the Suspended HA state. Therefore, it is recommended that you make sure both firewalls are running the same version of PAN-OS before upgrading capacity.

STEP 1 | Upgrade the capacity license on the passive firewall.

Follow the procedure to Upgrade the VM-Series Model.

The new VM-Series model displays on the dashboard after some processes restart on this passive peer. This upgraded peer is now is a non-functional state because of the capacity mismatch with its active peer.

If you have enabled session synchronization, verify that sessions are synchronized across HA peers before you continue to the next step. To verify session synchronization, run the **`show high-availability interface ha2`** command and make sure that the Hardware Interface counters on the CPU table are increasing as follows:

- In an active/passive configuration, only the active peer show packets transmitted and the passive device will only show packets received.

  If you have enabled HA2 keep-alive, the hardware interface counters on the passive peer will show both transmit and receive packets. This occurs because HA2 keep-alive is bidirectional which means that both peers transmit HA2 keep-alive packets.
- In an active/active configuration, you will see packets received and packets transmitted on both peers.

STEP 2 | Upgrade the capacity license on the active firewall.

Follow the procedure to Upgrade the VM-Series Model.

The new VM-Series model displays on the dashboard after the critical processes restart. The passive firewall becomes active, and this peer (previously active firewall) moves from the initial state to becoming the passive peer in the HA pair.

Enable Jumbo Frames on the VM-Series Firewall

By default, the maximum transmission unit (MTU) size for packets sent on a Layer 3 interface is 1500 bytes. This size can be manually set to any size from 512 to 1500 bytes on a per-interface basis. Some configurations require Ethernet frames with an MTU value greater than 1500 bytes. These are called jumbo frames.

To use jumbo frames on a firewall you must specifically enable jumbo frames at the global level. When this is enabled, the default MTU size for all Layer 3 interfaces is set to a value of 9192 bytes. This default value can then be set to any value in the range of 512 to 9216 bytes.

After setting a global jumbo frame size it becomes the default value for all Layer 3 interfaces that have not explicitly had an MTU value set at the interface configuration level. This can become a problem if you only want to exchange jumbo frames on some interfaces. In these situations, you must set the MTU value at every Layer 3 interface that you do not want to use the default value.

The following procedure describes how to enable jumbo frames on a firewall, set the default MTU value for all Layer 3 interfaces and to then set a different value for a specific interface.

STEP 1 | Enable jumbo frames and set a default global MTU value.

1. Select **Device** > **Setup** > **Session** and edit the Session Settings section.
2. Select **Enable Jumbo Frame**.
3. Enter a value for **Global MTU**.

   The default value is 9192. The range of acceptable values is: 512 - 9216.
4. Click **OK**.

   A message is displayed that informs you that enabling or disabling Jumbo Frame mode requires a reboot and that Layer 3 interfaces inherit the **Global MTU** value.
5. Click **Yes**.

   A message is displayed to inform you that Jumbo Frame support has been enabled and reminds you that a device reboot is required for this change to be activated.
6. Click **OK**.
7. Click **Commit**.

STEP 2 | Set the MTU value for a Layer 3 interface and reboot the firewall.

The value set for the interface overrides the global MTU value.

1. Select **Network** > **Interfaces**.
2. Select an interface of the Layer3 **Interface type**.
3. Select **Advanced** > **Other Info**.
4. Enter a value for **MTU**.

   The default value is 9192. The range of acceptable values is: 512 - 9216.
5. Click **OK**.
6. Click **Commit**.
7. Select **Device** > **Setup** > **Operations** and select **Reboot Device**.

Hypervisor Assigned MAC Addresses

By default, the VM-Series firewall uses the MAC address assigned to the physical interface by the host/hypervisor and use that MAC address on the VM-Series firewall deployed with Layer 3 interfaces. The firewall can then use the hypervisor assigned MAC address in its ARP responses. This capability allows non-learning switches, such as the VMware vSwitch to forward traffic to the dataplane interface on the firewall without requiring that promiscuous mode be enabled on the vSwitch. If neither promiscuous mode nor the use of hypervisor assigned MAC address is enabled, the host will drop the frame when it detects a mismatch between the destination MAC address for an interface and the host-assigned MAC address.

There is no option to enable or disable the use of hypervisor assigned MAC addresses on AWS and Azure. It is enabled by default for both platforms and cannot be disabled.

If you are deploying the VM-Series firewall in Layer 2, virtual wire, or tap interface modes, you must enable promiscuous mode on the virtual switch to which the firewall is connected. The use of hypervisor assigned MAC address is only relevant for Layer 3 deployments where the firewall is typically the default gateway for the guest virtual machines.

When hypervisor assigned MAC address functionality is enabled on the VM-Series firewall, make note of the following requirements:

- **IPv6 Address on an Interface**—In an active/passive HA configuration (see VM-Series in High Availability), Layer 3 interfaces using IPv6 addresses must not use the EUI-64 generated address as the interface identifier (Interface ID). Because the EUI-64 uses the 48-bit MAC address of the interface to derive the IPv6 address for the interface, the IP address is not static. This results in a change in the IP address for the HA peer when the hardware hosting the VM-Series firewall changes on failover, and leads to an HA failure.
- **Lease on an IP Address**—When the MAC address changes, DHCP client, DHCP relay and PPPoE interfaces might release the IP address because the original IP address lease could terminate.
- **MAC address and Gratuitous ARP**—VM-Series firewalls with hypervisor assigned MAC addresses in a high-availability configuration behave differently than the hardware appliances with respect to MAC addressing. Hardware firewalls use self-generated floating MAC addresses between devices in an HA pair, and the unique MAC address used on each dataplane interface (say eth 1/1) is replaced with a virtual MAC address that is common to the dataplane interface on both HA peers. When you enable the use of the hypervisor assigned MAC address on the VM-Series firewall in HA, the virtual MAC address is not used. The dataplane interface on each HA peer is unique and as specified by the hypervisor.

  Because each dataplane interface has a unique MAC address, when a failover occurs, the now active VM-Series firewall must send a gratuitous ARP so that neighboring devices can learn the updated MAC/IP address pairing. Hence, to enable a stateful failover, the internetworking devices must not block or ignore gratuitous ARPs; make sure to disable the anti-ARP poisoning feature on the internetworking devices, if required.

Perform the following steps to configure the VM-Series firewall to use the interface MAC addresses provided by the host/hypervisor.

STEP 1 | Select **Device** > **Management** > **Setup**.

STEP 2 | Disable (clear) the option to **Use Hypervisor Assigned MAC Address**.

When the MAC address change occurs, the firewall generates a system log to record this transition and the interface generates a gratuitous ARP.

STEP 3 | **Commit** the change on the firewall. You do not need to reboot the firewall.

License the VM-Series Firewall

Before you can start using your VM-Series firewall to secure east-west and north-south traffic on your network, you must activate the licenses for the services you purchased to secure your network.

If you are an authorized CSSP partner, see Licenses for Cloud Security Service Providers (CSSPs) for information that pertains to you.

For details on creating a support account and activating the licenses:

- License Types—VM-Series Firewalls
- Serial Number and CPU ID Format for the VM-Series Firewall
- Create a Support Account
- Register the VM-Series Firewall
- Switch Between the BYOL and the PAYG Licenses
- Renew VM-Series Firewall License Bundles
- Activate the License
- Deactivate the License(s) (to release the licenses attributed to a firewall)
- Licensing API
- Licenses for Cloud Security Service Providers (CSSPs)

License Types—VM-Series Firewalls

The following licenses and subscriptions are available for the VM-Series firewall:

- **Capacity License**—The VM-Series firewall requires a base license, also called a *capacity license,* to enable the model number (VM-50, VM-100, VM-200, VM300, VM-500, VM-700, or VM-1000-HV) and the associated capacities on the firewall. Capacity licenses are included in a bundle and can be perpetual or term-based:
  - **Perpetual License**—A license with no expiration date that allows you to use the VM-Series firewall at the licensed capacity, indefinitely. Perpetual licenses that are available for the VM-Series capacity license only.

    The perpetual licence is available so long as the support entitlement and subscriptions are renewed at the same level as the capacity license. When renewing your license, if you opt to renew for a lesser quantity than the originally purchased quantity, you will forfeit the perpetual licenses that you do not renew. For example, if your capacity license is for quantity 100, you must renew support and subscriptions for quantity 100 in order to retain the capacity license for all 100 going forward.
  - **Term-Based License**—A term-based license allows you to use the VM-Series firewall for a specified period of time. It has an expiration date and you will be prompted to renew the license before it expires. Term-based licenses are available for the capacity licenses, support entitlements, and subscriptions.
- **Support**—In addition to the capacity license, you need a support entitlement that provides access to technical support and software updates. With a license bundle, a premium support entitlement is included. If you need USG support, you must purchase BYOL on AWSGov Cloud and Azure Government.
- **Subscription Bundles**—The subscriptions allow you to enforce policies that safely enable applications and content on the network. For example, the Threat Prevention subscription, allows you to obtain content updates that include the most up-to-date threat information for malware detection. You can choose from two license bundles:
  - Basic bundle includes the VM-Series capacity license, and a premium support entitlement.
  - Bundle 1 includes the VM-Series capacity license, Threat Prevention license and a premium support entitlement.
  - Bundle 2 includes the VM-Series capacity license with the complete suite of licenses that includes Threat Prevention, GlobalProtect, WildFire, PAN-DB URL Filtering, and a premium support entitlement.

  With both license bundles, see Renew VM-Series Firewall License Bundles for renewal options. If you need to add more VM-Series firewalls before the renewal timeline, contact your partner, reseller, or Palo Alto Networks representative.
- **VM-Series ELA**—For enterprises with high growth, the VM-Series enterprise licensing agreement (VM-Series ELA) provides a fixed price licensing option that allows up to unlimited deployment of VM-Series firewalls with BYOL. The ELA is offered in one and three-year term agreements with no true-up at the end of the term.

  There are two flavors of the VM-Series ELA:
  - If you purchased the VM-Series ELA before December 4, 2018, you have the legacy VM-Series ELA which includes your choice of a single VM-Series model that you can deploy on any supported hypervisor or cloud environment. With this ELA, you receive a single license authorization code for capacity, support, GlobalProtect, PAN-DB URL Filtering, Threat Prevention, WildFire subscriptions for every instance of the VM-Series firewall. You also get unlimited deployments of the Panorama virtual appliance included with a device management license for 1000 firewalls on each.

Palo Alto Networks will begin phasing out the legacy VM-Series ELA on April 16, 2019. Existing enterprise license customers will be notified by their support representative when their account is migrated to the Multi-Model ELA. Licensing tokens will be distributed according to your VM-Series firewall subscription agreement — no additional action is necessary for continued operation of your firewalls. If you would like to Manage VM-Series ELA License Tokens, you must designate an ELA administrator. Only a super user role on the Palo Alto Networks Customer Support Portal (CSP) can assign an ELA administrator.

- The VM-Series Enterprise License Agreement (Multi-Model ELA) you purchase after December 4, 2018 (either as a new purchase or as a repurchase of the legacy VM-Series ELA) is called the multi-model VM-Series ELA that includes most models of the VM-Series firewall portfolio along with the GlobalProtect, PAN-DB URL Filtering, Threat Prevention, WildFire subscriptions, and support entitlement. You also get unlimited deployments of the Panorama virtual appliance with a device management license for 1000 firewalls on each.

VM-Series Firewall for NSX Licenses

In order to automate the provisioning and licensing of the VM-Series firewall for NSX in the VMware integrated NSX solution, two license bundles are available:

- One bundle includes the VM-Series capacity license (VM-100, VM-200, VM-300, VM-500, or VM-1000-HV only), Threat Prevention license and a premium support entitlement.
- Another bundle includes the VM-Series capacity license (VM-100, VM-200, VM-300, VM-500, or VM-1000-HV only) with the complete suite of licenses that include Threat Prevention, GlobalProtect, WildFire, PAN-DB URL Filtering, and a premium support entitlement.

VM-Series Firewall in Amazon Web Services (AWS) and Azure Licenses

You can license the VM-Series firewall in AWS and Azure in two ways:

- **Bring Your Own License (BYOL)**—A license that is purchased from a partner, reseller, or directly from Palo Alto Networks. Both Individual capacity and support licenses and subscription bundles are supported for BYOL. With individual licenses, you must apply the auth code after you deploy the VM-Series firewall; with a bundle, you can include a single auth code in the bootstrap package for all the subscriptions included in the bundle in order to license the firewall at launch.
- **Usage-Based License**—Also called a *pay-per-use* or *pay-as-you-go* (PAYG) license. This type of license can be purchased from the AWS Marketplace and the Azure public Marketplace. Usage-based licenses are not available on the Azure Government Cloud Marketplace.

  AWS supports hourly and annual PAYG options; Azure supports the hourly PAYG option only.

  With the usage-based licenses, the firewall is prelicensed and ready for use as soon as you deploy it; you do not receive an auth code. When the firewall is stopped or terminated on the AWS or Azure console, the usage-based licenses are suspended or terminated.

  Usage-based licenses are available in the following pricing bundles:

  - Bundle 1: Includes the VM-Series capacity license (VM-300 only), Threat Prevention license that includes IPS, AV, malware prevention, and a premium support entitlement.
  - Bundle 2: Includes the VM-Series capacity license (VM-300 only), Threat Prevention (includes IPS, AV, malware prevention), GlobalProtect, WildFire, PAN-DB URL Filtering licenses, and a premium support entitlement.

  If you have an evaluation copy of the VM-Series firewall and would like to convert it to a fully licensed (purchased) copy for the same license type (BYOL to BYOL), you

can deactivate the evaluation license and activate the purchased license in place. See Upgrade the VM-Series Firewall for instructions.

You cannot switch between the PAYG and the BYOL licenses. To move from PAYG to BYOL, contact your Palo Alto Networks channel partner or sales representative to purchase a BYOL license and get an BYOL auth code that you can use to license your firewall. If you have deployed your firewall and want to switch the license, see Switch Between the BYOL and the PAYG Licenses.

VM-Series Enterprise License Agreement (Multi-Model ELA)

The VM-Series Enterprise License Agreement (VM-Series ELA) is a one- or three-year comprehensive licensing agreement that enables you to purchase VM-Series firewalls, along with the GlobalProtect, PAN-DB URL Filtering, Threat Prevention, WildFire subscriptions. It also includes a support entitlement and a device management license for Panorama. The multi-model VM-Series ELA provides simplified license management with a single contract that allows you to deploy any model of the VM-Series firewall that meets your enterprise security needs.

When you purchase the multi-model VM-Series ELA, you forecast the number of firewalls that you'll need over the term of your subscription. Based on your forecast and an additional allotment that accommodates for future growth, your account on the Customer Support Portal (CSP) is credited with a license token pool that allows you to deploy any model of the VM-Series firewall. Depending on the firewall model and the number of firewalls that you deploy, a specified number of tokens are deducted from your available license token pool. The tokens drawn from your account are calculated based on the value of each firewall model:

- VM-50—10 tokens
- VM-100—25 tokens
- VM-300—50 tokens
- VM-500—140 tokens
- VM-700—300 tokens

With the VM-Series ELA, there is no true-up due at the end of the term which means that you are not billed retroactively even if you deploy more firewalls than your original forecast. So, to balance flexibility with accountability, the VM-Series ELA terms of use includes a bounded and unbounded period that explains how you can consume tokens and deploy firewalls as the need arises. For details, refer to the ELA terms and conditions. The VM-Series firewalls that you deploy with the VM-Series ELA do not have a perpetual license and on the expiry of the term, you must renew the agreement to extend the support entitlement and get continued access to software and content release updates on the firewalls.

With the ELA administrator role on the CSP, you can transfer or split the licensing tokens among other administrators who belong to different departments with their own CSP accounts. This sharing enables other administrators in your enterprise to deploy the VM-Series firewall on demand as long as they have tokens available in their respective CSP accounts. See Manage VM-Series ELA License Tokens to invite other administrators to share ELA tokens and deploy any model of the VM-Series firewall that meets your enterprise security need.You can also reclaim tokens to remove CSP accounts from the VM-Series ELA if want to redistribute tokens based on changing organizational needs.

The following videos provide a walkthrough of the VM-Series Multi-Model ELA.

Manage VM-Series ELA License Tokens

The VM-Series Enterprise License Agreement (Multi-Model ELA) (VM-Series ELA) gives you the flexibility of having a single contract that you can share with other administrators in your enterprise. You must have the super user role on the Palo Alto Networks Customer Support Portal (CSP) to activate the ELA, and upon activating the ELA authorization code you inherit the ELA administrator role on the CSP.

With the ELA administrator role, you can manage the license token pool available to deploy VM-Series firewalls and subscriptions included in the agreement. You can invite other administrators to share the VM-Series ELA tokens, grant which models and how many instances of the VM-Series firewalls are available to each administrator, as well as remove CSP accounts from your VM-Series ELA. Depending on what you allocate for each grantee, they receive a specific number of tokens that they can then use to deploy VM-Series firewalls.

Additional purchases and grants do not directly add to the number of available VM-Series firewalls in a CSP account; instead, ELA license tokens are added to the VM-Series ELA token pool. The ELA license tokens can subsequently be allocated by the ELA administrator to a given CSP account to increase the number of available VM-Series firewalls.

STEP 1 | (Legacy VM-Series ELA Customers only) Designate an ELA administrator to manage tokens.

Existing enterprise license customers who have been migrated to the Multi-Model ELA must designate an ELA administrator to manage VM-Series ELA license tokens. Upon conversion, no other action is necessary for continued operation of your firewalls, however, you will not be able to (re)allocate tokens for deploying firewalls until an ELA administrator has been assigned. Only an administrator with a super user role on the CSP has the ability to designate an ELA administrator, who in turn, can manage tokens or grant tokens to other administrators.

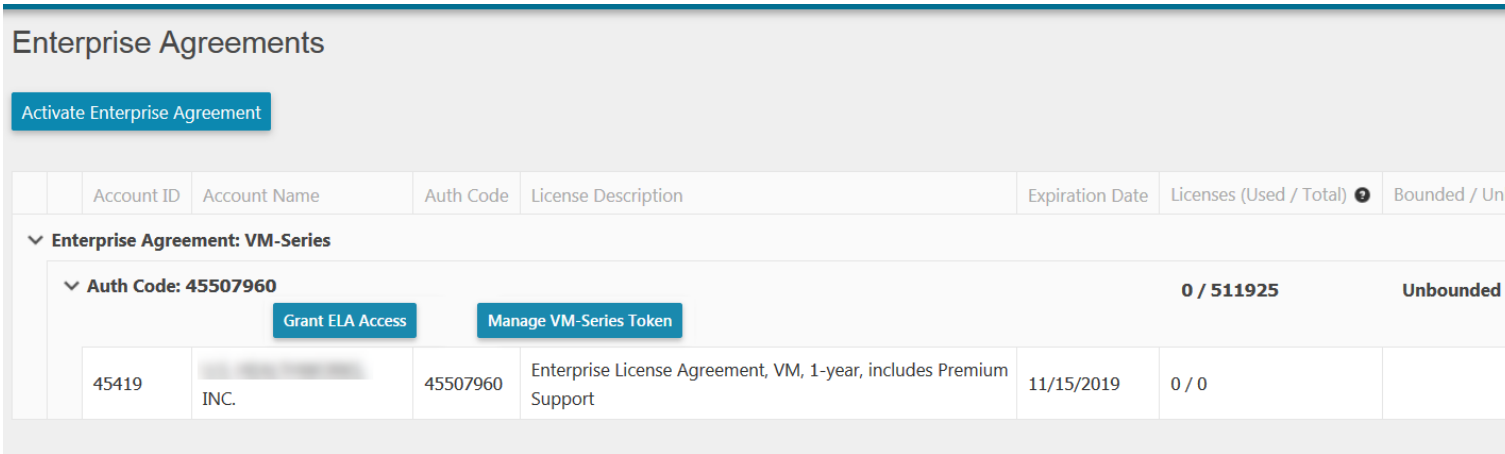
1. Log in to the Palo Alto Networks CSP.
2. Select **Members** > **Manage Users**.
3. Click on the pencil icon under **Actions** to edit the user to whom you want to assign the ELA administrator role.
4. Select **ELA Administrator** and then click the check mark to add the new role to the selected user.
5. Continue to step 3.

STEP 2 | Activate the ELA authorization code.

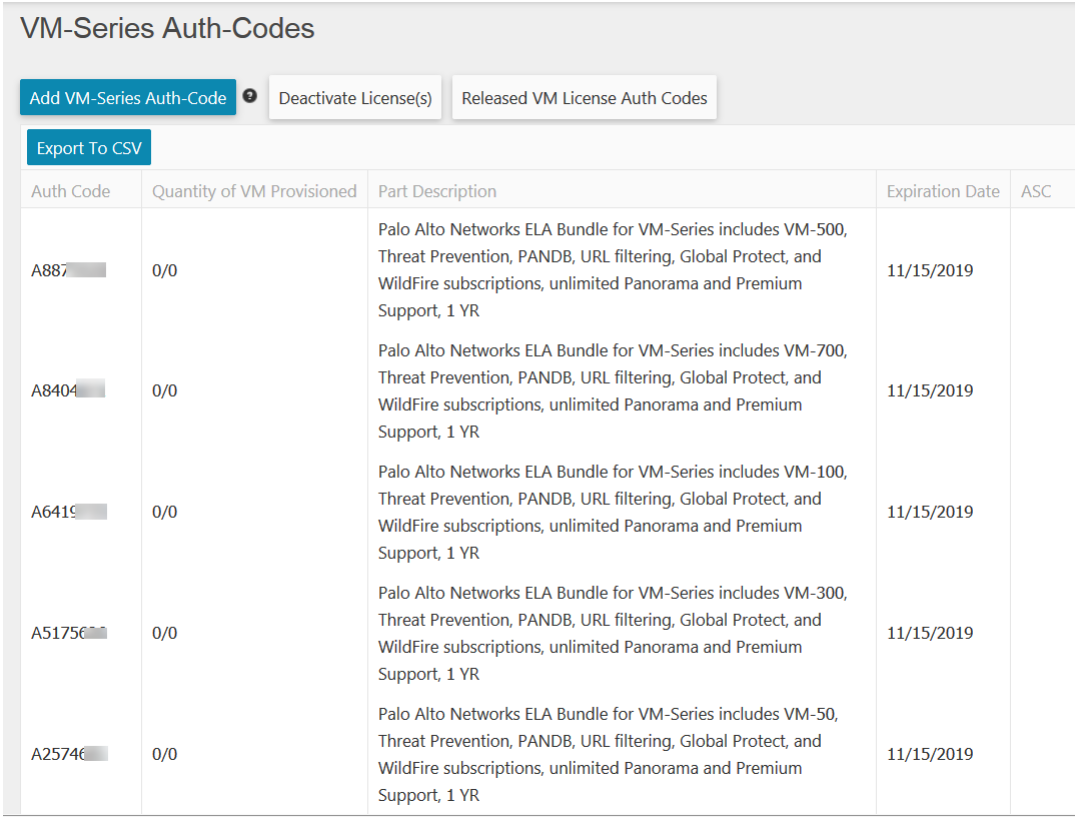
The administrative user who activates the ELA inherits the ELA administrator and super user role on the CSP and has the ability to manage the tokens or grant the tokens to other administrators.

1. Log in to the Palo Alto Networks CSP.
2. Select **Assets** > **Enterprise Agreements** > **Activate Enterprise Agreement**.
3. Enter the **Authorization Code** and **Agree and Submit** the EULA.

   Verify the authorization code is registered to your account under Enterprise Agreements: VM-Series. The page displays the Auth Code, Account ID, Account Name, License Description, Expiration Date, the number of Licenses (used/total) you have, and how many are available to deploy within the bounded and unbounded period of the agreement.

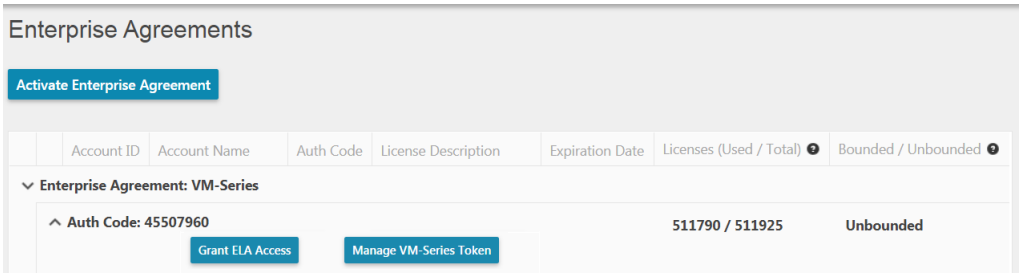


4. Select **Assets** > **VM-Series Auth-Codes** to view the authorization codes for deploying each model of the VM-Series firewall and associated subscriptions included with the ELA.



STEP 3 | Grant ELA access to other administrators in your enterprise.

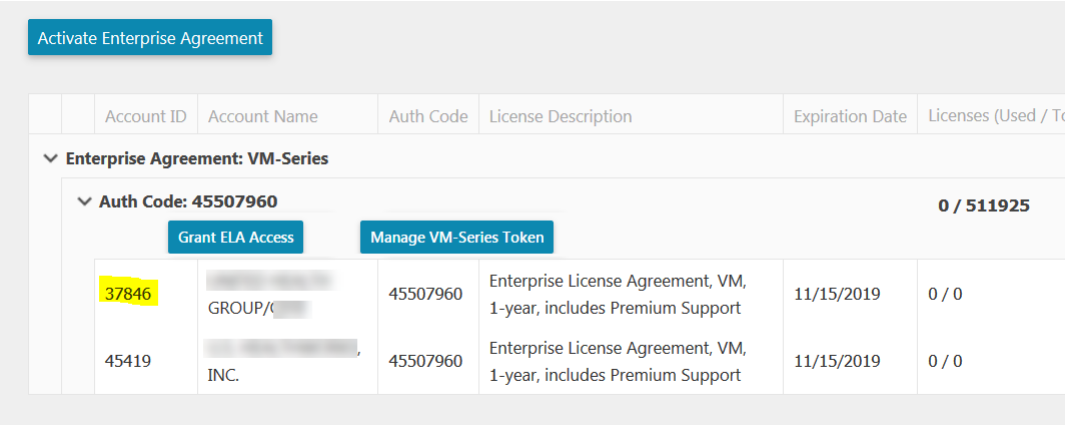
This capability allows you to share the VM-Series ELA with other administrators within your enterprise or department so that they can deploy VM-Series firewalls on demand. As an ELA administrator, you can grant access to other users who are registered with an email address on the CSP.



1. On **Assets** > **Enterprise Agreements**, select **Grant ELA Access**.
2. Enter the **Destination Email** address of the administrator whom you want to invite.

   The destination email address that you enter above must be a registered user on the CSP so that they can log in and accept the grant. If the email address is not registered on the CSP, you must first create a new account for the user on **Members** > **Create New User**.
3. Select **Notify User** to trigger a notification email to the email address you entered.

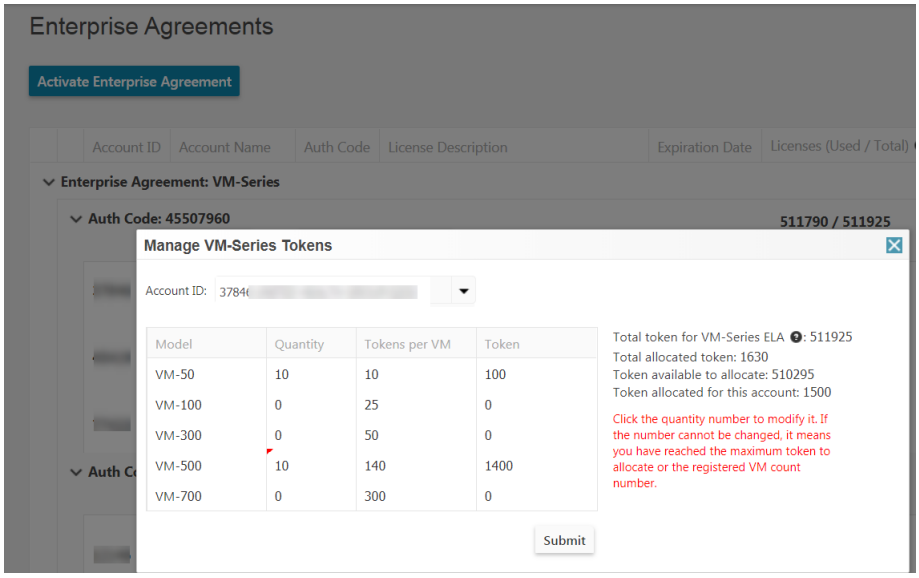
   The recipient must log in to the CSP to Accept the VM-Series ELA. After the recipient accepts the grant, the account ID is available on **Assets** > **Enterprise Agreements**.



STEP 4 | Allocate tokens for deploying firewalls.

1. Select **Assets** > **Enterprise Agreements** > **Manage VM-Series Tokens**.

   For each account ID, you can specify the number of firewalls by model that you want to allocate. Based on the quantity and firewall model, the number of tokens are automatically calculated and become available for use. In this example, you are allowing 10 instances each of the VM-50 and the VM-500.



2. Verify that the accurate number of firewall instances are deposited in the account.

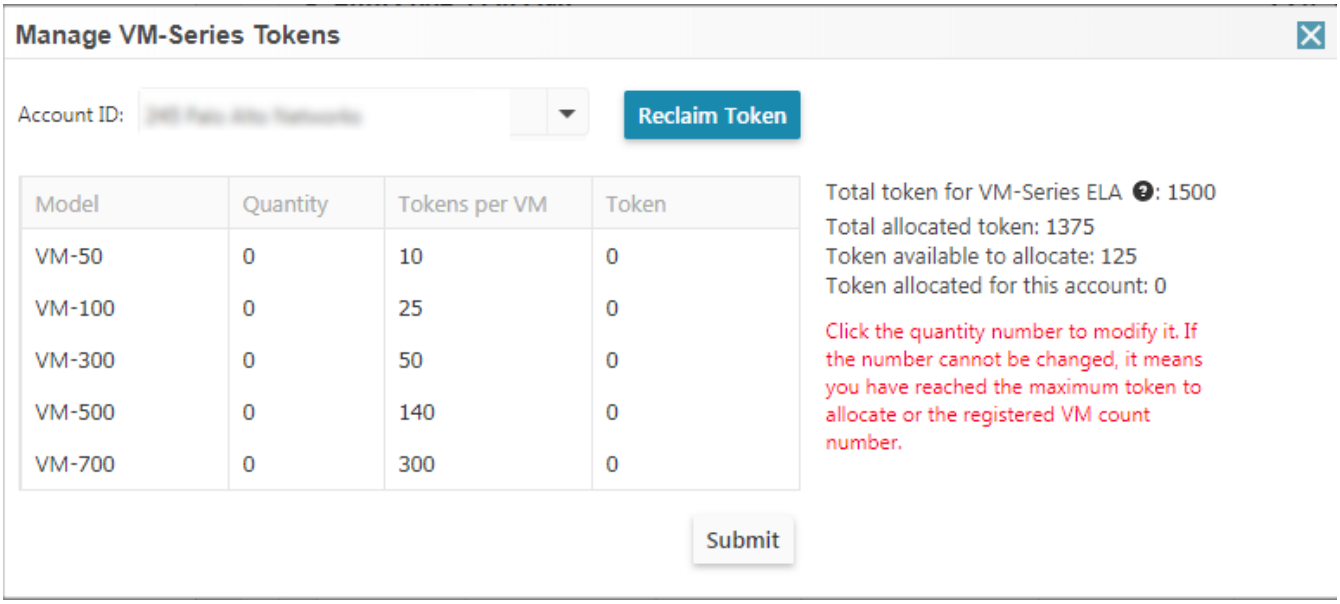
   Select **Assets** > **VM-Series Auth-Code** to confirm the auth codes you allotted. In this example, the account has the ability to provision 10 instances each of the VM-50 and the VM-500. As the recipients deploy firewalls, the number of tokens are deducted from the total available pool, and you can view the number of firewall instances that they have provisioned as a ratio of the total quantity you allocated for them. As your security needs evolve, you have the flexibility to allocate more quantity and allow access to a different VM-Series firewall model as long as you have tokens available.

STEP 5 | Remove a CSP account from the VM-Series ELA to reclaim tokens.

You cannot reclaim a portion of the tokens allocated to a CSP account. By reclaiming tokens, you are removing the entirety of the CSP account from the VM-Series ELA and reallocating all associated tokens to the token pool.

1. Verify that all tokens associated with the CSP account that you want to remove are not being utilized by the VM-Series firewalls. Deactivate the VM-Series firewalls as necessary to provision tokens for removal.
2. Select **Assets** > **Enterprise Agreements** > **Manage VM-Series Token**.

   Select the account ID from whom you want to reclaim tokens from and click **Reclaim Token**. If tokens are available for reclamation, you will receive a confirmation of a successful removal.

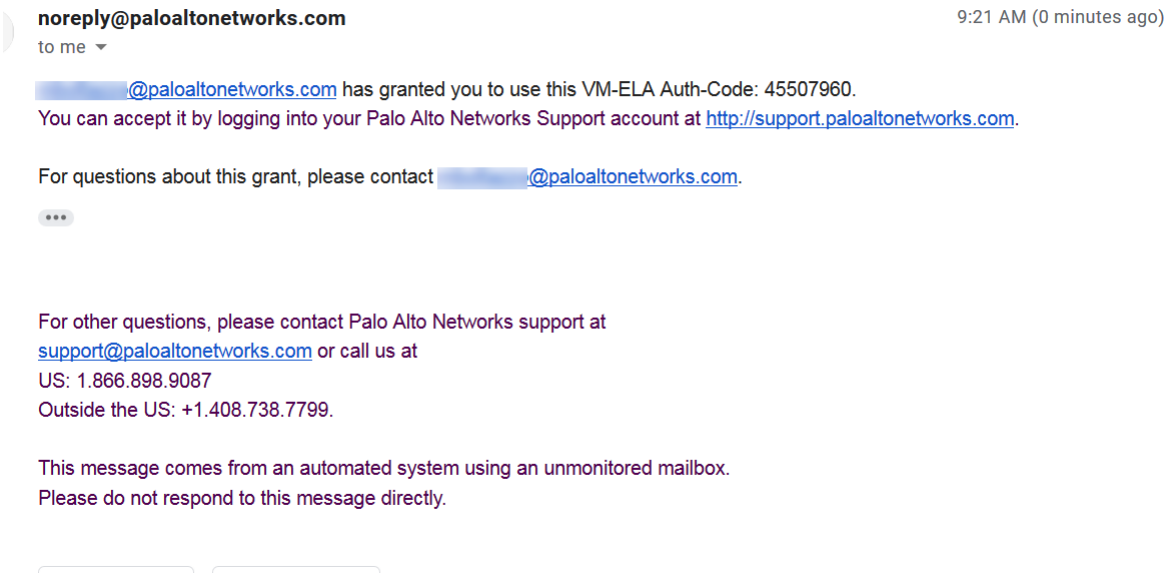


Accept the VM-Series ELA

If your enterprise has purchased a VM-Series ELA, your ELA administrator can invite you to share the contract and share the license token pool so that you have access to VM-Series firewall auth codes which enable you to deploy VM-Series firewalls on demand. When you receive a grant for access to the VM-Series ELA, you get an email notification that includes a link to log in to the Palo Alto Networks Customer Support Portal (CSP) and you must agree and accept the terms of use. After you accept the ELA terms of use, the ELA administrator can allocate which VM-Series firewall models and how many you are entitled to use; the corresponding number of VM-Series ELA tokens are deposited in your account.

STEP 1 | Check your email inbox for the grant notification.

The notification includes the email address of the ELA administrator who has invited you to share the VM-Series ELA.

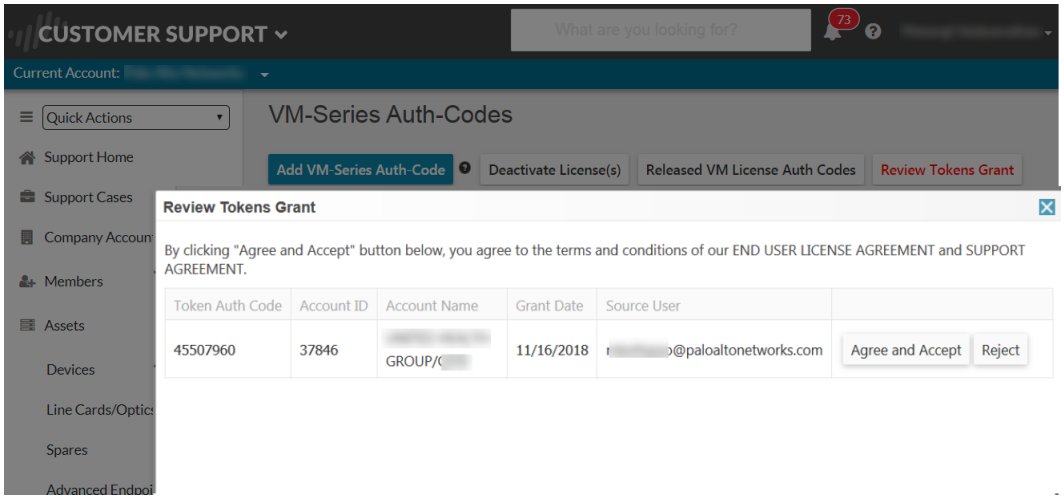


STEP 2 | Accept the grant.

You must review the terms and accept the EULA and the support agreement before the ELA admin can allocate tokens which enable you to deploy VM-Series firewalls.

1. Log in to the Palo Alto CSP.
2. Select **VM-Series Auth Codes** to **Review Tokens Grant**.

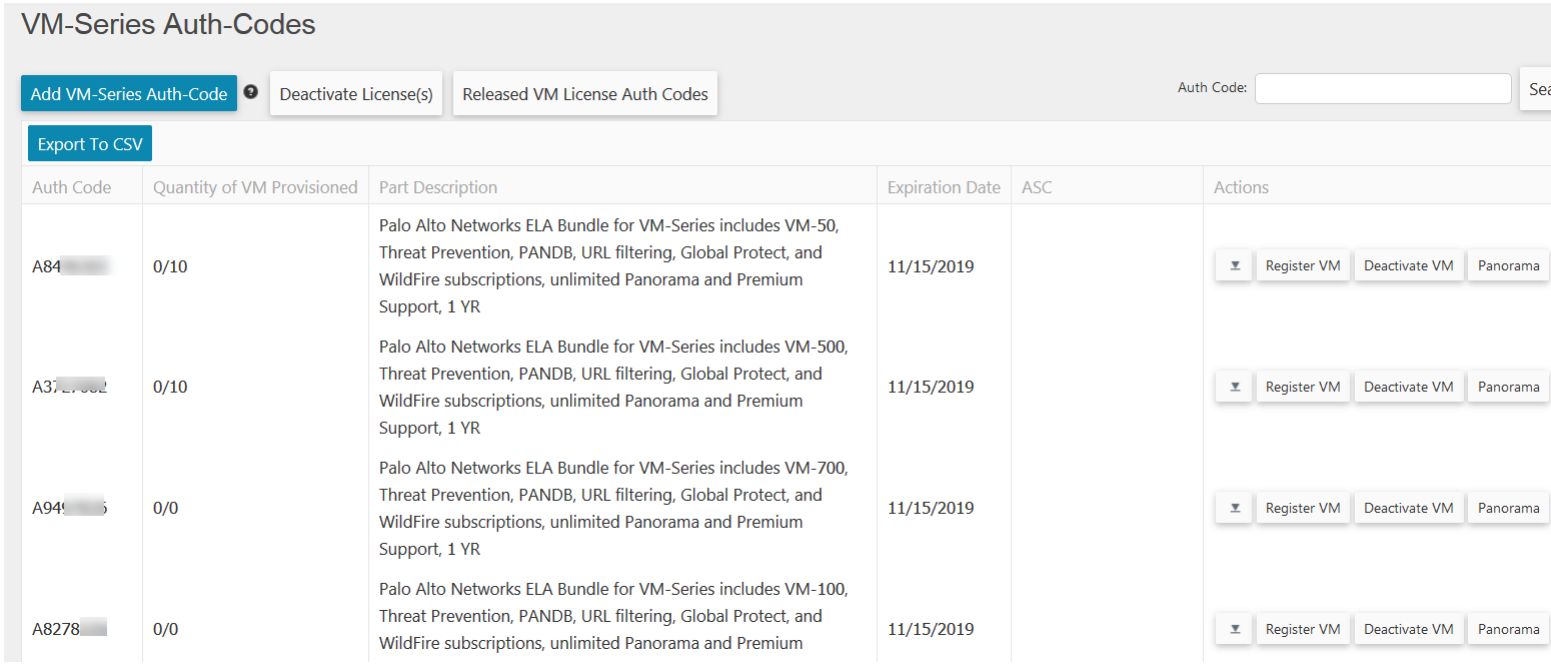
   You must Agree and Accept the grant. If you reject it, the ELA Admin who gave you the grant receives an email notification that you declined the grant. Do make sure to let the ELA administrator know that you have accepted the grant so that you he/she can allocate the VM-Series firewall models and quantity that you can deploy.



If you belong to multiple accounts on the CSP and accidentally accept the grant in to the wrong account, you must request the ELA administrator to resend the grant to you. Do not start using the auth code to provision firewalls until you accept the grant in the correct account.

STEP 3 | Verify which VM-Series models and how many are allocated for you.

After the ELA administrator allocates the VM-Series firewall models and number of instances you can provision, you can select **Assets** > **VM-Series Auth Codes** to view which models and how many of each are allocated for you. For example, the grant in the following screenshot displays the auth codes that enable you to deploy 10 instances each of the VM-50 and the VM-500.



As you deploy firewalls and register them to the CSP, the number of provisioned firewalls is incremented. The **Quantity of VM Provisioned** displays the ratio of provisioned to total available for each model.

Serial Number and CPU ID Format for the VM-Series Firewall

When you launch an instance of the VM-Series firewall, each instance of the firewall is uniquely identified using the CPU ID and serial number of the firewall. The format of the CPU ID and the serial number include information on the hypervisor and the license type for each instance of the VM-Series firewall.

- With the usage-based licensing model of the VM-Series firewalls, at launch the firewall generates a serial number and CPU ID, and you use these details to Register the Usage-Based Model of the VM-Series Firewall in AWS and Azure (no auth code).
- With the BYOL model, you must Register the VM-Series Firewall (with auth code) on the Customer Support portal (CSP). For a firewall with direct internet access, you can apply the auth code on the firewall to generate a license file that includes the serial number. For a firewall that is offline, you must use the CSP to input the CPU ID, UUID, and the auth code to generate a license file that includes the serial number and install the license on the firewall.

License Type	Serial Number	CPU ID
BYOL	15 digits, all numeric Example: 0071 **51** 345678909	<Hypervisor>:<ActualCPUID> Example: **ESX**:12345678
PAYG	15 digits, alphanumeric Example: **4** DE0YTAYOGMYYTN	<Hypervisor>:<Instance-ID>:<CloudProductCode>:<CloudRegion> Example: **AWSMP**:1234567890abcdef0:6kxdw3bbmdeda3o6i1ggqt4km:u west1

Create a Support Account

A support account is required to access software updates and to get technical support or open a case with Palo Alto Networks technical support.

For all licensing options except for usage-based licenses that are currently only available in AWS, you require a support account so that you can download the software package required to install the VM-Series firewall. The support account also allows you to view and manage all assets—appliances, licenses, and subscriptions—that you have registered with Palo Alto Networks.

If you have an existing support account, continue with Register the VM-Series Firewall.

STEP 1 | Go to https://www.paloaltonetworks.com/support/tabs/overview.html.

STEP 2 | Click the **Register** link (bottom of the page), and enter the corporate email address to associate with the support account.

STEP 3 | Choose one of the following options and fill in the details in the user registration form:

For a usage-based license in AWS

1. Click **Register your Amazon Web Services VM-Series Instance**.
2. On the AWS Management Console, find the AWS Instance ID, AWS Product Code, and the AWS Zone in which you deployed the firewall.
3. Fill in the other details.

For all other licenses

1. Click **Register device using Serial Number or Authorization Code**.
2. Enter the capacity auth code and the sales order number or customer ID.
3. Fill in the other details.

STEP 4 | **Submit** the form. You will receive an email with a link to activate the user account; complete the steps to activate the account.

After your account is verified and the registration is complete, you can log in to the support portal.

Register the VM-Series Firewall

When you purchase a VM-Series firewall, you receive an email that includes an auth code for a capacity license for the VM-Series model, a support entitlement auth code (for example, PAN-SVC-PREM-VM-100 SKU), and one or more auth codes for the subscription licenses. To use the auth code(s), you must register the code to the support account on the Palo Alto Networks Customer Support website. In the case of the VMware integrated NSX solution, the email contains a single authorization code that bundles the capacity license for one or more instances of the VM-Series model, the support entitlement, and one or more subscription licenses.

For the usage-based licenses in AWS, you do not receive an auth code. However, in order to activate your premium support entitlement with Palo Alto Networks, you must create a support account and register the VM-Series firewall on the Palo Alto Networks Customer Support website.

Use the instructions in this section to register the capacity auth code or firewall with your support account:

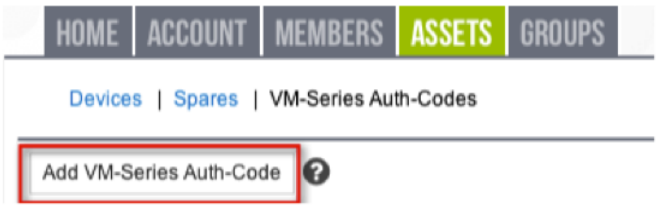
- Register the VM-Series Firewall (with auth code)
- Register the Usage-Based Model of the VM-Series Firewall in AWS and Azure (no auth code)

Register the VM-Series Firewall (with auth code)

Complete the following procedure to register your VM-Series firewall with an auth code.

STEP 1 | Log in to the Palo Alto Networks Customer Support website with your account credentials. If you need a new account, see Create a Support Account.

STEP 2 | Select **Assets** and click **Add VM-Series Auth-Codes**.



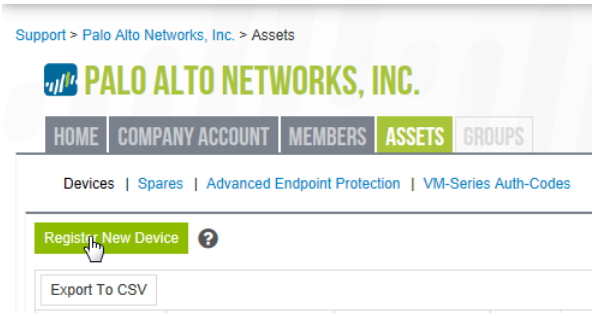
STEP 3 | In the **Add VM-Series Auth-Code** field, enter the capacity auth code you received by email, and click the checkmark on the far right to save your input. The page will display the list of auth codes registered to your support account.

You can track the number of VM-Series firewalls that have been deployed and the number of licenses that are still available for use against each auth code. When all the available licenses are used, the auth code does not display on the VM-Series Auth-Codes page. To view all the assets that are deployed, select **Assets** > **Devices**.

Register the Usage-Based Model of the VM-Series Firewall in AWS and Azure (no auth code)

Before you begin the registration process, log in to the VM-Series firewall and jot down the serial number and the CPU ID (UUID is optional) from the dashboard.

STEP 1 | On the **Assets** tab (after you log in to the Palo Alto Networks Customer Support website), click **Register New Device**.

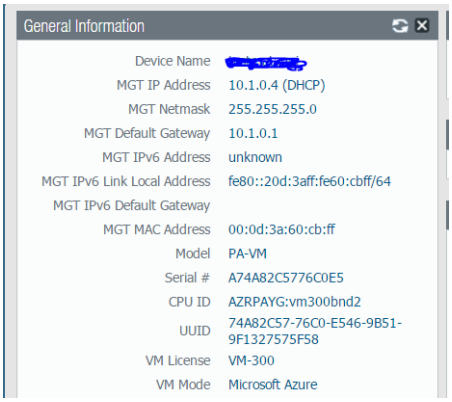


STEP 2 | Select **Register usage-based VM-Series models (hourly/annual) purchased from public cloud Marketplace**.

STEP 3 | Select your **Cloud Marketplace** vendor and **Submit**.

STEP 4 | Enter the **Serial #**, the **CPU ID**, and the **UUID** of the VM-Series firewall.

For example, from the Dashboard of the VM-Series firewall on Azure you will see the following information.



If you plan to use the firewall offline, please select the Offline checkbox and enter the PAN-OS version you plan to use.

STEP 5 | **Agree and Submit** to accept the EULA and register the firewall.

STEP 6 | Verify that the details on the licenses you purchased are displayed on the **Assets** page of the support portal.

Switch Between the BYOL and the PAYG Licenses

The VM-Series firewall cannot be converted between the BYOL and PAYG licensing options. If you have already deployed and configured a VM-Series firewall with the PAYG or BYOL option in AWS or Azure, and now want to switch to the other option, use the following instructions to save and export the configuration on your existing firewall, deploy a new firewall, and then restore the configuration on the new firewall.

STEP 1 | Save a backup of the current configuration file and store it to an external server.

1. Select **Device** > **Setup** > **Operations** and **Export named configuration snapshot**.
2. Select the XML file that contains your running configuration (for example, running-config.xml) and click **OK** to export the configuration file.
3. Save the exported file to a location external to the firewall.

STEP 2 | Deploy a new firewall and register or activate the license, as appropriate.

For a new PAYG instance:

1. In the AWS or Azure Marketplace, select the software image for the PAYG licensing bundle you want to deploy.
2. Deploy a new VM-Series firewall in the AWS or Azure public cloud. See Set Up the VM-Series Firewall on AWS or Set up the VM-Series Firewall on Azure.
3. Register the Usage-Based Model of the VM-Series Firewall in AWS and Azure (no auth code).

For a new BYOL instance:

1. Contact your sales representative or reseller to purchase a BYOL license, and get a BYOL auth code that you can use to license your firewall.
2. Register the VM-Series Firewall (with auth code).
3. Deploy a new VM-Series firewall in the AWS or Azure public cloud. See Set Up the VM-Series Firewall on AWS or Set up the VM-Series Firewall on Azure.
4. Activate the License for the VM-Series Firewall (Standalone Version).

STEP 3 | On the newly deployed firewall, restore the configuration that you exported.

1. Access the web interface of the newly deployed firewall.
2. Select **Device** > **Setup** > **Operations**, click **Import named configuration snapshot**, Browse to the configuration file on the external host, and click **OK**.
3. Click **Load named configuration snapshot**, select the **Name** of the configuration file you just imported, and click **OK**.
4. Click **Commit** to overwrite the running configuration with the snapshot you just imported.
5. Verify that the configuration on the new firewall matches the firewall that you are replacing, before you delete the firewall or deactivate the licenses on the replaced firewall.

Renew VM-Series Firewall License Bundles

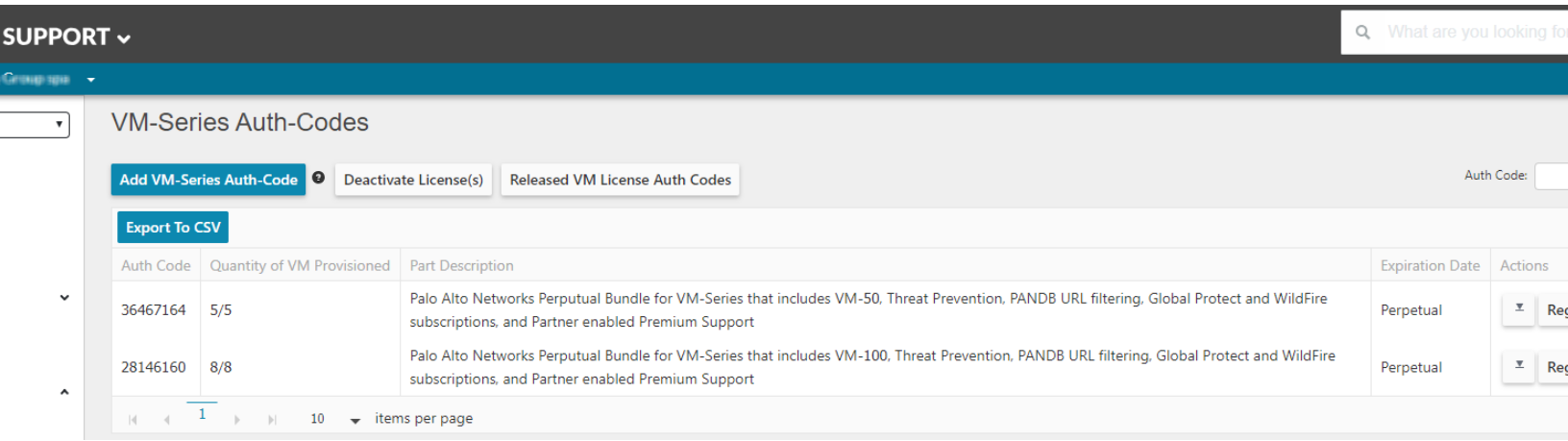
When your VM-Series firewall bundle licenses are due for renewal, you can log in to the Palo Alto Networks Customer Support Portal and adjust the license quantity to meet your deployment needs. At renewal, you can review your usage trends and based your future needs, pick from the following options:

- **Renew**—You can opt to renew all licenses as is, or to increase or decrease the licensed quantity. If you decrease the number of licenses you need, you must opt to get a basic bundle for the firewalls you are not renewing, otherwise you will forfeit the portion that you do not renew. If you increase the license quantity, the addition is added to your existing auth code.
- **Change to Basic Bundle**—If you have a VM-Series bundle 1 or a bundle 2 license that includes subscriptions, you can change to a basic bundle that includes a perpetual capacity license and support entitlement. When you switch to the basic bundle, you retain the VM-Series firewall model that you had previously purchased. All firewalls that are currently deployed and are associated with the existing auth code will continue to function, and the support entitlement will have a new expiration date. For any unprovisioned firewalls, you'll receive a new auth code that you can use to deploy new instances.
- **Forfeit**—Relinquish the licenses that you no longer need. If you have deployed the firewalls that you don't want to renew, you need to select the serial number of the instances for which you want to discontinue renewals. You can continue to use these firewall instances with the software and content versions that are currently installed, but your subscriptions and support entitlements are no longer valid. And to forfeit the license of VM-Series firewalls that you have not provisioned, just select the quantity that you want to forfeit.

STEP 1 | Log in to the Palo Alto Networks Customer Support Portal with your account credentials.

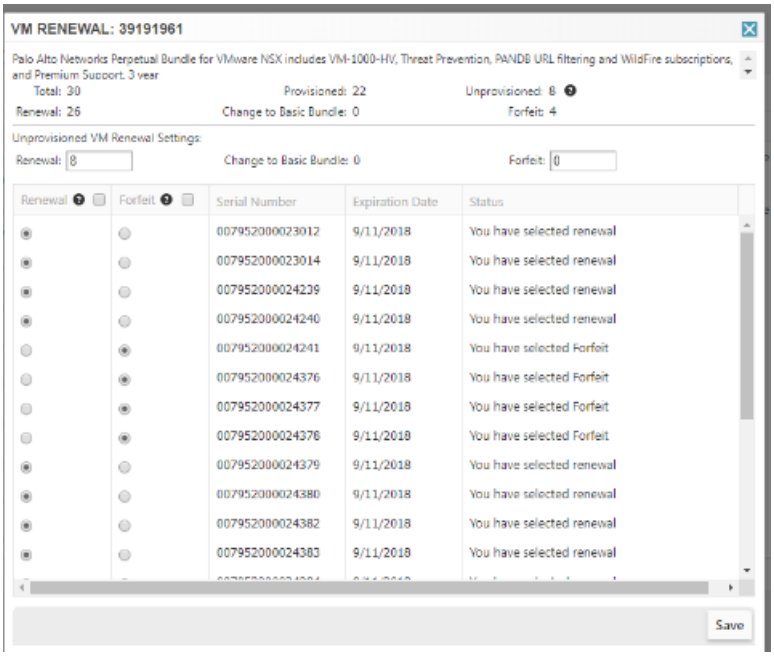
STEP 2 | Select **Assets** > **VM-Series Auth-Codes** and find the auth code you want to renew.

The **Renew** option displays for auth codes that are eligible for renewal.



STEP 3 | Click the **Renew** link to select the serial numbers to **Renew**, **Change to Basic Bundle**, or **Forfeit**.

If you have provisioned the firewall, select the appropriate option in the row that corresponds to the Serial Number. If you have unprovisioned instances of the firewall, select the quantity for each renewal option you choose under **Unprovisioned VM Renewal Settings**.



STEP 4 | **Save** your changes.

You will receive an onscreen confirmation that your changes are submitted for processing. After submitting your changes, if you select Renew again, you can view the status of your request against each serial number. If renewal processing has started, and you need to make additional revisions, you will be unable to save changes. For assistance, you can contact the renewals team at renewals@paloaltonetworks.com.

Activate the License

To activate the license on your VM-Series firewall, you must have deployed the VM-Series firewall and completed initial configuration. To deploy the firewall, see VM-Series Deployments.

Use the instructions in this section for all the BYOL models including AWS and Azure; for usage-based licensing in AWS and Azure, you do not need to activate the license. For the usage-based licenses, you must Register the Usage-Based Model of the VM-Series Firewall in AWS and Azure (no auth code) in order to activate your premium support entitlement.

For usage-based models of the VM-Series firewall in the AWS Marketplace, instances with short and long AWS instance IDs are supported.

Until you activate the license on the VM-Series firewall, the firewall does not have a serial number, the MAC address of the dataplane interfaces are not unique, and only a minimal number of sessions are supported. Because the MAC addresses are not unique until the firewall is licensed, to prevent issues caused by overlapping MAC addresses, make sure that you do not have multiple, unlicensed VM-Series firewalls.

When you activate the license, the licensing server uses the UUID and the CPU ID of the virtual machine to generate a unique serial number for the VM-Series firewall. The capacity auth code in conjunction with the serial number is used to validate your entitlement.

After you license a VM-Series firewall, if you need to delete and redeploy the VM-Series firewall, make sure to Deactivate the License(s) on the firewall. Deactivating the license allows you to transfer the active licenses to a new instance of the VM-Series firewall without help from technical support.

- Activate the License for the VM-Series Firewall (Standalone Version)
- Activate the License for the VM-Series Firewall for VMware NSX
- Troubleshoot License Activation Issues

Activate the License for the VM-Series Firewall (Standalone Version)

If you have not elected to use the bootstrapping workflow using a subscription bundle, you must deploy the VM-Series firewall and complete initial configuration before you can activate the license on your VM-Series firewall.

- If your VM-Series firewall has direct internet access.

  To activate the license, the firewall must be configured with an IP address, netmask, default gateway, and DNS server IP address.

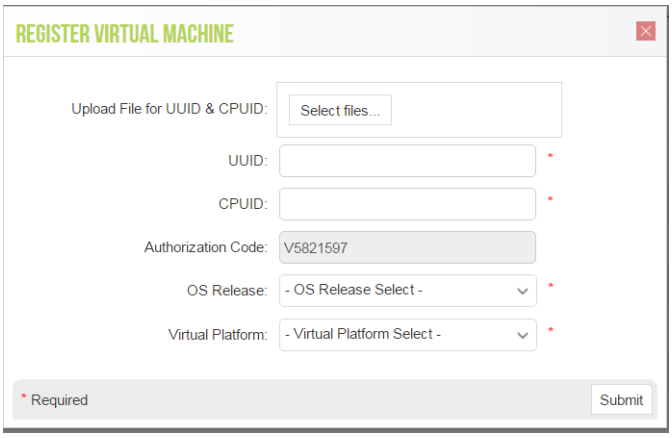
  The firewall must have a valid DNS configuration and have network connectivity to access the Palo Alto Networks licensing server.

  1. If you are activating a license on an already-licensed VM-Series firewall, you must Install a License Deactivation API Key.
  2. Select **Device** > **Licenses** and select the **Activate feature using authorization code** link.
  3. Enter the capacity auth code that you registered on the support portal. The firewall will connect to the update server (updates.paloaltonetworks.com), and download the license and reboot automatically.

4. Log back in to the web interface and confirm that the **Dashboard** displays a valid serial number. If the term **Unknown** displays, it means the device is not licensed.
5. On **Device** > **Licenses**, verify that **PA-VM** license is added to the device.

   If you see an error message, check Troubleshoot License Activation Issues.

- If your VM-Series firewall does not have internet access.
  1. Select **Device** > **Licenses** and click the **Activate Feature using Auth Code** link.
  2. Click **Download Authorization File**, and download the **authorizationfile.txt** on the client machine.
  3. Copy the **authorizationfile.txt** to a computer that has access to the internet and log in to the support portal. Click **My VM-Series Auth-Codes** link and select the applicable auth code from the list and click the **Register VM** link.
  4. On the **Register Virtual Machine** tab upload the authorization file. Select the PAN-OS version and the hypervisor on which you have deployed the firewall, to complete the registration process. The serial number of your VM-Series firewall will be attached to your account records.



  5. Navigate to **Assets** > **My Devices** and search for the VM-Series device just registered and click the **PA-VM** link. This will download the VM-Series license key to the client machine.
  6. Copy the license key to the machine that can access the web interface of the VM-Series firewall and navigate to **Device** > **Licenses**.

     License keys must be installed through the web interface. The firewall does not support license key installation through SCP or FTP.
  7. Click **Manually Upload License** link and enter the license key. When the capacity license is activated on the firewall, a reboot occurs.
  8. Log in to the device and confirm that the **Dashboard** displays a valid serial number and that the **PA-VM** license displays in the **Device** > **Licenses** tab.

Activate the License for the VM-Series Firewall for VMware NSX

Panorama serves as the central point of administration for the VM-Series firewalls for VMware NSX and the license activation process is automated when Panorama has direct internet access. Panorama connects to the Palo Alto Networks update server to retrieve the licenses, and when a new VM-Series firewall for NSX is deployed, it communicates with Panorama to obtain the license. If Panorama is not connected to the internet, you need to manually license each instance of the VM-Series firewall so that the firewall can connect to Panorama. For an overview of the components and requirements for deploying the VM-Series firewall for NSX, see VM-Series for NSX Firewall Overview.

For this integrated solution, the auth code (for example, PAN-VM-1000-HV-SUB-BND-NSX2) includes licenses for threat prevention, URL filtering and WildFire subscriptions and premium support for the requested period.

In order to activate the license, you must have completed the following tasks:

- Registered the auth code to the support account. If you don't register the auth code, the licensing server will fail to create a license.
- Entered the auth code in the Service Definition on Panorama. On Panorama, select **VMware Service Manager** to add the **Authorization Code** to the **VMware Service Definition**.

If you have purchased an evaluation auth code, you can license up to 5 VM-Series firewalls with the VM-1000-HV capacity license for a period of 30 or 60 days. Because this solution allows you to deploy one VM-Series firewall per ESXi host, the ESXi cluster can include a maximum of 5 ESXi hosts when using an evaluation license.

The following process of activating the licenses is manual. If you have a custom script or an orchestration service, you can use the Licensing API to automate the process of retrieving the licenses for the VM-Series firewalls.

- Activate Licenses on VM-Series Firewalls on NSX When Panorama has Internet Access
- Activate Licenses on VM-Series Firewalls on NSX When Panorama has No Internet Access

Activate Licenses on VM-Series Firewalls on NSX When Panorama has Internet Access

Complete the following procedure to activate the VM-Series firewall for NSX when Panorama has access to the internet.

STEP 1 | Verify that the VM-Series firewall is connected to Panorama.

1. Log in to Panorama.
2. Select **Panorama** > **Managed Devices** and check that the firewall displays as Connected.

STEP 2 | Verify that each firewall is licensed.

Select **Panorama** > **Device Deployment** > **Licenses** and verify that Panorama has matched the auth code and applied the licenses to each firewall.

If you do not see the licenses, click **Refresh**. Select the VM-Series firewalls for which to retrieve subscription licenses and click **OK**.

Activate Licenses on VM-Series Firewalls on NSX When Panorama has No Internet Access

Complete the following procedure to activate the VM-Series firewall for NSX when Panorama does not have access to the internet.

STEP 1 | Locate the CPU ID and UUID of the VM-Series firewall.

1. From the vCenter server obtain the IP address of the firewall.
2. Log into the web interface and select **Dashboard**.
3. Get the **CPU ID** and the **UUID** for the firewall from the General Information widget.

STEP 2 | Activate the auth code and generate the license keys.

1. Log in to the Palo Alto Networks Customer Support website with your account credentials. If you need a new account, see Create a Support Account.
2. Select **Assets** > **VM-Series Auth Codes**, click **Add VM-Series Auth Codes** to enter the auth code.
3. Select **Register VM** in the row that corresponds to the auth code that you just registered, enter the CPU ID and the UUID of the firewall and click **Submit**. The portal will generate a serial number for the firewall.

4. Select **Assets** > **Devices** and search for the serial number.
5. Click the link the Actions column to download each key locally to your laptop. In addition to the subscription license key, you must get the capacity license and the support license keys.

STEP 3 | Upload the keys to the firewall.

1. Log in to the firewall web interface.
2. Select **Device** > **Licenses**, and select **Manually upload license key**.
3. **Browse** to select a key and click **OK** to install the license on the firewall.

   Install the capacity license key file (pa-vm.key) first. When you apply the capacity license key, the VM-Series firewall will reboot. On reboot, the firewall will have a serial number that you can use to register the firewall as a managed device on Panorama.
4. Repeat the process to install each key on the firewall.
5. Select **Dashboard** and verify that you can see the **Serial #** in the General Information widget.

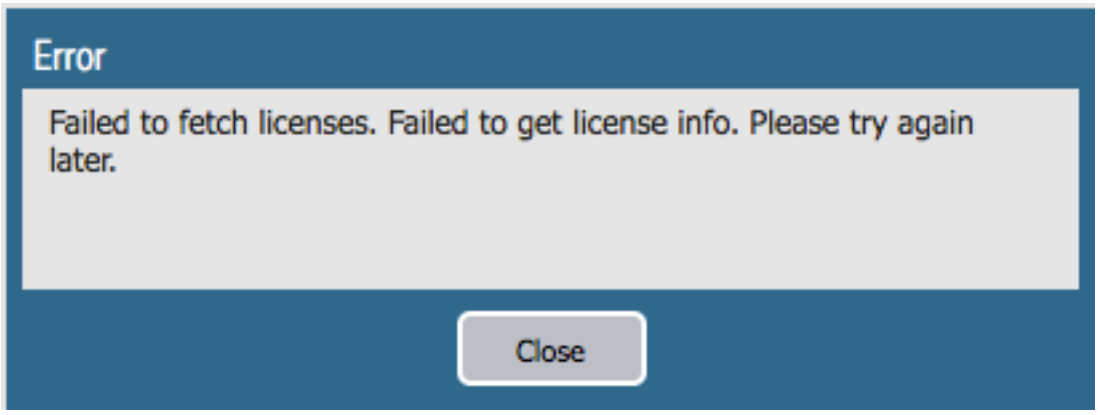
STEP 4 | Add the serial number of the firewall on Panorama.

Select **Panorama** > **Managed Devices** and click **Add** to enter the serial number for the VM-Series firewall for NSX. The firewall should now be able to connect with Panorama so that it can obtain its configuration and policy rules.

Troubleshoot License Activation Issues

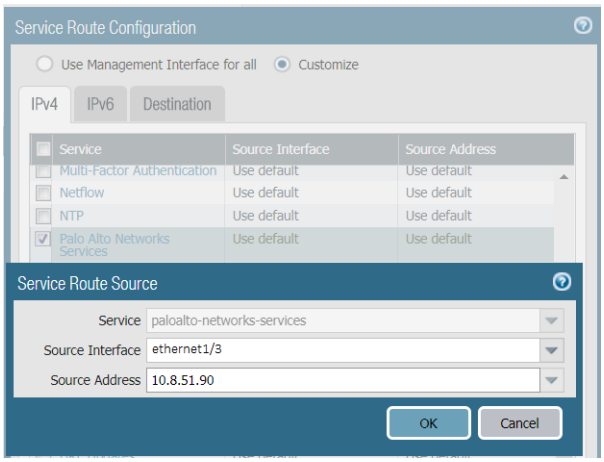
Some of the most common issues with activating your license is covered in this section.

- If you see an error that reads **Failed to fetch licenses. Failed to get license info. Please try again later**or a generic communications error message displays.



Verify the following:

- Can the firewall route traffic to the Palo Alto Networks server using a service route? By default, the firewall uses the management interface to access the server. If you plan on using a dataplane interface, make sure that you have set up a service route.

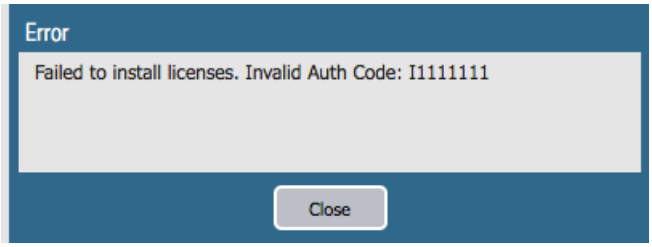


- Is routing over the internet working? SSH into the firewall and ping an publicly accessible IP address such as 4.2.2.2. Be sure to use the source option if you are using a dataplane interface. For example: ping count 3 source 10.0.1.1 host 4.2.2.2.
- Is DNS set up correctly? SSH into the firewall and ping a DNS name such as google.com. For example:

```
warby@warbylan> ping count 3 source 10.0.1.1 host google.com
PING google.com (216.58.195.78) from 10.0.1.1 : 56(84) bytes of data.
64 bytes from sfo07s16-in-f78.1e100.net (216.58.195.78): icmp_seq=1 ttl=55 time=11.6 ms
64 bytes from sfo07s16-in-f78.1e100.net (216.58.195.78): icmp_seq=2 ttl=55 time=11.9 ms
64 bytes from sfo07s16-in-f78.1e100.net (216.58.195.78): icmp_seq=3 ttl=55 time=11.5 ms

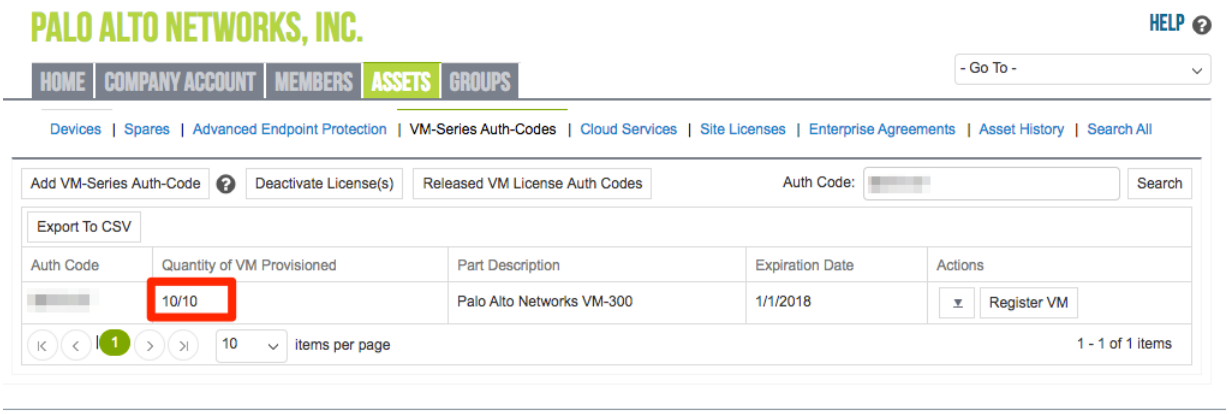
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2025ms
rtt min/avg/max/mdev = 11.586/11.721/11.975/0.200 ms
```

- If you see an error that reads Invalid Auth Code:



Verify the following:

- You have entered the auth code properly.
- You have registered the auth code to your account on the support portal.
- Your auth code has not reached the maximum provisioning capacity for the VM-Series firewalls.



Deactivate the License(s)

The license deactivation process enables you to self-manage licenses. Whether you want to remove one or more active licenses or subscriptions attributed to a firewall (hardware-based or VM-Series firewall) or you want to deactivate the VM-Series firewall and unassign all active licenses and subscriptions, begin the deactivation process on the firewall or Panorama (not on the Palo Alto Networks Customer Support web site).

To successfully deactivate a license, you must install a license deactivation API key and enable verification of the update server identity (enabled by default). PAN-OS uses this deactivation API key to authenticate with all update a license services. The deactivation API is key is not required for manual license deactivation, where there is not connectivity between the firewall and license server.

If the firewall/Panorama has internet access and can communicate with the Palo Alto Networks Licensing servers, the license removal process completes automatically with a click of a button. If the firewall/Panorama does not have internet access, you must complete the process manually in a two-step process. In the first step, from the firewall or Panorama, you generate and export a license token file that includes information on the deactivated keys. In the second step, while logged in to the Palo Alto Networks Customer Support website, upload the token file to dissociate the license keys from the firewall.

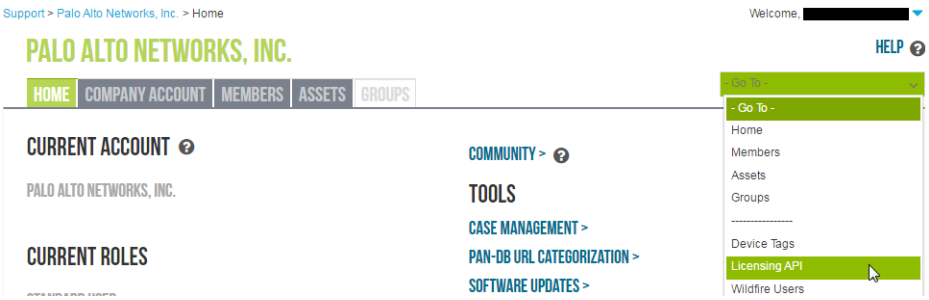
- Install a License Deactivation API Key
- Deactivate a Feature License or Subscription Using the CLI
- Deactivate VM

Install a License Deactivation API Key

Retrieve your license API key from the Customer Support Portal and install it using the CLI on the firewall and Panorama. You must have superuser privileges on the firewall or Panorama to install the license API key. When you install a license API key on Panorama, Panorama pushes the API key to its managed devices. If the managed device has an API key installed, Panorama overwrites the old API key with the new one.

STEP 1 | Retrieve the license deactivation API key from the Customer Support Portal.

1. Log in to the Customer Support Portal.
2. From the Go To drop-down, select **License API**.
3. Copy the API key.



STEP 2 | Use the CLI to install the API key copied in the previous step.

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

STEP 3 | After installing the license deactivation API key, Deactivate VM as normal.

Deactivating a VM-Series license requires a software restart.

STEP 4 | To replace a license deactivation API key, use the following CLI command to delete an installed API key.

```
request license api-key delete
```

To deactivate a VM-Series firewall after deleting the API key, you must install a new one.

Deactivate a Feature License or Subscription Using the CLI

If you accidentally installed a license/subscription on a firewall and need to reassign the license to another firewall, you can deactivate an individual license and re-use the same authorization code on another firewall without help from Technical Support. This capability is supported on the CLI only; this process is supported both on the hardware-based firewalls and on the VM-Series firewall.

STEP 1 | Log into the CLI on the firewall.

STEP 2 | (Direct internet access only) View the name of the license key file for the feature you want to deactivate.

```
request license deactivate key features ?
```

STEP 3 | (Direct internet access only) Deactivate the license or subscription.

```
request license deactivate key features <name> mode auto
```

where, name is the full name for the license key file.

For example:

```
admin@vmPAN2> request license deactivate key features
 WildFire_License_2015_01_28_I5820573.key mode auto007200002599

WildFire License Success

Successfully removed license keys
```

STEP 4 | (When there is no direct internet access) View the name of the license key file for the feature you want to deactivate.

```
request license deactivate key features
```

STEP 5 | (When there is no direct internet access) Deactivate the license manually.

```
request license deactivate key features <name> mode manual
```

For example:

```
admin@PA-VM> request license deactivate key features
 PAN_DB_URL_Filtering_2015_01_28_I6134084.key mode manual

Successfully removed license keys

dact_lic.01282015.100502.tok
```

The token file uses the format `dact_lic.timestamp.tok`, where the timestamp is in the `dmmyyyy.hrminsec` format.

STEP 6 | Verify that the token file was generated.

```
show license-token-files
```

STEP 7 | Export the token file to an SCP or TFTP server and save it to your computer.

```
scp export license-token-file to <username@serverIP> from <token_filename>
```

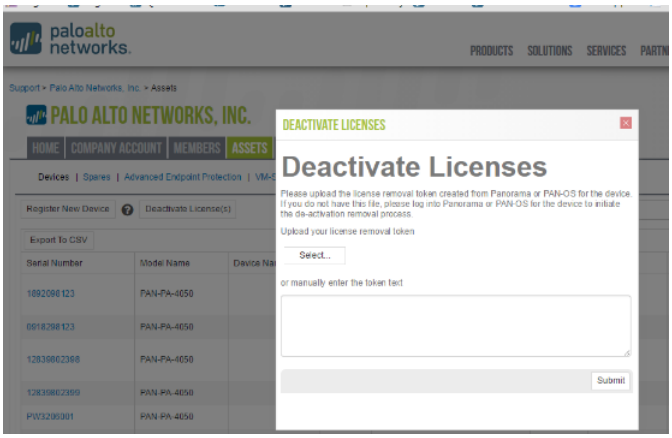
For example:

```
scp export license-token-file to admin@10.1.10.55:/tmp/ from
dact_lic.01282015.100502.tok
```

STEP 8 | Log into the Palo Alto Networks Customer Support website.

STEP 9 | Click the **Deactivate License(s)** link on the **Assets** tab.

STEP 10 | While logged in to the Palo Alto Networks Customer Support website, upload the token file to complete the deactivation.



Deactivate VM

When you no longer need a BYOL instance of the VM-Series firewall, you can free up all active licenses—subscription licenses, VM-Capacity licenses, and support entitlements— using the web interface, CLI, or the XML API on the firewall or Panorama. The licenses are credited back to your account and you can use the same authorization codes on a different instance of the VM-Series firewall.

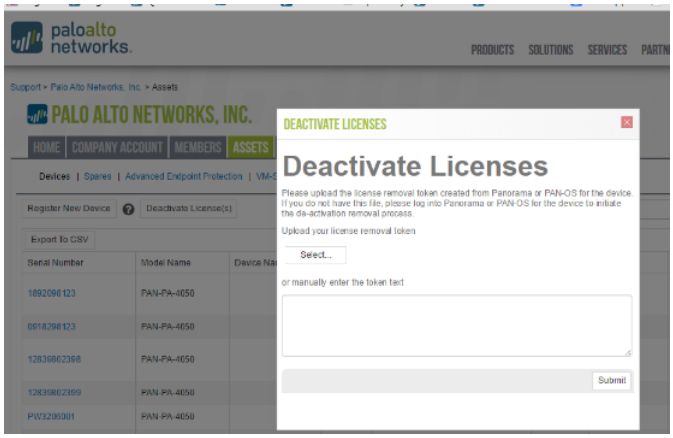
Deactivating a VM removes all the licenses/entitlements and places the VM-Series firewall in an unlicensed state; the firewall will not have a serial number and can support only a minimal number of sessions. Because the configuration on the firewall is left intact, you can re-apply a set of licenses and restore complete functionality on the firewall, if needed.

Make sure to deactivate licenses before you delete the VM-Series firewall. If you delete the firewall before deactivating the licenses you have two options:

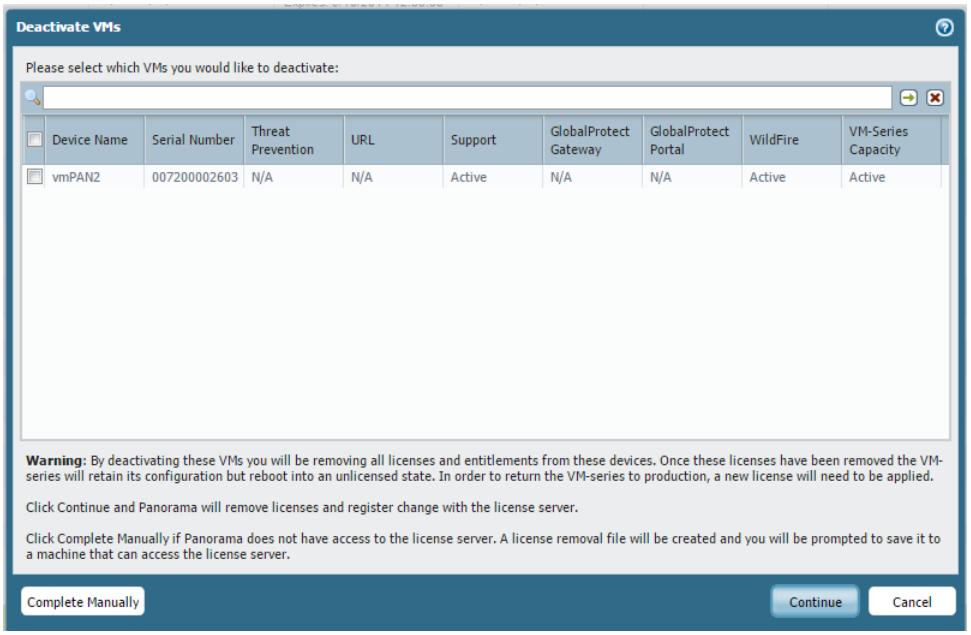
- *If the device was managed by Panorama, you can deactivate the license from Panorama.*
- *If the device was not managed by Panorama, you must contact Palo Alto Networks Customer Support.*

- From the firewall
  1. Log into the web interface and select **Device** > **Licenses**.
  2. Select **Deactivate VM** in the License Management section.
  3. Verify the list of licenses/entitlements that will be deactivated on the firewall.

4. Pick one of the following options to start deactivating the VM:
   - Click **Continue**, if the firewall can communicate directly with the Palo Alto Networks Licensing server. You will be prompted to reboot the firewall; on reboot the licenses are deactivated.
   - Click **Complete Manually**, if the firewall does not have internet access. Click the **Export license token** link to save the token file to your local computer. For example, the token filename is 20150128_1307_dact_lic.01282015.130737.tok. You will be prompted to reboot the firewall; on reboot the licenses are deactivated.
5. (Manual process only) Complete the following tasks to register the changes with the Licensing server:
   1. Log into the Palo Alto Networks Customer Support website.
   2. Click the Deactivate License(s) link on the **Assets** tab.
   3. While logged in to the Palo Alto Networks Customer Support website, upload the token file to complete the deactivation.

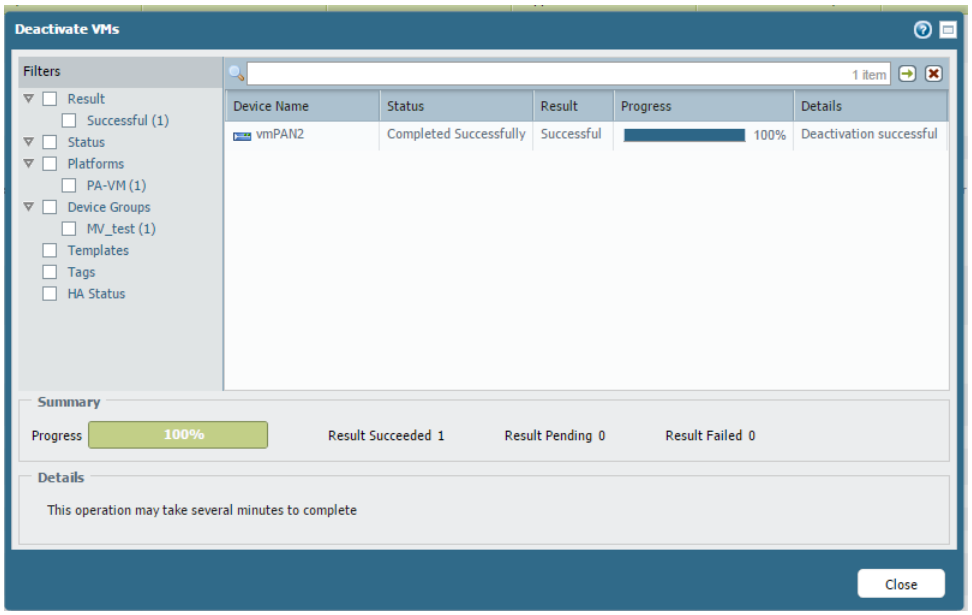


- From Panorama
  1. Log in to the Panorama web interface and select **Panorama** > **Device Deployment** > **Licenses**.
  2. **Deactivate VMs** and select the VM-Series firewall that you want to deactivate.



3. Pick one of the following options to deactivate the VM:

- **Continue**—If Panorama can communicate directly with the Palo Alto Networks Licensing servers and can register the changes. To verify that the licenses have been deactivated on the firewall, click **Refresh on Panorama** > **Device Deployment** > **Licenses**. The firewall is automatically rebooted.
- **Complete Manually**—If Panorama does not have internet access. Panorama generates a token file. Click the **Export license token** link to save the token file to your local computer. The successful completion message is displayed on-screen, and the firewall will be automatically rebooted.

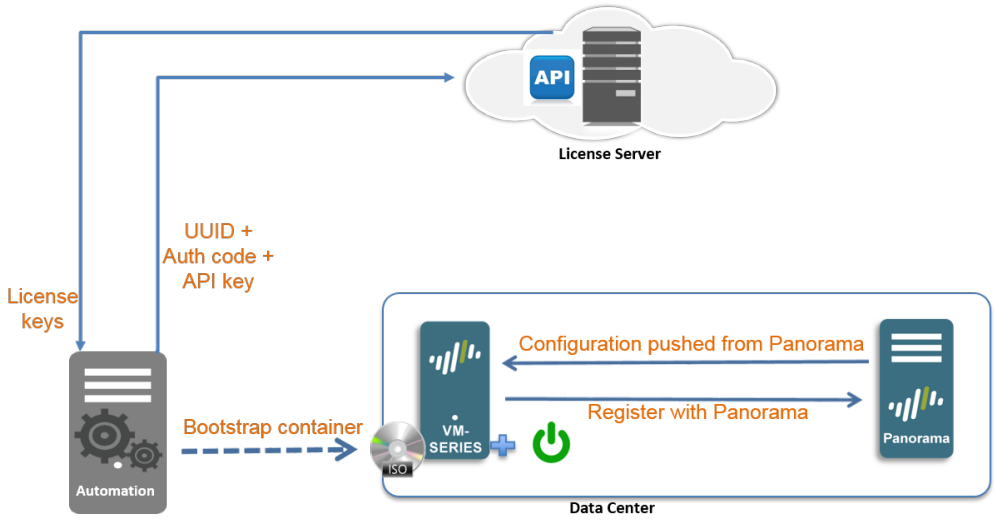


4. (Manual process only) To use the token file register the changes with the licensing server, see step e above.
5. Remove the deactivated VM-Series firewall as a managed device on Panorama.
    1. Select **Panorama** > **Managed Devices**.
    2. Select the firewall that you deactivated from the list of managed devices, and click **Delete**.

    Instead of deleting the firewalls, if you prefer, you can create a separate device group and assign the deactivated VM-Series firewalls to this device group.

Licensing API

To successfully license firewalls that do not have direct internet access, Palo Alto Networks provides a licensing API. You can use this API with a custom script or an orchestration service to register auth codes, retrieve licenses attached to an auth code, renew licenses, and to deactivate all licenses on a VM-Series firewall (Deactivate VM).



The API also allows you to view the details of an auth code so that you can track the number of unused licenses attached to an auth-code or auth-code bundle that enables you to license more than one instance of the firewall. An auth-code bundle includes the VM-Series model, subscriptions and support in a single, easy to order format; you can use this bundle multiple times to license VM-Series firewalls as you deploy them.

To use the API, each support account is assigned a unique key. Each API call is a POST request, and the request must include the API key to authenticate the request to the licensing server. When authenticated, the licensing server sends the response in json (content-type application/json).

- Manage the Licensing API Key
- Use the Licensing API
- Licensing API Error Codes

Manage the Licensing API Key

To get the API key required to use the licensing API, your account must have super user privileges on the support portal.

The expiration date of the API key is the same date as that of the latest subscription in your support account. If you renew your current subscriptions and need to reset the expiration date of the API key, you can either regenerate a key (and replace the existing key with this new key wherever you've used it) or contact Palo Alto Networks support for help with extending the term of your existing API key.

STEP 1 | Get your Licensing API key.

1. Log in to the Palo Alto Networks Support portal with an account that has super user privileges.
2. Select **Licensing API** from the **—Go To—** drop-down.
3. Click **Enable** to view your key and copy it for use. Once you generate a key, the key is enabled until you regenerate or disable it.

STEP 2 | Regenerate or revoke the API key.

1. You can generate a new API key or revoke the use of the key.
   - Click **Regenerate** to generate a new key. If you suspect that an API key may be compromised, you can generate a new key, which process automatically invalidates the old key.
   - Select **Disable** if you no longer plan to use the key. Disabling the API key revokes it.

Use the Licensing API

The base URI for accessing the licensing API is:

`https://api.paloaltonetworks.com`

You must have a Licensing API key to visit this site. Based on the task you want to perform—for example, activate licenses, deactivate licenses, or track license use—the URL changes.

An API request must use the HTTP POST method, and you must include the API key in the apikey HTTP request header and pass the request parameters as URL-encoded form data with content-type:

`application/x-www-form-urlencoded`

The API Version is optional and can include the following values—0 or 1. If specified, it must be included in the `version` HTTP request header. The current API version is 1; if you do not specify a version, or specify version 0, the request uses the current API version.

All API responses are represented in json.

Before you begin, Get your Licensing API key. This is required before you can perform any of the following tasks:

- Activate Licenses
- Deactivate Licenses
- Track License Usage

Activate Licenses

URL: **`https://api.paloaltonetworks.com/api/license/activate`**

Parameters: uuid, cpuid, authCode, and serialNumber.

Use these parameters to accomplish the following:

- For first time or initial license activation, provide the cpuid, uuid, auth-code in the API request.
- If you did not save the license keys or had a network connection trouble during initial license activation, to retrieve the license(s) again for a firewall that you have previously activated, you can either provide the cpuid and uuid in the API request, or provide the serial number of the firewall in the API request.

Header: apikey

Sample request for initial license activation using Curl:

```
curl -i -H "apikey:$APIKEY" --data-urlencode cpuid=51060400FFFBAB1F --
data-urlencode uuid=564D0E5F-3F22-5FAD-DA58-47352C6229FF --data-urlencode
 authCode=I7115398 https://api.paloaltonetworks.com/api/license/activate
```

Sample API response:

```
[{"lfidField":"13365773","partidField":"PAN-SVC-PREM-VM-300","featureFi--
eld":"Premium","feature_descField":"24 x 7 phone support;
 advanced replacement hardware service","keyField":"m4iZEL1t3n6Oa
+6ll1L7itDZTphYw48N1AMOZXutDgExC5f5pOA52+Qg1jmAxanB
\nKOyat4FJI4k2hWiBYz9cONuKoiaNOtAGhJvAuZmYgqAZejKueWrTzCuLrwxI/iEw
```

```
\nkRGR3cYG+j6o84RitR937m2iOk2v9o8RSfLVilgX28nqmcO8LcAnTqbrRWdFtwVk
\nluz47AUMXauuqwpMipouQYjk0ZL7fTHHslhyL7yFjCyxBoYXOt3JiqQ0OCDdBdDI
\n91RkVPylEwTKgSXm3xpzbmC2ciUR5b235gyqdyW8eQXKvaThuR8YyHr1Pdw/lAjs
\npyyIVFa6FufPacfB2RHApQ==
\n","auth_codeField":"","errmsgField":null,"typeField":"SUP","regDateField":"2016-06-03
 12:00:00 AM","PropertyChanged":null},
{"lfidField":"13365774","partidField":"PAN-VM-300-TP","featureField":"Threat
 Prevention","feature_descField":"Threat Prevention","keyField":"NqaXoaFG
+9qj0t9Vu7FBMizDArj+pmFaQEd6I2OqfBfAibXrvuoFKeXX/K2yXtrl
\n2qJhNq3kwXBDxn181z3nrUOsQd/eW68dyp4jb1MfAwEM8mlnCyLhDRM3EE+umS4b
\ndZBRH5AQjPoaON7xZ46VMFovOR+asOUJXTptS/Eu1bLAI7PBp3+nm04dYTF9O50O
\ndey1jmGoiBZ9wBkesvukg3dVZ7gxppDvz14+wekYEJqPfM0NZyxsC5dnoxg9pciF
\ncFelhnTYlma1lXrCqjJcFdniHRwO0RE9CIKWe0g2HGo1uo2eq1XMxL9mE5t025im
\nblMnhL06smrCdtXmb4jjtg==
\n","auth_codeField":"","errmsgField":null,"typeField":"SUB","regDateField":"2016-06-03
 12:00:00 AM","PropertyChanged":null}
...<truncated>
```


The feature_Field in the response indicates the type of key that follows in the keyField. Copy each key to a text file and save it with the .key extension. Because the key is in json format, it does not have newlines; make sure to convert it to newlines if needed for your parser. Make sure to name each key appropriately and save it to the /license folder of the bootstrap package. For example, include the authcode with the type of key to name it as I3306691_1pa-vm.key (for the capacity license key), I3306691_1threat.key (for the Threat Prevention license key), I3306691_1wildfire.key (for the WildFire subscription license key).

Sample API request for retrieving previously activated licenses using Curl:

```
curl -i -H "apikey:$APIKEY" --data-urlencode serialNumber=007200006142
 https://api/paloaltonetworks.com/api/license/activate
```

Sample API response:


```
[{"lfidField":"13365773","partidField":"PAN-SVC-PREM-
VM-300","featureField":"Premium","feature_descField":"24 x 7 phone
 support; advanced replacement hardware service","keyField":"m4iZEL1t3n6Oa
+6ll1L7itDZTphYw48N1AMOZXutDgExC5f5pOA52+Qg1jmAxanB
\nKOyat4FJI4k2hWiBYz9cONuKoiaNOtAGhJvAuZmYgqAZejKueWrTzCuLrwxI/iEw
\nkRGR3cYG+j6o84RitR937m2iOk2v9o8RSfLVilgX28nqmcO8LcAnTqbrRWdFtwVk
\nluz47AUMXauuqwpMipouQYjk0ZL7fTHHslhyL7yFjCyxBoYXOt3JiqQ0OCDdBdDI
\n91RkVPylEwTKgSXm3xpzbmC2ciUR5b235gyqdyW8eQXKvaThuR8YyHr1Pdw/lAjs
\npyyIVFa6FufPacfB2RHApQ==
\n","auth_codeField":"","errmsgField":null,"typeField":"SUP","regDateField":"2016-06-03
 "expirationField":"8/29/2016 12:00:00 AM","PropertyChanged":null},
{"lfidField":"13365774","partidField":"PAN-VM-300-TP","featureField":"Threat
 Prevention","feature_descField":"Threat Prevention","keyField":"NqaXoaFG
+9qj0t9Vu7FBMizDArj+pmFaQEd6I2OqfBfAibXrvuoFKeXX/K2yXtrl
\n2qJhNq3kwXBDxn181z3nrUOsQd/eW68dyp4jb1MfAwEM8mlnCyLhDRM3EE+umS4b
\ndZBRH5AQjPoaON7xZ46VMFovOR+asOUJXTptS/Eu1bLAI7PBp3+nm04dYTF9O50O
\ndey1jmGoiBZ9wBkesvukg3dVZ7gxppDvz14+wekYEJqPfM0NZyxsC5dnoxg9pciF
\ncFelhnTYlma1lXrCqjJcFdniHRwO0RE9CIKWe0g2HGo1uo2eq1XMxL9mE5t025im
\nblMnhL06smrCdtXmb4jjtg==
\n","auth_codeField":"","errmsgField":null,"typeField":"SUB","regDateField":"2016-06-03
 12:00:00 AM","PropertyChanged":null}
```


...<truncated>

Deactivate Licenses

URL: **`https://api.paloaltonetworks.com/api/license/deactivate`**

Parameters: encryptedToken

To deactivate the license(s) on a firewall that does not have direct internet access, you must generate the license token file locally on the firewall and then use this token file in the API request. For details on generating the license token file, see Deactivate VM or Deactivate a Feature License or Subscription Using the CLI.

Header: apikey

Request: https://api.paloaltonetworks.com/api/license/deactivate?encryptedtoken@<token>

Sample API request for license deactivation using Curl:

```
curl -i -H "apikey:$APIKEY" --data-urlencode
 encryptedtoken@dact_lic.05022016.100036.tok https://
api.paloaltonetworks.com/api/license/deactivate
```

Sample API response:

```
[{"serialNumField":"007200006150","featureNameField":"","issueDateField":"","successFie
{"serialNumField":"007200006150","featureNameField":"","issueDateField":"","successFiel
{"serialNumField":"007200006150","featureNameField":"","issueDateField":"","successFiel
{"serialNumField":"007200006150","featureNameField":"","issueDateField":"","successFiel
{"serialNumField":"007200006150","featureNameField":"","issueDateField":"","successFiel
{"serialNumField":"007200006150","featureNameField":"","issueDateField":"","successFiel
```

Track License Usage

URL: **`https://api.paloaltonetworks.com/api/license/get`**

Parameters: authCode

Header: apikey

Request: https://api.paloaltonetworks.com/api/license/get?authCode=<authcode>

Sample API request for tracking license usage using Curl:

```
curl -i -H "apikey:$APIKEY" --data-urlencode authcode=I9875031 https://
api.paloaltonetworks.com/api/license/get
```

Sample API response:

```
HTTP/1.1 200 OK
Date: Thu, 05 May 2016 20:07:16 GMT
Content-Length: 182

{"AuthCode":"I9875031","UsedCount":4,"TotalVMCount":10,"UsedDeviceDetails":
[{"UUID":"420006BD-113D-081B-F500-2E7811BE80C
9","CPUID":"D7060200FFFBAB1F","SerialNumber":"007200006142"}]}.....
```

Licensing API Error Codes

The HTTP Error Codes that the licensing server returns are as follows:

- 200 Success
- 400 Error

- 401 Invalid API Key
- 500 Server Error

Licenses for Cloud Security Service Providers (CSSPs)

The Palo Alto Networks CSSP partners program allows service providers to provide security as a service or as a hosted application to their end customers. The license offerings that Palo Alto Networks provides for authorized Cloud Security Service Provider (CSSP) partners are different from the offerings for enterprise users.

For CSSP partners, Palo Alto Networks supports a usage-based model for the VM-Series firewalls bundled with subscriptions and support. CSSP partners can combine a term-based capacity license for the VM-Series Models with a choice of subscription licenses for Threat Prevention, URL Filtering, AutoFocus, GlobalProtect, and WildFire, and support entitlements that provide access to technical support and software updates. If you plan on deploying the firewalls in an HA configuration, you can purchase the cost-effective high availability option.

- Get the Auth Codes for CSSP License Packages
- Register the VM-Series Firewall with a CSSP Auth Code
- Add End-Customer Information for a Registered VM-Series Firewall

Get the Auth Codes for CSSP License Packages

To be a CSSP Partner, you have to enroll in the Palo Alto Networks CSSP partners program. For information on enrolling in the CSSP program, contact your Palo Alto Networks Channel Business Manager. If you are enrolled, the Palo Alto Network Support portal provides tools that allow you to select a license package, track license usage, and apply license entitlements.

A license package is a combination of the following options:

- Usage term—The pay-per-use options are hourly, monthly, 1-year, and 3-years.
- VM-Series firewall model—The VM-100, VM-200, VM-300, and VM-1000-HV that give you the model number and the capacities associated with each model.
- Subscription bundle—The three options are basic, bundle 1, and bundle 2. The basic option does not include any subscriptions; bundle 1 has the Threat Prevention license that includes IPS, AV, malware prevention; bundle 2 has the Threat Prevention (includes IPS, AV, malware prevention), GlobalProtect, WildFire, and PAN-DB URL Filtering licenses.
- Level of support—Premium support or backline support.
- Redundant firewalls—The option are either high availability (HA) or without HA. This option is a cost-effective option if you plan to deploy a pair of redundant firewalls.

The offering PAN-VM-300-SP-PREM-BND1-YU, for example, is a one-year term package that includes the VM-300 with premium support and the subscription bundle 1. Each package supports up to a maximum of 10,000 instances of the VM-Series firewall.

After you select your license package, you receive an email with your auth code; the fulfillment process can take up to 48 hours.

STEP 1 | Log in to the Palo Alto Networks Customer Support website with your account credentials. If you need a new account, see Create a Support Account.

STEP 2 | Select **CSSP** > **Order History**, to view the list of auth codes registered to your support account.

As you deploy firewalls, you must register each instance of the firewall against an auth code.

Register the VM-Series Firewall with a CSSP Auth Code

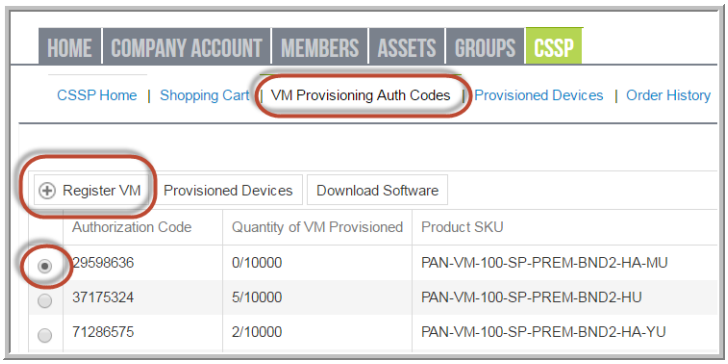
To activate the license on your VM-Series firewall, you must have deployed the VM-Series firewall and completed initial configuration. As a CSSP partner, you can choose from the following options to register a firewall:

- API—Use the Licensing API if you have a custom script or an orchestration service. With this option, the firewall does not need direct internet access.
- Bootstrap—Use this option to automatically configure the firewall and license it on first boot. See Bootstrap the VM-Series Firewall.
- Firewall web interface—You can Activate the License for the VM-Series Firewall (Standalone Version) using the firewall web interface. This workflow is valid for firewalls with or without internet access.
- Customer Support Portal—Use this option to manually register the firewall on the Palo Alto Networks Customer Support portal, as shown below.

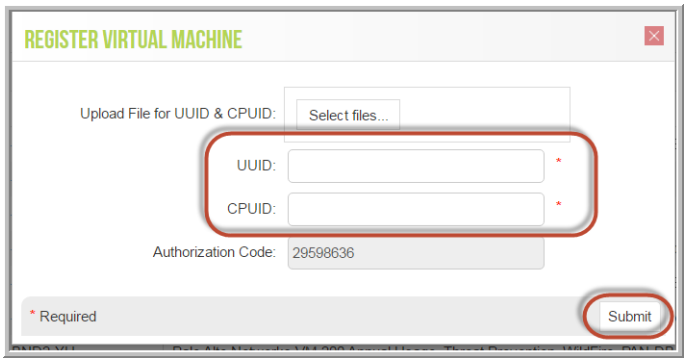
STEP 1 | Log in to the Palo Alto Networks Customer Support website with your account credentials. If you need a new account, see Create a Support Account.

STEP 2 | Select **CSSP** > **Order History**, to view the list of auth codes registered to your support account.

STEP 3 | Select **CSSP** > **VM Provisioning Auth Codes**, select an **Authorization Code** and click **Register VM**.



STEP 4 | Enter the **UUID** and **CPUID** of the VM instance and click **Submit**. The portal will generate a serial number for the firewall.



You can track the number of VM-Series firewalls that have been deployed and the number of licenses that are still available for use against each auth code. To view all the total number of firewalls registered against a specific auth code, select CSSP >

VM Provisioning Auth Codes, then select an Authorization Code and click Provisioned Devices.

Add End-Customer Information for a Registered VM-Series Firewall

For CSSP licensees, after you register the firewall, you can use either the Palo Alto Networks Support portal or the Licensing API to link the serial number of the VM-Series firewall with the customer for whom you provisioned the firewall.

- Add End-Customer Information for a Registered VM-Series Firewall (Customer Support Portal). The Support portal authenticates with user name and password.
- Add End-Customer Information for a Registered VM-Series Firewall (API). The API authenticates using the Licensing API key.

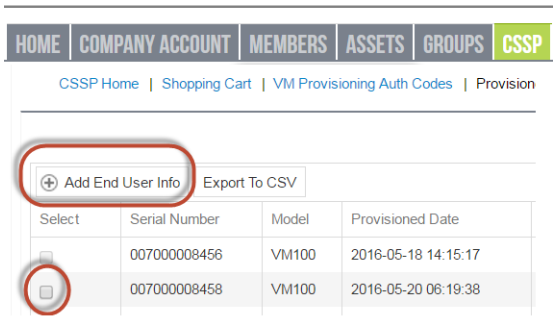
Add End-Customer Information for a Registered VM-Series Firewall (Customer Support Portal)

Complete the following procedure to add end-customer information for a registered firewall through the Customer Support Portal.

STEP 1 | Log in to the Palo Alto Networks Customer Support website with your account credentials.

STEP 2 | Select **CSSP** > **Provisioned Devices**.

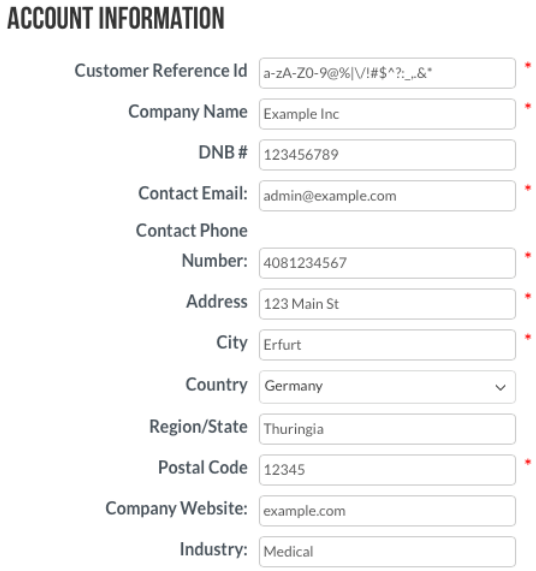
STEP 3 | Select the **Serial Number** and click **Add End User Info**.



STEP 4 | Enter the **Account Information** for the customer as follows.

- Customer Reference Id: Required
- Company Name: Required
- DNB #: Data Universal Numbering System (D-U-N-S) number
- Contact Email: Required, end-user email address
- Contact Phone Number: End-user phone number
- Address: Required, end-user address
- Country: Required, ISO 2-letter country code
- City: Required, end-user city name
- Region/State: Required; for the United States and Canada, you must enter an ISO 2-letter subdivision code; for all other countries, any text string is valid
- Postal Code: Required, end-user postal code
- Company Website: End-user website URL
- Industry: End-user industry type, such as networking or consultancy

Click **Submit** to save the details.



After you add account information, you can find all firewalls registered to a customer. In Search Existing End User, enter the customer ID or customer name and click Search to find all firewalls provisioned for the customer.

Add End-Customer Information for a Registered VM-Series Firewall (API)

The URL for accessing the API is https://api.paloaltonetworks.com/api/license/ReportEndUserInfo.

An API request must use the HTTP POST method, and you must include HTTP requests headers that include the API key and specify the content type as JSON. API responses are in JSON format.

STEP 1 | Get your Licensing API key.

STEP 2 | Use the ReportEndUserInfo API to add end-user information for a VM-Series Firewall that is registered to a CSSP.

URL: **`https://api.paloaltonetworks.com/api/license/ReportEndUserInfo`**

Headers:

- Content-Type: application/json
- apiKey: *API Key*

Parameters:

- `SerialNumbers`: Required, provide at least one valid firewall serial number
- `CustomerReferenceId`: Required
- `CompanyName`: Required, end-user company name
- `DnBNumber`: Data Universal Numbering System (D-U-N-S) number
- `PhoneNumber`: End-user phone number
- `EndUserContactEmail`: Required, end-user email address
- `Address`: Required, end-user address
- `Country`: Required, ISO 2-letter country code
- `City`: Required, end-user city name

- `Region/State`: Required; for the United States and Canada, you must enter an ISO 2-letter subdivision code; for all other countries, any alpha string is valid
- `PostalCode`: Required, end-user postal code
- `Industry`: End-user industry type, such as networking or consultancy
- `WebSite`: End-user website URL
- `CreatedBy`: System or person submitting this information

Sample request to add end-user information for a registered VM-Series firewall using Curl:

```
curl -X POST -H "Content-Type: application/json" -H
 "apiKey:921d4450e988397138ca8a68vf2fc5d687870b3f11cb9439946a521dc4dc7cd8"
 "http://api.paloaltonetworks.com/api/license/ReportEndUserInfo?
serialNumbers=0001A101234&CustomerAccountId=12345&CompanyName=ExampleInc&DnBNumber=12
 Main
 St&Country=US&Region=CA&City=Sunnydale&State=CA&PostalCode=12345&Industry=Medical&Ph
 Doe"
```

Sample API response:

```
"{"Message": "End User Information Updated Successfully"}"
```

If you receive an error, see Licensing API Error Codes.

Set Up a VM-Series Firewall on an ESXi Server

The VM-Series firewall is distributed using the Open Virtualization Alliance (OVA) format, which is a standard method of packaging and deploying virtual machines. You can install this solution on any x86 device that is capable of running VMware ESXi.

In order to deploy a VM-Series firewall you must be familiar with VMware and vSphere including vSphere networking, ESXi host setup and configuration, and virtual machine guest deployment.

If you would like to automate the process of deploying a VM-Series firewall, you can create a gold standard template with the optimal configuration and policies, and use the vSphere API and the PAN-OS XML API to rapidly deploy new VM-Series firewalls in your network. For more information, see the article: VM-Series Data Center Automation.

See the following topics for information on:

- Supported Deployments on VMware vSphere Hypervisor (ESXi)
- VM-Series on ESXi System Requirements and Limitations
- Install a VM-Series firewall on VMware vSphere Hypervisor (ESXi)
- Troubleshoot ESXi Deployments
- Performance Tuning of the VM-Series for ESXi

Supported Deployments on VMware vSphere Hypervisor (ESXi)

You can deploy one or more instances of the VM-Series firewall on the ESXi server. Where you place the VM-Series firewall on the network depends on your topology. Choose from the following options (for environments that are not using VMware NSX):

- **One VM-Series firewall per ESXi host**—Every VM server on the ESXi host passes through the firewall before exiting the host for the physical network. VM servers attach to the firewall via virtual standard switches. The guest servers have no other network connectivity and therefore the firewall has visibility and control to all traffic leaving the ESXi host. One variation of this use case is to also require all traffic to flow through the firewall, including server to server (east-west traffic) on the same ESXi host.
- **One VM-Series firewall per virtual network**—Deploy a VM-Series firewall for every virtual network. If you have designed your network such that one or more ESXi hosts has a group of virtual machines that belong to the internal network, a group that belongs to the external network, and some others to the DMZ, you can deploy a VM-Series firewall to safeguard the servers in each group. If a group or virtual network does not share a virtual switch or port group with any other virtual network, it is completely isolated from all other virtual networks within or across the host(s). Because there is no other physical or virtual path to any other network, the servers on each virtual network, must use the firewall to talk to any other network. Therefore, it allows the firewall visibility and control to all traffic leaving the virtual (standard or distributed) switch attached to each virtual network.
- **Hybrid environment**—Both physical and virtual hosts are used, the VM-Series firewall can be deployed in a traditional aggregation location in place of a physical firewall appliance to achieve the benefits of a common server platform for all devices and to unlink hardware and software upgrade dependencies.

Continue with VM-Series on ESXi System Requirements and Limitations and Install a VM-Series firewall on VMware vSphere Hypervisor (ESXi).

VM-Series on ESXi System Requirements and Limitations

This section lists requirements and limitations for the VM-Series firewall on VMware vSphere Hypervisor (ESXi). To deploy the VM-Series firewall, see Install a VM-Series firewall on VMware vSphere Hypervisor (ESXi).

- VM-Series on ESXi System Requirements
- VM-Series on ESXi System Limitations

VM-Series on ESXi System Requirements

You can create and deploy multiple instances of the VM-Series firewall on an ESXi server. Because each instance of the firewall requires a minimum resource allocation—number of CPUs, memory and disk space—on the ESXi server, make sure to conform to the specifications below to ensure optimal performance.

The VM-Series firewall has the following requirements:

- The host CPU must be a x86-based Intel or AMD CPU with virtualization extension.
- VMware ESXi with vSphere 5.1, 5.5, 6.0, or 6.5 for VM-Series running PAN-OS 8.0. The VM-Series firewall on ESXi is deployed with VMware virtual machine hardware version 9 (vmx-09); no other VMware virtual machine hardware versions are supported.
- See VM-Series System Requirements for the minimum hardware requirements for your VM-Series model.
- Minimum of two network interfaces (vmNICs). One will be a dedicated vmNIC for the management interface and one for the data interface. You can then add up to eight more vmNICs for data traffic. For additional interfaces, use VLAN Guest Tagging (VGT) on the ESXi server or configure subinterfaces on the firewall.

  The use of hypervisor assigned MAC address is enabled by default. vSphere assigns a unique vmNIC MAC address to each dataplane interface of the VM-Series firewall. If you disable the use hypervisor assigned MAC addresses, the VM-Series firewall assigns each interface of a MAC address from its own pool. Because this causes the MAC addresses on each interface to differ, you must enable promiscuous mode (see Before deploying the OVA file, set up virtual standard switch(es) and virtual distributed switch(es) that you will need for the VM-Series firewall.) on the port group of the virtual switch to which the dataplane interfaces of the firewall are attached to allow the firewall to receive frames. If neither promiscuous mode nor hypervisor assigned MAC address is enabled, the firewall will not receive any traffic. This is because vSphere will not forward frames to a virtual machine when the destination MAC address of the frame does not match the vmNIC MAC address.

  Data Plane Development Kit (DPDK) is enabled by default on VM-Series firewalls on ESXi. For more information about DPDK, see Enable DPDK on ESXi.
- To achieve the best performance out of the VM-Series firewall, you can make the following adjustments to the host before deploying the VM-Series firewall. See Performance Tuning of the VM-Series for ESXi for more information.
  - Enable DPDK. DPDK allows the host to process packets faster by bypassing the Linux kernel. Instead, interactions with the NIC are performed using drivers and the DPDK libraries.
  - Enable SR-IOV. Single root I/O virtualization (SR-IOV) allows a single PCIe physical device under a single root port to appear to be multiple separate physical devices to the hypervisor or guest.

    Do not configure a vSwitch on the physical port on which you enable SR-IOV. To communicate with the host or other virtual machines on the network, the VM-Series firewall must have exclusive access to the physical port and associated virtual functions (VFs) on that interface.

- Enable multi-queue support for NICs. Multi-queue allows network performance to scale with the number of vCPUs and allows for parallel packet processing by creating multiple TX and RX queues.

Do not use the VMware snapshots functionality on the VM-Series on ESXi. Snapshots can impact performance and result in intermittent and inconsistent packet loss.See VMWare's best practice recommendation with using snapshots.

If you need configuration backups, use Panorama or Export named configuration snapshot from the firewall (Device > Set up > Operations). Using the Export named configuration snapshot exports the active configuration (running-config.xml) on the firewall and allows you to save it to any network location.

VM-Series on ESXi System Limitations

The VM-Series firewall functionality is very similar to the Palo Alto Networks hardware firewalls, but with the following limitations:

- Dedicated CPU cores are recommended.
- High Availability (HA) Link Monitoring is not supported on VM-Series firewalls on ESXi. Use Path Monitoring to verify connectivity to a target IP address or to the next hop IP address.
- Up to 10 total ports can be configured; this is a VMware limitation. One port will be used for management traffic and up to 9 can be used for data traffic.
- Only the vmxnet3 driver is supported.
- Virtual systems are not supported.
- vMotion of the VM-Series firewall is not supported. However, the VM-Series firewall can secure guest virtual machines that have migrated to a new destination host, if the source and destination hosts are members of all vSphere Distributed Switches that the guest virtual machine used for networking.
- Forged transmit and promiscuous mode must be enabled on the ESXi vSwitch port groups connected to Layer 2 and vwire interfaces on the VM-Series firewall.
- To use PCI devices with the VM-Series firewall on ESXi, memory mapped I/O (MMIO) must be below 4GB. You can disable MMIO above 4GB in your server's BIOS. This is an ESXi limitation.

Install a VM-Series firewall on VMware vSphere Hypervisor (ESXi)

To install a VM-Series firewall you must have access to the Open Virtualization Alliance format (OVA) template. Use the auth code you received in your order fulfillment email to register your VM-Series firewall and gain access to the OVA template. The OVA is downloaded as a zip archive that is expanded into three files: the .ovf extension is for the OVF descriptor file that contains all metadata about the package and its contents; the .mf extension is for the OVF manifest file that contains the SHA-1 digests of individual files in the package; and the .vmdk extension is for the virtual disk image file that contains the virtualized version of the firewall.

- Plan the Interfaces for the VM-Series for ESXi
- Provision the VM-Series Firewall on an ESXi Server
- Perform Initial Configuration on the VM-Series on ESXi
- (Optional) Add Additional Disk Space to the VM-Series Firewall
- Use VMware Tools on the VM-Series Firewall on ESXi and vCloud Air

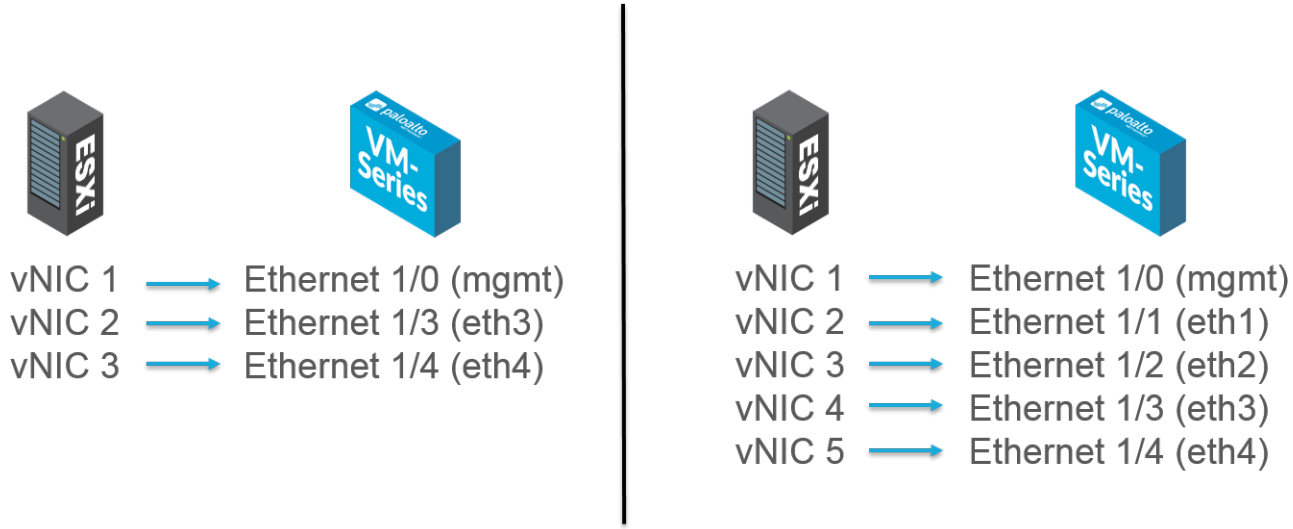
Plan the Interfaces for the VM-Series for ESXi

By planning the mapping of VM-Series Firewall vNICs and interfaces, you can avoid reboots and configuration issues. The following table describes the default mapping between VMware vNICs and VM-Series interfaces when all 10 vNICs are enabled on ESXi.

VMware vNIC	VM-Series Interfaces
1	Ethernet 1/0 (mgmt)
2	Ethernet 1/1 (eth1)
3	Ethernet 1/2 (eth2)
4	Ethernet 1/3 (eth3)
5	Ethernet 1/4 (eth4)
6	Ethernet 1/5 (eth5)
7	Ethernet 1/6 (eth6)
8	Ethernet 1/7 (eth7)
9	Ethernet 1/8 (eth8)
10	Ethernet 1/9 (eth9)

The mapping on the VM-Series Firewall remains the same no matter which vNICs you add on ESXi. No matter which interfaces you activate on the firewall, they always take the next available vNIC on ESXi. In the following example, eth3 and eth4 on the VM-Series Firewall are paired to vNICs 2 and 3 on ESXi respectively. If you add want to add two additional interfaces, you must activate vNICs 4 and 5; doing

this requires you to power down the VM-Series firewall. If you activate eth1 and eth2 on the VM-Series Firewall, the interfaces will reorder themselves. This can result in a mapping mismatch and impact traffic.



To avoid issues like those described in the preceding example, you can do the following:

- Activate all nine vNICs beyond the first when provisioning your ESXi host. Adding all nine vNICs as placeholders before powering on the VM-Series Firewall allows you to use any VM-Series interfaces regardless of order.
- By activating the vNICs before powering on the VM-Series Firewall, adding additional interfaces in the future no longer requires a reboot. Because each vNIC on ESXi requires that you choose a network, you can create an empty port group as a network placeholder.
- Do not remove VM-Series Firewall vNICs to avoid mapping mismatches.

Provision the VM-Series Firewall on an ESXi Server

Use these instruction to deploy the VM-Series firewall on a (standalone) ESXi server. For deploying the VM-Series NSX edition firewall, see Set Up the VM-Series Firewall on VMware NSX.

STEP 1 | Download the OVA file.

Register your VM-Series firewall and obtain the OVA file from the Palo Alto Networks Customer Support web site.

The file contains the base installation. After the base installation is complete, you will need to download and install the latest PAN-OS version from the support portal. This will ensure that you have the latest fixes that were implemented since the base image was created. For instructions, see Upgrade the PAN-OS Software Version (Standalone Version).

STEP 2 | Before deploying the OVA file, set up virtual standard switch(es) and virtual distributed switch(es) that you will need for the VM-Series firewall.

If you are deploying the VM-Series firewall with Layer 3 interfaces, your firewall will use Hypervisor Assigned MAC Addresses by default. If you choose to disable the use of hypervisor assigned MAC address, you must configure (set to **Accept**) any virtual switch attached to the VM-Series firewall to allow the following modes:

- Promiscuous mode
- MAC address changes

- Forged transmits

If you are deploying the firewall with Layer 2, virtual wire, or tap interfaces, you must configure any virtual switch attached to the VM-Series firewall to allow (set to Accept) the modes listed above.

To configure a virtual standard switch to receive frames for the VM-Series firewall:

1. Configure a virtual standard switch from the vSphere Client by navigating to **Home** > **Inventory** > **Hosts and Clusters**.
2. Click the **Configuration** tab and under **Hardware** click **Networking**. For each VM-Series firewall attached virtual switch, click on **Properties**.
3. Highlight the virtual switch and click **Edit**. In the vSwitch properties, click the **Security** tab and set **Promiscuous Mode**, **MAC Address Changes** and **Forged Transmits** to **Accept** and then click **OK**. This change will propagate to all port groups on the virtual switch.

To configure a virtual distributed switch to receive frames for the VM-Series firewall:

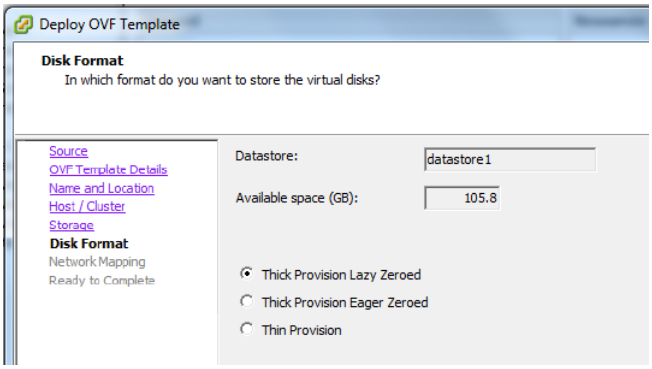
1. Select **Home** > **Inventory** > **Networking**. Highlight the **Distributed Port Group** you want to edit and select the **Summary** tab.
2. Click **Edit Settings** and select **Policies** > **Security** and set **Promiscuous Mode, MAC Address Changes** and **Forged Transmits** to **Accept** and then click **OK**.

STEP 3 | Deploy the OVA.

If you add additional interfaces (vmNICs) to the VM-Series firewall, a reboot is required because new interfaces are detected during the boot cycle. To avoid the need to reboot the firewall, make sure to add the interfaces at initial deployment or during a maintenance window so that you can reboot the firewall.

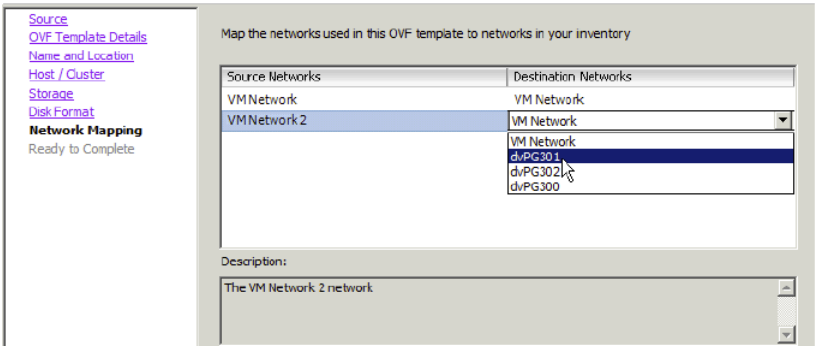
To view the progress of the installation, monitor the Recent Tasks list.

1. Log in to vCenter using the vSphere client. You can also go directly to the target ESXi host if needed.
2. From the vSphere client, select **File** > **Deploy OVF Template**.
3. Browse to the OVA file that you downloaded in 1, select the file and then click **Next**. Review the templates details window and then click **Next** again.
4. Name the VM-Series firewall instance and in the **Inventory Location** window, select a Data Center and Folder and click **Next**
5. Select an ESXi host for the VM-Series firewall and click **Next**.
6. Select the datastore to use for the VM-Series firewall and click **Next**.
7. Leave the default settings for the datastore provisioning and click **Next**. The default is **Thick Provision Lazy Zeroed**.

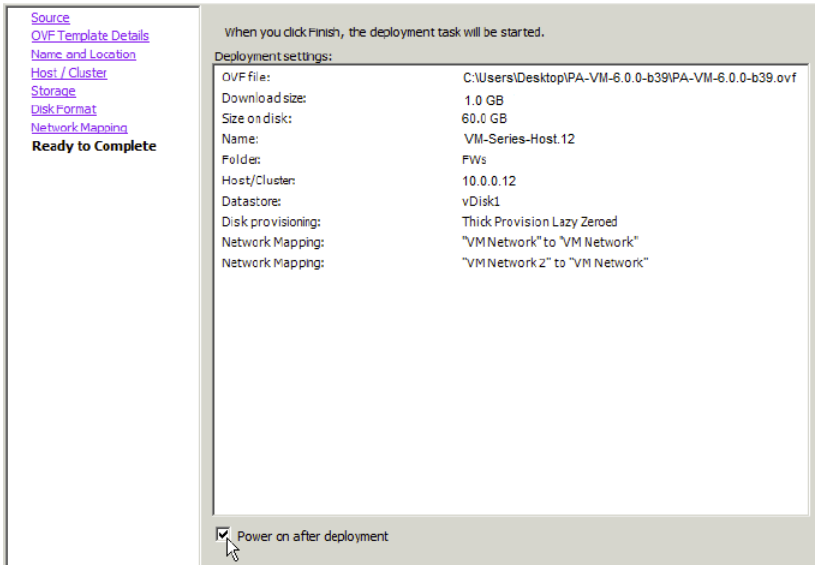


Do not configure CPU affinity for the VM-Series firewall. The vCenter/ESXi server optimizes the CPU placement for the VM-Series and the firewall performs best when you do not modify the non-uniform memory access (NUMA) configuration.

8. Select the networks to use for the two initial vmNICs. The first vmNIC will be used for the management interface and the second vmNIC for the first data port. Make sure that the **Source Networks** maps to the correct **Destination Networks**.



9. Review the details window, select the **Power on after deployment** check box and then click **Next**.



10. When the deployment is complete, click the **Summary** tab to review the current status.

Perform Initial Configuration on the VM-Series on ESXi

Use the virtual appliance console on the ESXi server to set up network access to the VM-Series firewall. By default, the VM-Series firewall uses DHCP to obtain an IP address for the management interface. However, you can assign a static IP address. After completing the initial configuration, access the web interface to complete further configurations tasks. If you have Panorama for central management, refer to the Panorama Administrator's Guide for information on managing the device using Panorama.

If you are using bootstrapping to perform the configuration of your VM-Series firewall on ESXi, refer to Bootstrap the VM-Series Firewall on ESXi.

For general information about bootstrapping, see Bootstrap the VM-Series Firewall.

STEP 1 | Gather the required information from your network administrator.

- IP address for MGT port
- Netmask
- Default gateway
- DNS server IP address

STEP 2 | Access the console of the VM-Series firewall.

1. Select the **Console** tab on the ESXi server for the VM-Series firewall, or right click the VM-Series firewall and select **Open Console**.
2. Press enter to access the login screen.
3. Enter the default username/password (admin/admin) to log in.
4. Enter **`configure`** to switch to configuration mode.

STEP 3 | Configure the network access settings for the management interface. You should restrict access to the firewall and isolate the management network. Additionally, do not make the allowed network larger than necessary and never configure the allowed source as 0.0.0.0/0.

Enter the following commands:

```
set deviceconfig system type static
```

```
set deviceconfig system ip-address <Firewall-IP> netmask <netmask>
default-gateway <gateway-IP> dns-setting servers primary <DNS-IP>
```

where *<Firewall-IP>* is the IP address you want to assign to the management interface, *<netmask>* is the subnet mask, *<gateway-IP>* is the IP address of the network gateway, and *<DNS-IP>* is the IP address of the DNS server.

STEP 4 | Commit your changes and exit the configuration mode.

Enter **`commit`**.

Enter **`exit`**.

STEP 5 | Verify network access to external services required for firewall management, such as the Palo Alto Networks Update Server.

1. Use the ping utility to verify network connectivity to the Palo Alto Networks Update server as shown in the following example. Verify that DNS resolution occurs and the response includes the IP address for the Update server; the update server does not respond to a ping request.

```
admin@PA-200> ping
host updates.paloaltonetworks.com
```

```
PING updates.paloaltonetworks.com (10.101.16.13) 56(84)bytes of data.
From 192.168.1.1 icmp_seq=1 Destination Host Unreachable
From 192.168.1.1 icmp_seq=2 Destination Host Unreachable
From 192.168.1.1 icmp_seq=3 Destination Host Unreachable
From 192.168.1.1 icmp_seq=4 Destination Host Unreachable
```

After verifying DNS resolution, press Ctrl+C to stop the ping request.

2. Use the following CLI command to retrieve information on the support entitlement for the firewall from the Palo Alto Networks update server:

```
request support
check
```

If you have connectivity, the update server will respond with the support status for your firewall.

An unlicensed VM-Series firewall can process up to approximately 1230 concurrent sessions. Depending on the environment, the session limit can be reached very quickly. Therefore, apply the capacity auth-code and retrieve a license before you begin testing the VM-Series firewall; otherwise, you might have unpredictable results, if there is other traffic on the port group(s).

Add Additional Disk Space to the VM-Series Firewall

The VM-Series firewall requires a virtual disk 40GB, of which 17GB is used for logging. For larger deployments, to aggregate data from all next-generation firewalls and provide visibility across all the traffic on your network, use Panorama for centralized logging and reporting. In smaller deployments, where you do not use Panorama but require more log storage capacity, use the following procedure to add a new virtual disk that can support 40GB to 2TB of storage capacity for logs.

When configured to use a virtual disk, the virtual appliance does not use the default 17GB storage for logging. Therefore, if it loses connectivity to the virtual disk, logs could be lost during the failure interval.

To allow for redundancy, place the newly created virtual disk on a datastore that provides RAID redundancy. RAID10 provides the best write performance for applications with high logging characteristics.

STEP 1 | Power off the VM-Series firewall.

STEP 2 | On the ESX(i) server, add the virtual disk to the firewall.

1. Select the VM-Series firewall on the ESX(i) server.
2. Click **Edit Settings**.
3. Click **Add** to launch the Add Hardware wizard, and select the following options when prompted:
    1. Select **Hard Disk** for the hardware type.
    2. Select **Create a new virtual disk**.
    3. Select **SCSI** as the virtual disk type.

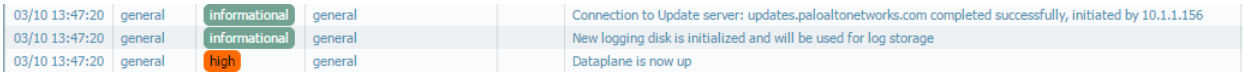
4. Select the **Thick provisioning** disk format.
5. In the location field, select **Store with the virtual machine option**. The datastore does not have to reside on the ESX(i) server.
6. Verify that the settings look correct and click **Finish** to exit the wizard. The new disk is added to the list of devices for the virtual appliance.

STEP 3 | Power on the firewall.

When powered on, the virtual disk is initialized for first-time use. The time that the initialization process takes to complete varies by the size of the new virtual disk.

When the new virtual disk is initialized and ready, all logs from the existing disk will be moved over to the new virtual disk. Newly generated log entries will now be written to this new virtual disk.

A system log entry that records the new disk is also generated.



If you reuse a virtual disk, that is if the disk was previously used for storing PAN-OS logs, all logs from the existing disk will not be moved over to the virtual disk.

STEP 4 | Verify the size of the new virtual disk.

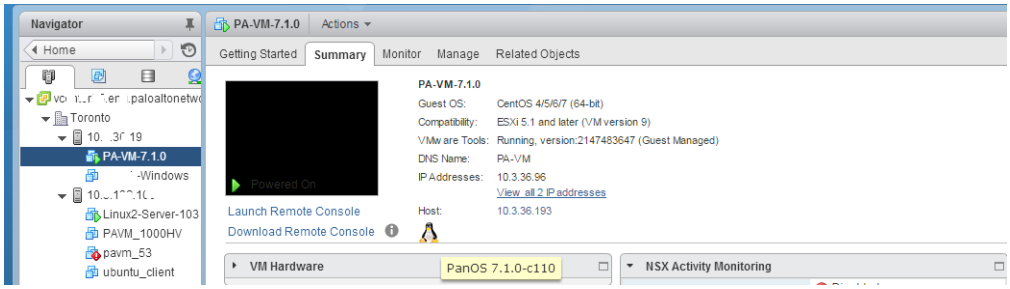
1. Select **Device** > **Setup** > **Management**.
2. In the Logging and Reporting Settings section, verify that the **Log Storage** capacity accurately displays the new disk capacity.

Use VMware Tools on the VM-Series Firewall on ESXi and vCloud Air

VMware Tools is a utility that improves the ability to manage the VM-Series firewall from vCenter server and vCloud Director. VMware Tools is bundled with the software image for the VM-Series firewall and all updates will be made available with a new ovf image; you cannot manually install or upgrade VMware Tools using the vCenter server or vCloud Director.

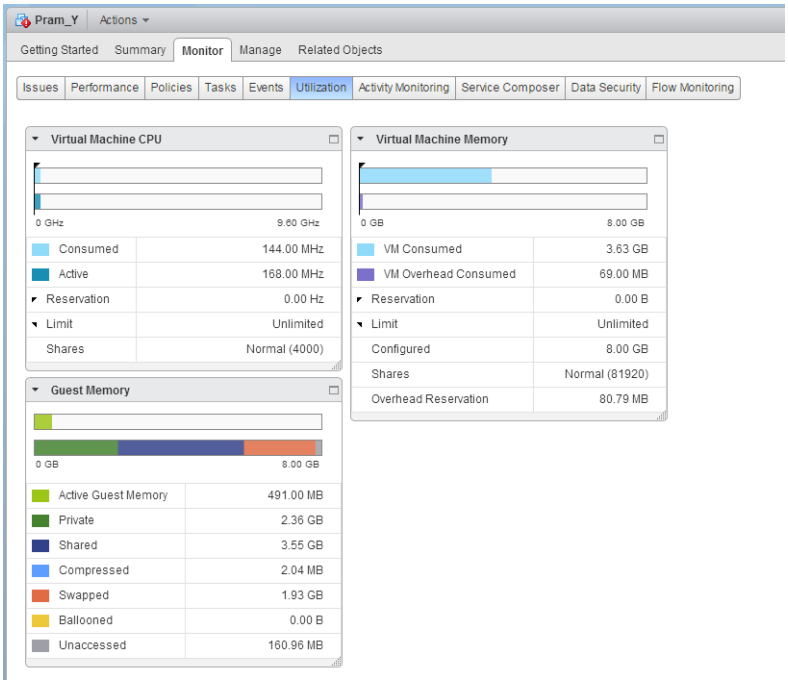
- View the IP address(es) on the management interface and the software version on the firewall and Panorama.

  In the Hosts and Cluster section on the vCenter server, select the firewall or Panorama and view the **Summary** tab for information on the IP address(es) assigned to the management interface and the software version currently installed.



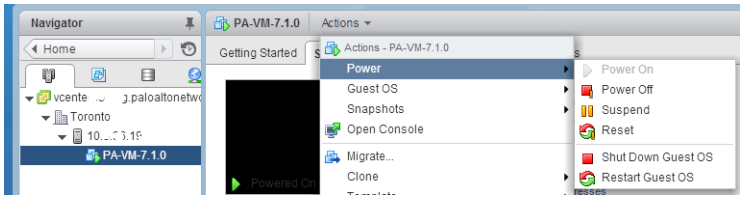
- View resource utilization metrics on hard disk, memory, and CPU. Use these metrics to enable alarms on the vCenter server.

  In the Hosts and Cluster section on the vCenter server, select the firewall or Panorama and view the **Monitor** > **Utilization** tab for information on hard disk, memory, and CPU usage.



- Gracefully shutdown or restart the firewall and Panorama from the vCenter server.

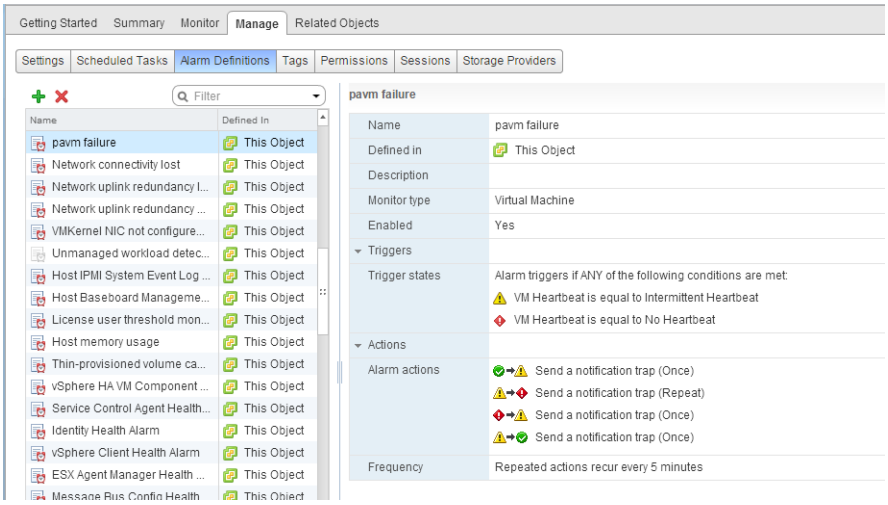
  In the Hosts and Cluster section on the vCenter server, select the firewall or Panorama and select the **Actions** > **Power** drop-down.



- Create alarm definitions for events you want to be notified on, or for which you want to specify an automated action.

  Refer to the VMware documentation for details on creating alarm definitions.

In the Hosts and Cluster section on the vCenter server, select the firewall or Panorama and select the **Manage** > **Alarm Definitions** to add a new trigger and specify an action when a threshold is met. For example, missing heartbeats for a specified duration, or when memory resource usage exceeds a threshold. The following screenshot shows you how to use notifications for heartbeat monitoring on the firewall or Panorama.



Troubleshoot ESXi Deployments

Many of the troubleshooting steps for the VM-Series firewall are very similar to the hardware versions of PAN-OS. When problems occur, you should check interface counters, system log files, and if necessary, use debug to create captures. For more details on PAN-OS troubleshooting, refer to the article on Packet Based Troubleshooting.

The following sections describe how to troubleshoot some common problems:

- Basic Troubleshooting
- Installation Issues
- Licensing Issues
- Connectivity Issues

Basic Troubleshooting

Recommendation for Network Troubleshooting Tools

It is useful to have a separate troubleshooting station to capture traffic or inject test packets in the virtualized environment. It can be helpful to build a fresh OS from scratch with common troubleshooting tools installed such as tcpdump, nmap, hping, traceroute, iperf, tcpedit, netcat, etc. This machine can then be powered down and converted to a template. Each time the tools are needed, the troubleshooting client (virtual machine) can be quickly deployed to the virtual switch(es) in question and used to isolate networking problems. When the testing is complete, the instance can simply be discarded and the template used again the next time it is required.

For performance related issues on the firewall, first check the **Dashboard** from the firewall web interface. To view alerts or create a tech support or stats dump files navigate to **Device** > **Support**.

For information in the vSphere client go to **Home** > **Inventory** > **VMs and Templates**, select the VM-Series firewall instance and click the **Summary** tab. Under **Resources**, check the statistics for consumed memory, CPU and storage. For resource history, click the **Performance** tab and monitor resource consumption over time.

Installation Issues

- Issues with deploying the OVA
- Why does the firewall boot into maintenance mode?
- How do I modify the base image file for the VM-1000-HV license?

Issues with deploying the OVA

The VM-Series is delivered as a file in the Open Virtualization Alliance (OVA) format. The OVA image is downloaded as a zip archive that is expanded into three files. If you are having trouble deploying the OVA image, make sure the three files are unpacked and present and, if necessary, download and extract the OVA image again.

- The ovf extension is for the OVF descriptor file that contains all metadata about the package and its contents.
- The mf extension is for the OVF manifest file that contains the SHA-1 digests of individual files in the package.
- The vmdk extension is for the virtual disk image file.

The virtual disk in the OVA image is large for the VM-Series; this file is nearly 900MB and must be present on the computer running the vSphere client or must be accessible as a URL for the OVA image. Make sure the network connection is sufficient between the vSphere client computer and the target ESXi host. Any firewalls in the path will need to allow TCP ports 902 and 443 from the vSphere client to the ESXi host(s).There needs to be sufficient bandwidth and low latency on the connection otherwise the OVA deployment can take hours or timeout and fail.

ESX 6.5.0a build 4887370 limits you to 2 CPU cores per socket. If you are deploying a VM-300, VM-500 or VM-700 to which you want to allocate more than 2 vCPUs per socket, refer to the VMware KB: https://kb.vmware.com/s/article/53354, for a workaround.

Why does the firewall boot into maintenance mode?

If you have purchased the VM-1000-HV license and are deploying the VM-Series firewall in standalone mode on a VMware ESXi server or on a Citrix SDX server, you must allocate the minimum memory required by you VM-Series model.

To fix this issue, you must either modify the base image file (see How do I modify the base image file for the VM-1000-HV license?) or edit the settings on the ESXi host or the vCenter server before you power on the VM-Series firewall.

Also, verify that the interface is VMXnet3; setting the interface type to any other format will cause the firewall to boot into maintenance mode.

How do I modify the base image file for the VM-1000-HV license?

If you have purchased the VM-1000-HV license and are deploying the VM-Series firewall in standalone mode on a VMware ESXi server or on a Citrix SDX server, use these instructions to modify the following attributes that are defined in the base image file (.ova or .xva) of the VM-Series firewall.

Important: Modifying the values other than those listed hereunder will invalidate the base image file.

STEP 1 | Open the base image file, for example 7.0.0, with a text editing tool such as notepad.

STEP 2 | Search for 4096 and change the memory allocated to 5012 (that is 5 GB) here:

```
<Item>
        <rasd:AllocationUnits>byte * 2^20</rasd:AllocationUnits>
        <rasd:Description>Memory Size</rasd:Description>
        <rasd:ElementName>4096MB of memory</rasd:ElementName>
        <rasd:InstanceID>2</rasd:InstanceID>
        <rasd:ResourceType>4</rasd:ResourceType>
        <rasd:VirtualQuantity>4096</rasd:VirtualQuantity>
<Item>
        <rasd:AllocationUnits>byte * 2^20</rasd:AllocationUnits>
        <rasd:Description>Memory Size</rasd:Description>
        <rasd:ElementName>5120MB of memory</rasd:ElementName>
        <rasd:InstanceID>2</rasd:InstanceID>
        <rasd:ResourceType>5</rasd:ResourceType>
        <rasd:VirtualQuantity>5120</rasd:VirtualQuantity>
```

STEP 3 | Change the number of virtual CPU cores allotted from 2 to 4 or 8 as desired for your deployment:

```
<Item>
        <rasd:AllocationUnits>hertz * 10^6</rasd:AllocationUnits>
```

```
        <rasd:Description>Number of Virtual CPUs</rasd:Description>
        <rasd:ElementName>2 virtual CPU(s)</rasd:ElementName>
        <rasd:InstanceID>1</rasd:InstanceID>
        <rasd:ResourceType>3</rasd:ResourceType>
        <rasd:VirtualQuantity>2</rasd:VirtualQuantity>
        <vmw:CoresPerSocket ova:required="false">2</vmw:CoresPerSocket>
      </Item>
<Item>
        <rasd:AllocationUnits>hertz * 10^6</rasd:AllocationUnits>
        <rasd:Description>Number of Virtual CPUs</rasd:Description>
        <rasd:ElementName>4 virtual CPU(s)</rasd:ElementName>
        <rasd:InstanceID>1</rasd:InstanceID>
        <rasd:ResourceType>3</rasd:ResourceType>
        <rasd:VirtualQuantity>4</rasd:VirtualQuantity>
        <vmw:CoresPerSocket ova:required="false">2</vmw:CoresPerSocket>
      </Item>
```

Alternatively, you can deploy the firewall and before you power on the VM-Series firewall, edit the memory and virtual CPU allocation directly on the ESXi host or the vCenter server.

Licensing Issues

- Why am I unable to apply the support or feature license?
- Why does my cloned VM-Series firewall not have a valid license?
- Will moving the VM-Series firewall cause license invalidation?

Why am I unable to apply the support or feature license?

Have you applied the capacity auth-code on the VM-Series firewall? Before you can activate the support or feature license, you must apply the capacity auth-code so that the device can obtain a serial number. This serial number is required to activate the other licenses on the VM-Series firewall.

Why does my cloned VM-Series firewall not have a valid license?

VMware assigns a unique UUID to each virtual machine including the VM-Series firewall.So, when a VM-Series firewall is cloned, a new UUID is assigned to it. Because the serial number and license for each instance of the VM-Series firewall is tied to the UUID, cloning a licensed VM-Series firewall will result in a new firewall with an invalid license. You will need a new auth-code to activate the license on the newly deployed firewall. You must apply the capacity auth-code and a new support license in order to obtain full functionality, support, and software upgrades on the VM-Series firewall.

Will moving the VM-Series firewall cause license invalidation?

If you are manually moving the VM-Series firewall from one host to another, be sure to select the option, **This guest was moved** to prevent license invalidation.

Connectivity Issues

- Why is the VM-Series firewall not receiving any network traffic?

Why is the VM-Series firewall not receiving any network traffic?

On the VM-Series firewall. check the traffic logs (**Monitor** > **Logs**). If the logs are empty, use the following CLI command to view the packets on the interfaces of the VM-Series firewall:

```
show counter global filter delta yes
```

```
Global counters:
Elapsed time since last sampling: 594.544 seconds
-------------------------------------------------------------------------------
Total counters shown: 0
-------------------------------------------------------------------------------
```

In the vSphere environment, check for the following issues:

- Check the port groups and confirm that the firewall and the virtual machine(s) are on the correct port group

  Make sure that the interfaces are mapped correctly.

  Network adapter 1 = management

  Network adapter 2= Ethernet1/1

  Network adapter 3 = Ethernet1/2

  For each virtual machine, check the settings to verify the interface is mapped to the correct port group.
- Verify that either promiscuous mode is enabled for each port group or for the entire switch or that you have configured the firewall to Hypervisor Assigned MAC Addresses.

  Since the dataplane PAN-OS MAC addresses are different than the VMNIC MAC addresses assigned by vSphere, the port group (or the entire vSwitch) must be in promiscuous mode if not enabled to use the hypervisor assigned MAC address:

  - Check the VLAN settings on vSphere.

    The use of the VLAN setting for the vSphere port group serves two purposes: It determines which port groups share a layer 2 domain, and it determines whether the uplink ports are tagged (802.1Q).
  - Check the physical switch port settings

    If a VLAN ID is specified on a port group with uplink ports, then vSphere will use 802.1Q to tag outbound frames. The tag must match the configuration on the physical switch or the traffic will not pass.

    Check the port statistics if using virtual distributed switches (vDS); Standard switches do not provide any port statistics

Performance Tuning of the VM-Series for ESXi

The VM-Series firewall for ESXi is a high-performance appliance but may require tuning of the hypervisor to achieve the best results. This section describes some best practices and recommendations for facilitating the best performance of the VM-Series firewall. For the best performance, ESXi 6.0.0.0 or later is recommended.

- Install the NIC Driver on ESXi
- Enable DPDK on ESXi
- Enable SR-IOV on ESXi
- Enable Multi-Queue Support for NICs on ESXi

Install the NIC Driver on ESXi

For the best performance, use SR-IOV with Intel 10GB network interfaces which requires the ixgbe 4.4.1 driver to support multiple queues for each interface.

STEP 1 | Obtain a list of network interfaces on the ESXi host.

1. Log in to the ESXi host CLI.
2. Use the following command to return a list of network interfaces:

```
$ esxcli network nic list
```

STEP 2 | Determine the driver version for a particular interface.

You can use either **ethtool** or **esxcli** to determine the currently-installed driver version. The following example uses vmnic4 and returns driver version 3.21.6.

- ethtool:

```
$ ethtool -l <nic-name>
$ ethtool -I vmnic4
driver: ixgbe
version: 3.21.6iov
firmware-version: 0x80000389
bus-info: 0000:04:00.0
```

- esxcli:

```
$ esxcli network nic get -n <nic-name>
$ esxcli network nic get -n vmnic4
   Advertised Auto Negotiation: true
   Advertised Link Modes:
   Auto Negotiation: true
   Cable Type:
   Current Message Level: 7
   Driver Info:
         Bus Info: 0000:04:00.0
         Driver: ixgbe
         Firmware Version: 0x80000389
         Version: 3.21.6iov
   Link Detected: false
   Link Status: Down
   Name: vmnic4
   PHYAddress: 0
```

```
   Pause Autonegotiate: true
   Pause RX: true
   Pause TX: true
   Supported Ports: FIBRE
   Supports Auto Negotiation: true
   Supports Pause: true
   Supports Wakeon: false
   Transceiver: external
   Wakeon: None
```

STEP 3 | Install the new driver.

1. Download the 4.4.1 driver from the VMware website.
2. Copy the file to the ESXi host datastore.
3. Enable maintenance mode on the ESXi host.
4. Use one of the following commands to install the new driver.
   - `$ esxcli software vib install -d <path to driver .zip file>`
   - `$ esxcli software vib install -v <path to driver .vib file>`

Enable DPDK on ESXi

Data Plane Development Kit (DPDK) enhances VM-Series performance by increasing network interface card (NIC) packet processing speed. On the VM-Series firewall, DPDK is enabled by default on ESXi. If you disable DPDK, the NIC uses packet mmap instead of DPDK. To take advantage of DPDK, you must use a NIC with one of the following drivers:

All data interfaces must be using the same driver to support DPDK.

Supported Drivers	
Virtual Driver	VMXNET3
Intel Driver	ixgbe, ixgbevf, i40e, i40evf

You can disable DPDK using the command **`set system setting dpdk-pkt-io off`**.

Enable SR-IOV on ESXi

Single root I/O virtualization (SR-IOV) allows a single PCIe physical device under a single root port to appear to be multiple separate physical devices to the hypervisor or guest. Enable SR-IOV by enabling virtual function devices on the SR-IOV NIC and the modify the guest settings in vCenter.

SR-IOV on the VM-Series for ESXi requires one of the following Intel NIC drivers.

Driver Filename	Version
ixgbe/ixgbe.ko	4.2.0.4.1

Driver Filename	Version
ixgbevf/ixgbevf.ko	2.14.2
i40e/i40e.ko	1.3.49
i49evf/i40evf.ko	1.2.25

Complete the following procedure to enable SR-IOV.

STEP 1 | Enable virtual function devices on the SR-IOV NIC.

1. Log in to the ESXi host CLI.
2. Use the following command:

```
$ esxcli system module parameters set -m <nic_driver> -p “max_vfs=<n>”
```

For example, for ixgbe, you can specify:

```
$ esxcli system module parameters set -m ixgbe -p "max_vfs=8"
```

Max VFs (max_vfs) is a comma-separated list, where each number corresponds to a separate port/NIC. If you have multi-port NIC or multiple NICs using the same driver, you must specify multiple max_vfs values, one for each port/NIC.

STEP 2 | Modify the guest settings in vCenter.

1. Log in to vCenter and select your VM-Series firewall guest machine.
2. Select **Manage** > **Settings** > **VM Hardware** and **Edit** the hardware settings.
3. Select **Virtual Hardware**.
4. Choose **PCI Device** from the **New device** drop-down and click **Add**.
5. Edit the settings of the added PCI device, select the PCI ID corresponding to an available virtual function device.

STEP 3 | Reboot the ESXi host for your changes to take effect.

Enable Multi-Queue Support for NICs on ESXi

Multi-queue allows network performance to scale with the number of vCPUs and allows for parallel packet processing by creating multiple TX and RX queues. Modify the .vmx file or access Advanced Settings to enable multi-queue.

STEP 1 | Enable multi-queue.

1. Open the .vmx file.
2. Add the following parameter:

```
ethernetX.pnicFeatures = “4”
```

STEP 2 | Enable receive-side scaling (RSS).

1. Log in to the CLI on the ESXi host.
2. Execute the following command:

```
$ vmkload_mod -u ixgbe
$ vmkload_mod ixgbe RSS="4,4,4,4,4,4"
```

STEP 3 | For the best performance, allocate additional CPU threads per ethernet/vSwitch device. This is limited by the amount of spare CPU resources available on the ESXi host.

1. Open the .vmx file.
2. Add the following parameter:

```
ethernetX.ctxPerDev = "1"
```

Set Up the VM-Series Firewall on vCloud Air

The VM-Series firewall can be deployed in a virtual data center (vDC) on vCloud Air using the vCloud Air portal, from the vCloud Director portal or using the vCloud Air API.

About the VM-Series Firewall on vCloud Air

You can deploy the VM-Series firewall in a virtual data center (vDC) on VMware vCloud Air using the vCloud Air portal or from the vCloud Director portal. And to centrally manage all your physical and VM-Series firewalls, you can use an existing Panorama or deploy a new Panorama on premise or on vCloud Air.

The VM-Series firewall on vCloud Air requires the following:

- ESXi version of the software image, an Open Virtualization Alliance (OVA) file, from the Palo Alto Networks Customer Support web site. Currently, the vCloud Air Marketplace does not host the software image.

  In order to efficiently deploy the VM-Series firewall, include the firewall software image in a vApp. A vApp is a container for preconfigured virtual appliances (virtual machines and operating system images) that is managed as a single object. For example, if your vApp includes a set of multi-tiered applications and the VM-Series firewall, each time you deploy the vApp, the VM-Series firewall automatically secures the web server and database server that get deployed with the vApp.
- License and subscriptions purchased from a partner, reseller, or directly from Palo Alto Networks, in the Bring Your Own License (BYOL) model; the usage-based licensing for the VM-Series on vCloud Air is not available.
- Due to the security restrictions imposed on vCloud Air, the VM-Series firewall on vCloud Air is best deployed with Layer 3 interfaces and the interfaces must be enabled to use the hypervisor assigned MAC address. If you do not enable hypervisor assigned MAC address, the VMware vSwitch cannot forward traffic to the dataplane interfaces on the VM-Series firewall because the vSwitch on vCloud Air does not support promiscuous mode or MAC forged transmits. The VM-Series firewall cannot be deployed with tap interfaces, Layer 2 interfaces, or virtual wire interfaces.

The VM-Series firewall on vCloud Air can be deployed in an active/passive high availability configuration. However, the VM-Series firewall on vCloud Air does not support VM Monitoring capabilities for virtual machines that are hosted on vCloud Air.

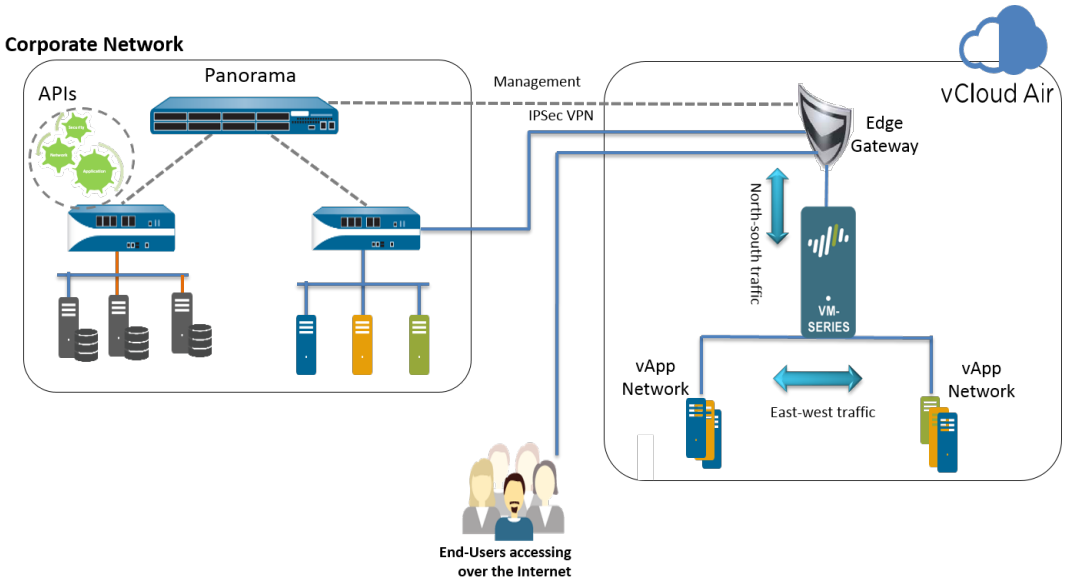
To learn all about vCloud Air, refer to the VMware vCloud Air documentation.

Deployments Supported on vCloud Air

To enable applications safely, block known and unknown threats, and to keep pace with changes in your environment, you can deploy the VM-Series firewall on vCloud Air with Layer 3 interfaces in the following ways:

- **Secure the virtual data center perimeter**—Deploy the VM-Series firewall as a virtual machine that connects isolated and routed networks on vCloud Air. In this deployment the firewall secures all north-south traffic traversing the infrastructure on vCloud Air.
- **Set up a hybrid cloud**—Extend your data center and private cloud into vCloud Air and use a VPN connection to enable communication between the corporate network and the data center. In this deployment, the VM-Series firewall uses IPSec to encrypt traffic and secure users accessing the cloud.
- **Secure traffic between application subnets in the vDC**—To improve security, segment your network and isolate traffic by creating application tiers, and then deploy the VM-Series firewall to protect against lateral threats between subnets and application tiers.

The following illustration combines all three deployments scenarios and includes Panorama. Panorama streamlines policy updates, centralizes policy management, and provides centralized logging and reporting.



Deploy the VM-Series Firewall on vCloud Air

Use the instructions in this section to deploy your VM-Series firewall in an on-demand or dedicated vDC on vCloud Air. This procedure assumes that you have set up your vDC, including the gateways required to allow traffic in and out of the vDC, and the networks required for routing management traffic and data traffic through the vDC.

STEP 1 | Obtain the VM-Series OVA image from the Palo Alto Networks Customer Support web site; the vCloud Air Marketplace does not host the software image currently.

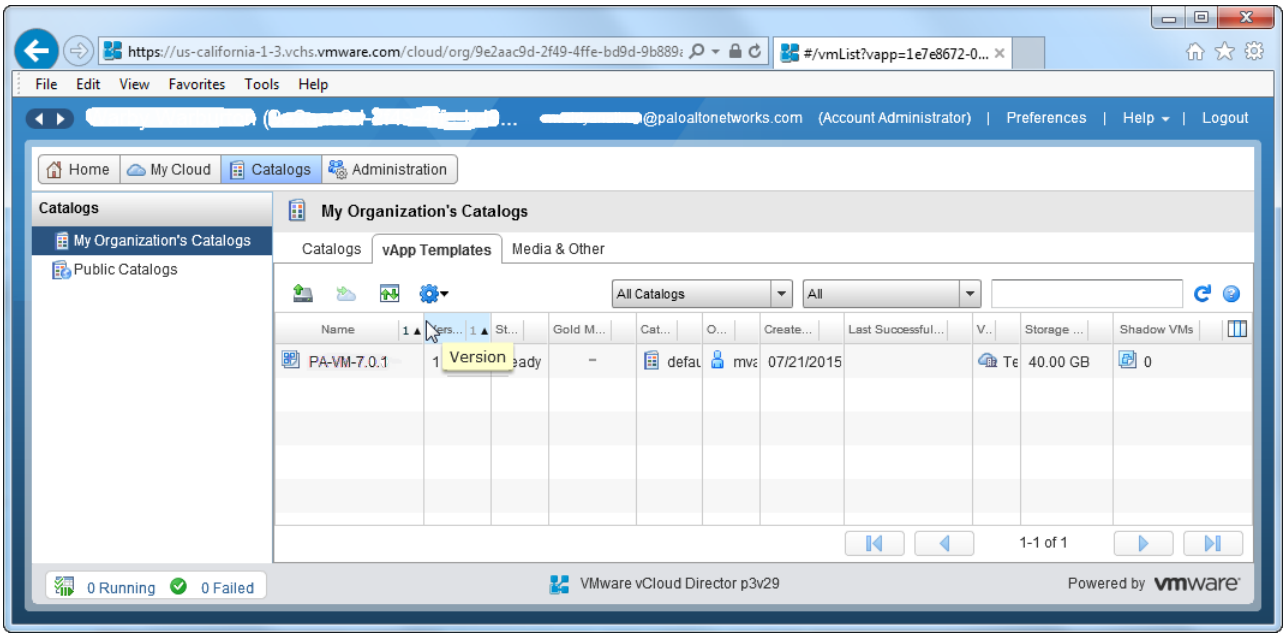
1. Go to: www.paloaltonetworks.com/services/support.html.
2. Filter by **PAN-OS for VM-Series Base Images** and download the OVA image. For example, PA-VM-ESX-8.0.0.ova.

STEP 2 | Extract the Open Virtualization Format (OVF) file from the OVA image and import the OVF file in to your vCloud Air catalog.

When extracting files from the OVA image, make sure to place all the files—.mf, .ovf, and .vmdk—within the same directory.

For instructions to extract the OVF file from the OVA image, refer to the VMware documentation: https://www.vmware.com/support/developer/ovf/#sthash.WUp55ZyE.dpuf

When you import the OVF file, the software image for the VM-Series firewall is listed in **My Organization's Catalogs**.



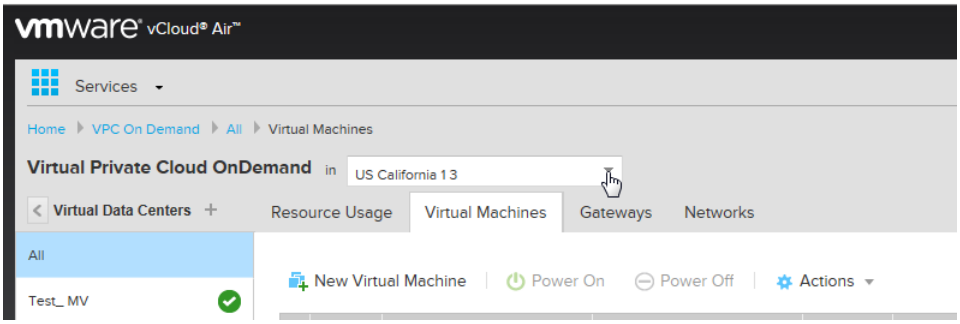
STEP 3 | Choose your workflow.

A vApp is a collection of templates for preconfigured virtual appliances that contain virtual machines, and operating system images.

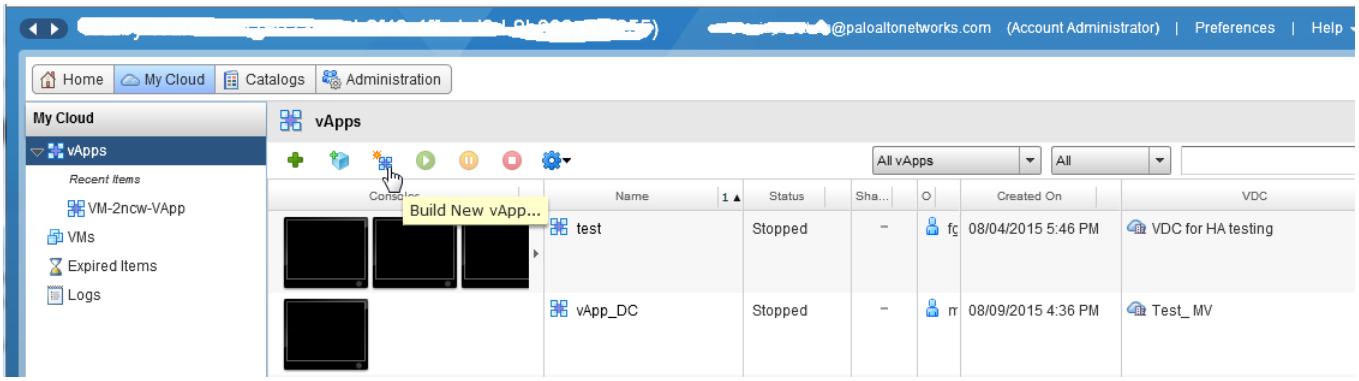
- If you want to create a new vDC and a new vApp that includes the VM-Series firewall, go to step 4.
- If you have already deployed a vDC and have a vApp and now want to add the VM-Series firewall to the vApp to secure traffic, go to step 5.

STEP 4 | Create a vDC and a vApp that includes the VM-Series firewall.

1. Log in to vCloud Air.
2. Select **VPC OnDemand** and select the location in which you want to deploy the VM-Series firewall.



3. Select **Virtual Data Centers** and click **+** to add a new Virtual Data Center.
4. Select the vDC, right click and select **Manage Catalogs in vCloud Director**. You will be redirected to the vCloud Director web interface.
5. Create a new vApp that contains one or more virtual machines including the VM-Series firewall:
    1. Select **My Cloud** > **vApps**, and click **Build New vApp**.



    2. Select **Name and Location**, and the **Virtual Datacenter** in which this vApp will run. By default, **Leases** for runtime and storage never expire and the vApp is not automatically stopped.
    3. **Add Virtual Machines**. To add the VM-Series firewall image from the **Look in:** drop-down, select **My Organization's Catalog**, select the image and click **Add**. Click **Next**
    4. Configure **Resources** to specify the Storage Policies for the virtual machines when deployed. The VM-Series firewall uses the **Standard** option.
    5. Configure the **Virtual Machines**. Name each virtual machine and select the network to which you want it to connect. You must connect NIC 0 (for management access) to the default routed network; NIC 1 is used for data traffic. You can add additional NICs later.
    6. Verify the settings and click **Finish.**
    7. Continue to step 6.

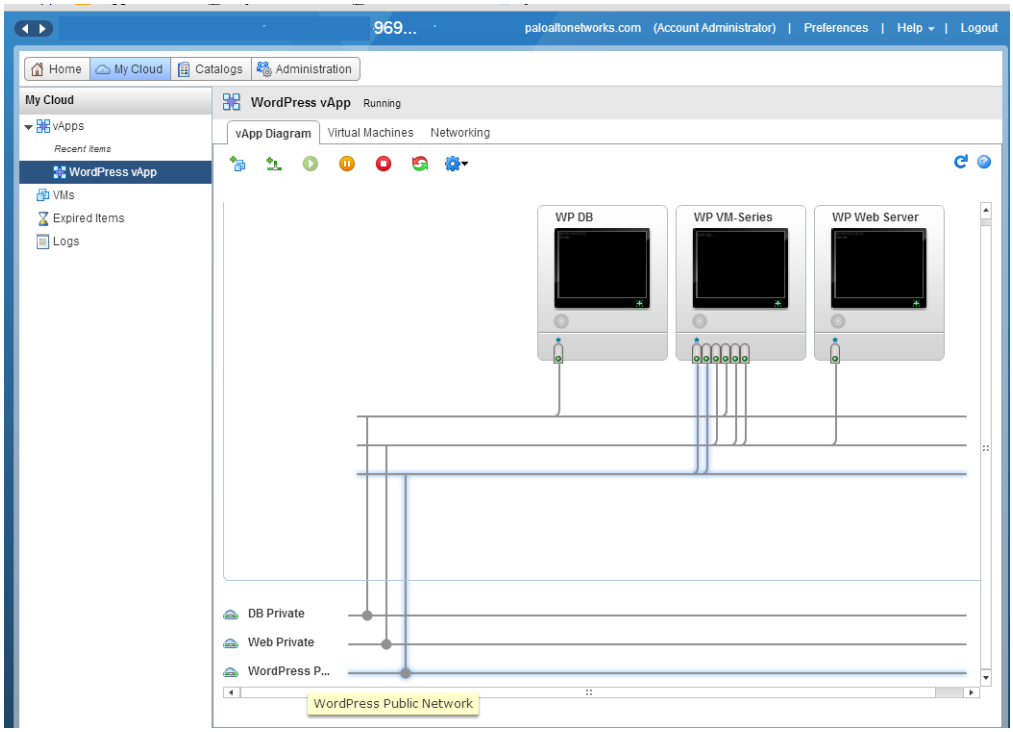
STEP 5 | Add the VM-Series Firewall into a vApp.

1. Log in to vCloud Air.
2. Select your existing **Virtual Data Center** from the left pane, right click and select **Manage Catalogs in vCloud Director**. You will be redirected to the vCloud Director web interface.
3. Select **My Cloud** > **vApps** and click the **Name** of the vApp in which to include the VM-Series firewall.
4. Open the vApp (double-click on the name), select **Virtual Machines** and click + to add a virtual machine.
    1. In the **Look in:** drop-down, choose **My Organization's Catalog**, select the VM-Series firewall image and click **Add**. Click **Next**.

2. Click **Next to** skip **Configure Resources**. The VM-Series firewall uses the **Standard** option and you do not to modify the Storage Policy.
3. Enter a **Name** for the firewall and for management access **(NIC 0)**, select the default routed network and the **IP Mode**— Static or DHCP. You can configure NIC 1 and add additional NICs in step 6. Click **Next**.
4. Verify how this vApp connects to the vDC— Gateway Address and Network Mask for the virtual machines in this vApp.
5. Verify that you have added the VM-Series firewall and click **Finish.**
6. Continue to step 6.

STEP 6 | Connect the data interface(s) of the VM-Series firewall to an isolated or a routed network, as required for your deployment.

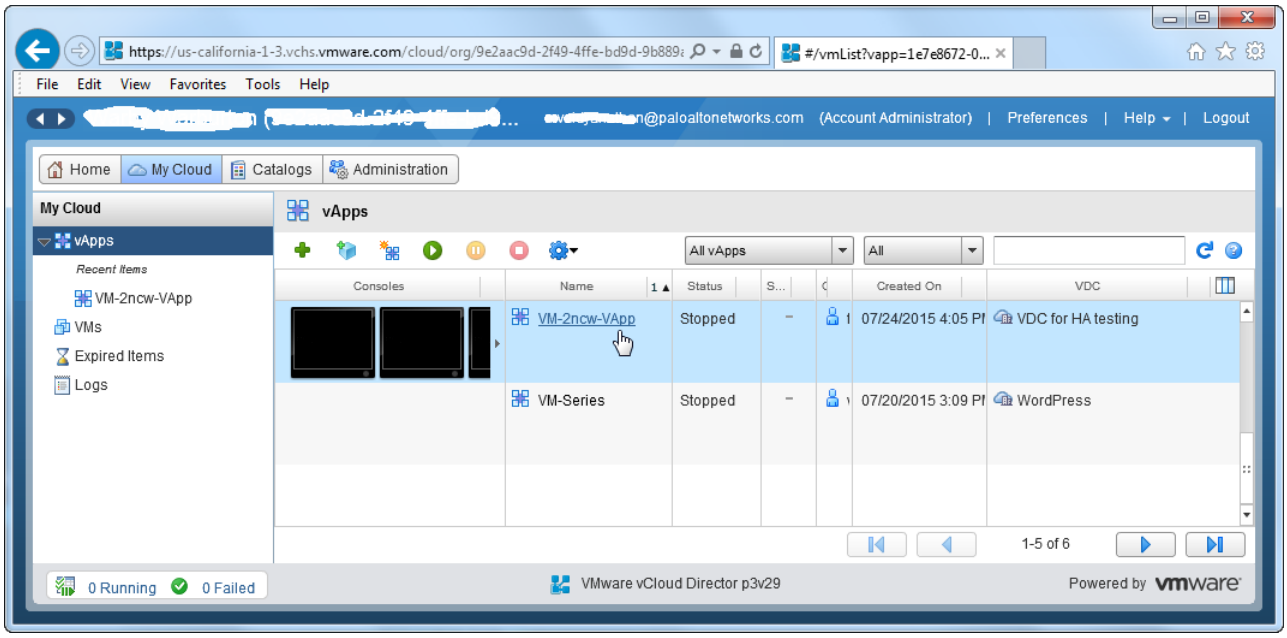
1. In vCloud Director, select **My Cloud** > **vApps** and select the vApp you just created or edited.
2. Select **Virtual Machines** and select the VM-Series firewall. Then, right-click and select **Properties**.
3. Select **Hardware**, scroll to the NICs section and select **NIC 1**.
4. Attach the dataplane network interface to a vApp network or an organizational VDC network based on your connectivity needs for data traffic to the VM-Series firewall. To create a new network:
    1. In the Network drop-down, click **Add Network**.
    2. Select the **Network Type** and give it a name and click **OK**.
    3. Verify that the new network is attached to the interface.
5. To add additional NICs to the firewall, click **Add** and repeat step 4 above. You can attach a maximum of seven dataplane interfaces to the VM-Series firewall.
6. Verify that the management interface of the VM-Series firewall is attached to the default routed subnet on the vDC and at least one dataplane interface is connected to a routed or isolated network.
    1. Select **My Cloud** > **vApps** and double-click the **Name** of the vApp you just edited.
    2. Verify network connectivity in the **vApp Diagram**.



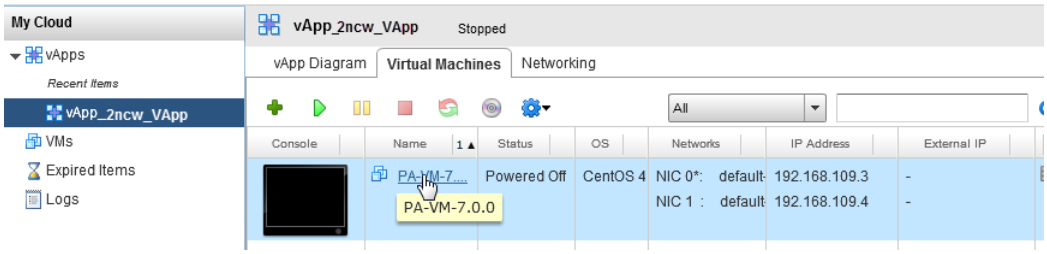
STEP 7 | (Optional) Edit the hardware resources allocated for the VM-Series firewall.

Required only if you need to allot additional CPU, memory, or hard disk to the firewall.

1. Select **My Cloud** > **vApps** and double-click the **Name** of the vApp you just deployed.



2. Select **Virtual Machine** and click on the **Name** of the VM-Series firewall to access the Virtual Machine Properties.



3. Add additional **Hardware** resources for the VM-Series firewall:
   - See VM-Series System Requirements for the minimum vCPU, memory, and disk requirements for your VM-Series model.
   - NICs: One management and up to seven dataplane interfaces.

STEP 8 | Power on the VM-Series firewall.

STEP 9 | Configure an IP address for the VM-Series firewall management interface.

Perform Initial Configuration on the VM-Series on ESXi.

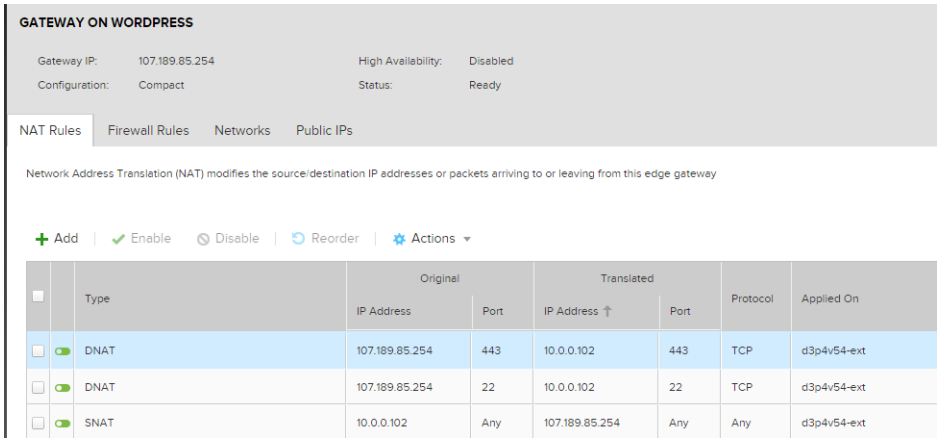
The VM-Series firewall on vCloud Air supports VMware Tools, and you can Use VMware Tools on the VM-Series Firewall on ESXi and vCloud Air to view the management IP address of the VM-Series firewall.

STEP 10 | Define NAT rules on the vCloud Air Edge Gateway to enable Internet access for the VM-Series firewall.

1. Select **Virtual Data Centers** > **Gateways**, select the gateway and double-click to add **NAT Rules**.
2. Create two DNAT rules. One for allowing SSH access and one for HTTPS access to the management port's IP address on the VM-Series firewall.

3. Create a SNAT rule for translating the internal source IP address for all traffic initiated from the management port on the VM-Series firewall to an external IP address.

   To send and receive traffic from the dataplane interfaces on the firewall, you must create additional DNAT and SNAT rules on the vCloud Air Edge Gateway.



STEP 11 | Log in to the web interface of the firewall.

In this example, the URL for the web interface is https://107.189.85.254

The NAT rule on the Edge Gateway translates the external IP address and port 107.189.85.254:443 to the private IP address and port 10.0.0.102:443.

STEP 12 | Add the auth code(s) to activate the licenses on the firewall.

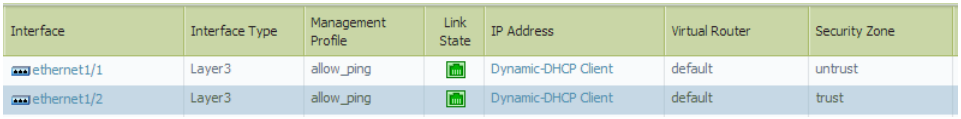
Activate the License.

STEP 13 | Configure the VM-Series firewall to use the hypervisor assigned MAC address.

Hypervisor Assigned MAC Addresses

STEP 14 | Configure the dataplane interfaces as Layer 3 interfaces.

1. Select **Network** > **Interfaces** > **Ethernet**.
2. Click the link for **ethernet 1/1** and configure as follows:
   - **Interface Type: Layer3**
   - Select the **Config** tab, assign the interface to the default router.
   - On the **Config** tab, select **New Zone** from the **Security Zone** drop-down. Define a new zone, for example untrust, and then click **OK**.
   - Select **IPv4**, assign a static IP address.
   - On **Advanced** > **Other Info**, expand the **Management Profile** drop-down, and select **New Management Profile**.
   - Enter a **Name** for the profile, such as allow_ping, and select Ping from the Permitted Services list, then click **OK**.
   - To save the interface configuration, click **OK**.
3. Repeat the process for each additional interface.
4. Click **Commit** to save the changes.



Set Up a VM-Series Firewall on the Citrix SDX Server

To reduce your carbon footprint and consolidate key functions on a single server, you can deploy one or more instances of the VM-Series firewall on the Citrix SDX server. Deploying the VM-Series firewall in conjunction with the NetScaler VPX secures application delivery along with network security, availability, performance, and visibility.

About the VM-Series Firewall on the SDX Server

One or more instances of the VM-Series firewall can be deployed to secure east-west and/or north-south traffic on the network; virtual wire interfaces, Layer 2 interfaces, and Layer 3 interfaces are supported. To deploy the firewall, see Install the VM-Series Firewall on the SDX Server.

Once deployed the VM-Series firewall works harmoniously with the NetScaler VPX (if needed), which is a virtual NetScaler appliance deployed on the SDX server. The NetScaler VPX provides load balancing and traffic management functionality and is typically deployed in front of a server farm to facilitate efficient access to the servers. For a complete overview of NetScaler feature/functionality, refer to http://www.citrix.com/netscaler. When the VM-Series is paired to work with the NetScaler VPX, the complementary capabilities enhance your traffic management, load balancing, and application/network security needs.

This document assumes that you are familiar with the networking and configuration on the NetScaler VPX. In order to provide context for the terms used in this section, here is a brief refresher on the NetScaler owned IP addresses that are referred to in this document:

- NetScaler IP address (NSIP): The NSIP is the IP address for management and general system access to the NetScaler itself, and for HA communication.
- Mapped IP address (MIP): A MIP is used for server-side connections. It is not the IP address of the NetScaler. In most cases, when the NetScaler receives a packet, it replaces the source IP address with a MIP before sending the packet to the server. With the servers abstracted from the clients, the NetScaler manages connections more efficiently.
- Virtual server IP address (VIP): A VIP is the IP address associated with a vserver. It is the public IP address to which clients connect. A NetScaler managing a wide range of traffic may have many VIPs configured.
- Subnet IP address (SNIP): When the NetScaler is attached to multiple subnets, SNIPs can be configured for use as MIPs providing access to those subnets. SNIPs may be bound to specific VLANs and interfaces.

For examples on deploying the VM-Series firewall and the NetScaler VPX together, see Supported Deployments—VM Series Firewall on Citrix SDX .

VM-Series on SDX System Requirements and Limitations

This section lists requirements and limitations for the VM-Series firewall on the Citrix SDX server.

- VM-Series on SDX System Requirements
- VM-Series on SDX System Limitations

VM-Series on SDX System Requirements

You can deploy multiple instances of the VM-Series firewall on the Citrix SDX server. Because each instance of the firewall requires a minimum resource allocation—number of CPUs, memory and disk space—on the SDX server, make sure to conform to the specifications below to ensure optimal performance.

Requirement	Details
SDX platforms	• 11500, 11515, 11520, 11530, 11540, 11542 • 13500, 14500, 16500, 18500, 20500 • 22040, 22060, 22080, 22100, 22120 • 24100, 24150 • 17550, 19550, 20550, 21550
SDX version	10.1+ 10.1 is not supported; a software version higher than 10.1. is required.
Citrix XenServer version	6.0.2 or later
Minimum System Resources  *Plan and allocate the total number of data interfaces that you might require on the VM-Series firewall. This task is essential during initial deployment, because adding or removing interfaces to the VM-Series firewall after initial deployment will cause the data interfaces (Eth 1/1 and Eth 1/2) on the VM-Series firewall to re-map to the adapters on the SDX server. Each data interface sequentially maps to the adapter with the lowest numerical value, and this remapping*	• The host CPU must be a x86-based Intel or AMD CPU with virtualization extension. • Two network interfaces: one dedicated for management traffic and one for data traffic. For management traffic, you can use the 0/x interfaces on the management plane or the 10/x interfaces on the dataplane. Assign additional network interfaces for data traffic, as required for your network topology. • See VM-Series System Requirements for the minimum hardware requirements for your VM-Series model.

Requirement	Details
can cause a configuration mismatch on the firewall.	

VM-Series on SDX System Limitations

The VM-Series firewall deployed on the Citrix SDX server has the following limitations:

- Up to 24 total ports can be configured. One port will be used for management traffic and up to 23 can be used for data traffic.
- Link aggregation is not supported.

For the supported deployments, see Supported Deployments—VM Series Firewall on Citrix SDX .

To deploy the firewall, see Install the VM-Series Firewall on the SDX Server.

Supported Deployments—VM Series Firewall on Citrix SDX

In the following scenarios, the VM-Series firewall secures traffic destined to the servers on the network. It works in conjunction with the NetScaler VPX to manage traffic before or after it reaches the NetScaler VPX.

- Scenario 1—Secure North-South Traffic
- Scenario 2—Secure East-West Traffic (VM-Series Firewall on Citrix SDX)

Scenario 1—Secure North-South Traffic

To secure north-south traffic using a VM-Series firewall on an SDX server, you have the following options:

- VM-Series Firewall with L3 Interfaces Between the NetScaler VPX and the Servers
- VM-Series Firewall with L2 or Virtual Wire Interfaces Between the NetScaler VPX and the Servers
- VM-Series Firewall Before the NetScaler VPX

VM-Series Firewall with L3 Interfaces Between the NetScaler VPX and the Servers

Deploying the firewall with L3 interfaces between the NetScaler VPX and the servers allows you to scale more easily as you deploy new servers and new subnets. You can deploy multiple instances of the firewall to manage traffic to each new subnet and then configure the firewalls as a high availability pair, if needed.

Using an L3 interface allows you make minimal changes to the SDX server/network configuration because the SNIP to reach the servers is removed from the NetScaler VPX and is configured on the VM-Series firewall. With this approach, only one data interface is used on the VM-Series firewall, hence only one zone can be defined. As a result, when defining the policy rules you must specify the source and destination IP address/subnets across which to enforce security rules. For details, see Deploy the VM-Series Firewall Using L3 Interfaces.

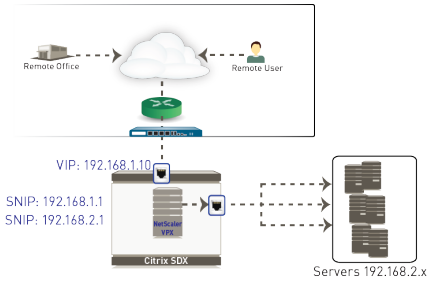


Figure 1: Topology After Adding the VM-Series Firewall with L3 Interfaces

In this example, the public IP address that the clients connect to (VIP on the NetScaler VPX), is 192.168.1.10. For providing access to the servers on subnet 192.168.2.x, the configuration on the VPX references the subnets (SNIP) 192.168.1.1 and 192.168.2.1. Based on your network configuration and default routes, the routing on servers might need to be changed.

When you set up the VM-Series firewall, you must add a data interface (for example eth1/1), and assign two IP addresses to the interface. One IP address must be on the same subnet as the VIP and the other must be on the same subnet as the servers. In this example, the IP addresses assigned to the data interfaces are 192.168.1.2 and 192.168.2.1. Because only one data interface is used on the VM-Series firewall, all traffic belongs to a single zone, and all intra zone traffic is implicitly allowed in policy. Therefore, when

defining the policy rules you must specify the source and destination IP address/subnets across which to enforce security rules.

Even after you add the VM-Series firewall on the SDX server, the IP address that the clients continue to connect to is the VIP of the NetScaler VPX (192.168.1.10). However, to route all traffic through the firewall, on the NetScaler VPX you must define a route to the subnet 192.168.2.x. In this example, to access the servers this route must reference the IP address 192.168.1.2 assigned to the data interface on the VM-Series firewall. Now all traffic destined for the servers is routed from the NetScaler VPX to the firewall and then on to the servers. The return traffic uses the interface 192.168.2.1 on the VM-Series and uses the SNIP 192.168.1.1 as its next hop.

For security compliance, if USIP (Use client Source IP) is enabled on the NetScaler VPX, then the VM-Series firewall requires a default route that points to the SNIP 192.168.1.1, in this example. If a default NAT (mapped/SNIP) IP address is used, then you do not need to define a default route on the VM-Series firewall.

For instructions, see Deploy the VM-Series Firewall Using L3 Interfaces.

VM-Series Firewall with L2 or Virtual Wire Interfaces Between the NetScaler VPX and the Servers

Deploying the VM-Series firewall using L2 interfaces or virtual wire interfaces between the NetScaler VPX and the servers requires reconfiguration on the NetScaler VPX to remove direct connection to the servers. The VM-Series firewall can then be cabled and configured to transparently intercept and enforce policy on traffic destined to the servers. In this approach two data interfaces are created on the firewall and each belongs to a distinct zone. The security policy is defined to allow traffic between the source and destination zones. For details, see Deploy the VM-Series Firewall Using Layer 2 (L2) or Virtual Wire Interfaces.

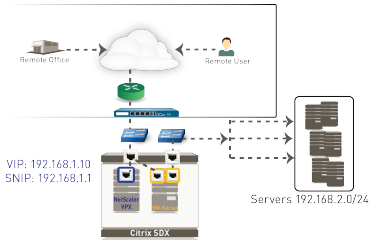
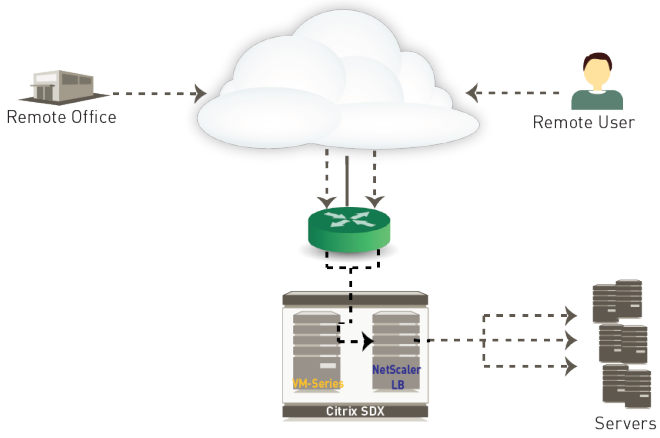


Figure 2: Topology After Adding the VM-Series Firewall with L2 or Virtual Wire Interfaces

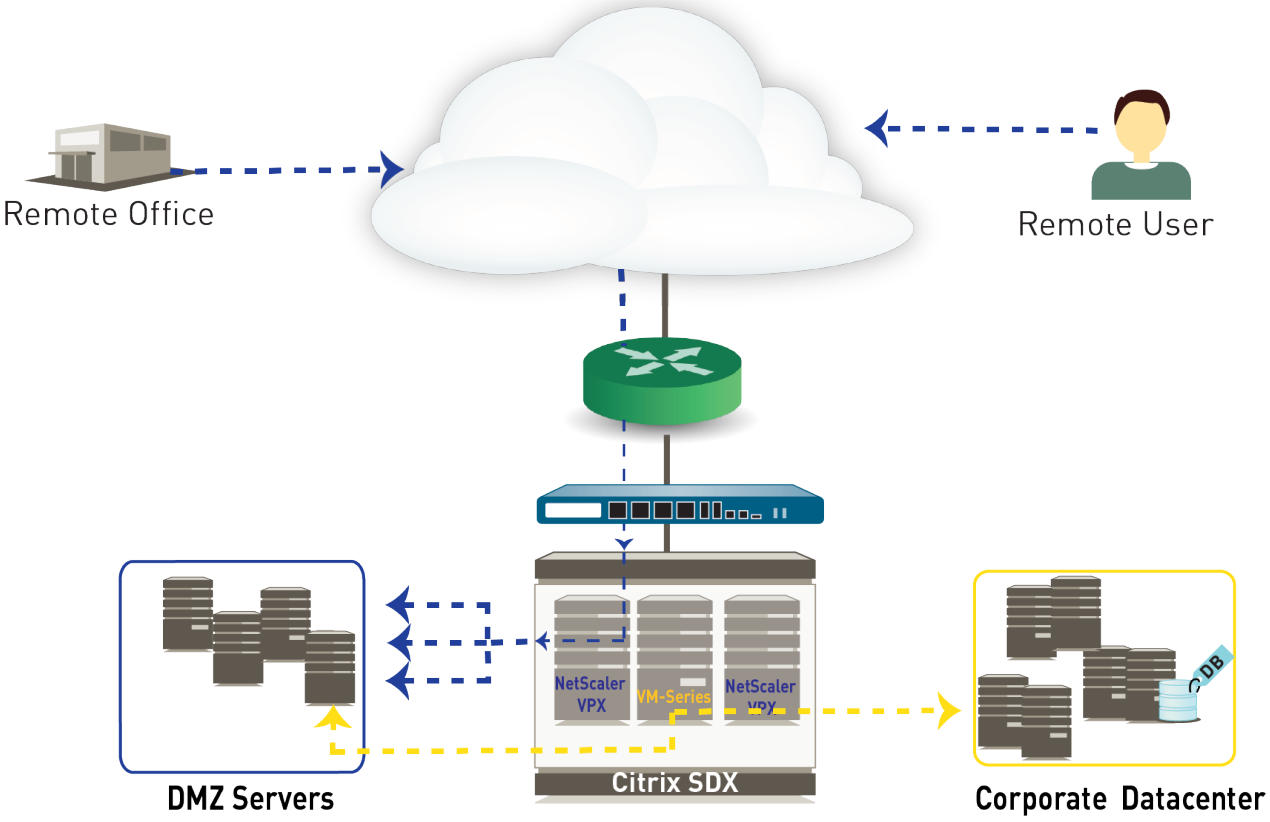
VM-Series Firewall Before the NetScaler VPX

In this scenario, the perimeter firewall is replaced with the VM-Series firewall that can be deployed using L3, L2, or virtual wire interfaces. All traffic on your network is secured by the VM-Series firewall before the request reaches the NetScaler VPX and is forwarded to the servers. For details, see Deploy the VM-Series Firewall Before the NetScaler VPX.



Scenario 2—Secure East-West Traffic (VM-Series Firewall on Citrix SDX)

The VM-Series firewall is deployed along with two NetScaler VPX systems that service different server segments on your network or operate as termination points for SSL tunnels. In this scenario, the perimeter firewall secures incoming traffic. Then, the traffic destined to the DMZ servers flows to a NetScaler VPX that load balances the request. To add an extra layer of security to the internal network, all east-west traffic between the DMZ and the corporate network are routed through the VM-Series firewall. The firewall can enforce network security and validate access for that traffic. For details, see Secure East-West Traffic with the VM-Series Firewall.



Install the VM-Series Firewall on the SDX Server

A support account and a valid VM-Series license are required to obtain the .xva base image file that is required to install the VM-Series firewall on the SDX server. If you have not already registered the capacity auth-code that you received with the order fulfillment email, with your support account, see Register the VM-Series Firewall. After registration is completed, continue to the following tasks:

- Upload the Image to the SDX Server
- Provision the VM-Series Firewall on the SDX Server

Upload the Image to the SDX Server

To provision the VM-Series firewall, you need to obtain the .xva image file and upload it to the SDX server.

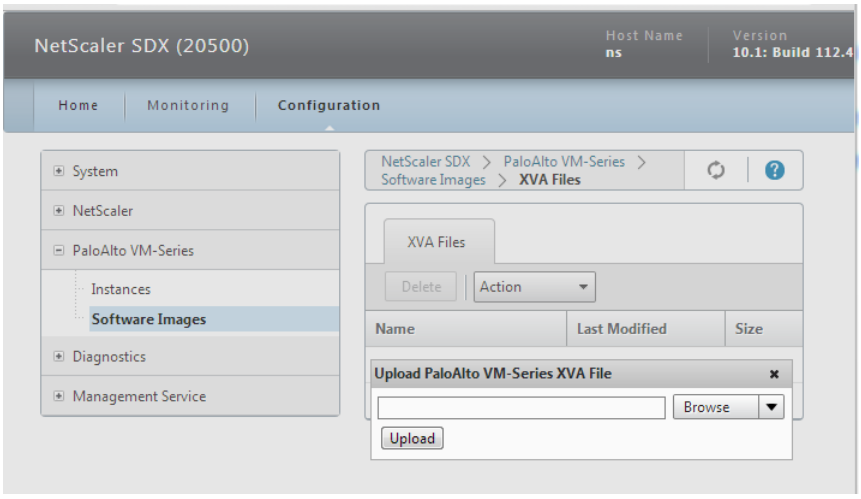
STEP 1 | Download and extract the base image zip file to a local computer.

1. Go to https://support.paloaltonetworks.com/ and download the **VM-Series Citrix SDX Base Image** zip file.
2. Unzip the base image zip file, and extract the **.xva** file.

   This .xva file is required for installing the VM-Series firewall.

STEP 2 | Upload the image from the local computer onto the Citrix SDX server.

1. Launch the web browser and log in to the SDX server.
2. Select **Configuration** > **Palo Alto VM-Series** > **Software Images**.
3. In the **Action** drop-down, select **Upload...** and **Browse** to the location of the saved *.xva* image file.
4. Select the image and click **Open**.
5. **Upload** the image to the SDX server.



Provision the VM-Series Firewall on the SDX Server

STEP 1 | Access the SDX server.

Launch the web browser and connect to the SDX server.

STEP 2 | Create the VM-Series firewall.

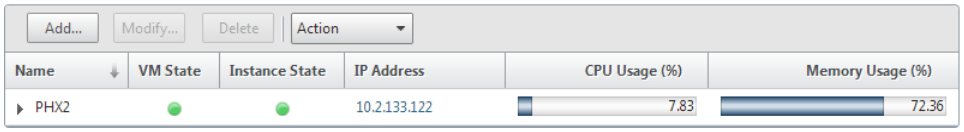
Allocate the total number of data interfaces that you might require on the VM-Series firewall during initial deployment. Adding or removing interfaces to the VM-Series firewall after initial deployment will cause the data interfaces (Eth 1/1 and Eth 1/2) on the VM-Series firewall to re-map to the adapters on the SDX server. Each data interface sequentially maps to the adapter with the lowest numerical value, and can therefore cause a configuration mismatch on the firewall.

1. Select **Configuration** > **Palo Alto VM-Series** > **Instances**.
2. Click **Add**.
3. Enter a name for the VM-Series firewall.
4. Select the .xva image that you uploaded earlier. This image is required to provision the firewall.
5. Allocate the memory, additional disk space, and the virtual CPUs for the VM-Series firewall. To verify resource allocation recommendations, see VM-Series on SDX System Requirements.
6. Select the network interfaces:
   - Use the management interfaces 0/1 or 0/2 and assign an IP address, netmask, and gateway IP address.

     If needed, you can use a data interface on the SDX server for managing the firewall.

   - Select the data interfaces that will be used for handling traffic to and from the firewall.

     If you plan to deploy the interfaces as Layer 2 or virtual wire interfaces, select the Allow L2 Mode option so that the firewall can receive and forward packets for MAC addresses other than its own MAC address.



7. Review the summary and click **Finish** to begin the installation process. It takes 5-8 minutes to provision the firewall. When completed, use the management IP address to launch the web interface of the firewall.

   Continue with Activate the License.

Secure North-South Traffic with the VM-Series Firewall

This section includes information on deploying the NetScaler VPX and the VM-Series firewall on the Citrix SDX server:

- Deploy the VM-Series Firewall Using L3 Interfaces
- Deploy the VM-Series Firewall Using Layer 2 (L2) or Virtual Wire Interfaces
- Deploy the VM-Series Firewall Before the NetScaler VPX (Using Virtual Wire Interfaces)

Deploy the VM-Series Firewall Using L3 Interfaces

To secure north-south traffic, this scenario shows you how to deploy the VM-Series firewall as a L3 deployment; the VM-Series firewall is placed to secure traffic between the NetScaler VPX and the servers on your network.

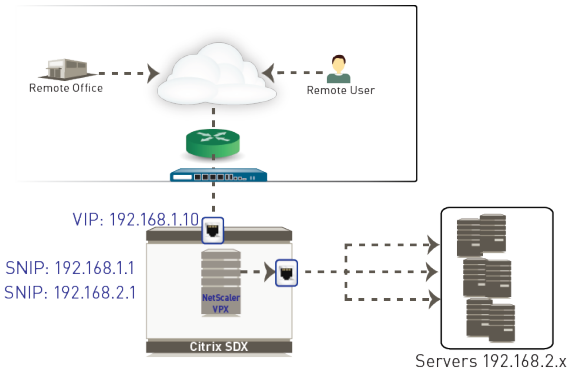


Figure 3: Topology Before Adding the VM-Series Firewall

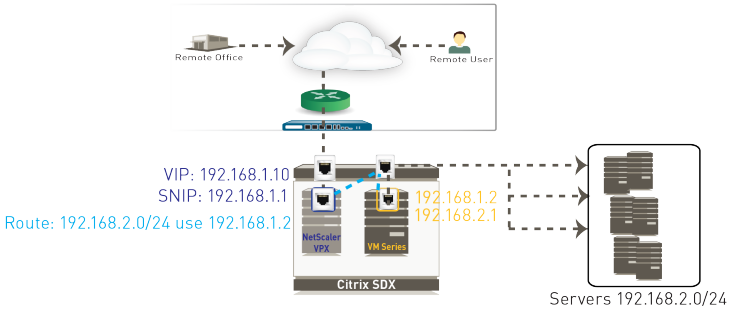


Figure 4: Topology After Adding the VM-Series Firewall

The following procedure includes the tasks you must perform to deploy the VM-Series firewall. For firewall configuration instructions refer to the PAN-OS Documentation. The workflow and configuration on the NetScaler VPX is beyond the scope of this document; for details on configuring the NetScaler VPX, refer to the Citrix documentation.

STEP 1 | Install the VM-Series Firewall on the SDX Server.

When provisioning the VM-Series firewall on the SDX server, you must ensure that you select the data interface accurately so that the firewall can access the server(s).

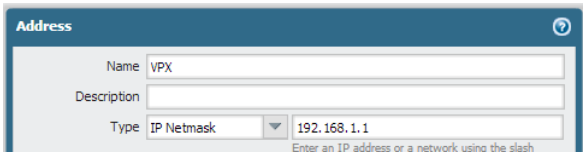
STEP 2 | Configure the data interface on the firewall.

1. Select **Network** > **Virtual Router** and then select the **default** link to open the Virtual Router dialog and **Add** the interface to the virtual router.
2. (Required only if the USIP option is enabled on the NetScaler VPX) On the **Static Routes** tab on the virtual router, select the interface and add the NetScaler SNIP (192.68.1.1 in this example) as the **Next Hop**. The static route defined here will be used to route traffic from the firewall to the NetScaler VPX.
3. Select **Network** > **Interfaces** > **Ethernet** and then select the interface you want to configure.
4. Select the **Interface Type**. Although your choice here depends on your network topology, this example uses **Layer3**.
5. On the **Config** tab, in the **Virtual Router** drop-down, select **default**.
6. Select **New Zone** from the **Security Zone** drop-down. In the Zone dialog, define a **Name** for new zone, for example default, and then click **OK**.
7. Select the **IPv4 or IPv6** tab, click **Add** in the IP section, and enter two IP addresses and network mask to the interface—one for each subnet that is being serviced. For example, 192.168.1.2 and 192.168.2.1.
8. (Optional) To enable you to ping or SSH in to the interface, select **Advanced** > **Other Info**, expand the **Management Profile** drop-down, and select **New Management Profile**. Enter a **Name** for the profile, select **Ping** and **SSH** and then click **OK**.
9. To save the interface configuration, click **OK**.
10. Click **Commit** to save your changes to the firewall.

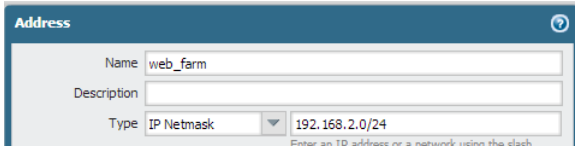
STEP 3 | Create a basic policy to allow traffic between the NetScaler VPX and the web servers.

In this example, because we have set up only one data interface, we specify the source and destination IP address to allow traffic between the NetScaler VPX and the servers.

1. Select **Policies** > **Security,** and click **Add**.
2. Give the rule a descriptive name in the **General** tab.
3. In the **Source** tab, select **Add** in the Source Address section and select the New **Address** link.
4. Create a new address object that specifies the SNIP on the NetScaler VPX. In this example, this IP address is the source for all requests to the servers.



5. In the **Destination** tab, select **Add** in the Destination Address section and select the **New Address** link.
6. Create a new address object that specifies the subnet of the web servers. In this example, this subnet hosts all the web servers that service the requests.



7. In the **Application** tab, select web-browsing.
8. In the **Actions** tab, complete these tasks:
    1. Set the **Action Setting** to **Allow**.
    2. Attach the default profiles for antivirus, anti-spyware, and vulnerability protection, under **Profile Setting**.

9. Verify that logging is enabled at the end of a session under **Options**. Only traffic that matches a security rule will be logged.

		Source	Destination					
	Name	Address	Address	Application	Service	Action	Profile	Options
1	Allow All	VPX	web_farm	web-browsing	any			
2	Deny All	any	any	any	any		none	

10. Create another rule to deny all other traffic from any source and any destination IP address on the network.

    Because all intra-zone traffic is allowed by default, in order to deny traffic other that web-browsing, you must create a deny rule that explicitly blocks all other traffic.

    Go back to Secure North-South Traffic with the VM-Series Firewall, or see Secure East-West Traffic with the VM-Series Firewall.

    For an overview of the deployments, see Supported Deployments—VM Series Firewall on Citrix SDX.

Deploy the VM-Series Firewall Using Layer 2 (L2) or Virtual Wire Interfaces

To secure north-south traffic, this scenario shows you how to deploy the VM-Series firewall in a L2 or a virtual wire deployment. The VM-Series firewall secures traffic destined to the servers. The request arrives at the VIP address of the NetScaler VPX and is processed by the VM-Series firewall before it reaches the servers. On the return path, the traffic is directed to the SNIP on the NetScaler VPX and is processed by the VM-Series firewall before it is sent back to the client.

For the topology before adding the VM-Series firewall, see Topology Before Adding the VM-Series Firewall.

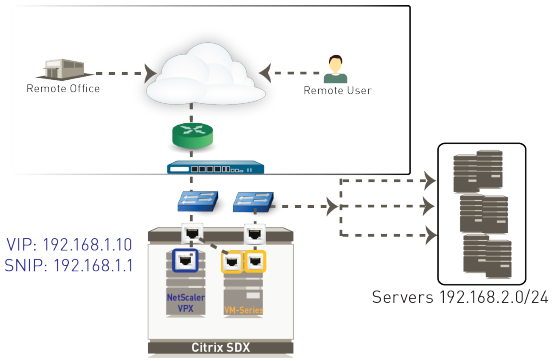


Figure 5: Topology After Adding the VM-Series Firewall

The following task includes the basic configuration steps you must perform to deploy the VM-Series firewall. For firewall configuration instructions refer to the PAN-OS documentation. The workflow and configuration on the NetScaler VPX is beyond the scope of this document; for details on configuring the NetScaler VPX, refer to the Citrix documentation.

STEP 1 | Install the VM-Series Firewall on the SDX Server.

On the SDX server, make sure to enable **Allow L2 Mode** on each data interface. This setting allows the firewall to bridge packets that are destined for the VIP of the NetScaler VPX.

STEP 2 | Re-cable the server-side interface assigned to the NetScaler VPX.

Because the NetScaler VPX will reboot when recabled, evaluate whether you would like to perform this task during a maintenance window.

If you have already deployed a NetScaler VPX and are now adding the VM-Series firewall on the SDX server, you have two ports assigned to the VPX. When you deploy the VM-Series firewall, the NetScaler VPX will now only require one port for handling client-side traffic.

Therefore, before you configure the data interfaces the VM-Series, you must remove the cable from the interface that connects the VPX to the server farm and attach it to the firewall so that all traffic to the server farm is processed by the firewall.

STEP 3 | Configure the data interfaces.

This example shows the configuration for virtual wire interfaces.

Interface	Interface Type	Link State	Virtual Router	VLAN / Virtual-Wire	Security Zone
PA-VM					
ethernet1/1	Virtual Wire		none	vwire1	Client
ethernet1/2	Virtual Wire		none	vwire1	Server

1. Launch the web interface of the firewall.
2. Select **Network** > **Interfaces** > **Ethernet**.
3. Click the link for an interface (for example ethernet 1/1) and select the **Interface Type** as **Layer2** or **Virtual Wire**.

   Virtual Wire Configuration

   Each virtual wire interface (ethernet 1/1 and ethernet 1/2) must be connected to a security zone and a virtual wire. To configure these settings, select the **Config** tab and complete the following tasks:

   1. In the Virtual wire drop-down click **New Virtual Wire**, define a **Name** and assign the two data interfaces (ethernet 1/1 and ethernet 1/2) to it, and then click **OK**.
   2. When configuring ethernet 1/2, select this virtual wire.
   3. Select **New Zone** from the **Security Zone** drop-down, define a **Name** for new zone, for example *client*, and then click **OK**.

   Layer 2 Configuration

   For each Layer 2 interface, you require a security zone. Select the **Config** tab and complete the following tasks:

   1. Select **New Zone** from the **Security Zone** drop-down, define a **Name** for new zone, for example *client*, and then click **OK**.
4. Repeat steps b and c above for the other interface.
5. Click **Commit** to save changes to the firewall.

STEP 4 | Create a basic policy rule to allow traffic through the firewall.

This example shows how to enable traffic between the NetScaler VPX and the web servers.

		Source	Destination				
	Name	Zone	Zone	Application	Service	Action	Options
1	Allow All	Client	Server	oracle web-browsing	application-d...		

1. Select **Policies** > **Security**, and click **Add**.
2. Give the rule a descriptive name in the **General** tab.
3. In the **Source** tab, set the **Source Zone** to the client-side zone you defined. In this example, select client.

4. In the **Destination** tab, set the **Destination Zone** to the server-side zone you defined. In this example, select server.
5. In the **Application** tab, click **Add** to select the applications to which you want to allow access.
6. In the **Actions** tab, complete these tasks:
    1. Set the **Action Setting** to **Allow**.
    2. Attach the default profiles for antivirus, anti-spyware, vulnerability protection and URL filtering, under **Profile Setting**.
7. Verify that logging is enabled at the end of a session under **Options**. Only traffic that matches a security rule will be logged.

    Go back to Secure North-South Traffic with the VM-Series Firewall, or see Secure East-West Traffic with the VM-Series Firewall.

    For an overview of the deployments, see Supported Deployments—VM Series Firewall on Citrix SDX.

Deploy the VM-Series Firewall Before the NetScaler VPX

The following example shows how to deploy the VM-Series firewall to process and secure traffic before it reaches the NetScaler VPX. In this example, the VM-Series firewall is deployed with virtual wire interfaces, and the client connection requests are destined to the VIP on the NetScaler VPX. Note that you can deploy the VM-Series firewall using L2 or L3 interfaces, based on your specific needs.

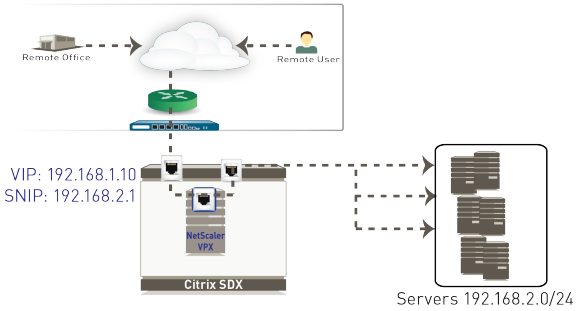


Figure 6: Topology Before Adding the VM-Series Firewall

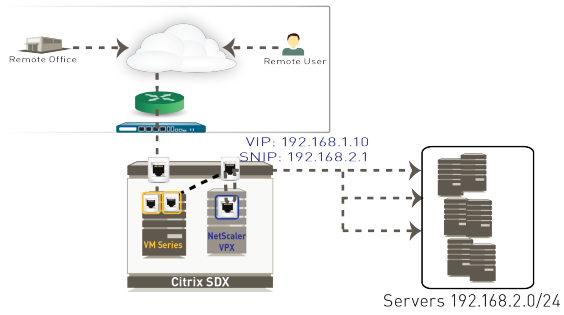


Figure 7: Topology after adding the VM-Series firewall

The following table includes the basic configuration tasks you must perform on the VM-Series firewall. For firewall configuration instructions refer to the PAN-OS documentation. The workflow and configuration on the NetScaler VPX is beyond the scope of this document; for details on configuring the NetScaler VPX, refer to the Citrix documentation.

STEP 1 | Install the VM-Series Firewall on the SDX Server.

On the SDX server, make sure to enable **Allow L2 Mode** on the data interface. This setting allows the firewall to bridge packets that are destined for the VIP of the NetScaler VPX.

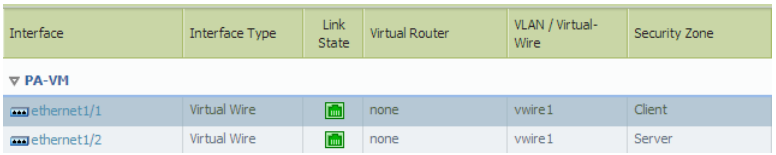
STEP 2 | Re-cable the client-side interface assigned to the NetScaler VPX.

Because the NetScaler VPX will reboot when recabled, evaluate whether you would like to perform this task during a maintenance window.

If you have already deployed a NetScaler VPX and are now adding the VM-Series firewall on the SDX server, you have two ports assigned to the VPX. When you deploy the VM-Series firewall, the NetScaler VPX will now only require one port that connects it to the server farm.

Therefore, before you configure the data interfaces the VM-Series, you must remove the cable from the interface that connects the VPX to the client-side traffic and attach it to the firewall so that all incoming traffic is processed by the firewall.

STEP 3 | Configure the data interfaces.

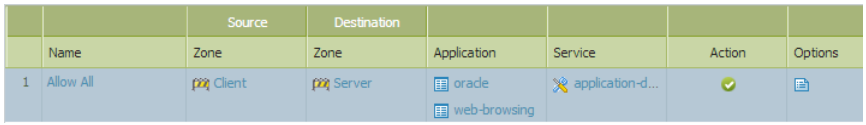


1. Launch the web interface of the firewall.
2. Select **Network** > **Interfaces** > **Ethernet**.
3. Click the link for an interface, for example ethernet 1/1, and select the **Interface Type** as **Virtual Wire**.
4. Click the link for the other interface and select the **Interface Type** as **Virtual Wire**.
5. Each virtual wire interface must be connected to a security zone and a virtual wire. To configure these settings, select the **Config** tab and complete the following tasks:
   - In the Virtual wire drop-down click **New Virtual Wire**, define a **Name** and assign the two data interfaces (ethernet 1/1 and ethernet 1/2) to it, and then click **OK**.

     When configuring ethernet 1/2, select this virtual wire.
   - Select **New Zone** from the **Security Zone** drop-down, define a **Name** for new zone, for example client, and then click **OK**.
6. Repeat step e for the other interface.
7. Click **Commit** to save changes to the firewall.

STEP 4 | Create a basic policy rule to allow traffic through the firewall.

This example shows how to enable traffic between the NetScaler VPX and the web servers.



1. Select **Policies** > **Security**, and click **Add**.
2. Give the rule a descriptive name in the **General** tab.
3. In the **Source** tab, set the **Source Zone** to the client-side zone you defined. In this example, select client.
4. In the **Destination** tab, set the **Destination Zone** to the server-side zone you defined. In this example, select server.
5. In the **Application** tab, click **Add** to select the applications to which you want to allow access.
6. In the **Actions** tab, complete these tasks:

1. Set the **Action Setting** to **Allow**.
2. Attach the default profiles for antivirus, anti-spyware, vulnerability protection and URL filtering, under **Profile Setting**.

7. Verify that logging is enabled at the end of a session under **Options**. Only traffic that matches a security rule will be logged.

Go back to Secure North-South Traffic with the VM-Series Firewall, or see Secure East-West Traffic with the VM-Series Firewall.

For an overview of the deployments, see Supported Deployments—VM Series Firewall on Citrix SDX.

Secure East-West Traffic with the VM-Series Firewall

The following example shows you how to deploy your VM-Series firewall to secure the application or database servers on your network. This scenario is relevant to you if you have two NetScaler VPX instances, where one instance authenticates users and terminates SSL connections and then load balances requests to the DMZ servers and the other VPX instance load balances connections to the corporate servers that host the application and database servers on your network.

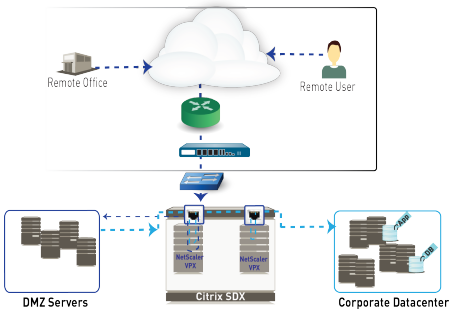


Figure 8: Topology Before Adding the VM-Series Firewall

The communication between the servers in the DMZ and the servers in the corporate datacenter is processed by both instances of the NetScaler VPX. For content that resides in the corporate datacenter, a new request in handed off to the other instance of the NetScaler VPX which forwards the request to the appropriate server.

When the VM-Series firewall is deployed (this example uses L3 interfaces), the flow of traffic is as follows:

- All incoming requests are authenticated and the SSL connection is terminated on the first instance of the NetScaler VPX. For content that resides in the DMZ, the NetScaler VPX initiates a new connection to the server to fetch the requested content. Note that the north-south traffic destined to the corporate datacenter or to the servers in the DMZ are handled by the edge firewall and not by the VM-Series firewall.

  For example, when a user (source IP 1.1.1.1) requests content from a server on the DMZ, the destination IP is 20.5.5.1 (VIP of the NetScaler VPX). The NetScaler VPX then replaces the destination IP address, based on the protocol to the internal server IP address, say 192.168.10.10. The return traffic from the server is sent back to the NetScaler VPX at 20.5.5.1 and sent to the user with IP address 1.1.1.1.
- All requests between the DMZ servers and the Corporate datacenter are processed by the VM-Series firewall. For content that resides in the corporate datacenter, the request is transparently processed (if deployed using L2 or virtual wire interfaces) or routed (using Layer3 interfaces) by the VM-Series firewall. It is then handed off to the second instance of the NetScaler VPX. This instance of the NetScaler VPX load balances the request across the servers in the corporate datacenter and services the request. The return traffic uses the same path as the incoming request.

  For example, when a server on the DMZ (say 192.168.10.10) needs content from a server in the corporate datacenter (say 172.16.10.20), the destination IP address is 172.168.10.3 (the VIP on the second NetScaler). The request is sent to the VM-Series firewall at 192.168.10.2, where the firewall performs a policy lookup and routes the request to 172.168.10.3. The second NetScaler VPX replaces the destination IP address, based on protocol, to the internal server IP address 172.16.10.20. The return traffic from 172.168.10.20 is then sent to the NetScaler VPX at 172.168.10.3, and the source IP address

for the request is set as 172.168.10.3 and is routed to the VM-Series firewall at 172.168.10.2. On the VM-Series firewall, a policy lookup is again performed and the traffic is routed to the server in the DMZ (192.168.10.10).

In order to filter and report on user activity on your network, because all requests are initiated from the NetScaler VPX, you must enable HTTP Header insertion or the TCP Option for IP Insertion on the first instance of the NetScaler VPX.

STEP 1 | Install the VM-Series Firewall on the SDX Server

If you plan to deploy the VM-Series firewall using virtual wire or L2 interfaces, make sure to enable L2 Mode on each data interface on the SDX server.

STEP 2 | Re-cable the interfaces assigned to the NetScaler VPX.

Because the NetScaler VPX will reboot when recabled, evaluate whether you would like to perform this task during a maintenance window.

STEP 3 | Configure the data interfaces.

Select **Network** > **Interfaces** and assign the interfaces as type Layer3 (see step 2, Layer2 (see step 3) or virtual wire (see step 3).

STEP 4 | Create security policy to allow application traffic between the DMZ and the corporate data center.

Zone: DMZ to Corporate

Note that the implicit deny rule will deny all inter-zone traffic except what is explicitly allowed by security policy.

1. Click **Add** in the **Policies** > **Security** section.
2. Give the rule a descriptive name in the **General** tab.
3. In the **Source** tab, set the **Source Zone** to DMZ and **Source Address** to 192.168.10.0/24.
4. In the **Destination** tab, set the **Destination Zone** to Corporate and the **Destination Address** to 172.168.10.0/24
5. In the **Application** tab, select the applications that you want to allow. For example, Oracle.
6. Set the **Service** to **application-default**
7. In the **Actions** tab, set the **Action Setting** to Allow.
8. Leave all the other options at the default values.
9. Click **Commit** to save your changes.

For securing north-south traffic, see Secure North-South Traffic with the VM-Series Firewall.

For an overview of the deployments, see Supported Deployments—VM Series Firewall on Citrix SDX.

Set Up the VM-Series Firewall on VMware NSX

The VM-Series firewall for VMware NSX is jointly developed by Palo Alto Networks and VMware. This solution uses the NetX API to integrate the Palo Alto Networks next-generation firewalls and Panorama with VMware ESXi servers to provide comprehensive visibility and safe application enablement of all data center traffic including intra-host virtual machine communications.

The following topics provide information about the VM-Series for NSX:

VM-Series for NSX Firewall Overview

NSX, VMware's Networking and Security platform designed for the software-defined data center (SDDC), offers the ability to deploy the Palo Alto Networks firewall as a service on a cluster of ESXi servers. The term *SDDC* is a VMware term that refers to a data center where infrastructure—compute resources, network and storage—is virtualized using VMware NSX.

To keep pace with the changes in the agile SDDC, the VM-Series firewall for NSX simplifies the process of deploying a Palo Alto Networks next-generation firewall and continually enforcing security and compliance for the east-west traffic in the SDDC. For details on the VM-Series for NSX, see the following topics:

- What are the Components of the VM-Series for NSX Solution?
- How Do the Components in the VM-Series Firewall for NSX Solution Work Together?
- What are the Benefits of the NSX VM-Series firewall for NSX Solution?
- What is Multi-Tenant Support on the VM-Series Firewall for NSX?

What are the Components of the VM-Series for NSX Solution?

The following tables show the components of this joint Palo Alto Networks and VMware solution. The following topics describe each component in more detail:

- vCenter Server
- NSX Manager
- Panorama
- VM-Series Firewall for NSX
- Ports/Protocols used Network Communication

VMware Components	
vCenter Server	The vCenter server is the centralized management tool for the vSphere suite.
NSX Manager	VMware's Networking and Security platform must be installed and registered with the vCenter server. The NSX Manager is required to deploy the VM-Series firewall on the ESXi hosts within a ESXi cluster.
ESXi Server	ESXi is a hypervisor that enables compute virtualization.

Palo Alto Networks Components	
PAN-OS	The VM-Series base image (PA-VM-NSX-8.0.zip) is used for deploying the VM-Series firewall for NSX with PAN-OS 8.0. The minimum system requirement for deploying the VM-Series firewall for NSX on the ESXi server depends on your VM-Series model. See VM-Series System Requirements for the minimum hardware requirements for your VM-Series model.
Panorama Panorama must be running the same release version or	Panorama is the centralized management tool for the Palo Alto Networks next-generation firewalls. In this solution, Panorama works with the NSX Manager to deploy, license, and centrally administer—configuration and policies—on the VM-Series firewall for NSX.

Palo Alto Networks Components	
later version that the firewalls that it will manage.	Panorama must be able to connect to the NSX Manager, the vCenter server, the VM-Series firewalls and the Palo Alto Networks update server. The resources required by Panorama depend on the mode Panorama will run in: Legacy or Panorama (recommended). New 8.0 Panorama installations run in Panorama mode while a Panorama upgraded to 8.0 runs in Legacy mode. For more information about the modes and the requirements associated with each mode, see Set Up the Panorama Virtual Appliance. In Panorama Mode, set the memory, number of CPUs, and storage based on the log storage capacity of Panorama: • 2TB storage—8 CPUs and 16GB memory • 4TB storage—8 CPUs and 32GB memory • 6 to 8TB storage—12 CPUs and 32GB memory • 10 to 16TB storage—12 CPUs and 64GB memory • 18 to 24TB storage—16 CPUs and 64GB memory • System Disk Space: 81GB • Log Storage Capacity: 2TB to 24TB In Legacy Mode, set the memory and the number of cores based on the number of firewalls that Panorama will manage: • 1 to 10 firewalls: 4 cores and 4GB memory • 11 to 50 firewalls: 8 cores and 8GB memory • 51 to 1,000 firewalls: 8 cores and 16GB memory • System Disk Space: 52GB • Log Storage Capacity: 11GB (default log storage on the system disk) to 8TB (if you add a virtual logging disk)
VM-Series Firewall for NSX	The VM-100, VM-200, VM-300, VM-500, and VM-1000-HV, support NSX.

Versions Supported	
vCenter/ESXi	• 5.5 • 6.0 • 6.5a (requires Panorama VMware NSX Plugin 1.0.1 or higher and NSX Manager 6.3)
NSX Manager	• 6.1 • 6.2 • 6.3 (requires Panorama VMware NSX Plugin 1.0.1 or higher)

vCenter Server

The vCenter server is required to manage the NSX Manager and the ESXi hosts in your data center. This joint solution requires that the ESXi hosts be organized into one or more clusters on the vCenter server and must be connected to a distributed virtual switch.

For information on clusters, distributed virtual switch, DRS, and the vCenter server, refer to your VMware documentation: http://www.vmware.com/support/vcenter-server.html

NSX Manager

NSX is VMware's network virtualization platform that is completely integrated with vSphere. The NSX Firewall and the Service Composer are key features of the NSX Manager. The NSX firewall is a logical firewall that allows you to attach network and security services to the virtual machines, and the Service Composer allows you to group virtual machines and create policy to redirect traffic to the VM-Series firewall (called the Palo Alto Networks NGFW service on the NSX Manager).

Panorama

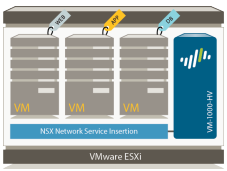
Panorama is used to register the VM-Series firewall for NSX as the *Palo Alto Networks NGFW* service on the NSX Manager. Registering the Palo Alto Networks NGFW service on the NSX Manager allows the NSX Manager to deploy the VM-Series firewall for NSX on each ESXi host in the ESXi cluster.

Panorama serves as the central point of administration for the VM-Series firewalls running on NSX. When a new VM-Series firewall is deployed in NSX, it communicates with Panorama to obtain the license and receives its configuration/policies from Panorama. All configuration elements, policies, and dynamic address groups on the VM-Series firewalls can be centrally managed on Panorama using Device Groups and Templates. The REST-based XML API integration in this solution, enables Panorama to synchronize with the NSX Manager and the VM-Series firewalls to allow the use of dynamic address groups and share context between the virtualized environment and security enforcement. For more information, see Policy Enforcement using Dynamic Address Groups.

VM-Series Firewall for NSX

The VM-Series firewall for NSX is the VM-Series firewall that is deployed on the ESXi hypervisor. The integration with the NetX API makes it possible to automate the process of installing the VM-Series firewall directly on the ESXi hypervisor, and allows the hypervisor to forward traffic to the VM-Series firewall without using the vSwitch configuration; it therefore, requires no change to the virtual network topology.

The VM-Series firewall for NSX only supports virtual wire interfaces. On this firewall, ethernet 1/1 and ethernet 1/2 are bound together through a virtual wire and use the NetX dataplane API to communicate with the hypervisor. Layer 2 or Layer 3 interfaces are neither required nor supported on the VM-Series firewall for NSX, and therefore no switching or routing actions can be performed by the firewall. For enabling traffic separation in a multi-tenancy environment, you can create additional zones that internally map to a pair of virtual wire subinterfaces on the parent virtual wire interfaces, ethernet 1/1 and ethernet 1/2.



Ports/Protocols used Network Communication

In order to enable the network communication required to deploy the VM-Series firewall for NSX, you must allow the use of the following protocols/ports and applications.

- **Panorama**—To obtain software updates and dynamic updates, Panorama uses SSL to access updates.paloaltonetworks.com on TCP/443; this URL leverages the CDN infrastructure. If you need a single IP address, use staticupdates.paloaltonetworks.com. The App-ID for updates is paloalto-updates.

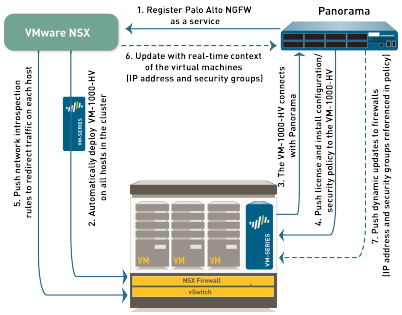
  The NSX Manager and Panorama use SSL to communicate on TCP/443.
- **VM-Series Firewall for NSX**—If you plan to use WildFire, the VM-Series firewalls must be able to access wildfire.paloaltonetworks.com on port 443. This is an SSL connection and the App-ID is paloalto-wildfire-cloud.

The management interface on the VM-Series firewall uses SSL to communicate with Panorama over TCP/3978.

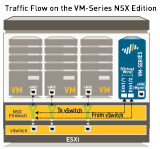
- **vCenter Server** The vCenter Server must be able to reach the deployment web server that is hosting the VM-Series OVA. The port is TCP/80 by default or App-ID web-browsing.

How Do the Components in the VM-Series Firewall for NSX Solution Work Together?

To meet the security challenges in the software-defined data center, the NSX Manager, ESXi servers and Panorama work harmoniously to automate the deployment of the VM-Series firewall.



1. **Register the Palo Alto Networks NGFW service**—The first step is to register the Palo Alto Networks NGFW as a service on the NSX Manager. The registration process uses the NetX management plane API to enable bi-directional communication between Panorama and the NSX Manager. Panorama is configured with the IP address and access credentials to initiate a connection and register the Palo Alto Networks NGFW service on the NSX Manager. The service definition includes the URL for accessing the VM-Series base image that is required to deploy the VM-Series firewall for NSX, the authorization code for retrieving the license and the device group and template to which the VM-Series firewalls will belong. The NSX manager uses this management plane connection to share updates on the changes in the virtual environment with Panorama.
2. **Deploy the VM-Series automatically from NSX**—The NSX Manager collects the VM-Series base image from the URL specified during registration and installs an instance of the VM-Series firewall on each ESXi host in the ESXi cluster. From a static management IP pool or a DHCP service (that you define on the NSX Manager), a management IP address is assigned to the VM-Series firewall and the Panorama IP address is provided to the firewall. When the firewall boots up, the NetX dataplane integration API connects the VM-Series firewall to the hypervisor so that it can receive traffic from the vSwitch.



3. **Establish communication between the VM-Series firewall and Panorama**—The VM-Series firewall then initiates a connection to Panorama to obtain its license. Panorama retrieves the license from the update server and pushes it to the firewall. The VM-Series firewall receives the license and reboots with a valid serial number.

   If your Panorama is offline, which means that it does not have direct Internet access to retrieve the licenses and push them to the firewalls, you must manually license each firewall. If your VM-Series firewall does not have internetaccess*, you must add the serial number of the firewall to Panorama so that it is registered as a managed device, so that you can push the appropriate template and device group settings from Panorama.*
4. **Install configuration/policy from Panorama to the VM-Series firewall**—The VM-Series firewall reconnects with Panorama and provides its serial number. Panorama now adds the firewall to the device

group and template that was defined in the service definition and pushes the configuration and policy rules to the firewall. The VM-Series firewall is now available as a security virtual machine that can be further configured to safely enable applications on the network.

5. **Push traffic redirection rules to NSX Manager**—Create security groups and define network introspection rules that specify the guests from which traffic will be steered to the VM-Series firewall. See Integrated Policy Rules for details.

   To ensure that traffic from the guests is steered to the VM-Series firewall, you must have VMware Tools installed on each guest. If VMware Tools is not installed, the NSX Manager does not know the IP address of the guest and therefore, the traffic cannot be steered to the VM-Series firewall. For more information, see Steer Traffic from Guests that are not Running VMware Tools. This is not required if you are running NSX Manager 6.2.4 or later.

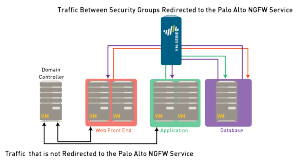
6. **Receive real-time updates from NSX Manager**—The NSX Manager sends real-time updates on the changes in the virtual environment to Panorama. These updates include information on the security groups and IP addresses of guests that are part of the security group from which traffic is redirected to the VM-Series firewall. See Integrated Policy Rules for details.
7. **Use dynamic address groups in policy and push dynamic updates from Panorama to the VM-Series firewalls**—On Panorama, use the real-time updates on security groups to create dynamic address groups, bind them to security policies and then push these policies to the VM-Series firewalls. Every VM-Series firewall in the device group will have the same set of policies and is now completely marshaled to secure the SDDC. See Policy Enforcement using Dynamic Address Groups for details.

Integrated Policy Rules

Panorama serves as the single point of configuration that provides the NSX Manager with the contextual information required to redirect traffic from the guest virtual machines to the VM-Series firewall. The traffic steering rules are defined on Panorama and pushed to NSX Manager; these determine what traffic from which guests in the cluster are steered to the Palo Alto Networks NGFW service. Security enforcement rules are also defined on Panorama and pushed to the VM-Series firewalls for the traffic that is steered to the Palo Alto Networks NGFW service.

- **Steering Rules**—The rules for directing traffic from the guests on each ESXi host are defined on Panorama and applied by NSX Manager as partner security services rules.

  For traffic that needs to be inspected and secured by the VM-Series firewall, the steering rules created on Panorama allow you to redirect the traffic to the Palo Alto Networks NGFW service. This traffic is then steered to the VM-Series firewall and is first processed by the VM-Series firewall before it goes to the virtual switch.



  Traffic that does not need to be inspected by the VM-Series firewall, for example network data backup or traffic to an internal domain controller, does not need to be redirected to the VM-Series firewall and can be sent to the virtual switch for onward processing.
- **Rules centrally managed on Panorama and applied by the VM-Series firewall**—The next- generation firewall rules are applied by the VM-Series firewall. These rules are centrally defined and managed on Panorama using templates and device groups and pushed to the VM-Series firewalls. The VM-Series firewall then enforces security policy by matching on source or destination IP address—the use of dynamic address groups allows the firewall to populate the members of the groups in real time—and forwards the traffic to the filters on the NSX Firewall.

To understand how the NSX Manager and Panorama stay synchronized with the changes in the SDDC and ensure that the VM-Series firewall consistently enforces policy, see Policy Enforcement using Dynamic Address Groups.

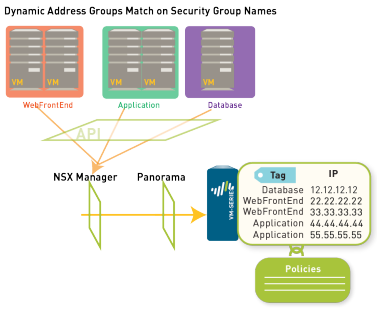
Policy Enforcement using Dynamic Address Groups

Unlike the other versions of the VM-Series firewall, because both virtual wire interfaces (and subinterfaces) belong to the same zone, the VM-Series firewall for NSX uses dynamic address groups as the traffic segmentation mechanism. A security policy rule on the VM-Series firewall for NSX must have the same source and destination zone, therefore to implement different treatment of traffic, you use dynamic address groups as source or destination objects in security policy rules.

Dynamic address groups offer a way to automate the process of referencing source and/or destination addresses within security policies because IP addresses are constantly changing in a data center environment. Unlike static address objects that must be manually updated in configuration and committed whenever there is an address change (addition, deletion, or move), dynamic address groups automatically adapt to changes.

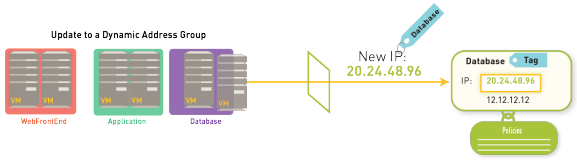
Any dynamic address groups created in a device group belonging to NSX configuration and configured with the match criterion **_nsx_<*dynamic address group name*>** trigger the creation on corresponding security groups on the NSX Manager. In an ESXi cluster with multiple customers or tenants, the ability to filter security groups for a service profile (zone on Panorama) on the NSX Manager allows you to enforce policy when you have overlapping IP addresses across different security groups in your virtual environment.

If, for example, you have a multi-tier architecture for web applications, on Panorama you create three dynamic address groups for the WebFrontEnd servers, Application servers and the Database servers. When you commit these changes on Panorama, it triggers the creation of three corresponding security groups on NSX Manager.



On NSX Manager, you can then add guest VMs to the appropriate security groups. Then, in security policy you can use the dynamic address groups as source or destination objects, define the applications that are permitted to traverse these servers, and push the rules to the VM-Series firewalls.

Each time a guest is added or modified in the ESXi cluster or a security group is updated or created, the NSX Manager uses the PAN-OS REST-based XML API to update Panorama with the IP address, and the security group to which the guest belongs. To trace the flow of information, see Dynamic Address Groups—Information Relay from NSX Manager to Panorama.



To ensure that the name of each security group is unique, the vCenter server assigns a Managed Object Reference (MOB) ID to the name you define for the security group. The syntax used to display the name of a security group on Panorama is serviceprofileid-

specified_name-securitygroup-number; for example, serviceprofile13-WebFrontEnd-securitygroup-47.

When Panorama receives the API notification, it verifies/updates the IP address of each guest and the security group and the service profile to which that guest belongs. Then, Panorama pushes these real-time updates to all the firewalls that are included in the device group and notifies device groups in the service manager configuration on Panorama.

On each firewall, all policy rules that reference these dynamic address groups are updated at runtime. Because the firewall matches on the security group tag to determine the members of a dynamic address group, you do not need to modify or update the policy when you make changes in the virtual environment. The firewall matches the tags to find the current members of each dynamic address group and applies the security policy to the source/destination IP address that are included in the group.

What are the Benefits of the NSX VM-Series firewall for NSX Solution?

The VM-Series firewall for VMware NSX is focused on securing east-west communication in the software-defined data center. Deploying the firewall has the following benefits:

- **Sturdier Centralized Management**—The firewalls deployed using this solution are licensed and managed by Panorama, the Palo Alto Networks central management tool. Panorama serves as a single point of configuration for integration with NSX. It gives the NSX Manager the information is it needs to steer redirect traffic to the VM-Series firewall for inspection and enforcement. Using Panorama to manage both the perimeter and data center firewalls (the hardware-based and virtual firewalls) allows you to centralize policy management and maintain agility and consistency in policy enforcement throughout the network.
- **Automated Deployment**—The NSX Manager automates the process of delivering next-generation firewall security services and the VM-Series firewall allows for transparent security enforcement. When a new ESXi host is added to a cluster, a new VM-Series firewall is automatically deployed, provisioned and available for immediate policy enforcement without any manual intervention. The automated workflow allows you to keep pace with the virtual machine deployments in your data center. The hypervisor mode on the firewall removes the need to reconfigure the ports/ vswitches/ network topology; because each ESXi host has an instance of the firewall, the traffic does not need to traverse the network or be backhauled for inspection and consistent enforcement of policies.
- **Ease in Administering Tenants in Shared and Dedicated Compute Infrastructure** —This integration provides the flexibility in configuring the firewall to handle multiple zones for traffic segmentation, defining shared or specific policy sets for each tenant or sub-tenant, and includes support for overlapping IP addresses across tenants or sub-tenants. Whether you have a shared cluster and need to define tenant specific policies and logically isolate traffic for each tenant (or sub-tenant), or you have a dedicated cluster for each tenant, this solution enables you to configure the firewall for your needs. And if you need a dedicated instance of the VM-Series firewall for each tenant in a cluster that hosts the workloads for multiple tenants, you can deploy multiple instances of the VM-Series firewall on each host in an ESXi cluster. For more information, see What is Multi-Tenant Support on the VM-Series Firewall for NSX?
- **Tighter Integration Between Virtual Environment and Security Enforcement for Dynamic Security**—Dynamic address groups maintain awareness of changes in the virtual machines/applications and ensure that security policy stays in tandem with the changes in the network. This awareness provides visibility and protection of applications in an agile environment.

In summary, this solution ensures that the dynamic nature of the virtual network is secured with minimal administrative overhead. You can successfully deploy applications with greater speed, efficiency, and security.

What is Multi-Tenant Support on the VM-Series Firewall for NSX?

Multi-tenancy on the VM-Series firewall enables you to secure more than one *tenant* or more than one *sub-tenant*. A tenant is a customer or an organization such as Palo Alto Networks. A sub-tenant is a department or business unit within the organization such as Marketing, Accounting, or Human Resources. To allow you to secure multiple tenants, Panorama provides the flexibility to create multiple sets of security policy rules for each tenant, and multiple zones to isolate traffic from each sub-tenant and redirect traffic to the appropriately configured VM-Series firewall. You can also deploy more than one instance of the VM-Series firewall on each host within an ESXi cluster.

Panorama and managed VM-Series firewalls must be running PAN-OS 7.1 or greater to support multi-tenancy.

To deploy a multi-tenant solution, create one or more *service definition(s)* and *service profile zone(s)* on Panorama. A service definition on Panorama specifies the configuration of the VM-Series firewall using one device group and one template. This means that each instance of the VM-Series firewalls that is deployed using a service definition has one common set of policy rules for securing the tenants and sub-tenants in the ESXi cluster.

A service profile zone within a Panorama template is used to segment traffic from each sub-tenant using virtual wire subinterfaces. When you create a new service profile zone, Panorama pushes the zone as a part of the template configuration to the firewall, and the firewall automatically creates a pair of virtual wire subinterfaces, for example ethernet1/1.3 and ethernet 1/2.3 so that the firewall can isolate traffic for a sub-tenant. Because a template supports up to 32 subinterface pairs, you can logically isolate traffic and secure up to 32 sub-tenants.

Panorama registers each service definition as a service definition on the NSX Manager and each service profile zone as a service profile within the corresponding service definition. And, when you deploy the service definition from the NSX Manager, an instance of the VM-Series firewall is deployed on each host in the ESXi cluster. And you can use the steering rules defined on Panorama and applied to the NSX Manager to specify what traffic to redirect to the VM-Series firewall based on NSX security groups, and to which tenant or sub-tenant based on the service profile.

Based on your requirements, you can choose from the following multi-tenancy options:

- **Shared cluster with shared VM-Series firewalls**- Multiple tenants share the cluster and the VM-Series firewall. A single instance of the VM-Series firewall is deployed on each host in the cluster. In order to separate traffic from each tenant, you create a zone for each tenant, and you define a single, common set of policy rules to secure the virtual machines for all tenants. See Use Case: Shared Compute Infrastructure and Shared Security Policies.
- **Dedicated cluster with dedicated VM-Series firewalls**- A single tenant occupies the cluster, and a single instance of the VM-Series firewall is deployed on each host in the cluster. In this deployment, the tenant can have a single zone and a single policy set, or the tenant can have multiple zones for sub-tenants that require traffic separation (one zone per sub-tenant) and a single policy set with zone-based rules to secure traffic for each sub-tenant. Use Case: Shared Security Policies on Dedicated Compute Infrastructure.
- **Shared cluster with dedicated VM-Series firewalls**- Multiple tenants share the cluster and multiple instances of the VM-Series firewalls are deployed on each host in a cluster so that each tenant can have a dedicated instance of the VM-Series firewall. This deployment provides scalability and better performance on shared infrastructure for each tenant. Based on each tenant's needs, you will define two or more service definitions for the cluster.

  When deploying multiple instances of the VM-Series firewall, you must ensure that each ESXi host has the sufficient CPU, memory and hard disk resources required to support the VM-Series firewalls and the other virtual machines that will be running on it.

VM-Series Firewall for NSX Deployment Checklist

To deploy the VM-Series firewall for NSX, use the following workflow:

- **Step 1: Set up the Components**—To deploy the VM-Series firewall for NSX, set up the following components (see What are the Components of the VM-Series for NSX Solution?):
  - Set up the vCenter server, install and register the NSX Manager with the vCenter server.

    If you have not already set up the virtual switch(es) and grouped the ESXi hosts in to clusters, refer to the VMware documentation for instructions on setting up the vSphere environment. This document does not take you through the process of setting up the VMware components of this solution.

    Unless you Enable Large Receive Offload, do not modify the default value (1500 bytes) of the MTU on the virtual Distributed Switch (vDS) in the vSphere infrastructure. Modifying the MTU to any other value causes the VM-Series firewall for NSX to discard packets.
  - Upgrade Panorama to version 8.0. If you are new to Panorama, refer to the Panorama documentation for instructions on setting up and upgrading Panorama. See Migrate Panorama 7.1 Configuration to Panorama 8.0 Configuration for information about converting your 7.1 configuration formats to 8.0 configuration formats.
  - Configure an SSL/TLS Service Profile. If you are running NSX Manager 6.2.3 or earlier, you must configure an SSL/TLS Service profile that allows TLSv1.0 and apply it to the Panorama management interface. If you are running NSX Manager 6.2.4 or later, an SSL/TLS Service profile is not required.
  - Install the VMware NSX Plugin.
  - Install a License Deactivation API Key. Deleting the Palo Alto Networks Service Deployment on NSX Manager automatically triggers license deactivation. A license deactivation API key is required to successfully deactivate the VM-Series license.
  - Download and save the ovf template for the VM-Series firewall for NSX on a web server. The ovf template must match your VM-Series model. If you are using the VM-200, select the VM-100 ovf (PA-VM-NSX-8.0.0.vm100.ovf). If using the VM-1000-HV, select the VM-300 ovf (PA-VM-NSX-8.0.0.vm300.ovf).

    The NSX Manager must have network access to this web server so that it can deploy the VM-Series firewall as needed. You cannot host the ovf template on Panorama.

    *Give the ova filename a generic name that does not include a version number. Using a generic naming convention, such as **https://acme.com/software/PA-VM-NSX.ova** allows you to overwrite the ova each time a newer version becomes available.*
  - Register the capacity auth-code for the VM-Series firewall for NSX with your support account on the Support Portal. For details, see Upgrade the VM-Series Firewall.
- **Step 2: Register**—Configure Panorama to Register the VM-Series Firewall as a Service on the NSX Manager. When registered, the VM-Series firewall is added to the list of network services that can be transparently deployed as a service by the NSX Manager. The connection between Panorama and the NSX Manager is also required for licensing and configuring the firewall.

  If you had configured Panorama to register the VM-Series firewall as a service on the NSX Manager in an earlier version, see Changes to default behavior to learn about the changes upon upgrade to version 8.0.

  - (On Panorama) Create a service manager to enable communication between Panorama and NSX Manager.

- (On Panorama) Create the service definition. If you upgrade from an earlier version, your existing service definition is automatically migrated for you. For details, see changes to default behavior.

- **Step 3: Deploy the VM-Series Firewall**—Before you can deploy the VM-Series firewall in NSX, each host in the cluster must have the necessary NSX components required to deploy the firewall.
  - (On NSX Manager) Enable SpoofGuard and define rules to block non-IP protocols.
  - (On NSX Manager) Define the IP address pool. An IP address from the defined range is assigned to the management interface of each instance of the VM-Series firewall.

    The NSX Manager uses the IP address as a match criterion to steer traffic to the VM-Series firewall. If VMware tools is not installed on the guest, see Steer Traffic from Guests that are not Running VMware Tools*. This is not required if you are running NSX Manager 6.2.4 or later.*
  - (On NSX Manager) Prepare the ESXi host for the VM-Series firewall.
  - (On NSX Manager) Deploy the VM-Series firewall. The NSX Manager automatically deploys an instance of the VM-Series firewall on each ESXi host in the cluster.
  - (On NSX Manager) Add VMs to the relevant security groups.
  - (On Panorama) Apply policies to the VM-Series firewall. From Panorama, you define, push, and administer policies centrally on all the VM-Series firewalls. This centralized administration mechanism allows you to secure guests/applications with minimal administrative intervention.
- **Step 4: Create Security Groups and Steering Rules**—How you choose to deploy the security groups and steering rules depends on whether your deployment focus is Security Centric or Operations Centric.

  In a Security Centric deployment, your security administrator creates the security group and steering rules in Panorama. You might start with an existing set of security policies and a set of named source and destination groups. Any new dynamically deployed applications fit into predefined security policies defined on Panorama. Panorama pushes these named groups to NSX Manager, where the virtualization administrator picks up the group names and defines which VMs go into them.

  In an Operations Centric deployment, security groups are defined by a virtualization administrator based upon the need to classify and categorize VM workloads. In this case, security groups are defined and populated in the NSX Manager. Security groups created in NSX Manager must be associated with dynamic address groups on Panorama, which is completed after the firewalls are deployed. In this case, NSX base functionality is deployed first and the VM-Series firewalls are added later.

  You must decide whether a Security Centric or an Operations Centric deployment is right for your NSX environment before continuing. This document describes the procedure for a Security Centric deployment.

  Security Centric—Create the service definition(s) that specify the configuration for the VM-Series firewall, create dynamic address groups, and create policies to redirect traffic to the VM-Series firewall. See Create Security Groups and Steering Rules in a Security Centric Deployment.
  - (On Panorama) Set up the dynamic address groups that map to security groups on NSX Manager. A security group assembles the specified guests/applications so that you can apply policy to the group.
  - (On Panorama) Create the security policy rules to redirect traffic to the Palo Alto Networks service profile.

  Operations Centric—On the NSX Manager, create security groups and policies to redirect traffic to the VM-Series firewall. See Create Security Groups and Steering Rules in an Operations Centric Deployment.
  - (On NSX Manager) Set up the security groups. A security group assembles the specified guests/applications so that you can apply policy to the group.
  - (On NSX Manager) Create the NSX Firewall policies to redirect traffic to the Palo Alto Networks service profile.

- **Step 5: Monitor and Maintain Network Security**—Panorama provides a comprehensive, graphical view of network traffic. Using the visibility tools on Panorama—the Application Command Center (ACC), logs, and the report generation capabilities—you can centrally analyze, investigate and report on all network activity, identify areas with potential security impact, and translate them into secure application enablement policies. Refer to the Panorama Administrator's Guide for more information.

The following additional tasks are not required parts of the main VM-Series for NSX deployment procedure and should only be completed if and when necessary for your deployment.

- **Upgrade the Software Version—**When upgrading the VM-Series firewalls for NSX, you must first upgrade Panorama before upgrading the firewalls. To upgrade the firewalls, see Upgrade the PAN-OS Software Version (VM-Series for NSX).

  - *For upgrading the PAN-OS version on the firewall, do not modify the VM-Series OVA URL in Panorama > VMware Service Manager.*
  - *Do not use the VMware snapshots functionality on the VM-Series firewall for NSX. Snapshots can impact performance and result in intermittent and inconsistent packet loss. See VMware's best practice recommendation with using snapshots. If you need configuration backups, use Panorama or Export named configuration snapshot from the firewall (Device > Set up > Operations). Using the Export named configuration snapshot exports the active configuration (running-config.xml) on the firewall and allows you to save it to any network location.*
- Migrate Your Panorama 7.1 Configuration to 8.0 Configuration—If you upgrade your existing VM-Series firewall for NSX deployment to 8.0 and plan to use the Security Centric workflow going forward, Migrate Panorama 7.1 Configuration to Panorama 8.0 Configuration. After migrating your configuration, continue with the 8.0 Panorama-driven workflow.

If you need to reinstall or remove the VM-Series from your NSX deployment, see the How to Remove VM-Series Integration from VMwareNSX knowledge base article.

Install the VMware NSX Plugin

To deploy the VM-Series for NSX solution, you must install the VMware NSX plugin on Panorama. If you are upgrading to PAN-OS 8.0 and already have integrated VMware NSX and the Palo Alto Networks VM-Series firewalls configured in your environment, the plugin will be installed automatically and your existing configuration is maintained.

If another version of the plugin is currently installed, selecting Install removes it and installs the selected version.

STEP 1 | Download the VMware NSX plugin from the Palo Alto Networks Customer Support website.

STEP 2 | Select **Panorama** > **Plugins**.

1. Select **Upload**.
2. Select **Browse** and locate the plugin file on your management device.
3. Select **Install** in the Action column to install the plugin. Panorama will alert you when the installation is complete.
4. Select the version of the plugin and click **Install** in the Action column to install the plugin. Panorama will alert you when the installation is complete.

When installing the plugin on Panoramas in an HA pair, install the plugin on the passive peer before the active peer. After installing the plugin on the passive peer, it will transition to a non-functional state. Installing the plugin on the active peer returns the passive peer to a functional state.

STEP 3 | If you are upgrading your version of the NSX plugin, complete a manual configuration sync.

1. Select **Panorama** > **VMware NSX** > **Service Managers**.
2. Select **NSX Config-Sync** in the Action column.
3. Click **Yes**.
4. When the sync is complete, click **OK**.

Register the VM-Series Firewall as a Service on the NSX Manager

You need to enable communication between Panorama and the NSX Manager and then register the VM-Series firewall as a service on the NSX Manager. When registered, the VM-Series firewall is added to the list of network services that can be transparently deployed as a service by the NSX Manager.

- Enable Communication Between the NSX Manager and Panorama
- Create Template(s) and Device Group(s) on Panorama
- Create the Service Definitions on Panorama

Enable Communication Between the NSX Manager and Panorama

To automate the provisioning of the VM-Series firewall for NSX, enable communication between the NSX Manager and Panorama. This is a one-time setup, and only needs to be modified if the IP address of the NSX Manager changes or if the capacity license for deploying the VM-Series firewall is exceeded.

In this workflow, you must also install the API key required to complete the deactivation process from Panorama. The API key ensures that the VM-Series firewall licenses are automatically deactivated when you delete a service profile on the NSX Manager, and the licenses/entitlements are credited back to your account so that they become available for use later.

STEP 1 | Log in to the Panorama web interface.

Using a secure connection (https) from a web browser, log in using the IP address and password you assigned during initial configuration (https://<*IP address*>).

STEP 2 | Set up access to the NSX Manager.

1. Select **Panorama** > **VMware NSX** > **Service Managers** and click **Add**.
2. Enter the **Service Manager Name**.

   On the NSX Manager, this name displays in the Service Manager column on **Networking & Security** > **Service Definitions** > **Service Managers**.
3. (Optional) Add a **Description** that identifies the VM-Series firewall as a service.
4. Enter the **NSX Manager URL**—IP address or FQDN—at which to access the NSX Manager.
5. Enter the **NSX Manager Login** credentials—username and password, so that Panorama can authenticate to the NSX Manager.

   The ampersand (&) special character is not supported in the NSX Manager account password. If a password includes an ampersand, the connection between Panorama and NSX Manager fails.

   Any vSphere environment password can impact infrastructure updates and should be accounted for with respect to Panorama. For example, if you change your NSX Manager login password, ensure that you update the password on Panorama immediately. An incorrect password breaks the connection between Panorama and NSX Manager. Panorama does not receive updates about changes to your deployment while disconnected from NSX Manager. Additionally, if you change your vCenter password but do not update it on NSX Manager, Panorama will not receive updates from vCenter. However, the connection status between Panorama and NSX manager will remain Registered.
6. Click **OK**.

STEP 3 | Commit your changes to Panorama.

Select **Commit** and Commit Type: **Panorama**.

STEP 4 | Verify the connection status on Panorama.

Name	Description	NSX Manager URL	NSX Manager Login	Service Definitions	Status	Last Dynamic Update	Action
PAN-SERVICE-MANAGER		[redacted]	admin	PAN-SD-1	Registered	-	Synchronize Dynamic Objects NSX Config-Sync

To view the connection status between Panorama and the NSX Manager.

1. Select **Panorama** > **VMware NSX** > **Service Managers**.
2. Verify the message in the **Status** column.

   When the connection is successful, the status displays as **Registered**. This indicates that Panorama and the NSX Manager are in sync and the VM-Series firewall is registered as a service on the NSX Manager.

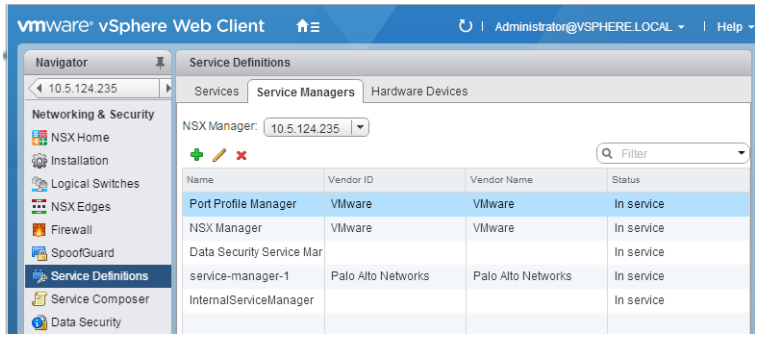
   The unsuccessful status messages are:

   - **Not connected**: Unable to reach/establish a network connection to the NSX Manager.
   - **Not authorized**: The access credentials (username and/or password) are incorrect.
   - **Not registered**: The service, service manager, or service profile is unavailable or was deleted on the NSX Manager.
   - **Out of sync**: The configuration settings defined on Panorama are different from what is defined on the NSX Manager.Click the link for details on the reasons for failure. For example, NSX Manager may have a service definition with the same name as defined on Panorama. To fix the error, use the service definition name listed in the error message to validate the service definition on the NSX Manager. Until the configuration on Panorama and the NSX Manager is synchronized, you cannot add a new service definition on Panorama.
   - **No service/ No service profile**: Indicates an incomplete configuration on the NSX Manager.

   If you make a change and need to manually sync, see (Optional) Synchronize the configuration between Panorama and the NSX Manager.

STEP 5 | Verify that the firewall is registered as a service on the NSX Manager.

1. On the vSphere web client, select **Networking & Security** > **Service Definitions** > **Service Managers**.



2. Verify that **Palo Alto Networks** displays as a vendor in the list of services available for installation.

STEP 6 | Install a License Deactivation API Key.

Complete steps 1 and 2 in the link above to copy the API key from the CSP and install the license deactivation API key on the Panorama CLI. This API key ensures that VM-Series firewalls are automatically deactivated when you delete a Palo Alto Networks Service Deployment on the NSX Manager. So when a firewall is terminated, the licenses are deactivated and credited back to your account.

STEP 7 | If you are running VMware NSX plugin 2.0.4 or later, you can configure Panorama to automatically synchronize dynamic objects with NSX manager as if you issued an **Synchronize Dynamic Objects**. By default, the DAG Sync interval is disabled and the value is set to zero (0). To enable the DAG Sync, set the interval between one hour and 72 hours. Setting a value of zero hours disables the DAG sync. To configure or disable the interval, complete the following procedure.

1. Log in to the Panorama CLI.
2. Execute the following command.

   ```
   request plugins vmware_nsx dag-sync-interval interval <interval-in-hours>
   ```

   You can view the configured value with the following show command.

   ```
   show plugins vmware_nsx dag-sync-interval
   ```

Create Template(s) and Device Group(s) on Panorama

To manage the VM-Series firewalls for NSX using Panorama, the firewalls must belong to a device group and a template. Device groups allow you to assemble firewalls that need similar policies and objects as a logical unit; the configuration is defined using the **Objects** and **Policies** tabs on Panorama. Use templates to configure the settings that are required for the VM-Series firewalls to operate on the network and associate; the configuration is defined using the **Device** and **Network** tabs on Panorama. And each template containing zones used in your NSX configuration on Panorama must be associated with a service definition; at a minimum, you must create a zone within the template so that the NSX Manager can redirect traffic to the VM-Series firewall.

Each virtual wire zone belonging to the NSX-related template becomes available as a *service profile* on the Service Composer on the NSX Manager. When you create NSX-related zone on Panorama, Panorama pushes the zone as a part of the template configuration to the firewall, and the firewall automatically creates a pair of virtual wire subinterfaces, for example ethernet1/1.3 and ethernet 1/2.3, to isolate traffic for a tenant or sub-tenant. On the firewall, you can then Create Security Groups and Steering Rules to secure traffic that arrives on the virtual wire subinterface pair that maps to the zone.

If you are new to Panorama, refer to the Panorama Administrator's Guide for instructions on setting up Panorama.

STEP 1 | Add a device group or a device group hierarchy.

1. Select **Panorama** > **Device Groups**, and click **Add**. You can also create a device group hierarchy.
2. Enter a unique **Name** and a **Description** to identify the device group.
3. Click **OK**.

   After the firewalls are deployed and provisioned, they will display under **Panorama** > **Managed Devices** and will be listed in the device group.
4. Click **Commit** and select **Panorama** as the **Commit Type** to save the changes to the running configuration on Panorama.

STEP 2 | Add a template or a template stack.

1. Select **Panorama** > **Templates**, and click **Add**. You can also configure a template stack.
2. Enter a unique **Name** and a **Description** to identify the template.
3. Click **OK**.
4. Click **Commit**, and select **Panorama** as the **Commit Type** to save the changes to the running configuration on Panorama.

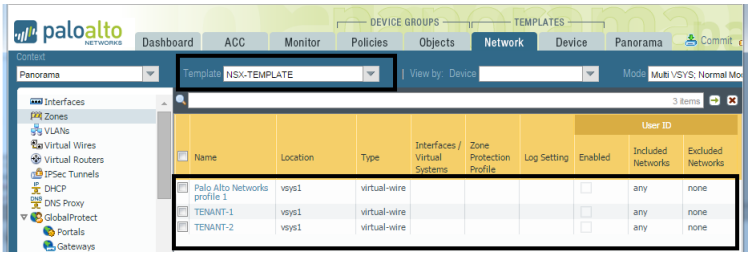
STEP 3 | Create the zone(s) for each template.

Each zone is mapped to a service profile on NSX Manager. To qualify, a zone must be of the virtual wire type and in a template or member template of a template stack associated with a service definition.

For a single-tenant deployment, create one zone. If you have multi-tenant deployment, create a zone for each sub-tenant.

You can add up to 32 zones in each template.

1. Select **Network** > **Zones**.
2. Select the correct template in the **Template** drop-down.
3. Select **Add** and enter a zone **Name**.
4. Set the interface **Type** to **Virtual Wire**.
5. Click **OK**.
6. Verify that the zones are attached to the correct template.



7. Click **Commit**, and select **Panorama** as the **Commit Type** to save the changes to the running configuration on Panorama.

   Panorama creates a corresponding service profile on NSX Manager for each qualified zone upon commit.

Create the Service Definitions on Panorama

A service definition specifies the configuration for the VM-Series firewalls installed on each host in an ESXi cluster. The service definition must include the device group, the license auth-codes for deploying the VM-Series firewalls, and a template with one or more NSX service profile zones. Typically, you create a service definition for the VM-Series firewall in an ESXi cluster. If you have different ESXi clusters that have workloads that require the VM-Series firewall to handle traffic differently, you can create multiple service definitions on Panorama.

On a Panorama commit, each service definition is registered on the NSX Manager. On registration with the NSX Manager, the NetX API implementation makes each zone (defined within the template) available for redirecting traffic. When you deploy the VM-Series firewalls, you can select the profile name for the VM-Series firewall(s) to which you want to redirect traffic from the objects in NSX security groups. The appropriately configured firewall can then inspect the traffic and enforce policy from the virtual machines that belong to the NSX security groups.

STEP 1 | (Optional) Configure a Notify Group

Create a notify group by specifying devices groups that should be notified of changes in the virtual environment. The firewalls included in the specified device groups receive a real-time update of security groups and IP addresses of guest VMs in them. The firewalls use this update to determine the most current list of members that constitute dynamic address groups referenced in policy

1. Select **Panorama** > **VMware NSX** > **Notify Group** and click **Add**.
2. Give your Notify Group a descriptive **Name**.

3. Select the boxes of all devices groups that should be notified of changes to the virtual environment. If a device group does not have a check box available, it means that the device group is automatically included by virtue of the device group hierarchy.
4. Click **OK**.

STEP 2 | Add a new service definition.

You can create up to 32 service definitions on Panorama.

1. Select **Panorama** > **VMware NSX** > **Service Definitions**.
2. Select **Add** to create a new service definition. The maximum number of characters in a service definition name is 40.

   On the NSX Manager, this service definition name displays in the Services column on **Networking & Security** > **Service Definitions** > **Services**.
3. (Optional) Add a **Description** that identifies the function or purpose for the VM-Series firewalls that will be deployed using this service definition.

STEP 3 | Assign a device group and a template for the service definition.

Make sure to Create the zone(s) for each template.

Because the firewalls deployed in this solution will be centrally administered from Panorama, you must specify the **Device Group** and the **Template** that the firewalls belong to. All the firewalls that are deployed using this service definition belong to the specified template and device group.

1. Select the device group or device group hierarchy in the **Device Group** drop-down.
2. Select the template or the template stack in the **Template** drop-down.

You cannot reuse a template or a device group assigned to one service definition in another service definition.

STEP 4 | Specify the location of the OVF file.

Download the zip file, unzip it to extract and save the .ovf, mf and .vmdk files to the same directory. Both the files are used to deploy each instance of the firewall.

If needed, modify the security settings on the server so that you can download the file types. For example, on the IIS server modify the Mime Types configuration; on an Apache server edit the .htaccess file.

In **VM-Series OVF URL**, add the location of the web server that hosts the ovf file. Both http and https are supported protocols. For example, enter **https://acme.com/software/PA-VM-NSX.8.0.0.ovf**

Select the ovf file that matches the VM-Series model you plan to deploy. For the VM-200, use vm100.ovf. For the VM-1000-HV, use vm300.ovf.

To deploy a multi-tenant solution, the ovf file must be PAN-OS 8.0.0 or a later version.

You can use the same ovf version or different versions across service definitions. Using different ovf versions across service definitions allows you to vary the PAN-OS version on the VM-Series firewalls in different ESXi clusters.

STEP 5 | (Optional) Select a Notify Group.

To create context awareness between the virtual and security environments so that policy is consistently applied to all traffic steered to the firewalls, select the device groups to notify when there are changes in the virtual environment.

Select each device group to which you want to enable notifications in the **Notify Device Groups** drop-down. If a device group does not have a checkbox available, it means that the device group is automatically included by virtue of the device group hierarchy.

The firewalls included in the specified device groups receive a real-time update of security groups and IP addresses. The firewalls use this update to determine the most current list of members that constitute dynamic address groups referenced in policy.

STEP 6 | Save the service definition and attach it to the service manager.

1. Click **OK**.
2. Select **Panorama** > **VMware NSX** > **Service Manager** and click the link of the service manager name.
3. Under Service Definitions, click **Add** and select your service definition from the drop-down.
4. Click **OK**.
5. Select **Commit** and Commit Type: **Panorama**.

   Committing the changes triggers the process of registering each service definition as a security service on the NSX Manager.

STEP 7 | Add the authorization code to license the firewalls.

The auth-code must be for the VM-Series model NSX bundle; for example, PAN-VM-300-PERP- BND-NSX.

Verify that the order quantity/ capacity is adequate to support the number of firewall you need to deploy in your network.

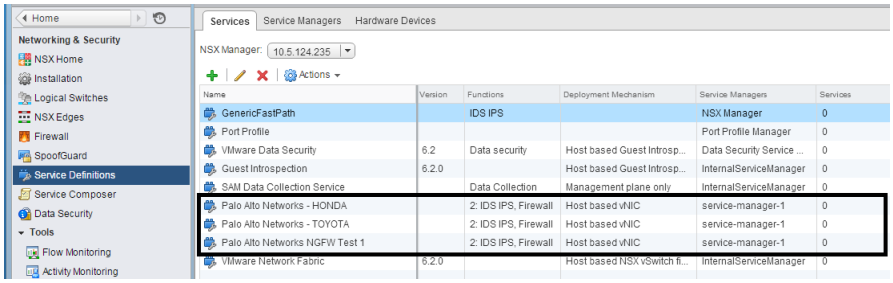
1. Select **Panorama** > **Device Groups** and choose the device group you associated with the service definition you just created.
2. Under Dynamically Added Device Properties, add the authorization code you received with your order fulfillment email and select a PAN-OS software version from the SW Version drop-down.

   When a new firewall is deployed under NSX and added to the selected device group, the authorization code is applied and the firewall is upgraded to the select version of PAN-OS.

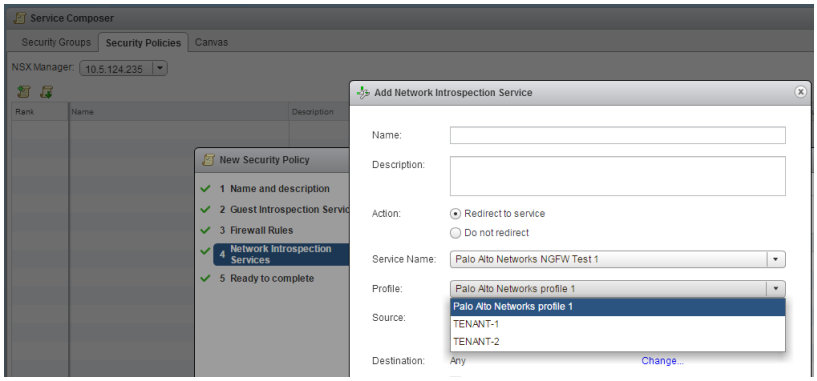
   On the support portal, you can view the total number of firewalls that you are authorized to deploy and the ratio of the number of licenses that have been used to the total number of licenses enabled by your auth-code.
3. Synchronize the configuration between Panorama and the NSX Manager.
   1. Select **Panorama** > **VMware NSX** > **Service Managers**.
   2. Select **NSX Config-Sync** under the Actions column.
   3. Click **Yes** to confirm the sync.

STEP 8 | Verify that the service definition and the NSX service profile that you defined on Panorama are registered on the NSX Manager.

1. On the NSX Manager, to verify that the service definition is available, select **Networking & Security** > **Service Definitions** > **Services**. The service definition is listed as a Service on the NSX Manager.



2. To verify that the zones are available on the NSX Manager:
    1. Select **Networking and Security** > **Service Composer** > **Security Policies**, and click **Create Security Policy**.
    2. Select **Network Introspection Services**, and click **Add**.
    3. In the **Service Name** drop-down, select a Palo Alto Networks service that you verified in the step above.
    4. In the **Profile** drop-down, verify that you can view all the zones you defined for that service definition on Panorama.



STEP 9 | (Optional) Synchronize the configuration between Panorama and the NSX Manager.

If you add or update the service definitions configured on Panorama, select **NSX Config Sync** in the Action column under **Panorama** > **VMware NSX** > **Service Managers** to synchronize the changes on the NSX Manager.

This link is not available, if you have any pending commits on Panorama.

If the synchronization fails, view the details to know whether to fix the error on Panorama or on the NSX Manager. For example, if you delete a service definition on Panorama, but the service definition cannot be deleted from the NSX Manager because it is referenced in a rule on the NSX Manager, the synchronization will fail with an error message that indicates the reason for failure.

Deploy the VM-Series Firewall

After registering the VM-Series firewall as a service (Palo Alto Networks NGFW) on the NSX Manager and creating security groups and steering rules, complete the following tasks on the NSX Manager.

- Enable SpoofGuard
- Define an IP Address Pool (Required only if the management interface is not configured for DHCP)
- Prepare the ESXi Host for the VM-Series Firewall
- Deploy the Palo Alto Networks NGFW Service
- Enable Large Receive Offload

Support for vMotion of guest virtual machines in the vSphere/NSX Environment

When a guest VM is vMotioned from one host to another within a cluster, the target host NSX distributed firewall will steer all new sessions to the VM-Series firewall on the destination host. To ensure that all active (existing sessions) remain uninterrupted during and after the guest vMotion, the NSX Manager polls the VM-Series firewall for existing allowed sessions and then shares these sessions with the NSX distributed firewall on the destination host. All existing sessions that were allowed by the original VM-Series will be allowed by the NSX distributed firewall (filtering module) on the destination host without steering to the target host VM-Series firewall to prevent session loss.

The VM-Series firewall runs as a service on each host of the cluster and therefore is never vMotioned.

Enable SpoofGuard

The NSX distributed firewall can only redirect traffic to the VM-series firewall when it matches an IP address that is known to the vCenter Server. This means that any non-IP L2 traffic, or IP traffic that does not match the IP addresses known to the vCenter Server, will not match the redirection rules defined on the NSX Manager and be steered to the VM-Series firewall. Therefore, to ensure that all traffic is correctly filtered, you need to perform the following steps:

- Enable SpoofGuard to prevent unknown IP traffic that might otherwise bypass the VM-series firewall.

  When SpoofGuard is enabled if the IP address of a virtual machine changes, traffic from the virtual machine will be blocked until you inspect and approve the change in IP address in the NSX SpoofGaurd interface.
- Configure the NSX firewall rules to block non-IP L2 traffic that cannot be steered to the VM-Series firewall.

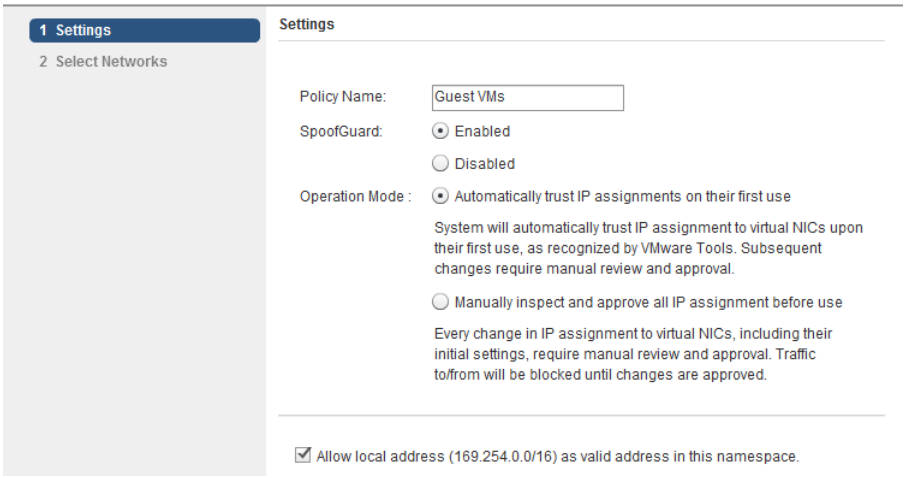
vCenter uses VMware Tools to learn the IP address(es) of each guest. If VMware Tools is not installed on some of your guests, see Steer Traffic from Guests that are not Running VMware Tools.

STEP 1 | Enable SpoofGuard for the port group(s) containing the guests.

When enabled, for each network adapter, SpoofGuard inspects packets for the prescribed MAC and its corresponding IP address.

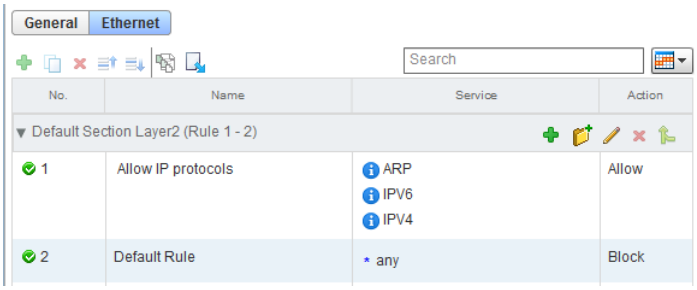
1. Select **Networking and Security** > **SpoofGuard**.
2. Click **Add** to create a new policy, and select the following options:
   - SpoofGuard: **Enabled**

- Operation Mode: **Automatically trust IP assignments on their first use**.
- **Allow local address as valid address in this namespace**.
- Select Networks: Select the port groups to which the guests are connected.



STEP 2 | Select the IP protocols to allow.

1. Select **Networking and Security** > **Firewall** > **Ethernet**.
2. **Add** a rule that allows **ARP**, **IPv4** and **IPv6** traffic.
3. **Add** a rule that blocks everything else.



Define an IP Address Pool

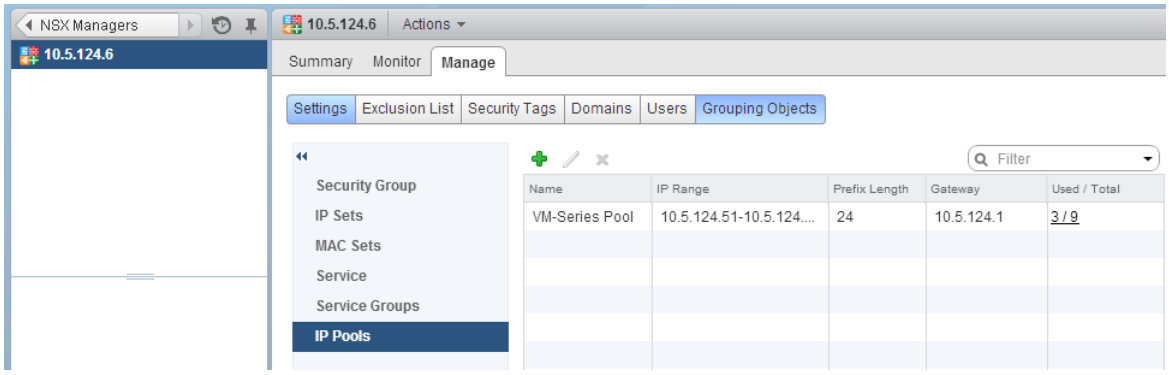
You can configure the management interface on the VM-Series firewall to use an IP address from a static IP pool or to be a DHCP client.

If you opt to use an IP pool, which is a range of (static) IP addresses that are reserved for establishing management access to the VM-Series firewalls, when the NSX Manager deploys a new VM-Series firewall, the first available IP address from this range is assigned to the management interface of the firewall.

STEP 1 | In the **Networking & Security Inventory**, select the **NSX Manager**, and double click to open the configuration details of the NSX Manager.

STEP 2 | Select **Manage** > **Grouping Objects** > **IP Pools**.

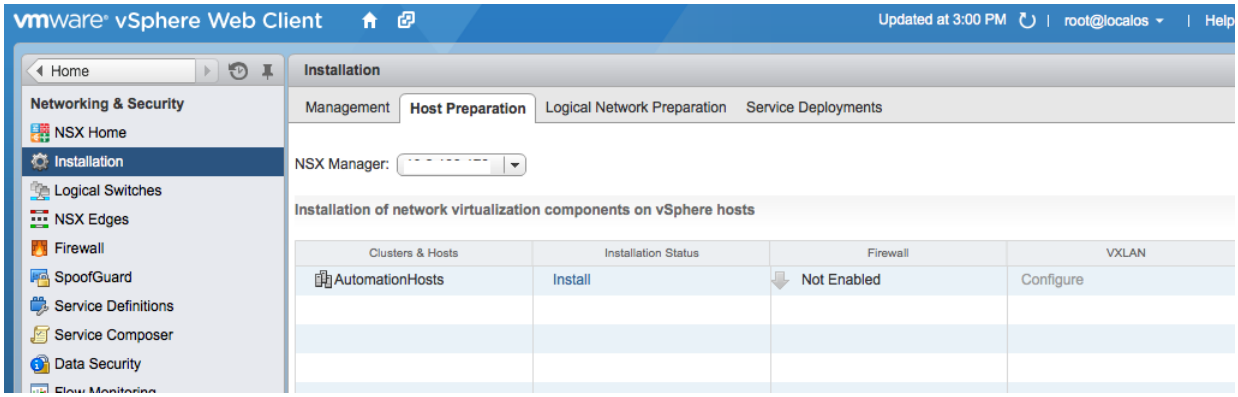
STEP 3 | Click **Add IP Pool** and specify the network access details requested in the screen including the range of static IP addresses that you want to use for the Palo Alto Networks NGFW.



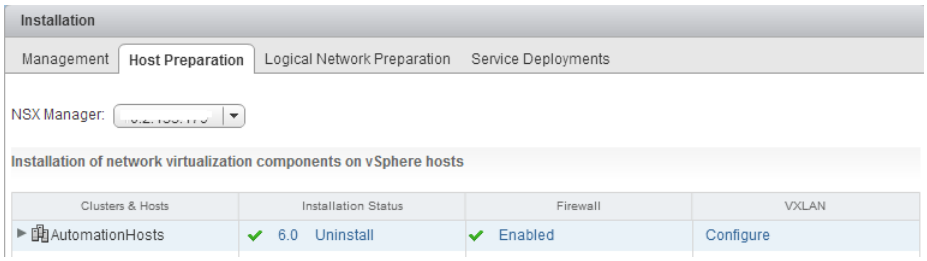
Prepare the ESXi Host for the VM-Series Firewall

Before you deploy the VM-Series firewall, each host in the cluster must have the necessary NSX components that allow the NSX firewall and the VM-Series firewall to work together. The NSX Manager will install the components— the Ethernet Adapter Module (.eam) and the SDK —required to deploy the VM-Series firewall.

STEP 1 | On the NSX Manager, select **Networking and Security** > **Installation** > **Host Preparation**.

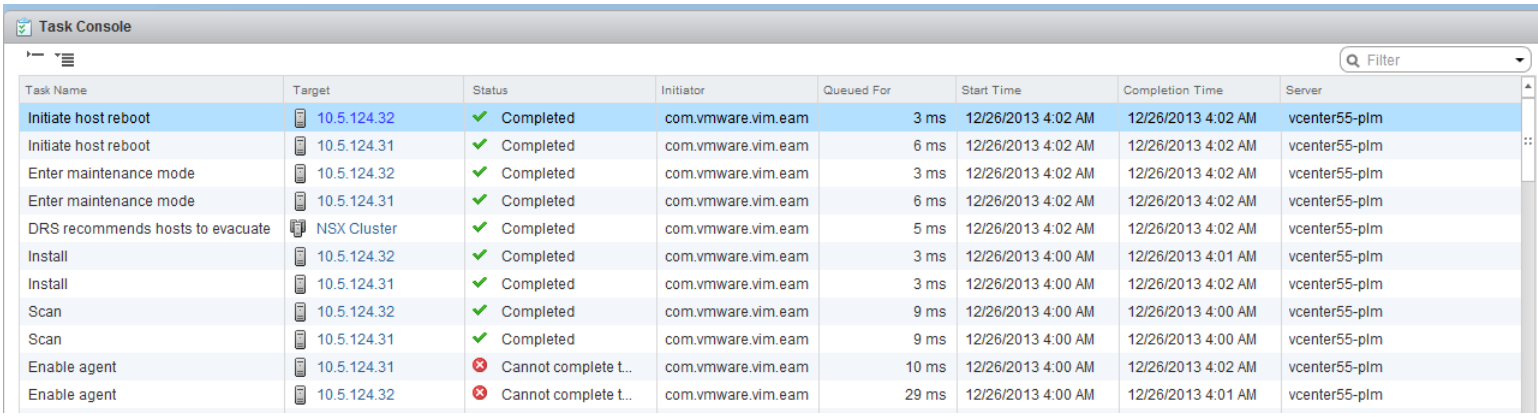


STEP 2 | Click **Install** and verify that the installation status is successful.



As new ESXi hosts are added to a cluster, this process is automated and the necessary NSX components are automatically installed on each guest on the ESXi host.

STEP 3 | If the Installation Status is not ready or a warning displays on screen, click the **Resolve** link. To monitor the progress of the re-installation attempt, click the **More Tasks** link and look for the successful completion of the following tasks:

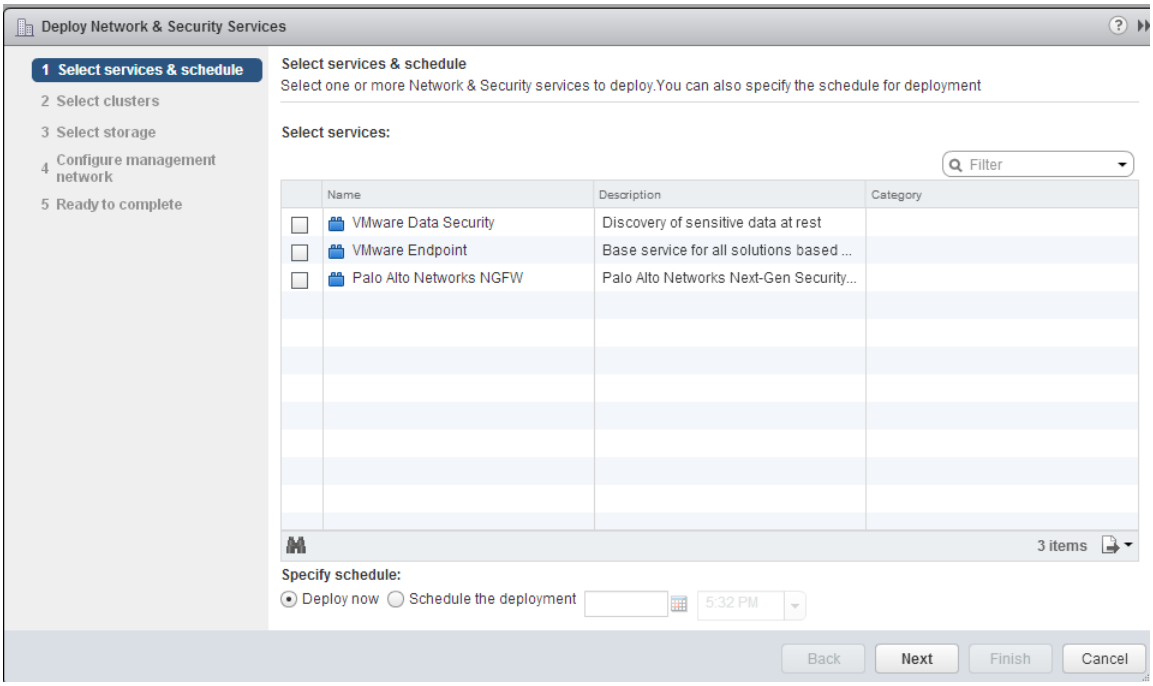


Deploy the Palo Alto Networks NGFW Service

Use the following steps to automate the process of deploying an instance of the VM-Series firewall for NSX on each ESXi host in the specified cluster.

STEP 1 | Select **Networking and Security** > **Installation** > **Service Deployments**.

STEP 2 | Click **New Service Deployment** (green plus icon), and select the service definition for the Palo Alto Networks next generation firewall you want to deploy, **Palo Alto Networks NGFW** service in this example. Click **Next**.

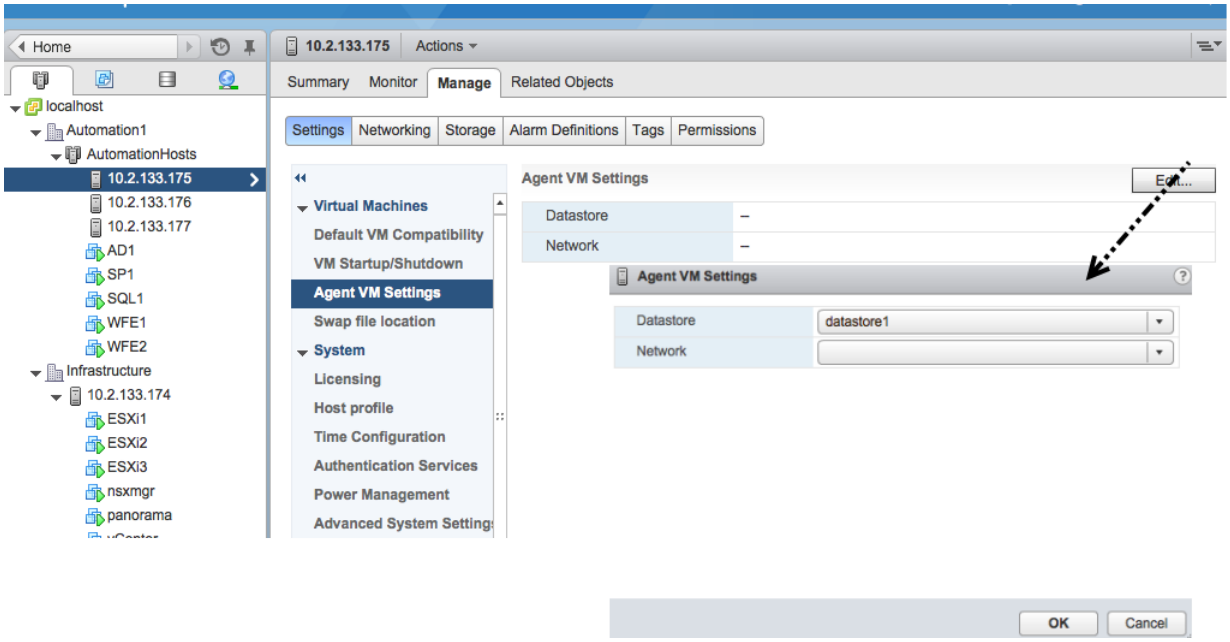


STEP 3 | Select the **Datacenter** and the cluster(s) on which the service will be deployed. One instance of the firewall will be deployed on each host in the selected cluster(s).

STEP 4 | Select the datastore from which to allocate disk space for the firewall. Select one of the following options depending on your deployment:

- If you have allocated shared storage for the cluster, select an available shared datastore.

- If you have not allocated shared storage for the cluster, select the **Specified-on-host** option. Be sure to select the storage on each ESXi host in the cluster. Also select the network that will be used for the management traffic on the VM-Series firewall.



STEP 5 | Select the port group that provides management network traffic access to the firewall.

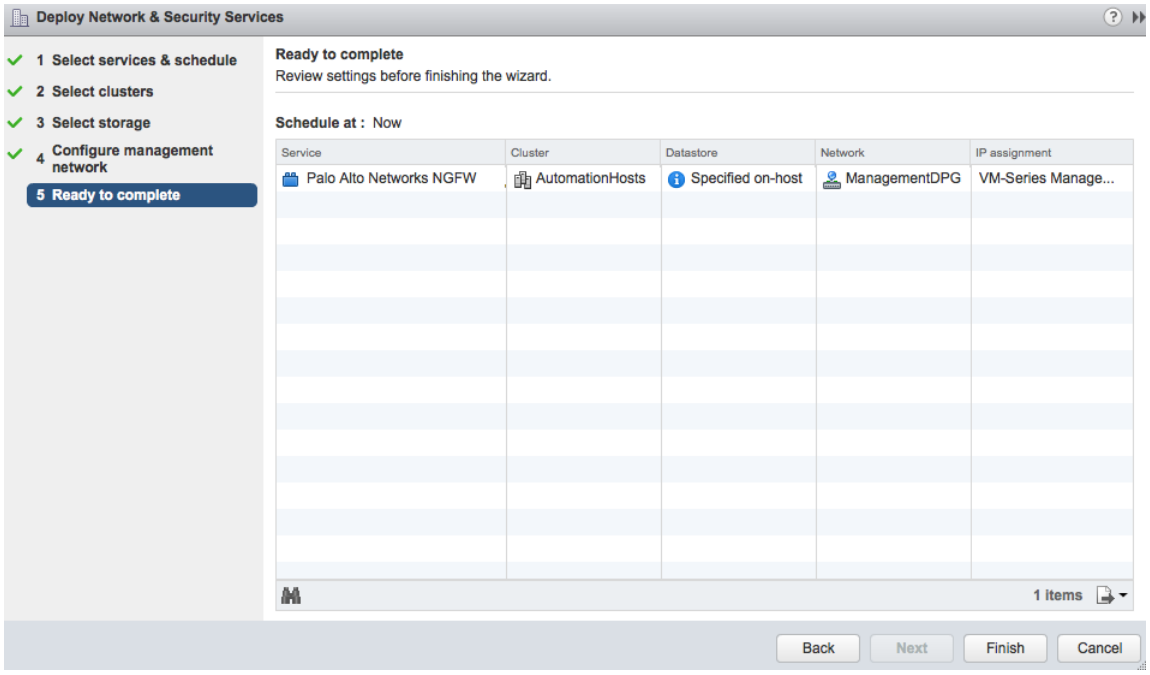
STEP 6 | Select the IP address pool assignment.

- **Use IP Pool** (Define an IP Address Pool) from which to assign a management IP address for each firewall when it is being deployed.
- **Use DHCP** on the management interface.

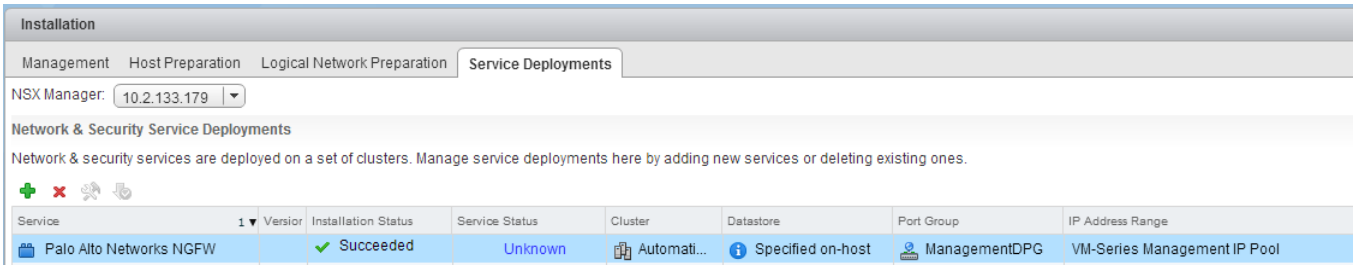
If you use an IP pool, on deployment, the display name for the VM-Series firewall on Panorama includes the hostname of the ESXi host. For example: PA-VM:10.5.1.120.

If you use DHCP, the display name for the VM-Series firewall does not include the name of the ESXi host.

STEP 7 | Review the configuration and click **Finish**.



STEP 8 | Verify that the NSX Manager reports the **Installation Status** as **Successful**. This process can take a while; click the **More tasks** link on vCenter to monitor the progress of the installation.

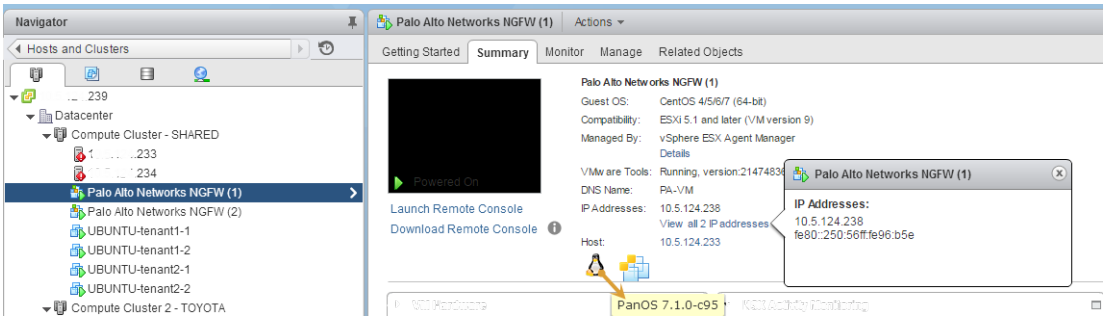


If the installation of VM-Series fails, the error message is displayed on the Installation Status column. You can also use the Tasks tab and the Log Browser on the NSX Manager to view the details for the failure and refer to the VMware documentation for troubleshooting steps.

STEP 9 | Verify that the firewall is successfully deployed.

1. On the vCenter server, select **Hosts and Clusters** to check that every host in the cluster(s) has one instance of the firewall.
2. View the management IP address(es) and the PAN-OS version running on the firewall directly from vCenter server. VMware Tools is bundled with the PAN-OS software image and is automatically enabled when you launch the VM-Series firewall.

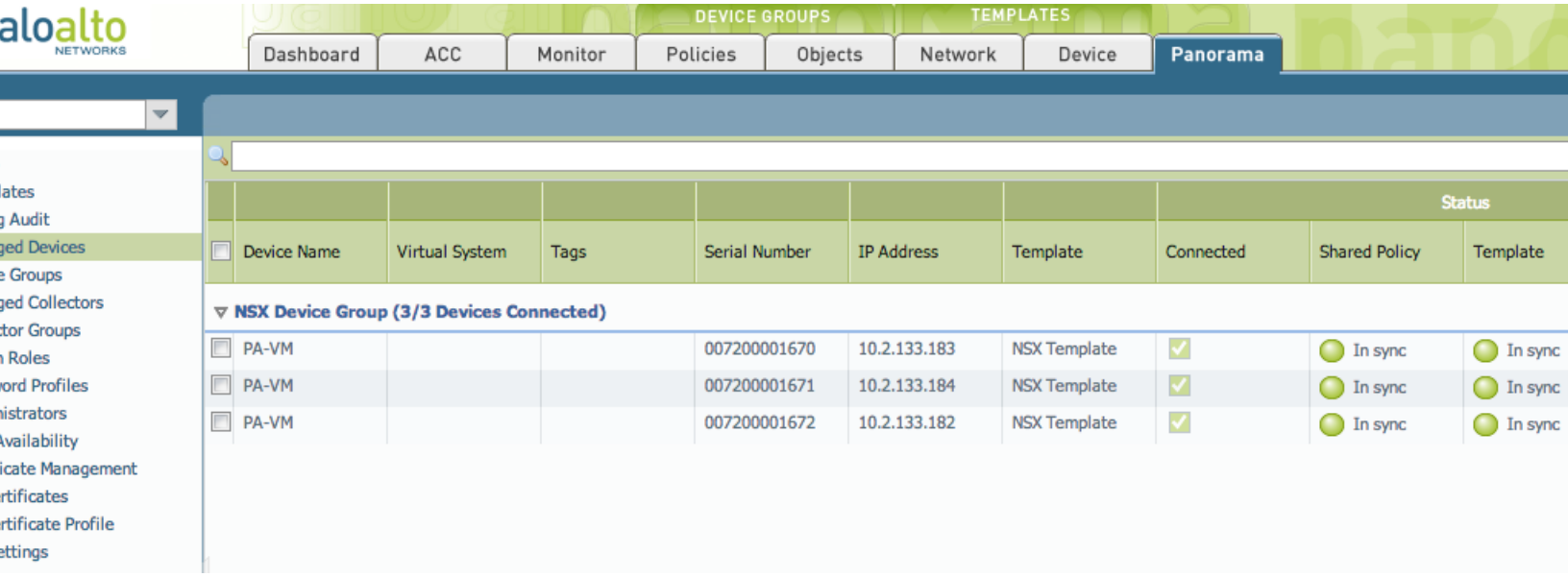
   With VMware Tools, you can view resource utilization metrics on hard disk, memory, and CPU, and use these metrics to enable alarms or actions on the vCenter server. The heartbeats allow you to verify that the firewall is live and trigger actions to ensure high availability. You can also perform a graceful shutdown and restart of the firewall using the power off function on vCenter.



STEP 10 | Access the Panorama web interface to make sure that the VM-Series firewalls are connected and synchronized with Panorama.

1. Select **Panorama** > **Managed Devices** to verify that the firewalls are connected and synchronized.

   If the firewall gets its IP address from an IP Pool, the **Display Name** for the firewall includes the hostname of the ESXi server on which it is deployed, for example PA-VM:ESX1.Sydney. If the firewall gets a DHCP assigned IP address, the hostname of the ESXi server does not display.



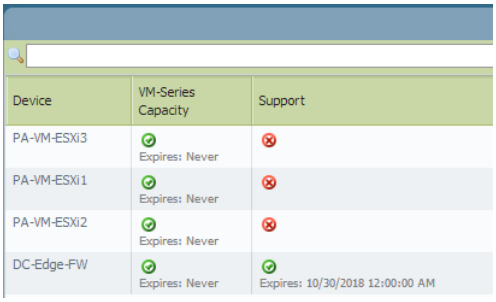
2. Click Commit, and select Commit Type as **Panorama**.

A periodic Panorama commit is required to ensure that Panorama saves the device serial numbers to configuration. If you reboot Panorama without committing the changes, the managed devices will not connect back to Panorama; although the Device Group will display the list of devices, the devices will not display in Panorama > Managed Devices.

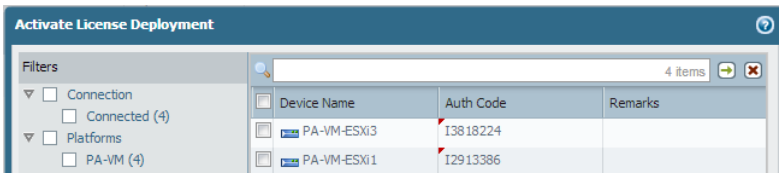
STEP 11 | Verify that the capacity license is applied and apply any additional licenses that you have purchased. At a minimum, you must activate the support license on each firewall.

When Panorama does not have internet access (Offline), you must manually license each firewall, and then add the serial number of the firewall to Panorama so that it is registered as a managed device, and can receive the template and device group settings from Panorama. See Activate the License for the VM-Series Firewall for VMware NSX for more information.

1. Select **Panorama** > **Device Deployment** > **Licenses** to verify that the VM-Series capacity license is applied.



2. To apply additional licenses on the VM-Series firewalls:
   - Click **Activate** on **Panorama** > **Device Deployment** > **Licenses**.
   - Find or filter for the firewall, and in the **Auth Code** column, enter the authorization code for the license to activate. Only one authorization code can be entered at a time, for each firewall.

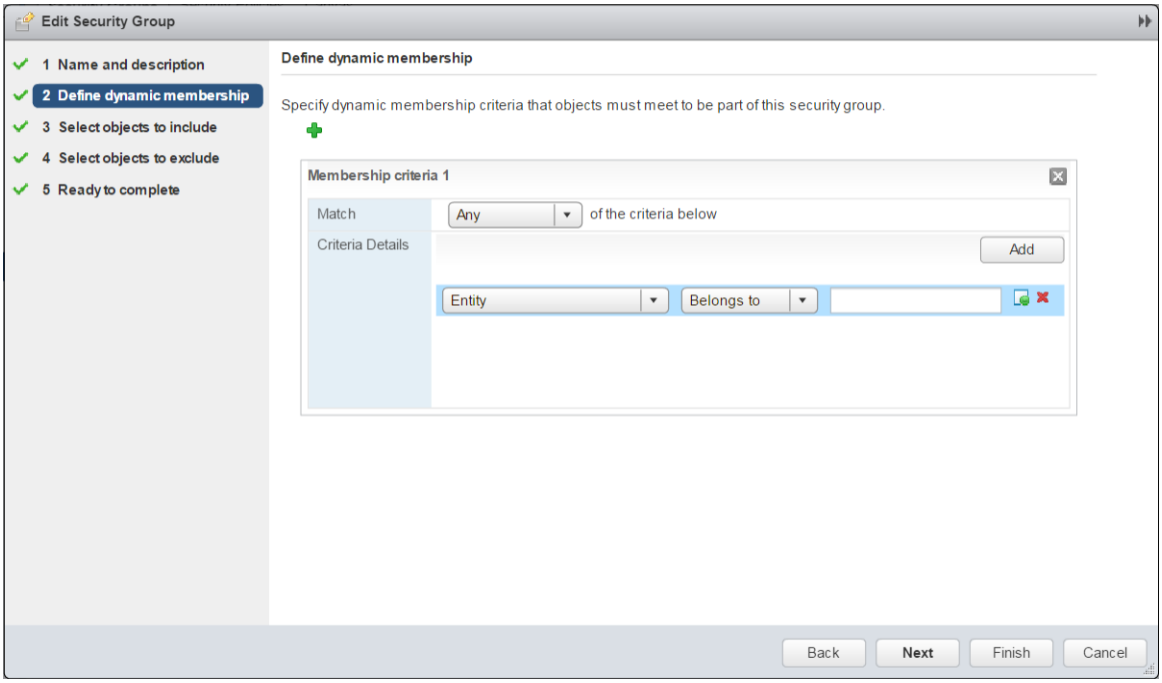


3. Click **Activate**, and verify that the result of the license activation was successful.

STEP 12 | (Optional) Upgrade the PAN-OS version on the VM-Series firewalls, see Upgrade the PAN-OS Software Version (VM-Series for NSX).

STEP 13 | Add guest VMs to the right security groups for traffic from those VMs to be redirected to the VM-Series firewall.

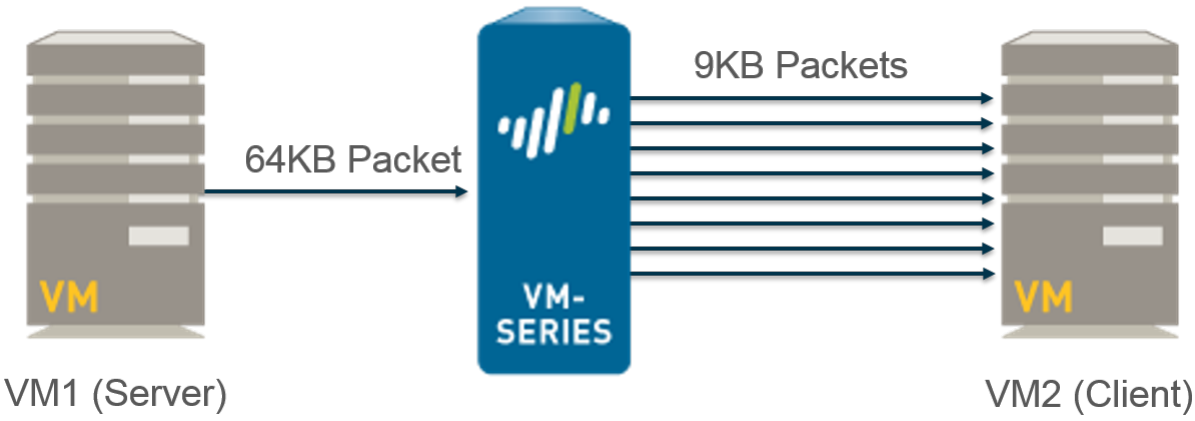
1. Log in to vCenter.
2. Select **Networking & Security** > **Service Composer** > **Security Groups**.
3. Highlight the security group to which you want to assign guest VMs and click the **Edit Security Group** icon.
4. Select **Define dynamic membership** and click the + icon.
5. Click **Add**.
6. Define the dynamic membership criteria that the guest VMs must meet to be part of the selected security group. The criteria you use depends on your network deployment. For example, you might choose to group VMs by an Entity such as Logical Switch or Distributed Port Group.



7. Click **Finish**.
8. Repeat this procedure for each security group that should have its traffic redirected to the VM-Series firewall.

Enable Large Receive Offload

Large receive offload (LRO) is a technique for increasing the inbound throughput on high-bandwidth network connections by decreasing CPU overhead. Without LRO, the firewall drops packets larger than the configured maximum transmission unit MTU, which is a maximum of 9216 bytes when the firewall is enabled for jumbo frames. With LRO enabled, the firewall accepts packets up to 64KB in size and the does not drop packets larger than the configured MTU. Instead, it segments the larger packets into smaller chunks of 9000 bytes. For example, if the VM1 sends a 64KB packet to VM2 and the packet is divided into eight segments.



LRO is disabled by default on new NSX deployments and on upgrade to 8.0. You can enable or disable LRO and view the LRO status on through the CLI. Enabling LRO on the VM-Series firewall automatically enables jumbo frames. Additionally, LRO and TCP Segmentation Offload (TSO) must be enabled on VMXNET3 network adapter on the VM-Series firewall host machine.

STEP 1 | Verify that large receive offload and TCP segmentation offload is enabled on the host.

For information about LRO and TSO on the host machine, see the VMware vSphere documentation.

1. Log in to vSphere and navigate to your host machine.
2. Select **Manage** > **Settings** > **System** > **Advanced System Settings.**
3. Locate the following parameters and verify that their value is set 1. A 1 indicates that the parameter is enabled on the VMXNET3 adapter.
   - For LRO—Net.Vmxnet3HwLRO
   - For TSO—Net.UseHwTSO and Net.UseHwTSO6

STEP 2 | Enable LRO on the VM-Series firewall.

1. Access the firewall CLI.
2. Use the following command to enable LRO:

```
admin@PA-VM> set
system setting lro enable
```

3. Reboot the firewall using the following command:

```
> request restart
system
```

4. Verify the LRO is enabled with the following command:

```
admin@PA-VM> show
system setting lro
Device LRO mode:                          on
Current device mtu size:                  9192
```

You can disable LRO using the command ***set system setting lro disable****.*

Create Security Groups and Steering Rules

The following topics describe how to create security groups and policies to steer traffic to the VM-Series firewall. Follow the link below that matches your deployment process—Security Centric or Operations Centric.

- Create Security Groups and Steering Rules in a Security Centric Deployment
- Create Security Groups and Steering Rules in an Operations Centric Deployment

Create Security Groups and Steering Rules in a Security Centric Deployment

The following topics describe how to create policies on Panorama to steer traffic to the VM-Series firewall. In order for the VM-Series firewall to secure traffic, you must complete the following tasks:

- Set Up Dynamic Address Groups on Panorama
- Create Steering Rules on Panorama

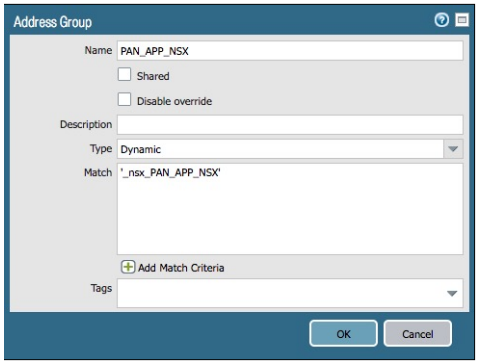
Set Up Dynamic Address Groups on Panorama

A security group is a logical container that assembles guests across multiple ESXi hosts in the cluster. When you create a dynamic address group that meets the right criteria and commit your changes, a corresponding security group is created on the NSX Manager. Creating security groups are required to manage and secure the guests; to understand how security groups enable policy enforcement, see Policy Enforcement using Dynamic Address Groups.

STEP 1 | Configure a dynamic address group for each security group required for your deployment.

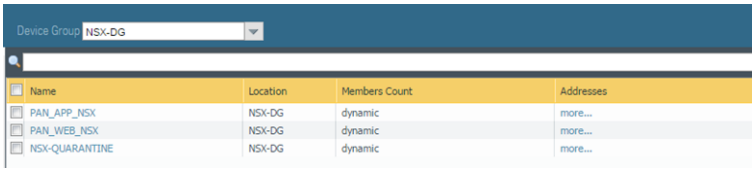
Shared dynamic address groups are not supported on the VM-Series for VMware NSX.

1. Select **Objects** > **Address Groups**.
2. Verify that you are configuring the dynamic address groups in a device group associated with an NSX service definition.
3. Click **Add** and enter a **Name** and **Description** for the address group.
4. Select **Type** as **Dynamic**.
5. Define the match criteria.



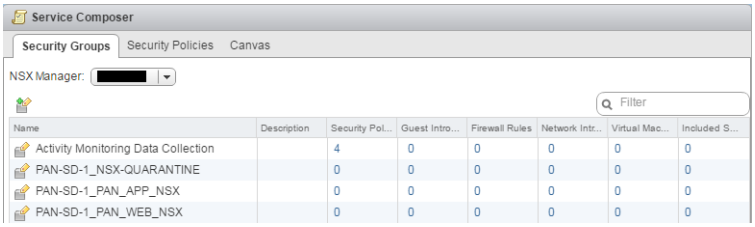
For the dynamic address group to become a security group in NSX Manager, the match criteria string must be enclosed in single quotes with the prefix _nsx_ followed by the exact name of the Address Group. For example, ***'_nsx_PAN_APP_NSX'****.*

6. Repeat this process for each security group you require.



STEP 2 | Verify that the corresponding security groups are created on the NSX Manager.

1. Select **Network and Security** > **Service Composer** > **Security Groups**.
2. Verify that your dynamic address groups appear as security groups on the Security Groups list. Each security group is prefixed with your service definition followed by an underscore and the dynamic address group name.



Create Steering Rules on Panorama

Do **not** apply the traffic redirection policies unless you understand how rules work on the NSX Manager as well as on the VM-Series firewall and Panorama. The default policy on the VM-Series firewall is set to *deny all* traffic, which means that all traffic redirected to the VM-Series firewall will be dropped. To create policies on Panorama and push them to the VM-Series firewall, see Apply Policies to the VM-Series Firewall.

Create security policy rules in the associated device group. For each security rule set the Rule Type to Intrazone, select one zone in the associated template, and select the dynamic address groups as the source and destination. Creating a qualifying security policy in Panorama helps in the creation of a corresponding steering rule on NSX Manager upon steering rule generation and commit in Panorama.

STEP 1 | Create security policy.

1. In Panorama, select **Policies** > **Security** > **Pre Rules**.
2. Verify that you are configuring the dynamic address groups in a device group associated with an NSX service definition.
3. Click **Add** and enter a **Name** and **Description** for your security policy rule.
4. Set the Rule Type to **intrazone (Devices with PAN-OS 6.1 or later)**.
5. In the Source tab, set the source zone to the zone from the template associate with the service definition. Then select a dynamic address group (NSX security group) you created previously as the Source Address. Do not add any static address groups, IP ranges, or netmasks as a Source Address.
6. In the Destination tab, Panorama does not allow you to set a destination zone because you set the rule type to intrazone. Then select a dynamic address group (NSX security group) you created previously as the Destination Address. Do not add any static address groups, IP ranges, or netmasks as a Destination Address.
7. Click **OK**.
8. Repeat steps 1 through 7 for each steering rule you require.
9. **Commit** your changes.

	Name	Location	Tags	Type	Source				Destination	
					Zone	Address	User	HIP Profile	Zone	Address
1	STEERING-RULE-1	NSX-DG	none	intrazone	PAN_NSX_1	PAN_APP_NSX	any	any	(intrazone)	PAN_WEB_NSX
2	STEERING-RULE-2	NSX-DG	none	intrazone	PAN_NSX_1	PAN_WEB_NSX	any	any	(intrazone)	PAN_APP_NSX

STEP 2 | Generate steering rules.

Panorama generates a steering rule for each qualifying security policy rule.

1. Select **Panorama** > **VMware NSX** > **Steering Rules**.
2. Select **Auto-Generate Steering Rules**.

   Panorama will populate the list of steering rules based on qualified security policy rules in the device group attached in the service definition.

Name	Description	NSX Traffic Direction	Device Group	Security Policy
auto_NSX_DG_STEERING_RULE_1		inout	NSX-DG	STEERING-RULE-1
auto_NSX_DG_STEERING_RULE_2		inout	NSX-DG	STEERING-RULE-2

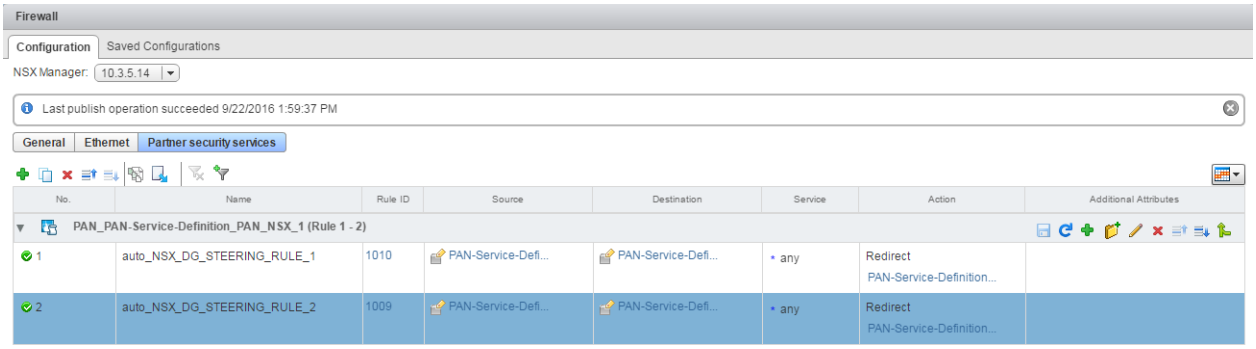
3. (Optional) Modify the NSX Traffic Direction and add NSX Services to a Steering Rule.

   By default, the NSX Traffic Direction is set to **inout** and no NSX Services are selected. When no NSX Services are specified, any type of traffic is redirected to the VM-Series firewall.

   1. Select the auto-generated steering to be modified.
   2. To change the traffic direction, select the direction from the **NSX Traffic Direction** drop-down.
   3. Click **Add** under NSX Services and choose a service from the **Services** drop-down. Repeat this step to add additional services.
   4. Click **OK**.
4. **Commit** your changes.

STEP 3 | Verify that the corresponding traffic steering rules were created on the NSX Manager.

1. Select **Network and Security** > **Firewall** > **Configuration** > **Partner Security Services**.
2. Confirm that the traffic steering rules your created on Panorama are listed.



Create Security Groups and Steering Rules in an Operations Centric Deployment

In an operations-centric deployment, you create security groups and traffic redirection rules on the NSX Manager instead of Panorama. Then your security rules configured on Panorama enforce the traffic redirected to the VM-Series firewall. Complete the following tasks when deploying the VM-Series firewall for NSX in an operations-centric deployment:

- Set Up Security Groups on the NSX Manager
- Create Steering Rules on NSX Manager

Set Up Security Groups on the NSX Manager

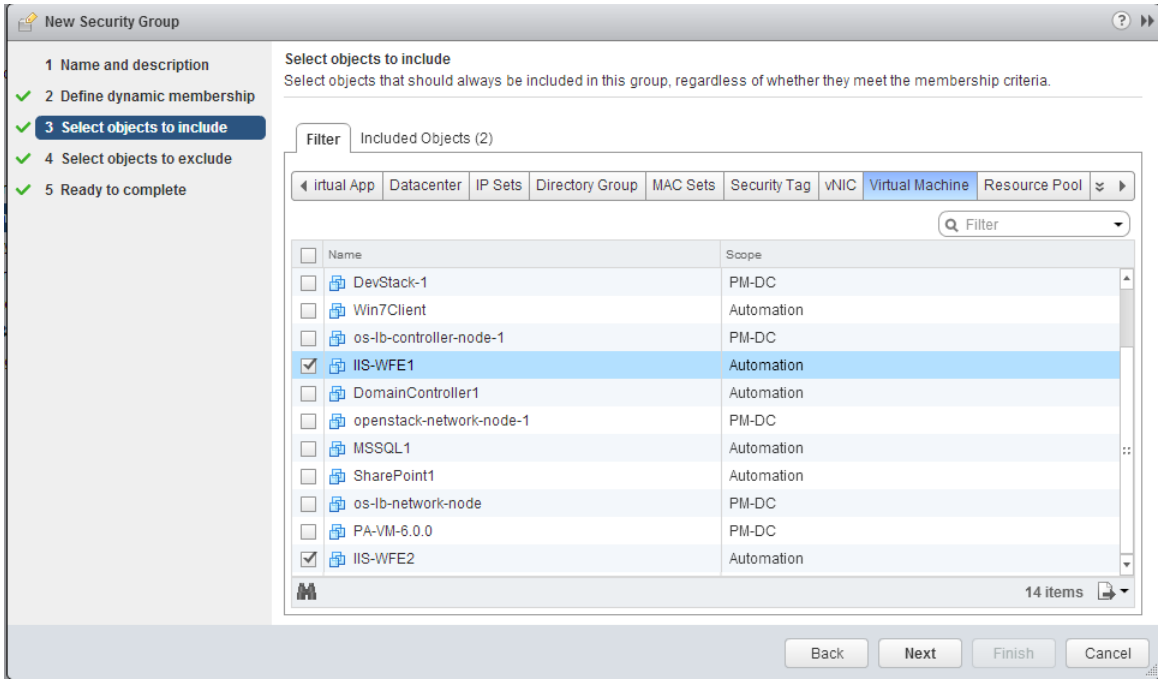
A security group is a logical container that assembles guests across multiple ESXi hosts in the cluster. Creating security groups makes it easier to manage and secure the guests; to understand how security groups enable policy enforcement, see Policy Enforcement using Dynamic Address Groups.

STEP 1 | Log in to the vSphere user interface.

STEP 2 | Select **Networking and Security** > **Service Composer** > **Security Groups**, and add a **New Security Group**.

STEP 3 | Add a **Name** and **Description**. This name will display in the match criteria list when defining dynamic address groups on Panorama.

STEP 4 | Select the guests that constitute the security group. You can either add members dynamically or statically. You can **Define Dynamic Membership** by matching on security tags (recommended), or statically **Select the Objects to Include**. In the following screenshot, the guests that belong to the security group are selected using the **Objects Type: Virtual Machine** option.



STEP 5 | Review the details and click **OK** to create the security group.

Create Steering Rules on NSX Manager

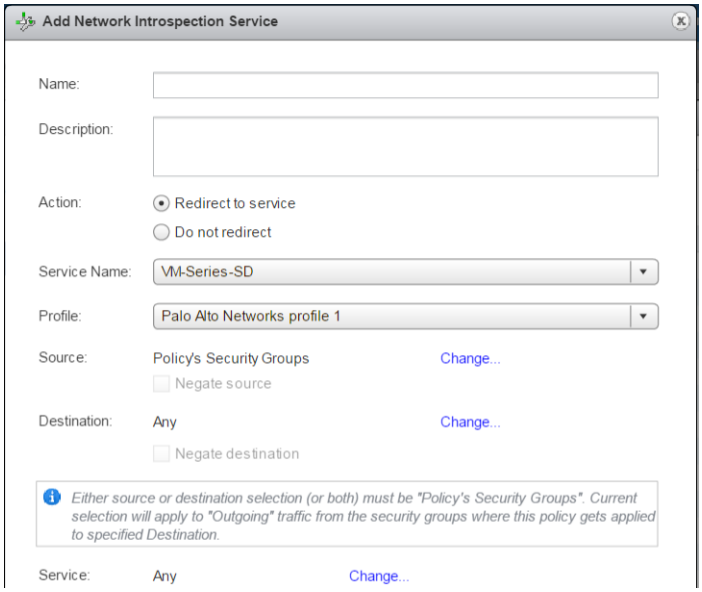
Do not apply the traffic redirection policies unless you understand how rules work on the NSX Manager as well as on the VM-Series firewall and Panorama. The default policy on the VM-Series firewall is set to deny all traffic, which means that all traffic redirected to the VM-Series firewall will be dropped. To create policies on Panorama and push them to the VM-Series firewall, see Apply Security Policies to the VM-Series Firewall.

STEP 1 | Select **Networking and Security** > **Service Composer** > **Security Policies** and click **Create Security Policy** ( ).

STEP 2 | Add a rule **Name**.

STEP 3 | Add a network introspective service.

1. Select **Network Introspection Service** and click the green plus icon.
2. **Name** the network introspection service and add a **Description**.
3. Select **Redirect to Service** under Action.
4. Select your service definition under Service Name.
5. Select you service profile under Profile.
6. Select a **Source** and a **Destination**. By default, traffic source is set to Policy's Security Groups. This option dynamically includes all security groups where this policy is applied. Alternatively, you can choose to have traffic from any source redirected to the firewall or specify certain security groups. However, vSphere requires that Source or Destination (or bother) be set Policy's Security Group. If you select Any or specific security groups for Destination, then Source must be set to Policy's Security Group.
7. (Optional) Select specific network services to be redirected to the firewall. If you choose any service or services, all other traffic will not be redirect to the firewall.
8. Click **OK**.
9. Repeat steps 1 through 6 to add additional network introspection services.
10. Click **Finish** to save your configuration.



STEP 4 | Apply redirection policy to security groups.

1. Highlight a security policy by clicking it.
2. Select **Networking and Security** > **Service Composer** > **Security Policies** and click Apply Security Policy ( ).
3. Apply the redirection rules by checking all appropriate zones.
4. Click **OK**.

Apply Security Policies to the VM-Series Firewall

Now that you have created the steering rules on Panorama and pushed them to the NSX Manager, you can now use Panorama for centrally administering policies on the VM-Series firewalls.

To manage centralized policy, use the dynamic address group as a source or destination address in security policy and push it to the firewalls; the firewalls can dynamically retrieve the IP addresses of the virtual machines that are included in each security group to enforce compliance for traffic that originates from or is destined to the virtual machines in the specified group.

STEP 1 | Log in to Panorama.

STEP 2 | (Operations-centric deployments only) Create dynamic-address groups.

Skip this step for security-centric deployments. If you are performing a security-centric deployment, you have already created dynamic-address groups.

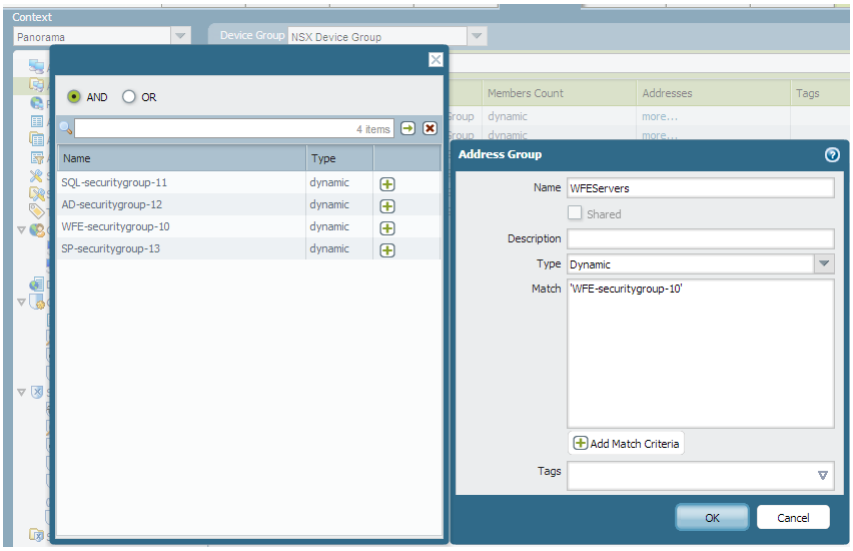
After creating the security redirection rules on the NSX Manager, the names of the security groups that are referenced in security policy will be available on Panorama.

Shared dynamic address groups are not supported on the VM-Series for VMware NSX.

1. Select **Objects** > **Address Groups**.
2. Select the Device Group you created for managing your VM-Series on NSX firewall from the **Device Group** drop-down.
3. Click **Add** and enter a **Name** and **Description** for the dynamic address group.
4. Select **Type** as **Dynamic**.
5. Add Match Criteria to your dynamic address group.

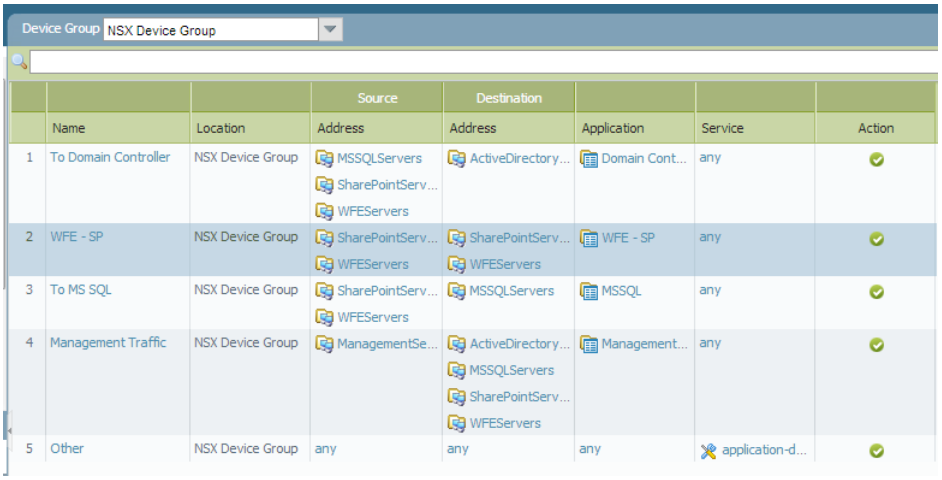
   Some browser extensions may block API calls between Panorama and NSX which prevents Panorama from receiving match criteria. If Panorama displays no match criteria and you are using browser extensions, disable the extensions and Synchronize Dynamic Objects to populate the tags available to Panorama.
6. Click **Add Match Criteria**.
7. Select the **And** or **Or** operator and click the plus (+) icon next to the security group name to add it to the dynamic address group.

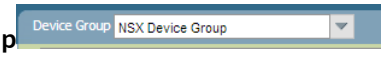
   The security groups that display in the match criteria dialog are derived from the groups you defined on the Distributed Firewall Partner Security Services or on the Service Composer on the NSX Manager. Only the security groups that are referenced in the security policies and from which traffic is redirected to the VM-Series firewall are available here.



8. Click **OK**.
9. Repeat these steps to create the appropriate number of dynamic address groups required for your deployment.
10. **Commit** your changes.

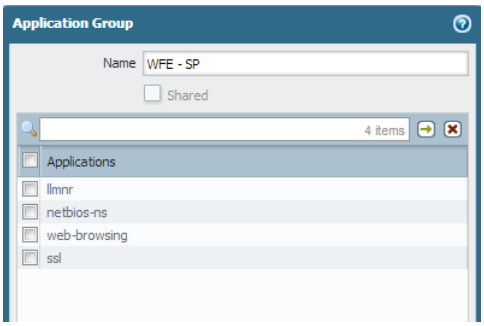
STEP 3 | Create security policy rules.



1. Select **Policies** > **Security** > **Prerules**.
2. Select the **Device Group** 

that you created for managing the VM-Series firewalls for NSX in Register the VM-Series Firewall as a Service on the NSX Manager.
3. Click **Add** and enter a **Name** and a **Description** for the rule. In this example, the security rule allows all traffic between the WebFrontEnd servers and the Application servers.
4. Select the **Source Zone** and **Destination Zone**. The zone name must be the same in both columns.
5. For the **Source Address** and **Destination Address**, select or type in an address, address group or region. In this example, we select an address group, the Dynamic address group you created previously.

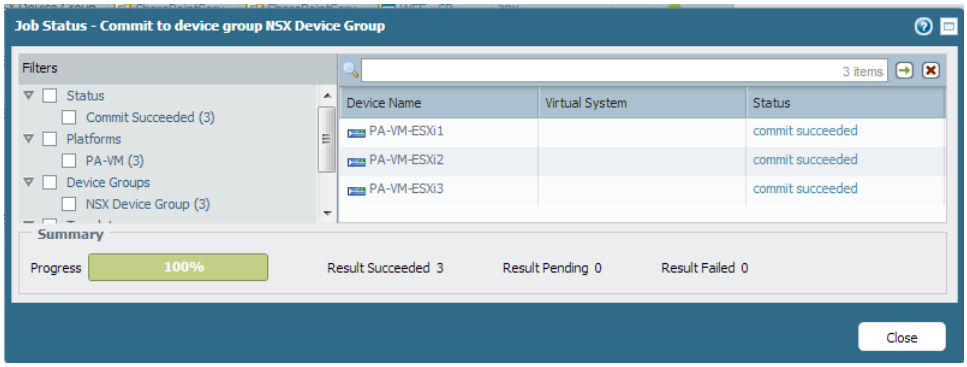
6. Select the **Application** to allow. In this example, we create an **Application Group** that includes a static group of specific applications that are grouped together.
   1. Click **Add** and select **New Application Group**.
   2. Click **Add** to select the application to include in the group. In this example, we select the following:
   3. Click **OK** to create the application group.



7. Specify the action— **Allow** or **Deny**—for the traffic, and optionally attach the default security profiles for antivirus, anti-spyware, and vulnerability protection, under Profiles.
8. Repeats the steps above to create the pertinent policy rules.
9. Click **Commit**, select Commit Type as **Panorama**. Click **OK**.

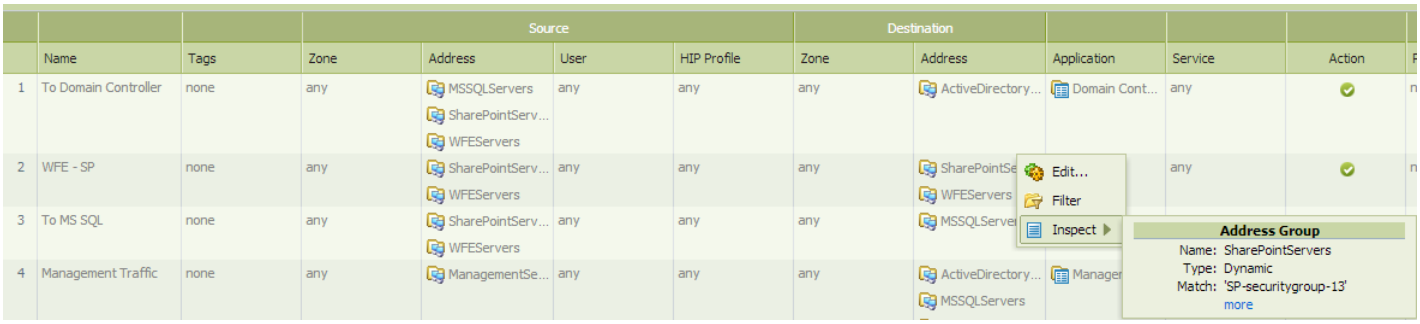
STEP 4 | Apply the policies to the VM-Series firewalls for NSX.

1. Click **Commit**, and select Commit Type **Device Groups**.
2. Select the device group, NSX Device Group in this example and click **OK**.
3. Verify that the commit is successful.

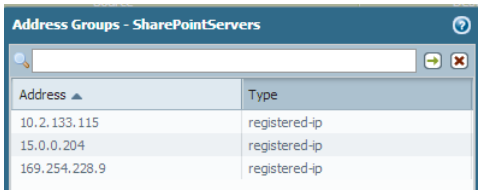


STEP 5 | Validate that the members of the dynamic address group are populated on the VM-Series firewall.

1. From Panorama, switch device context to launch the web interface of a firewall to which you pushed policies.
2. On the VM-Series firewall, select **Policies** > **Security**, and select a rule.
3. Select the drop-down arrow next to the address group link, and select **Inspect**. You can also verify that the match criteria is accurate.



4. Click the **more** link and verify that the list of registered IP addresses is displayed.



Policy will be enforced for all IP addresses that belong to this address group, and are displayed here.

STEP 6 | (Optional) Use template to push a base configuration for network and device configuration such as DNS server, NTP server, Syslog server, and login banner.

Refer to the Panorama Administrator's Guide for information on using templates.

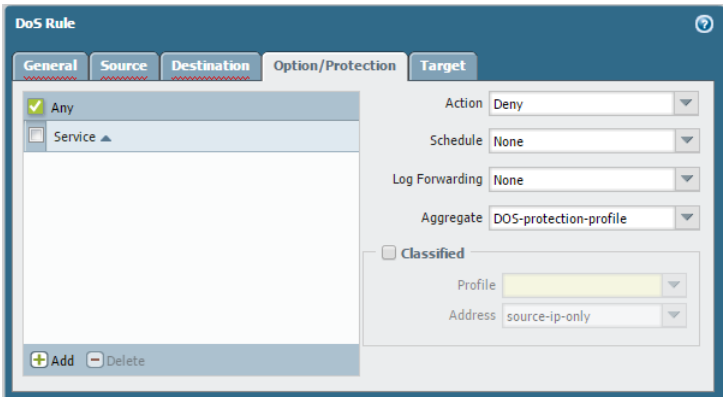
STEP 7 | Create a Zone Protection profile and attach it to a zone.

A zone protection profile provides flood protection and has the ability to protect against port scanning, port sweeps and packet-based attacks. It allows you to secure intra-tier and inter-tier traffic between virtual machines within your data center and traffic from the Internet that is destined to the virtual machines (workloads) in your data center.

1. Select your **Template**.
2. Select **Network** > **Network Profiles** > **Zone Protection** to add and configure a new profile.
3. Select **Network** > **Zones**, click the default-zone listed and select the profile in the **Zone Protection Profile** drop down.

STEP 8 | Create a DoS Protection profile and attach it to DoS Protection policy rule.

1. Select your **Device Group**.
2. Select **Objects** > **Security Profiles** > **DoS Protection** to add and configure a new profile.
   - A classified profile allows the creation of a threshold that applies to a single source IP. For example, you can configure a max session rate for an IP address that matched the policy, and then block that single IP address once the threshold is triggered.
   - An aggregate profile allows the creation of a max session rate for all packets matching the policy. The threshold applies to new session rate for all IP addresses combined. Once the threshold is triggered it affects all traffic that matches the policy.
3. Create a new DoS Protection policy rule in **Policy** > **DoS Protection**, and attach the new profile to it.



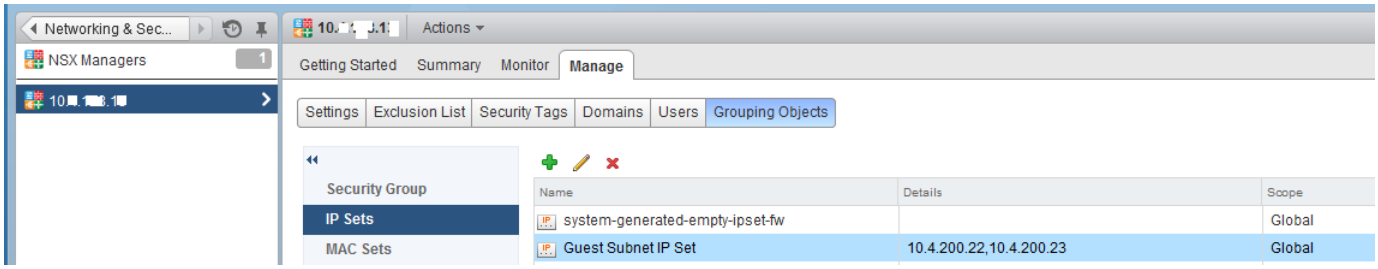
Steer Traffic from Guests that are not Running VMware Tools

VMware Tools contains a utility that allows the NSX Manager to collect the IP address(es) of each guest running in the cluster. NSX Manager uses the IP address as a match criterion to steer traffic to the VM-Series firewall. If you do not have VMware tools installed on each guest, the IP address(es) of the guest is unavailable to the NSX Manager and traffic cannot be steered to the VM-Series firewall.

The following steps allow you to manually provision guests without VMware Tools so that traffic from each of these guests can be managed by the VM-Series firewall.

STEP 1 | Create an IP set that includes the guests that need to be secured by the VM-Series firewall. This IP set will be used as the source or destination object in an NSX distributed firewall rule in step 4 below.

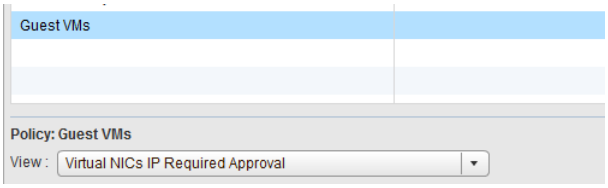
1. Select **NSX Managers** > **Manage** > **Grouping Objects** > **IP Sets**.
2. Click **Add** and enter the IP address of each guest that does not have VMware tools installed, and needs to be secured by the VM-Series firewall. Use commas to separate individual IP addresses; IP ranges or subnets are not valid.



STEP 2 | Verify that SpoofGaurd is enabled. If not enabled, see Enable SpoofGuard.

STEP 3 | Manually approve the IP address(es) for each guest in SpoofGuard; this validates that the approved IP addresses is the accurate address for that network adapter. For a manually-configured IP address, make sure to add the IP address to the IP set before approving it in SpoofGuard.

1. Select the new SpoofGuard policy you created to earlier and **View: Inactive Virtual NICs**.
2. Select the guest and add the IP address in the Approved IP field and Publish changes.
3. Review and approve all previously approved IP addresses too.



STEP 4 | Attach the IP sets to the Security Groups on NSX, to enforce policy.

1. Select **Networking and Security** > **Service Composer** > **Security Groups**.
2. Select **Select objects to include** > **IP Sets**, add the IP set object to include.

What is Multi-NSX Manager Support on the VM-Series for NSX?

Multi-NSX Manager support on the VM-Series firewall for NSX allows you to connect a single Panorama to multiple NSX Managers running individual vCenter servers. Using a single Panorama allows you to manage common objects and policies and synchronize them across multiple vCenter servers. You can now configure and manage multiple NSX Managers in a single location, eliminating the need to replicate common configuration many times on multiple Panorama servers.

- Plan Your Multi-NSX Deployment
- Deploy the VM-Series Firewall in a Multi-NSX Manager Environment

Plan Your Multi-NSX Deployment

You must carefully plan your device group hierarchy and template stacks and consider how they interact with the other components needed for deployment. Service definitions reference device groups and template stacks and push that information to the firewalls in the related ESXi clusters.

- **Configure your device groups**—Devices groups are logical units that group firewalls based on common aspects that require similar policy configurations. Each service definition requires a device group and each device group can only be referenced in one service definition.

  A device group inherits policy rules and object settings from device groups above it in the device group hierarchy. This allows you to configure common or shared settings in parent device groups and unique settings in child or grandchild device groups. By default, Panorama has a Shared device group and any configuration in the shared device group is pushed to all device groups. When configuring any policy rules or object settings, confirm that you have selected the right device group.

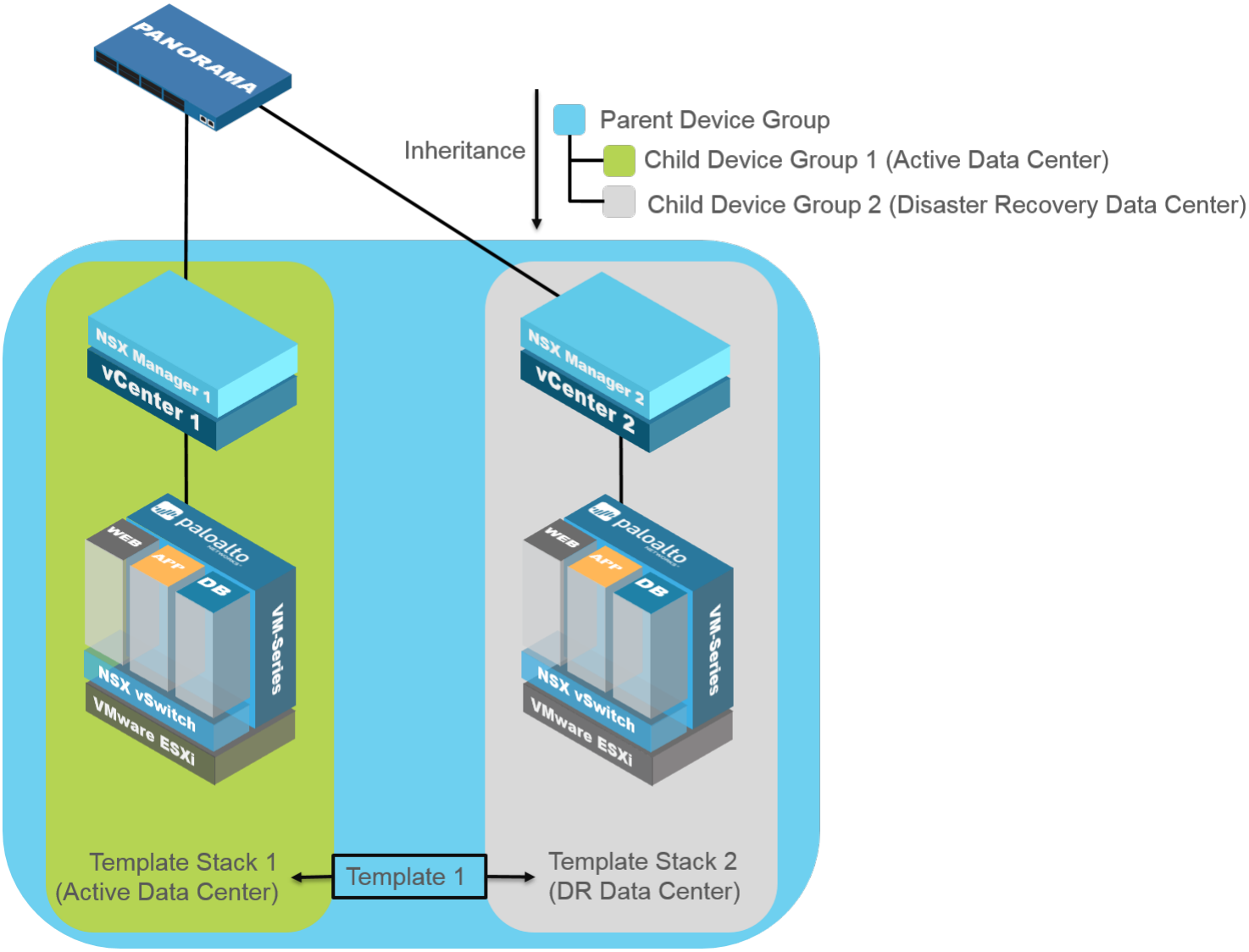
  See Managing Device Groups in the Panorama 8.0 Administrator's Guide for information on configuring and managing device groups.
- **Configure your templates**—A template contains settings that enable a firewall to connect to your network, such as interface and zone configurations. Each service definition requires a template and each template can only be referenced in one service definition.

  When assigning a template stack to a service definition, consider the priority of the templates in the stack to ensure that the right configuration is pushed to the correct firewalls. If the templates in a stack contain overlapping configuration, the template with her priority takes precedence and the same setting in lower templates are ignored. Therefore, ensure that template configuration unique to an NSX Manager is given higher priority in the template stack assigned to that NSX Manager's service definition.

  See Manage Templates and Template Stacks in the Panorama 8.0 Administrator's Guide for information on configuring and managing templates.
- Create your service definition—A service definition specifies the configuration for the VM-Series firewalls on each host in the ESXi cluster. Each individual NSX manager configuration requires at least one service definition. A service manager can have multiple service definitions but each service definition can only have one device group and one template or template stack. After a device group or template has been assigned to a service definition, you can no longer select that device group or template for future service definitions.

For example, in a disaster recovery deployment scenario, you would need to create identical device groups for each data center. Because all the policy rules and objects are the same for data centers, you can perform all you configuration in a single device group. However, you cannot use the same device group in two service definitions. To ensure that each data center gets the same policy rules, create a child device group for each data center under the device group with the common configuration. These child device groups do

not need any configuration of their own because they inherit everything the VM-Series firewalls need from the parent device group. And because each data center is identical, configure your network settings in a template (Template 1). Create a template stack for each data center and assign Template 1 to each stack.

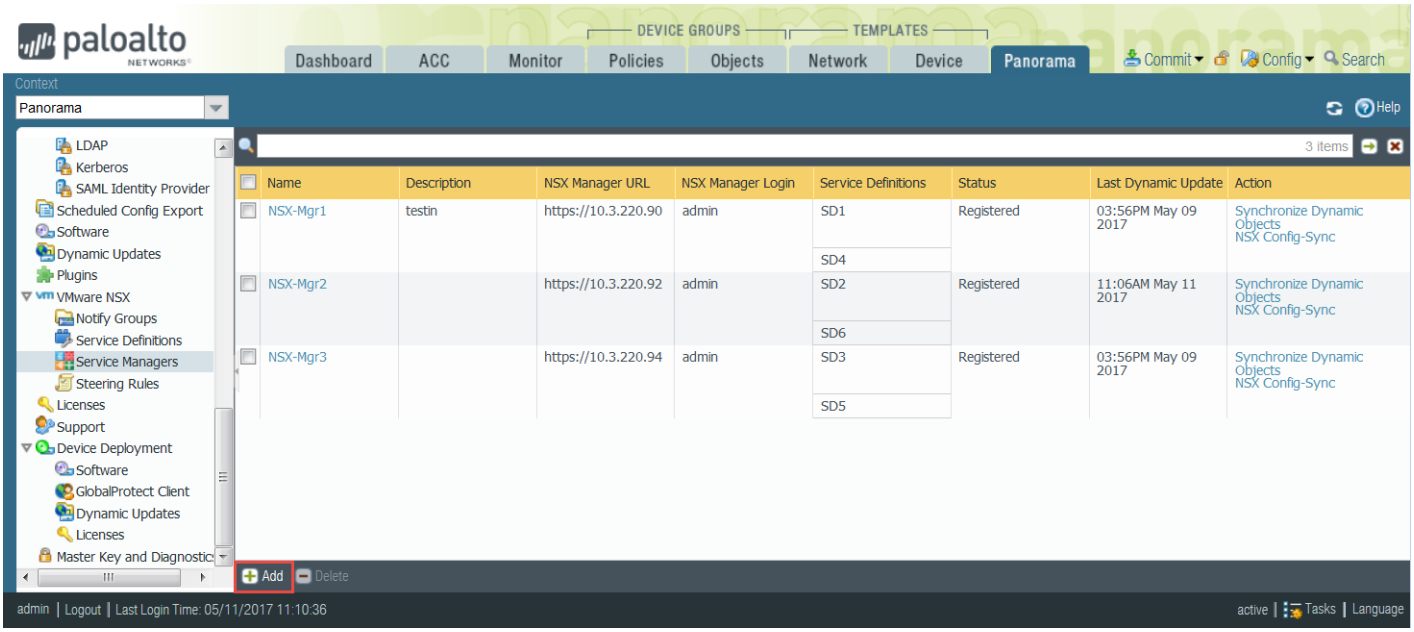


Deploy the VM-Series Firewall in a Multi-NSX Manager Environment

Whether you are deploying a single NSX Manager or a multi-NSX Manager environment, set up the connection between an NSX Manager and Panorama before you continue on to set up the next NSX Manager with Panorama.

STEP 1 | Install the VMware NSX Plugin version 2.0 as it allows you to connect up to 16 NSX Managers. This version of the plugin allows you to add more than one Service Manager to your VM-Series firewall for NSX configuration on Panorama.

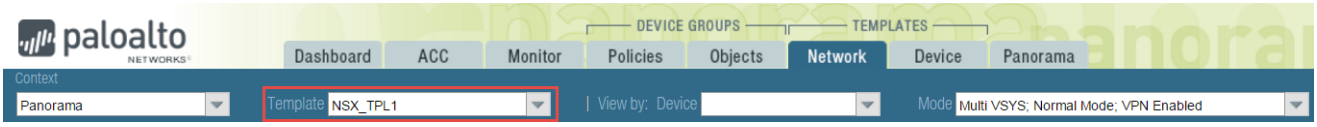
STEP 2 | Enable Communication Between the NSX Manager and Panorama.



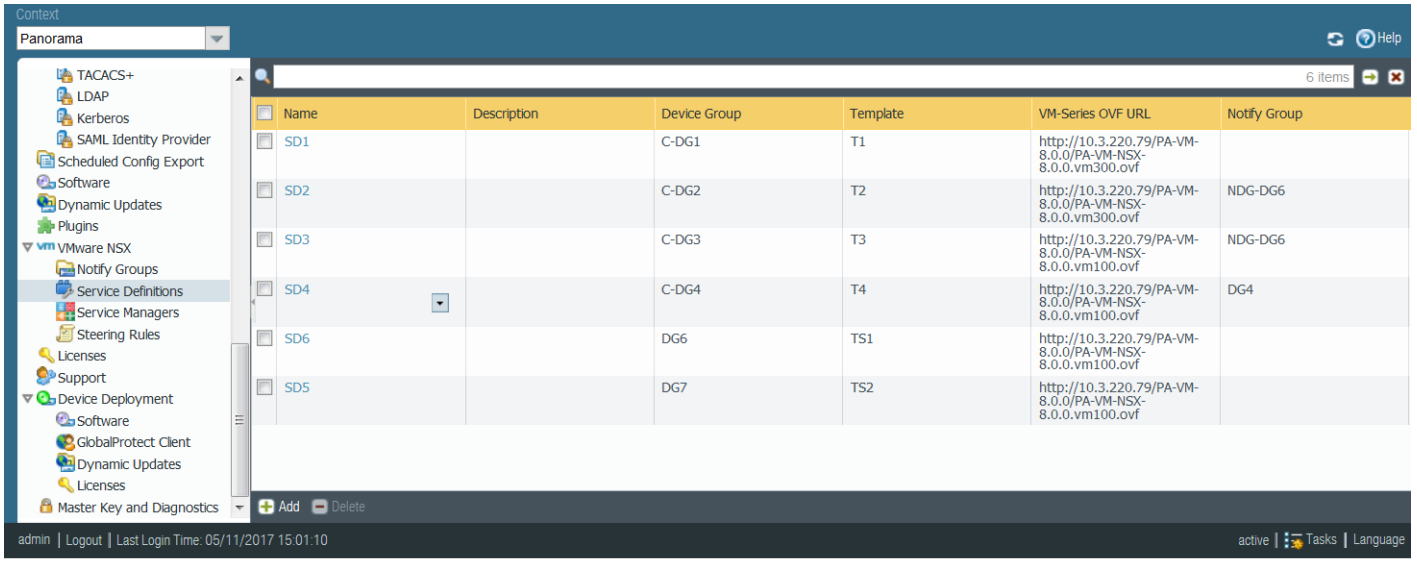
STEP 3 | Create Template(s) and Device Group(s) on Panorama. Device groups and templates push the security policy and network settings to the VM-Series firewalls in each ESXi cluster.

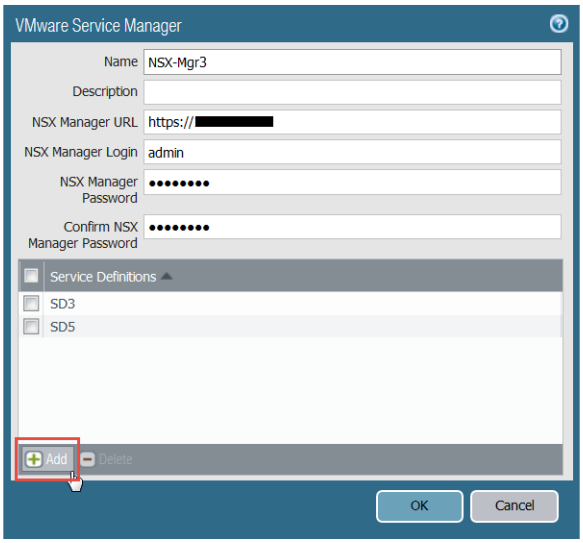
When configuring policy rules and objects, verify that you have selected the correct device group.

When configuring network and device settings, verify that you have selected the correct template or template stack.



STEP 4 | Create the Service Definitions on Panorama and attach them to the service manager. Each service definition can reference one device group and one template or template stack. Panorama supports up to 32 service definitions across all service managers.



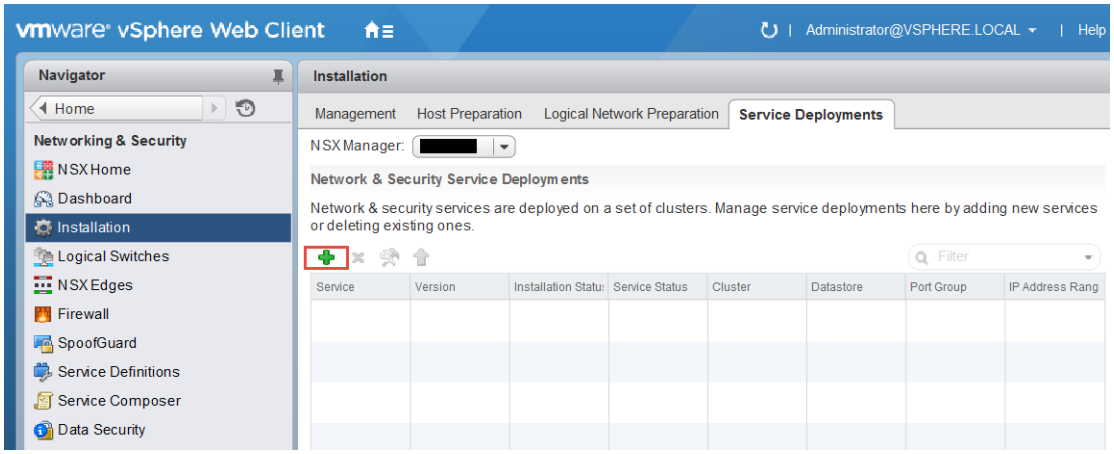


STEP 5 | Configure dynamic address groups or security groups and redirect traffic to the VM-Series firewall.

- For security-centric deployments Set Up Dynamic Address Groups on Panorama and Create Steering Rules on Panorama.
- For operations-centric deployments Set Up Security Groups on the NSX Manager and Create Steering Rules on NSX Manager.

Verify that you have selected the correct device group so the right steering rules are sent to the corresponding NSX Manager.

STEP 6 | Deploy the Palo Alto Networks NGFW Service on each ESXi cluster by using the relevant service definitions.



STEP 7 | Repeat this process for each NSX Manager.

1. Select **Panorama** > **VMware NSX** > **Service Managers** and click **Add**.
2. Enable Communication Between the NSX Manager and Panorama.

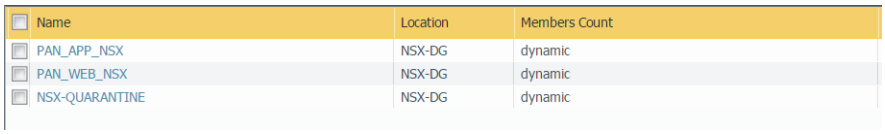
Dynamically Quarantine Infected Guests

Threat and traffic logs in PAN-OS include the source or destination universally unique identifier (UUID) of guest VMs in your NSX deployment. This allows the VM-Series for NSX to support the tagging of guest VMs with NSX security tags. With the guest VMs' UUID now included in the log events, the firewall, based on the filtered log events, can tag the affected guest VM via NSX Manager API. This allows for automatic location of compromised VMs in the NSX environments. NSX can then put all associated UUIDs under policies to quarantine those VMs from the rest of the network.

Panorama includes predefined payload formats for threat and traffic logs in the HTTP Server Profile. These payload formats correspond to predefined security tags in NSX. When a guest VM is found in the threat or traffic logs, Panorama makes an API call to NSX Manager telling NSX Manager to tag the guest VM with the tag specified in the HTTP Server Profile. When the guest VM becomes tagged, NSX Manager dynamically moves the tagged guest VM into the quarantine security group, which places the guest VM into the quarantine dynamic address group.

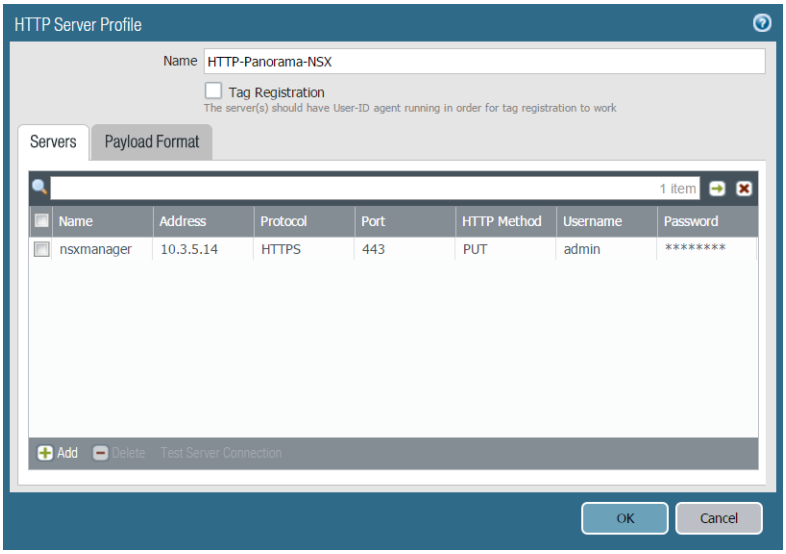
STEP 1 | Confirm that you have content update version 636 or later installed on Panorama.

STEP 2 | Create a dynamic address to be your quarantine dynamic address group.

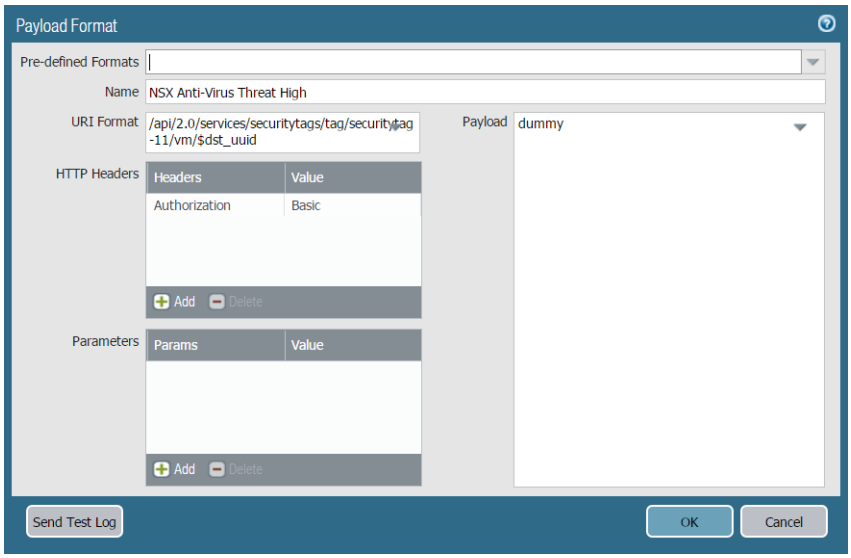


STEP 3 | Create an HTTP Server Profile to send API calls to NSX Manager.

1. Select **Panorama** > **Server Profiles** > **HTTP** and **Add** a new HTTP Server Profile.
2. Enter a descriptive **Name**.
3. Select **Add** to provide the details of NSX Manager.
4. Enter a **Name** for NSX Manager.
5. Enter the **IP Address** of NSX Manager.
6. Select the Protocol (HTTP or HTTPS). The default Port is 80 or 443 respectively.
7. Select PUT under the HTTP Method column.
8. Enter the username and password for NSX Manager.

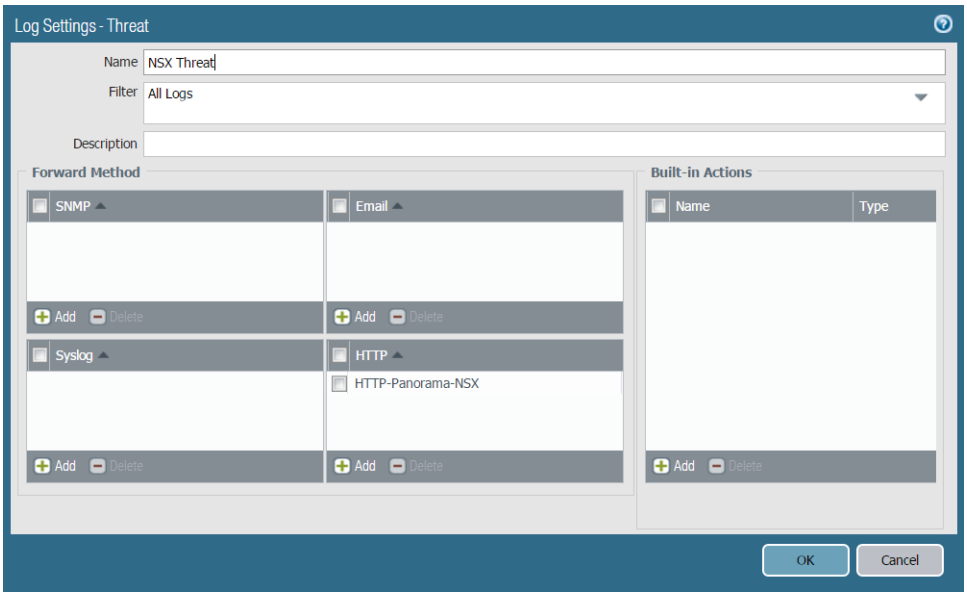


9. Select **Payload Format** and choose an NSX payload format from the Pre-defined Formats drop-down. This populates the URI Format, HTTP Headers, and Payload fields with the correct information to send the HTTP API call to NSX Manager. Additionally, the chosen format determines which security tag NSX Manager applies to infected guest VMs. In the example below, **NSX Anti-Virus Threat High** is selected which corresponds to the **ANTI_VIRUS.VirusFound.threat=high** security tag on NSX Manager.



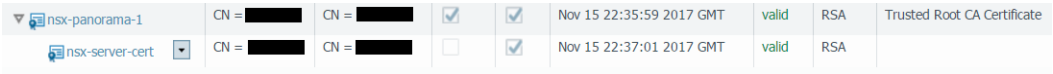
STEP 4 | Define the match criteria for when Panorama will forward logs to the NSX Manager, and attach the HTTP server profile to use.

1. Select **Panorama** > **Log Settings** for Threat or Traffic logs.
2. Enter a descriptive name for the new log settings.
3. (Optional) Under Filter, you can add filters such as severity to narrow the logs that are forwarded to NSX Manager. If All Logs is selected, all threat or traffic logs that meet the criteria set in the HTTP Server profile are sent to NSX Manager.
4. Click **Add** under HTTP and select the HTTP Server Profile configured in step 3.
5. Click **OK**.



STEP 5 | Configure an NSX server certificate for Panorama to forward logs to NSX manager.

1. Select **Panorama** > **Certificate Management** > **Certificates**.
2. Create a root CA certificate with CN=IP address of Panorama.
3. Create a signed certificate with CN=IP address of NSX Manager.
4. Export the root CA certificate in PEM format without a private key.
5. Export the signed certificate in PEM format with a private key.



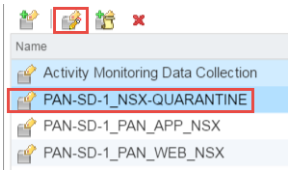
6. Using a tool such as OpenSSL, concatenate the exported certificates into a single PEM file for upload to NSX manager. Use the following commands in OpenSSL to complete this step.

```
cat cert_NSX_Root_CA.crt cert_NSX_Signed1.pem > cert_NSX_cert_chain.pem
openssl pkcs12 -export -in cert_NSX_cert_chain.pem -out cert_NSX_cert.p12
```

7. Log in to NSX Manager and select **Manage Appliance Settings** > **SSL Certificates** > **Upload PKC#12 Keystore**. Click **Choose File**, locate the p12 file you created in the previous step, and click **Import**.

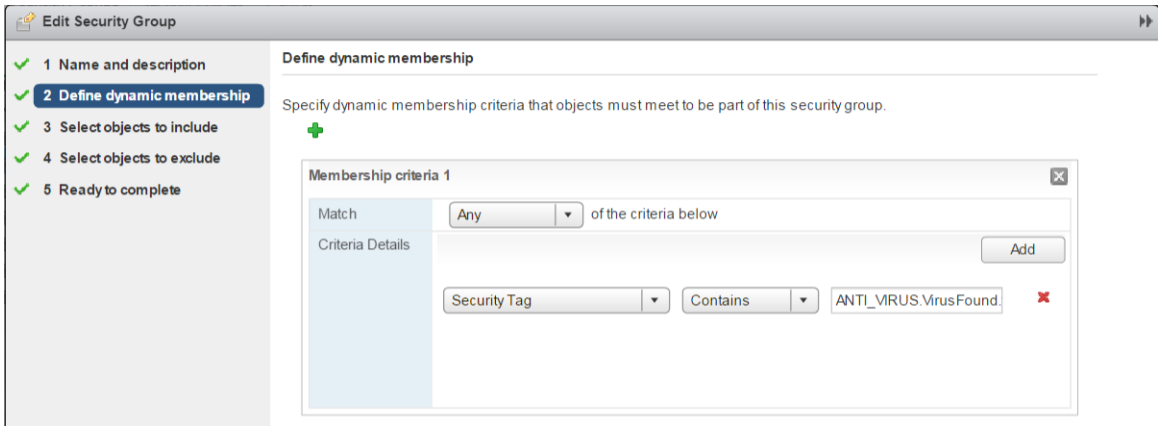
STEP 6 | Associate a security group with a security tag in vCenter.

1. Log in to vCenter.
2. Select **Networking & Security** > **Service Composer** > **Security Groups**.
3. Select a security group that is counterpart to the quarantine dynamic address group you created previously and click **Edit Security Group**.



4. Select Define dynamic membership and click the + icon.
5. Click **Add**.
6. Set the criteria details to Security Tag Contains and then enter the NSX security tag that corresponds to the NSX payload format you chose in 3. Each of the predefined NSX payload formats corresponds to an NSX security tag. To view the NSX security tags in NSX, select **Networking & Security** > **NSX Managers** > **NSX Manager IP** > **Manage** > **Security Tags**.

   In this example, **NSX Anti-Virus Threat High** is used in the HTTP Server Profile so **ANTI_VIRUS.VirusFound.threat=high** is the NSX Security Tag that is used here.
7. Click Finish.



STEP 7 | After the guest VM is cleared for removal from quarantine, manually remove the NSX security tag from the guest VM in NSX.

1. Log in to vCenter.
2. Select **VMs and Templates** and choose the quarantined guest.
3. Select **Summary** > **Security Tags** > **Manage**.
4. Uncheck the security tag used by the quarantine security group and click OK.
5. Refresh the page and the quarantine security will no longer be listed under **Summary** > **Security Group Membership**.

Source and destination UUID fields in threat and traffic logs may be blank after a guest VM is removed from quarantine. This can occur when running NSX 6.2.3 or earlier or if NSX steering rules do not use the inout direction. You can resolve this by upgrading NSX to 6.2.4 or issue an NSX Config-sync under **Panorama** > **VMware NSX** > **Service Manager** and reboot the PA-VM to resolve this issue.

Migrate Panorama 7.1 Configuration to Panorama 8.0 Configuration

When you upgrade Panorama in your VMware NSX deployment from 7.1 to 8.0, all your existing configuration is maintained. However, that configuration will remain in the Operations Centric formats. Complete the following procedure to migrate your Operations Centric configuration into Security Centric formats. Do not complete this procedure if you plan to manage your deployment using Operations Centric workflows after upgrading to 8.0.

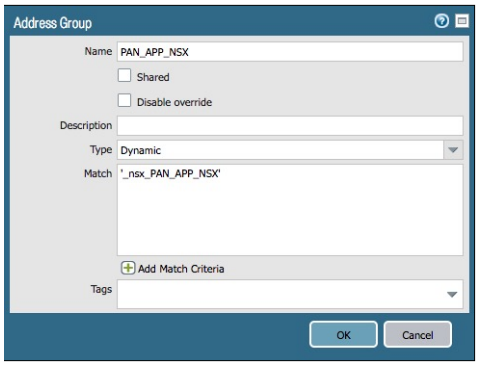
STEP 1 | Upgrade Panorama.

The VMware NSX plugin is automatically installed upon upgrade to 8.0.

STEP 2 | Update the match criteria format in your dynamic address groups.

1. Select **Objects** > **Address Groups** and click the link name for your first dynamic address group.
2. Delete the existing match criteria entry.
3. Enter the new match criteria in the following format:

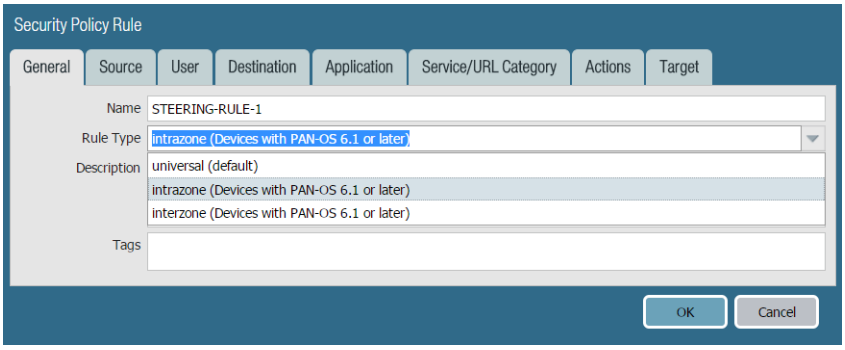
```
'_nsx_<dynamic-address-group-name>'
```



4. Click **OK**.
5. Repeat this process for each dynamic address group.

STEP 3 | Change security policy used as NSX steering rules to intrazone.

1. Select **Policies** > **Security** > **Pre Rules** and click the link name for your first security policy rule.
2. On the General tab, change the **Rule Type** to intrazone.

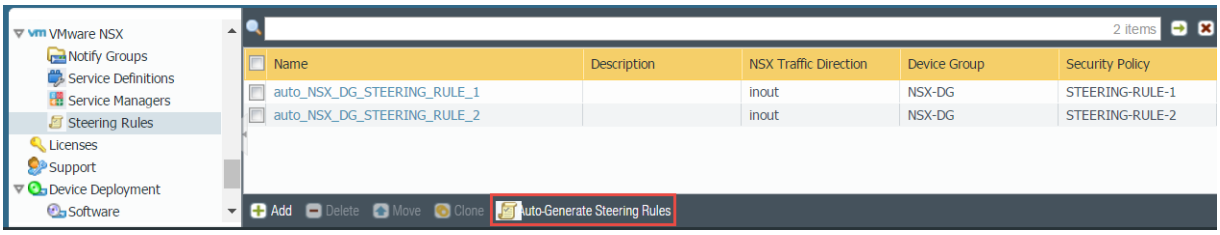


3. Click **OK**.

4. Repeat this process for each security policy rule.

STEP 4 | Generate new steering rules.

1. Select **Panorama** > **VMware NSX** > **Steering Rules**.
2. Click **Auto-Generate Steering Rules**.

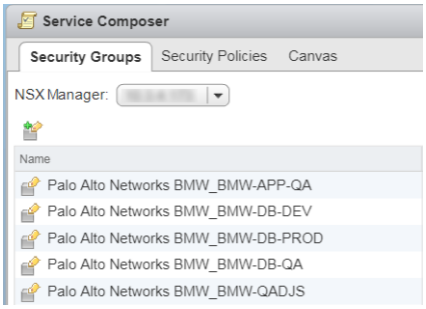


STEP 5 | **Commit** your changes.

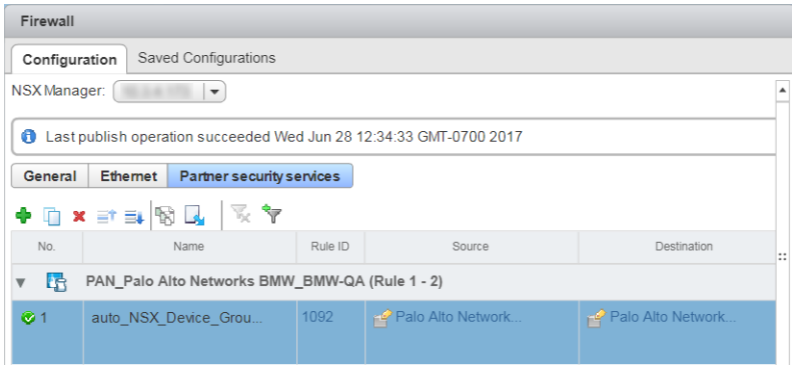
When you commit your changes, Panorama pushes updates to NSX Manager.

1. Verify that NSX Manager created new security groups.
   1. Login to vCenter and select **Networking & Security** > **Security Groups**.
   2. The new security groups (mapped to the updated dynamic address groups) should appear in the following format:

      <service-definition-name> - <dynamic-address-group-name>



2. Verify that NSX Manager created new steering rules.
   1. Select **Networking & Security** > **Firewall** > **Configuration** > **Partner security services**.
   2. The new steering rules (mapped to the security policy rules you create on Panorama) are listed above the old steering rules.

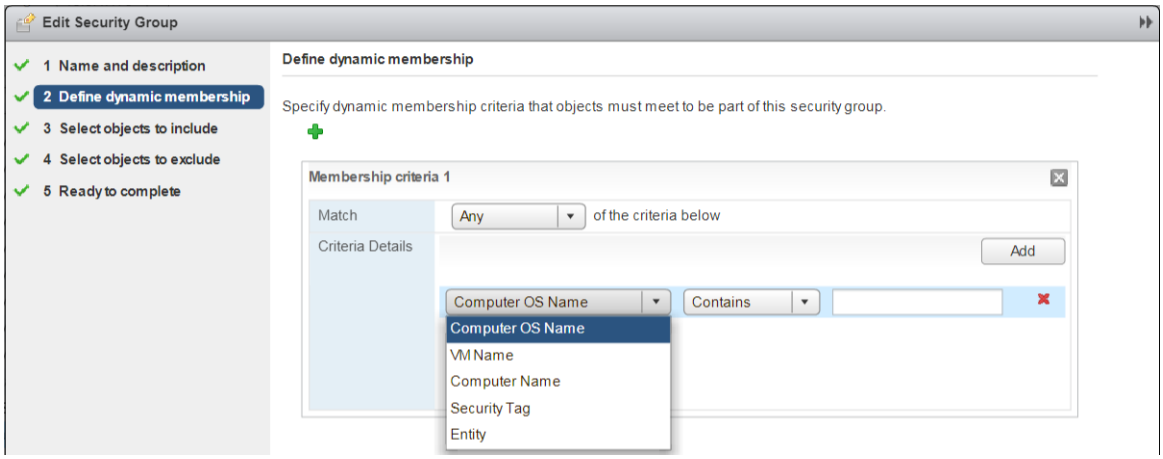


STEP 6 | Add match criteria to the newly created security groups to ensure that your VMs are placed in the correct security group.

There two ways to complete this task—recreate the match criteria from the old security group in the new security group or nest the old security group within the new security group.

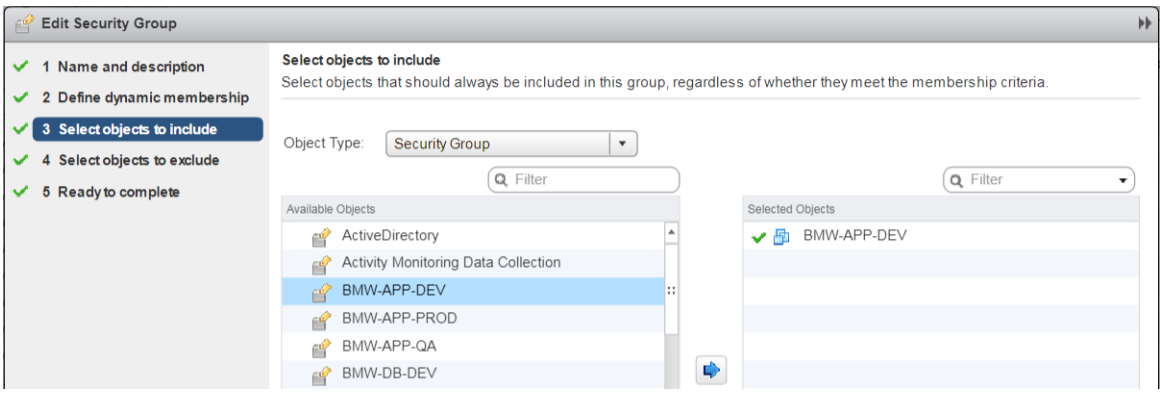
To recreate the match criteria from the old security group, complete the following procedure.

1. Select **Network & Security** > **Service Composer** > **Security Groups**.
2. Click on a new security group and select **Edit Security Group**.
3. Select **Define dynamic membership** and click the plus icon.
4. Add the same match criteria in the corresponding old security group.
5. Repeat this process for each new security group.
6. Delete the old security groups.



To nest the old security group within the new security group, complete the following procedure. In this method, VMs in the old security group are added to the new security group. Additionally, any new VM that meets the criteria of the old security group is automatically added to the new security group.

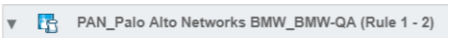
1. Select **Network & Security** > **Service Composer** > **Security Groups**.
2. Click on a new security group and select **Edit Security Group**.
3. Select **Select objects to include**.
4. Select the **Security Group** Object Type.
5. Choose the corresponding old security group under Available Objects and move it to Selected Objects by clicking the right arrow icon.
6. Click **Finish**.



STEP 7 | Delete the old steering rules from vCenter.

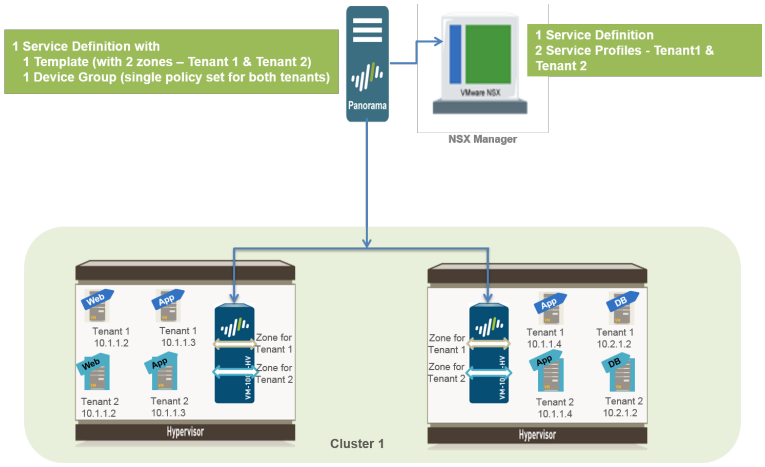
1. Select **Networking & Security** > **Firewall** > **Configuration** > **Partner security services**.
2. Delete the old steering rules. Take care not to delete the Palo Alto Networks rules created by the 8.0 workflow. These steering rule sections use the following naming convention.

<service-definition-name> - <dynamic-address-group-name>



Use Case: Shared Compute Infrastructure and Shared Security Policies

This use case allows you to logically isolate traffic from two tenants that share an ESXi cluster and have a common set of security policies. In order to isolate traffic from each tenant you need to create a service definition with a template that includes two zones. Zone-based traffic separation makes it possible to distinguish traffic between virtual machines that belong to separate tenants, when it traverses through the firewall. The firewall is able to distinguish traffic between tenant virtual machines based on a service profiles and security groups created on the NSX Manager, which are available as match criteria in Dynamic Address Groups on the firewall. Therefore, even with overlapping IP addresses, you can segregate traffic from each tenant and secure each tenant's virtual machines using zone-base policy rules (source and destination zones must be the same) and dynamic address groups.

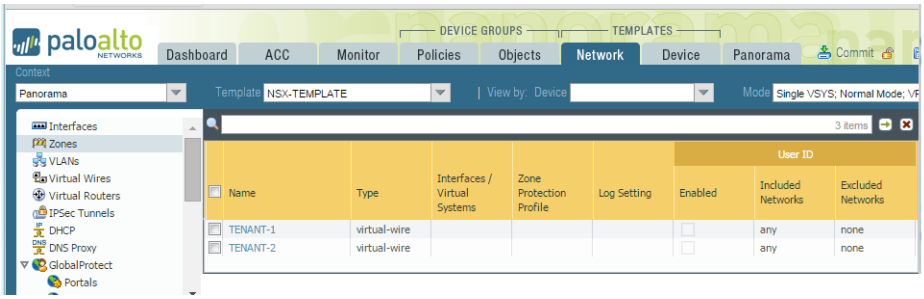


STEP 1 | Enable Communication Between the NSX Manager and Panorama.

This is one-time task and is required if you have not enabled access between the NSX Manager and Panorama.

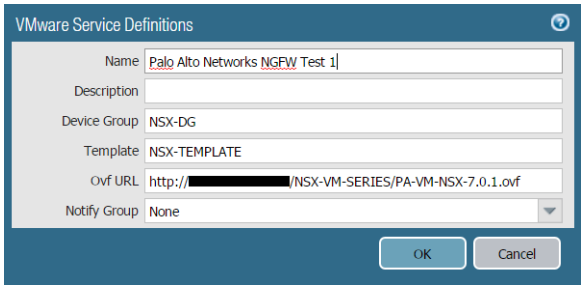
STEP 2 | Create Template(s) and Device Group(s) on Panorama.

1. Log in to the Panorama web interface.
2. Select **Panorama** > **Templates** to add a template. This use case has a template named NSX-Template.
3. Select **Panorama** > **Device Groups** and add device group. This use case has a device group named NSX-DG.
4. Create two zones within the Template. To isolate traffic for each tenant, you need two zones in this use case.
    1. Select **Network** > **Zones**.
    2. Select the correct template in the **Template** drop-down.
    3. Select **Add** and enter a zone **Name**. For example, **Tenant1**.
    4. Sets the interface **Type** to **Virtual Wire**.
    5. Click **OK**.
    6. Repeat the steps to add another zone, for example, **Tenant2**.
    7. Verify that the zones are attached to the correct template.



STEP 3 | Create the Service Definitions on Panorama.

1. Select **Panorama** > **VMware NSX** > **Service Definitions**.
2. Select **Add** and fill in the details.



3. Click **Commit**, and select **Panorama** as the **Commit Type** to save the changes to the running configuration on Panorama.

STEP 4 | Create Security Groups and Steering Rules.

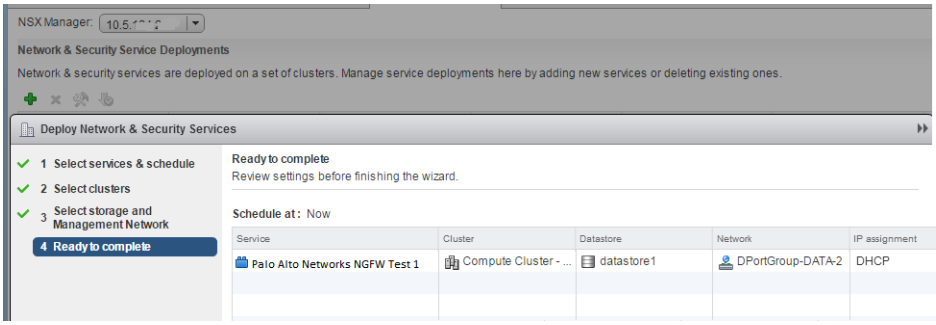
1. Select **Objects** > **Address Groups** and Set Up Dynamic Address Groups on Panorama for each tenant's virtual machines. For example, this use case has two security groups per tenant; one security group for the web servers and the other security group for the application servers.
2. Select **Policies** > **Security** > **Pre Rules** to set up security policy rules for sending traffic to the VM-Series firewall.
3. Select **Panorama** > **VMware NSX** > **Steering Rules** and click **Auto-Generate Steering Rules**.
4. **Commit** your changes

STEP 5 | Prepare the ESXi Host for the VM-Series Firewall.

The ESXi hosts in the cluster must have the necessary NSX components that allow the NSX firewall and the VM-Series firewall to work together. The NSX Manager will install the components— the Ethernet Adapter Module (.eam) and the SDK —required to deploy the VM-Series firewall.

STEP 6 | Deploy the Palo Alto Networks NGFW Service.

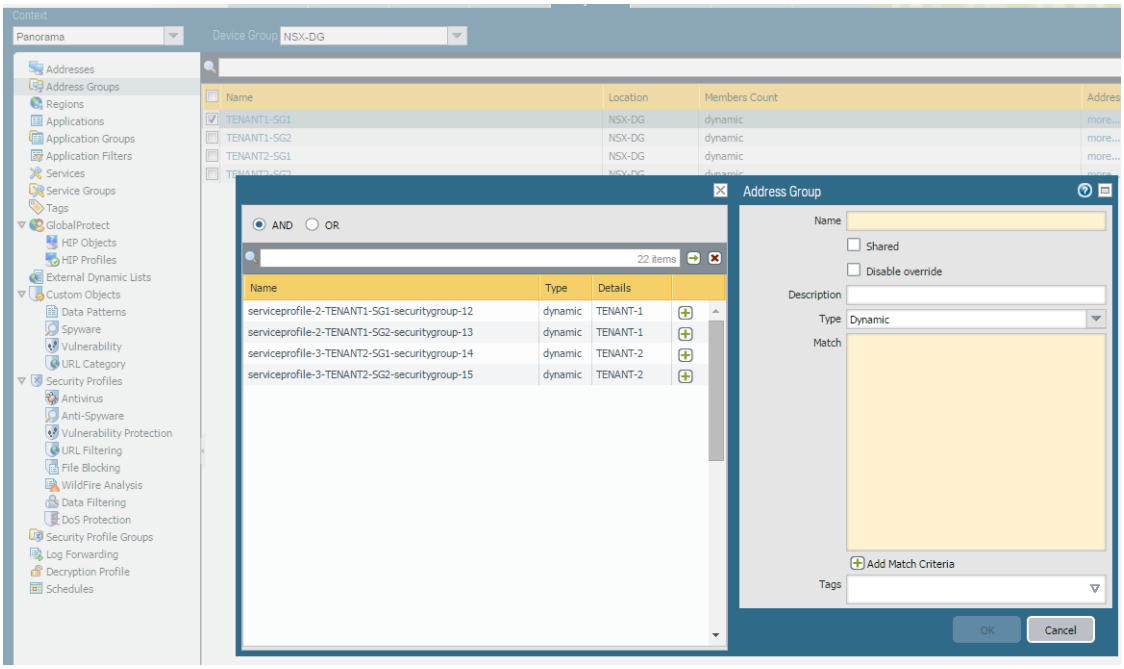
1. Select **Networking and Security** > **Installation** > **Service Deployments**.
2. Click **New Service Deployment** (green plus icon), and select the service definition for the Palo Alto Networks next generation firewall you want to deploy, **Palo Alto Networks NGFW Test 1** in this example, make your selections including the appropriate ESXi cluster to which you want to deploy the firewall and click **Finish**.



3. Verify that the NSX Manager reports the **Installation Status** as **Successful**.
4. Verify that the VM-Series firewall is successfully deployed.
    1. On the vCenter server, select **Hosts and Clusters** to check that every host in the cluster(s) has one instance of the firewall.
    2. View the management IP address(es) and the PAN-OS version running on the firewall directly from vCenter server. VMware Tools is bundled with the PAN-OS software image and is automatically enabled when you launch the VM-Series firewall.

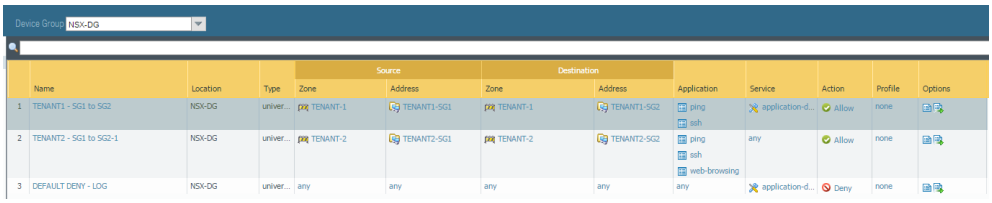
STEP 7 | Apply Security Policies to the VM-Series Firewall.

1. Create Dynamic Address groups for each tenant on Panorama. The dynamic address group(s) that match on the name of the security group(s) you defined on the NSX Manager.
    1. On Panorama, select **Objects** > **Address Groups**.
    2. Select the correct **Device Group** from the drop-down and click **Add**.
    3. Add a **Name** for the address group and set Type as **Dynamic** and **Add Match Criteria**. Verify that you select the correct tags for each tenant, the tag includes the service profile ID, the security group name and the security group ID. For example, for this use case there are four dynamic address groups:



2. On Panorama, create security policy rules and use the dynamic address groups as source or destination address objects in security policy rules and push it to the firewalls.
    1. Select **Policies** > **Security** > **Prerules** and click **Add**.

2. Create rules for each tenant. This use case has the following policy rules:



3. Click Commit, and select Commit Type as Device Groups. Select the device group, NSX-DG in this example and click OK.

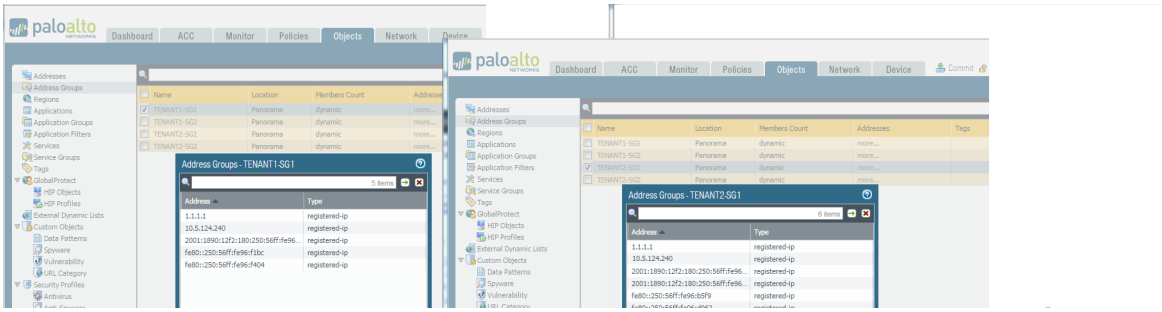
STEP 8 | Verify that traffic from each tenant is secured.

1. Log in to the CLI on the firewall and enter the following command to view the subinterfaces on the firewall:

```
show interface all
total configured hardware interfaces: 2
name id    speed/duplex/state        mac address
--------------------------------------------------------
ethernet1/1             16    auto/auto/up d4:f4:be:c6:af:10
ethernet1/2             17    auto/auto/up d4:f4:be:c6:af:11
aggregation groups: 0
total configured logical interfaces: 6

name                id vsys zone         forwarding
------------------- ----- ---- -----------------
ethernet1/1      16    1                vwire:ethernet1/2
ethernet1/1.3    4099  1    TENANT-1   vwire:ethernet1/2.3
ethernet1/1.4     4100   1   TENANT-2     vwire:ethernet1/2.4
ethernet1/2        17    1 vwire:ethernet1/1
ethernet1/2.3    4355  1    TENANT-1 vwire:ethernet1/1.3
ethernet1/2.4      4356  1 TENANT-2 vwire:ethernet1/1.4
```

2. On the web interface of the VM-Series firewall, select **Objects** > **Address Groups** and verify that you can view the IP address for the members of each Dynamic Address Group. The following is an example of duplicate IP addresses in dynamic address groups across both tenants.



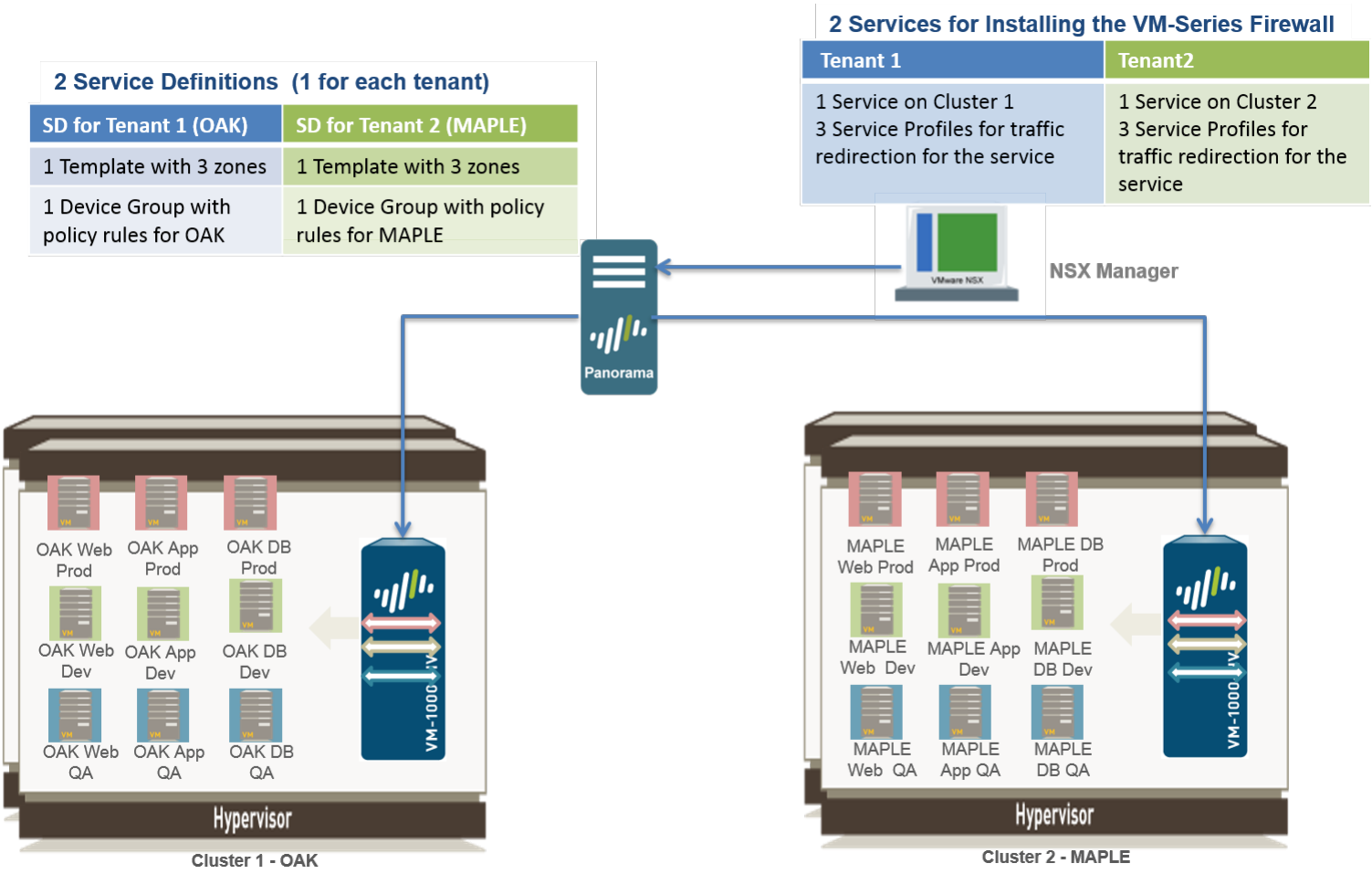
3. View the **ACC** and the **Monitor** > **Logs** > **Traffic**. Filter on the zone name to ensure that traffic from the virtual machines for each tenant is secured.

Use Case: Shared Security Policies on Dedicated Compute Infrastructure

If you are a Managed Service Provider who needs to secure a large enterprise (*tenant*) with multiple departments (*sub-tenants*), and each tenant requires dedicated compute infrastructure and security policy rules, you need to create a service definition for each tenant.

In this use case, each tenant—Oak and Maple— has a dedicated ESXi cluster. And each tenant has sub-tenants—Dev, QA, and Prod—whose workloads are deployed in the cluster. You need to define two service definitions to allow the VM-Series firewalls for each tenant to have Security policies for their respective ESXi clusters. The service definition for each tenant includes multiple zones (with corresponding virtual wire subinterface pairs) for isolating traffic from each sub-tenant. Each zone is mapped to a service profile on the NSX Manager, which allows the firewall to distinguish traffic from the virtual machines for each sub-tenant and to enforce zone-based security policy rules within the common set of policy rules for the tenant. Zone-based policies in combination with the Dynamic Address groups also allow you to secure sub-tenants who may have overlapping networks, and hence have duplicate IP addresses. To uniquely identify virtual machines assigned to each sub-tenant and successfully enforce policy, the NSX Manager provides the service profile and security group to which a virtual machine belongs as match criteria in dynamic address groups on Panorama. For more information, see Policy Enforcement using Dynamic Address Groups.

You can also configure role-based access control using access domains on Panorama. Access domains allow you to control administrative access to specific device groups (to manage policies and objects) and templates (to manage network and device settings), so that each tenant administrator can manage the configuration for their VM-Series firewalls. Role-based access also allows you to limit log visibility for the respective tenant only.

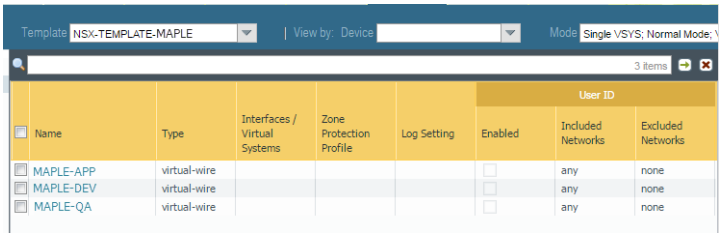


STEP 1 | Enable Communication Between the NSX Manager and Panorama.

This is one-time task and is required if you have not enabled access between the NSX Manager and Panorama.

STEP 2 | Create Template(s) and Device Group(s) on Panorama.

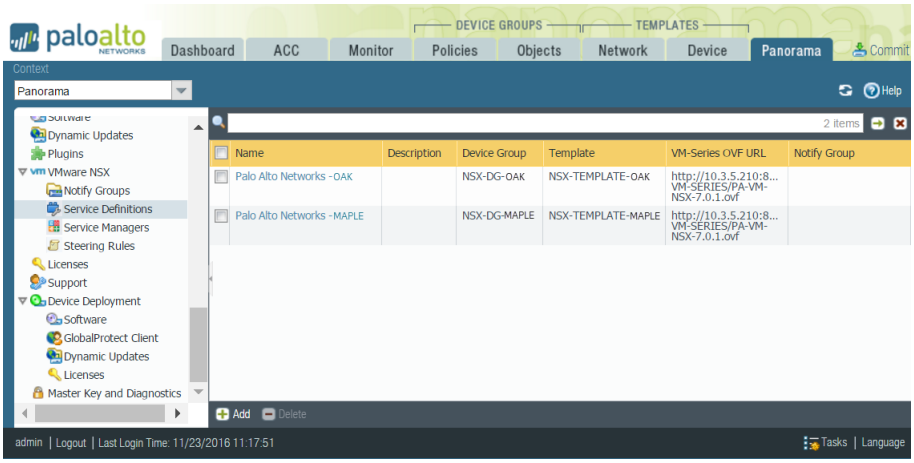
1. Log in to the Panorama web interface.
2. Select **Panorama** > **Templates** to add templates. This use case has two template named NSX-Template-MAPLE and NSX-Template-OAK.
3. Select **Panorama** > **Device Groups** and add device groups. This use case has two device groups named NSX-DG-OAK and NSX-DG-MAPLE.
4. Create NSX service profile zones within each template. To isolate traffic for each tenant in this use case, you need three zones for each tenant.
    1. Select **Network** > **Zones**.
    2. Select the correct template in the **Template** drop-down.
    3. Select **Add** and enter a zone **Name**. For example, **Tenant1**.
    4. Sets the interface **Type** to **Virtual Wire**.
    5. Click **OK**.
    6. Repeat the steps a-e to add additional zones for each sub-tenant.
    7. Verify that the zones are attached to the correct template.



5. Repeat step d for the other template.

STEP 3 | Create the Service Definitions on Panorama.

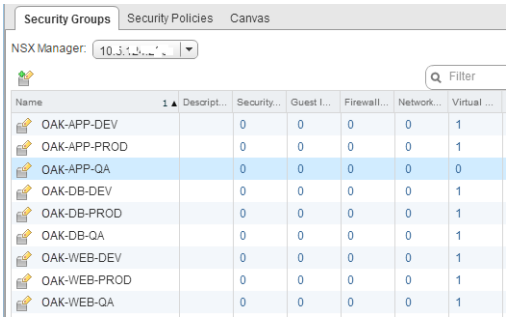
1. Select **Panorama** > **VMware NSX** > **Service Definitions**.
2. Select **Add**. Fill in the details for the service definition for each tenant. In this example, the two service definitions are Palo Alto Networks - Maple and Palo Alto Networks - Oak.



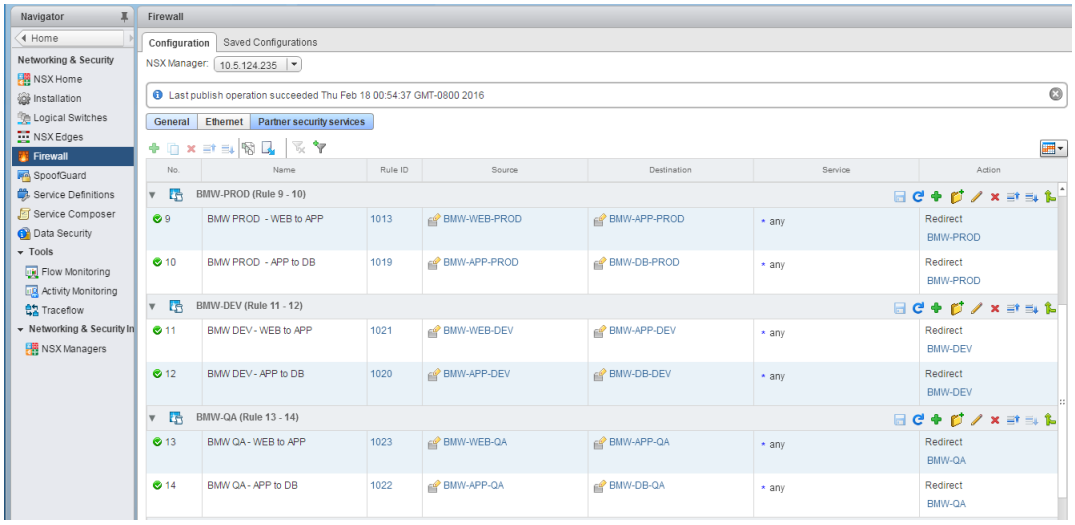
3. Click **Commit**, and select **Panorama** as the **Commit Type** to save the changes to the running configuration on Panorama.

STEP 4 | Create Security Groups and Steering Rules.

1. Select **Objects** > **Address Groups** and Set Up Dynamic Address Groups on Panorama for each tenant's virtual machines. For example, this use case has two security groups per tenant; one security group for the web servers and the other security group for the application servers.



2. Select **Policies** > **Security** > **Pre Rules** to set up security policy rules for sending traffic to the VM-Series firewall.
3. Select **Panorama** > **VMware NSX** > **Steering Rules** and click **Auto-Generate Steering Rules**.
4. **Commit** your changes

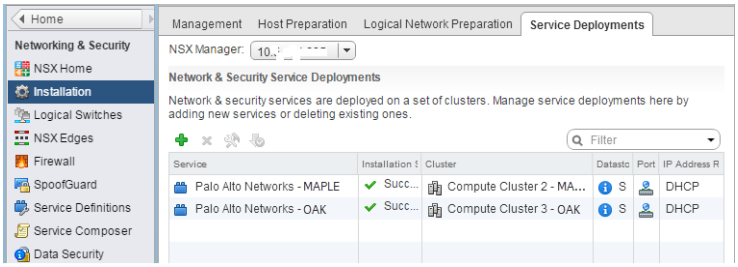


STEP 5 | Prepare the ESXi Host for the VM-Series Firewall

The ESXi hosts in the cluster must have the necessary NSX components that allow the NSX firewall and the VM-Series firewall to work together. The NSX Manager will install the components— the Ethernet Adapter Module (.eam) and the SDK —required to deploy the VM-Series firewall.

STEP 6 | Deploy the Palo Alto Networks NGFW Service

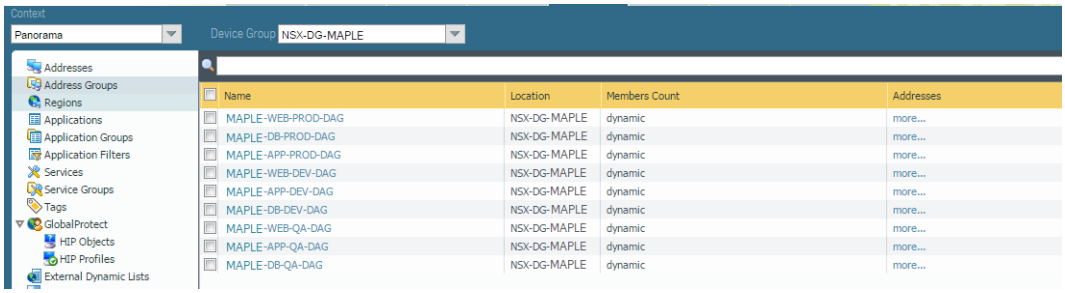
1. Select **Networking and Security** > **Installation** > **Service Deployments**.
2. Click **New Service Deployment** (green plus icon), and select the service definition for the Palo Alto Networks next generation firewall you want to deploy, **Palo Alto Networks NGFW Test 1** in this example, make your selections and click **Finish**.
3. Verify that the NSX Manager reports the **Installation Status** as **Successful**.



4. Verify that the VM-Series firewall is successfully deployed.
    1. On the vCenter server, select **Hosts and Clusters** to check that every host in each cluster has one instance of the firewall.
    2. View the management IP address(es) and the PAN-OS version running on the firewall directly from vCenter server. VMware Tools is bundled with the PAN-OS software image and is automatically enabled when you launch the VM-Series firewall.

STEP 7 | Apply Security Policies to the VM-Series Firewall

1. Create dynamic address groups for each sub-tenant on Panorama. The dynamic address group(s) match on the name of the security group(s) you defined on the NSX Manager.
    1. On Panorama, select **Objects** > **Address Groups**.
    2. Select a **Device Group** from the drop-down and click **Add**.
    3. Add a **Name** for the address group and set Type as **Dynamic** and **Add Match Criteria**. For ease of managing these groups, use the same name for the dynamic address group as that of the security group on the NSX Manager.

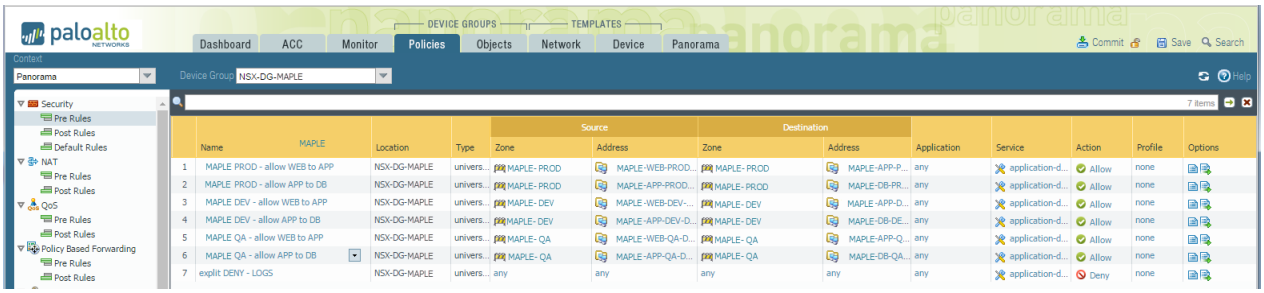


4. Create the dynamic address groups for the sub-tenants for the other tenant, Oak in this example.

2. On Panorama, create Security policies and use the dynamic address groups as source or destination address objects in security policy rules and push it to the firewalls.

    1. Select **Policies** > **Security** > **Pre Rules**.
    2. Select a **Device Group** from the drop-down and click **Add**.
    3. Create rules for each sub-tenant. Make sure to keep the source and destination zone the same in a policy rule. To ensure that only the application that is running on the server is allowed, allow the service on the application-default port only.

        This use case has the following policy rules for the tenant Maple:



3. Select the other **Device Group** from the drop-down and create the Security policies for the each sub-tenant for the other tenant, Oak in this example.
4. Click Commit, and select Commit Type as Device Groups. Select the device groups, NSX-DG-OAK and NSX-DG-MAPLE in this example and click OK.

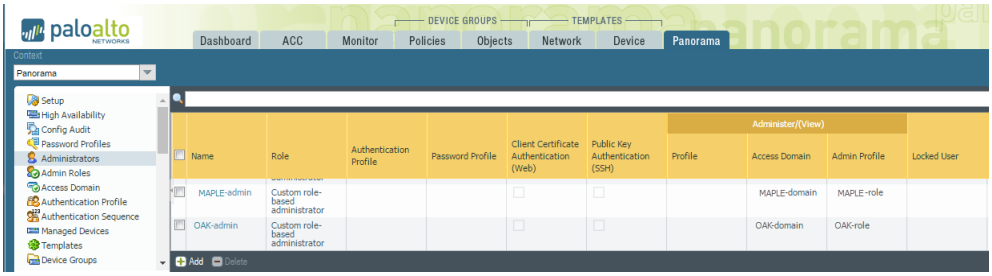
    The commit pushes the Security policies to the firewalls that belong to each device group, and they can enforce policy on the traffic redirected by the NSX Manager.

STEP 8 | Verify that traffic from each tenant is secured.

1. On Panorama, go to **Monitor** > **Logs** > **Traffic** and **Monitor** > **Logs** > **Threat** to view the Traffic logs and Threat logs. Select the device group for a tenant and sort on the Zone name for full visibility in to traffic from each sub-tenant.
2. On Panorama, use the ACC for visibility into traffic patterns and actionable information on threats. Use the widgets and filters to interact with the data on the ACC.
3. On the VM-Series firewall, select **Objects** > **Address Groups** to view the IP address for the members of each Dynamic Address Group.

STEP 9 | (Optional) Enable role-based access for tenant administrators to manage the configuration and policies for the VM-Series firewalls.

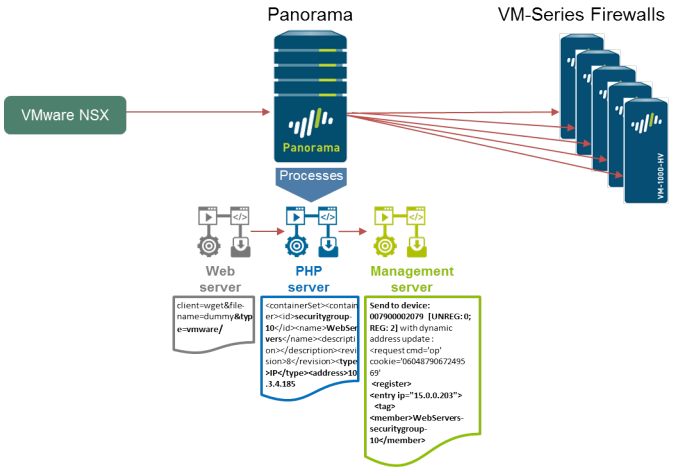
1. Create an access domain. An access domain allows you to restrict admin access to a specific device group and template. In this example, you create two access domains and restrict access to the device group and template for the respective tenant.
2. Configure an admin role for **Device Group and Template** role and allow the administrator to manage the access domain. The administrator can only manage the firewalls that belong to the access domain.
3. Create an administrative account and associate the access domain and admin role with the account.



Dynamic Address Groups—Information Relay from NSX Manager to Panorama

To enforce security policies in a VM-Series and NSX integrated data center, Panorama must be able to obtain information on the changes in the virtual landscape. As new virtual machines are deployed, changed, or deleted, the NSX Manager informs Panorama of IP addresses added, removed from security groups on the NSX Manager. Panorama in turn then, pushes this information to the VM-Series firewalls. Dynamic address groups referenced in firewall policies match against this information to determine the members that belong to the group. This process allows the firewall to enforce context-aware security policy, which secures traffic to and from these virtual machines. For details on dynamic address groups, see Policy Enforcement using Dynamic Address Groups.

The following diagram illustrates how the information is relayed from the NSX Manager to Panorama.



To understand this process, let's trace the information update sent from the NSX Manager to Panorama when a new server is added to a security group. Use the elements highlighted within the output in each phase of this example, to troubleshoot where the process failed.

STEP 1 | To view the updates in real-time, log in to the Panorama CLI.

Log in to the Command Line Interface on Panorama.

STEP 2 | Verify that the request from the NSX Manager is routed to the web server on Panorama.

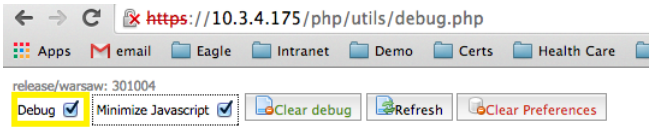
To check the webserver-log on Panorama during an NSX Security Group update, use the following command:

```
admin@Panorama> tail follow yes webserver-log cmsaccess.log
127.0.0.1 - - [Wed Dec 03 14:24:11 2014 PST] "POST /unauth/php/
RestApiAuthenticator.php HTTP/1.1" 200 433
127.0.0.1 - - [Wed Dec 03 14:24:11 2014 PST] "PUT /api/index.php?
client=wget&file-name=dummy&type=vmware/vmware/2.0/si/serviceprofile/
serviceprofile-1/containerset HTTP/1.0" 200 446
```

If your output does not include the elements above, check for routing issues. Ping the Panorama from the NSX Manager and check for ACLs or other network security devices that might be blocking the communication between the NSX Manager and Panorama.

STEP 3 | Verify that the request is parsed by the PHP daemon on Panorama.

1. Enable debug using the following URL: **https://<Panorama_IP>/php/utils/debug.php**



2. From the CLI, enter the following command to view the logs generated by the PHP server:

```
admin@Panorama> tail follow yes mp-log php.debug.log
[2014/12/03 14:24:11]
<request cmd="op" cookie="0604879067249569" refresh="no">
  <operations xml="yes">
    <show>
      <cli>
...
   <request>
      <partner>
        <vmware-service-manager>
          <update>
            <method>PUT</method>
            <type>update</type>
            <username>_vsm_admin</username>
           <password>4006474760514053</password>
<url>/vmware/2.0/si/serviceprofile/serviceprofile-1/containerset</url>
            <data><![CDATA[
<containerSet><container><id>securitygroup-10</id><name>WebServers</
name><description></description><revision>8</revision><type>IP</type><address>10.3.4.185</
address><address>10.3.4.186</address><address>15.0.0.203</address><address>15.0.0.202</
address></container></containerSet>]]></data>
```

```
</update>
        </vmware-service-manager>
      </partner>
    </request>
  </operations>
</request>
```

STEP 4 | The information is processed by the Management server on Panorama.

1. Enable debugging on the management server using the following command:

```
admin@Panorama> debug management-server on debug
```

2. Enter the following command to view the logs generated by the configd log:

```
admin@Panorama> tail follow yes mp-log configd.log
```

3. In the output check that the update was relayed from the PHP daemon to the management server daemon.

```
2014-12-03 14:24:11.143 -0800 debug:
 pan_job_progress_monitor(pan_job_mgr.c:3694): job-monitor:
 updated 0 jobs……2014-12-03 14:24:11.641 -0800 debug:
 recursive_add_params(pan_op_ctxt.c:158): > 'url'='/vmware/2.0/si/
serviceprofile/serviceprofile-1/containerset'
```

```
2014-12-03 14:24:11.641 -0800 debug:
 recursive_add_params(pan_op_ctxt.c:158): > 'data'='
<containerSet><container><id>securitygroup-10</id><name>WebServers</
name><description></description><revision>8</revision><type>IP</type><address>10.3.4.185</
address><address>10.3.4.186</address><address>15.0.0.203</address><address>15.0.0.202</
address></container></containerSet>'
2014-12-03 14:24:11.641 -0800 Received vshield update: PUT /vmware/2.0/si/
serviceprofile/serviceprofile-1/containerset
Received dynamic address update from VSM:
<request cmd='op' cookie='0604879067249569' client="xmlapi"><operations
 xml='yes'><request>
    <partner>
        <vmware-service-manager>
            <update>
                <method>PUT</method>
        <type>update</type>
<username>_vsm_admin</username>
<password>4006474760514053</password><url>/vmware/2.0/si/serviceprofile/
serviceprofile-1/containerset</url><data><![CDATA[
<containerSet><container><id>securitygroup-10</id><name>WebServers</
name><description></description><revision>8</revision><type>IP</type><address>10.3.4.185</
address><address>10.3.4.186</address><address>15.0.0.203</address><address>15.0.0.202</
address></container></containerSet>]]>
```

```
</data></update>
```

4. Look for the list of IP addresses and security group tags.

```
2014-12-03 14:24:11.646 -0800 debug:
 pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/
pan_cfg_mongo_tables.c:3721): ip: 10.3.4.185
2014-12-03 14:24:11.646 -0800 debug:
 pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/
pan_cfg_mongo_tables.c:3738): tag: WebServers-securitygroup-10
2014-12-03 14:24:11.646 -0800 debug:
 pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/
pan_cfg_mongo_tables.c:3721): ip: 15.0.0.202
2014-12-03 14:24:11.646 -0800 debug:
 pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/
pan_cfg_mongo_tables.c:3738): tag: WebServers-securitygroup-10
pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/
pan_cfg_mongo_tables.c:3738): tag: DomainControllers-securitygroup-16
2014-12-03 14:24:11.647 -0800 debug:
 pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/
pan_cfg_mongo_tables.c:3721): ip: 15.0.0.201
2014-12-03 14:24:11.648 -0800 debug:
 pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/
pan_cfg_mongo_tables.c:3738): tag: SQLServers-securitygroup-11
2014-12-03 14:24:11.665 -0800 debug:
 pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/
pan_cfg_mongo_tables.c:3738): tag: SharePointServers-securitygroup-13
2014-12-03 14:24:11.665 -0800 debug:
 pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/
pan_cfg_mongo_tables.c:3721): ip: 10.3.4.187
2014-12-03 14:24:11.665 -0800 debug:
 pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/
pan_cfg_mongo_tables.c:3738): tag: SharePointServers-securitygroup-13
```

```
...
```

5. Finally, verify that the update was relayed from the management server daemon to the managed firewalls.

```
Send to device: 007900002079 [UNREG: 0; REG: 2] with dynamic address
 update : <request cmd='op' cookie='0604879067249569' target-…. <register>
<entry ip="15.0.0.203">
  <tag>
<member>WebServers-securitygroup-10</member>
  </tag>
</entry>
<entry ip="10.3.4.186">
  <tag>
<member>WebServers-securitygroup-10</member>
  </tag>
</entry>
</register>
```

Set Up the VM-Series Firewall on AWS

The VM-Series firewall can be deployed in the public Amazon Web Services (AWS) cloud and AWS GovCloud. It can then be configured to secure access to the applications that are deployed on EC2 instances and placed into a Virtual Private Cloud (VPC) on AWS.

About the VM-Series Firewall on AWS

The Amazon Web Service (AWS) is a public cloud service that enables you to run your applications on a shared infrastructure managed by Amazon. These applications can be deployed on scalable computing capacity or EC2 instances in different AWS regions and accessed by users over the internet.

For networking consistency and ease of management of EC2 instances, Amazon offers the Virtual Private Cloud (VPC). A VPC is apportioned from the AWS public cloud, and is assigned a CIDR block from the private network space (RFC 1918). Within a VPC, you can carve public/private subnets for your needs and deploy the applications on EC2 instances within those subnets. To then enable access to the applications within the VPC, you can deploy the VM-Series firewall on an EC2 instance. The VM-Series firewall can then be configured to secure traffic to and from the EC2 instances within the VPC.

The VM-Series firewall is available in both the public AWS cloud and on AWS GovCloud. The VM-Series firewall in public AWS supports the Bring Your Own License (BYOL) model and the hourly Pay-As-You-Go (PAYG), the usage-based licensing model that you can avail from the AWS Marketplace. Because the AWS GovCloud does not have a Marketplace, the VM-Series firewall is available in the bring your own license (BYOL) option on AWS GovCloud; the usage-based (hourly or annual) options are not available on AWS GovCloud. For licensing details, see VM-Series Firewall in Amazon Web Services (AWS) and Azure Licenses.

AWS Instance Types

The VM-Series firewalls support the following AWS instance types— C3, C4, M3, M4.

You can deploy the VM-Series firewall on an AWS instance size with more resources than the minimum VM-Series System Requirements. If you choose a larger instance size for the VM-Series firewall model, although the firewall only uses the max vCPU cores and memory shown in table, it does take advantage of the faster network performance that AWS provides.

VM-Series Firewall on AWS GovCloud

AWS GovCloud is an isolated AWS region that meets the regulatory and compliance requirements of the US government agencies and customers.

To secure your workloads that contain all categories of Controlled Unclassified Information (CUI) data and government-oriented, publicly available data in the AWS GovCloud (US) Region, the VM-Series firewall provides the same robust security features in the standard AWS public cloud and on AWS GovCloud. The differences between the capability supported for the VM-Series firewall on AWS GovCloud and the standard AWS public cloud are:

- AWS Gov Cloud supports only the bring your own license (BYOL) option. The usage-based (hourly or annual) options are not available on AWS GovCloud because AWS GovCloud does not have a Marketplace.
- AWS GovCloud has a shared AMI. See AMI on AWS GovCloud to Deploy the VM-Series Firewall on AWS.
- VM-Series firewalls on PAN-OS 8.0.7 or later support bootstrapping on AWS GovCloud.

VM-Series Firewall on AWS China

The VM-Series firewall is available as a shared AMI with the BYOL option on AWS China (Beijing) region. You must have an AWS China account that is separate from your global AWS account to access this image and use AWS resources on AWS China.

To launch the VM-Series firewall in your AWS China account, find the AMI for the VM-Series firewall on the EC2 console (**Instances** > **Launch** > **Instance** > **Community AMIs**) using the AMI ID (ami-5157873c) or by searching for Palo Alto Networks. Make sure to review the VM-Series System Requirementsbefore Launch the VM-Series Firewall on AWS.

You cannot bootstrap the VM-Series firewall on AWS China.

AWS Terminology

This document assumes that you are familiar with the networking and configuration of the AWS VPC. In order to provide context for the terms used in this section, here is a brief refresher on the AWS terms (some definitions are taken directly from the AWS glossary) that are referred to in this document:

Term	Description
EC2	Elastic Compute Cloud A web service that enables you to launch and manage Linux/UNIX and Windows server instances in Amazon's datacenters.
AMI	Amazon Machine Image An AMI provides the information required to launch an instance, which is a virtual server in the cloud. The VM-Series AMI is an encrypted machine image that includes the operating system required to instantiate the VM-Series firewall on an EC2 instance.
ELB	Elastic Load Balancing ELB is an Amazon web service that helps you improve the availability and scalability of your applications by routing traffic across multiple Elastic Compute Cloud (EC2) instances. ELB detects unhealthy EC2 instances and reroutes traffic to healthy instances until the unhealthy instances are restored. ELB can send traffic only to the primary interface of the next hop load-balanced EC2 instance. So, to use ELB with a VM-Series firewall on AWS, the firewall must be able to use the primary interface for dataplane traffic.
ENI	Elastic Network Interface An additional network interface that can be attached to an EC2 instance. ENIs can include a primary private IP address, one or more secondary private IP addresses, a public IP address, an elastic IP address (optional), a MAC address, membership in specified security groups, a description, and a source/destination check flag.

Term	Description
IP address types for EC2 instances	An EC2 instance can have different types of IP addresses. • Public IP address: An IP address that can be routed across the internet. • Private IP address: A IP address in the private IP address range as defined in the RFC 1918. You can choose to manually assign an IP address or to auto assign an IP address within the range in the CIDR block for the subnet in which you launch the EC2 instance. If you are manually assigning an IP address, Amazon reserves the first four (4) IP addresses and the last one (1) IP address in every subnet for IP networking purposes. • Elastic IP address (EIP): A static IP address that you have allocated in Amazon EC2 or Amazon VPC and then attached to an instance. Elastic IP addresses are associated with your account, not with a specific instance. They are elastic because you can easily allocate, attach, detach, and free them as your needs change. An instance in a public subnet can have a Private IP address, a Public IP address, and an Elastic IP address (EIP); an instance in a private subnet will have a private IP address and optionally have an EIP.
Instance type	Amazon-defined specifications that stipulate the memory, CPU, storage capacity, and hourly cost for an instance. Some instance types are designed for standard applications, whereas others are designed for CPU-intensive, memory-intensive applications, and so on.
VPC	Virtual Private Cloud An elastic network populated by infrastructure, platform, and application services that share common security and interconnection.
IGW	Internet gateway provided by Amazon. Connects a network to the internet. You can route traffic for IP addresses outside your VPC to the internet gateway.
IAM Role	Identity and Access Management Required for enabling High Availability for the VM-Series firewall on AWS. The IAM role defines the API actions and resources the application can use after assuming the role. On failover, the IAM Role allows the VM-Series firewall to securely make API requests to switch the dataplane interfaces from the active peer to the passive peer. An IAM role is also required for VM Monitoring. See List of Attributes Monitored on the AWS VPC.
Subnets	A segment of the IP address range of a VPC to which EC2 instances can be attached. EC2 instances are grouped into subnets based on your security and operational needs. There are two types of subnets: • Private subnet: The EC2 instances in this subnet cannot be reached from the internet.

Term	Description
	• Public subnet: The internet gateway is attached to the public subnet, and the EC2 instances in this subnet can be reached from the internet.
Security groups	A security group is attached to an ENI and it specifies the list of protocols, ports, and IP address ranges that are allowed to establish inbound/outbound connections on the interface. *In the AWS VPC, security groups and network ACLs control inbound and outbound traffic; security groups regulate access to the EC2 instance, while network ACLs regulate access to the subnet. Because you are deploying the VM-Series firewall, set more permissive rules in your security groups and network ACLs and allow the firewall to safely enable applications in the VPC.*
Route tables	A set of routing rules that controls the traffic leaving any subnet that is associated with the route table. A subnet can be associated with only one route table.
Key pair	A set of security credentials you use to prove your identity electronically. The key pair consists of a private key and a public key. At time of launching the VM-Series firewall, you must generate a key pair or select an existing key pair for the VM-Series firewall. The private key is required to access the firewall in maintenance mode.
CloudWatch	Amazon CloudWatch is a monitoring service that allows you to collect and track metrics for the VM-Series firewalls on AWS. When enabled, the firewalls use AWS APIs to publish native PAN-OS metrics to CloudWatch.

Management Interface Mapping for Use with Amazon ELB

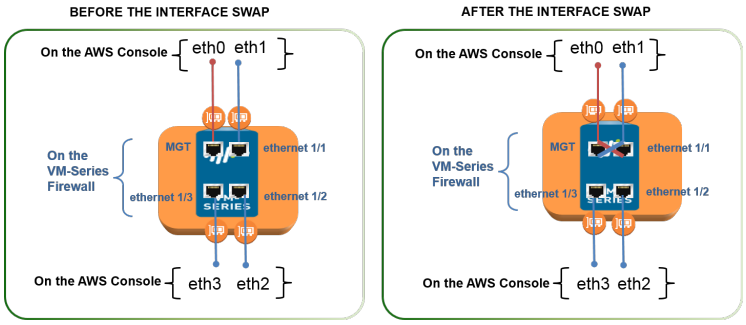
By default, the elastic network interface (ENI) eth0 maps to the MGT interface on the firewall and ENI eth1 maps to ethernet 1/1 on the firewall. Because the ELB can send traffic only to the primary interface of the next hop load-balanced EC2 instance, the VM-Series firewall must be able to use the primary interface for dataplane traffic.

The firewall can receive dataplane traffic on the primary interface in the following scenarios where the VM-Series firewall is behind the Amazon ELB (for a topology diagram, see VM-Series with ELB):

- The VM-Series firewall(s) is securing traffic outbound directly to the internet without the need for using a VPN link or a Direct Connect link back to the corporate network.
- The VM-Series firewall secures an internet-facing application when there is exactly one back-end server, such as a web server, for each firewall. The VM-Series firewalls and web servers can scale linearly, in pairs, behind ELB.

At present, for use cases that require an ELB sandwich-type deployment to scale out firewalls and application layer EC2 instances, swapping the management interface will not allow you to seamlessly deploy the ELB solution. The ability to swap the management interface only partially solves the integration with ELB.

To allow the firewall to send and receive dataplane traffic on eth0 instead of eth1, you must swap the mapping of the ENIs within the firewall such that ENI eth0 maps to ethernet 1/1 and ENI eth1 maps to the MGT interface on the firewall as shown below.



Swapping how the interfaces are mapped allows ELB to distribute and route traffic to healthy instances of the VM-Series firewall located in the same or different Availability Zones on AWS for increased capacity and fault tolerance.

To swap the interfaces, you have the following options:

- **At launch**—When you launch the firewall, you can either enter the **`mgmt-interface-swap=enable`** command in the **User data** field on the AWS management console (see Launch the VM-Series Firewall on AWS) or CLI or you can include the new **`mgmt-interface-swap`** operational command in the bootstrap configuration.
- **After launch**—After you launch the firewall, Use the VM-Series Firewall CLI to Swap the Management Interface (**`set system setting mgmt-interface-swap enable yes`** operational command) on the firewall.

- *Pick one method to consistently specify the interface swap setting—in the bootstrap configuration, from the CLI on the firewall, or using the Amazon EC2 User data field on the AWS console—to prevent unpredictable behavior on the firewall.*
- *Ensure that you have access to the AWS console (management console or CLI) to view the IP address of the eth1 interface. Also, verify that the AWS Security Group rules allow connections (HTTPS and SSH) to the new management interface.*
- *Swap the management interface before you configure the firewall or define policy rules. If you have already configured the VM-Series firewall, check whether any IP address changes for eth0 and eth1 impact policy rules.*

Deployments Supported on AWS

The VM-Series firewall secures inbound and outbound traffic to and from EC2 instances within the AWS Virtual Private Cloud (VPC). Because the AWS VPC only supports an IP network (Layer 3 networking capabilities), the VM-Series firewall can only be deployed with Layer 3 interfaces.

- Deploy the VM-Series firewall to secure the EC2 instances hosted in the AWS Virtual Private Cloud.

  If you host your applications in the AWS cloud, deploy the VM-Series firewall to protect and safely enable applications for users who access these applications over the internet. For example, the following diagram shows the VM-Series firewall deployed in the Edge subnet to which the internet gateway is attached. The application(s) are deployed in the private subnet, which does not have direct access to the internet.

  When users need to access the applications in the private subnet, the firewall receives the request and directs it to the appropriate application, after verifying security policy and performing Destination NAT. On the return path, the firewall receives the traffic, applies security policy and uses Source NAT to deliver the content to the user. See Use Case: Secure the EC2 Instances in the AWS Cloud.

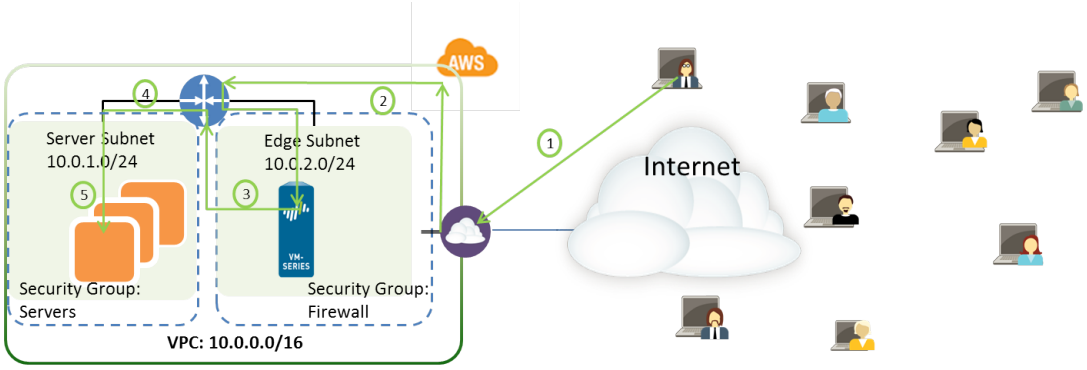


Figure 9: VM-Series for EC2 Instances

- Deploy the VM-Series firewall for VPN access between the corporate network and the EC2 instances within the AWS Virtual Private Cloud.

  To connect your corporate network with the applications deployed in the AWS Cloud, you can configure the firewall as a termination point for an IPSec VPN tunnel. This VPN tunnel allows users on your network to securely access the applications in the cloud.

  For centralized management, consistent enforcement of policy across your entire network, and for centralized logging and reporting, you can also deploy Panorama in your corporate network. If you need to set up VPN access to multiple VPCs, using Panorama allows you to group the firewalls by region and administer them with ease.

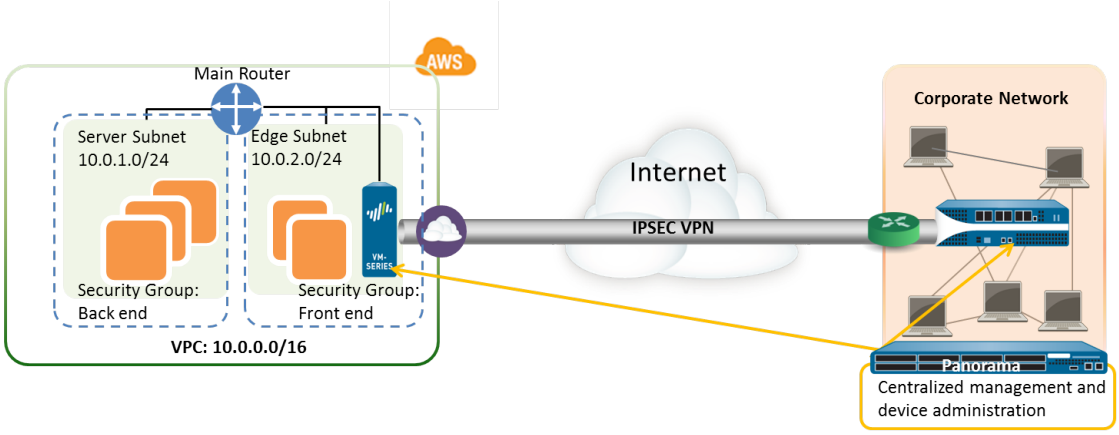


Figure 10: VM-Series for VPN Access

- Deploy the VM-Series firewall as a GlobalProtect gateway to secure access for remote users using laptops. The GlobalProtect agent on the laptop connects to the gateway, and based on the request, the gateway either sets up a VPN connection to the corporate network or routes the request to the internet. To enforce security compliance for users on mobile devices (using the GlobalProtect App), the GlobalProtect gateway is used in conjunction with the GlobalProtect Mobile Security Manager. The GlobalProtect Mobile Security Manager ensures that mobile devices are managed and configured with the device settings and account information for use with corporate applications and networks.

  In each of the use cases above, you can deploy the VM-Series firewall in an active/passive high availability (HA) pair. For information on setting up the VM-Series firewall in HA, see Use Case: Use Dynamic Address Groups to Secure New EC2 Instances within the VPC.

- Deploy the VM-Series firewall with the Amazon Elastic Load Balancing (ELB) service, whereby the firewall can receive dataplane traffic on the primary interface in the following scenarios where the VM-Series firewall is behind the Amazon ELB:
  - The VM-Series firewall(s) is securing traffic outbound directly to the internet without the need for using a VPN link or a Direct Connect link back to the corporate network.
  - The VM-Series firewall secures an internet-facing application when there is exactly one back-end server, such as a web server, for each firewall. The VM-Series firewalls and web servers can scale linearly, in pairs, behind ELB.

  If you want to Auto Scale VM-Series Firewalls with the Amazon ELB, use the CloudFormation Template available in the GitHub repository to deploy the VM-Series in an ELB sandwich topology with an internet-facing classic ELB and an either an internal classic load balancer or an internal application load balancer (internal ELB).

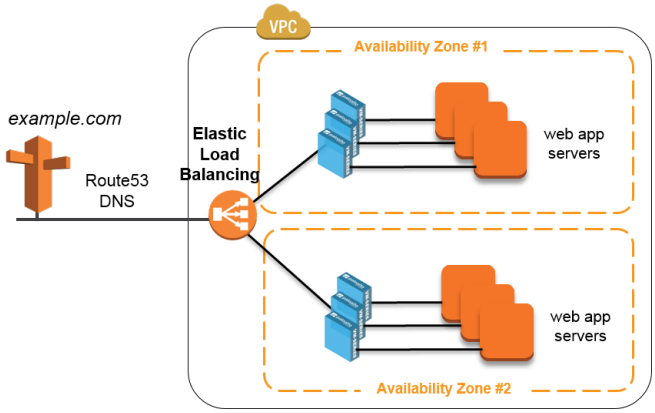


Figure 11: VM-Series with ELB

You cannot configure the firewall to send and receive dataplane traffic on eth0 when the firewall is in front of ELB. The VM-Series firewall must be placed behind the Amazon ELB.

You can either Use the VM-Series Firewall CLI to Swap the Management Interface *or enable it on bootstrap. For details, see* Management Interface Mapping for Use with Amazon ELB*.*

If you want to deploy a load balancer sandwich topology, see Auto Scale VM-Series Firewalls with the Amazon ELB*.*

Deploy the VM-Series Firewall on AWS

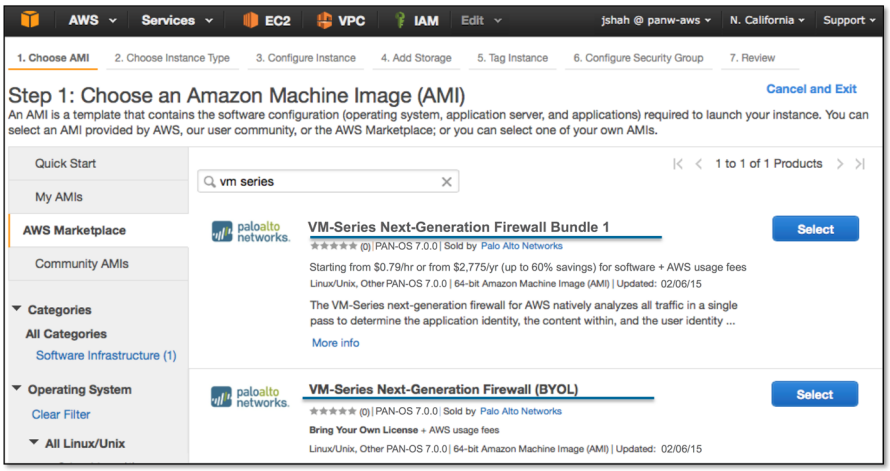
The VM-Series firewall has been optimized and expanded to deliver improved performance and expanded capacities, which necessitates a change in the number of cores and memory allocated to the EC2 instance. For the new resource footprint, you need to match the appropriate Instance sizes available on AWS before you upgrade your VM-Series firewalls on AWS running PAN-OS 7.1 or earlier versions.; For details, refer to Upgrading the VM-Series with PAN-OS 8.0 on AWS*.*

Obtain the AMI

Because the AWS GovCloud does not have a Marketplace, the process of obtaining the AMI is different in the public AWS cloud and in the AWS GovCloud.

AMI in the Public AWS Cloud

The AMI for the VM-Series firewall is available in the AWS Marketplace for both the Bring Your Own License (BYOL) and the Usage-based pricing options.



For purchasing licenses with the BYOL option, contact your Palo Alto Networks sales engineer or reseller.

AMI on AWS GovCloud

The Bring Your Own License (BYOL) model of the VM-Series firewall is available as a shared AMI on AWS GovCloud.

With a GovCloud account you can find the AMI for the VM-Series firewall on the EC2 console (**Instances** > **Launch Instance** > **Community AMIs**) using the AMI ID (ami-4add672b) or by searching for Palo Alto Networks. Alternatively, you can also use the link to directly launch the AMI in your GovCloud account.

Make sure to review the supported EC2 instance types before you launch the firewall. For details, see Launch the VM-Series Firewall on AWS.

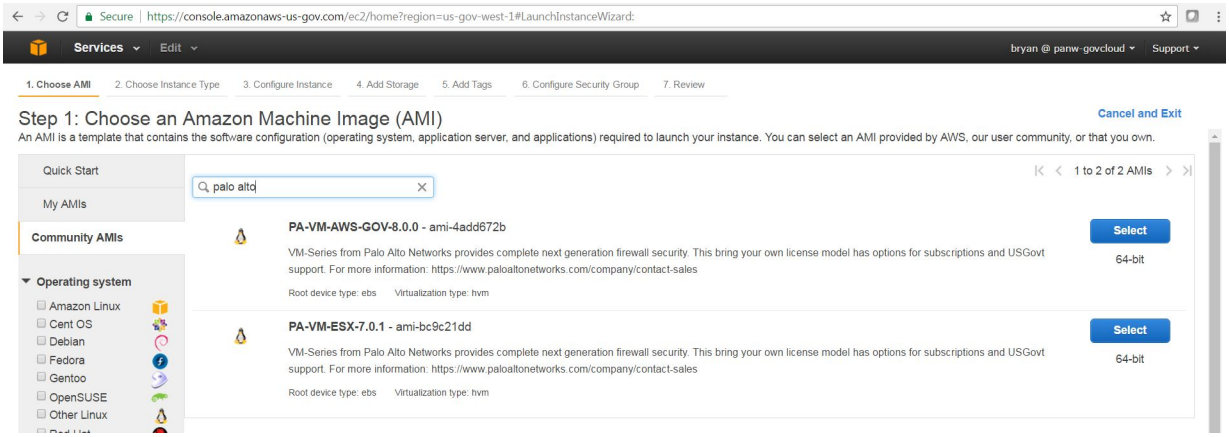


Table 1: Review System Requirements and Limitations for VM-Series on AWS

Requirement	Details
EC2 instance types	The EC2 instance type you select must meet the VM-Series System Requirements for the VM-Series firewall model. If you deploy the VM-Series firewall on an EC2 instance type that does not meet these requirements, the firewall will boot into maintenance mode *To support VM Monitoring and high availability on AWS, the VM-Series firewall must be able to directly reach the AWS API service endpoints without any proxy servers between the firewall management interface and the AWS API endpoints (such as ec2.us-west-2.amazonaws.com).*
Amazon Elastic Block Storage (EBS)	The VM-Series firewall must use the Amazon Elastic Block Storage (EBS) volume for storage. EBS optimization provides an optimized configuration stack and additional, dedicated capacity for Amazon EBS I/O.
Networking	Because the AWS only supports Layer 3 networking capabilities, the VM-Series firewall can only be deployed with Layer 3 interfaces. Layer 2 interfaces, virtual wire, VLANs, and subinterfaces are not supported on the VM-Series firewall deployed in the AWS VPC.
Interfaces	Support for a total of eight interfaces is available—one management interface and a maximum of seven Elastic Network Interfaces (ENIs) for data traffic. The VM-Series firewall does not support hot attachment of ENIs; to detect the addition or removal of an ENI you must reboot the firewall. *Your EC2 instance type selection determines the total number of ENIs you can enable. For example, the c3.8xlarge supports eight (8) ENIs.*
Support entitlement and Licenses	For the Bring Your Own License model, a support account and a valid VM-Series license are required to obtain the Amazon Machine Image (AMI) file, which is required to install the VM-Series firewall in the AWS VPC. The

Requirement	Details
	licenses required for the VM-Series firewall—capacity license, support license, and subscriptions for Threat Prevention, URL Filtering, WildFire, etc—must be purchased from Palo Alto Networks. To purchase the licenses for your deployment, contact your sales representative. See VM-Series Firewall in Amazon Web Services (AWS) and Azure Licenses. For the usage-based licensing model, hourly and annual pricing bundles can be purchased and billed directly to AWS. You must however, register your support entitlement with Palo Alto Networks. For details see, Register the Usage-Based Model of the VM-Series Firewall in AWS and Azure (no auth code).

Planning Worksheet for the VM-Series in the AWS VPC

For ease of deployment, plan the subnets within the VPC and the EC2 instances that you want to deploy within each subnet. Before you begin, use the following table to collate the network information required to deploy and insert the VM-Series firewall into the traffic flow in the VPC:

Configuration Item	Value
VPC CIDR	
Security Groups	
Subnet (public) CIDR	
Subnet (private) CIDR	
Subnet (public) Route Table	
Subnet (private) Route Table	
Security Groups • Rules for Management Access to the firewall (eth0/0) • Rules for access to the dataplane interfaces of the firewall • Rules for access to the interfaces assigned to the application servers.	
VM-Series firewall behind ELB	
EC2 Instance 1 (VM-Series firewall) *An EIP is only required for the dataplane interface*	Subnet: Instance type: Mgmt interface IP: Mgmt interface EIP:

Configuration Item	Value
that is attached to the public subnet.	Dataplane interface eth1/1 • Private IP: • EIP (if required): • Security Group: Dataplane interface eth1/2 • Private IP: • EIP (if required): • Security Group:
EC2 Instance 2 (Application to be secured) Repeat these set of values for additional application(s) being deployed.	Subnet: Instance type: Mgmt interface IP: Default gateway: Dataplane interface 1 • Private IP
Requirements for HA	If you are deploying the VM-Series firewalls in a high availability (active/passive) configuration, you must ensure the following: • Create an IAM role and assign the role to the VM-Series firewall when you are deploying the instance. See IAM Roles for HA. • Deploy the HA peers in the same AWS availability zone. • The active firewall in the HA pair must have at a minimum three ENIs: two dataplane interfaces and one management interface. The passive firewall in the HA pair, must have one ENI for management, and one ENI that functions as dataplane interface; you will configure the dataplane interface as an HA2 interface. *Do not attach additional dataplane interfaces to the passive firewall in the HA pair. On failover, the dataplane interfaces from the previously active firewall are moved — detached and then attached—to the now active (previously passive) firewall.*

Launch the VM-Series Firewall on AWS

If you have not already registered the capacity auth-code that you received with the order fulfillment email, with your support account, see Register the VM-Series Firewall. After registering, deploy the VM-Series firewall by launching it in the AWS VPC as follows:

STEP 1 | Access the AWS Console.

Log in to the AWS console and select the EC2 Dashboard.

STEP 2 | Set up the VPC for your network needs.

Whether you launch the VM-Series firewall in an existing VPC or you create a new VPC, the VM-Series firewall must be able to receive traffic from the EC2 instances and perform inbound and outbound communication between the VPC and the internet.

Refer to the AWS VPC documentation for instructions on creating a VPC and setting it up for access.

For an example with a complete workflow, see Use Case: Secure the EC2 Instances in the AWS Cloud.

1. Create a new VPC or use an existing VPC. Refer to the AWS Getting Started documentation.
2. Verify that the network and security components are defined suitably.
   - Enable communication to the internet. The default VPC includes an internet gateway, and if you install the VM-Series firewall in the default subnet it has access to the internet.
   - Create subnets. Subnets are segments of the IP address range assigned to the VPC in which you can launch the EC2 instances. The VM-Series firewall must belong to the public subnet so that it can be configured to access the internet.
   - Create security groups as needed to manage inbound and outbound traffic from the EC2 instances/subnets.
   - Add routes to the route table for a private subnet to ensure that traffic can be routed across subnets and security groups in the VPC, as applicable.
3. If you want to deploy a pair of VM-Series firewalls in HA, you must define IAM Roles for HA before you can Configure Active/Passive HA on AWS.
4. (Optional) If you are using bootstrapping to perform the configuration of your VM-Series firewall, refer to Bootstrap the VM-Series Firewall on AWS. For more information about bootstrapping, see Bootstrap the VM-Series Firewall.

STEP 3 | Launch the VM-Series firewall.

Although you can add additional network interfaces (ENIs) to the VM-Series firewall when you launch, AWS releases the auto-assigned Public IP address for the management interface when you restart the firewall. Hence, to ensure connectivity to the management interface you must assign an Elastic IP address for the management interface, before attaching additional interfaces to the firewall.

If you want to conserve EIP addresses, you can assign one EIP address to the eth 1/1 interface and use this interface for both management traffic and data traffic. To restrict services permitted on the interface or limit IP addresses that can log in the eth 1/1 interface, attach a management profile to the interface.

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 VPC.
   3. Select the public subnet to which the VM-Series management interface will attach.
   4. Select **Automatically assign a public IP address**. This allows you to obtain a publicly accessible IP address for the management interface of the VM-Series firewall.

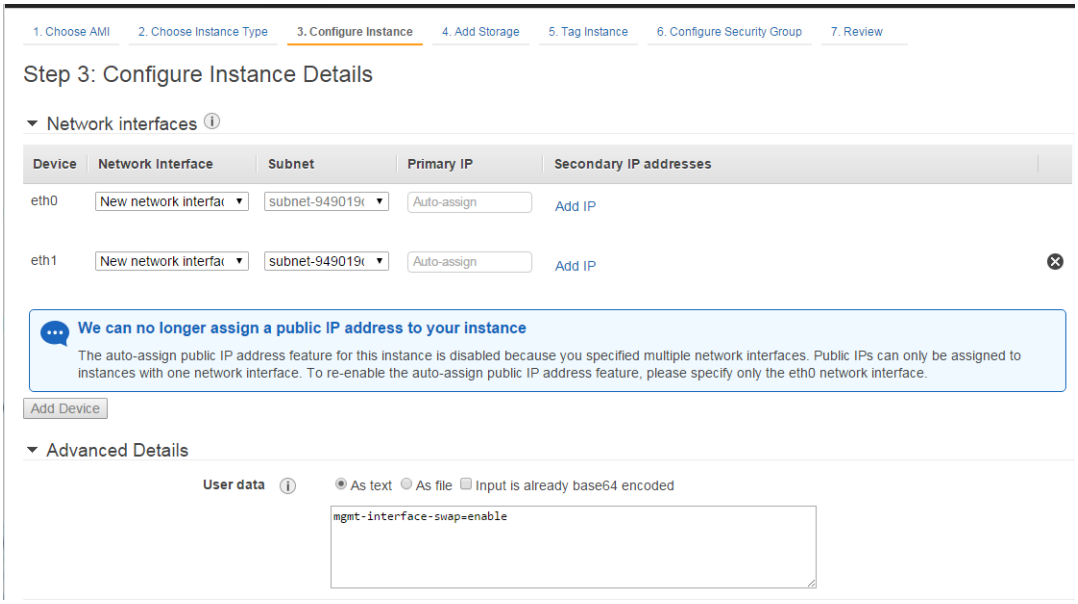
      You can later attach an Elastic IP address to the management interface; unlike the public IP address that is disassociated from the firewall when the instance is terminated, the Elastic IP address provides persistence and can be reattached to a new (or replacement) instance of the

VM-Series firewall without the need to reconfigure the IP address wherever you might have referenced it.

5. Select **Launch as an EBS-optimized instance**.
6. Add another network interface for deployments with ELB so that you can swap the management and data interfaces on the firewall. 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`** as text to perform the interface swap during launch.



7. Accept the default **Storage** settings.

   This key pair is required for first time access to the firewall. It is also required to access the firewall in maintenance mode.
8. (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.
9. Select an existing **Security Group** or create a new one. This security group is for restricting access to the management interface of the firewall. At a minimum consider enabling https and ssh access for the management interface.
10. If prompted, select an appropriate **SSD** option for your setup.
11. Select **Review and Launch**. Review that your selections are accurate and click **Launch**.
12. Select an existing key pair or create a new one, and acknowledge the key disclaimer.
13. 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 4 | 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 public IP address 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 steps 3-xii to access the CLI.

   If you added an additional ENI to support deployments with ELB, you must first create and assign an Elastic IP address to the ENI to access the CLI, see step 6.

   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 aceess 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 5 | Shutdown the VM-Series firewall.

1. On the EC2 Dashboard, select **Instances**.
2. From the list, select the VM-Series firewall and click **Actions** > **Stop**.

STEP 6 | Create and assign an Elastic IP address (EIP) to the ENI used for management access to the firewall and reboot the VM-Series firewall.

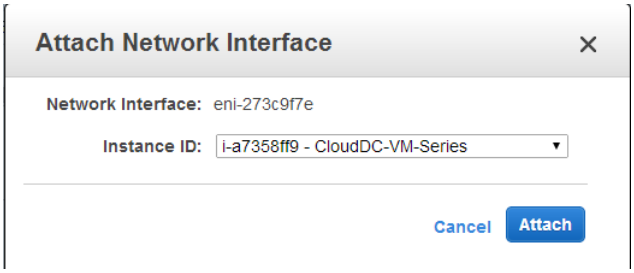
1. Select **Elastic IPs** and click **Allocate New Address**.
2. Select **EC2-VPC** and click **Yes, Allocate**.
3. Select the newly allocated EIP and click **Associate Address**.
4. Select the **Network Interface** and the **Private IP address** associated with the management interface and click **Yes,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

STEP 7 | Create virtual network interface(s) and attach the interface(s) to the VM-Series firewall. The virtual network interfaces are called Elastic Network Interfaces (ENIs) on AWS, and serve as the dataplane network interfaces on the firewall. These interfaces are used for handling data traffic to/from the firewall.

You will need at least two ENIs that allow inbound and outbound traffic to/from the firewall. You can add up to seven ENIs to handle data traffic on the VM-Series firewall; check your EC2 instance type to verify the maximum number supported on it.

1. On the EC2 Dashboard, select **Network Interfaces**, and click **Create Network Interface**.
2. Enter a descriptive name for the interface.
3. Select the subnet. Use the subnet ID to make sure that you have selected the correct subnet. You can only attach an ENI to an instance in the same subnet.
4. Enter the **Private IP** address to assign to the interface or select **Auto-assign** to automatically assign an IP address within the available IP addresses in the selected subnet.
5. Select the **Security group** to control access to the dataplane network interface.
6. Click **Yes, Create**.

7. To attach the ENI to the VM-Series firewall, select the interface you just created, and click **Attach**.



8. Select the **Instance ID** of the VM-Series firewall, and click **Attach**.
9. Repeat the steps above for creating and attaching at least one more ENI to the firewall.

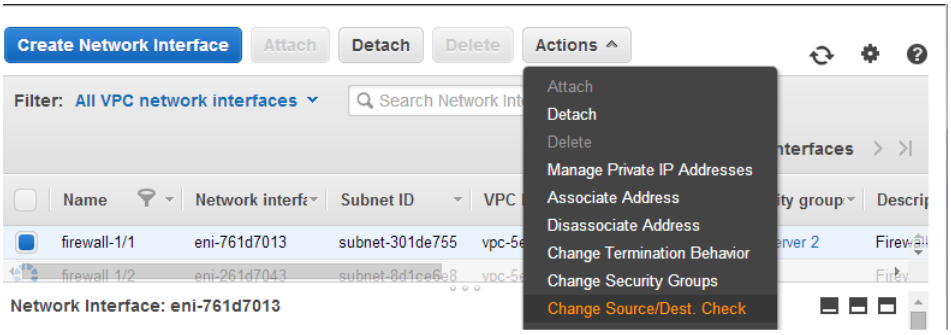
STEP 8 | (Not required for the Usage-based licensing model) Activate the licenses on the VM-Series firewall.

This task is not performed on the AWS management console. Access to the Palo Alto Networks support portal and the web interface of the VM-Series firewall is required for license activation.

See Activate the License.

STEP 9 | Disable Source/Destination check on every firewall dataplane network interface(s). Disabling this option allows the interface to handle network traffic that is not destined to the IP address assigned to the network interface.

1. On the EC2 Dashboard, select the network interface, for example eth1/1, in the **Network Interfaces** tab.
2. In the **Action** drop-down, select **Change Source/Dest. Check**.



3. Click **Disabled** and **Save** your changes.
4. Repeat Steps 1-3 for each firewall dataplane interface.

STEP 10 | Configure the dataplane network interfaces as Layer 3 interfaces on the firewall.

For an example configuration, see steps 14 through 17 in Use Case: Secure the EC2 Instances in the AWS Cloud.

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>). 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, for example VM_Series_untrust, and then click **OK**.
   - On the **IPv4** tab, select either **Static** or **DHCP Client**.

     If using the **Static** option, click **Add** in the IP section, and enter the IP address and network mask for the interface, for example 10.0.0.10/24.

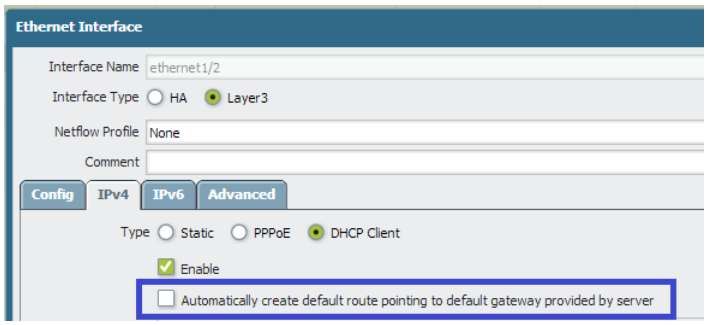
     Make sure that the IP address matches the ENI IP address that you assigned earlier.

     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.
4. Click the link for **ethernet 1/2** and configure as follows:
   - **Interface Type**: **Layer3**
   - Security Zone: VM_Series_trust
   - **IP address**: Select the **Static** or **DHCP Client** radio button.

     For static, click **Add** in the IP section, and enter the IP address and network mask for the interface. Make sure that the IP address matches the attached ENI IP address that you assigned earlier.
5. Click **Commit**. Verify that the link state for the interfaces are up.

For DHCP, clear the Automatically create default route to default gateway provided by server check box. For an interface that is attached to the private subnet in the VPC,

disabling this option ensures that traffic handled by this interface does not flow directly to the internet gateway on the VPC.



STEP 11 | Create NAT rules to allow inbound and outbound traffic from the servers deployed within the VPC.

1. Select **Policies** > **NAT** on the web interface of the firewall.
2. Create a NAT rule to allow traffic from the dataplane network interface on the firewall to the web server interface in the VPC.
3. Create a NAT rule to allow outbound access for traffic from the web server to the internet.

STEP 12 | Create security policies to allow/deny traffic to/from the servers deployed within the VPC.

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

STEP 13 | Commit the changes on the firewall.

Click **Commit**.

STEP 14 | Verify that the VM-Series firewall is securing traffic and that the NAT rules are in effect.

1. Select **Monitor** > **Logs** > **Traffic** on the web interface of the firewall.
2. View the logs to make sure that the applications traversing the network match the security policies you implemented.

Use the VM-Series Firewall CLI to Swap the Management Interface

If you did not swap the management interface (MGT) with the dataplane interface (ethernet 1/1) when deploying the firewall, you can use the CLI to enable the firewall to receive dataplane traffic on the primary interface after launching the firewall.

STEP 1 | Complete Steps 1 through 7 in Launch the VM-Series Firewall on AWS.

Before you proceed, verify that the firewall has a minimum of two ENIs (eth0 and eth1). If you launch the firewall with only one ENI, the interface swap command will cause the firewall to boot into maintenance mode.

STEP 2 | On the EC2 Dashboard, view the IP address of the eth1 interface and verify that the AWS Security Group rules allow connections (HTTPS and SSH) to the new management interface (eth1).

STEP 3 | Log in to the VM-Series firewall CLI and enter the following command:

```
set system setting mgmt-interface-swap enable yes
```

STEP 4 | Confirm that you want to swap the interface and use the eth1 dataplane interface as the management interface.

STEP 5 | Reboot the firewall for the swap to take effect. Use the following command:

```
request restart system
```

STEP 6 | Verify that the interfaces have been swapped. Use the following command:

```
debug show vm-series interfaces all
Phoenix_interface   Base-OS_port   Base-OS_MAC        PCI-ID         Driver
mgt(interface-swap) eth0   0e:53:96:91:ef:29   0000:00:04.0   ixgbevf
Ethernet1/1           eth1    0e:4d:84:5f:7f:4d       0000:00:03.0
  ixgbevf
```

Enable CloudWatch Monitoring on the VM-Series Firewall on AWS

The VM-Series firewall on AWS can publish native PAN-OS metrics to AWS CloudWatch, which you can use to monitor the firewalls. These metrics allow you to assess performance and usage patterns that you can use to take action for launching or terminating instances of the VM-Series firewalls.

The firewalls use AWS APIs to publish the metric to a *namespace* on AWS at a specified time interval. The namespace is the location to which CloudWatch collects and aggregates the selected metric for all instances configured to use the namespace. You can then monitor the metric in CloudWatch or create auto scaling policies to trigger alarms and take an action to manually deploy a new instance of the firewall when the monitored metric reaches a threshold value. Refer to the AWS CloudWatch and Auto Scaling Groups (ASG) documentation on best practices for setting the alarm conditions for a scale out or scale in action.

The VM-Series firewall can publish any of the following PAN-OS metrics to CloudWatch:

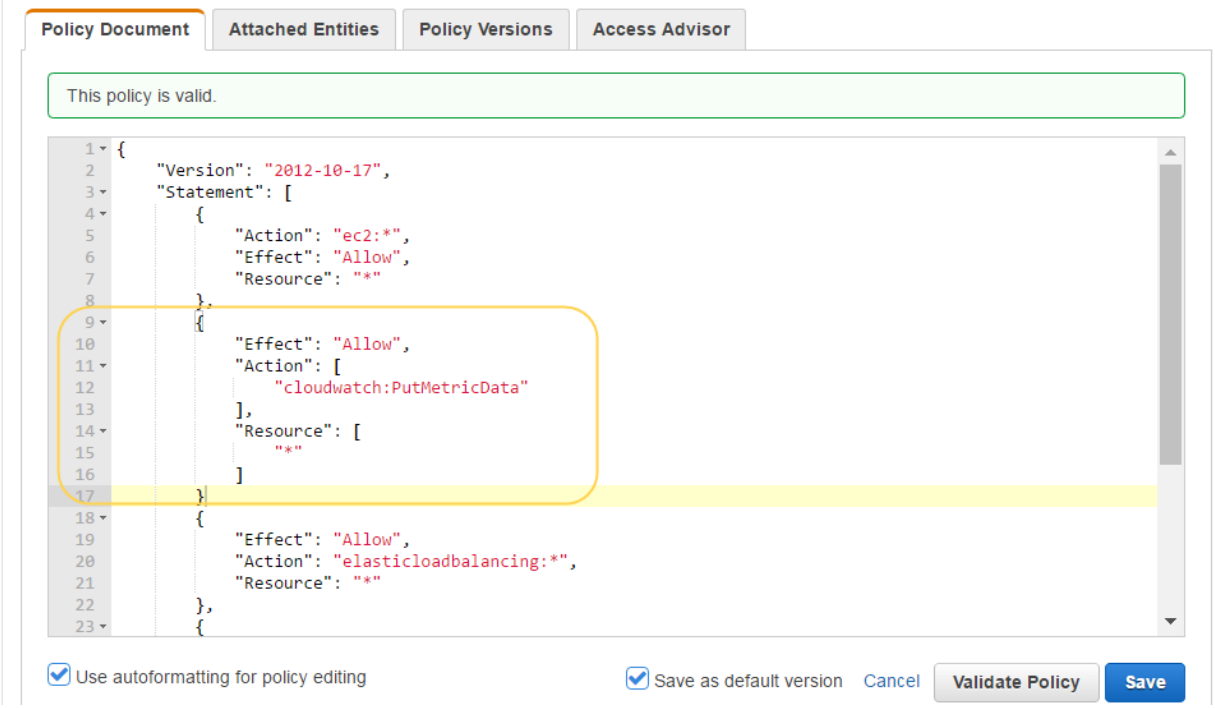
Metric	Description
Dataplane CPU Utilization (%)	Monitors the dataplane CPU usage to measure the traffic load on the firewall.
Dataplane Packet Buffer Utilization (%)	Monitors the dataplane buffer usage to measure buffer utilization. If you have a sudden burst in traffic, monitoring buffer utilization allows you to ensure that the firewall does not deplete the dataplane buffer and drop packets.
Session Utilization (%)	Monitors the sessions are currently active for TCP, UDP, ICMP and SSL and the packet rate, new connection establish rate, and throughput on the firewall to determine session utilization.
SSLProxyUtilization (%)	Monitors the percentage of SSL forward proxy sessions with clients for SSL/TLS decryption.

Metric	Description
GlobalProtect Gateway Tunnel Utilization (%)	Monitors the active GlobalProtect tunnels set up on a gateway to measure tunnel utilization. Use this metric if the VM-Series firewall is deployed as a VPN gateway on AWS to secure remote users.
Total Active Sessions	Monitors the total number of sessions that are active on the firewall. An active session is a session that is on the firewall's flow lookup table for which packets will be inspected and forwarded, as required by policy.
GlobalProtect Gateway Active Tunnels	Monitors the number of active GlobalProtect sessions on a firewall deployed as a GlobalProtect gateway. Use this metric if the VM-Series firewall is deployed a VPN gateway on AWS to secure remote users; check the datasheet for the maximum number of active tunnels supported for your firewall model.

STEP 1 | Assign the appropriate permissions for the AWS Identity and Access Management (IAM) user role that you use to deploy the VM-Series firewall on AWS.

Whether you newly Launch the VM-Series Firewall on AWS or upgrade an existing VM-Series firewall on AWS to PAN-OS 8.0, the IAM role associated with your instance must have permissions to publish metrics to CloudWatch.

1. On the AWS console, select IAM.
2. Edit the IAM role to grant the following permissions:



STEP 2 | Enable CloudWatch on the VM-Series firewall on AWS.

1. Log in to the web interface on the VM-Series firewall
2. Select **Device** > **Operations** > **AWS CloudWatch**.

3. Select **Enable CloudWatch Monitoring**.
4. Enter the **CloudWatch Namespace** to which the firewall can publish metrics. The namespace cannot begin with **AWS**.
5. Set the **Update Interval** to a value between 1-60 minutes. This is the frequency at which the firewall publishes the metrics to CloudWatch. The default is 5 minutes.
6. **Commit** the changes.

   Until the firewall starts to publish metrics to CloudWatch, you cannot configure alarms for PAN-OS metrics.

STEP 3 | Verify that you can see the metrics on CloudWatch.

1. On the AWS console, select **CloudWatch** > **Metrics**, to view CloudWatch metrics by category.
2. From the Custom Metrics drop-down, select the namespace.
3. Verify that you can see PAN-OS metrics in the viewing list.

STEP 4 | Configure alarms and action for PAN-OS metrics on CloudWatch.

Refer to the AWS documentation: http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/AlarmThatSendsEmail.html

A VM-Series firewall with bootstrap configuration will take about 7-9 minutes to be available for service. So, here are some examples on how to set alarms that trigger auto scaling for the VM-Series firewall:

- If you have deployed 2 instances of the VM-Series firewalls as Global Protect Gateways that secure remote users, use the GlobalProtect Gateway Active Tunnels metric. You can configure an alarm for when the number of active tunnels is greater than 300 for 15 minutes, you can deploy 2 new instances of the VM-Series firewall, which are bootstrapped and configured to serve as Global Protect Gateways.
- If you are using the firewall to secure your workloads in AWS, use the Session Utilization metric to scale in or scale out the firewall based on resource usage. You can configure an alarm for when the session utilization metric is greater than 60% for 15 minutes, to deploy one instance of the VM-Series instance firewall. And conversely, if Session Utilization is less than 50% for 30 minutes, terminate an instance of the VM-Series firewall.

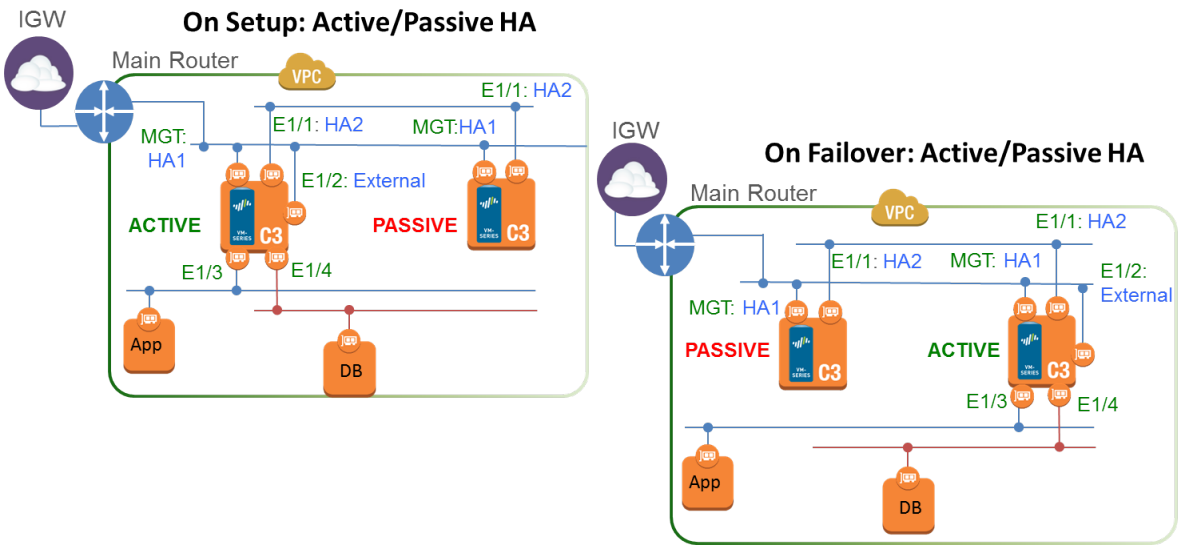
High Availability for VM-Series Firewall on AWS

The VM-Series firewall on AWS supports active/passive HA only; if it is deployed with Amazon Elastic Load Balancing (ELB), it does not support HA (in this case ELB provides the failover capabilities).

- Overview of HA on AWS
- IAM Roles for HA
- HA Links
- Heartbeat Polling and Hello Messages
- Device Priority and Preemption
- HA Timers
- Configure Active/Passive HA on AWS

Overview of HA on AWS

To ensure redundancy, you can deploy the VM-Series firewalls on AWS in an active/passive high availability (HA) configuration. The active peer continuously synchronizes its configuration and session information with the identically configured passive peer. A heartbeat connection between the two devices ensures failover if the active device goes down. When the passive peer detects this failure it becomes active and triggers API calls to the AWS infrastructure to move all the dataplane interfaces (ENIs) from the failed peer to itself. The failover time can vary from 20 seconds to over a minute depending on the responsiveness from the AWS infrastructure.



IAM Roles for HA

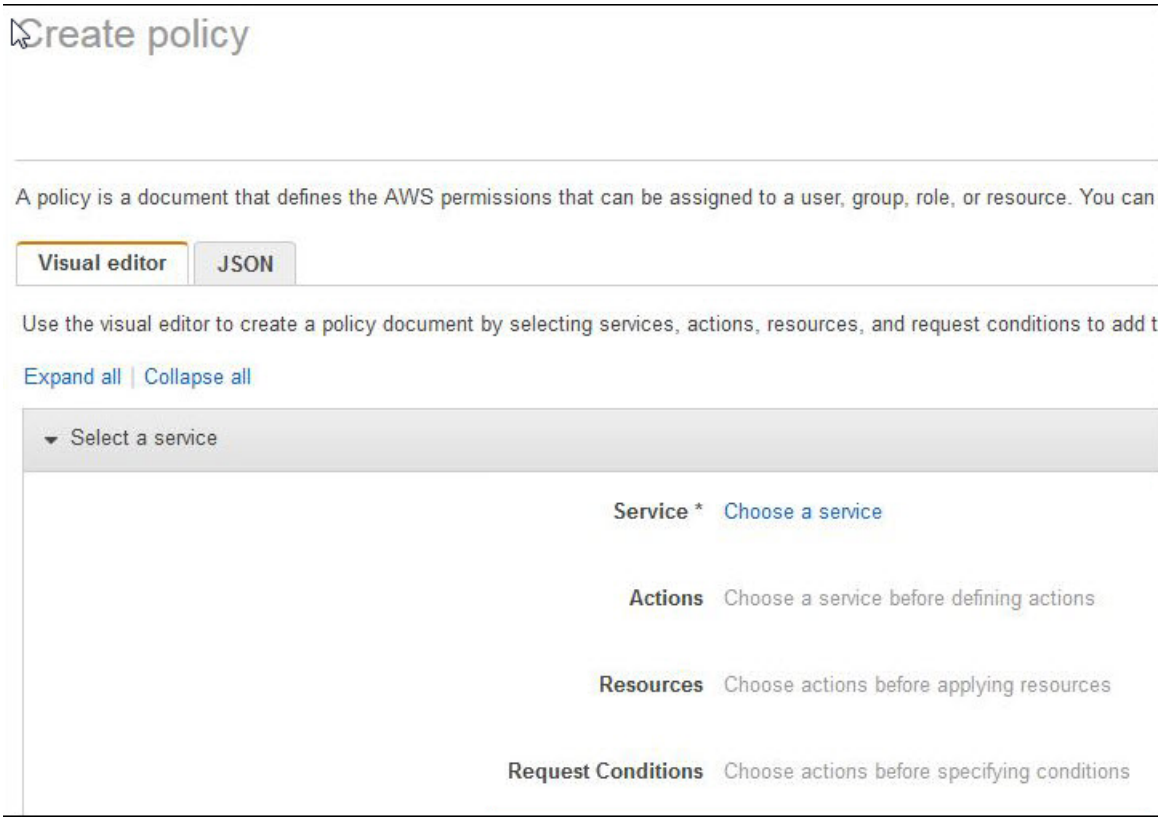
AWS requires that all API requests must be cryptographically signed using credentials issued by them. In order to enable API permissions for the VM-Series firewalls that will be deployed as an HA pair, you must create a policy and attach that policy to a role in the AWS Identity and Access Management (IAM) service. The role must be attached to the VM-Series firewalls at launch. The policy gives the IAM role permissions for initiating API actions for detaching and attaching network interfaces from the active peer in an HA pair to the passive peer when a failover is triggered.

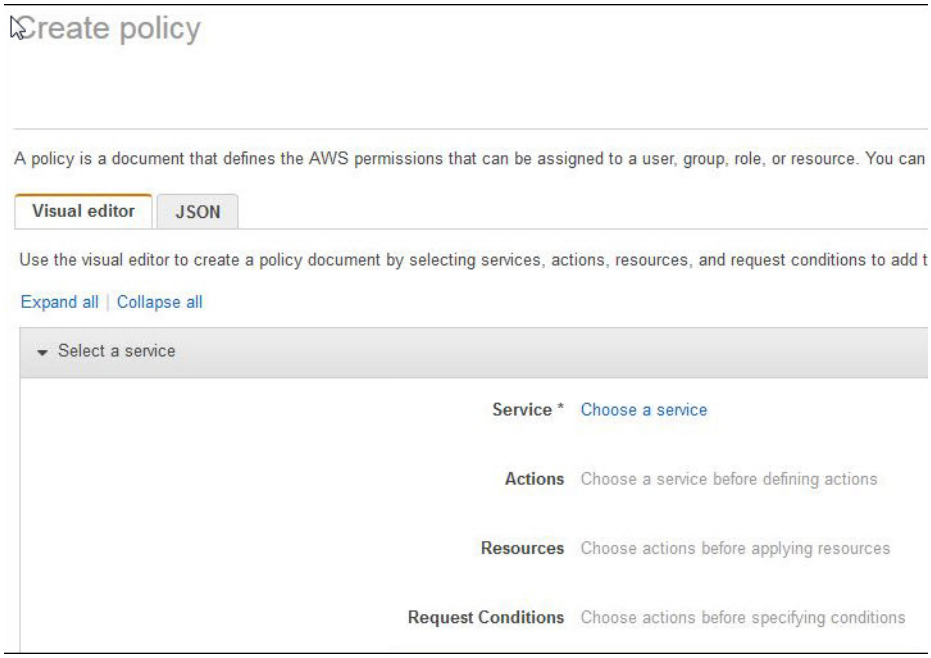
For detailed instructions on creating policy, refer to the AWS documentation on Creating Customer Managed Polices. For detailed instructions on creating an IAM role, defining which accounts or AWS services can assume the role, defining which API actions and resources the application can use upon assuming the role, refer to the AWS documentation on IAM Roles for Amazon EC2.

The IAM policy, which is configured in the AWS console, must have permissions for the following actions and resources (at a minimum):

- AttachNetworkInterface—For permission to attach an ENI to an instance.
- DescribeNetworkInterface—For fetching the ENI parameters in order to attach an interface to the instance.
- DetachNetworkInterface—For permission to detach the ENI from the EC2 instance.
- DescribeInstances—For permission to obtain information on the EC2 instances in the VPC.
- Wild card (*)—In the Amazon Resource Name (ARN) field use the * as a wild card.

The following screenshot shows the access management settings for the IAM role described above:





The permissions you need are:

```
{"Version": "2012-10-17","Statement": [{"Sid": "VisualEditor0","Effect":
"Allow","Action":
["ec2:AttachNetworkInterface","ec2:DetachNetworkInterface","ec2:DescribeInstances","ec2:D
"*"}]}
```

HA Links

The devices in an HA pair use HA links to synchronize data and maintain state information. on AWS, the VM-Series firewall uses the following ports:

- **Control Link**—The HA1 link is used to exchange hellos, heartbeats, and HA state information, and management plane sync for routing and User-ID information. This link is also used to synchronize configuration changes on either the active or passive device with its peer.

  The Management port is used for HA1. TCP port 28769 and 28260 for cleartext communication; port 28 for encrypted communication (SSH over TCP).
- **Data Link**—The HA2 link is used to synchronize sessions, forwarding tables, IPSec security associations and ARP tables between devices in an HA pair. Data flow on the HA2 link is always unidirectional (except for the HA2 keep-alive); it flows from the active device to the passive device.

  Ethernet1/1 must be assigned as the HA2 link. The HA data link can be configured to use either IP (protocol number 99) or UDP (port 29281) as the transport.

The VM-Series on AWS does not support backup links for HA1 or HA2.

Heartbeat Polling and Hello Messages

The firewalls use hello message and heartbeats to verify that the peer device is responsive and operational. Hello messages are sent from one peer to the other at the configured *Hello Interval* to verify the state of the device. The heartbeat is an ICMP ping to the HA peer over the control link, and the peer responds to the ping to establish that the devices are connected and responsive. For details on the HA timers that trigger a failover, see HA Timers. (The HA timers for the VM-Series firewall are the same as that of the PA-5000 Series firewalls).

Device Priority and Preemption

The devices in an HA pair can be assigned a *device priority* value to indicate a preference for which device should assume the active role and manage traffic upon failover. If you need to use a specific device in the HA pair for actively securing traffic, you must enable the preemptive behavior on both the firewalls and assign a device priority value for each device. The device with the lower numerical value, and therefore *higher priority*, is designated as active and manages all traffic on the network. The other device is in a passive state, and synchronizes configuration and state information with the active device so that it is ready to transition to an active state should a failure occur.

By default, preemption is disabled on the firewalls and must be enabled on both devices. When enabled, the preemptive behavior allows the firewall with the *higher priority* (lower numerical value) to resume as active after it recovers from a failure. When preemption occurs, the event is logged in the system logs.

HA Timers

High availability (HA) timers are used to detect a firewall failure and trigger a failover. To reduce the complexity in configuring HA timers, you can select from three profiles: **Recommended**, **Aggressive**, and **Advanced**. These profiles auto-populate the optimum HA timer values for the specific firewall platform to enable a speedier HA deployment.

Use the **Recommended** profile for typical failover timer settings and the **Aggressive** profile for faster failover timer settings. The **Advanced** profile allows you to customize the timer values to suit your network requirements.

HA Timer on the VM-Series on AWS	Default values for Recommended/Aggressive profiles
Promotion hold time	2000/500 ms
Hello interval	8000/8000 ms
Heartbeat interval	2000/1000 ms
Max number of flaps	3/3
Preemption hold time	1/1 min
Monitor fail hold up time	0/0 ms
Additional master hold up time	500/500 ms

Configure Active/Passive HA on AWS

STEP 1 | Make sure that you have followed the prerequisites.

For deploying a pair of VM-Series firewalls in HA in the AWS cloud, you must ensure the following:

- Select the IAM role you created when launching the VM-Series firewall on an EC2 instance; you cannot assign the role to an instance that is already running. See IAM Roles for HA.

  For detailed instructions on creating an IAM role, defining which accounts or AWS services can assume the role, and defining which API actions and resources the application can use upon assuming the role, refer to the AWS documentation.

- The active firewall in the HA pair must have at a minimum three ENIs: two dataplane interfaces and one management interface.

  The passive firewall in the HA pair, must have one ENI for management, and one ENI that functions as dataplane interface; you will configure the dataplane interface as an HA2 interface.

  Do not attach additional dataplane interfaces to the passive firewall in the HA pair. On failover, the dataplane interfaces from the previously active firewall are moved — detached and then attached—to the now active (previously passive) firewall.
- The HA peers must be deployed in the same AWS availability zone.

STEP 2 | Launch the VM-Series Firewall on AWS.

IMPORTANT: If you are using the PAN-OS 8.0 AMI to deploy the VM-Series firewall on AWS, you must upgrade to 8.0.1 before you configure HA.

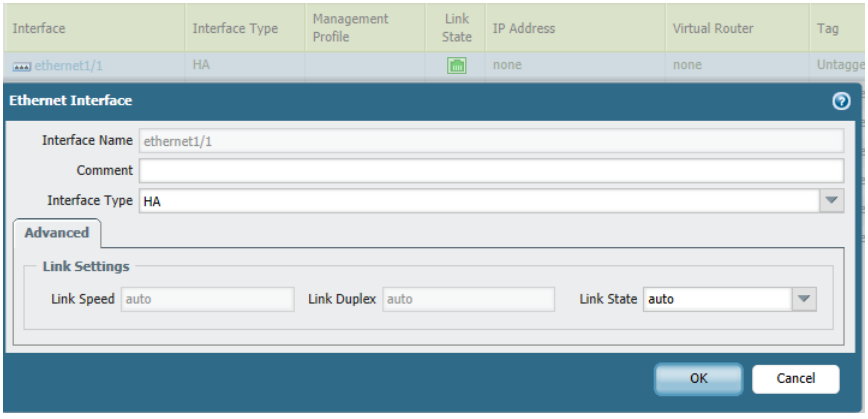
1. Select **Device** > **Software**, and click **Check Now** for latest updates.
2. **Download** PAN-OS 8.0.1 (or later) version to upgrade.
3. **Install** the update.
4. After the installation successfully completes, reboot using one of the following methods:
   1. If you are prompted to reboot, click **Yes**.
   2. If you are not prompted to reboot, select **Device** > **Setup** > **Operations** and **Reboot Device** (Device Operations section).

STEP 3 | Enable HA.

1. Select **Device** > **High Availability** > **General**, and edit the Setup section.
2. Select **Enable HA**.

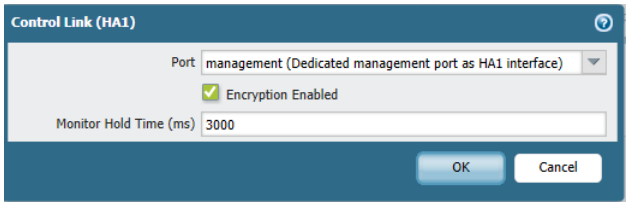
STEP 4 | Configure ethernet 1/1 as an HA interface. This interface must be used for HA2 communication.

1. Select **Network** > **Interfaces**.
2. Confirm that the link state is up on ethernet1/1.
3. Click the link for ethernet1/1 and set the **Interface Type** to HA.



STEP 5 | Set up the Control Link (HA1) to use the management port.

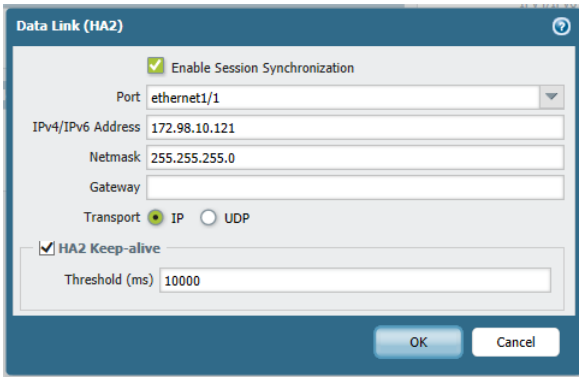
1. Select **Device** > **High Availability** > **General**, and edit the Control Link (HA1) section.



2. (Optional) Select **Encryption Enabled**, for secure HA communication between the peers. To enable encryption, you must export the HA key from a device and import it into the peer device.
   1. Select **Device** > **Certificate Management** > **Certificates**.
   2. Select **Export HA key**. Save the HA key to a network location that the peer device can access.
   3. On the peer device, navigate to **Device** > **Certificate Management** > **Certificates**, and select **Import HA key** to browse to the location that you saved the key and import it in to the peer device.

STEP 6 | Set up the Data Link (HA2) to use ethernet1/1.

1. Select **Device** > **High Availability** > **General**, edit the Data Link (HA2) section.
2. Select **Port** ethernet1/1.
3. Enter the IP address for ethernet1/1. This IP address must be the same that assigned to the ENI on the EC2 Dashboard.
4. Enter the **Netmask**.
5. Enter a **Gateway** IP address if the HA1 interfaces are on separate subnets.
6. Select **IP** or **UDP** for **Transport**. Use **IP** if you need Layer 3 transport (IP protocol number 99). Use **UDP** if you want the firewall to calculate the checksum on the entire packet rather than just the header, as in the IP option (UDP port 29281).



7. (Optional) Modify the **Threshold** for **HA2 Keep-alive** packets. By default, **HA2 Keep-alive** is enabled for monitoring the HA2 data link between the peers. If a failure occurs and this threshold (default is 10000 ms) is exceeded, the defined action will occur. A critical system log message is generated when an HA2 keep-alive failure occurs.

   You can configure the HA2 keep-alive option on both devices, or just one device in the HA pair. If you enable this option on one device, only that device will send the keep-alive messages.

STEP 7 | Set the device priority and enable preemption.

Use this setting if you want to make sure that a specific device is the preferred active device. For information, see Device Priority and Preemption.

1. Select **Device** > **High Availability** > **General** and edit the Election Settings section.
2. Set the numerical value in **Device Priority**. Make sure to set a lower numerical value on the device that you want to assign a higher priority to.

If both firewalls have the same device priority value, the firewall with the lowest MAC address on the HA1 control link will become the active device.

3. Select **Preemptive**.

   You must enable preemptive on both the active and the passive device.
4. Modify the failover timers. By default, the HA timer profile is set to the **Recommended** profile and is suited for most HA deployments.

STEP 8 | (Optional) Modify the wait time before a failover is triggered.

1. Select **Device** > **High Availability** > **General** and edit the Active/Passive Settings.
2. Modify the **Monitor fail hold up time** to a value between 1-60 minutes; default is 1 minute. This is the time interval during which the firewall will remain active following a link failure. Use this setting to avoid an HA failover triggered by the occasional flapping of neighboring devices.

STEP 9 | Configure the IP address of the HA peer.

1. Select **Device** > **High Availability** > **General**, and edit the Setup section.
2. Enter the IP address of the HA1 port on the peer. This is the IP address assigned to the management interface (ethernet 0/0), which is also the HA1 link on the other firewall.
3. Set the **Group ID** number between 1 and 63. Although this value is not used on the VM-Series firewall on AWS, but cannot leave the field blank.

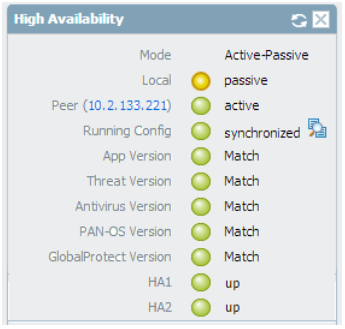
STEP 10 | Configure the other peer.

Repeat steps 3 to 9 on the HA peer.

STEP 11 | After you finish configuring both devices, verify that the devices are paired in active/passive HA.

1. Access the **Dashboard** on both devices, and view the **High Availability** widget.
2. On the active device, click the **Sync to peer** link.
3. Confirm that the devices are paired and synced, as shown below:

   - On the passive device: The state of the local device should display **passive** and the configuration is **synchronized**.



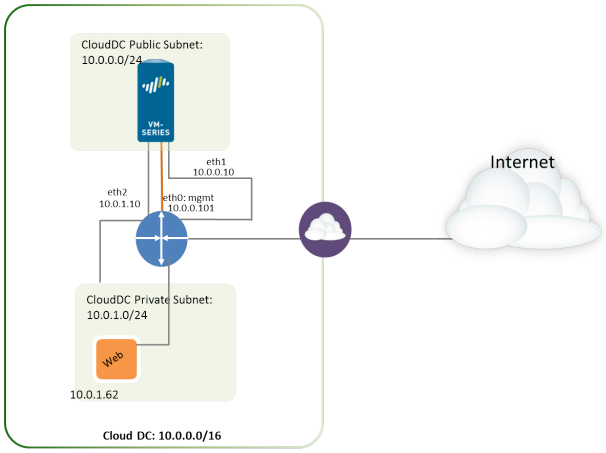
   - On the active device: The state of the local device should display **active** and the configuration is **synchronized**.

STEP 12 | Verify that failover occurs properly.

1. Shut down the active HA peer.
    1. On the EC2 Dashboard, select **Instances**.
    2. From the list, select the VM-Series firewall and click **Actions** > **Stop**.
2. Check that the passive peer assumes the role of the active peer and that the dataplane interfaces have moved over to the now active HA peer.

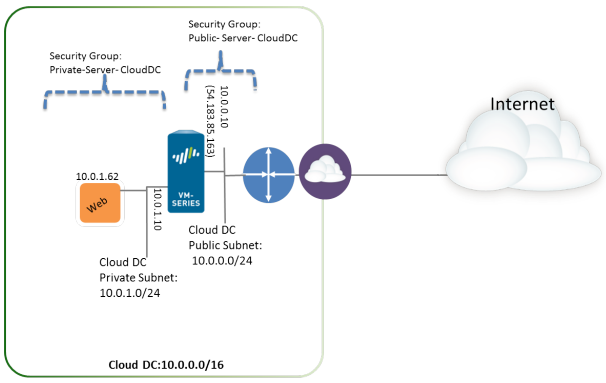
Use Case: Secure the EC2 Instances in the AWS Cloud

In this example, the VPC is deployed in the 10.0.0.0/16 network with two /24 subnets: 10.0.0.0/24 and 10.0.1.0/24. The VM-Series firewall will be launched in the 10.0.0.0/24 subnet to which the internet gateway is attached. The 10.0.1.0/24 subnet is a private subnet that will host the EC2 instances that need to be secured by the VM-Series firewall; any server on this private subnet uses NAT for a routable IP address (which is an Elastic IP address) to access the internet. Use the Planning Worksheet for the VM-Series in the AWS VPC to plan the design within your VPC; recording the subnet ranges, network interfaces and the associated IP addresses for the EC2 instances, and security groups, will make the setup process easier and more efficient.



The following image depicts the logical flow of traffic to/from the web server to the internet. Traffic to/from the web server is sent to the data interface of the VM-Series firewall that is attached to the private subnet. The firewall applies policy and processes incoming/outgoing traffic from/to the internet gateway of the VPC. The image also shows the security groups to which the data interfaces are attached.

Logical Traffic Flow Diagram



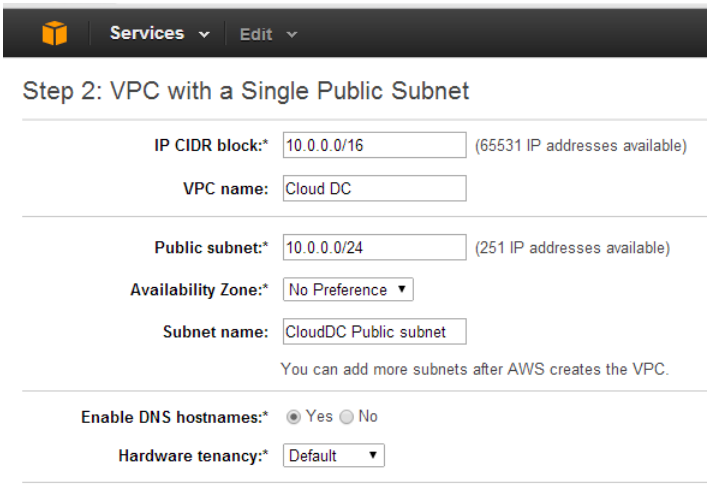
The management IP address and the security group associated with it, are not depicted in this diagram

STEP 1 | Create a new VPC with a public subnet (or select an existing VPC).

1. Log in to the AWS console and select the **VPC** Dashboard.
2. Verify that you've selected the correct geographic area (AWS region). The VPC will be deployed in the currently selected region.

3. Select **Start VPC Wizard**, and select **VPC with a Single Public Subnet**.

   In this example, the IP CIDR block for the VPC is 10.0.0.0/16, the VPC name is Cloud DC, the public subnet is 10.0.0.0/24, and the subnet name is Cloud DC Public subnet. You will create a private subnet after creating the VPC.

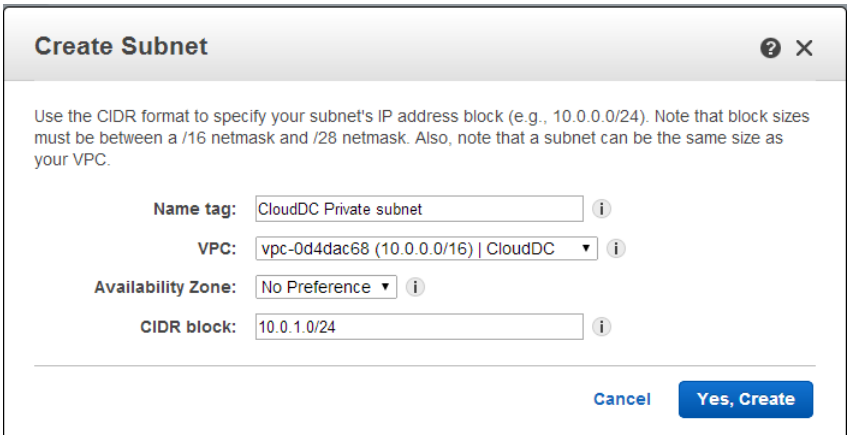


4. Click **Create VPC**.

STEP 2 | Create a private subnet.

Select **Subnets**, and click **Create a Subnet**. Fill in the information.

In this example, the **Name tag** for the subnet is Web/DB Server Subnet, it is created in the Cloud Datacenter VPC and is assigned a CIDR block of 10.0.1.0/24.



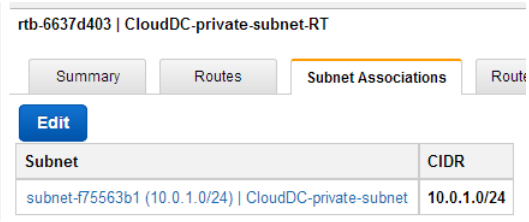
STEP 3 | Create a new route table for each subnet.

Although a main route table is automatically created on the VPC, we recommend creating new route tables instead of modifying the default route table.

To direct outbound traffic from each subnet, you will add routes to the route table associated with each subnet, later in this workflow.

1. Select **Route Tables** > **Create Route Table**.
2. Add a **Name**, for example CloudDC-public-subnet-RT, select the **VPC** you created in step 1, and click **Yes, Create**.
3. Select the route table, click **Subnet Associations** and select the public subnet.

4. Select **Create Route Table**.
5. Add a **Name**, for example CloudDC-private-subnet-RT, select the **VPC** you created in step 1, and click **Yes, Create**.
6. Select the route table, click **Subnet Associations** and select the private subnet.



STEP 4 | Create Security Groups to restrict inbound/outbound internet access to the EC2 instances in the VPC.

By default, AWS disallows communication between interfaces that do not belong to the same security group.

Select **Security Groups** and click the **Create Security Group** button. In this example, we create three security groups with the following rules for inbound access:

- CloudDC-Management that specifies the protocols and source IP addresses that can connect to the management interface of the VM-Series firewall. At a minimum you need SSH, and HTTPS. In this example, we enable SSH, ICMP, HTTP, and HTTPS on the network interfaces that are attached to this security group.

  The management interface (eth 0/0) of the VM-Series firewall will be assigned to CloudDC-management-sg.
- Public-Server-CloudDC that specifies the source IP addresses that can connect over HTTP, FTP, SSH within the VPC. This group allows traffic from the external network to the firewall.

  The dataplane interface eth1/1 of the VM-Series firewall will be assigned to Public-Server-CloudDC.
- Private-Server-CloudDC that has very limited access. It only allows other EC2 instances on the same subnet to communicate with each other, and with the VM-Series firewall.

  The dataplane interface eth1/2 of the VM-Series firewall and the application in the private subnet will be attached to this security group.

  The following screenshot shows the security groups for this use case.

Name tag	Group ID	Group Name	VPC	Description
CloudDC-private-subnet-sg	sg-6c32c409	Private-Server-CloudDC	vpc-0d4dac68 (10.0.0.0/16) |...	For Private Servers to comm...
CloudDC-public-subnet-sg	sg-6832c40d	Public-Server-CloudDC	vpc-0d4dac68 (10.0.0.0/16) |...	External Traffic to VM-Series
CloudDC-management-sg	sg-9735c3f2	CloudDC-Managment	vpc-0d4dac68 (10.0.0.0/16) |...	CloudDC-Management
	sg-1035c375	default	vpc-0d4dac68 (10.0.0.0/16) |...	default VPC security group

STEP 5 | Deploy the VM-Series firewall.

Only the primary network interface that will serve as the management interface will be attached and configured for the firewall during the initial launch. The network interfaces required for handling data traffic will be added in step 6.

See step 3 in Launch the VM-Series Firewall on AWS.

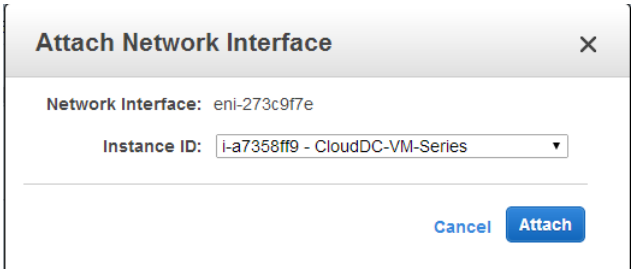
STEP 6 | Create and attach virtual network interface(s), referred to as Elastic Network Interfaces (ENIs), to the VM-Series firewall. These ENIs are used for handling data traffic to/from the firewall.

1. On the EC2 Dashboard, select **Network Interfaces**, and click **Create Network Interface**.
2. Enter a descriptive name for the interface.
3. Select the subnet. Use the subnet ID to make sure that you have selected the correct subnet. You can only attach an ENI to an instance in the same subnet.
4. Enter the **Private IP** address that you want to assign to the interface or select **Auto-assign** to automatically assign an IP address within the available IP addresses in the selected subnet.
5. Select the **Security group** to control access to the network interface.
6. Click **Yes, Create**.

   In this example, we create two interfaces with the following configuration:

Name	Network interfa	Subnet ID	VPC ID	Zone	Security group	Description	Instance ID
CloudDC-VM-Series-Untrust	eni-bcf355e5	subnet-ef5563a9	vpc-0d4dac68	us-west-1a	Public-Server-...	CloudDC-VM-Series-untrust	i-a7358ff9
CloudDC-VM-Series-Trust	eni-abf355f2	subnet-f75563b1	vpc-0d4dac68	us-west-1a	Private-Server-...	CloudDC-VM-Series-Trust	i-a7358ff9

   - For Eth1/1 (VM-Series-Untrust)
     - Subnet: 10.0.0.0/24
     - Private IP:10.0.0.10
     - Security group: Public-Server-CloudDC
   - For Eth1/2 (VM-Series-Trust)
     - Subnet: 10.0.1.0/24
     - Private IP:10.0.1.10
     - Security group: Private-Server-CloudDC
7. To attach the ENI to the VM-Series firewall, select the interface you just created, and click **Attach**.



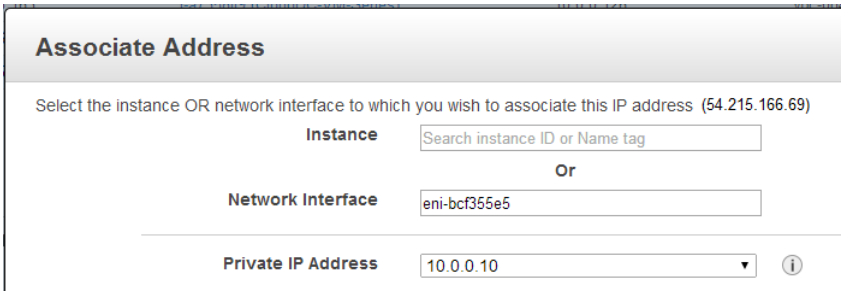
8. Select the **Instance ID** of the VM-Series firewall, and click **Attach**.
9. Repeat steps 7 and 8 to attach the other network interface.

STEP 7 | Create an Elastic IP address and attach it to the firewall dataplane network interface that requires direct internet access.

In this example, VM-Series_Untrust is assigned an EIP. The EIP associated with the interface is the publicly accessible IP address for the web server in the private subnet.

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 interface and click **Yes, Associate**.



In this example, the configuration is:

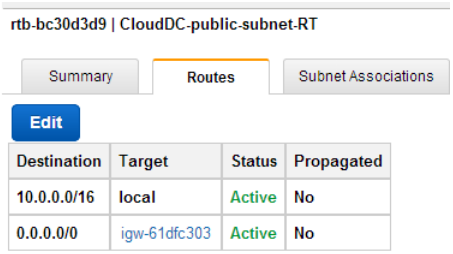
Address	Instance	Private IP Address	Scope	Public DNS
54.183.85.163	i-a7358ff9 (CloudDC-VM-Series)	10.0.0.126	vpc-0d4dac68	ec2-54-183-85-163.us-west-...
54.215.166.69	i-a7358ff9 (CloudDC-VM-Series)	10.0.0.10	vpc-0d4dac68	ec2-54-215-166-69.us-west-...

STEP 8 | Disable Source/Destination check on each network interface attached to the VM-Series firewall. Disabling this attribute allows the interface to handle network traffic that is not destined to its IP address.

1. Select the network interface in the **Network Interfaces** tab.
2. In the **Action** drop-down, select **Change Source/Dest. Check**.
3. Click **Disabled** and **Save** your changes.
4. Repeat steps 1-3 for additional network interfaces, firewall-1/2 in this example.

STEP 9 | In the route table associated with the public subnet (from step 3), add a default route to the internet gateway for the VPC.

1. From the VPC Dashboard, select **Route Tables** and find the route table associated with the public subnet.
2. Select the route table, select **Routes** and click **Edit**.
3. Add a route to forward packets from this subnet to the internet gateway. In this example, 0.0.0.0 indicates that all traffic from/to this subnet will use the internet gateway attached to the VPC.

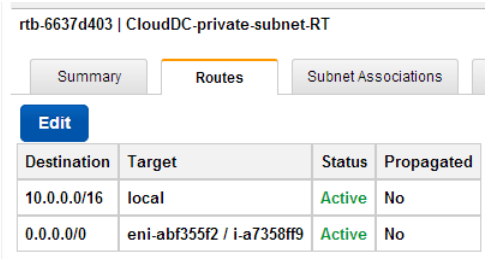


STEP 10 | In the route table associated with the private subnet, add a default route to send traffic to the VM-Series firewall.

Adding this route enables the forwarding of traffic from the EC2 instances in this private subnet to the VM-Series firewall.

1. From the VPC Dashboard, select **Route Tables** and find the route table associated with the private subnet.
2. Select the route table, select **Routes** and click **Edit**.

3. Add a route to forward packets from this subnet to the VM-Series firewall network interface that resides on the same subnet. In this example, 0.0.0.0/0 indicates that all traffic from/to this subnet will use eni-abf355f2 (ethernet 1/2, which is CloudDC-VM-Series-Trust) on the VM-Series firewall.



For each web or database server deployed on an EC2 instance in the private subnet, you must define a default route to the IP address of the VM-Series firewall so that the firewall is the default gateway for the server.

Perform steps 11 through 16 on the VM-Series firewall

STEP 11 | Configure a new administrative password for the firewall.

An SSH tool such as PuTTY is required to access the CLI on the firewall and change the default administrative password. You cannot access the web interface until you SSH and change the default password.

1. Use the public IP address you configured on the firewall, 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 Launch the VM-Series Firewall on AWS, steps 3-xi to access the CLI.
2. Enter the following command to log in to the firewall:

   ssh -i <*private_key_name*> admin@<*public-ip_address*>
3. Configure a new password, using the following command and follow the onscreen prompts:

   set password

   configure commit
4. Terminate the SSH session.

STEP 12 | Access the web interface of the VM-Series firewall.

Open a web browser and enter the EIP of the management interface. For example: https://54.183.85.163

STEP 13 | Activate the licenses on the VM-Series firewall. This step is only required for the BYOL license; the usage-based licenses are automatically activated.

See Activate the License.

STEP 14 | On the VM-Series firewall, configure the dataplane network interfaces on the firewall as Layer 3 interfaces.

1. Select **Network** > **Interfaces** > **Ethernet**.
2. Click the link for **ethernet 1/1** and configure as follows:
   - **Interface Type**: **Layer3**
   - Select 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, for example untrust, and then click OK.
- Select IPv4, select **DHCP Client**; the private IP address that you assigned to the network interface in the AWS management console will be acquired automatically.
- On the **Advanced** > **Other Info** tab, expand the Management Profile drop-down, and select **New Management Profile**.
- Enter a **Name** for the profile, such as allow_ping, and select **Ping** from the Permitted Services list, then click **OK**.
- To save the interface configuration, click **OK**.

3. Click the link for **ethernet 1/2** and configure as follows:
   - **Interface Type**: **Layer3**
   - Select 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, for example trust, and then click **OK**.
   - Select **IPv4**, select **DHCP Client**.
   - On the **IPv4** tab, clear the **Automatically create default route to default gateway provided by server** check box. For an interface that is attached to the private subnet in the VPC, disabling this option ensures that traffic handled by this interface does not flow directly to the IGW on the VPC.
   - On the **Advanced** > **Other Info**, expand the Management Profile drop-down, and select the allow_ping profile you created earlier.
   - Click **OK** to save the interface configuration.
4. Click **Commit** to save the changes. Verify that the Link state for the interface is up 

. If the link state is not up, reboot the firewall.

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Security Zone
ethernet1/1	Layer3	allow_ping		Dynamic-DHCP Client	default	untrust
ethernet1/2	Layer3	allow_ping		Dynamic-DHCP Client	default	trust

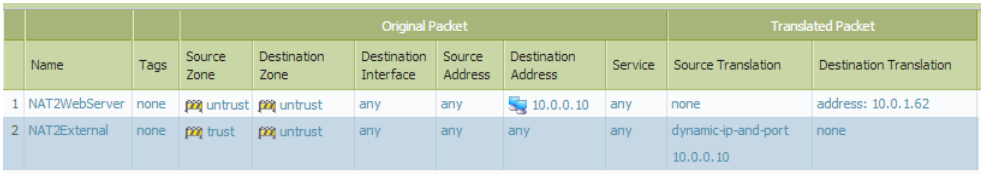
STEP 15 | On the VM-Series firewall, create Destination NAT and Source NAT rules to allow inbound/outbound traffic to/from the applications deployed within the VPC.

1. Select **Policies** > **NAT**.
2. Create a Destination NAT rule that steers traffic from the firewall to the web server.
   1. Click **Add**, and enter a name for the rule. For example, NAT2WebServer.
   2. In the **Original Packet** tab, make the following selections:
      - **Source Zone**: untrust (where the traffic originates)
      - **Destination Zone**: untrust (the zone for the firewall dataplane interface with which the EIP for the web server is associated.)
      - **Source Address**: Any
      - **Destination Address**: 10.0.0.10
      - In the **Translated Packet** tab, select the Destination Address Translation check box and set the **Translated Address**: to 10.0.1.62, which is the private IP address of the web server.
   3. Click **OK**.

			Original Packet						Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	NAT2WebServer	none	untrust	untrust	any	any	10.0.0.10	any	none	address: 10.0.1.62

3. Create a Source NAT rule to allow outbound traffic from the web server to the internet.
   1. Click **Add**, and enter a name for the rule. For example, NAT2External.

2. In the **Original Packet** tab, make the following selections:
   - **Source Zone**: trust (where the traffic originates)
   - **Destination Zone**: untrust (the zone for the firewall dataplane interface with which the EIP for the web server is associated.)
   - **Source Address**: Any
   - **Destination Address**: Any
3. In the **Translated Packet** tab, make the following selections in the Source Address Translation section:
   - **Translation Type**: Dynamic IP and Port
   - **Address Type**: Translated Address
   - **Translated Address**: 10.0.0.10 (the firewall dataplane interface in the untrust zone.)
4. Click **OK**.



			Original Packet						Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	NAT2WebServer	none	untrust	untrust	any	any	10.0.0.10	any	none	address: 10.0.1.62
2	NAT2External	none	trust	untrust	any	any	any	any	dynamic-ip-and-port 10.0.0.10	none

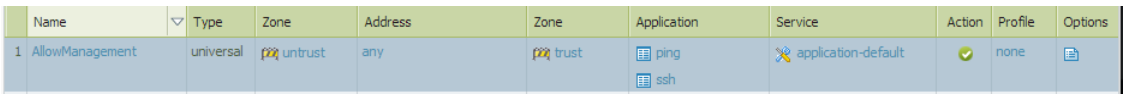
4. Click **Commit** to save the NAT policies.

STEP 16 | On the VM-Series firewall, create security policies to manage traffic.

Instead of entering a static IP address for the web server, use a dynamic address group. Dynamic address groups allow you to create policy that automatically adapts to changes so that you do not need to update the policy when you launch additional web servers in the subnet. For details, see Use Case: Use Dynamic Address Groups to Secure New EC2 Instances within the VPC.

1. Select **Policies** > **Security**.

   In this example, we have four rules. A rule that allows management access to the firewall traffic, a rule to allow inbound traffic to the web server, a third rule to allow internet access to the web server, and in the last rule we modify a predefined intrazone-default rule to log all traffic that is denied.
2. Create a rule to allow management access to the firewall.
   1. Click **Add** and enter a **Name** for the rule. Verify that the **Rule Type** is universal.
   2. In the **Source** tab, add untrust as the **Source Zone**.
   3. In the **Destination** tab, add trust as the **Destination Zone**.
   4. In the **Applications** tab, **Add** ping and ssh.
   5. In the **Actions** tab, set the **Action** to Allow.
   6. Click **OK**.

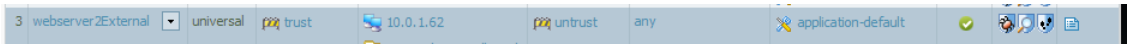


	Name	Type	Zone	Address	Zone	Application	Service	Action	Profile	Options
1	AllowManagement	universal	untrust	any	trust	ping ssh	application-default	✓	none	

3. Create a rule to allow inbound traffic to the web server.
   1. Click **Add** and enter a **Name** for the rule and verify that the **Rule Type** is universal.
   2. In the **Source** tab, add untrust as the **Source Zone**.
   3. In the **Destination** tab, add trust as the **Destination Zone**.
   4. In the **Applications** tab, **Add** web-browsing.
   5. In the **Service/URL Category** tab, verify that the service is set to application-default.
   6. In the **Actions** tab, set the **Action** to Allow.

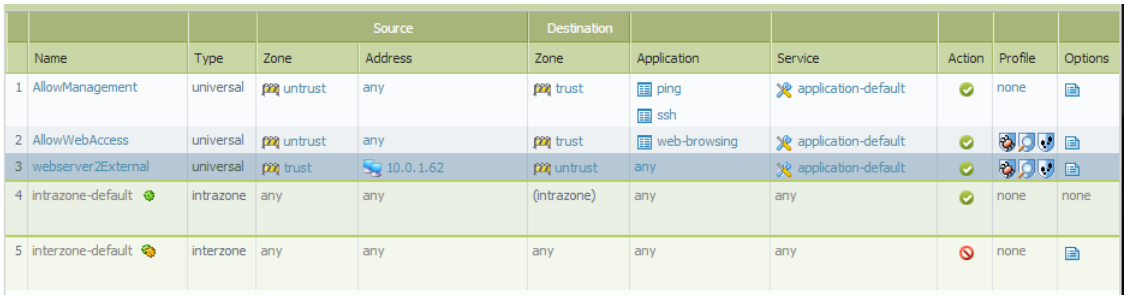
7. In the Profile Settings section of the **Actions** tab, select **Profiles** and then attach the default profiles for antivirus, anti-spyware, and vulnerability protection.
8. Click **OK**.

4. Create a rule to allow internet access to the web server.
    1. Click **Add** and enter a **Name** for the rule and verify that the Rule Type is universal.
    2. In the **Source** tab, add trust as the **Source Zone**.
    3. In the Source Address section of the **Source** tab, add 10.0.1.62, the IP address of the web server.
    4. In the **Destination** tab, add untrust as the **Destination Zone**.
    5. In the **Service/URL Category** tab, verify that the service is set to **application-default**.
    6. In the **Actions** tab, set the **Action** to Allow.
    7. In the Profile Settings section of the **Actions** tab, select **Profiles** and then attach the default profiles for antivirus, anti-spyware, and vulnerability protection.
    8. Click **OK**.



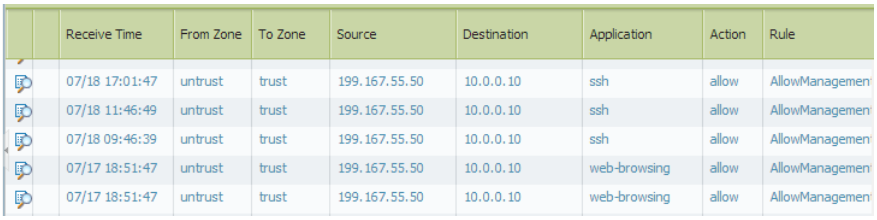
5. Edit the interzone-default rule to log all traffic that is denied. This predefined interzone rule is evaluated when no other rule is explicitly defined to match traffic across different zones.
    1. Select the **interzone-default** rule and click **Override**.
    2. In the **Actions** tab, select **Log at session end**.
    3. Click **OK**.

6. Review the complete set of security rules defined on the firewall.
7. Click **Commit** to save the policies.



STEP 17 | Verify that the VM-Series firewall is securing traffic.

1. Launch a web browser and enter the IP address for the web server.
2. Log in to the web interface of the VM-Series firewall and verify that you can see the traffic logs for the sessions at **Monitor** > **Logs** > **Traffic**.
    - Traffic inbound to the web server (arrives at EC2 instance in the AWS VPC):



    - Traffic outbound from the web server (EC2 instance in the AWS VPC):

		Receive Time	From Zone	To Zone	Source	Destination	Application	Action	Rule
		07/21 12:32:42	trust	untrust	10.0.1.62	204.2.134.164	ntp	allow	webserver2External
		07/21 12:32:12	trust	untrust	10.0.1.62	204.2.134.164	ntp	allow	webserver2External
		07/21 12:31:42	trust	untrust	10.0.1.62	50.7.96.4	ntp	allow	webserver2External
		07/21 12:31:12	trust	untrust	10.0.1.62	50.7.96.4	ntp	allow	webserver2External

You have successfully deployed the VM-Series firewall as a cloud gateway!

Use Case: Use Dynamic Address Groups to Secure New EC2 Instances within the VPC

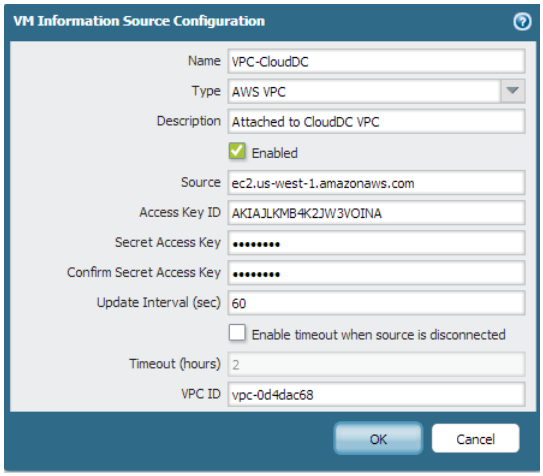
In a dynamic environment such as the AWS-VPC where you launch new EC2 instances on demand, the administrative overhead in managing security policy can be cumbersome. Using Dynamic Address Groups in security policy allows for agility and prevents disruption in services or gaps in protection.

In this example, we illustrate how you can monitor the VPC and use Dynamic Address Groups in security policy to discover and secure EC2 instances. As you spin up EC2 instances, the Dynamic Address Group collates the IP addresses of all instances that match the criteria defined for group membership, and then security policy is applied for the group. The security policy in this example allows internet access to all members of the group.

This workflow in the following section assumes that you have created the AWS VPC and deployed the VM-Series firewall and some applications on EC2 instances. For instructions on setting up the VPC for the VM-Series, see Use Case: Secure the EC2 Instances in the AWS Cloud.

STEP 1 | Configure the firewall to monitor the VPC.

1. Select **Device** > **VM Information Sources**.
2. Click **Add** and enter the following information:
    1. A **Name** to identify the VPC that you want to monitor. For example, VPC-CloudDC.
    2. Set the **Type** to AWS VPC.
    3. In **Source**, enter the URI for the VPC. The syntax is **ec2.<*your_region*>.amazonaws.com**
    4. Add the credentials required for the firewall to digitally sign API calls made to the AWS services. You need the following:
        - **Access Key ID**: Enter the alphanumeric text string that uniquely identifies the user who owns or is authorized to access the AWS account.
        - **Secret Access Key**: Enter the password and confirm your entry.
    5. (**Optional**) Modify the **Update interval** to a value between 5-600 seconds. By default, the firewall polls every 5 seconds. The API calls are queued and retrieved within every 60 seconds, so updates may take up to 60 seconds plus the configured polling interval.



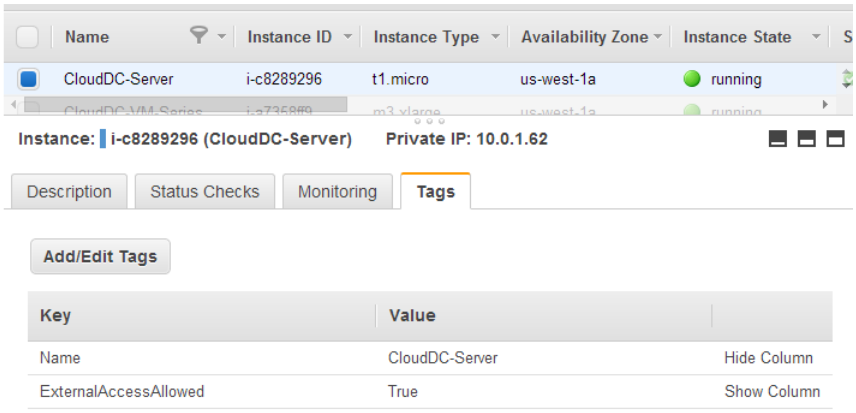
6. Enter the **VPC ID** that is displayed on the VPC Dashboard in the AWS management console.
7. Click **OK**, and **Commit** the changes.
8. Verify that the connection **Status** displays as connected

STEP 2 | Tag the EC2 instances in the VPC.

For a list of tags that the VM-Series firewall can monitor, see List of Attributes Monitored on the AWS VPC.

A tag is a name-value pair. You can tag the EC2 instances either on the EC2 Dashboard on the AWS management console or using the AWS API or AWS CLI.

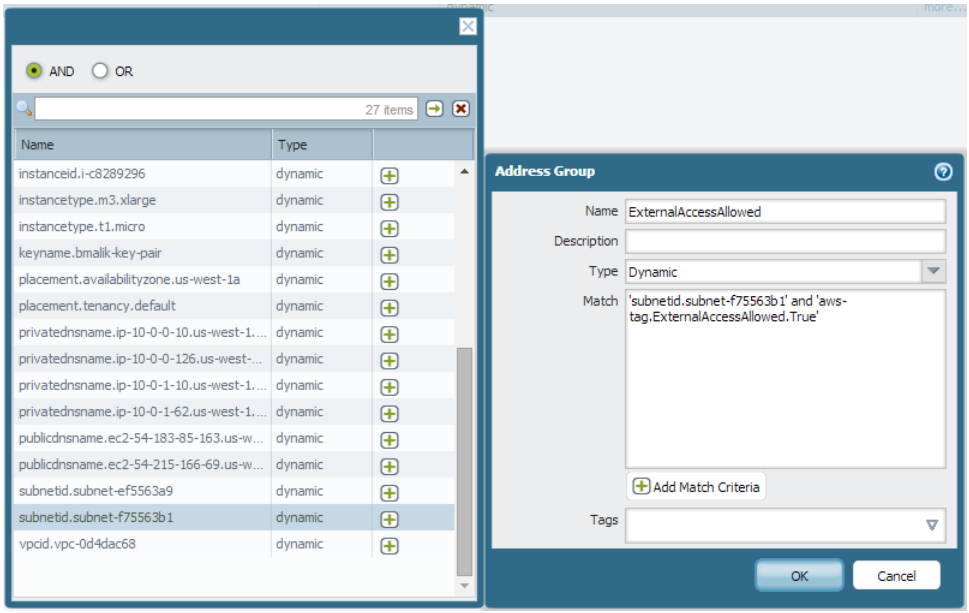
In this example, we use the EC2 Dashboard to add the tag:



STEP 3 | Create a dynamic address group on the firewall.

View the tutorial to see a big picture view of the feature.

1. Select **Object** > **Address Groups**.
2. Click **Add** and enter a **Name** and a **Description** for the address group.
3. Select **Type** as **Dynamic**.
4. Define the match criteria.
   1. Click **Add Match Criteria**, and select the **And** operator.
   2. Select the attributes to filter for or match against. In this example, we select the ExternalAccessAllowed tag that you just created and the subnet ID for the private subnet of the VPC.



5. Click **OK**.
6. Click **Commit**.

STEP 4 | Use the dynamic address group in a security policy.

To create a rule to allow internet access to any web server that belongs to the dynamic address group called ExternalServerAccess.

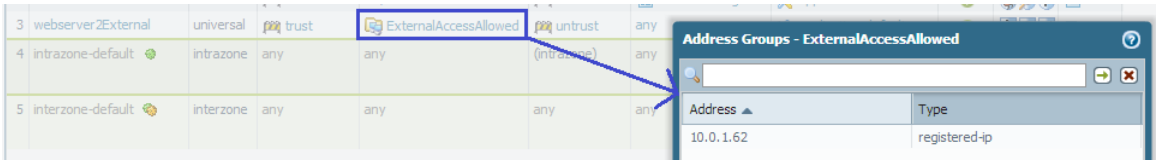
1. Select **Policies** > **Security**.
2. Click **Add** and enter a **Name** for the rule and verify that the **Rule Type** is universal.
3. In the **Source** tab, add trust as the **Source Zone**.
4. In the Source Address section of the **Source** tab, **Add** the ExternalServerAccess group you just created.
5. In the **Destination** tab, add untrust as the **Destination Zone**.
6. In the **Service/URL Category** tab, verify that the service is set to **application-default**.
7. In the **Actions** tab, set the **Action** to Allow.
8. In the Profile Settings section of the **Actions** tab, select **Profiles** and then attach the default profiles for antivirus, anti-spyware, and vulnerability protection.
9. Click **OK**.

10. Click **Commit**.

STEP 5 | Verify that members of the dynamic address group are populated on the firewall.

Policy will be enforced for all IP addresses that belong to this address group, and are displayed here.

1. Select **Policies** > **Security**, and select the rule.
2. Select the drop-down arrow next to the address group link, and select **Inspect**. You can also verify that the match criteria is accurate.
3. Click the **more** link and verify that the list of registered IP addresses is displayed.

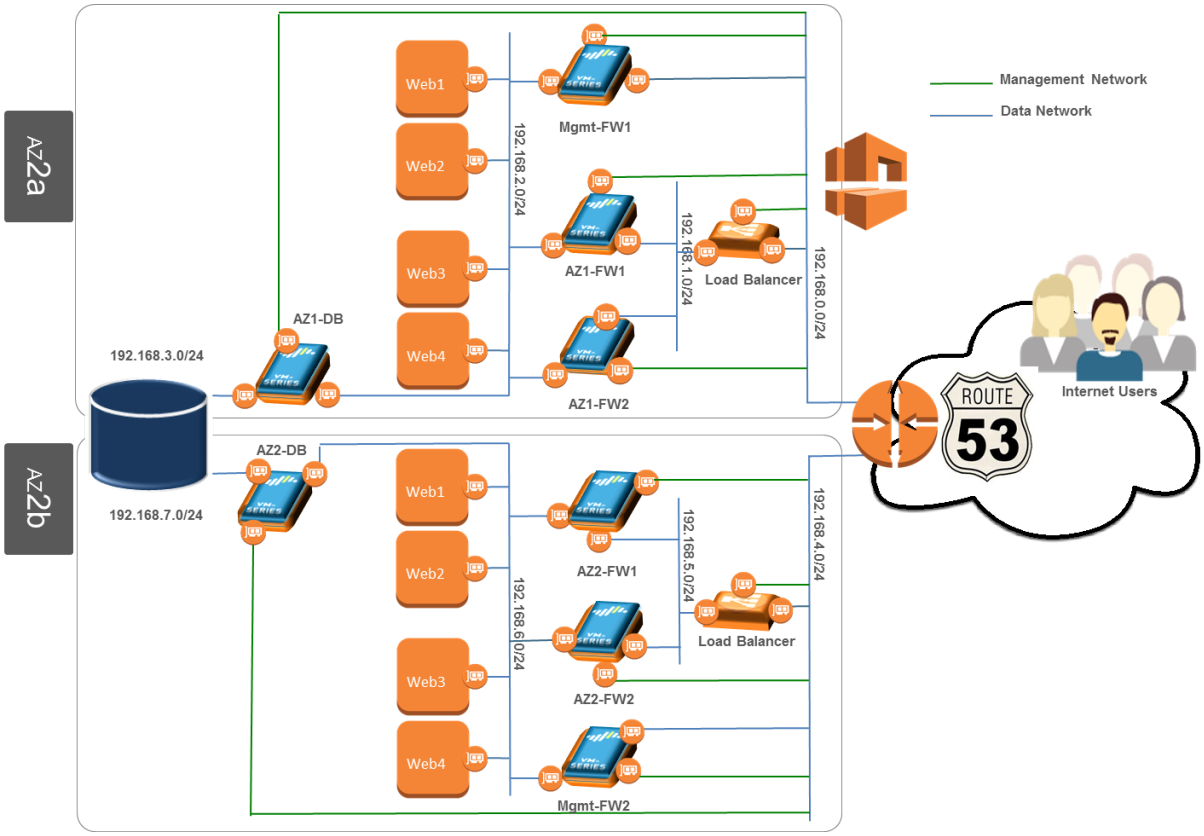


Use Case: Deploy the VM-Series Firewalls to Secure Highly Available Internet-Facing Applications on AWS

The AWS infrastructure and services provide an architecture that can scale and grow with your business. In addition to performance and application availability demands, your business requires assured security and application enablement. In order to reduce the attack surface for threats and to ensure that your business-critical servers, applications, and data are secure, you require the Palo Alto Networks VM-Series firewall. Together, AWS and the VM-Series firewall deliver operational efficiency with increased agility and optimal security.

Solution Overview—Secure Highly Available Internet-Facing Applications

In this use case, we show you how to secure highly available two-tier applications in Amazon Web Services (AWS) that are accessed by users over the internet. This setup is one specific example that uses WordPress and MySQL as the 2-tier applications. It includes a relational database service, a DNS-based global load balancing web service, Citrix NetScaler load balancers, and several VM-Series firewalls to secure north-south and east-west traffic flows to the applications in the Amazon Virtual Private Cloud (VPC). For high availability, the VPC spans two Availability Zones (AZs) on AWS. There are many other applications and architectures that Palo Alto Networks firewalls can secure; this use case is just one option.



The following table lists the elements required to deploy the solution for highly available internet-facing applications on AWS.

Solution Elements	Solutions Components	Description
Internet-Facing Applications	Amazon Elastic Compute Cloud (EC2) Instances	Web applications that are accessed by users over the internet. These applications are typically deployed in a multi-tier architecture on EC2 instances in an AWS VPC. AWS provides the infrastructure for ensuring uptime, scalability, and performance to meet your business needs.
Load Balancers	Examples include: Citrix NetScaler VPX, F5 Networks BIG-IP Local Traffic Manager (LTM), and NGINX Plus	The load balancer monitors the availability of servers, the database service, and the firewalls to ensure a seamless failover when an instance fails. This use case shows how to use the Citrix NetScaler VPX for deploying a highly available web application, but you can use a different load balancer.
Firewalls	VM-Series	Multiple instances of the VM-Series firewall are deployed to secure all your applications and database servers. The firewalls secure each subnet and restrict

Solution Elements	Solutions Components	Description
		access in a way that matches the business and technical requirements of your multi-tier architecture. This segmentation provides multiple layers of defense to ensure that business-critical services and data are always safe.
Global Server Load Balancing (GSLB) Service	Amazon Route 53	Amazon Route 53 is a DNS-based GSLB web service that provides DNS and multi-Availability Zone (AZ)/VPC redundancy. Route53 allows you to create and manage DNS records, connect user requests to an infrastructure, such as your web servers and load balancers running on AWS, and perform health checks to monitor the health of your servers and route traffic appropriately.
Database Service	Amazon Relational Database Service (RDS)	The Amazon RDS is tightly integrated with other Amazon Web Services. Amazon RDS offers a selection of engines for your database instances.

See Deploy the Solution Components for Highly Available Internet-Facing Applications on AWS for the configuration details.

Deploy the Solution Components for Highly Available Internet-Facing Applications on AWS

Use these high-level tasks to deploy the components listed in the Solution Overview—Secure Highly Available Internet-Facing Applications.

- Set Up the VPC

  Create the VPC and add the subnets, security groups, internet gateway, and a route table. You will also create Elastic Network Interfaces (ENIs) and allocate Elastic IP Addresses for some instances in the VPC. Duplicate this set up in another Availability Zone for redundancy.
- Deploy the VM-Series Firewalls in the VPC

  Deploy and configure four VM-Series firewalls in each Availability Zone—a pair of firewalls to secure the web farm, one to secure the RDS, and one firewall for outbound access from the VPC. The firewall that regulates outbound access to the internet also secures all the management traffic to and from the firewalls, servers, and services in the VPC. This use case focuses primarily on how to set up the firewalls for securing your internet-facing multi-tiered application(s). It also briefly covers the process of deploying and configuring the NetScaler VPX to load balance traffic across the VM-Series firewalls.
- Deploy the Web Farm in the VPC
- Set Up the Amazon Relational Database Service (RDS)
- Configure the Citrix NetScaler VPX
- Verify Traffic Enforcement
- Set up Amazon Route 53

Set Up the VPC

Setting up the VPC requires you to—at a minimum—create the VPC, add the subnets, create the security groups, deploy EC2 instances, and attach ENIs with private IP addresses. To allow external access to the servers in the VPC, you also require an internet gateway and an Elastic IP Address for each EC2 instance that needs access to the internet. For this use case, the VPC setup is as follows:

STEP 1 | Create the VPC and add the subnets.

In this example, we create four subnets within the 192.168.0.0/16 VPC as follows:

- 192.168.0.0/24 (Public: for external access and management)
- 192.168.1.0/24 (Firewall: for connecting the firewalls)
- 192.168.2.0/24 (Web: for connecting to the web farm)
- 192.168.3.0/24 (DB: for connecting to the database server)

Name	Subnet ID	State	VPC	CIDR	Available IPs	Availability Zone	Route Table
Firewall	subnet-35c4016c	available	vpc-f85d869d (192.168.0.0/16) |...	192.168.1.0/24	251	us-west-1b	rtb-4e79d52b | ...
Public	subnet-3cc40165	available	vpc-f85d869d (192.168.0.0/16) |...	192.168.0.0/24	251	us-west-1b	rtb-4e79d52b | ...
Web	subnet-29c40170	available	vpc-f85d869d (192.168.0.0/16) |...	192.168.2.0/24	251	us-west-1b	rtb-4e79d52b | ...
DB	subnet-2bc40172	available	vpc-f85d869d (192.168.0.0/16) |...	192.168.3.0/24	251	us-west-1b	rtb-4e79d52b | ...

STEP 2 | Set up the other basic components in the VPC.

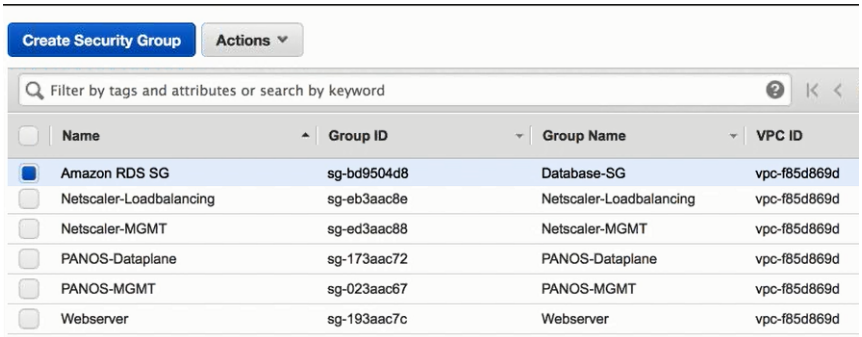
Ensure that the web server security group allows access only to destinations that are in the same subnet.

- Set up the internet gateway for incoming and outgoing traffic to/from the VPC and attach the internet gateway to the VPC.
- Set up the security groups. These groups are a basic form of security based on IP addresses, ports, and protocols. Security groups do not provide next-generation features like App-ID or threat protection but these groups are part of a complimentary solution that helps secure the VPC.

This example has six security groups that control access to the subnets within the VPC:

- **PANOS-MGMT**—Attach to the management interface of each VM-Series firewall. The inbound access rules for this security group allow SSH and HTTPS traffic.
- **PANOS-Dataplane**—Attach to the dataplane interfaces of each VM-Series firewall. The inbound access rules for this security group allow all traffic.
- **Webserver**—Attach to the interfaces of each web server. The inbound access rules for this security group allow all traffic that is sourced from the PAN-OS Dataplane security group.
- **NetScaler-MGMT**—Attach to the management interface of the Citrix NetScaler load balancer. The inbound access rules for this security group allow SSH and HTTPS traffic.
- **NetScaler-Loadbalancing**—Attach to the other interfaces on the Citrix NetScaler load balancer that are used to load balance traffic to the web farm. The inbound access rules for this security group allow all traffic.
- **Amazon RDS SG**—Attach to the interfaces on the Relational Database Service. The inbound access rules for this security group allow traffic on port 3306.

For instructions, refer to the AWS documentation.



- Allocate Elastic IP Addresses. For details on assigning Elastic IP Addresses, refer to the AWS documentation.

AWS has a default maximum number of Elastic IP Addresses; if your specific architecture requires more than the default, you can request more Elastic IP Addresses through AWS.

This example uses seven Elastic IP Addresses. See Allocate and associate Elastic IP Addresses for the firewall and the NetScaler VPX.

- Set up the route tables:
- Rename the main router with a descriptive name (this route table is automatically created when you create the VPC) and attach the internet gateway to this route table.
- Add a new route table. This route table is required for routing traffic from the web servers to the VM-Series firewall; this route table alleviates the need to create a default route on each web server as you horizontally scale out your web farm.

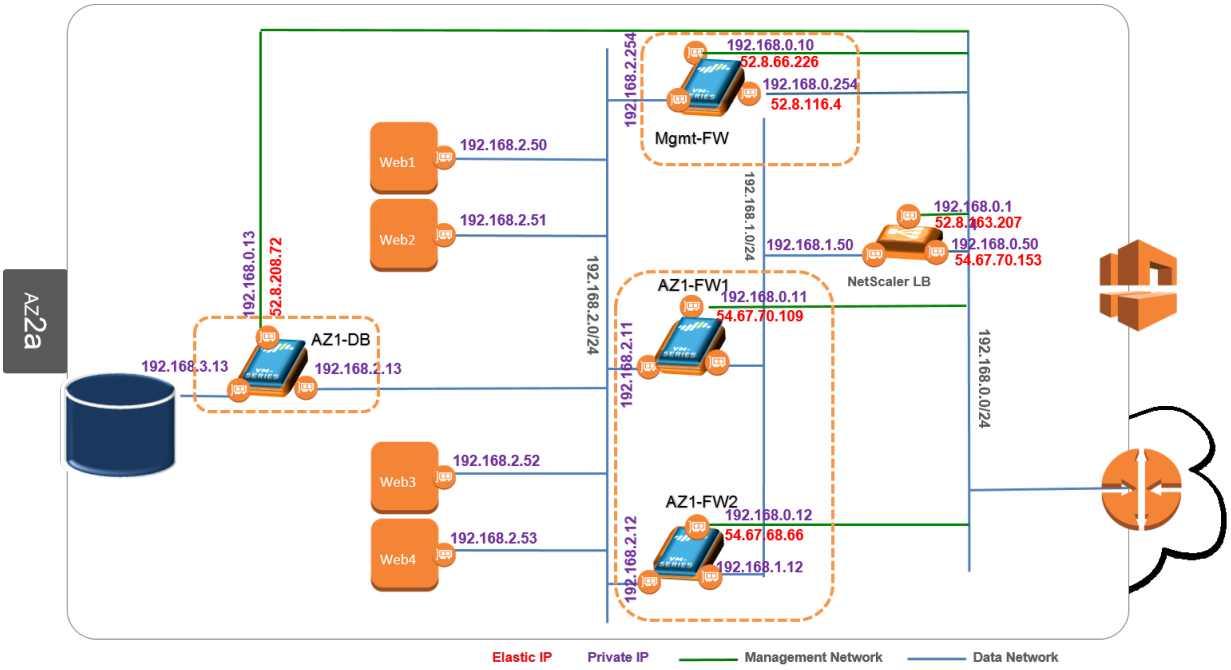
STEP 3 | Create the subnets, security groups, and routes in the other Availability Zone.

Repeat steps 1 to 2.

For the complete workflow, see Deploy the Solution Components for Highly Available Internet-Facing Applications on AWS

Deploy the VM-Series Firewalls in the VPC

You must deploy the firewalls, license the firewalls as appropriate, configure the network interfaces, and create policies that limit application and data traffic flows as appropriate for each server and application.



In this use case, each Availability Zone has four VM-Series firewalls:

- **Mgmt-FW**—A firewall that secures inbound and outbound traffic necessary for managing and updating the infrastructure. It secures all inbound and outbound management traffic to and from the EC2 instances and services in the VPC, including database engine updates, SSH and HTTPS access to the EC2 instances and services, and SNMP. See Launch the VM-Series Firewalls and the NetScaler VPX and Configure the VM-Series Firewall for Securing Outbound Access from the VPC.
- **AZ1-FW1 and AZ1-FW2**—A pair of firewalls that manage traffic from the NetScaler VPX to the web farm. In the event that a firewall fails, the load balancer uses service monitors to detect the failure and redirect traffic through the other firewall. See Launch the VM-Series Firewalls and the NetScaler VPX and Configure the Firewalls that Secure the Web Farm.
- **AZ1-DB**—A firewall to segment the web farm from the Relational Database Service (RDS). This architecture allows you to add a layer of security and isolate the database service and limit the exposure of front-end servers to risks and threats. See Launch the VM-Series Firewalls and the NetScaler VPX and Configure the Firewall that Secures the RDS.

Launch the VM-Series Firewalls and the NetScaler VPX

On the AWS management console, launch the firewalls, launch the load balancer, and edit the route tables you added when you created the VPC.

STEP 1 | Launch the firewalls and perform initial configuration.

1. Launch the firewalls. See Deploy the VM-Series Firewall on AWS for system requirements and step-by-step instructions for launching the firewall and performing initial configuration. For this use case, you deploy four VM-Series firewalls on each AZ.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public
AZ1-FW1	i-33a383f1	c3.xlarge	us-west-1b	running	Initializing	None	
AZ1-FW2	i-d0a48412	c3.xlarge	us-west-1b	running	Initializing	None	
Mgmt-FW	i-4da2828f	c3.xlarge	us-west-1b	running	2/2 checks ...	None	
AZ1-DB	i-2ba484e9	c3.xlarge	us-west-1b	running	Initializing	None	

The IP address assigned to the management interfaces (eth0) of each firewall is as follows:

- **Mgmt-FW**—192.168.0.10
- **AZ1-FW1**—192.168.0.11
- **AZ1-FW2**—192.168.0.12
- **AZ1-DB**—192.168.0.13

2. Establish an SSH connection to the IP address assigned to the management interface and perform initial configuration on the command line interface (CLI) of the VM-Series firewall.
3. Create and attach two ENIs to each firewall; these interfaces will serve as the dataplane interfaces on each firewall. Connect each ENI to the appropriate subnet and security group.

   - **Mgmt-FW**—The dataplane interface IP addresses are:
     - 192.168.2.254 (to web farm)
     - 192.168.0.254 (external connectivity for internet access)
   - **AZ1-FW1**—The dataplane interface IP addresses are:
     - 192.168.1.11 (to NetScaler)
     - 192.168.2.11 (to web farm)
   - **AZ1-FW2**—The dataplane interface IP addresses are:
     - 192.168.1.12 (to NetScaler)
     - 192.168.2.12 (to web farm)
   - **AZ1-DB**—The dataplane interface IP addresses are:
   - 192.168.2.13 (to web farm)
   - 192.168.3.13 (to RDS)

STEP 2 | Launch the NetScaler VPX.

Refer to the Citrix NetScaler documentation for instructions.

1. Choose the Amazon Machine Image (AMI) from the AWS Marketplace and launch the NetScaler VPX. In this example, the NetScaler IP address used for management access is 192.168.0.14.

   To log in to the NetScaler management console, you must assign an Elastic IP Address on the management interface.
2. Attach two ENIs to the NetScaler VPX. Later in this example, Configure the Citrix NetScaler VPX interface IP addresses as:

   - 192.168.0.50—Virtual IP address that will be used for external access.
   - 192.168.1.50—Subnet IP address that will be used for connecting to the web farm within the VPC.

STEP 3 | Allocate and associate Elastic IP Addresses for the firewall and the NetScaler VPX.

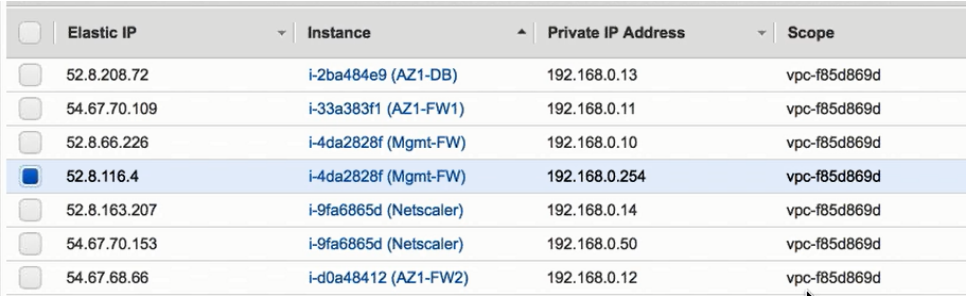
Assign Elastic IP Addresses to the interfaces that provide access from the internet. In this example, the Elastic IP Addresses are as follows:

- One EIP address maps to the management interface of each of the four VM-Series firewalls.

  With the exception of the VM-Series firewall that secures management access, the Elastic IP address that maps to the management interface of each VM-Series firewall will be used for out-of-band management.

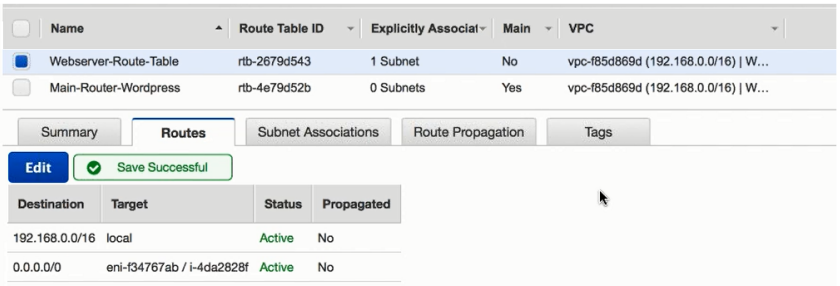
- One EIP address maps to the public-facing interface on the VM-Series firewall that manages outbound access from the VPC.

- Two EIP addresses map to the NetScaler VPX: one is associated with the NetScaler IP address and the other is bound to the Virtual IP address.

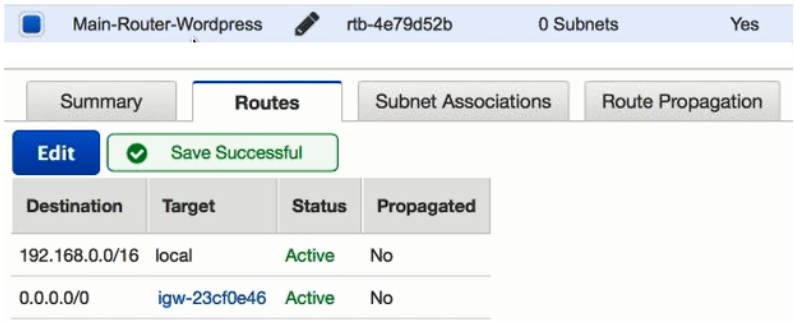


STEP 4 | Edit the route tables.

1. Add a new route table, if you did not add one when setting up the VPC.
2. Add a new route that directs all traffic from the web farm to the ENI that is attached to the web server subnet on the VM-Series firewall (Mgmt-FW).



3. Create and attach the internet gateway to the main router on the VPC to allow outbound internet access from the VPC.



Configure the VM-Series Firewall for Securing Outbound Access from the VPC

The Mgmt-FW in this use case is the VM-Series firewall that secures inbound management traffic, such as infrastructure updates that include DNS and apt-get updates for all web servers. This firewall is also the default gateway for all outbound traffic from the web farm to the internet.

STEP 1 | Launch the firewalls and perform initial configuration.

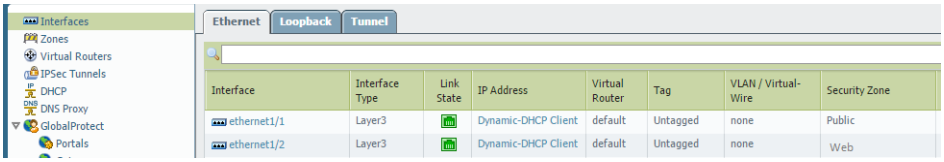
STEP 2 | Allocate and assign Elastic IP Addresses.

This use case requires one Elastic IP Address for the management interface of the VM-Series firewall and one for the dataplane interface that allows internet access from the VPC. See step 3.

STEP 3 | Log in to the web interface of the VM-Series firewall using the Elastic IP Address assigned to the management interface.

STEP 4 | Configure the network interfaces. Select **Network** > **Interfaces** > **Ethernet** and click the links to configure ethernet1/1 and ethernet1/2.

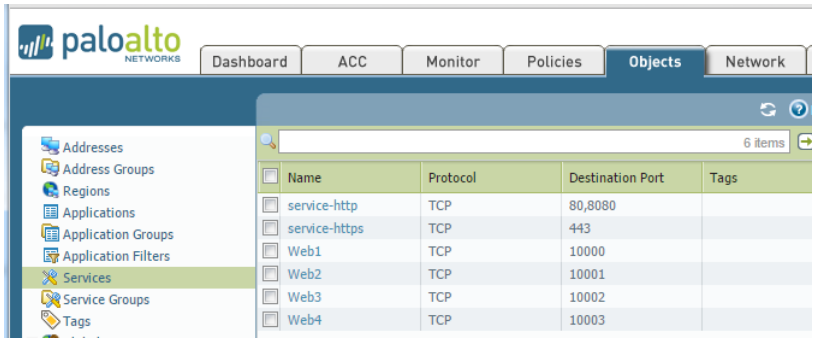
1. Configure a DHCP client on each interface and create and attach security zones to each interface.
2. When configuring the interface that is connected to the web farm (ethernet1/2 in this use case), clear the check box to **Automatically create default route to default gateway provided by server**. For an interface that is attached to the private subnet in the VPC, disabling this option ensures that traffic handled by this interface does not flow directly to the internet gateway on the VPC.



STEP 5 | Create service objects and a service group.

A service object allows you to specify the port number that an applications can use if you plan to use a non-default port for an application. You use these objects in NAT policy (step 7) so that the firewall can perform port translation to route traffic properly.

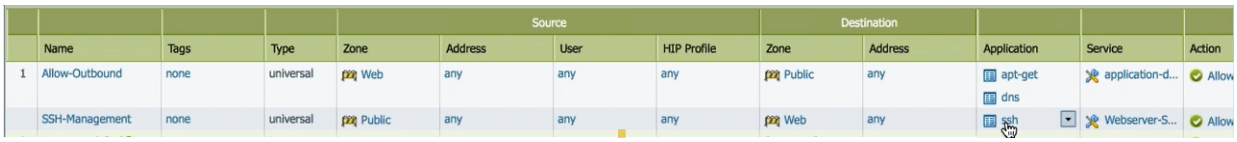
1. Select **Objects** > **Services** and **Add** the service objects to enable TCP access to the web servers on ports 10000, 10001, 10002, and 10003.



2. Combine these service objects into a service group. Select **Objects** > **Service Groups** and **Add** a service group named Webserver_Services and **Add** Web1, Web 2, Web3, and Web4 to the group.

STEP 6 | Define security policy for sanctioned applications.

For example, allow SSH for inbound management and allow application and DNS updates to the web servers in the VPC. Because this use case employs non-default ports for SSH access, change the Service for SSH Management from 'application-default' to 'Webserver_Services' (the service group created in the last step) to define the ports that provide access to the web servers.



STEP 7 | Define NAT policy rules.

These rules ensure that the firewall performs IP address and port translation and secures all inbound and outbound traffic on the web server farm.

1. Create NAT rules for permitting inbound access to each web server. You need to enable destination translation to the service objects you defined earlier for each web server.
2. Create an outbound NAT rule that allows internet access for the web servers in the VPC. This rule allows the firewall to translate the source IP address as the public-facing interface on the management firewall. The AWS internet gateway then translates the private IP address to the Elastic IP Address associated with the interface for routing the traffic to the internet.

See Port Translation for Service Objects for details on how the firewall performs IP address and port translation to properly route traffic.

			Original Packet						Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	Web1	none	Public	Public	any	any	192.168.0.254	Web1	none	address: 192.168.2.50 port: 22
2	Web2	none	Public	Public	any	any	192.168.0.254	Web2	none	address: 192.168.2.51 port: 22
3	Web3	none	Public	Public	any	any	192.168.0.254	Web3	none	address: 192.168.2.52 port: 22
4	Web4	none	Public	Public	any	any	192.168.0.254	Web4	none	address: 192.168.2.53 port: 22
5	Outbound-NAT	none	Web	Public	any	any	any	any	dynamic-ip-and-port ethernet1/1	none

STEP 8 | To ensure that traffic is routed properly to the firewall, perform the following tasks on the AWS management console:

1. Create a route table for the web farm subnet and add a new route that directs all traffic from the web farm to the ENI that is attached to the web server subnet on the VM-Series firewall (Mgmt-FW). See steps 4-b.
2. Disable source and destination checks on the dataplane network interface(s) assigned to the firewall. Disabling this option allows the interface to handle network traffic that is not destined to the IP address assigned to the interface. Select the network interface in the **Network Interfaces** tab on the EC2 Dashboard, for example eth1/1, and in the **Action** drop-down, select **Change Source/Dest. Check**. Click **Disabled** and **Save** your changes.

Configure the Firewalls that Secure the Web Farm

Use these instructions to configure the redundant pair of VM-Series firewalls that secure the web servers within an Availability Zone.

For a topology and solution details see, Use Case: Deploy the VM-Series Firewalls to Secure Highly Available Internet-Facing Applications on AWS and Solution Overview—Secure Highly Available Internet-Facing Applications.

STEP 1 | Launch the firewalls and perform initial configuration.

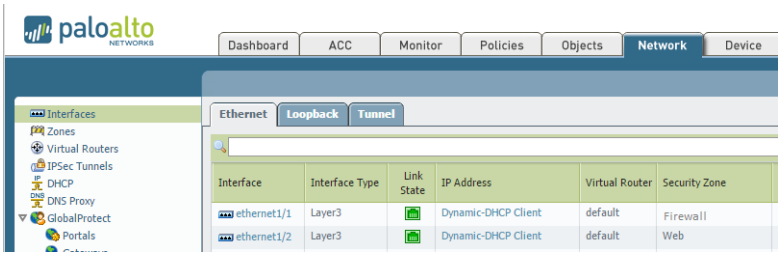
STEP 2 | Allocate and assign Elastic IP Addresses.

This use case requires one Elastic IP Address for the management interface of each VM-Series firewall. See step 3.

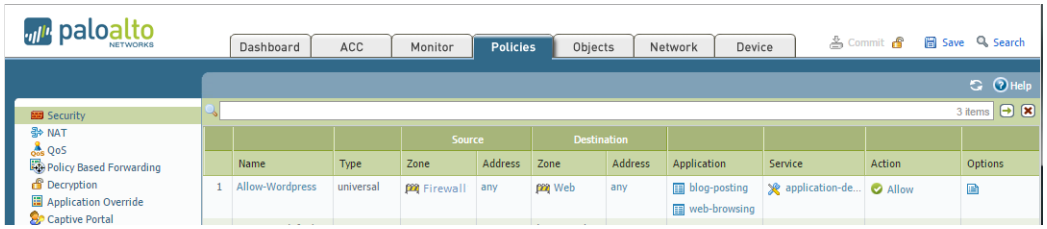
STEP 3 | Log in to the web interface of the VM-Series firewall using the EIP address assigned to the management interface.

STEP 4 | Configure the network interfaces. Select **Network** > **Interfaces** > **Ethernet** and click the links to configure ethernet1/1 and ethernet1/2.

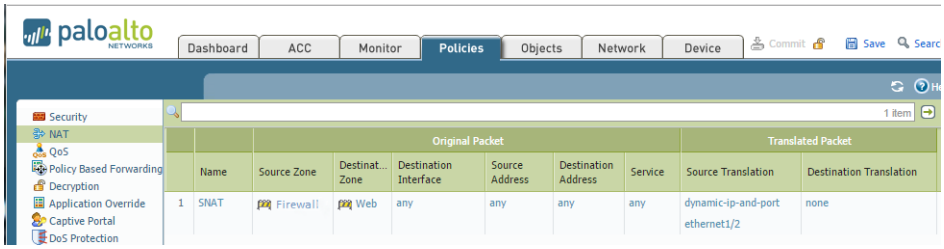
1. Configure a DHCP client on each interface and create and attach security zones to each interface.
2. Clear the check box to **Automatically create default route to default gateway provided by server** to ensure that the web servers do not use the default route provided by the firewall.



STEP 5 | Create a security policy rule to allow the sanctioned applications. Because we use the WordPress application in this example, the policy rule allows the web-browsing and blog-posting applications for WordPress.



STEP 6 | Create a NAT policy rule to ensure symmetric routing of traffic when the NetScaler VPX load balances traffic across the two (or more) firewalls that are protecting the web servers. This NAT policy rule is required to translate the private IP addresses to public IP addresses that can be routed to external networks. It also ensures that the same firewall manages the request and response traffic for a web server in the web farm.



Configure the Firewall that Secures the RDS

This task helps you set up the VM-Series firewall that secures the database service on AWS. For the topology and solution details, see Use Case: Deploy the VM-Series Firewalls to Secure Highly Available Internet-Facing Applications on AWS and Solution Overview—Secure Highly Available Internet-Facing Applications.

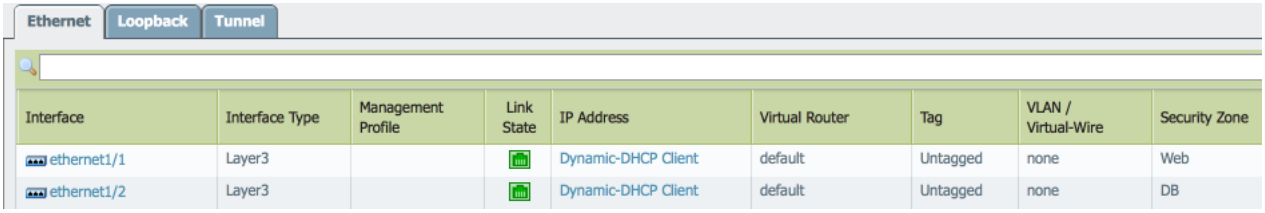
STEP 1 | Launch the firewalls and perform initial configuration.

STEP 2 | Allocate and assign Elastic IP Addresses for the management interface of the VM-Series firewall. See step 3.

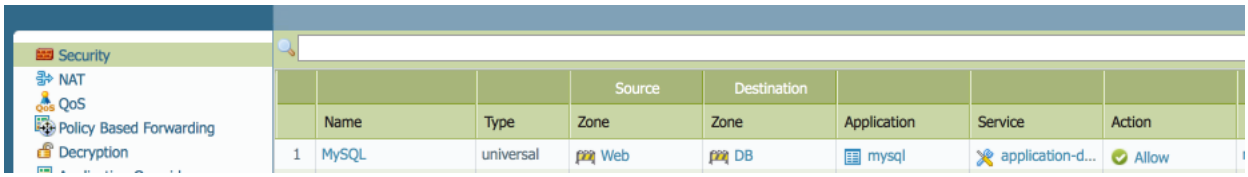
STEP 3 | Log in to the web interface of the VM-Series firewall using the Elastic IP Address assigned to the management interface.

STEP 4 | Configure the network interfaces. Select **Network** > **Interfaces** > **Ethernet** and click the links to configure ethernet1/1 and ethernet1/2.

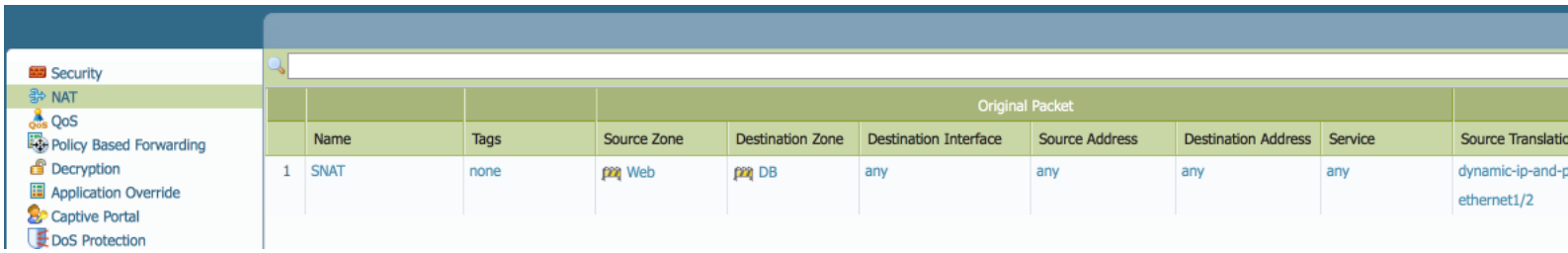
1. Configure a DHCP client on each interface and create and attach security zones to each interface.
2. Clear the check box to **Automatically create default route to default gateway provided by server** to ensure that the RDS does not use the default route provided by the firewall to directly access the internet.



STEP 5 | Create the security policy rule that allows traffic to pass from the web servers to the database server.



STEP 6 | Create a Source NAT policy that allows outbound traffic initiated by the database server to be routed through ethernet1/2 interface (192.168.3.13) on the firewall to the web servers.



You cannot configure routing on the Amazon RDS. Source NAT policy on the firewall is required to ensure that the traffic is routed properly.

Deploy the Web Farm in the VPC

This workflow shows you how to deploy the web server and configure the WordPress application. These instructions are included solely for the purpose of taking you through the implementation in this use case. For concepts and details on deploying WordPress, refer to the WordPress documentation.

For the topology and solution details, see Use Case: Deploy the VM-Series Firewalls to Secure Highly Available Internet-Facing Applications on AWS and Solution Overview—Secure Highly Available Internet-Facing Applications.

STEP 1 | Launch the web server in the VPC.

1. Launch an Ubuntu instance (version 14.04) in the Web server subnet.
2. Add an ENI and assign an IP address (for example, 192.168.2.50).
3. Log in to the web server using the VM-Series firewall configured for management access.

```
ssh –i ‘keypair.pem’ –p 10000 ubuntu@52.8.208.92
```

STEP 2 | Configure the web server for access.

1. Create and edit eth0.cfg file.

   sudo vi /etc/network/interfaces.d/eth0.cfg
2. Configure the file with a static network setting to direct database traffic to the VM-Series firewall that secures the database service. The following settings are the same for each web server:

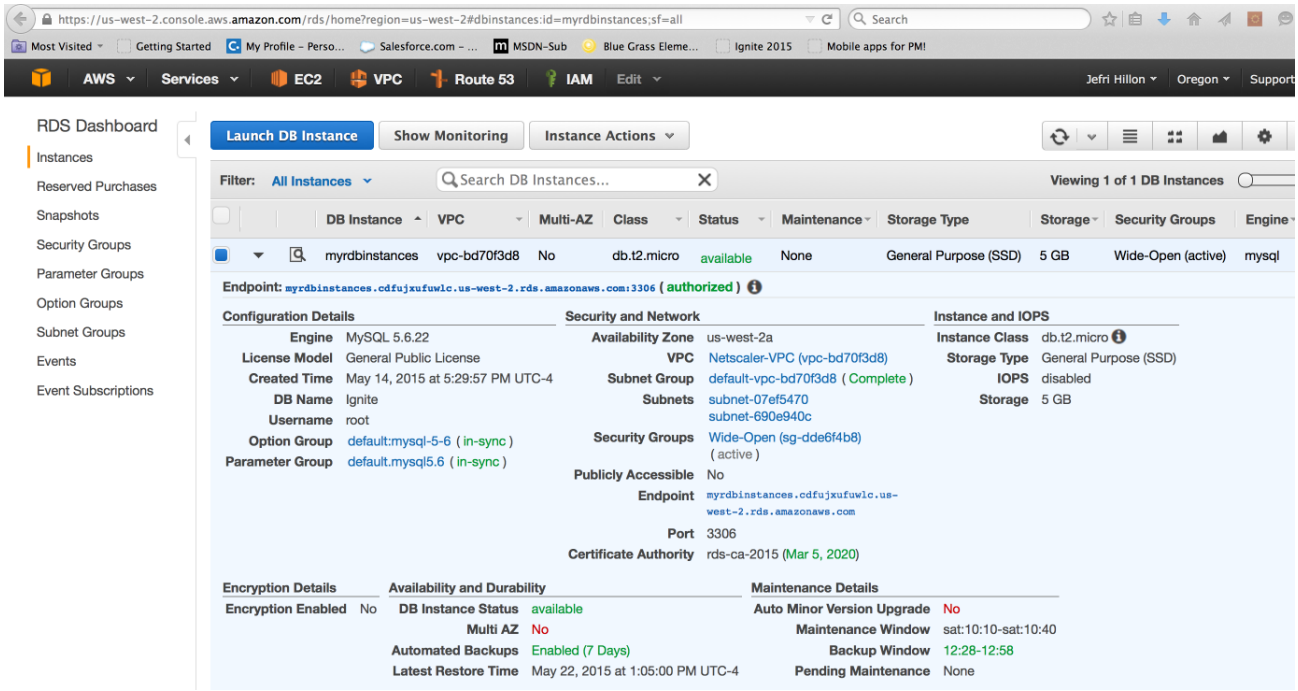
```
# The primary network interface auto eth0 iface eth0 inet dhcp
#static route for database segment up route add -net 192.168.3.0 netmask
 255.255.255.0 gw 192.168.2.13 dev eth0
```

3. Reboot to restart the networking on the web server.

```
sudo reboot now
```

STEP 3 | Connect the web server to the database service.

1. Establish an SSH connection to the server after the reboot.
2. (One-time task—only when you deploy the first web server) Configure the database **Endpoint** name. This is the DNS name and port for your DB instance and is displayed on the RDS instance.



3. Connect to the database. For example:

```
mysql -u awsuser -h myrdbinstances.cdfujxufuwlc.us-
west-2.rds.amazonaws.com -p
```

4. Create the database and add WordPress users and permissions. For example:

```
CREATE DATABASE Ignite;
CREATE USER 'student'@'%' IDENTIFIED BY 'paloalto';
GRANT ALL PRIVILEGES ON Ignite.* TO 'student'@'%';
FLUSH PRIVILEGES;
Exit
```

STEP 4 | Install and configure WordPress.

1. Install updates, Apache, and WordPress on each server.

```
sudo apt-get update
sudo apt-get install apache2
sudo apt-get install wordpress
```

2. Create the WordPress path in Apache.

```
sudo ln -s /usr/share/wordpress /var/www/html/wordpress
```

3. Create a WordPress configuration file and add a username and password for a new user. For example:

```
sudo gzip -d /usr/share/doc/wordpress/examples/setup-mysql.gz
sudo bash /usr/share/doc/wordpress/examples/setup-mysql -n Ignite -u
 student -t myrdbinstances.cdfujxufuwlc.us-west-2.rds.amazonaws.com
192.168.2.50
```

4. Move the existing WordPress configuration file to a file that will match the domain name.

```
Sudo mv /etc/wordpress/config-192.168.2.50.php /etc/wordpress/config-
wordpress.ignite-aws-demo.com.php
```

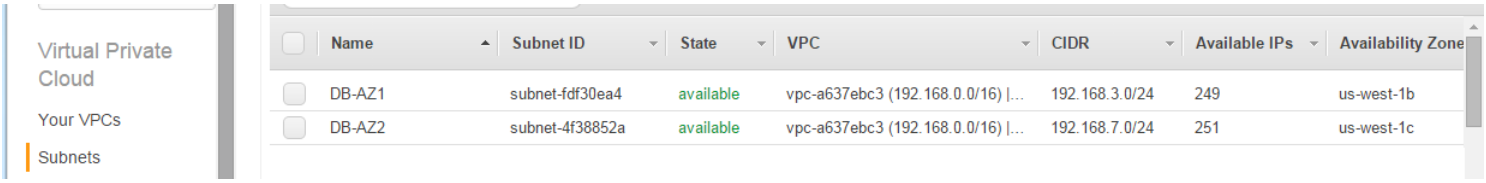
If you see the error `config-<Route53>.php file is inaccessible` when verifying access to the WordPress application, confirm that the file owner is `www-data` and that the spelling and syntax are accurate.

Set Up the Amazon Relational Database Service (RDS)

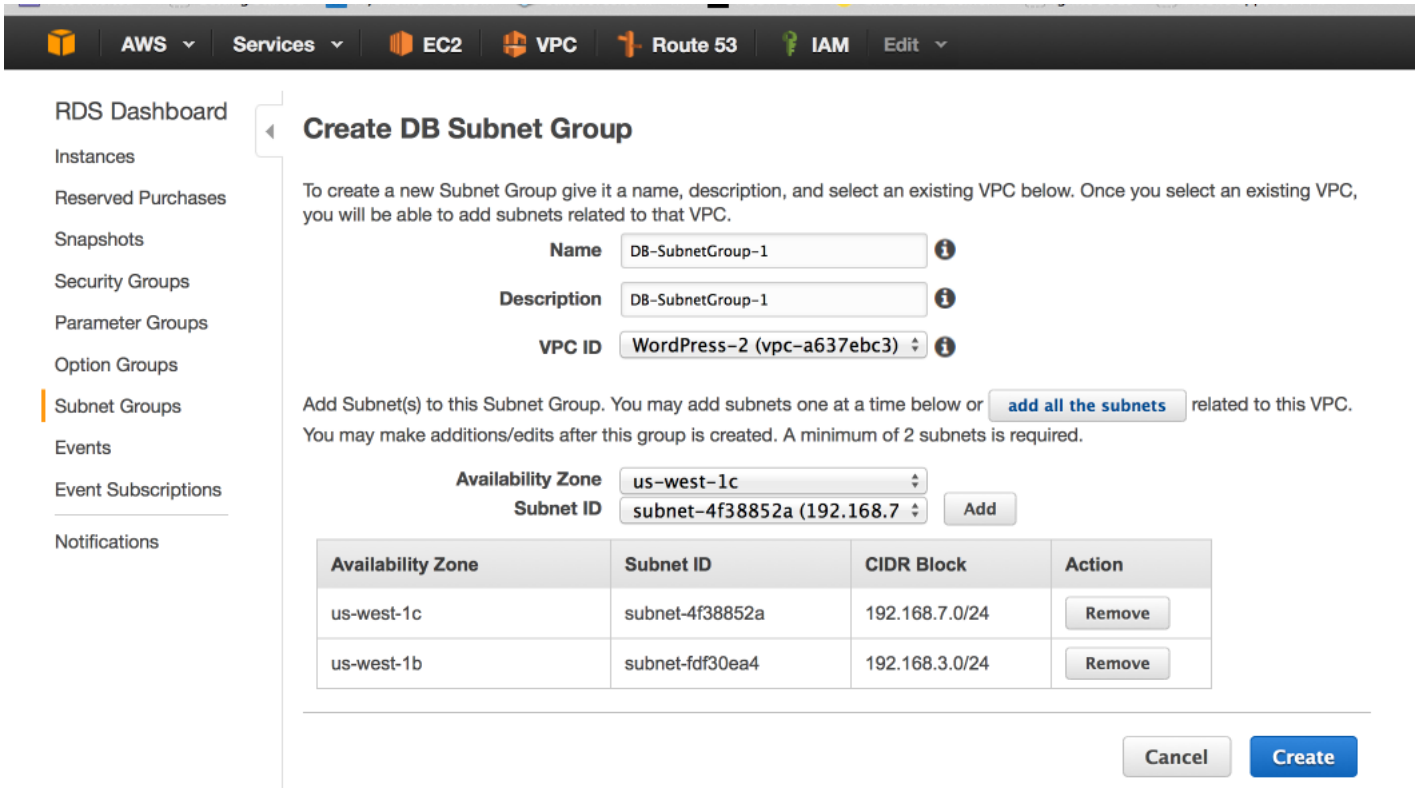
This section shows how to set up the database service for this use case. These instructions are included solely for the purpose of taking you through the implementation of this specific use case. For setup and conceptual information on the service, refer to Amazon Relational Database Service documentation.

For the topology and solution details, see Use Case: Deploy the VM-Series Firewalls to Secure Highly Available Internet-Facing Applications on AWS and Solution Overview—Secure Highly Available Internet-Facing Applications.

STEP 1 | In the VPC Dashboard, make sure there are two database subnets. If not, create a second one (a minimum of two subnets is required for the RDS).

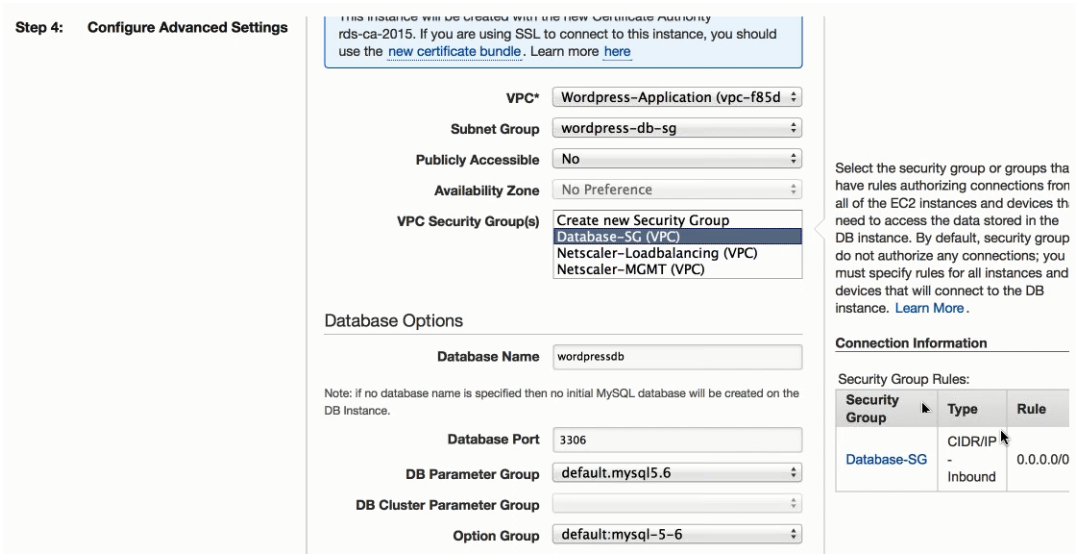


STEP 2 | In the RDS Dashboard, create a **DB Subnet Group** that includes both subnets.

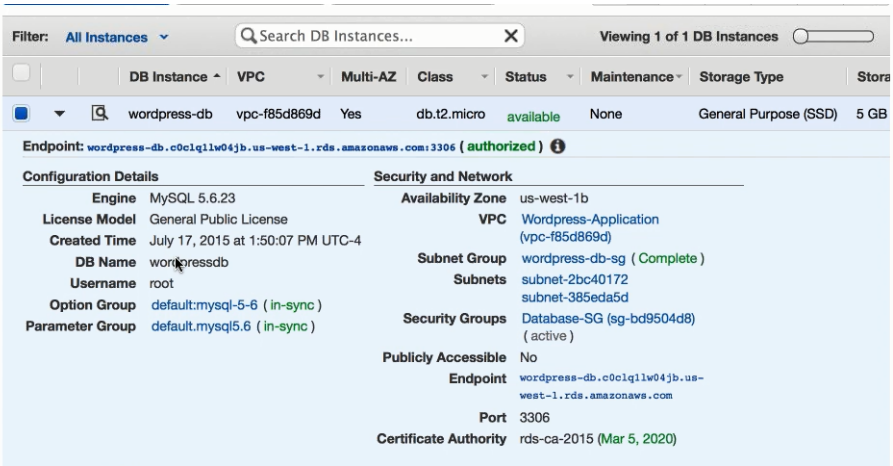


STEP 3 | Launch the **Create DB Wizard**. This example uses the following options:

- **DB Engine**—My SQL
- **Multi-AZ Deployment**—Yes
- **DB Instance class and Advanced Settings**—Based on your deployment needs



STEP 4 | Verify that the RDS is running.



Configure the Citrix NetScaler VPX

This section shows you how to set up the NetScaler VPX load balancer for this use case. These instructions are included solely for the purpose of taking you through the implementation in this use case. For set up and conceptual information on the NetScaler VPX, refer to the Citrix documentation.

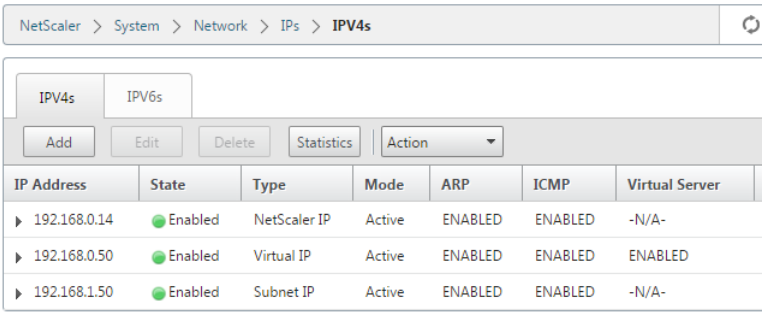
For the topology and solution details, see Use Case: Deploy the VM-Series Firewalls to Secure Highly Available Internet-Facing Applications on AWS and Solution Overview—Secure Highly Available Internet-Facing Applications.

STEP 1 | Launch the NetScaler VPX and assign an Elastic IP Address.

1. Launch the NetScaler VPX.
2. Allocate and associate Elastic IP Addresses for the firewall and the NetScaler VPX.

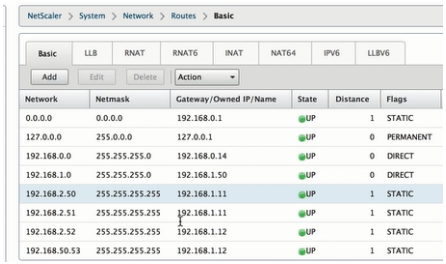
STEP 2 | Configure the Virtual IP and the Subnet IP on the NetScaler VPX.

1. On the NetScaler management console, select **Configuration** > **System** > **Network** > **IPs**.
2. **Add** the Virtual IP and the Subnet IP addresses.



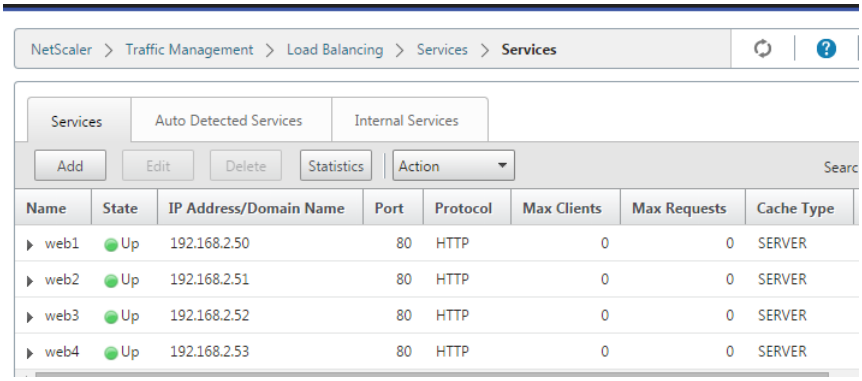
STEP 3 | Add static routes to direct traffic to the web servers. Make sure to add routes for the web servers in both Availability Zones.

Add the routes in **Configuration** > **System** > **Network** > **Routes**. In this example, we add routes to direct traffic from web1 and web2 through eth 1/1 on AZ1-FW1 and traffic from web 3 and web4 to eth1/1 on AZ1-FW2.



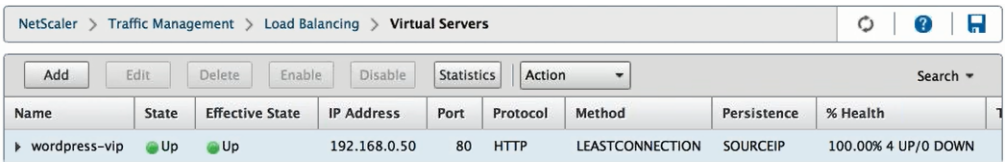
STEP 4 | Create a service for each web server.

Add the web services in **Configuration** > **Traffic Management** > **Load Balancing** > **Services**.



STEP 5 | Configure the virtual server. The Virtual server IP address is the only IP address that is exposed to users who connect to the web server from the internet.

1. **Add** a Virtual Server IP address in **Configuration** > **Traffic Management** > **Load Balancing** > **Virtual Servers**.



2. Bind the web services you created in step 4 to this virtual server.
3. Edit the settings for the virtual server to enable IP address persistence. IP address persistence is required for the application to authenticate properly. Based on your preference, select **Cookie-based** or **Source-IP-based** persistence.

STEP 6 | Test your configuration.

Verify that you can log in to the web server.

The WordPress application in this use case would be accessible at **`http://ignite-aws-demo.com/wordpress`**.

Set up Amazon Route 53

Use Amazon Route 53 as the DNS service for your registered domain names.

For an overview of the topology and solution details see, Use Case: Deploy the VM-Series Firewalls to Secure Highly Available Internet-Facing Applications on AWS and Solution Overview—Secure Highly Available Internet-Facing Applications.

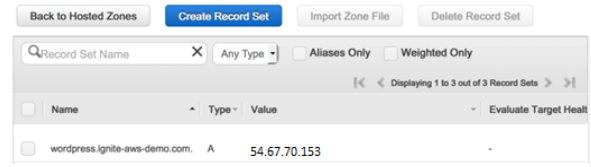
STEP 1 | Create a hosted zone(s) for a domain(s).

Refer to the AWS documentation on Creating a Public Hosted Zone.

STEP 2 | Add the resource record sets to route traffic to the domain(s).

To create a resource record set in your hosted zone, refer to Working with Resource Record Sets.

In this example, the record set resolves the desired domain to the Elastic IP Address on the NetScaler VPX that fronts the web servers in the VPC. It is a Type A IPv4 address that is the Elastic IP Address assigned to the VIP (192.168.0.50) on the NetScaler VPX.

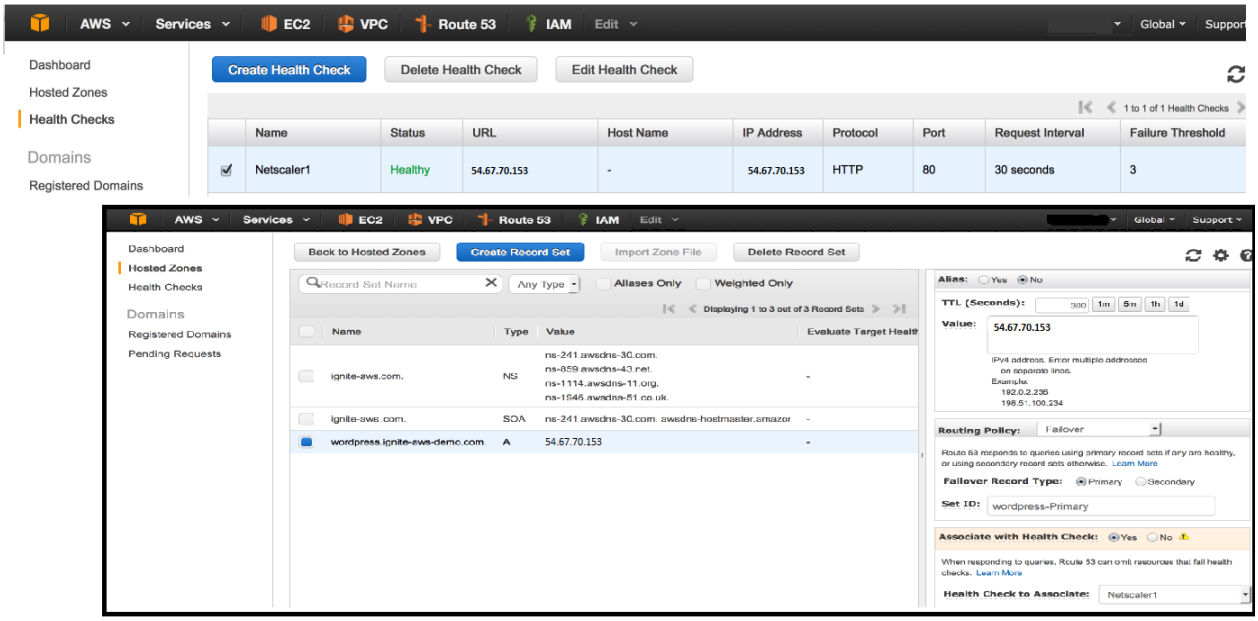


In a redundant configuration, configure the domain to resolve to every Elastic IP Address associated with a VIP on the NetScaler VPX.

The Citrix NetScaler can host multiple applications on one IP address with Content Switching enabled.

STEP 3 | Create a health check and associate it with a record set.

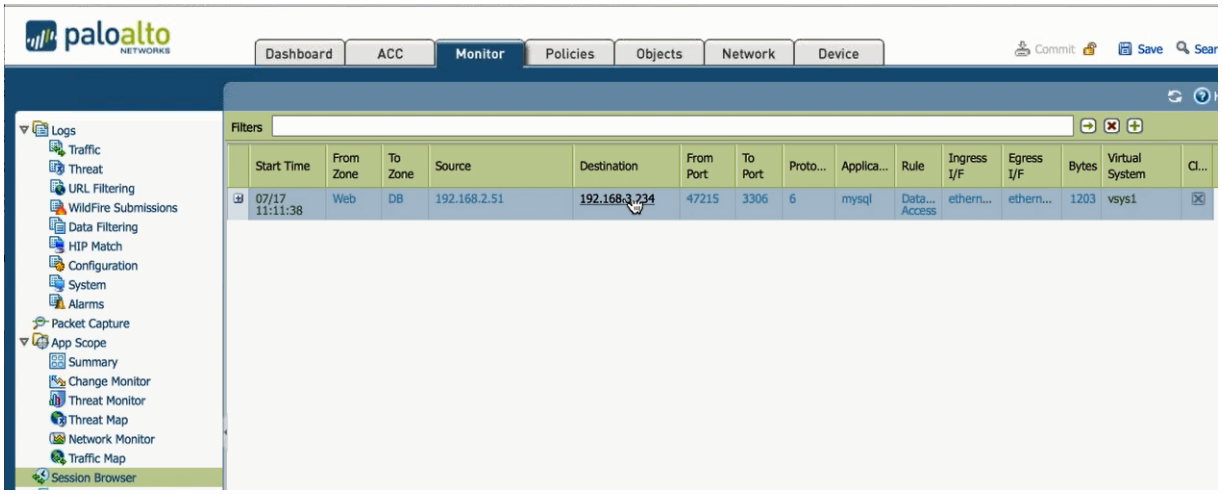
Use Route 53 health checks to validate that the application is available for a given Availability Zone. If Route 53 detects a failure, such as an Availability Zone failure, NetScaler VPX failure, or failure of the web servers, it stops serving the associated ElasticIP Address via DNS resolution until the health check is successful.



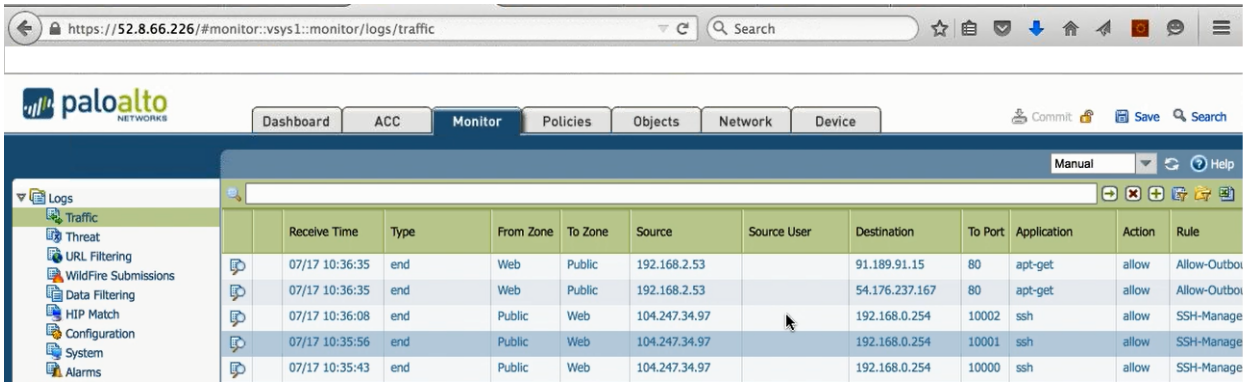
Verify Traffic Enforcement

Access the WordPress server and monitor the logs on the VM-Series firewalls to verify that policy is being enforced for your multi-tiered applications on AWS.

STEP 1 | On the web interface of the VM-Series firewall, select **Monitor** > **Logs** > **Traffic**. The following screenshot from the Mgmt-FW firewall shows that management traffic (SSH) and infrastructure traffic (application updates) to the web servers are secured.



STEP 2 | Check the session browser (**Monitor** > **Session Browser**) on the firewall for sessions that are still in progress. By default, a traffic log is generated after a session terminates. The following screenshot is from the VM-Series firewall that is securing the RDS.



For the overview of the topology and solution details see, Use Case: Deploy the VM-Series Firewalls to Secure Highly Available Internet-Facing Applications on AWS and Solution Overview—Secure Highly Available Internet-Facing Applications.

Port Translation for Service Objects

This table shows how the firewall performs IP address and port translation for routing traffic to the web farm when you have configured service objects with NAT policy in Create service objects and a service group. and Define NAT policy rules.

Server	Private IP: Port	Private IP: Translated Port	Public IP: Port
Web1	192.168.2.50:22	192.168.2.50:10000	52.8.66.226:10000
Web2	192.168.2.51:22	192.168.2.51:10001	52.8.66.226:10001
Web3	192.168.2.52:22	192.168.2.52:10002	52.8.66.226:10002

Server	Private IP: Port	Private IP: Translated Port	Public IP: Port
Web4	192.168.2.53:22	192.168.2.53:10003	52.8.66.226:10003

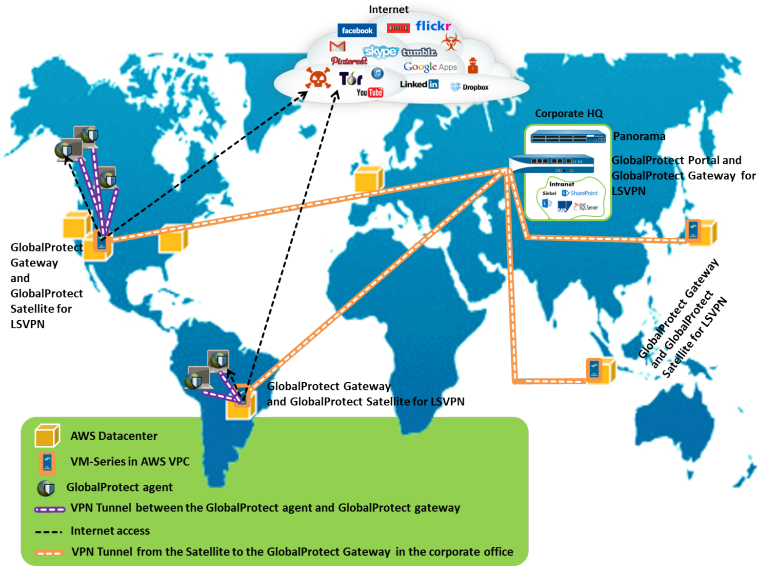
Use Case: VM-Series Firewalls as GlobalProtect Gateways on AWS

Securing mobile users from threats and risky applications is often a complex mix of procuring and setting up the security and IT infrastructure, ensuring bandwidth and uptime requirements in multiple locations around the globe while staying within your budget.

The VM-Series firewall on AWS melds the security and IT logistics required to consistently and reliably protect devices used by mobile users in regions where you do not have a presence. By deploying the VM-Series firewall in the AWS cloud, you can quickly and easily deploy GlobalProtect™ gateways in any region without the expense or IT logistics that are typically required to set up this infrastructure using your own resources.

To minimize latency, select AWS regions that are closest to your users, deploy the VM-Series firewalls on EC2 instances, and configure the firewalls as GlobalProtect gateways. With this solution, the GlobalProtect gateways in the AWS cloud enforce security policy for internet traffic so there is no need to backhaul that traffic to the corporate network. Additionally, for access to resources on the corporate network, the VM-Series firewalls on AWS leverage the LSVPN functionality to establish IPSec tunnels back to the firewall on the corporate network.

For ease of deployment and centralized management of this distributed infrastructure, use Panorama to configure the GlobalProtect components used in this solution. Optionally, to ensure that mobile devices, such as smartphones and tablets, are safe for use on your network, use a Mobile Device Manager to configure and manage mobile devices.



- Components of the GlobalProtect Infrastructure
- Deploy GlobalProtect Gateways on AWS

Components of the GlobalProtect Infrastructure

To block risky applications and protect mobile users from malware, you must set up the GlobalProtect infrastructure, which includes the GlobalProtect portal, the GlobalProtect gateway, and the GlobalProtect app. Additionally, for access to corporate resources, you must set up an IPSec VPN connection between the

VM-Series firewalls on AWS and the firewall in the corporate headquarters using LSVPN (a hub and spoke VPN deployment).

- The GlobalProtect agent/app is installed on each end-user system that is allowed to access corporate applications and resources. The agent first connects to the portal to obtain information on the gateways and then establishes a secure VPN connection to the closest GlobalProtect gateway. The VPN connection between the end-user system and the gateway ensures data privacy.
- The GlobalProtect portal provides the management functions for the GlobalProtect infrastructure. Every end-user system receives configuration information from the portal, including information about available gateways as well as any client certificates that may be required to connect to the GlobalProtect gateway(s). In this use case, the GlobalProtect portal is a hardware-based firewall that is deployed in the corporate headquarters.
- The GlobalProtect gateway delivers mobile threat prevention and policy enforcement based on applications, users, content, device, and device state. In this use case, the VM-Series firewalls on AWS function as the GlobalProtect gateways. The GlobalProtect gateway scans each user request for malware and other threats, and, if policy allows, sends the request to the internet or to the corporate network over the IPSec tunnel (to the LSVPN gateway).
- For LSVPN, you must configure the GlobalProtect portal, GlobalProtect gateway for LSVPN (hub), and the GlobalProtect Satellites (spokes).

  In this use case, the hardware-based firewall in the corporate office is deployed as the GlobalProtect portal and the LSVPN gateway. The VM-Series firewalls on AWS are configured to function as GlobalProtect satellites. The GlobalProtect satellites and gateway are configured to establish an IPSec tunnel that terminates on the gateway. When a mobile user requests an application or resource that resides on the corporate network, the VM-Series firewall routes the request over the IPSec tunnel.

Deploy GlobalProtect Gateways on AWS

To secure mobile users, in addition to deploying and configuring the GlobalProtect gateways on AWS, you need to set up the other components required for this integrated solution. The following table includes the recommended workflow:

- Deploy the VM-Series firewall(s) on AWS.

  See Deploy the VM-Series Firewall on AWS.

- Configure the firewall at the corporate headquarters.

  In this use case, the firewall is configured as the GlobalProtect portal and the LSVPN gateway.

  - Configure the GlobalProtectportal.
  - Configure the GlobalProtectportal for LSVPN.
  - Configure the portal to authenticateLSVPN satellites.
  - Configure the GlobalProtectgateway for LSVPN.

- Set up a template on Panorama for configuring the VM-Series firewalls on AWS as GlobalProtect gateways and LSVPN satellites.

  To easily manage this distributed deployment, use Panorama to configure the firewalls on AWS.

  - Create template(s) on Panorama.

  Then use the following links to define the configuration in the templates.

  - Configure the firewall asa GlobalProtect gateway.
  - Prepare the satellite tojoin the LSVPN.

- Create device groups on Panorama to define the network access policies and internet access rules and apply them to the firewalls on AWS.

  See Create device groups.

- Apply the templates and the device groups to the VM-Series firewalls on AWS, and verify that the firewalls are configured properly.

- Deploy the GlobalProtect client software.

  Every end-user system requires the GlobalProtect agent or app to connect to the GlobalProtect gateway.

  See Deploy the GlobalProtectclient software.

Auto Scale VM-Series Firewalls with the Amazon ELB Service

Palo Alto Networks delivers the Auto Scaling VM-Series Firewalls CloudFormation Templates and scripts for deploying an auto-scaling tier of VM-Series firewalls using several AWS services such as Lambda, auto scaling groups, Elastic Load Balancing (ELB), S3, SNS, and CloudWatch, and the VM-Series automation capabilities including the PAN-OS API and bootstrapping. The templates allow you to leverage the AWS scalability features designed to manage sudden surges in demand for application workload resources by independently scaling the VM-Series firewalls with changing workloads.

The following versions of these template are available on the Palo Alto Networks GitHub repository:

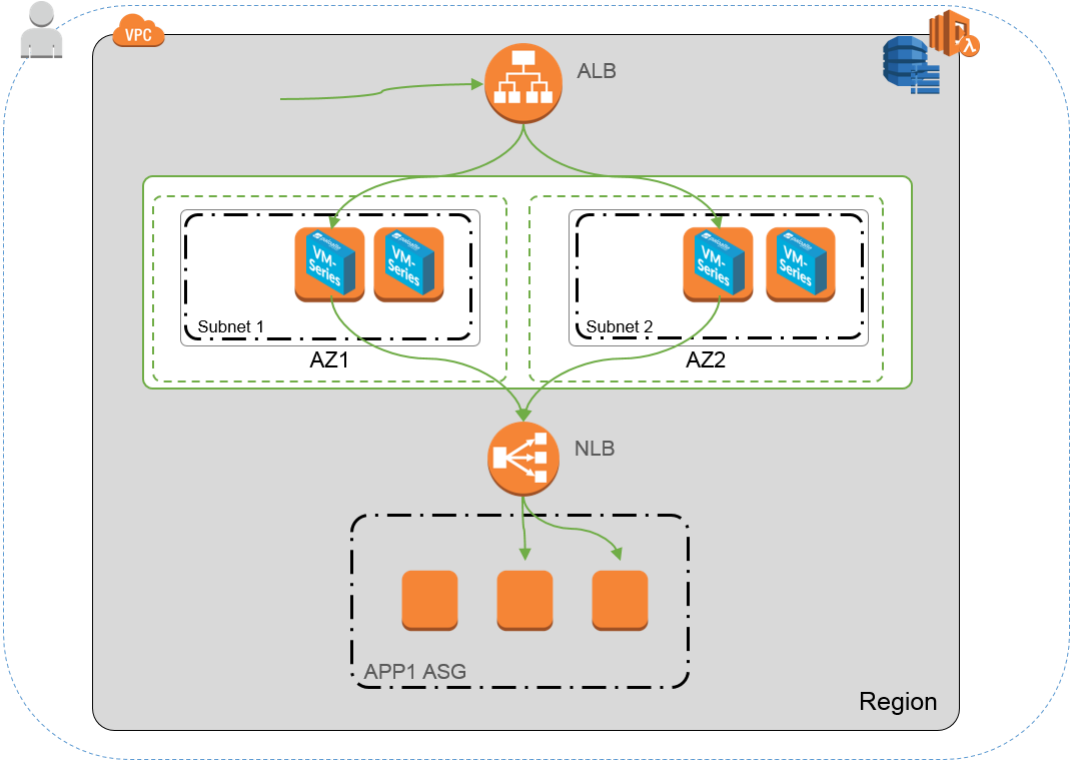
- VM-Series Auto Scale Template for AWS Version 2.0
- Auto Scale Template Version 1.2 (and earlier)

VM-Series Auto Scale Template for AWS Version 2.0

To help you manage increased application scale, version 2.0 of the auto scaling VM-Series firewall template provides a hub and spoke architecture that simplifies deployment. This version of the solution provides two templates that support a single and multi-VPC deployment both within a single AWS account and across AWS accounts.

- **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 firewalls automatically publish custom PAN-OS metrics that enable auto scaling.

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

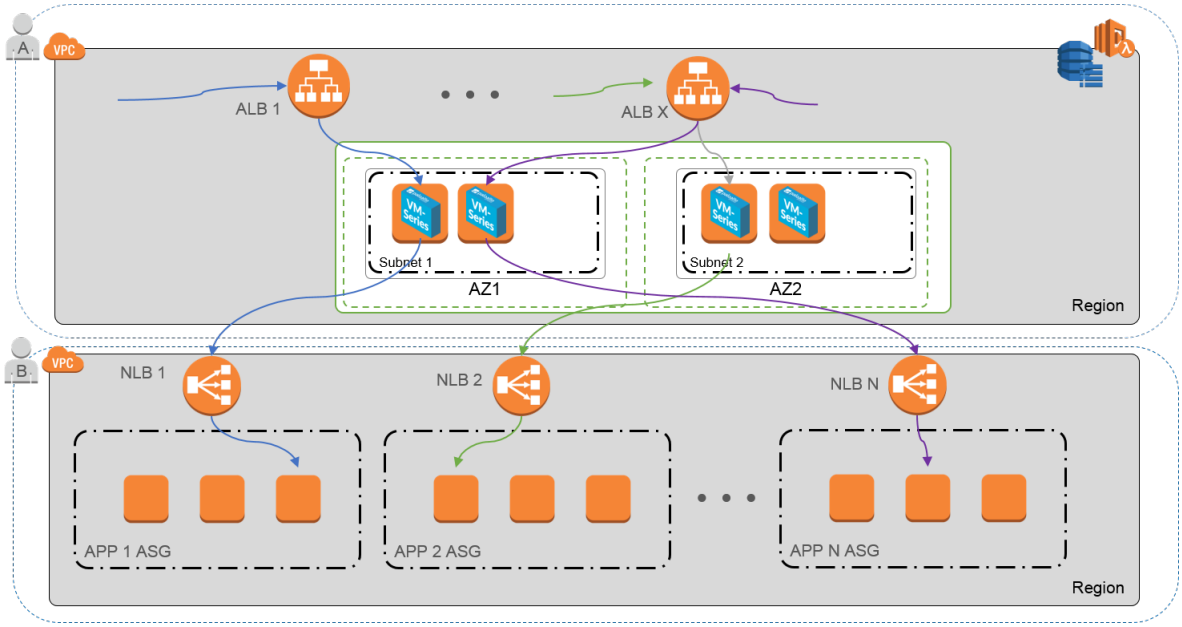


The following application template deploys the network load balancer (NLB) depicted in the preceding image.

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

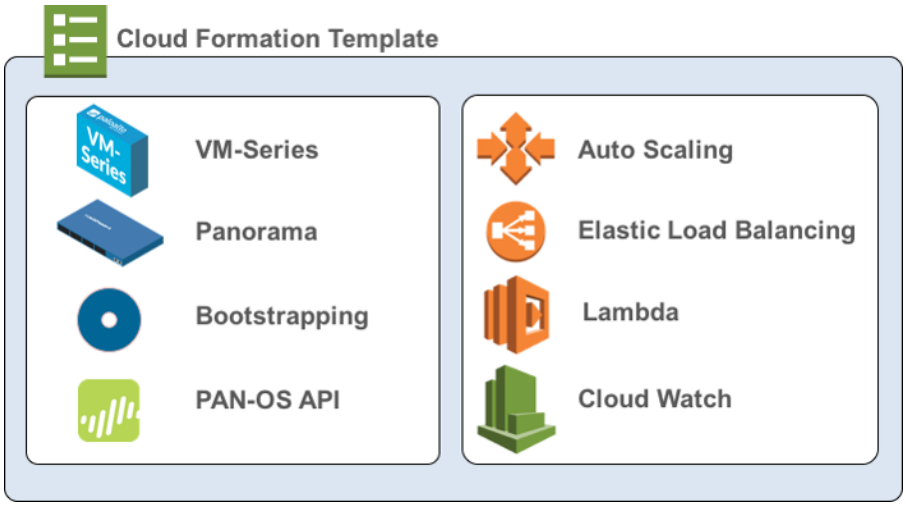
  The application template is community supported. This template is provided as an example to help you get started with a basic web application. For a production environment, either use your own application template or customize this template to meet your requirements.

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(s), which distributes traffic to an auto scaling tier of web or application 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 of firewalls.



- What Components Does the VM-Series Auto Scaling Template for AWS (v2.0) Leverage?
- How Does the VM-Series Auto Scaling Template for AWS (v 2.0) Enable Dynamic Scaling?
- Plan the VM-Series Auto Scaling Template for AWS (v 2.0)
- Customize the Firewall Template Before Launch (v2.0)
- Launch the VM-Series Auto Scaling Template for AWS (v2.0)
- Customize the Bootstrap.xml File (v2.0)
- Stack Update with VM-Series Auto Scaling Template for AWS (v2.0)
- Modify Administrative Account and Update Stack

What Components Does the VM-Series Auto Scaling Template for AWS (v2.0) Leverage?



The VM-Series Auto Scaling template for AWS includes the following building blocks :

Building Block	Description
Firewall template (Palo Alto Networks officially supported template)	The firewall-v2.0.template deploys a new VPC with two Availability Zones (AZs), subnets, route tables, and security groups required for routing traffic across these AZs, and an AWS NAT gateway. It also deploys an external application load balancer, and an Auto Scaling Group (ASG) with a VM-Series firewall in each AZ. Due to the many variations in a production environment including but not limited to the number of subnets, availability zones, route tables, security groups etc., you must deploy the firewall-v2.0.template in a new VPC. *VM-Series Auto Scaling template for AWS does not deploy Panorama, and Panorama is optional. Panorama provides ease of policy management and central visibility. If you want to use Panorama to manage the VM-Series firewalls that the solution deploys, you can either use an M-Series appliance inside your corporate network, or a Panorama virtual appliance on a VMware ESXi server inside your corporate network or in vCloud Air.* 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.
Application template (Community supported template)	The application template deploys a network load balancer and an ASG with a web server in each AZ. Because the network load balancer has a unique IP address per AZ, and the NAT policy rule on the firewalls must reference a single IP address, there is one ASG for each of the two AZs. All the firewalls in an ASG have identical configuration. This version of the auto scaling solution includes two application templates:

Building Block	Description
	• The panw_aws_nlb-v2.0.template allows you to deploy the application template resources within same VPC as the one in which you deployed the firewall template (same AWS account). • The panw_aws_nlb_vpcv-2.0.template allows you to deploy the application template resources in a separate VPC. This template supports both single and cross AWS account deployments.
Lambda functions	AWS Lambda provides robust, event-driven automation without the need for complex orchestration software. In the firewall-v2.0.template, AWS Lambda monitors a Simple Queue Service (SQS) to learn about network load balancers that publish to the queue. When the lambda function detects a new network load balancer, it creates a new NAT policy rule and applies it to the VM-Series firewalls within the ASG. The firewalls have a NAT policy rule for each application, and the firewalls use the NAT policy rule (that maps the port to network load balancer IP address) to forward traffic to the network load balancer in front of the application web servers. *You need to create the Security policy rule to allow or deny application traffic for your deployment. The sample bootstrap.xml file does not include any Security policy rules. Using Panorama to centrally manage the firewalls simplifies the process of creating Security policy rules.* The Lambda functions also add or remove elastic network interfaces (ENIs) when the firewall is launched or terminated, delete all the associated resources when an instance is terminated or the stack is deleted, remove the firewall as a managed device on Panorama, and deactivate the BYOL license when a firewall is terminated on a scale in event. To learn more about the lambda functions, refer to **http://paloaltonetworks-aws-autoscale-2-0.readthedocs.io/en/latest/**
Bootstrap files The bootstrap.xml file provided in the GitHub repository is provided for testing and evaluation only. For a production deployment, you must modify the sample credentials in the bootstrap.xml prior to launch.	This solution requires the init-cfg.txt file and the bootstrap.xml file so that the VM-Series firewall has the basic configuration for handling traffic. • The init-cfg.txt file includes the mgmt-interface-swap operational command to enable the firewall to receive dataplane traffic on its primary interface (eth0). This auto-scaling solution requires the swapping of the dataplane and management interfaces to enable the application load balancer to forward web traffic to the auto-scaling tier of VM-Series firewalls. For details see Management Interface Mapping for Use with Amazon ELB. • The bootstrap.xml file enables basic connectivity for the firewall network interfaces and allows the firewall to connect to AWS CloudWatch namespace that matches the stack name you enter when launching the template.

To deploy the solution, see Launch the VM-Series Auto Scaling Template for AWS (v2.0).

How Does the VM-Series Auto Scaling Template for AWS (v 2.0) Enable Dynamic Scaling?

The VM-Series firewalls that are deployed using the auto scaling template version 2.0 scale in and scale out based on custom PAN-OS metrics. The VM-Series firewalls natively publish these metrics to the Amazon CloudWatch console, and based on the metric(s) that you choose as the scaling parameter(s), you can define CloudWatch alarms and policies to dynamically deploy or terminate instances to handle the application traffic in your AWS deployment.

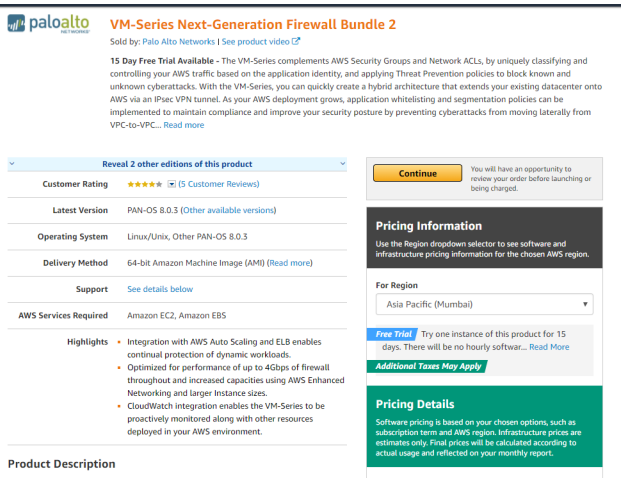
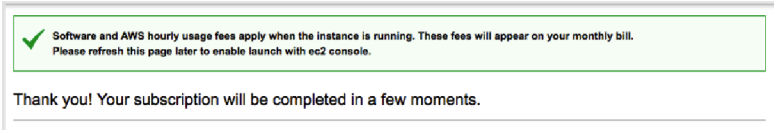
The firewalls publish metrics to AWS CloudWatch at a five-minute frequency (by default). When a metric that is being monitored reaches the configured threshold for the defined time interval, CloudWatch triggers an alarm and initiates an auto-scaling event.

When the auto-scaling event triggers the deployment of a new firewall, the new instance bootstraps at launch and a lambda function configures the firewall with NAT policy rules. A NAT policy rule is created for each application, and the rule references the IP addresses for each network load balancer in your deployment. When the application load balancer receives a request, it forwards the request to the firewall on the assigned TCP port. The firewall then inspects the traffic and forwards it to the corresponding network load balancer, which in turn forwards the request to a web server in its target group.

Plan the VM-Series Auto Scaling Template for AWS (v 2.0)

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

Planning Checklist for Version 2.0	
❑ Verify the requirements for deploying the VM-Series Auto Scaling template.	Version 2.0 of the auto scaling template requires AWS Lambda and S3 Signature versions 2 or 4, and can deploy VM-Series firewalls running PAN-OS 8.0. You need to look up the list of supported regions and the AMI IDs, to provide as an input in the firewall template.
❑ Assign the appropriate permissions for the IAM user role.	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. 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 her to write to the SQS queue that belongs to the firewall template.
❑ Collect the details required for a cross-account deployment.	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: • 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.
❑ Create a support account on the Palo Alto Networks Support portal, if you don't already have one.	With VM-Series Auto Scaling template version 2.0, you can opt for the BYOL or PAYG licenses. • 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 `/license` folder with filename as authcodes in the bootstrap package. See Launch the VM-Series Auto Scaling Template for AWS (v2.0) for details. • For PAYG, you must register the VM-Series firewalls to activate your support entitlement.
❑ (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.	In the AWS Marketplace, search for Palo Alto Networks, and select the bundle you plan to use. The VM-Series firewalls will fail to deploy if you have not accepted the EULA for the bundle you plan to use. • Search for **VM-Series Next Generation Firewall Bundle 2, for example**.  • Click **Continue**, and select **Manual Launch**. Review the agreement and click **Accept Software Terms** to accept the EULA.  You can now close the browser.
❑ Decide whether you plan to use the public S3 buckets or your private S3 bucket for AWS Lambda,	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. *Palo Alto Networks recommends using the bootstrap files in the public S3 bucket only for evaluating this solution. For a*

Planning Checklist for Version 2.0	
Python scripts, and templates.	*production deployment, you must create a private S3 bucket for the bootstrap package.* 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. 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.

❑ Download the templates, AWS Lambda code, and the bootstrap files.	• Get the files for deploying the firewall template (application load balancer and the VM-Series firewalls) from the GitHub repository at: https://github.com/PaloAltoNetworks/aws-elb-autoscaling/tree/master/Version-2.0
	
	Do not mix and match files across VM-Series Auto Scaling template versions.
	
	  • Templates and Lambda code:
	  • panw-aws.zip
	  • firewall-v2.0.template
	  • Bootstrap files:
	  • init-cfg.txt
	  • bootstrap.xml
	
	  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.
	  • iam-policy: The user who deploys the VM-Series Auto Scaling template must have either the administrative privileges or the permissions listed in this file to successfully launch this solution.
	• Get the files for deploying the NLB and the web servers from the GitHub repository at: https://github.com/PaloAltoNetworks/pan_nlb_v1
	  • Templates:
	  • pan_aws_nlb-2.0.template—Use this template to deploy the application template resources within same VPC as the one in which you deployed the firewall template (same AWS account).
	  • pan_aws_nlb_vpc-2.0.template—Use this template to deploy the application template resources in a different VPC. This template allows you to deploy the resources within the same AWS account or in a different AWS account as long as you have the appropriate permissions to support a cross-account deployment.
	  • pan_nlb_lambda.template
	  • Lambda code and Python scripts.

❑ Customize the bootstrap.xml file	To ensure that your production environment is secure, you must customize the bootstrap.xml file with a unique administrative username and password for production deployments. The default username and password are

Planning Checklist for Version 2.0	
for your production environment.	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.
❑ Decide whether you want to use Panorama for centralized logging, reporting, and firewall management.	Panorama is an option for administrative ease and is the best practice for managing the firewalls. It is not required to manage the auto scaling tier of VM-Series firewalls deployed in this solution. If you want to use Panorama, you can either use an M-Series appliance or a Panorama virtual appliance on a VMware ESXi server inside your corporate network. To successfully register the firewalls with Panorama, you must collect the following details: • 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. 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. • Template stack name and the device group name to which to assign the firewalls—You must first add a template and assign it to a template stack, create a device group on Panorama, and then include the template stack name and the device group name in the configuration (init-cfg.txt) file. *In order to reduce the cost and scale limits of using Elastic IP addresses, the firewalls do not have public IPs. 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.*
Get started	Launch the VM-Series Auto Scaling Template for AWS (v2.0)

Customize the Firewall Template Before Launch (v2.0)

To simplify the deployment workflow, the firewall-v2.0.template displays a limited set of parameters for which you need to provide inputs when launching the template. If you would like to view and customize other options included in the template, you can use a text editing tool such as Notepad or Visual Studio Code to specify values that you prefer before you Launch the VM-Series Auto Scaling Template for AWS (v2.0).

Use the following table to view the list of parameters that you are allowed to customize for your deployment of the auto scaling firewall template for AWS. Modifying parameters from this list is within the official support policy of Palo Alto Networks through the support options that you've purchased.

Parameter	Description	Default Value
CIDR Block for the VPC	The IP address space that you want to use for the VPC.  *The subnets you modify below must belong to this VPC CIDR block and be unique.*	192.168.0.0/16
Management Subnet CIDR Block	Comma-delimited list of CIDR blocks for the management subnet of the firewalls.	192.168.0.0/24, 192.168.10.0/24
Untrust Subnet CIDR Block	Comma-delimited list of CIDR blocks for the Untrust subnet.	192.168.1.0/24, 192.168.11.0/24
Trust Subnet CIDR Block	Comma-delimited list of CIDR blocks for the Trust subnet.	192.168.2.0/24, 192.168.12.0/24
NAT Gateway Subnet CIDR Block	Comma-delimited list of CIDR blocks for the AWS NAT Gateway.	192.168.100.0/24, 192.168.101.0/24
Lambda Subnet CIDR Block	Comma-delimited list of CIDR blocks for the Lambda functions.	192.168.200.0/24, 192.168.201.0/24
Firewall Instance size	AWS Instance Types and size that you want for the VM-Series firewalls in your deployment.	M4.xlarge
Choose your Scaling Parameter  *You do not need to modify the template for the scaling parameter. You can set AWS CloudWatch alarms on the AWS*	The template publishes all the following metrics to AWS CloudWatch: • CPU—DataPlane CPU Utilization • AS—Active Sessions • SU—Session Utilization • SSPU—SSL Proxy Utilization • GPU—GlobalProtect Gateway Utilization • GPAT—GlobalProtect Gateway Utilization ActiveTunnels • DPB—Dataplane Packet Buffer Utilization	Dataplane CPU Utilization

Parameter	Description	Default Value
console for one or more custom PAN-OS metrics on which you want to trigger autoscaling.		
Choose time in seconds for Scaling Period	The period in seconds over which the average statistic is applied. Must be a multiple of 60.	900
Maximum VM-Series Instances	Maximum number of VM-Series firewalls in the auto scaling group.	3
Minimum VM-Series Instances	Minimum number of VM-Series firewalls in the auto scaling group.	1
ScaleDown threshold value in percentage/value	Value at which a scale in event is triggered.	20
ScaleUp threshold value in percentage/value	Value at which scale out event is triggered.	80

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

You can choose to deploy the firewall template in one VPC and the sample application template in the same VPC as the one in which you deployed the firewalls, or in a different VPC.

If the applications that you want to secure belong to a separate AWS account, the sample application template includes support for cross-account deployments. The solution supports a hub and spoke architecture whereby you can deploy the firewall template in one AWS account and use it as a hub to secure your applications (spokes) that belong to the same or to different AWS accounts.

- 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 Plan the VM-Series Auto Scaling Template for AWS (v 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 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 causes 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 as shown here:

   op-command-modes=mgmt-interface-swap

   vm-auth-key=755036225328715

   panorama-server=10.5.107.20

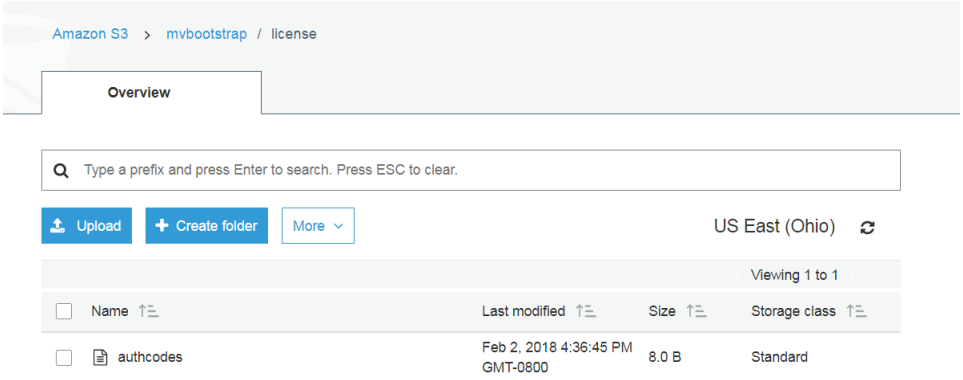
   panorama-server-2=10.5.107.21

   tplstackname=FINANCE_TG4

   dgname=finance_dg
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 to this file,and save the file as authcodes (no file extension) and upload it to the /license folder. 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 retrieves 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.

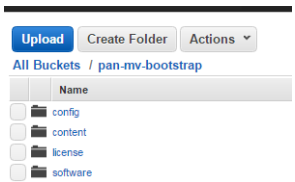
Required for using the VM-Series Auto Scaling template in a production environment.

The bootstrap.xml file in the GitHub repository is provided for testing and evaluation only. For a production deployment, you must Customize the Bootstrap.xml File (v2.0) prior to launch.

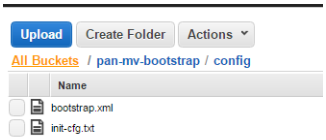
STEP 5 | Prepare the Amazon Simple Storage (S3) buckets for launching the VM-Series Auto Scaling template to a production environment.

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.

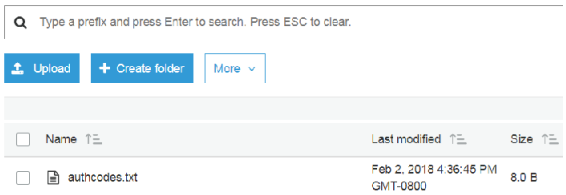
1. Create a new S3 bucket for the bootstrap files.
    1. Sign in to the AWS Management Console and open the S3 console.
    2. Click **Create Bucket**.
    3. Enter a **Bucket Name** and a **Region**, and click **Create**. The bucket must be at the S3 root level. If you nest the bucket, bootstrapping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



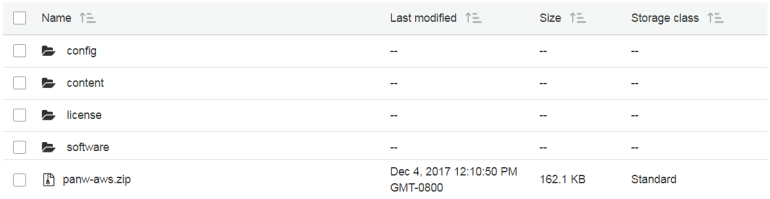
    3. Click the link to open the **config** folder.
    4. Select **Actions** > **Upload** and **Add Files**, browse to select the init-cfg.txt file and bootstrap.xml file, and click **Open**.
    5. Click **Start Upload** to add the files to the config folder. The folder can contain only two files: init-cfg.txt 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 an S3 bucket. In this example, the AWS Lambda code is in the same S3 bucket as the bootstrap package.
   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.



STEP 6 | Select the firewall template.

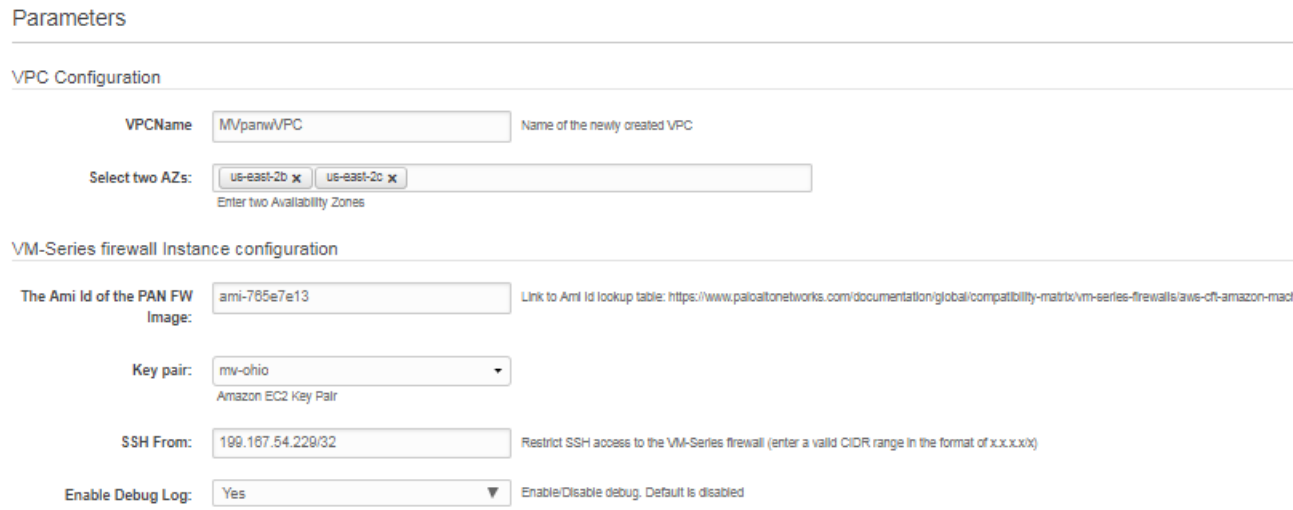
If you need to Customize the Firewall Template Before Launch (v2.0), do that now and select the modified template.

1. In the AWS Management Console, select **CloudFormation** > **Create Stack**.
2. Select **Upload a template to Amazon S3**, choose the firewall-v2.0.template 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**.
   2. Select the two Availability Zones that your setup spans in **Select two AZs**.

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

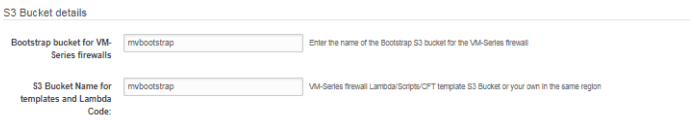


1. Look up the AMI ID for the VM-Series firewall and enter it. Make sure that the AMI ID matches the AWS region, PAN-OS-8.0 version and the BYOL or PAYG licensing option you opted to use.
2. Select the EC2 **Key pair** (from the drop-down) for launching the firewall. To log in to the firewalls, you must provide the name of this key pair and the private key associated with it.
3. Restrict SSH access to the firewall's management interface. Make sure to supply a CIDR block that corresponds to your dedicated management IP addresses or network. Do not make the allowed source network range larger than necessary and do not ever configure the allowed source as 0.0.0.0/0. Verify your IP address before configuring it on the 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 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 9 | Specify the name of the Amazon S3 bucket(s).

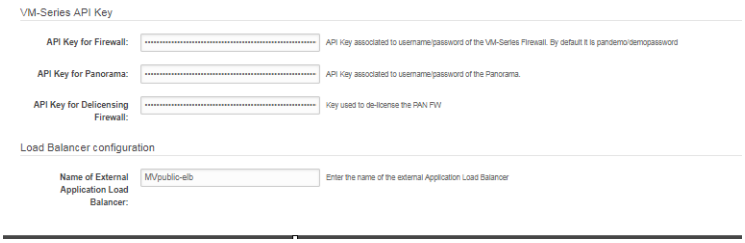
You can use one S3 bucket for the bootstrap package and the zip file.



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 fails and you cannot be able to 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.

STEP 10 | 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 bootstrap.xml 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, 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.

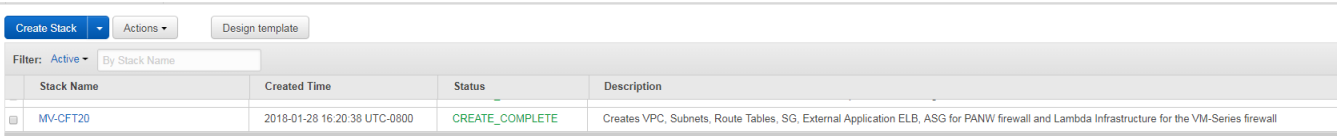
STEP 11 | Enter the name for the application load balancer.

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.

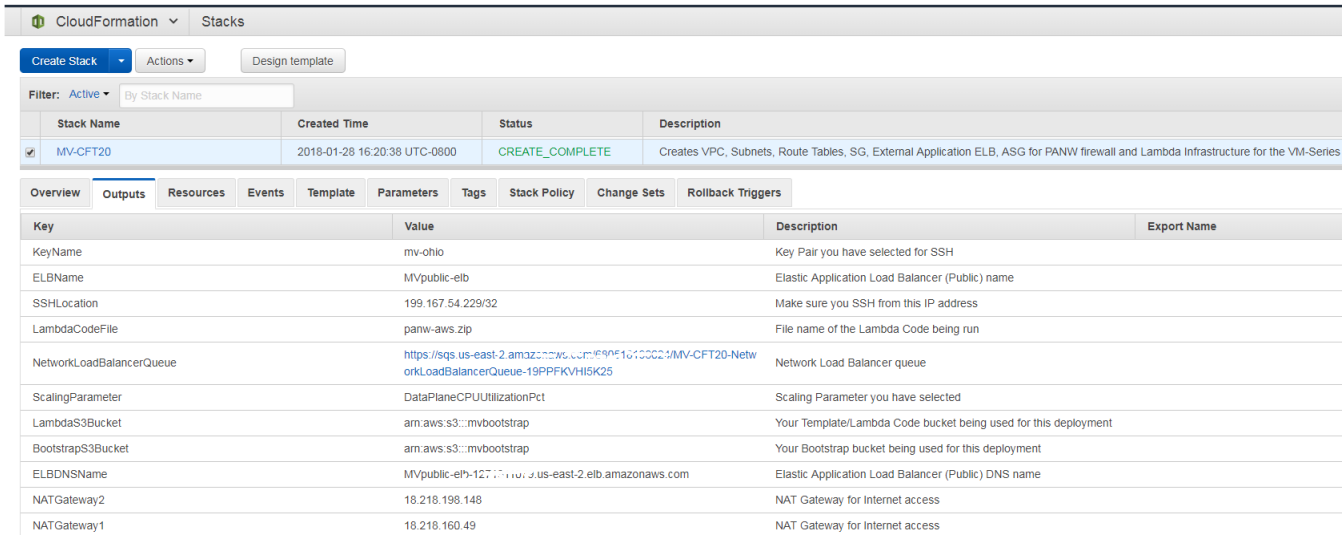
1. Select **I acknowledge that this template might cause AWS CloudFormation to create IAM resources**.
2. Click **Create** to launch the template. The CREATE_IN_PROGRESS event displays.
3. On successful deployment the status updates to CREATE_COMPLETE.



Unless you customized the template, the VM-Series Auto Scaling template launches an ASG that includes one VM-Series firewall in each AZ, behind the application load balancer.

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

1. On the AWS Management Console, select the stack name to view the **Output** for the list of resources.



2. 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.
3. 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 finish 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.*

STEP 15 | Save the following information. You need to provide these values as inputs when deploying the application template.

- IP addresses of the NAT Gateway in each AZ. You need this IP address to restrict HTTP access to the web servers if you deploy the application in a different VPC. Specifying this IP address ensures that the firewall secures access your applications in a different VPC, and that nobody can bypass the firewall to directly access the web server. The sample application template (panw_aws_nlb_vpc-2.0.template) displays a template validation error if you do not enter the NAT Gateway IP addresses; you must enter the IP addresses as a comma-separated list.
- Network Load Balancer SQS URL. A lambda function in the firewall stack monitors this queue so that it can learn about any network load balancers that you deploy, and create NAT policy rules (one per application) on the VM-Series firewalls that enable the firewalls to send traffic to the network load balancer IP address.

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. This application 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 to retrieve software updates. Use this template to evaluate the solution, but build your own template to deploy to production. For a custom template, make sure to enable SQS Messaging Between the Application Template and Firewall Template.

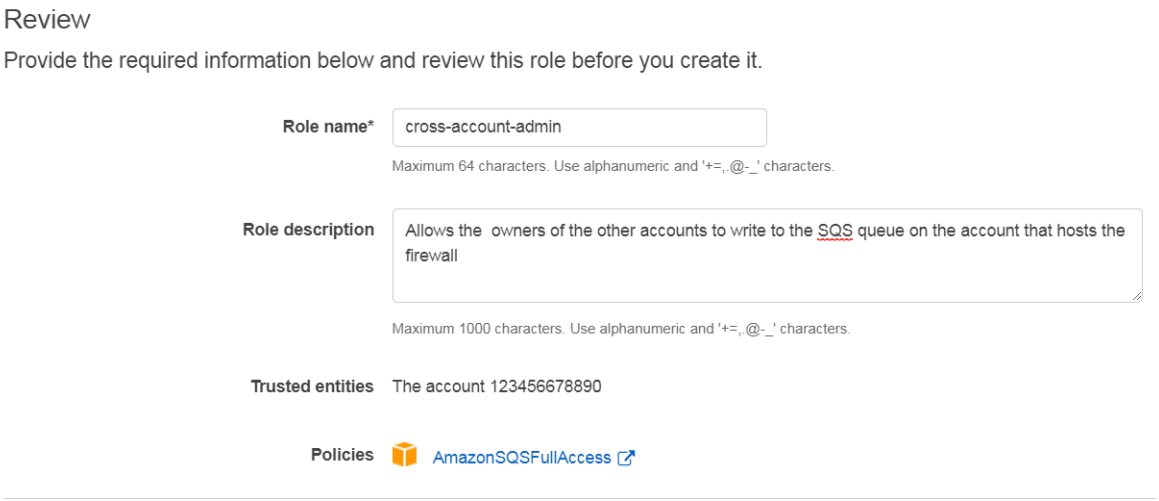
When launching the application template, you must select the template based on whether you want to deploy the application template within the same VPC (panw_aws_nlb-2.0.template) in which you deployed the firewall template or in a separate VPC (panw_aws_nlb_vpc-2.0.template). For a separate VPC, the

template provides supports for cross-account deployments. A cross-account deployment requires you to create an 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.

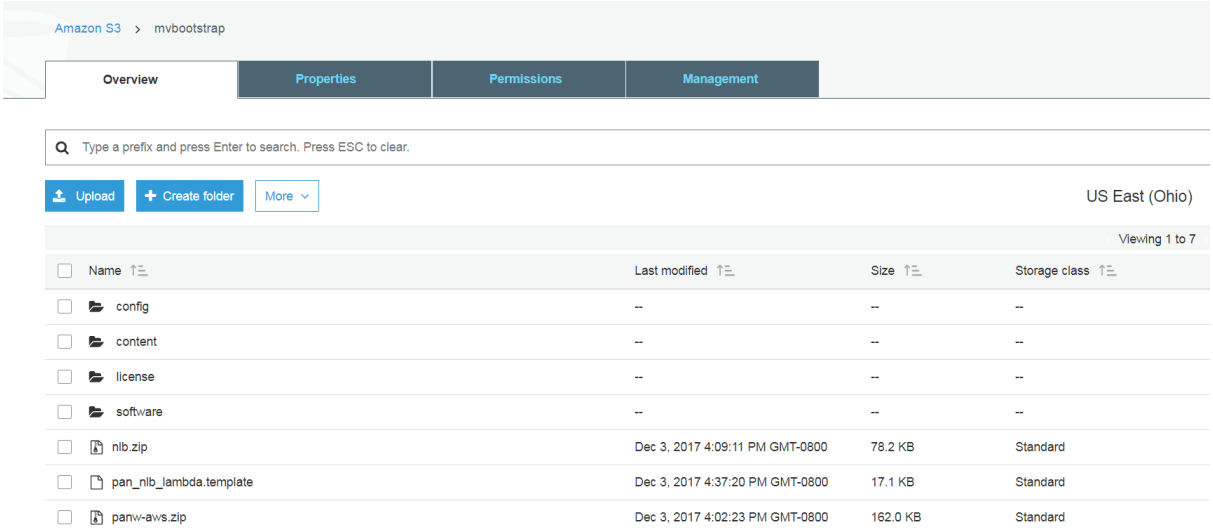
- For **Account ID**, type the AWS account ID of the account into which you are deploying the application template. Specifying that account ID allows you to grant access to the resources in your account that hosts the firewall template resources.
- Select **Require external ID** and enter a value that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



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

The application template is available at: https://github.com/PaloAltoNetworks/pan_nlb_v1.

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.



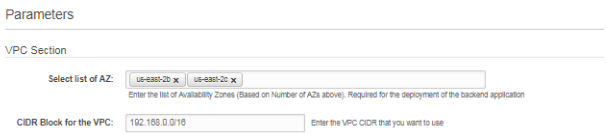
3. Copy the pan_nlb_lambda template into the same bucket to which you copied the nlb.zip file.

STEP 3 | Select the application template to launch.

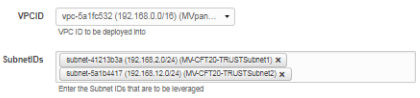
1. In the AWS Management Console, select **CloudFormation** > **Create Stack**.
2. Select **Upload a template to Amazon S3**, to choose the panw_aws_nlb-2.0.template to deploy the resources that the template launches within the same VPC as the firewalls, or the panw_aws_nlb_vpc-2.0.template to deploy 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 4 | 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.



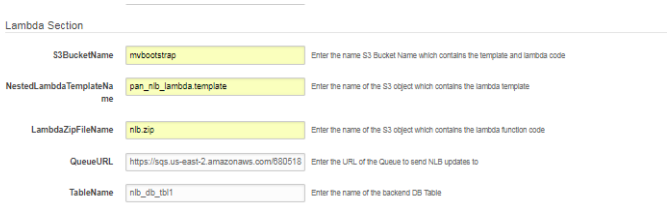
3. (Only if you are using the panw_aws_nlb-2.0.template to deploy the applications within the same VPC)



Select the **VPC ID** and the **Subnet IDs** associated with the trust subnet on the firewalls in each AZ. The network load balancer is attached to the trust subnet on the firewalls, to complete the load balancer sandwich topology.

4. Enter a name for the network load balancer.

STEP 5 | Configure the parameters for Lambda.



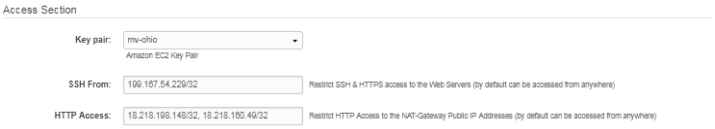
1. Enter the S3 bucket name where nlb.zip and the pan_nlb_lambda.template is stored.
2. Enter the name of the pan_nlb_lambda.template and the zip file name.
3. Paste the SQS URL that you copied earlier.
4. Enter a unique **TableName**. This table stores a mapping of the port and IP address for the applications associated with the network load balancer in your deployment.

   When you delete the application stack this table is deleted. Therefore, if multiple instances of the network load balancer write to the same table and the table is deleted, the NAT rules on the firewalls not function properly and the application traffic maybe be inaccurately forwarded to the wrong port/ network load balancer.

STEP 6 | Modify the web server EC2 instance type to meet your deployment needs.

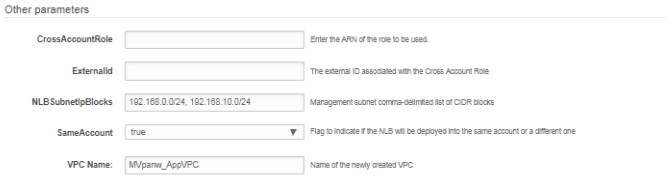
STEP 7 | Select the EC2 **Key pair** (from the drop-down) for launching the web servers. To log in to the web servers, you must provide the key pair name and the private key associated with it.

STEP 8 | (Only if you are using the panw_aws_nlb_vpc-2.0.template) Lock down access to the web servers.



1. Restrict **SSH From** access to the web servers. Only the IP addresses you list here can log in to the web servers.
2. Restrict HTTP access to the web servers. Enter the public IP addresses of the NAT gateway from the firewall template output; make sure add commas to separate IP addresses. Entering the NAT gateway IP address allows you to ensure that all web traffic to the application servers are secured by the VM-Series firewalls.

STEP 9 | (Only if you are using the panw_aws_nlb_vpc-2.0.template) Configure the other parameters requires to launch the application template stack in a different VPC.



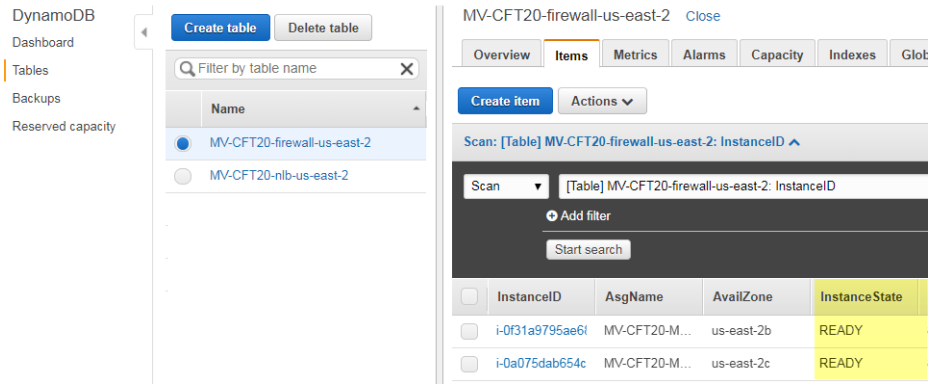
1. Select SameAccount **true** if you are deploying this application template within the same AWS account as the firewall template, and leave the cross account role and external ID blank; select **false** for a cross-account deployment.

   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.

2. Enter the **VPC Name**in which you want to deploy the application template resources.
3. Optional Change the **NLBSubnetIPBlocks** for the Management subnet for the network load balancer.

STEP 10 | Review the template settings and launch the template.

STEP 11 | Verify that the network load balancer is deployed and in a ready state.



STEP 12 | Get the **DNS name** for the application load balancer, and enter it into a web browser.

For example: http://MVpublic-elb-123456789.us-east-2.elb.amazonaws.com/

When the web page displays, you have successfully launched the auto scaling template.

STEP 13 | Verify that each firewall has a NAT policy rule to the IP address of each 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 has three NAT policy rules for ports 81, 82, and 83.

STEP 14 | 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.

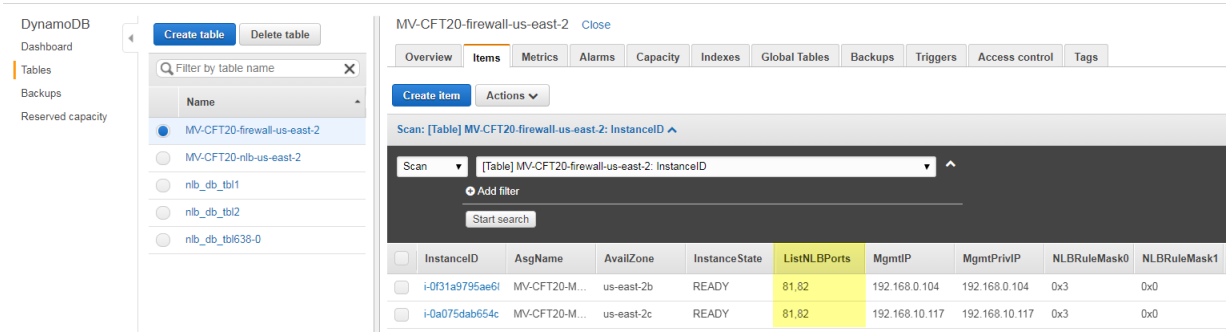
STEP 1 | On the AWS management console, verify the ports allocated for each network balancer on the DynamoDB table.

When you launch a new network load balancer, the application template must send an SQS message to the SQS URL you provided as input when you launched the template. The lambda function in the firewall template monitors the SQS and adds the port mapping to the DynamoDB table for the firewall template.

Starting at port 81, the port allocated for every additional network load balancer you deploy increments by 1. So, the second network load balancer uses port 82, and the third port uses port 83.

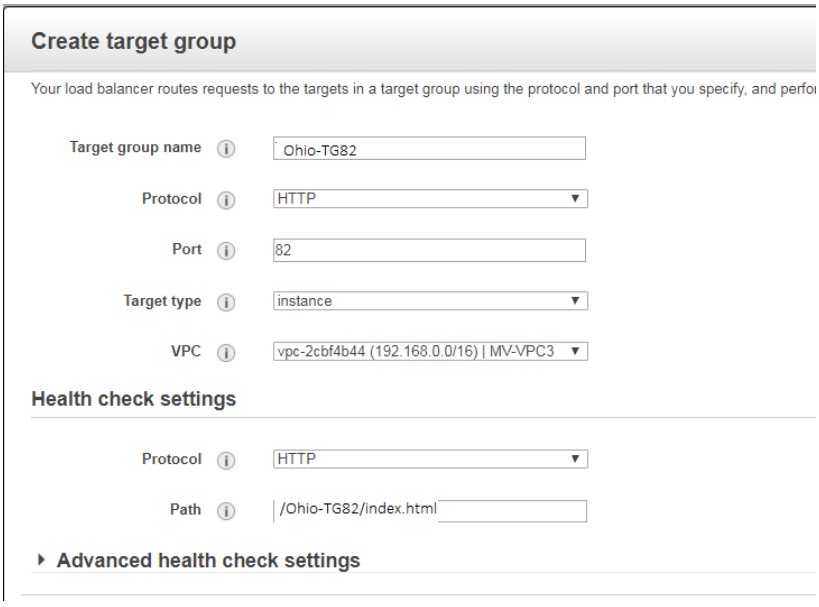
1. Select the **DynamoDB** service on the AWS management console.
2. Select **Tables** and click the table that matches the stack name for your firewall template. For example, MV-CFT20-firewall-us-east-2.

   In the Items list, view the ports used by the network load balancers that are publishing to the SQS associated with the firewall template.



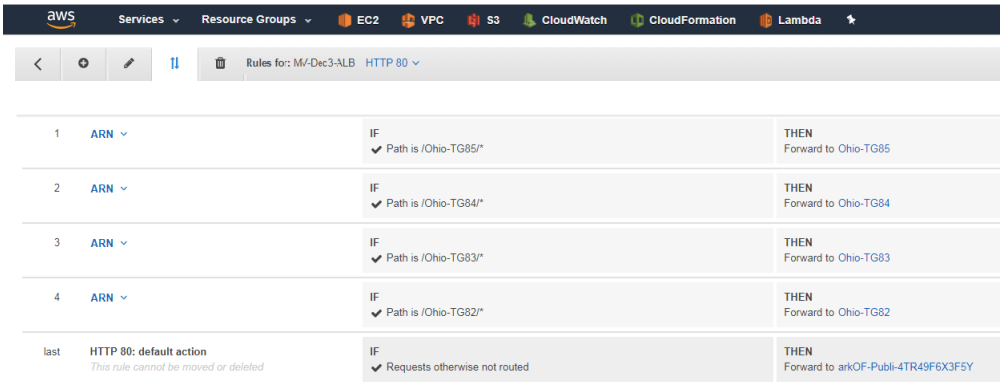
STEP 2 | Create a target group. The application load balancer sends requests to registered targets using the port and protocol that you specify for the servers in the target group.

When you add a new target group, use the port information that you verified on the DynamoDB table.



STEP 3 | 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:



STEP 4 | Attach the target group to both VM-Series firewalls auto scaling groups.

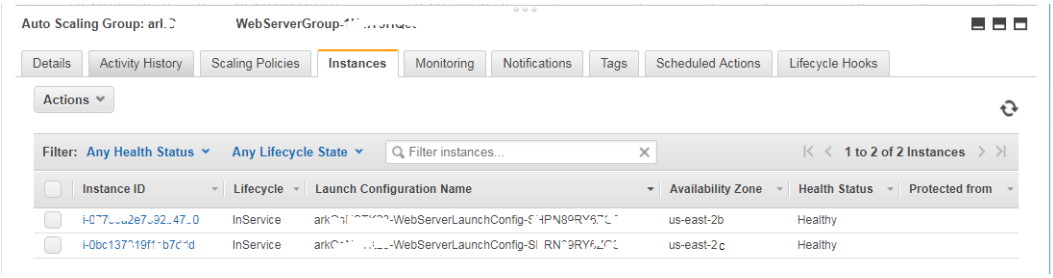
1. Select **Auto Scaling Groups** in the Auto Scaling section and select an auto scaling group that matches the stack name.
2. Select **Details** > **Edit**and select the new target group from the **Target Groups** drop-down.

STEP 5 | 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 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 6 | Verify 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.



Customize the Bootstrap.xml File (v2.0)

The bootstrap.xml file provided in the GitHub repository uses a default username and password for the firewall administrator. Before deploying the VM-Series Auto Scaling template in a production environment, at a minimum, you must create a unique username and password for the administrative account on the VM-Series firewall. Optionally, you can fully configure the firewall with zones, policy rules, security profiles and export a golden configuration snapshot. You can then use this configuration snapshot as the bootstrap.xml file for your production environment.

You have two ways to customize the bootstrap.xml file for use in a production environment:

- **Option 1**: Launch a VM-Series firewall on AWS using the bootstrap files provided in the GitHub repository, modify the firewall configuration and export the configuration to create a new bootstrap.xml file for the VM-Series Auto Scaling template. See Use the GitHub Bootstrap Files as Seed.
- **Option 2**: Launch a new VM-Series firewall on AWS without using the bootstrap files, add a NAT policy rule to ensure that the VM-Series firewall handles traffic properly, and export the configuration to create a new bootstrap.xml file for the VM-Series Auto Scaling template. See Create a new Bootstrap File from Scratch.

If you have deployed the template and now need to change the credentials for the administrative user or add a new admin user and update the template stack, see Modify Administrative Account and Update Stack.

Create a new Bootstrap File from Scratch

Launch a new VM-Series firewall on AWS using a PAN-OS 8.0 AMI in the AWS Marketplace (without using the sample bootstrap.xml file), and export the configuration to create a new bootstrap.xml file for use with the VM-Series Auto Scaling template v2.0.

STEP 1 | Deploy the VM-Series Firewall on AWS (no bootstrapping required) and use the public IP address to SSH into the Command Line Interface (CLI) of the VM-Series firewall. You will need to configure a new administrative password for the firewall.

STEP 2 | Log in to the firewall web interface.

STEP 3 | (Optional) Configure the firewall. You can configure the dataplane interfaces, zones and policy rules.

STEP 4 | **Commit** the changes on the firewall.

STEP 5 | Export the configuration file and name it as **`bootstrap.xml`**. (**Device** > **Setup** > **Operation** > **Export Named Configuration Snapshot**).

STEP 6 | Download the bootstrap.xml file from the GitHub repository, open it with a text editing tool, and copy lines 353 to 356. These lines define the AWS CloudWatch namespace to which the firewall publishes custom PAN-OS metrics that are required for the firewalls to auto scale.

STEP 7 | Edit the configuration file you exported earlier to include the AWS CloudWatch information.

Search for `</management>` and paste the lines 353 to 356 after `</management>`.

```
352          </management>
353          <aws-cloudwatch>
354            <enabled>yes</enabled>
355            <name>autoscale-default-panw-asg-name</name>
356          </aws-cloudwatch>
357        </setting>
```

STEP 8 | Delete the management interface configuration.

1. Search for `</service>` and delete the ip-address, netmask and default gateway that follow.
2. Search for `</type>` and delete the ip-address, netmask, default gateway, and public-key that follow.

```
326          </service>
327          <ip-address>192.168.10.16</ip-address>
328          <netmask>255.255.255.0</netmask>
329          <default-gateway>192.168.10.1</default-gateway>
330          <hostname>PA-VM</hostname>
331        </system>
332        <setting>
333          <config>
334            <rematch>yes</rematch>
335          </config>
336          <management>
337            <hostname-type-in-syslog>FQDN</hostname-type-in-syslog>
338            <initcfg>
339              <type>
340                <dhcp-client>
341                  <send-hostname>yes</send-hostname>
342                  <send-client-id>no</send-client-id>
343                  <accept-dhcp-hostname>no</accept-dhcp-hostname>
344                  <accept-dhcp-domain>no</accept-dhcp-domain>
345                </dhcp-client>
346              </type>
347              <ip-address>192.168.10.16</ip-address>
348              <netmask>255.255.255.0</netmask>
349              <default-gateway>192.168.10.1</default-gateway>
350              <public-key>c3NoLXJzYSBBQUFBQjNOemFDMXljMkVBQUFBREFRQUJBQUFCQVFDQTRCSjJwZFBSZlh0TjF2SDVqWW5GRUdYTVdvTmZlaU1FcCtBSlZRaVU4c2hEMHBmSUtOVTVSeHdGRFd4OVZZckRRRFVrLzQ
VEeHB2WXk3ZWtiam1IallYdTVXUFR4MnZSaXdiMmVzcS91K3FXbm9hSlQ1cXdjU2srbHRxN0prVjlGcC9HSy9jQkRDT0FqOVhmSHMvWi8xQ0VZRk9uZ0UrNTd5L2VwSjFFWWtxZXllLczZuRTBvbWxRajBHSmNhb
351            </initcfg>
352          </management>
```

STEP 9 | Save the file. You can now proceed with Launch the VM-Series Auto Scaling Template for AWS (v2.0).

Use the GitHub Bootstrap Files as Seed

Launch a VM-Series firewall on AWS from the AWS Marketplace using the bootstrap files provided in the GitHub repository, modify the firewall configuration for your production environment. Then, export the configuration to create a new bootstrap.xml file that you can now use for the VM-Series Auto Scaling template.

STEP 1 | To launch the firewall see Bootstrap the VM-Series Firewall on AWS.

STEP 2 | Add an elastic network interface (ENI) and associate an elastic IP address (EIP) to it, so that you can access the web interface on the VM-Series firewall. See Launch the VM-Series Firewall on AWS for details.

STEP 3 | Use the EIP address to log in to the firewall web interface with admin as the username and password.

STEP 4 | Add a secure password for the admin user account (**Device** > **Local User Database** > **Users**).

STEP 5 | (Optional) Configure the firewall for securing your production environment.

STEP 6 | **Commit** the changes on the firewall.

STEP 7 | Generate a new API key for the administrator account. Copy this new key to a new file. You will need to enter this API key when you launch the VM-Series Auto Scaling template; the AWS services use the API key to deploy the firewall and to publish metrics for auto scaling.

STEP 8 | Export the configuration file and save it as **`bootstrap.xml`**. (**Device** > **Setup** > **Operation** > **Export Named Configuration Snapshot**).

STEP 9 | Open the bootstrap.xml file with a text editing tool and delete the management interface configuration.

STEP 10 | (Required if you exported a PAN-OS 8.0 configuration) Ensure that the setting to validate the Palo Alto Networks servers is disabled. Look for **`<server-verification>no</server-verification>`**.

STEP 11 | If the check is **yes**, change it to **no**.

STEP 12 | Save the file. You can now proceed with Launch the VM-Series Auto Scaling Template for AWS (v2.0).

SQS Messaging Between the Application Template and Firewall Template

So that the VM-Series firewalls deployed using the firewall-v2.0.template can detect and send traffic to the network load balancers to which you want to automatically distribute incoming traffic, the firewall template includes a lambda function that monitors a Simple Queue Service for messages. The message allows the lambda function to learn about a new network load balancer and then automatically create a NAT policy rule on the firewall to send traffic to the IP address of the network load balancer. In order to route traffic properly within the AWS infrastructure, the message must also include basic information on the DNS, VPC ID, and the AZ to which the network load balancer belongs.

If you are building your own application template, you must set up your application template to post two types of messages to the SQS URL that the firewall template in the VM-Series autoscaling template version 2.0 uses to learn about network load balancers to which it must distribute traffic in your environment:

- ADD-NLB message that informs the firewalls when a new network load balancer is available.
- DEL-NLB message that informs the firewalls when a network load balancer has been terminated and is no longer available.

The following examples of each message type includes sample values. You need to modify these message with values that match your deployment.

ADD-NLB Message

```
msg_add_nlb= { 'MSG-TYPE': 'ADD-NLB', 'AVAIL-ZONES': [{'NLB-
IP':'192.168.2.101', 'ZONE-NAME':'us-east-2a', 'SUBNET-ID':
 'subnet-2a566243'}, {'NLB-IP':'192.168.12.101', 'ZONE-NAME':'us-east-2b',
 'SUBNET-ID': 'subnet-2a566243 '}], 'DNS-NAME': 'publicelb1-2119989486.us-
east-2.elb.amazonaws.com', 'VPC-ID': 'vpc-42ba9f2b', 'NLB-NAME':
 'publicelb1' }
```

DEL-NLB Message

```
msg_del_nlb= { 'MSG-TYPE': 'DEL-NLB', 'DNS-NAME': 'publicelb1-2119989486.us-
east-2.elb.amazonaws.com', }
```

Refer to the AWS documentation for details on how to send a message to an Amazon SQS Queue, or review the **describe_nlb_dns.py** in the sample application template package to see how the application template constructs the messages.

Stack Update with VM-Series Auto Scaling Template for AWS (v2.0)

A stack update allows you to modify the resources that the VM-Series Auto Scaling template—firewall-v2.0.template—deploys. Instead of deleting your existing deployment and redeploying the solution, use the stack update to modify the following parameters:

- License—Switch from BYOL to PAYG and vice versa or switch from one PAYG bundle to another.
- Other stack resources— Change the launch configuration parameters such as the Amazon Machine Image (AMI) ID, the AWS instance type, key pair for your auto scaling groups. You can also update the API key associated with the administrative user account on the firewall.

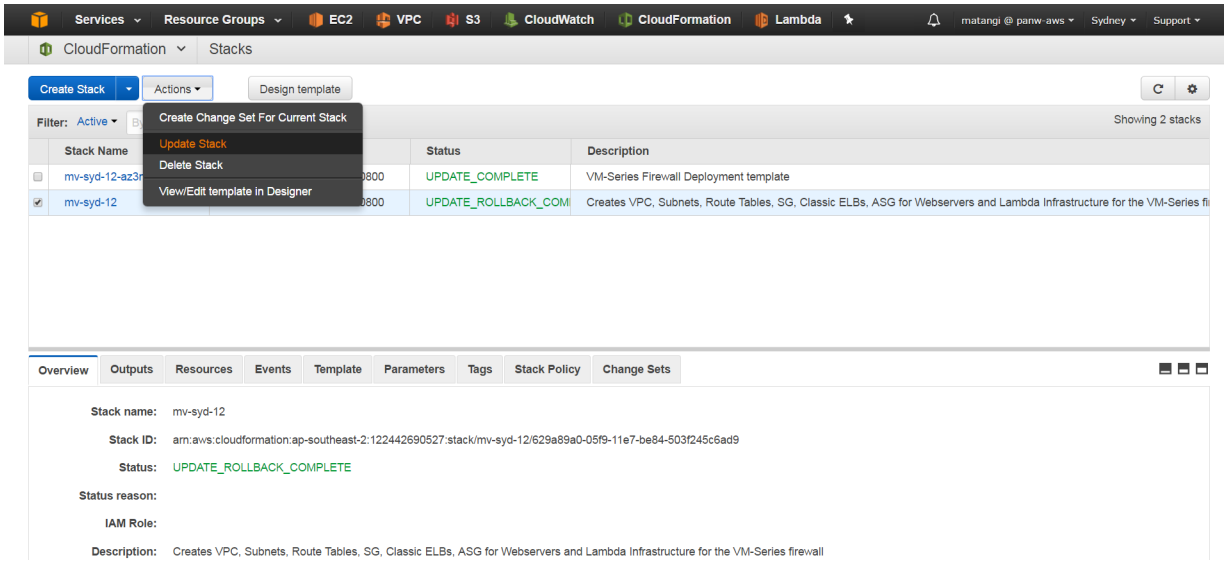
Changing the AMI-ID allows you to deploy new instances of the VM-Series firewalls with a different PAN-OS version.

When you deploy the VM-Series Auto Scaling template, the auto scaling groups and the launch configuration are automatically created for you. The launch configuration is a template that an auto scaling group uses to launch EC2 instance, and it specifies parameters such as the AMI ID, the instance type, key pair for your auto scaling group. To launch VM-Series firewalls with your updated parameters, you must first update the stack and then delete the existing auto scaling groups in each AZ. To prevent service disruption, delete the auto scaling group in one AZ first, and wait for the new firewall instances to launch with the updated stack parameters. Then, verify that the firewalls have inherited the updates you made before you proceed to complete the changes in the other AZ.

For critical applications, perform a stack update during a maintenance window.

You can update stack directly or create change sets. The workflow in this document takes you through the manual stack update.

STEP 1 | In the AWS CloudFormation console, select the parent stack that you want to update and choose **Actions** > **Update Stack**.



STEP 2 | Modify the resources that you want to update.

- PAN-OS version—To modify the PAN-OS version look up the AMI ID for the version you want to use and enter the ID.
- License option—Switch from BYOL to PAYG or across PAYG bundles 1 and 2.

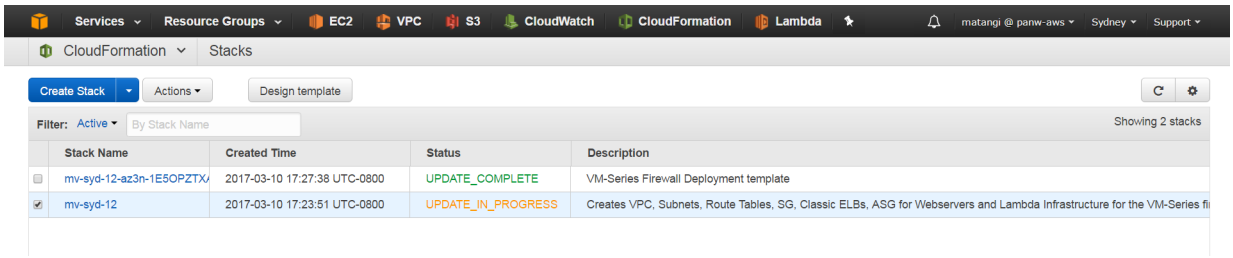
If you're switching to BYOL, make sure to include the auth code in the bootstrap package (See steps 3 and 5).

If you're switching between PAYG bundle version 1 and 2, look up the AMI ID for the VM-Series firewall.

- Other stack resources— You can modify the AMI ID, the instance type, security group, key pair for the stack resources, or the API key associated with the administrative user account on the firewall.

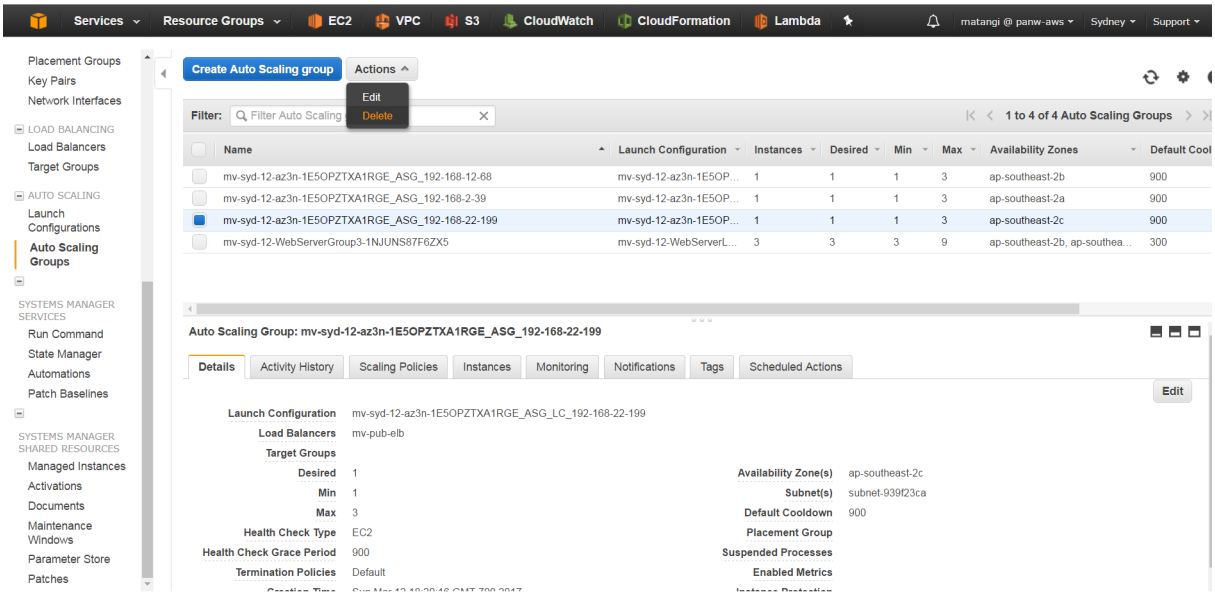
If you create a new administrative user account or modify the credentials of the existing administrator on the firewall, in order to update that stack and deploy new firewalls with the updated API key, you need to follow the workflow in Modify Administrative Account and Update Stack.

STEP 3 | Acknowledge the notifications and review the changes and click **Update** to initiate the stack update.



STEP 4 | On the **EC2 dashboard** > **Auto Scaling Groups** and pick an AZ in which to delete the ASG.

Deleting an ASG automatically triggers the process of redeploying a new ASG. The firewalls in the new ASG use the updated stack configuration.



STEP 5 | Verify that the updated parameters are used to launch the VM-Series firewalls in the new ASG.

Use a phased rollout process, where you test the new ASG thoroughly and ensure that the firealls are properly handling traffic. Then, wait one hour before continuing to the next ASG.

STEP 6 | Repeat steps 4 and 5 to replace the ASG in the other AZ.

Modify Administrative Account and Update Stack

If you have already deployed the template and now want to change the password for the administrative account or create a new administrative user account on the VM-Series firewall, you must generate a new API key and update the template stack with the new API key for the administrative user account. And in order to ensure that new firewall instances are configured with the updated administrative user account, you need to export the firewall configuration and rename it to bootstrap.xml, then upload it to the S3 bootstrap folder that the VM-Series AutoScaling template uses.

STEP 1 | Log in to the web interface of the firewall and change the credentials for an existing administrative user or create a new account.

STEP 2 | Generate the API key.

STEP 3 | Export the current running configuration and rename it to bootstrap.xml.

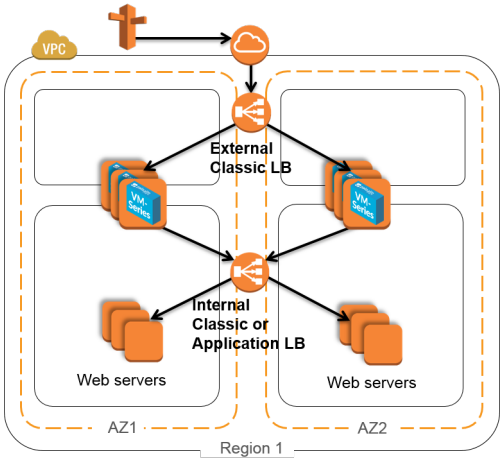
STEP 4 | Upload this bootstrap.xml file to the S3 bootstrap folder (see Customize the Bootstrap.xml File).

STEP 5 | Update the API key in the stack to ensure that newly launched firewalls will have the updated administrator account.

See Stack Update with VM-Series Auto Scaling Template for AWS (v2.0)or Stack Update with VM-Series Auto Scaling Template for AWS (v1.2) for details.

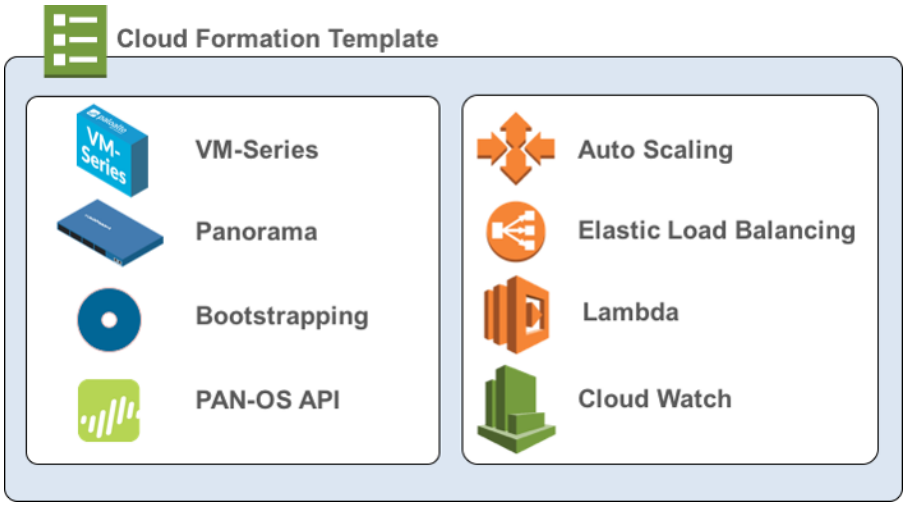
Auto Scale Template Version 1.2 (and earlier)

The auto scaling template version 1.2 deploys the VM-Series in an ELB sandwich topology with an internet-facing classic ELB and an either an internal classic load balancer or an internal application load balancer (internal ELB). The internet-facing ELB is accessible from the internet and distributes traffic that enters the VPC across a pool of VM-Series firewalls. The firewalls then redirect traffic using NAT policy to the internal ELB. The internal ELB, which is only accessible inside the VPC, distributes traffic to an auto scaling tier of web servers. The API integration with AWS CloudWatch allows the CloudWatch service to monitor the health and resource load on the EC2 instances—VM-Series firewalls and web servers—and then use that information to trigger a scale in or scale out event in the respective Auto Scaling Group (ASG).



- What Components Does the VM-Series Auto Scaling Template for AWS Deploy (Version 1.2 and earlier)?
- How Does the VM-Series Auto Scaling Template for AWS Enable Dynamic Scaling?
- Plan the VM-Series Auto Scaling Template for AWS
- Launch the VM-Series Auto Scaling Template for AWS
- Customize the Bootstrap.xml File
- NAT Policy Rule and Address Objects in the Auto Scaling Template
- Stack Update with VM-Series Auto Scaling Template for AWS (v1.2)
- Modify Administrative Account and Update Stack
- Troubleshoot the VM-Series Auto Scaling Template for AWS

What Components Does the VM-Series Auto Scaling Template for AWS Deploy (Version 1.2 and earlier)?



The VM-Series Auto Scaling template for AWS versions 1.2 and earlier provide two deployment options. The first option offers the flexibility to deploy a complete AWS environment along with the auto scaling tier of VM-Series firewalls in one streamlined workflow. The second option allows you to deploy only the auto-scaling tier of VM-Series firewalls into your existing AWS deployment.

The VM-Series Auto Scaling template for AWS does not deploy Panorama, and Panorama is optional in this solution.

If you want to use Panorama to manage the VM-Series firewalls that the solution deploys, you can either use an M-Series appliance inside your corporate network, or a Panorama virtual appliance on a VMware ESXi server inside your corporate network or in vCloud Air; you cannot deploy Panorama on AWS.

The VM-Series Auto Scaling template for AWS includes the following building blocks that make these options possible:

Building Block	Description
VPC template	The VPC templates automate the process of deploying a VPC with two or three Availability Zones (AZs). It deploys an external ELB, a web server farm and an internal ELB that load balances traffic to the web server farm. In addition to the subnets, route tables, and security groups required for routing traffic across these AZs, it also creates the Auto Scaling Group (ASG) for the web server farm and an AWS NAT gateway, if you opt for one. Depending on your preference for the internal ELB, you can choose from these two templates: • *vpc-classic-v.<number>template*—Use this template if you want to use a classic ELB for load balancing traffic to the internal web server farm. • *vpc-alb-v.<number>.template*— Use this template, if you prefer an application ELB for load balancing traffic to the internal web server farm. Both templates, deploy the classic ELB for internet-facing traffic.
Firewall template	The VPC template invokes the *firewall.template* to launch the VM-Series firewall.

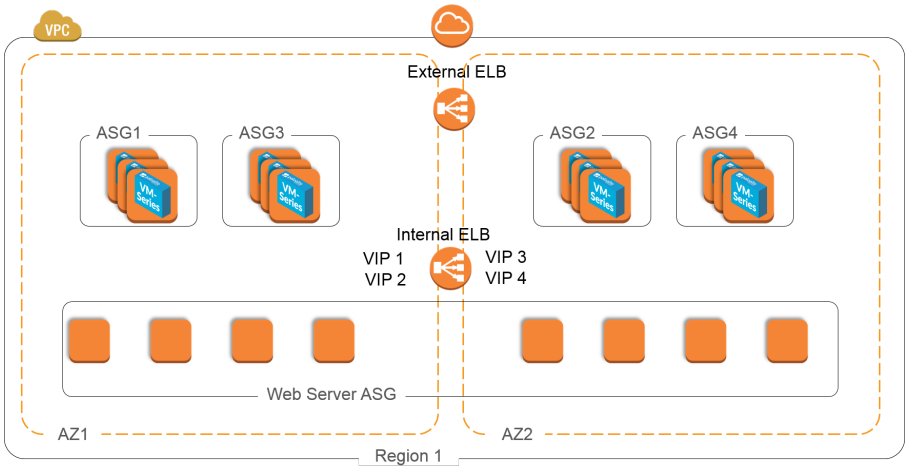
Building Block	Description
	If you have an existing VPC with the required subnets, security groups, web servers, and ELBs, and want to only deploy the VM-Series firewall at scale, you can use the firewall.template instead of the vpc.template. The firewall.template creates an initial ASG with a single VM-Series firewall to secure the web servers in each AZ, adds the ENIs for the trust and management interfaces, and triggers the bootstrap process including registration with Panorama. To enable auto scaling of the VM-Series firewalls, this template leverages PAN-OS metrics from the VM-Series firewall and publishes data on your preferred metric to AWS CloudWatch. You can select one of the following PAN-OS metrics—active sessions, dataplane CPU utilization, or dataplane CPU buffer utilization.
Lambda functions	AWS Lambda provides robust, event-driven automation without the need for complex orchestration software. In this template, AWS Lambda monitors the custom PAN-OS metrics and the internal ELB to enable dynamic scaling of the VM-Series firewalls. The Lambda functions add or remove elastic network interfaces (ENIs) when the firewall is launched or terminated, collect and publish CloudWatch metrics so that you can define auto scaling policy using CloudWatch alarms, delete all the associated resources when an instance is terminated or the stack is deleted, and remove the firewall as a managed device on Panorama. The Lambda functions also monitor the VIP addresses on the internal ELB so that it can add or remove an ASG for the VM-Series firewall so that it can ensure a 1:1 ratio between the internal ELB VIP and the VM-Series firewalls ASG.
Bootstrap files The bootstrap.xml file provided in the GitHub repository is provided for testing and evaluation only. For a production deployment, you must modify the bootstrap.xml prior to launch. See Customize the Bootstrap.xml File.	This solution requires the init-cfg.txt file and the bootstrap.xml file so that the VM-Series firewall has the basic configuration for handling traffic from the ELB. • The init-cfg.txt file includes the mgmt-interface-swap operational command to enable the firewall to receive dataplane traffic on its primary interface (eth0). For details see Management Interface Mapping for Use with Amazon ELB. • The bootstrap.xml file contains a NAT policy rule to properly route traffic in this auto scaling ELB environment. In order to perform NAT, the firewall requires a single IP address in the NAT policy rule, the firewall cannot use an FQDN or round-robin NAT to multiple IP addresses. But to enable auto scaling, the AWS ELB publishes an FQDN as a virtual IP address (VIP) rather that publishing an IP address. And as the internal ELB scales, the FQDN automatically resolves to multiple IP addresses (per AZ). The NAT policy rule included in the bootstrap. xml file resolved this conflict. The bootstrap.xml file references an address object within the NAT policy rule. When the firewall boots up, a Lambda function adds the IP address of the internal ELB in to the address object so that the NAT policy resolves to the correct IP address for the internal ELB, and can route traffic to and from the external ELB and the internal ELB in this solution.

To deploy the solution, see Launch the VM-Series Auto Scaling Template for AWS.

How Does the VM-Series Auto Scaling Template for AWS Enable Dynamic Scaling (v 1.2)?

The VM-Series firewalls scale in and scale out based on PAN-OS metrics and on application traffic.

- **PAN-OS metric-based scaling**—The VM-Series firewalls scale based on custom PAN-OS metrics that trigger alarms and policies to dynamically deploy or terminate instances to increase or decrease capacity in the VM-Series firewall ASG. To monitor traffic load on the VM-Series firewalls, you can configure alarms based on the following custom PAN-OS metrics—the number of active sessions on the firewall, dataplane CPU utilization, or dataplane buffer utilization. The VM-Series Auto Scaling template for AWS uses an AWS Lambda function to publish the metrics to AWS CloudWatch at a one-minute frequency. When a metric that is being monitored reaches a configured threshold for the defined time interval, CloudWatch triggers an alarm and initiates an auto-scaling event.
- **Application traffic-based scaling**—The VM-Series firewalls scale based on the internal ELB, which scales in response to the demands of the application traffic in the web server ASG. There is a 1:1 ratio between the number of internal ELB Virtual IP addresses and the number of ASGs for the VM-Series firewalls. So, when the Lambda function in the VM-Series Auto Scaling template for AWS detects the addition or the deletion of an internal ELB VIP address, an ASG for the VM-Series firewall is added or deleted in response to the change. And the IP address of the firewall is added or removed from the external ELB pool so that the external ELB can distribute traffic across all the available firewalls in the ASG.



The VM-Series firewalls within an ASG are identical in configuration. Each firewall is bootstrapped and configured with a NAT policy rule that directs all traffic to the IP address of the internal ELB.

Similarly, when traffic volume is reduced and an internal ELB VIP address is deleted, the Lambda function deletes the ASG and the VM-Series firewalls associated with the ASG. The IP address of the firewall is also removed from the external ELB pool.

Plan the VM-Series Auto Scaling Template for AWS (Version 1.2)

The GitHub repository provides VM-Series Auto Scaling template version 1.1 and version 1.2. Version 1.2 is the latest and it provides the mechanism to update the PAN-OS version of the auto scaling tier of VM-Series firewalls and other resources using the stack update capability for AWS CloudFormation templates. To accommodate your business needs, it also allows you to choose and switch across three licensing options, BYOL, PAYG bundle 1 and PAYG bundle 2.

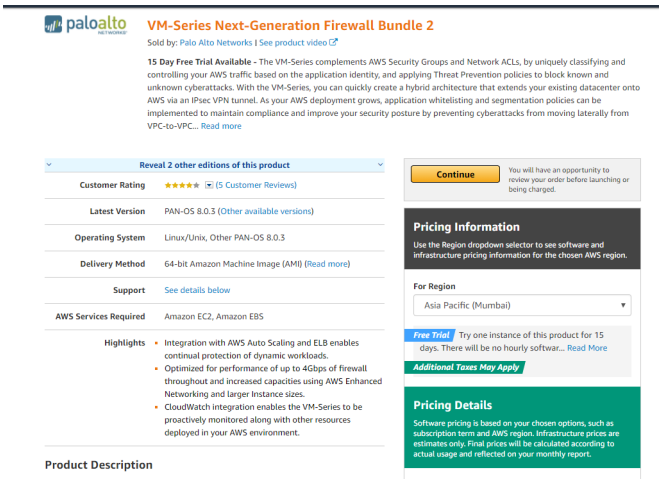
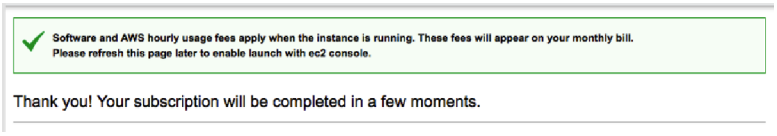
VM-Series Auto Scaling template version 1.1 provides support for PAYG bundle 2 only.

In order to launch the solution successfully, review this checklist before you begin.

- VM-Series Auto Scaling Template for AWS Version 1.2
- VM-Series Auto Scaling Template for AWS Version 1.1

VM-Series Auto Scaling Template for AWS Version 1.2

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

Planning Checklist for Version 1.2	
Verify the requirements for deploying the VM-Series Auto Scaling template.	The solution requires AWS Lambda and Signature versions 2 or 4 for PAN-OS 8.0; PAN-OS 7.1 requires signature version 2. Look up the list of supported regions and the AMI IDs.
Assign the appropriate permissions for the IAM user role.	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 file to successfully launch this solution. 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.
Create a Support Account on the Palo Alto Networks Support portal.	With VM-Series Auto Scaling template version 1.2, you can opt for the BYOL or PAYG (bundle 1 or bundle 2) licenses. For BYOL, you must register the auth code to your Palo Alto Networks support account prior to launching the VM-Series Auto Scaling template. For PAYG, you must register the VM-Series firewalls to activate your support entitlement.
(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.	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**.  • Click **Continue**, and select **Manual Launch**. Review the agreement and click **Accept Software Terms** to accept the EULA.  You can now close the browser.

Planning Checklist for Version 1.2	

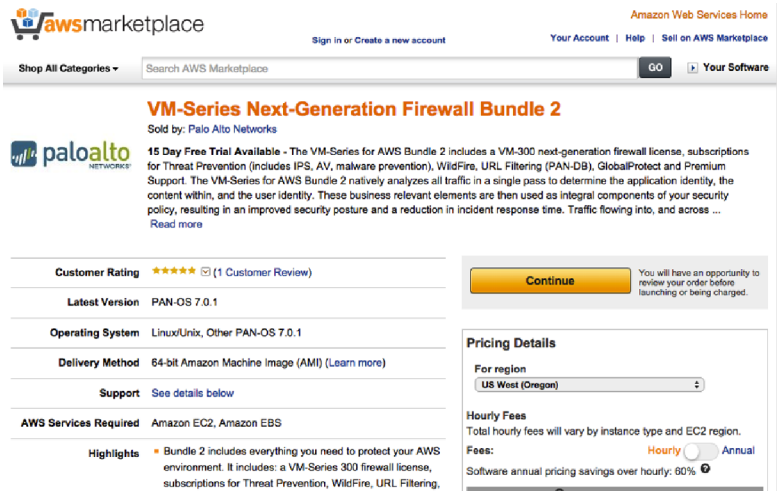
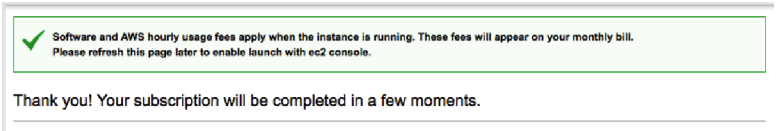
Download the Templates, AWS Lambda code, and the bootstrap files.
 	
Do not mix and match files across VM-Series Auto Scaling template versions.
	Get the files from the following GitHub repository at: https://github.com/PaloAltoNetworks/aws-elb-autoscaling/tree/master/Version-1.2
	• Templates and Lambda code:
	  • panw-aws.zip
	  • firewall.template
	  • vpc-classic-v1.2.template or vpc-alb-v1.2.template. (you need only one)
	  The vpc-classic-v1.2.template includes support for two classic ELBs; the vpc-alb-v1.2.template includes support for a classic ELB and an internal application ELB.
	  Use the vpc-alb.template if you want to deploy an application ELB for load balancing traffic to the internal web servers and a classic ELB for internet-facing traffic.
	  Use the vpc-classic.template if you want to deploy two classic ELBs; one for load balancing traffic to the internal web servers and another for internet-facing traffic.
	  The solution is supported by Palo Alto Networks Technical Support as it is published. You may modify the template to suit your specific use case but Palo Alto Networks Technical Support cannot assist with issues that arise from customization.
	• Bootstrap files:
	  • init-cfg.txt
	  • bootstrap.xml
	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. See Customize the Bootstrap.xml File.

Customize the bootstrap.xml file for your production environment.	To ensure that your production environment is secure, you must Customize the Bootstrap.xml File with a unique administrative username and password. 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.
Decide whether you want to use Panorama for centralized logging, reporting, and firewall management.	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. If you want to use Panorama, you can either use the M-Series appliance or a Panorama virtual appliance on a VMware ESXi server inside your corporate network, or use a Panorama virtual appliance on vCloud Air. To successfully register the firewalls with Panorama, you must collect the following details: • 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, you

Planning Checklist for Version 1.2	
	should 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 that allows Panorama to authenticate the firewalls in order to add each firewall as a managed device. You must include this key in the configuration (init-cfg.txt) file. 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. • 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.
Decide whether you want to use the AWS NAT gateway or assign an EIP address to the management interface on each VM-Series firewall.	To allow the firewalls to initiate outbound requests for retrieving updates, connecting to Panorama, and publishing metrics to AWS CloudWatch, you can either deploy an AWS NAT gateway or assign an EIP address to the management interface on each firewall. The AWS NAT gateway option allows you to conserve the use of EIP addresses; you only need one EIP address per Availability Zone (AZ). Hence, you must allocate a maximum of three EIP addresses if you deploy the VM-Series Auto Scaling template across three AZs. When you use a NAT gateway and are not using Panorama to manage the firewalls, you must deploy a jump server (a bastion host with an EIP address) 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. If you choose to assign an EIP address to the management interface of each VM-Series firewall, you must estimate the number of EIP addresses you need to enable outbound access for the VM-Series firewalls. Based on the size of your deployment, you may need to request an increase in the maximum number of EIP addresses for the AWS region; the default limit is 5 EIP addresses per account. This estimation is crucial to the deployment because AWS Lambda requires the EIP address to successfully launch the firewall.
Get started.	Launch the VM-Series Auto Scaling Template for AWS (v1.2) Stack Update with VM-Series Auto Scaling Template for AWS (v1.2)

VM-Series Auto Scaling Template for AWS Version 1.1

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

Planning Checklist for Version 1.1	
Verify the requirements for deploying the VM-Series Auto Scaling template version 1.1.	The solution requires AWS Lambda and Signature version 2, and is supported in the following regions: US East (N. Virginia), US West (Oregon), EU (Ireland), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney). The VM-Series firewalls deployed using version 1.1 have PAN-OS 7.1.
Assign the appropriate permissions for the IAM user role.	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 file to successfully launch the solution. 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.
Create a Support Account on the Palo Alto Networks Support portal.	All the VM-Series firewalls deployed by VM-Series Auto Scaling template version 1.1 support the usage-based (PAYG bundle 2) licenses. Version 1.1 does not support the BYOL option. You must register the VM-Series firewalls to activate your support entitlement.
Review and accept the End User License Agreement (EULA). Required, if you are launching a VM-Series firewall on AWS for the first time. The VM-Series Auto Scaling template will fail to deploy if you have not accepted the EULA.	• In the AWS Marketplace, search for Palo Alto Networks, and select **VM-Series Next Generation Firewall Bundle 2**.  • Click **Continue**, and select **Manual Launch**. Review the agreement and click **Accept Software Terms** to accept the EULA.  You can now close the browser.

Download the Templates, AWS Lambda code, and the bootstrap files.	Get the files from the following GitHub repository at: https://github.com/PaloAltoNetworks/aws-elb-autoscaling/tree/master/Version-1.1
	• Templates and Lambda code:
	  • panw-aws.zip
	  • firewall.template

Planning Checklist for Version 1.1	

	• vpc-classic-v1.1.template or vpc-alb-v1.1.template. (you need only one)
	
	The vpc-classic-v1.1.template includes support for two classic ELBs; the vpc-alb-v1.1.template includes support for a classic ELB and an internal application ELB.
	
	Use the vpc-alb.template if you want to deploy an application ELB for load balancing traffic to the internal web servers and a classic ELB for internet-facing traffic.
	
	Use the vpc-classic.template if you want to deploy two classic ELBs; one for load balancing traffic to the internal web servers and another for internet-facing traffic.
	
	The solution is supported by Palo Alto Networks Technical Support as it is published. You may modify the template to suit your specific use case but Palo Alto Networks Technical Support cannot assist with issues that arise from customization.
	• Bootstrap files:
	  • init-cfg.txt
	  • bootstrap.xml
	
	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. See Customize the Bootstrap.xml File.

Customize the bootstrap.xml file for your production environment.	To ensure that your production environment is secure, you must Customize the Bootstrap.xml File with a unique administrative username and password. 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.
Decide whether you want to use Panorama for centralized logging, reporting, and firewall management.	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. If you want to use Panorama, you can either use the M-Series appliance or a Panorama virtual appliance on a VMware ESXi server inside your corporate network, or use a Panorama virtual appliance on vCloud Air. And, if you use Panorama, you need the following information so that the firewalls can register with Panorama: • API key for an administrative user account on Panorama. AWS Lambda uses this key to make API requests to Panorama. By default, the VM-Series Auto Scaling template uses an API key with username and password, admin/admin. For better security, create an administrative account on Panorama and generate a new API key for the account. You must enter this key when you launch the VM-Series Auto Scaling template. • 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.

Planning Checklist for Version 1.1	
	• VM auth key that allows Panorama to authenticate the firewalls in order to add each firewall as a managed device. You must include this key in the configuration (init-cfg.txt) file. 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. • 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.
Decide whether you want to use the AWS NAT gateway or assign an EIP address to the management interface on each VM-Series firewall.	To allow the firewalls to initiate outbound requests for retrieving updates, connecting to Panorama, and publishing metrics to AWS CloudWatch, you can either deploy an AWS NAT gateway or assign an EIP address to the management interface on each firewall. The AWS NAT gateway option allows you to conserve the use of EIP addresses; you only need one EIP address per Availability Zone (AZ). Hence, you must allocate a maximum of three EIP addresses if you deploy the VM-Series Auto Scaling template across three AZs. When you use a NAT gateway and are not using Panorama to manage the firewalls, you must deploy a jump server (a bastion host with an EIP address) 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. If you choose to assign an EIP address to the management interface of each VM-Series firewall, you must estimate the number of EIP addresses you need to enable outbound access for the VM-Series firewalls. Based on the size of your deployment, you may need to request an increase in the maximum number of EIP addresses for the AWS region; the default limit is 5 EIP addresses per account. This estimation is crucial to the deployment because AWS Lambda requires the EIP address to successfully launch the firewall.
Get started.	Launch the VM-Series Auto Scaling Template for AWS (v1.1).

Launch the VM-Series Auto Scaling Template for AWS (v1.2 and earlier)

Pick the workflow for the VM-Series Auto Scaling template version you are deploying.

- Launch the VM-Series Auto Scaling Template for AWS (v1.2)
- Launch the VM-Series Auto Scaling Template for AWS (v1.1)

If you have deployed the template v1.2 and want to update resources see Stack Update with VM-Series Auto Scaling Template for AWS (v1.2).

Launch the VM-Series Auto Scaling Template for AWS (v1.2)

Use the following workflow to deploy all the components in this solution using the vpc-classic-v1.2.template or the vpc-alb-v1.2.template.

If you have an existing VPC with the required subnets, security groups, web servers, and ELBs, you only need to deploy the VM-Series firewall at scale, use the firewall.template. The workflow for using only the firewall.tempate is not documented in this version of the document, but it is very similar.

STEP 1 | Plan the VM-Series Auto Scaling Template for AWS.

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 authcode in the /license folder of the bootstrap package. For details, see Prepare 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 information on the bootstrapping process see Bootstrap the VM-Series Firewall; for details on the init-cfg.txt file, see Create 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 and the device group to which you want to assign the firewall. Enter:

     `tplname=`

     `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 on the bootstrapping process 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.

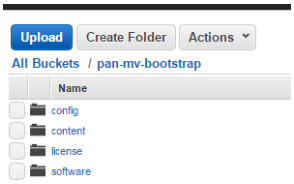
The bootstrap.xml file provided in the GitHub repository is provided for testing and evaluation only. For a production deployment, you must modify the bootstrap.xml prior to launch, see Customize the Bootstrap.xml File.

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

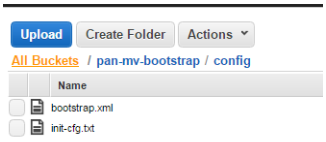
Make sure to create the S3 buckets in the same region in which you plan to deploy the template.

The VM-Series Auto Scaling template requires one S3 bucket for the VM-Series bootstrap files; and another S3 bucket for the AWS Lambda functions and the nested `firewall.template`.

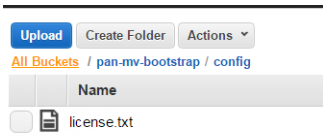
1. Create a new S3 bucket for the bootstrap files.
    1. Sign in to the AWS Management Console and open the S3 console.
    2. Click **Create Bucket**.
    3. Enter a **Bucket Name** and a **Region**, and click **Create**. The bucket must be at the S3 root level. If you nest the bucket, bootstrapping 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.



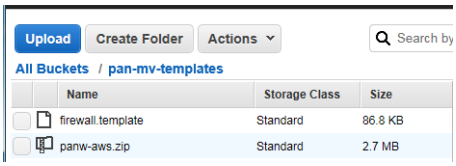
    3. Click the link to open the **config** folder.
    4. Select **Actions** > **Upload** and **Add Files**, browse to select the init-cfg.txt file and bootstrap.xml file, and click **Open**.
    5. Click **Start Upload** to add the files to the config folder. The folder can contain only two files: init-cfg.txt 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. Create another S3 bucket and upload the AWS Lambda code and the firewall.template to the S3 bucket.
   1. Click the bucket name.
   2. Click **Add Files** to select the panw-aws.zip file and the firewall.template, click **Open**.
   3. Click **Start Upload** to add the files to the S3 bucket.



STEP 6 | Select the VM-Series Auto Scaling template to launch.

1. In the AWS Management Console, select **CloudFormation** > **Create Stack**.
2. Select **Upload a template to Amazon S3**, choose the vpc-classic-v1.2.template or the vpc-alb-v1.2.template that you downloaded previously, and click **Open** and **Next**.
3. Specify the **Stack name** in 10 characters or less. The stack name allows you to uniquely identify all the resources that are deployed using this VM-Series Auto Scaling template. Using a longer stack name results in a failure to successfully deploy the template.

STEP 7 | Configure the parameters for the VPC.

1. Enter the parameters for the **VPC Configuration** as follows:
   1. Enter a **VPCName** and a **VPC CIDR**. The default CIDR is 192.168.0.0/16.
   2. Enter the IP address blocks for the management, untrust and trust subnets for the VM-Series firewalls in each Availability Zone. By default three subnets are allocated across three AZs. The default blocks for the management subnets are 192.168.0.0/24, 192.168.10.0/24 and 192.168.20.0/24, Untrust subnets are 192.168.1.0/24, 192.168.11.0/24 and 192.168.21.0/24 and Trust subnets are 192.168.2.0/24, 192.168.12.0/24 and 192.168.22.0/24

      If you modify the subnets, make sure that the management and untrust dataplane interfaces are in separate subnets.
   3. For **Do you want to create a NAT Gateway in each AZ**, enter **Yes** if you want the VM-Series Auto Scaling template to deploy an AWS NAT gateway. Enter **No**, if you want to assign EIPs to the management interface on each firewall to enable outbound access from the VPC. If you do not plan to allocate EIPs on the management interface for each VM-Series firewall, the AWS NAT gateway is required for the firewalls to access the Palo Alto Networks Update servers, Panorama, and to publish metrics to CloudWatch.
   4. (Required if you opted for the AWS NAT Gateway) Enter the IP address blocks for the NAT gateway in each AZ. The default assignment is 192.168.100.0/24, 192.168.101.0/24, 192.168.102.0/24, 192.168.103.0/24.
   5. (Required if you opted for the AWS NAT Gateway) Enter the IP address blocks for the Lambda functions in each AZ. The default assignment is 192.168.200.0/24, 192.168.201.0/24, 192.168.202.0/24, 192.168.203.0/24
   6. Select whether the uptime needs for your setup requires the VPC to span two or three Availability Zones in **Number of Availability Zones for deployment**.

7. Select your AZ preference from the **Select list of Availability Zones** drop-down. Make sure to select two or three based on the number of AZs you selected above.

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

1. Select the EC2 instance size for the VM-Series firewall.
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 have opted to use.
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.
4. Select the EC2 **Key pair** (from the drop-down) for launching the firewall. To log in to the firewall or the web servers, you must provide the name of this key pair and the private key associated with it.
5. 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.

STEP 9 | Specify the name of the Amazon S3 buckets.

1. Enter the name of the S3 bucket that contains the bootstrap files.

   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; ELB health checks will also fail.
2. Enter the name of the S3 bucket that contains the firewall.template and the Lambda code that you extracted from the 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.

STEP 11 | Specify the name for the ELBs.

The ELB name must be 12 characters or less. If the name is longer than 12 characters, the VM-Series Auto Scaling template will fail to deploy.

1. Enter the name for the internet-facing (or external) classic ELB.
2. Enter the name for the internal classic or application ELB.

STEP 12 | Configure the metric to monitor and define the thresholds for auto scaling. The custom PAN-OS metrics create CloudWatch alarms that execute auto scaling policies to scale in or scale out the VM-Series firewalls based on the thresholds you define.

1. Select one scaling metric:
   - Active Sessions (number)—Monitors the total number of sessions that are active on the firewall. Because the firewall uses NAT in this solution, the maximum number of sessions supported is 64, 000.
   - Dataplane CPU Utilization (%)—Monitors the dataplane CPU usage to measure the traffic load on the firewall.

- Dataplane Buffer Utilization (%)—Monitors the dataplane buffer usage to measure buffer utilization. If you have a sudden burst in traffic, monitoring buffer utilization allows you to ensure that the firewall does not deplete the dataplane buffer and cause dropped packets.

2. Enter the scaling period. This is the time interval for which a monitored metric must remain at the configured threshold to trigger a scaling event. The value is in seconds; choose one of these values for the scaling period: 60, 300, 900 (default), 3,600, 21,600, or 84,600.
3. Enter the maximum number of VM-Series firewalls in an ASG.
4. Enter the minimum number of VM-Series firewalls in an ASG. The minimum value of 1 means that every ASG will have at least one VM-Series firewall.
5. Enter the thresholds for a scaling event. This input can be a number or a percentage based on the scaling metric you selected above.

   For active sessions, as a best practice, set this value at a maximum of 51, 200 (80% of 64,000) to allow for scale out events to complete with a fully functioning firewall. Assess the traffic patterns for your application, and determine whether you need to set a more conservative threshold.

   For dataplane buffer utilization, set the value at a maximum of 40% so that the firewall can optimally handle a burst in traffic.

   Bootstrapping a PAN-OS firewall can take 10 to 15 minutes. Make sure to set some buffer in your scale thresholds to accommodate that boot time. For example, don't wait until the session table is 95% full before launching a new firewall in the auto scale group.

STEP 13 | Select the EC2 instance type for the web servers.

Make sure to pick an instance size that matches the expected load on your web servers so that the internal ELB does not fluctuate hugely with variable demand. If the internal ELB fluctuates, it will trigger scaling events for the ASGs and the corresponding VM-Series firewalls.

STEP 14 | (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 15 | 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 external ELB. The firewalls will be bootstrapped with a NAT policy rule and a basic Security policy rule. It will also launch two web servers in an ASG behind the internal ELB.

STEP 16 | Verify that the template has launched all required resources.

To modify or update the resources for this VM-Series Auto Scaling template, see Stack Update with VM-Series Auto Scaling Template for AWS (v1.2)

1. On the EC2 Dashboard, select **Load Balancers**.
2. Get the **DNS name** for the external ELB, 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 minimum number of firewalls you specified in the template and the web server ASG.

If you selected three AZs and the AWS NAT gateway, the VM-Series firewall ASG name displays this information as az3n; the details are appended to the stack name for example: VM-Auto-CFT-az3n-EB4Y7D3DMJ6E_ASG_LC_192-168-2-6

4. Log in to the VM-Series firewall.

   It may take up to 20 minutes for the firewalls to boot up and be available to handle traffic.

   Use the EIP address, if you allocated one. If you chose the NAT gateway option, you must deploy a jump server or use Panorama to access the web interface on the firewall.
5. Select **Monitor** > **Logs** > **Traffic** on the web interface of the firewall to view logs.

   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.

   If you are using Panorama, delete the internal ELB on AWS before you delete the stack. Deleting the internal ELB allows the VM-Series firewalls to shut down gracefully, and Panorama can remove the firewalls from the list of managed devices.

Launch the VM-Series Auto Scaling Template for AWS (v1.1)

Use the following workflow to deploy all the components in this solution using the vpc-classic-v1.1.template or the vpc-alb-v1.1.template.

If you have an existing VPC with the required subnets, security groups, web servers, and ELBs, you only need to deploy the VM-Series firewall at scale, use the firewall.template. The workflow for using only the firewall.tempate is not documented in this version of the document, but it is very similar.

STEP 1 | Plan the VM-Series Auto Scaling Template for AWS.

Make sure that you have completed the following tasks:

- Reviewed and accepted the EULA.
- 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 information on the bootstrapping process see Bootstrap the VM-Series Firewall; for details on the init-cfg.txt file, see Create 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.
3. 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 and the device group to which you want to assign the firewall. Enter:

tplname=

dgname=

- VM auth key. Enter:

vm-auth-key=

4. 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.

5. Save and close the file.

STEP 3 | 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.

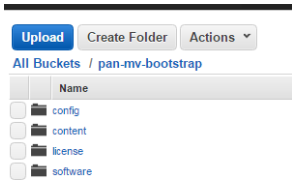
The bootstrap.xml file provided in the GitHub repository is provided for testing and evaluation only. For a production deployment, you must modify the bootstrap.xml prior to launch, see Customize the Bootstrap.xml File.

STEP 4 | Prepare the Amazon Simple Storage (S3) buckets for launching the VM-Series Auto Scaling template.

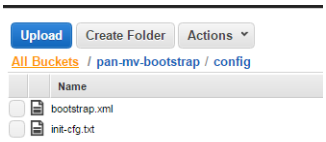
Make sure to create the S3 buckets in the same region in which you plan to deploy the template.

The VM-Series Auto Scaling template requires one S3 bucket for the VM-Series bootstrap files; and another S3 bucket for the AWS Lambda functions and the nested `firewall.template`.

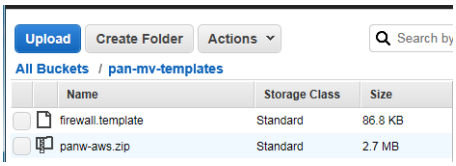
1. Create a new S3 bucket for the bootstrap files.
    1. Sign in to the AWS Management Console and open the S3 console.
    2. Click **Create Bucket**.
    3. Enter a **Bucket Name** and a **Region**, and click **Create**. The bucket must be at the S3 root level. If you nest the bucket, bootstrapping 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.



3. Create another S3 bucket and upload the AWS Lambda code and the firewall.template to the S3 bucket.
   1. Click the bucket name.
   2. Click **Add Files** to select the panw-aws.zip file and the firewall.template, click **Open**.
   3. Click **Start Upload** to add the files to the S3 bucket.



STEP 5 | Select the VM-Series Auto Scaling template that you want to launch.

1. In the AWS Management Console, select **CloudFormation** > **Create Stack**.
2. Select **Upload a template to Amazon S3**, choose the vpc-classic-v1.template or the vpc-alb-v1.template that you downloaded previously, and click **Open** and **Next**.
3. Specify the **Stack name** in 10 characters or less. The stack name allows you to uniquely identify all the resources that are deployed.

STEP 6 | Configure the parameters for the VPC.

1. Enter the parameters for the **VPC Configuration** as follows:
   1. Enter a **VPCName** and a **VPC CIDR**. The default CIDR is 192.168.0.0/16.
   2. Enter the IP address blocks for the management, untrust and trust subnets for the VM-Series firewalls in each Availability Zone. By default three subnets are allocated across three AZs. The default blocks for the management subnets are 192.168.0.0/24, 192.168.10.0/24 and 192.168.20.0/24, Untrust subnets are 192.168.1.0/24, 192.168.11.0/24 and 192.168.21.0/24 and Trust subnets are 192.168.2.0/24, 192.168.12.0/24 and 192.168.22.0/24
   3. For **Do you want to create a NAT Gateway in each AZ**, enter **Yes** if you want the VM-Series Auto Scaling template to deploy an AWS NAT gateway. Enter **No**, if you want to assign EIPs to the management interface on each firewall to enable outbound access from the VPC. If you do not plan to allocate EIPs on the management interface for each VM-Series firewall, the AWS NAT gateway is required for the firewalls to access the Palo Alto Networks Update servers, Panorama, and to publish metrics to CloudWatch.

4. (Required if you opted for the AWS NAT Gateway) Enter the IP address blocks for the NAT gateway in each AZ. The default assignment is 192.168.100.0/24, 192.168.101.0/24, 192.168.102.0/24, 192.168.103.0/24.
5. (Required if you opted for the AWS NAT Gateway) Enter the IP address blocks for the Lambda functions in each AZ. The default assignment is 192.168.200.0/24, 192.168.201.0/24, 192.168.202.0/24, 192.168.203.0/24
6. Select whether the uptime needs for your setup requires the VPC to span two or three Availability Zones in **Number of Availability Zones for deployment**.
7. Select your AZ preference from the **Select list of Availability Zones** drop-down. Make sure to select two or three based on the number of AZs you selected above.

STEP 7 | Select your preferences for the VM-Series firewalls.

1. Select the EC2 instance size for the VM-Series firewall.
2. Select the EC2 **Key pair** (from the drop-down) for launching the firewall. To log in to the firewall or the web servers, 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.

STEP 8 | Specify the name of the Amazon S3 buckets.

1. Enter the name of the S3 bucket that contains the bootstrap files.

   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; ELB health checks will also fail.
2. Enter the name of the S3 bucket that contains the firewall.template and the Lambda code that you extracted from the zip file.

STEP 9 | 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 th 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.

STEP 10 | Specify the name for the ELBs.

The ELB name must be 12 characters or less. If the name is longer than 12 characters, the VM-Series Auto Scaling template will fail to deploy.

1. Enter the name for the internet-facing (or external) classic ELB.
2. Enter the name for the internal classic or application ELB.

STEP 11 | Configure the metric to monitor and define the thresholds for auto scaling. The custom PAN-OS metrics create CloudWatch alarms that execute auto scaling policies to scale in or scale out the VM-Series firewalls based on the thresholds you define.

1. Select one scaling metric:

   - Active Sessions (number)—Monitors the total number of sessions that are active on the firewall. Because the firewall uses NAT in this solution, the maximum number of sessions supported is 64,000.

- Dataplane CPU Utilization (%)—Monitors the dataplane CPU usage to measure the traffic load on the firewall.
- Dataplane Buffer Utilization (%)—Monitors the dataplane buffer usage to measure buffer utilization. If you have a sudden burst in traffic, monitoring buffer utilization allows you to ensure that the firewall does not deplete the dataplane buffer and cause dropped packets.

2. Enter the scaling period. This is the time interval for which a monitored metric must remain at the configured threshold to trigger a scaling event. The value is in seconds; choose one of these values for the scaling period: 60, 300, 900 (default), 3,600, 21,600, or 84,600.
3. Enter the maximum number of VM-Series firewalls in an ASG.
4. Enter the minimum number of VM-Series firewalls in an ASG. The minimum value of 1 means that every ASG will have at least one VM-Series firewall.
5. Enter the thresholds for a scaling event. This input can be a number or a percentage based on the scaling metric you selected above.

   For active sessions, as a best practice, set this value at a maximum of 51, 200 (80% of 64,000) to allow for scale out events to complete with a fully functioning firewall. Assess the traffic patterns for your application, and determine whether you need to set a more conservative threshold.

   For dataplane buffer utilization, set the value at a maximum of 40% so that the firewall can optimally handle a burst in traffic.

   Bootstrapping a PAN-OS firewall can take 10 to 15 minutes. Make sure to set some buffer in your scale thresholds to accommodate that boot time. For example, don't wait until the session table is 95% full before launching a new firewall in the auto scale group.

STEP 12 | Select the EC2 instance type for the web servers.

Make sure to pick an instance size that matches the expected load on your web servers so that the internal ELB does not fluctuate hugely with variable demand. If the internal ELB fluctuates, it will trigger scaling events for the ASGs and the corresponding VM-Series firewalls.

STEP 13 | (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 14 | 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 external ELB. The firewalls will be bootstrapped with a NAT policy rule and a basic Security policy rule. It will also launch two web servers in an ASG behind the internal ELB.

STEP 15 | Verify that the template has launched all required resources.

1. On the EC2 Dashboard, select **Load Balancers**.
2. Get the **DNS name** for the external ELB, 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 minimum number of firewalls you specified in the template and the web server ASG.

If you selected three AZs and the AWS NAT gateway, the VM-Series firewall ASG name displays this information as az3n; the details are appended to the stack name for example: VM-Auto-CFT-az3n-EB4Y7D3DMJ6E_ASG_LC_192-168-2-6

4. Log in to the VM-Series firewall.

   It may take up to 20 minutes for the firewalls to boot up and be available to handle traffic.

   Use the EIP address, if you allocated one. If you chose the NAT gateway option, you must deploy a jump server or use Panorama to access the web interface on the firewall.
5. Select **Monitor** > **Logs** > **Traffic** on the web interface of the firewall to view logs.

   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 VM-Series Auto Scaling template might automatically deploy new ASGs.

   If you are using Panorama, delete the internal ELB on AWS before you delete the stack. Deleting the internal ELB allows the VM-Series firewalls to shut down gracefully, and Panorama can remove the firewalls from the list of managed devices.

Customize the Bootstrap.xml File

The bootstrap.xml file provided in the GitHub repository uses a default username and password for the firewall administrator. Before deploying the VM-Series Auto Scaling template in a production environment, at a minimum, you must create a unique username and password for the administrative account on the VM-Series firewall. Optionally, you can fully configure the firewall with zones, policy rules, security profiles and export a golden configuration snapshot. You can then use this configuration snapshot as the bootstrap.xml file for your production environment.

You have two ways to customize the bootstrap.xml file for use in a production environment:

- **Option 1**: Launch a VM-Series firewall on AWS using the bootstrap files provided in the GitHub repository, modify the firewall configuration and export the configuration to create a new bootstrap.xml file for the VM-Series Auto Scaling template. See Use the GitHub Bootstrap Files as Seed.
- **Option 2**: Launch a new VM-Series firewall on AWS without using the bootstrap files, add a NAT policy rule to ensure that the VM-Series firewall handles traffic properly, and export the configuration to create a new bootstrap.xml file for the VM-Series Auto Scaling template. See Create a new Bootstrap File from Scratch.

If you have deployed the template and now need to change the credentials for the administrative user or add a new admin user and update the template stack, see Modify Administrative Account and Update Stack.

Use the GitHub Bootstrap Files as Seed

Launch a VM-Series firewall on AWS from the AWS Marketplace using the bootstrap files provided in the GitHub repository, modify the firewall configuration for your production environment and export the configuration to create a new bootstrap.xml file that you can now use for the VM-Series Auto Scaling template.

STEP 1 | To launch the firewall see Bootstrap the VM-Series Firewall in AWS.

STEP 2 | Add an elastic network interface (ENI) and associate an elastic IP address (EIP) to it, so that you can access the web interface on the VM-Series firewall. See Launch the VM-Series Firewall on AWS for details.

STEP 3 | Use the EIP address to log in to the firewall web interface with admin as the username and password.

STEP 4 | Add a secure password for the admin user account (**Device** > **Local User Database** > **Users**).

STEP 5 | (Optional) Configure the firewall for securing your production environment.

STEP 6 | Select **Policies** > **NAT** to verify the firewall has the NAT policy rule required for the VM-Series Auto Scaling template. The NAT policy rule is included in the bootstrap.xml file, and is required to avoid blackholing traffic. The NAT policy rule routes traffic to the internal ELB and ensures symmetric return of the traffic from the web servers.

STEP 7 | **Commit** the changes on the firewall.

STEP 8 | Generate a new API key for the administrator account. Copy this new key to a new file. You will need to enter this API key when you launch the VM-Series Auto Scaling template; the AWS services use the API key to deploy the firewall and to publish metrics for auto scaling.

STEP 9 | Export the configuration file and save it as **`bootstrap.xml`**. (**Device** > **Setup** > **Operation** > **Export Named Configuration Snapshot**).

STEP 10 | Open the bootstrap.xml file with a text editing tool and delete the management interface configuration.

STEP 11 | (Required if you exported a PAN-OS 8.0 configuration) Ensure that the setting to validate the Palo Alto Networks servers is disabled. Look for **`<server-verification>no</server-verification>`**.

STEP 12 | If the check is **yes**, change it to **no**.

STEP 13 | Save the file. You can now proceed with Launch the VM-Series Auto Scaling Template for AWS.

Create a new Bootstrap File from Scratch

Launch a new VM-Series firewall on AWS using PAN-OS 8.0 without using the bootstrap files, add a NAT policy rule to ensure that the VM-Series firewall handles traffic properly, and export the configuration to create a new bootstrap.xml file for the VM-Series Auto Scaling template.

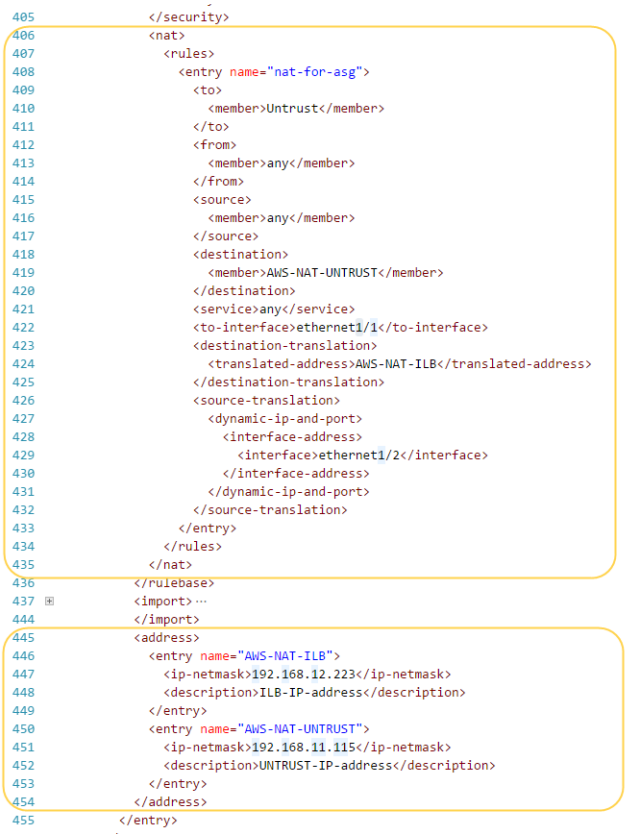
STEP 1 | Deploy the VM-Series Firewall on AWS (no bootstrapping required) and use the public IP address to SSH into the Command Line Interface (CLI) of the VM-Series firewall. You will need to configure a new administrative password for the firewall.

STEP 2 | Log in to the firewall web interface.

STEP 3 | (Optional) Configure the firewall. You can configure the dataplane interfaces, zones and policy rules. **Commit** the changes on the firewall.

STEP 4 | Export the configuration file and name it as **`bootstrap.xml`**. (**Device** > **Setup** > **Operation** > **Export Named Configuration Snapshot**).

STEP 5 | Download the bootstrap.xml file from the GitHub repository, open it with a text editing tool, and copy lines 406 to 435 and 445 to 454. These lines define the NAT policy rule and the address object required for the VM-Series Auto Scaling template. If you want to copy and paste the NAT policy rule and address objects, see NAT Policy Rule and Address Objects in the Auto Scaling Template.



STEP 6 | Use a text editing tool to open the configuration file you exported earlier.

1. Search for `</security>` and paste the lines 406 to 435 after `</security>`.
2. Search for `</import>` and paste the lines 445 to 454 after `</import>`.

STEP 7 | Delete the management interface configuration.

1. Search for `</service>` and delete the ip-address, netmask and default gateway that follow.
2. Search for `</type>` and delete the ip-address, netmask, default gateway, and public-key that follow.

STEP 8 | Save the file. You can now proceed with Launch the VM-Series Auto Scaling Template for AWS.

NAT Policy Rule and Address Objects in the Auto Scaling Template

To Customize the Bootstrap.xml File for deploying the VM-Series Auto Scaling Template for AWS in your production environment, you must copy the following NAT policy rule into your configuration file. You can find the NAT rule and address objects in the bootstrap.xml file in the GitHub repository.

- **NAT Policy Rule**

```
<nat>
  <rules>
    <entry name="nat-for-asg">
      <to>
        <member>Untrust</member>
      </to>
      <from>
        <member>any</member>
      </from>
      <source>
        <member>any</member>
       </source>
       <destination>
        <member>AWS-NAT-UNTRUST</member>
      </destination>
      <service>any</service>
      <to-interface>ethernet1/1</to-interface>
      <destination-translation>
         <translated-address>AWS-NAT-ILB</translated-address>
      </destination-translation>
      <source-translation>
        <dynamic-ip-and-port>
          <interface-address>
            <interface>ethernet1/2</interface>
          </interface-address>
        </dynamic-ip-and-port>
      </source-translation>
```

```
    </entry>
  </rules>
</nat>
```

- **NAT Policy Address Objects**

```
<address>
  <entry name="AWS-NAT-ILB">
   <ip-netmask>192.168.12.223</ip-netmask>
   <description>ILB-IP-address</description>
  </entry>
  <entry name="AWS-NAT-UNTRUST">
   <ip-netmask>192.168.11.115</ip-netmask>
   <description>UNTRUST-IP-address</description>
  </entry>
</address>
```

Stack Update with VM-Series Auto Scaling Template for AWS (v1.2)

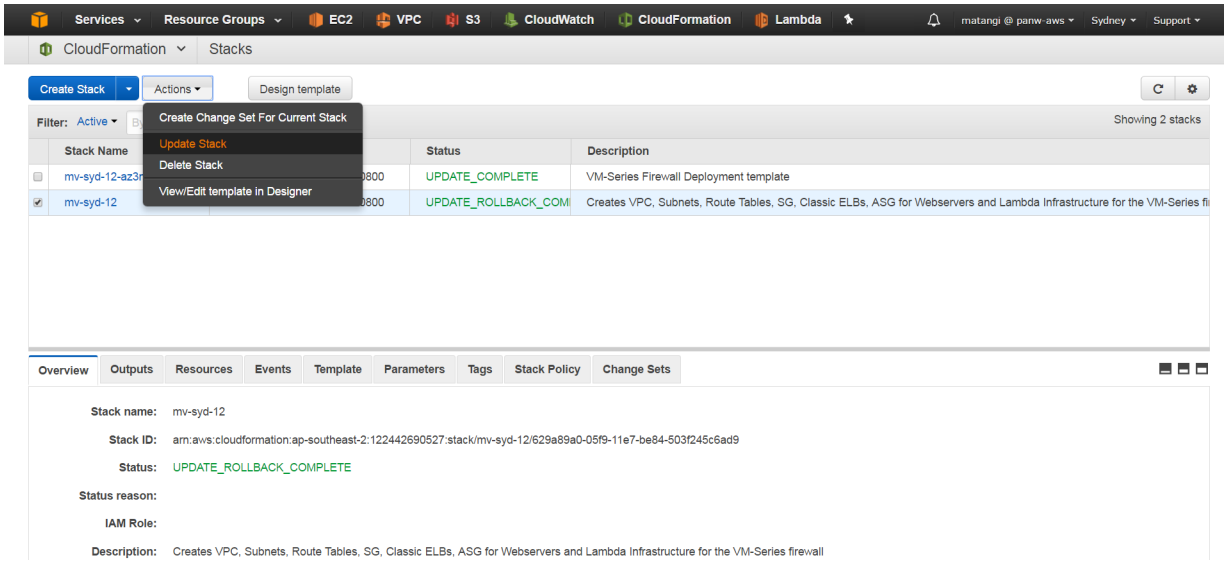
A stack update allows you to modify the resources that the VM-Series Auto Scaling template deploys. Instead of deleting your existing deployment and redeploying the solution, use the stack update to modify the following parameters:

- PAN-OS version—Deploy new VM-Series firewalls with a different PAN-OS version.
- License—Switch from BYOL to PAYG and vice versa or switch from one PAYG bundle to another.
- Other stack resources— Change the launch configuration parameters such as the Amazon Machine Image (AMI) ID, the instance type, key pair for your auto scaling groups. You can also update the API key associated with the administrative user account on the firewall.

When you deploy the VM-Series Auto Scaling template, the auto scaling groups and the launch configuration are automatically created for you. The launch configuration is a template that an auto scaling group uses to launch EC2 instance, and it specifies parameters such as the AMI ID, the instance type, key pair for your auto scaling group. To modify these parameters, you must update the stack and then replace the existing auto scaling group with a new auto scaling group that uses the updated stack parameters to create the launch configuration and deploy new instances with these new parameters; existing instances continue to run with the configuration that they were originally launched with. This phased rollout allows you to verify the updates in one AZ at a time and then complete the changes across the other AZs without disruption. For critical applications, perform a stack update during a maintenance window.

You can update stack directly or create change sets. The workflow in this document takes you through the manual stack update.

STEP 1 | In the AWS CloudFormation console, select the parent stack that you want to update and choose **Actions** > **Update Stack**.



STEP 2 | Modify the resources that you want to update.

- PAN-OS version—To modify the PAN-OS version look up the AMI ID for the version you want to use and enter the ID. If you are upgrading to PAN-OS 8.0 make sure to select an instance type that meets the VM-Series System Requirements.
- License option—Switch from BYOL to PAYG or across PAYG bundles 1 and 2.

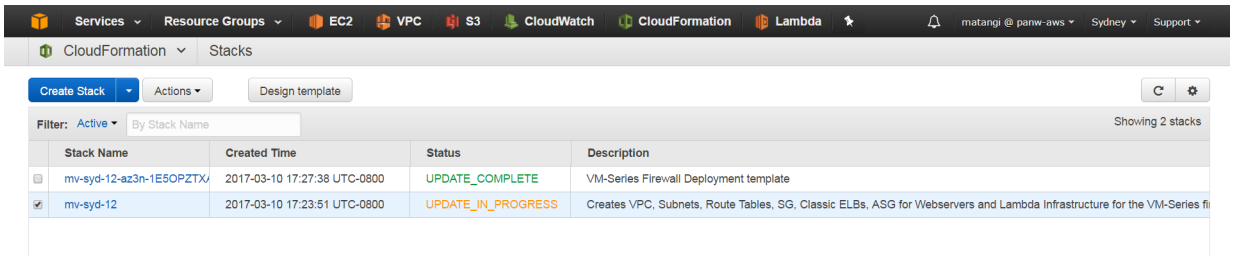
If you're switching to BYOL, make sure to include the auth code in the bootstrap package (See steps 3 and 5).

If you're switching between PAYG bundle version 1 and 2, look up the AMI ID for the VM-Series firewall.

- Other stack resources— You can modify the AMI ID, the instance type, security group, key pair for the stack resources, or the API key associated with the administrative user account on the firewall.

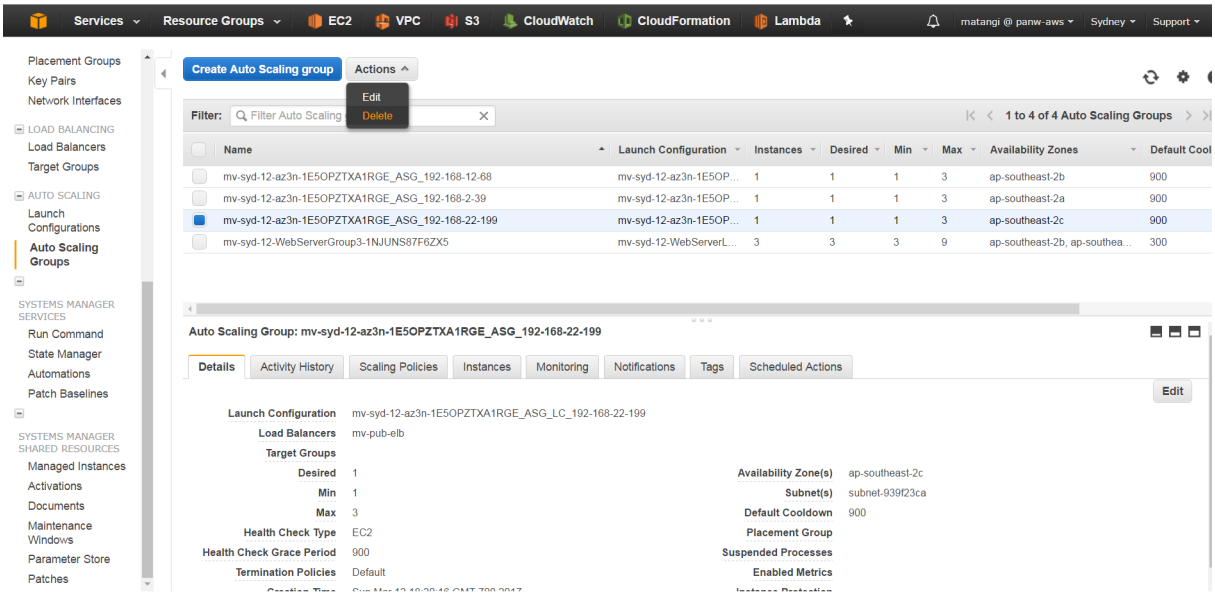
If you create a new administrative user account or modify the credentials of the existing administrator on the firewall, in order to update that stack and deploy new firewalls with the updated API key, you need to follow the workflow in Modify Administrative Account and Update Stack.

STEP 3 | Acknowledge the notifications and review the changes and click **Update** to initiate the stack update.

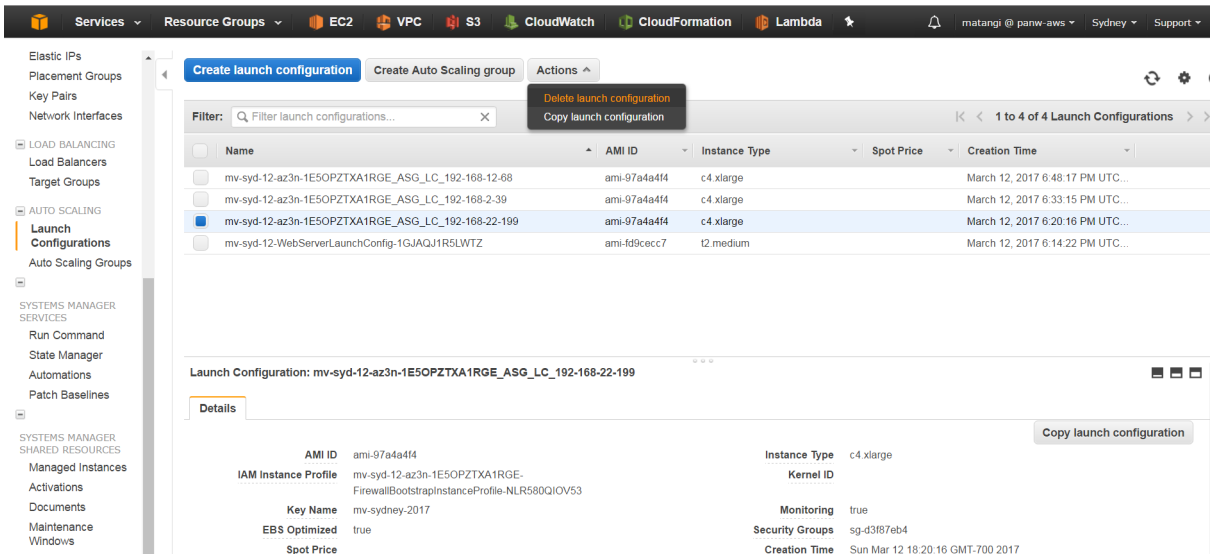


STEP 4 | On the **EC2 dashboard** > **Auto Scaling Groups** and pick an AZ in which to delete the ASG.

Deleting an ASG allows you to replace the existing ASGs (one at a time) with a new ASG that uses the new parameters.

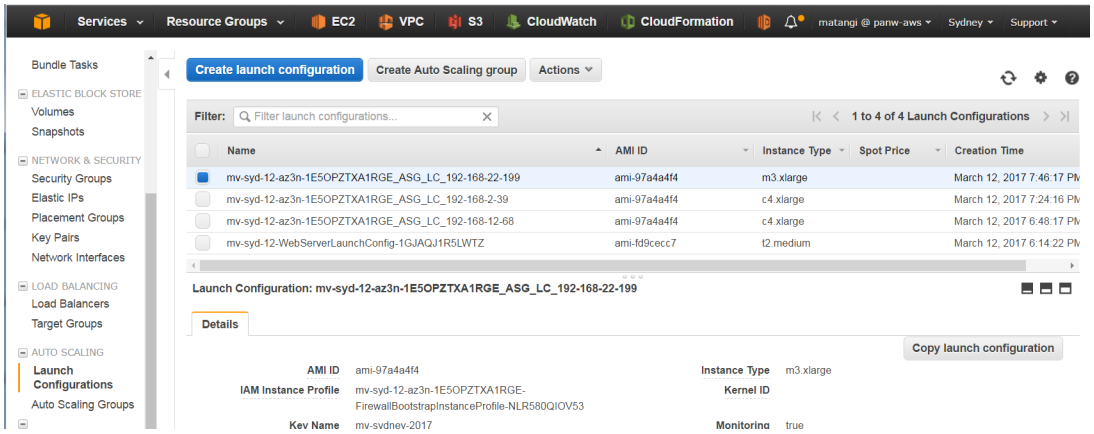


STEP 5 | Delete the launch configuration.



STEP 6 | Verify that the updated parameters are used to launch the VM-Series firewalls in the new ASG.

Test the new ASG thoroughly and ensure it is properly handling traffic. As a best practice, wait one hour before continuing to the next ASG.



STEP 7 | Repeat steps 4 through 6 to replace the ASGs in the remaining AZs.

Modify Administrative Account and Update Stack

If you have already deployed the template and now want to change the password for the administrative account or create a new administrative user account on the VM-Series firewall, you must generate a new API key and update the template stack with the new API key for the administrative user account. And in order to ensure that new firewall instances are configured with the updated administrative user account, you need to export the firewall configuration and rename it to bootstrap.xml, then upload it to the S3 bootstrap folder that the VM-Series AutoScaling template uses.

STEP 1 | Log in to the web interface of the firewall and change the credentials for an existing administrative user or create a new account.

STEP 2 | Generate the API key.

STEP 3 | Export the current running configuration and rename it to bootstrap.xml.

STEP 4 | Upload this bootstrap.xml file to the S3 bootstrap folder (see Customize the Bootstrap.xml File).

STEP 5 | Update the API key in the stack to ensure that newly launched firewalls will have the updated administrator account.

See Stack Update with VM-Series Auto Scaling Template for AWS (v2.0)or Stack Update with VM-Series Auto Scaling Template for AWS (v1.2) for details.

Troubleshoot the VM-Series Auto Scaling Template for AWS

When deploying a VM-Series Auto Scaling template version 1.2 or 1.1, if the template stack is unable to provision the resources specified in the template, the process automatically rolls back and deletes the resources that were successfully created. Because an initial error can trigger a cascade of additional errors, you need to review the logs to locate the first failure event.

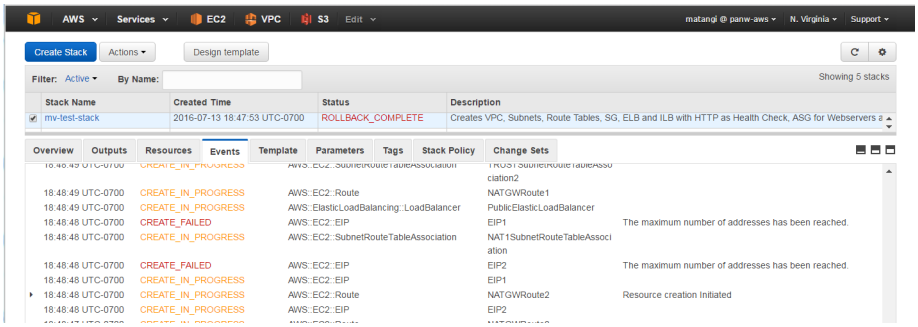
- Error: Inadequate number of Elastic IP addresses (EIPs)
- Error: Stack name is longer than 10 characters.
- Error: The instance size does not meet the minimum system requirements for the VM-Series firewall model.
- Error: Unable to log in to the firewall

- Error: AWS Lambda is not supported in the region in which you are deploying the VM-Series Auto Scaling template.
- Error: Failure to successfully create a resource with a message such as:
- Error: Failure to launch the VM-Series Auto Scaling template because of a missing required parameter or not specifying the AWS Availability Zones for the template.
- Error: Failure to launch the VM-Series Auto Scaling template because you did not accept the End User License Agreement (EULA) for the PAYG VM-Series Firewall Bundle you are deploying.

Error: Inadequate number of Elastic IP addresses (EIPs)

AWS Lambda requires EIP address to successfully launch the firewall.

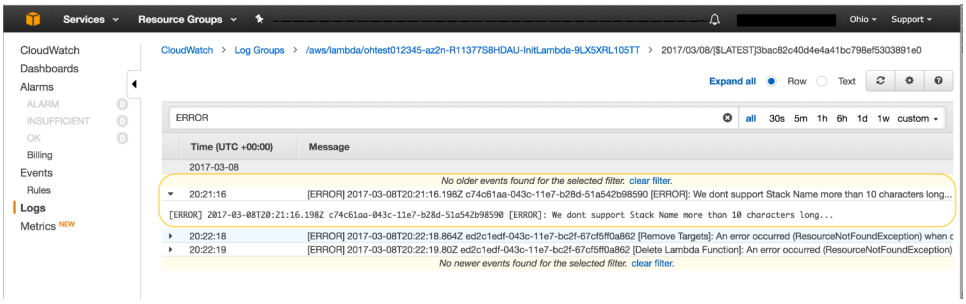
1. On the AWS Management Console, select **CloudFormation**.
2. In the Stack list, select the name of the template that failed to deploy and view the list of **Events**.
3. Look through the failure events for `maximum number of addresses has been reached`.



Error: Stack name is longer than 10 characters.

The VM-Series Auto Scaling template deployment fails if the stack name is longer than 10 characters in length.

1. On the AWS Management Console, select **CloudWatch** > **Logs**.
2. In the Log Groups list, select the name of the Log Stream for the template that failed to deploy so that you can find the error.
3. Filter for ERROR events and look for `stack name more than 10 characters long`.



Error: The instance size does not meet the minimum system requirements for the VM-Series firewall model.

The VM-Series Auto Scaling template deployment fails if the instance size you selected does not match the VM-Series System Requirements.

Error: Unable to log in to the firewall

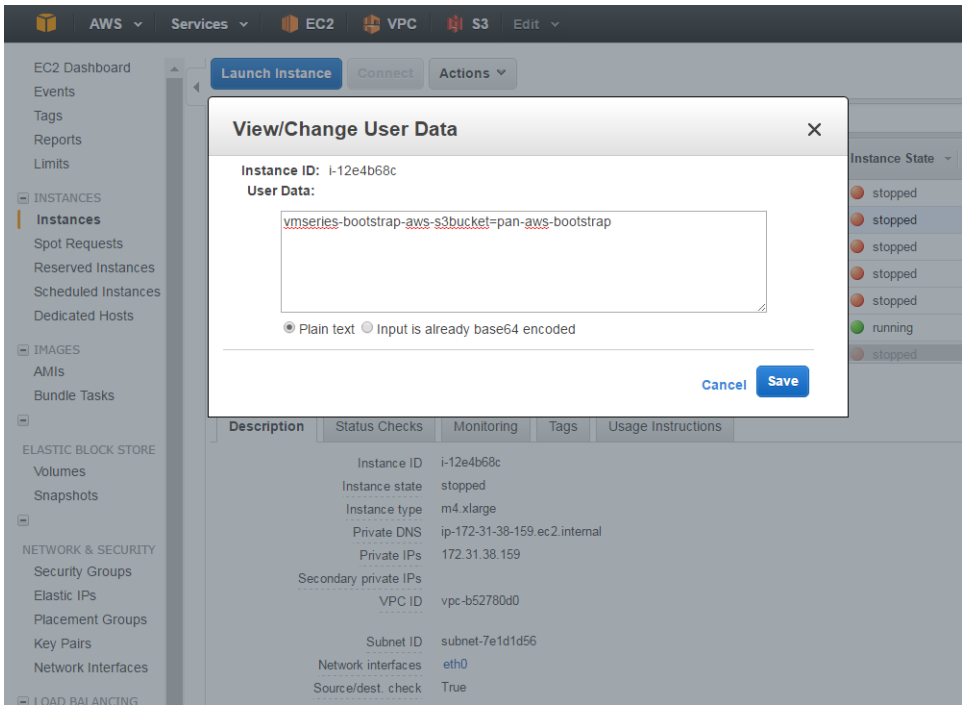
The reasons you cannot log in to the firewall can be because:

- The firewall is not configured properly because the bootstrap process failed.
- You chose the NAT gateway option to conserve the use of EIP addresses, so the firewall does not have a publicly accessible IP address. If you are not using Panorama to manage the firewall, to access the CLI or

web interface on the firewall on the private IP address assigned by AWS, you must deploy a bastion host or jump server on the same subnet as the firewall and assign a public IP address to the jump server. Then log in to the jump server and connect to the firewall.

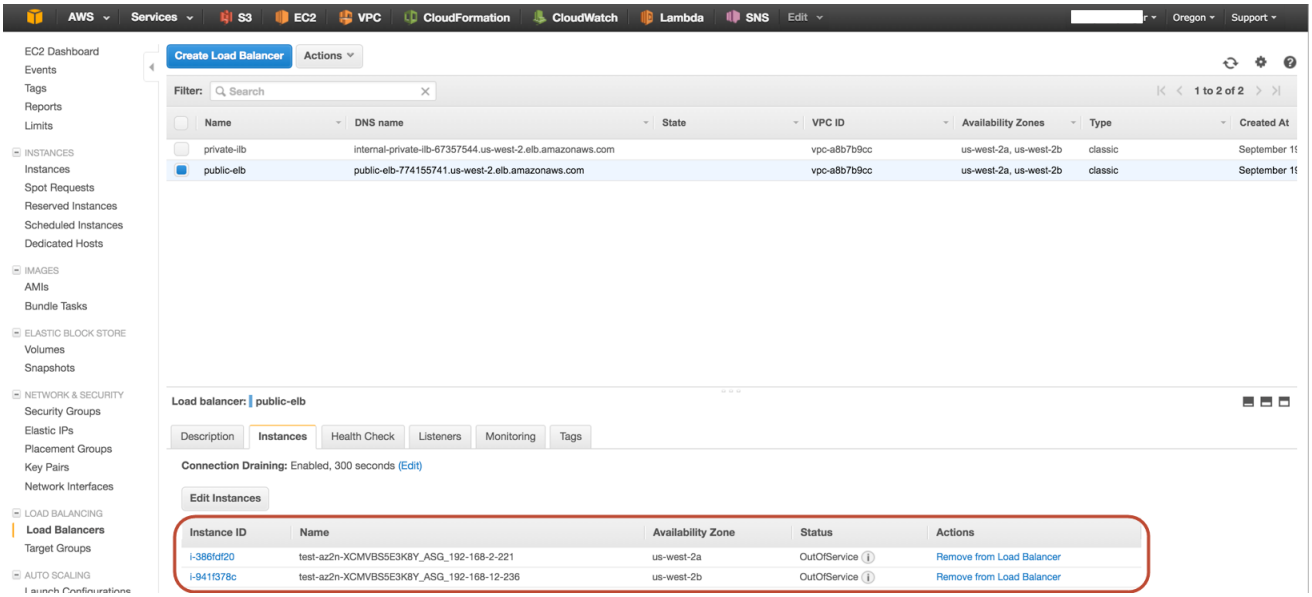
- You edited the bootstrap.xml file and the NAT policy is missing or incorrect.

1. To troubleshoot, first check that the template references the correct S3 bucket with the bootstrap files:
    1. On the EC2 Dashboard, select **Instances**.
    2. Select the firewall instance, and click **Actions** > **View/Change User Data**.
    3. Verify the name for the S3 bucket that contains the bootstrap files.



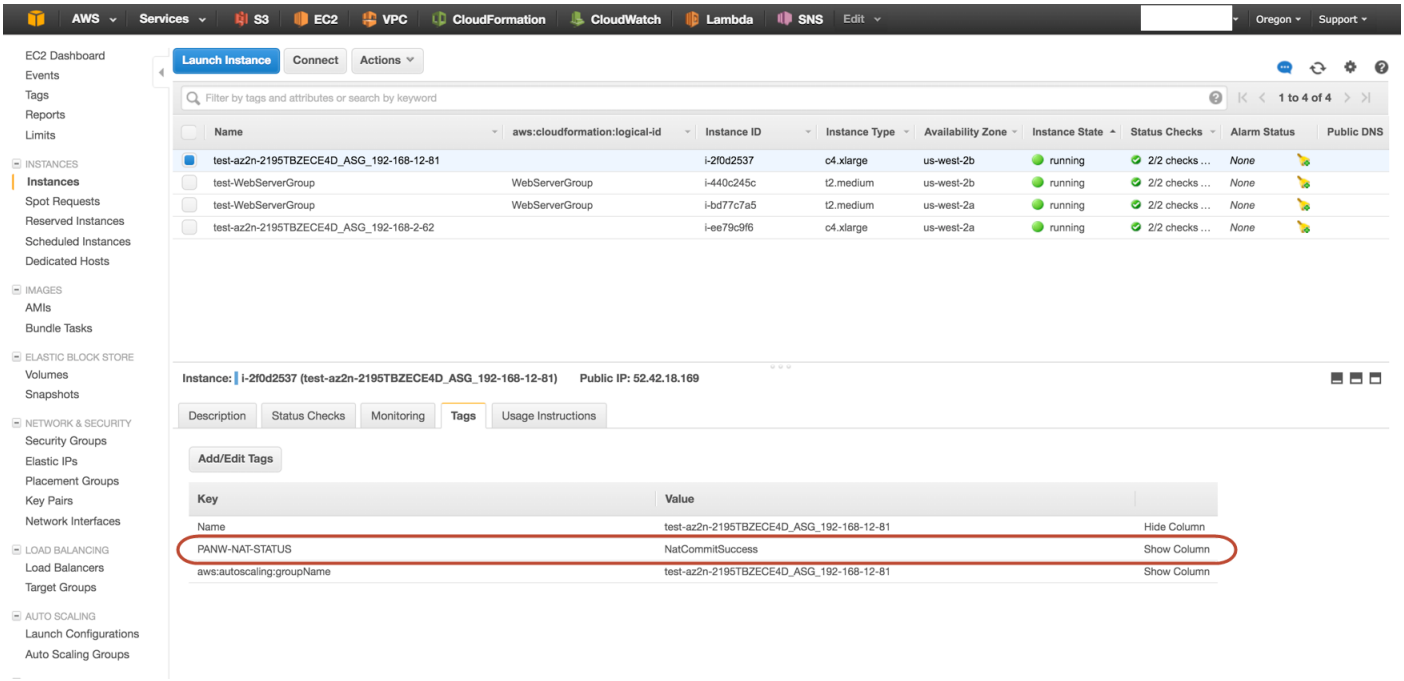
    4. Verify that you created the S3 bucket at the root level, directly under All Buckets. If you nest the S3 bucket, bootstrapping will fail because you cannot specify a path to the location of the bootstrap files. See Prepare the Amazon Simple Storage (S3) buckets for launching the VM-Series Auto Scaling template.
    5. Verify that the S3 bucket is in the same region in which you are deploying the VM-Series Auto Scaling template.
2. Check if the internet-facing ELB is in service. If bootstrapping fails, the VM-Series firewall for load balancing traffic will be out-of-service.
    1. Select **EC2** > **LoadBalancers**.
    2. Select the internet-facing (or external) classic ELB to verify that the VM-Series firewall instances are in-service.

        The following screenshot shows that the VM-Series firewalls are not in service.



3. If the VM-Series firewalls are in service, check that the NAT policy was successfully committed.

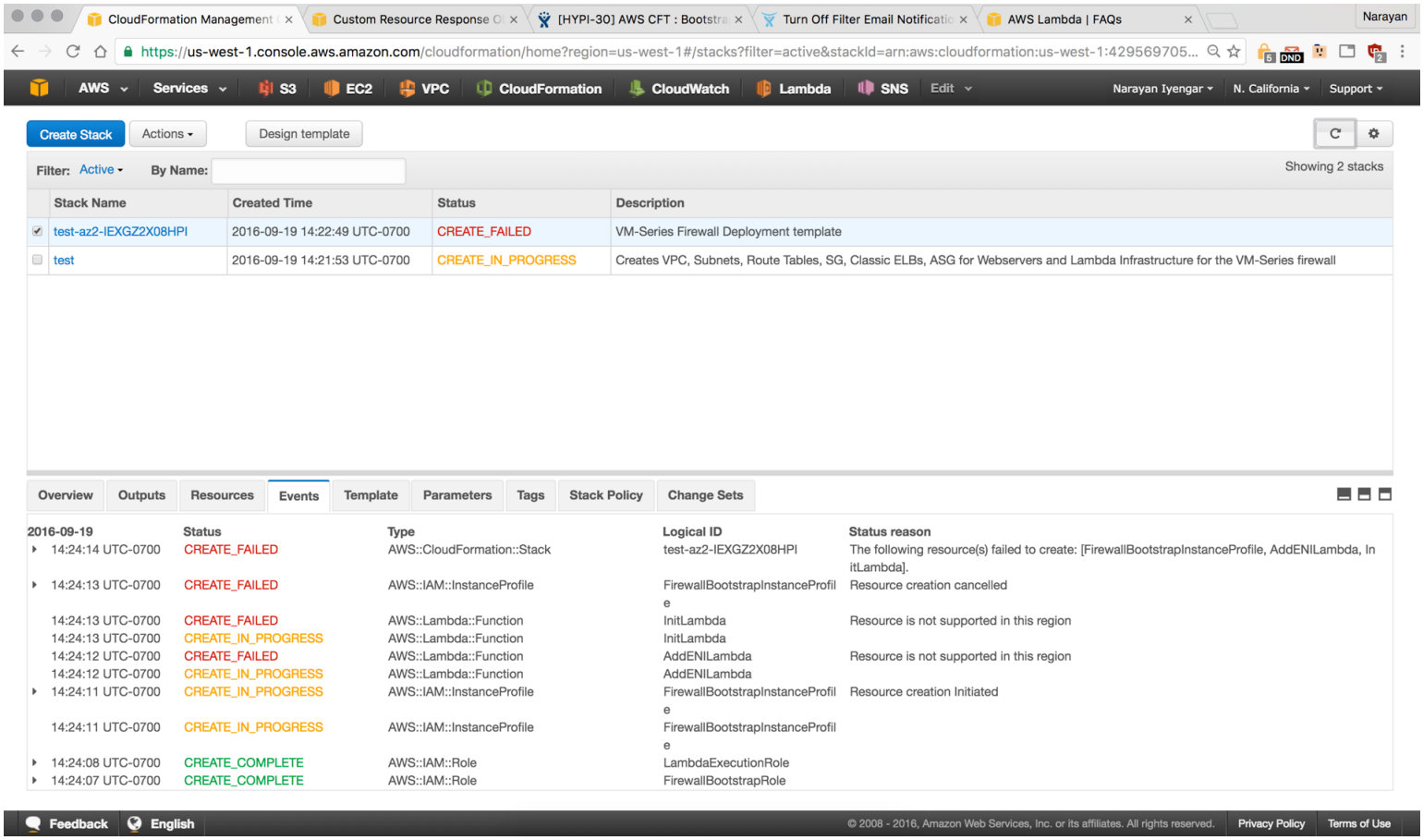
   If you edited the bootstrap.xml file and deleted or modified the NAT policy rules, the firewall may have a misconfiguration, that prevents traffic from being properly routed to the firewall.



Error: AWS Lambda is not supported in the region in which you are deploying the VM-Series Auto Scaling template.

To find the error:

1. On the AWS Management Console, select **CloudFormation**.
2. In the Stack list, select the name of the template that failed to deploy and view the list of **Events**. The error Resource is not supported in this region.



Error: Failure to successfully create a resource with a message such as:

```
Embedded stack arn:aws:cloudformation:<AWS region>:290198859335:stack/<name of your stack> was not successfully created: The following resource(s) failed to create:[ResourceName].
```

To find the errors:

1. On the AWS Management Console, select **CloudWatch**.
2. Click on **Logs** and then select **Lambda function** on the right. You'll see one or more log streams.
3. Search for [ERROR] and [CRITICAL].

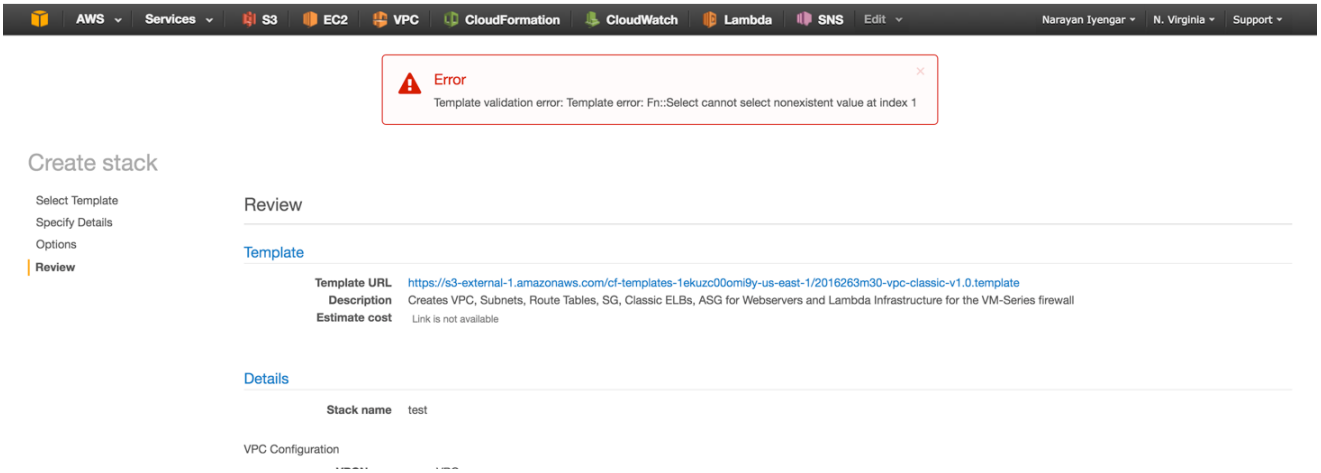
The following example shows that the ELB specified was not found:

Error: Failure to launch the VM-Series Auto Scaling template because of a missing required parameter or not specifying the AWS Availability Zones for the template.

To find the error:

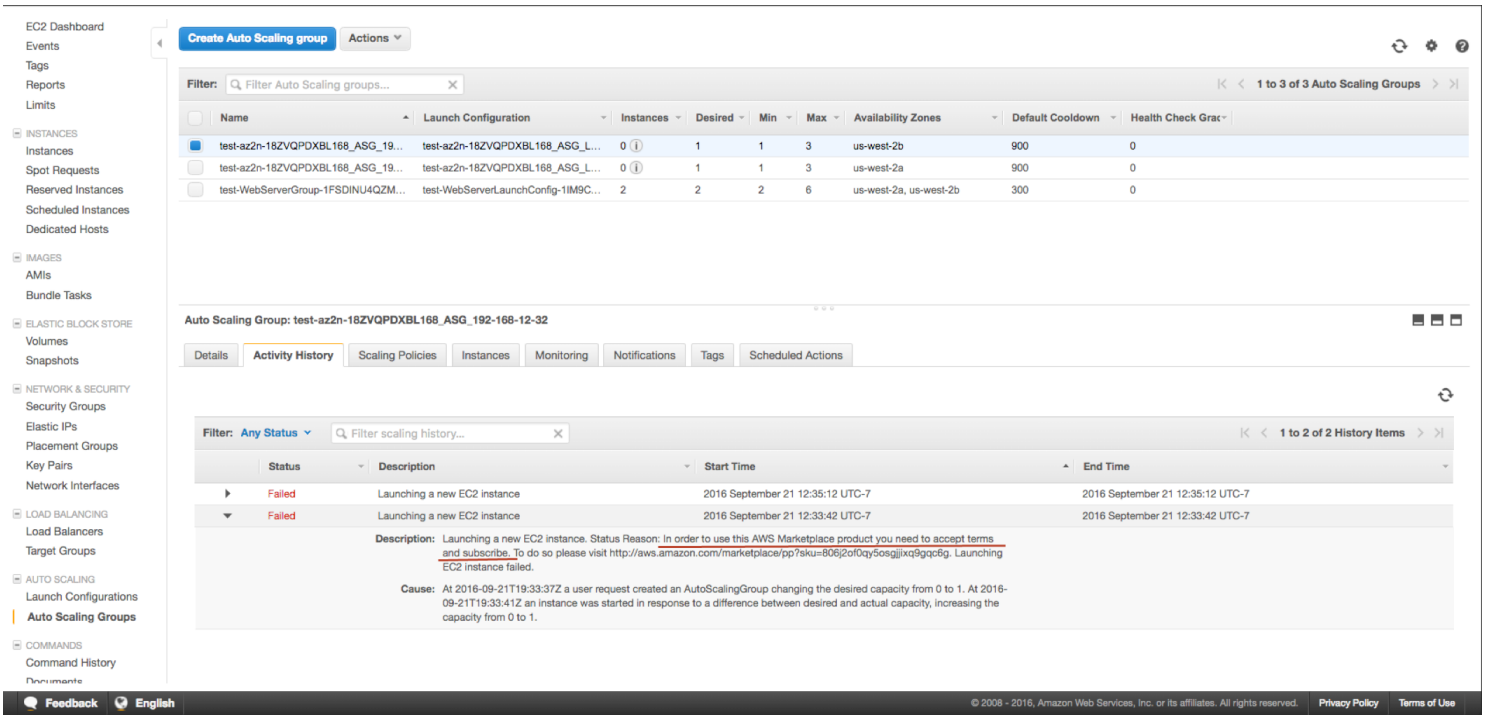
1. On the AWS Management Console, select **CloudFormation**.

2. In the Stack list, select the name of the template that failed to deploy. A generic template validation error displays.



Error: Failure to launch the VM-Series Auto Scaling template because you did not accept the End User License Agreement (EULA) for the PAYG VM-Series Firewall Bundle you are deploying.

1. On the EC2 Dashboard, select **Auto Scaling Groups**.
2. Check the details on the failure to launch the firewalls in the ASG. The error indicates that you must accept the terms for deploying the VM-Series firewalls.



List of Attributes Monitored on the AWS VPC

You can monitor up to a total of 32 attributes—14 pre-defined and 18 user-defined as key value pairs. The following attributes (or tag names) are available as match criteria for dynamic address groups.

Attribute	Format
Architecture	Architecture.<Architecture string>
Guest OS	GuestOS.<guest OS name>
Image ID	ImageId.<ImageId string>
Instance ID	InstanceId.<InstanceId string>
Instance State	InstanceState.<instance state>
Instance Type	InstanceType.<instance type>
Key Name	KeyName.<KeyName string>
Placement—Tenancy, Group Name, Availability	Placement.Tenancy.<string> Placement.GroupName.<string> Placement.AvailabilityZone.<string>
Private DNS Name	PrivateDnsName.<Private DNS Name>
Public DNS Name	PublicDnsName.<Public DNS Name>
Subnet ID	SubnetID.<subnetID string>
Tag (key, value)	aws-tag.<key>.<value> Maximum of 18 of these tags are supported per instance
VPC ID	VpcId.<VpcId string>

IAM Permissions Required for Monitoring the AWS VPC

In order to enable VM Monitoring the user's AWS login credentials tied to the AWS Access Key and Secret Access Key must have permissions for the attributes listed above. These privileges allow the firewall to initiate API calls for monitoring the virtual machines in the AWS VPC.

The IAM policy associated with the user must either have global read-only access such as AmazonEC2ReadOnlyAccess, or must include individual permissions for all of the monitored attributes. The following IAM policy example lists the permissions for initiating the API actions for monitoring the resources in the AWS VPC:

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeKeyPairs",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeRegions",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVpcs"
            ],
            "Resource": [
                "*"
            ]
}
    ]
}
```

Set Up the VM-Series Firewall on KVM

Kernel-based Virtual Machine (KVM) is an open-source virtualization module for servers running Linux distributions. The VM-Series firewall can be deployed on a Linux server that is running the KVM hypervisor.

This guide assumes that you have an existing IT infrastructure that uses Linux and have the foundation for using Linux/Linux tools. The instructions only pertain to deploying the VM-Series firewall on KVM.

> VM-Series on KVM— Requirements and Prerequisites
> Supported Deployments on KVM
> Install the VM-Series Firewall on KVM
> Performance Tuning of the VM-Series for KVM

VM-Series on KVM— Requirements and Prerequisites

Table 2: VM-Series on KVM System Requirements

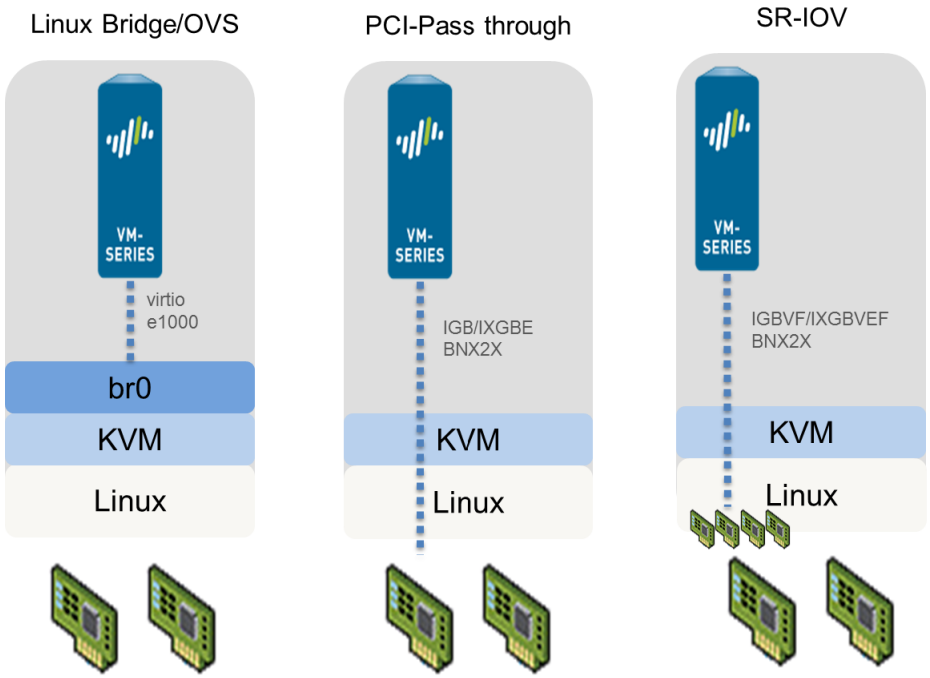
Requirements	Description
Hardware Resources	See VM-Series System Requirements for the minimum hardware requirements for your VM-Series model.

Software Versions	• Ubuntu:
	  • 14.04 LTS (QEMU-KVM 2.0.0 and libvirt 1.2.2)
	  • 16.04 LTS (QEMU-KVM 2.5.0 and libvirt 1.3.1)
	• CentOS/RedHat Enterprise Linux: 7.2 (QEMU-KVM 1.5.3 and libvirt 2.0.0)

Network Interfaces—Network Interface Cards and Software Bridges	The VM-Series on KVM supports a total of 25 interfaces— 1 management interface and a maximum of 24 network interfaces for data traffic.
	VM-Series deployed on KVM supports software-based virtual switches such as the Linux bridge or the Open vSwitch bridge, and direct connectivity to PCI passthrough or an SR-IOV capable adapter.
	If you plan to establish connectivity using PCI-passthrough or SR-IOV, you cannot configure a vSwitch on the physical port used for SR-IOV or PCI-passthrough. To communicate with the host or other virtual machines on the network, the VM-Series firewall must have exclusive access to the physical port and associated virtual functions (VFs) on that interface.
	• On the Linux bridge and OVS, the e1000 and virtio drivers are supported; the default driver rtl8139 is not supported.
	• Open vSwitch version support:
	  • Ubuntu 14.04 LTS: OVS 1.9.3 and OVS 2.3.1
	  • Ubuntu 16.04 LTS: OVS 2.5.0
	  • Ubuntu 16.04 LTS with OVS-DPDK: OVS 2.5.1
	  • CentOS/RHEL 7.2: OVS 2.5.0
	• For PCI passthrough/SR-IOV support, the VM-Series firewall has been tested for the following network cards:
	  • Intel 82576 based 1G NIC: SR-IOV support on all supported Linux distributions; PCI-passthrough support
	  • Intel 82599 based 10G NIC: SR-IOV support on all supported Linux distributions; PCI-passthrough support
	  • Broadcom 57112 and 578xx based 10G NIC: SR-IOV support on all supported Linux distributions; No PCI-passthrough support.
	  • Drivers: igb; ixgbe; bnx2x
	  • Drivers: igbvf; ixgbevf; bnx2x

Requirements	Description
	SR-IOV capable interfaces assigned to the VM-Series firewall, must be configured as Layer 3 interfaces or as HA interfaces.
Data Plane Development Kit (DPDK) Support	DPDK is enabled by default on VM-Series firewalls on KVM if one of the following NIC drivers is used: • Virtual Driver: virtio • NIC Drivers: ixgbe, ixgbevf, i40e, i40evf

Options for Attaching the VM-Series on the Network



- With a Linux bridge or OVS, data traffic uses the software bridge to connect guests on the same host. For external connectivity, data traffic uses the physical interface to which the bridge is attached.
- With PCI passthrough, data traffic is passed directly between the guest and the physical interface to which it is attached. When the interface is attached to a guest, it is not available to the host or to other guests on the host.
- With SR-IOV, data traffic is passed directly between the guest and the virtual function to which it is attached.

Prerequisites for VM-Series on KVM

Before you install the VM-Series firewall on the Linux server, review the following sections:

- Prepare the Linux Server
- Prepare to Deploy the VM-Series Firewall

Prepare the Linux Server

- Check the Linux distribution version. For a list of supported versions, see VM-Series on KVM System Requirements.
- Verify that you have installed and configured KVM tools and packages that are required for creating and managing virtual machines, such as Libvirt.
- If you want to use a SCSI disk controller to access the disk to which the VM-Series firewall stores data, you must use virsh to attach the virtio-scsi controller to the VM-Series firewall. You can then edit the XML template of the VM-Series firewall to enable the use of the virtio-scsi controller. For instructions, see Enable the Use of a SCSI Controller.

  KVM on Ubuntu 12.04 does not support the virtio-scsi controller.

- Verify that you have set up the networking infrastructure for steering traffic between the guests and the VM-Series firewall and for connectivity to an external server or the Internet. The VM-Series firewall can connect using a Linux bridge, the Open vSwitch, PCI passthrough, or SR-IOV capable network card.
  - Make sure that the link state for all interfaces you plan to use are up, sometimes you have to manually bring them up.
  - Verify the PCI ID of all the interfaces. To view the list, use the command: **`Virsh nodedev-list –tree`**
  - If using a Linux bridge or OVS, verify that you have set up the bridges required to send/receive traffic to/from the firewall. If not, create bridge(s) and verify that they are up before you begin installing the firewall.
  - If using PCI-passthrough or SR-IOV, verify that the virtualization extensions (VT-d/IOMMU) are enabled in the BIOS. For example, to enable IOMMU, `intel_iommu=on` must be defined in /etc/grub.conf. Refer to the documentation provided by your system vendor for instructions.
  - If using PCI-passthrough, ensure that the VM-Series firewall has exclusive access to the interface(s) that you plan to attach to it.

    To allow exclusive access, you must manually detach the interface(s) from the Linux server; Refer to the documentation provided by your network card vendor for instructions.

    To manually detach the interface(s) from the server., use the command:

    `Virsh nodedev-detach <pci id of interface>`

    For example, **`pci_0000_07_10_0`**

    In some cases, in /etc/libvirt/qemu.conf, you may have to uncomment `relaxed_acs_check = 1`.
  - If using SR-IOV, verify that the virtual function capability is enabled for each port that you plan to use on the network card. With SR-IOV, a single Ethernet port (physical function) can be split into multiple virtual functions. A guest can be mapped to one or more virtual functions.

    To enable virtual functions, you need to:

    1. Create a new file in this location: /etc/modprobe.d/

    2. Modify the file using the vi editor to make the functions persistent: vim /etc/modprobe.d/igb.conf

    3. Enable the number of number of virtual functions required: options igb max_vfs=4

    After you save the changes and reboot the Linux server, each interface (or physical function) in this example will have 4 virtual functions.

    Refer to the documentation provided by your network vendor for details on the actual number of virtual functions supported and for instructions to enable it.
- Configure the host for maximum VM-Series performance. Refer to Performance Tuning of the VM-Series for KVM for information about configuring each option.

- Enable DPDK. DPDK allows the host to process packets faster by bypassing the Linux kernel. Instead, interactions with the NIC are performed using drivers and the DPDK libraries. Open vSwitch is required to use DPDK with the VM-Series firewall.
- Enable SR-IOV. Single root I/O virtualization (SR-IOV) allows a single PCIe physical device under a single root port to appear to be multiple separate physical devices to the hypervisor or guest.
- Enable multi-queue support for NICs. Multi-queue virtio-net allows network performance to scale with the number of vCPUs and allows for parallel packet processing by creating multiple TX and RX queues.
- Isolate CPU Resource in a NUMA Node. You can improve performance of VM-Series on KVM by isolating the CPU resources of the guest VM to a single non-uniform memory access (NUMA) node.

Prepare to Deploy the VM-Series Firewall

- ❑ Purchase the VM-Series model and register the authorization code on the Palo Alto Networks Customer Support web site. See Create a Support Account and Register the VM-Series Firewall.
- ❑ Obtain the qcow2 image and save it on the Linux server. As a best practice, copy the image to the folder: /var/lib/libvirt/qemu/images.

  If you plan to deploy more than one instance of the VM-Series firewall, make the required number of copies of the image. Because each instance of the VM-Series firewall maintains a link with the .qcow2 image that was used to deploy the firewall, to prevent any data corruption issues ensure that each image is independent and is used by a single instance of the firewall.

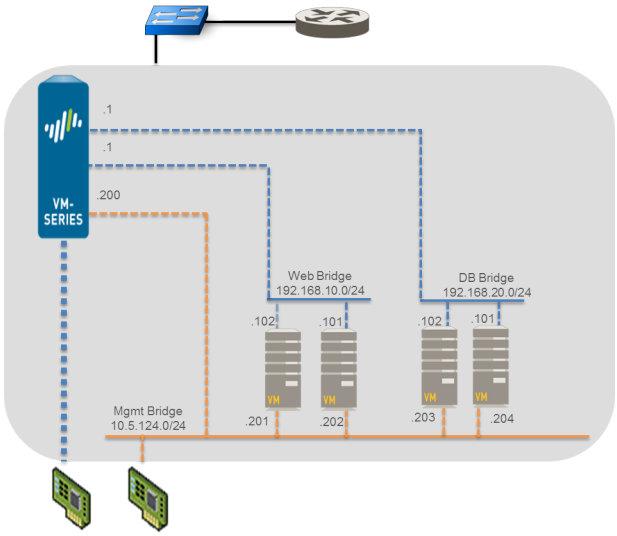
Supported Deployments on KVM

You can deploy a single instance of the VM-Series firewall per Linux host (single tenant) or multiple instances of the VM-Series firewalls on a Linux host. The VM-Series firewall can be deployed with virtual wire, Layer 2, or Layer 3 interfaces. If you plan on using SR-IOV capable interfaces on the VM-Series firewall, you can only configure the interfaces as Layer 3 interfaces.

- Secure Traffic on a Single Host
- Secure Traffic Across Linux hosts

Secure Traffic on a Single Host

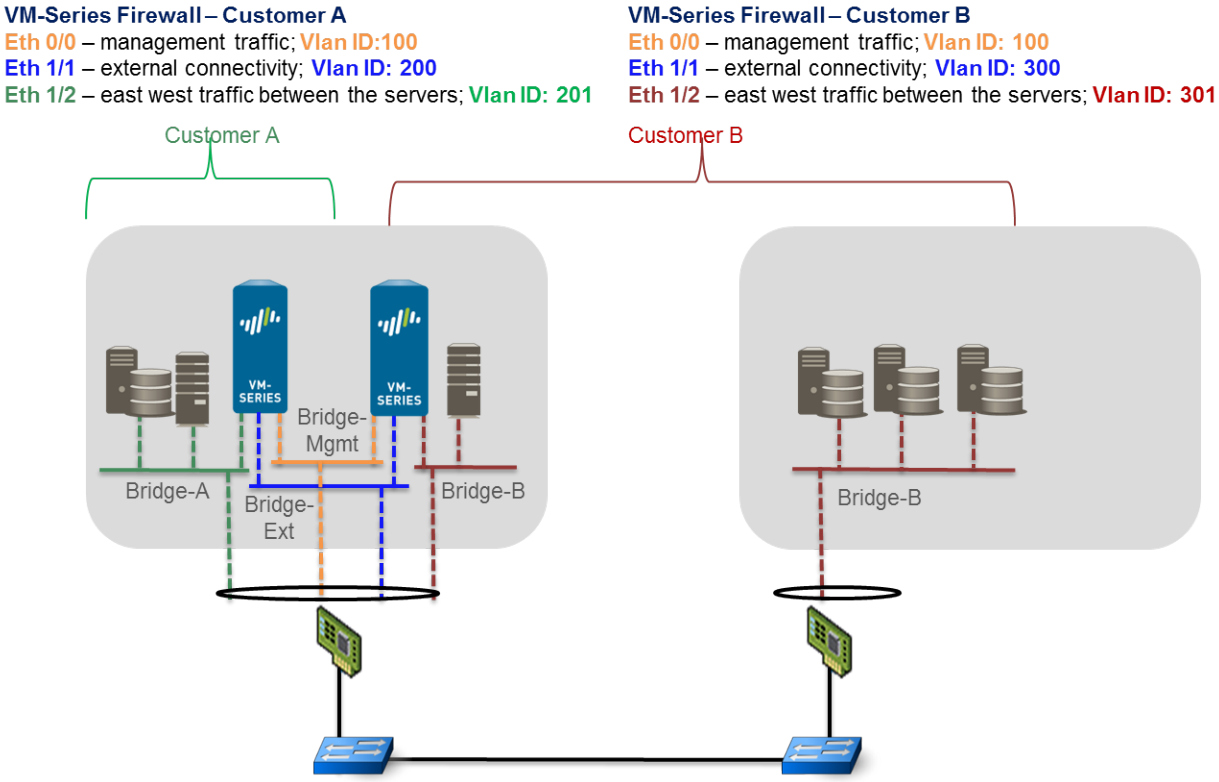
To secure east west traffic across guests on a Linux server, the VM-Series firewall can be deployed with virtual wire, Layer 2, or Layer 3 interfaces. The illustration below shows the firewall with Layer 3 interfaces, where the firewall and the other guests on the server are connected using Linux bridges. In this deployment, all traffic between the web servers and the database servers is routed through the firewall; traffic across the database servers only or across the web servers only is processed by the bridge and is not routed through the firewall.



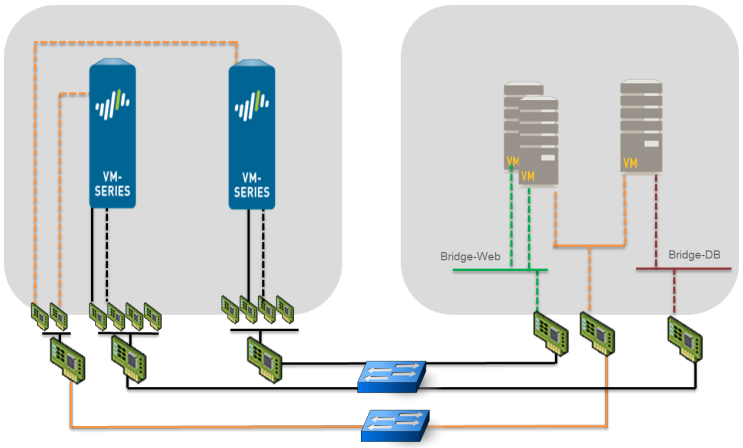
Secure Traffic Across Linux hosts

To secure your workloads, more than one instance of the VM-Series firewalls can be deployed on a Linux host. If, for example, you want to isolate traffic for separate departments or customers, you can use VLAN tags

to logically isolate network traffic and route it to the appropriate VM-Series firewall. In the following example, one Linux host hosts the VM-Series firewalls for two customers, Customer A and Customer B, and the workload for Customer B is spread across two servers. In order to isolate traffic and direct it to the VM-Series firewall configured for each customer, VLANs are used.



In another variation of this deployment, a pair of VM-Series firewalls are deployed in a high availability set up. The VM-Series firewalls in the following illustration are deployed on a Linux server with SR-IOV capable adapters. With SR-IOV, a single Ethernet port (physical function) can be split into multiple virtual functions. Each virtual function attached to the VM-Series firewall is configured as a Layer 3 interface. The active peer in the HA pair secures traffic that is routed to it from guests that are deployed on a different Linux server.



Install the VM-Series Firewall on KVM

The libvirt API that is used to manage KVM includes a host of tools that allow you to create and manage virtual machines. To install the VM-Series firewall on KVM you can use any of the following methods:

- Manually create the XML definition of the VM-Series firewall, then use virsh to import the definition. Virsh is the most powerful tool that allows for full administration of the virtual machine.
- Use virt-install to create the definition for the VM-Series firewall and install it.
- Use the desktop user interface called virt-manager; virt-manager provides a convenient wizard to help you through the installation process.

The following procedure uses virt-manager to install the VM-Series firewall on a server running KVM on RHEL; the instructions for using virsh or virt-install are not included in this document.

If you are deploying several VM-Series firewalls and want to automate the initial configuration on the firewall, see Use an ISO File to Deploy the VM-Series Firewall.

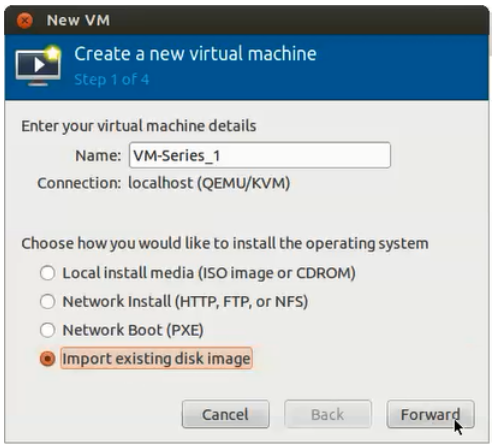
- Provision the VM-Series Firewall on a KVM Host
- Perform Initial Configuration of the VM-Series Firewall on KVM
- Enable the Use of a SCSI Controller
- Verify PCI-ID for Ordering of Network Interfaces on the VM-Series Firewall
- Use an ISO File to Deploy the VM-Series Firewall

Provision the VM-Series Firewall on a KVM Host

Use the following instructions to provision the KVM host for the VM-Series firewall.

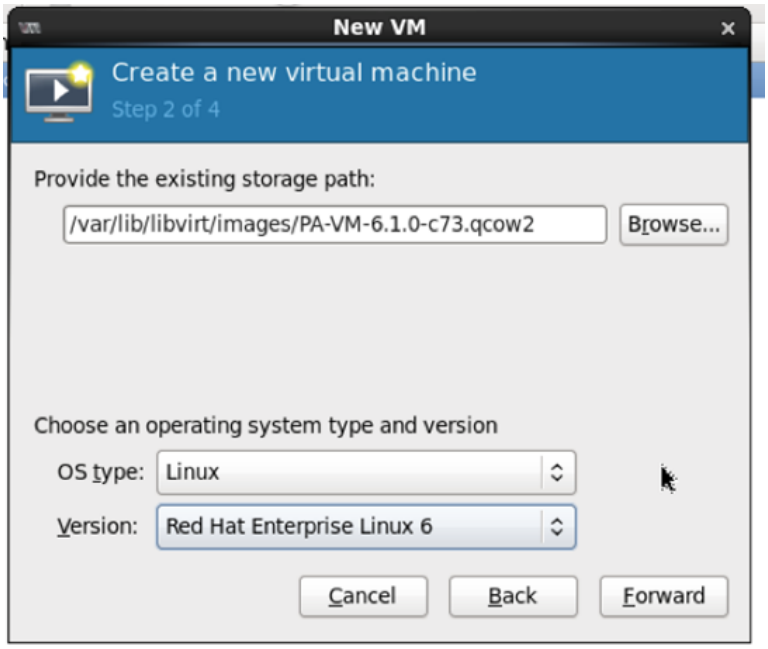
STEP 1 | Create a new virtual machine and add the VM-Series Firewall for KVM image to virt-mgr.

1. On the Virt-manager, select **Create a new virtual machine**.
2. Add a descriptive **Name** for the VM-Series firewall.



3. Select **Import existing disk image**, browse to the image, and set the **OS Type**: Linux and **Version**: Red Hat Enterprise Linux 6.

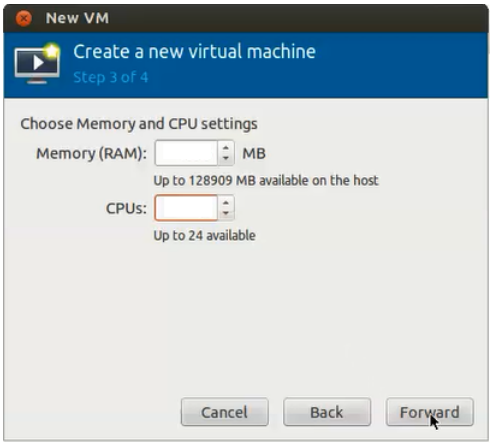
If you prefer, you can leave the OS Type and Version as Generic.



4. To add network adapters for the data interfaces:

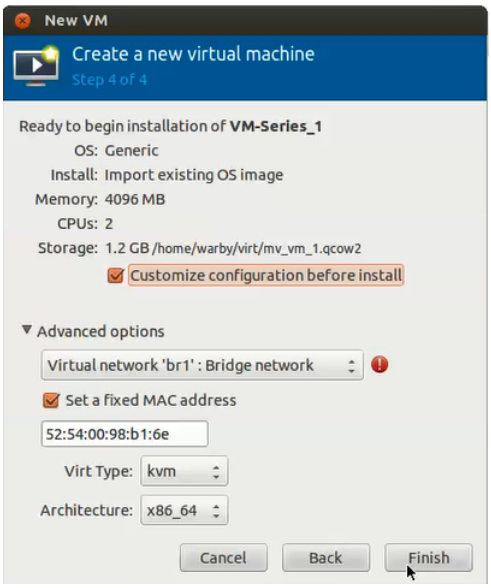
STEP 2 | Configure the memory and CPU settings.

1. Set the **Memory** to the minimum memory based on the VM-Series System Requirements of your VM-Series model.
2. Set **CPU** to the minimum CPUs based on the VM-Series System Requirements of your VM-Series model.



STEP 3 | Enable configuration customization and select the management interface bridge.

1. Select **Customize configuration before install**.
2. Under Advanced options, select the bridge for the management interface, and accept the default settings.

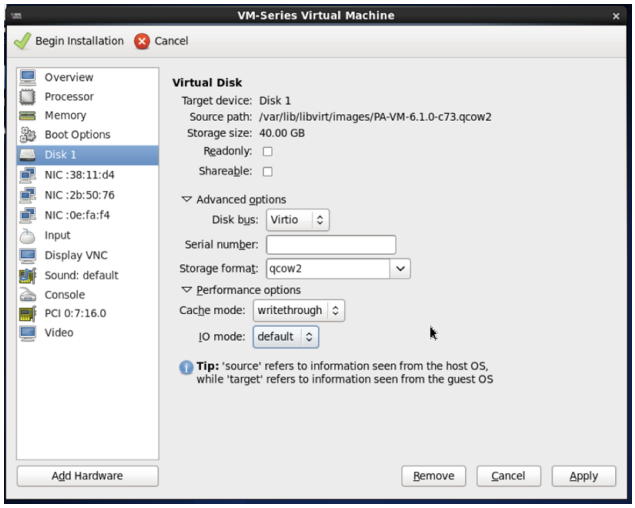


STEP 4 | Configure virtual disk settings.

1. Select **Disk**, expand Advanced options and select **Storage format** — qcow2; **Disk Bus**—Virtio or IDE, based on your set up.

   If you want to use a SCSI disk bus, see Enable the Use of a SCSI Controller.

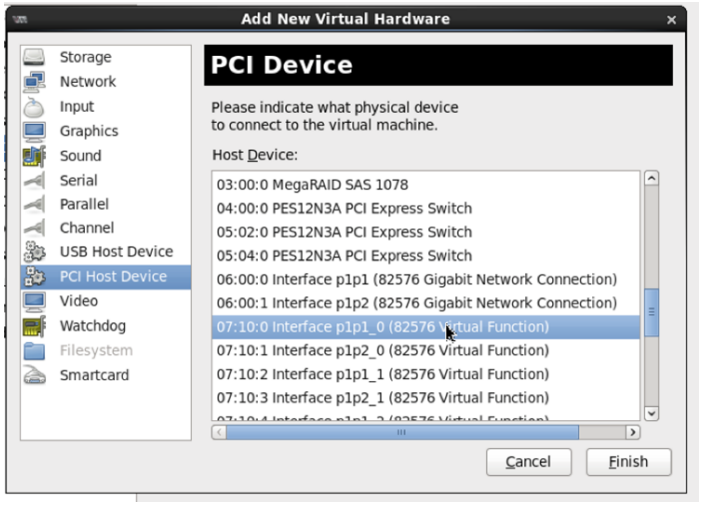
2. Expand Performance options, and set **Cache mode** to **writethrough**. This setting improves installation time and execution speed on the VM-Series firewall.



STEP 5 | Configure network adapters.

1. Select **Add Hardware** > **Network** if you are using a software bridge such as the Linux bridge or the Open vSwitch.
2. For **Host Device**, enter the name of the bridge or select it from the drop down list.
3. To specify the driver, set **Device Model** to e-1000 or virtio. These are the only supported virtual interface types.

4. Select **Add Hardware** > **PCI Host Device** for PCI-passthrough or an SR-IOV capable device.

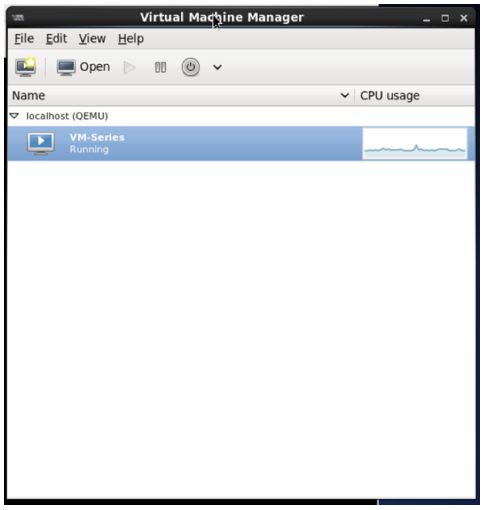


5. In the **Host Device** list, select the interface on the card or the virtual function.
6. Click **Apply** or **Finish**.

STEP 6 | Click **Begin Installation** 

. Wait 5-7 minutes for the installation to complete.

By default, the XML template for the VM-Series firewall is created and stored at etc/libvirt/qemu.



STEP 7 | (Optional) Bootstrap the VM-Series firewall

If you are using bootstrapping to perform the configuration of your VM-Series firewall on KVM, refer to Bootstrap the VM-Series Firewall on KVM. For more information about bootstrapping, see Bootstrap the VM-Series Firewall.

STEP 8 | Configure the network access settings for the management interface.

1. Open a connection to the console.
2. Log into the firewall with username/password: admin/admin.
3. Enter configuration mode with the following command:

```
configure
```

4. Use the following commands to configure the management interface:

   1. ```
      set deviceconfig system type static
      ```
   2. ```
      set deviceconfig system ip-address <Firewall-IP> netmask <netmask>
       default-gateway <gateway-IP> dns-setting servers primary <DNS-IP>
      ```

      where <*Firewall-IP*> is the IP address you want to assign to the management interface, <*netmask*> is the subnet mask, <*gateway-IP*> is the IP address of the network gateway, and <*DNS-IP*> is the IP address of the DNS server.
   3. ```
      commit
      ```

STEP 9 | Verify which ports on the host are mapped to the interfaces on the VM-Series firewall. In order to verify the order of interfaces on the Linux host, see Verify PCI-ID for Ordering of Network Interfaces on the VM-Series Firewall.

To make sure that traffic is handled by the correct interface, use the following command to identify which ports on the host are mapped to the ports on the VM-Series firewall.

```
admin@PAN-VM> debug show vm-series interfaces all
Phoenix_interface    Base-OS_port       Base-OS_MAC PCI-ID
 mgt                        eth0          52:54:00:d7:91:52 0000:00:03.0
 Ethernet1/1             eth1          52:54:00:fe:8c:80 0000:00:06.0
```
```

```
Ethernet1/2             eth2          0e:c6:6b:b4:72:06 0000:00:07.0
Ethernet1/3             eth3          06:1b:a5:7e:a5:78 0000:00:08.0
Ethernet1/4             eth4          26:a9:26:54:27:a1 0000:00:09.0
Ethernet1/5             eth5          52:54:00:f4:62:13 0000:00:10.0
```

STEP 10 | Access the web interface of the VM-Series firewall and configure the interfaces and define security rules and NAT rules to safely enable the applications that you want to secure.

Refer to the PAN-OS Administrator's Guide.

Perform Initial Configuration of the VM-Series Firewall on KVM

Use the virtual appliance console on the KVM server to set up network access to the VM-Series firewall. By default, the VM-Series firewall uses DHCP to obtain an IP address for the management interface. However, you can assign a static IP address. After completing the initial configuration, access the web interface to complete further configurations tasks. If you have Panorama for central management, refer to the Panorama Administrator's Guide for more information on managing the device using Panorama.

If you are using bootstrapping to perform the configuration of your VM-Series firewall on KVM, refer to Bootstrap the VM-Series Firewall on KVM.

For general information about bootstrapping, see Bootstrap the VM-Series Firewall.

STEP 1 | Gather the required information from your network administrator.

- Management port IP address
- Netmask
- Default gateway
- DNS server IP address

STEP 2 | Access the console of the VM-Series firewall.

1. Select the **Console** tab on the KVM server for the VM-Series firewall, or right-click the VM-Series firewall and select **Open Console**.
2. Press enter to access the login screen.
3. Enter the default username/password (admin/admin) to log in.
4. Enter **`configure`** to switch to configuration mode.

STEP 3 | Configure the network access settings for the management interface. You should restrict access to the firewall and isolate the management network. Additionally, do not make the allowed network larger than necessary and never configure the allowed source as 0.0.0.0/0.

Enter the following commands:

```
set deviceconfig system type static
```

```
set deviceconfig system ip-address <Firewall-IP> netmask <netmask>
default-gateway <gateway-IP> dns-setting servers primary <DNS-IP>
```

where <*Firewall-IP*> is the IP address you want to assign to the management interface, <*netmask*> is the subnet mask, <*gateway-IP*> is the IP address of the network gateway, and <*DNS-IP*> is the IP address of the DNS server.

STEP 4 | Commit your changes and exit the configuration mode.

Enter **`commit`**.

Enter **exit**.

STEP 5 | Verify which ports on the host are mapped to the interfaces on the VM-Series firewall. In order to verify the order of interfaces on the Linux host, see Verify PCI-ID for Ordering of Network Interfaces on the VM-Series Firewall.

To make sure that traffic is handled by the correct interface, use the following command to identify which ports on the host are mapped to the ports on the VM-Series firewall.

```
admin@PAN-VM> debug
show vm-series interfaces all
Phoenix_interface    Base-OS_port       Base-OS_MAC PCI-ID
 mgt                        eth0          52:54:00:d7:91:52 0000:00:03.0
 Ethernet1/1             eth1          52:54:00:fe:8c:80 0000:00:06.0
 Ethernet1/2             eth2          0e:c6:6b:b4:72:06 0000:00:07.0
 Ethernet1/3             eth3          06:1b:a5:7e:a5:78 0000:00:08.0
 Ethernet1/4             eth4          26:a9:26:54:27:a1 0000:00:09.0
 Ethernet1/5             eth5          52:54:00:f4:62:13 0000:00:10.0
```

STEP 6 | Access the web interface of the VM-Series firewall and configure the interfaces and define security rules and NAT rules to safely enable the applications that you want to secure.

Refer to the PAN-OS Administrator's Guide.

Enable the Use of a SCSI Controller

If you want the VM-Series firewall to use the disk bus type SCSI to access the virtual disk, use the following instructions to attach the virtio scsi controller to the firewall and then enable the use of the virtio-scsi controller.

KVM on Ubuntu 12.04 does not support the virtio-scsi controller; the virtio-scsi controller can only be enabled on the VM-Series firewall running on RHEL or CentOS.

This process requires virsh because Virt manager does not support the virtio-scsi controller.

STEP 1 | Create an XML file for the SCSI controller. In this example, it is called virt-scsi.xml.

```
[root@localhost~]# cat /root/virt-scsi.xml
<controller type='scsi' index='0' model='virtio-scsi'>
<address type='pci' domain='0x0000' bus='0x00' slot='0x0b'function='0x0'/>
</controller>
```

Make sure that the slot used for the virtio-scsi controller does not conflict with another device.

STEP 2 | Associate this controller with the XML template of the VM-Series firewall.

```
[root@localhost~]# virsh attach-device --config <VM-Series_name> /root/virt-
scsi.xml
Device attached successfully
```

STEP 3 | Enable the firewall to use the SCSI controller.

```
[root@localhost~]# virsh attach-disk <VM-Series_name>/var/lib/libvirt/
images/PA-VM-6.1.0-c73.qcow2
sda --cache none --persistent
Disk attached successfully
```

STEP 4 | Edit the XML template of the VM-Series firewall. In the XML template, you must change the target disk and the disk bus, used by the firewall.

By default, the XML template is stored at etc/libvirt/qemu.

```
<disk type='file' device='disk'>
      <driver name='qemu' type='qcow2' cache='writeback'/>
      <source file='/var/lib/libvirt/images/PA-VM-7.0.0-c73.qcow2'/>
      <target dev='sda' bus='scsi'/>
      <address type='drive' controller='0' bus='0' target='0' unit='0'/>
</disk>
```

Verify PCI-ID for Ordering of Network Interfaces on the VM-Series Firewall

Regardless of whether you use a virtual interfaces (Linux/OVS bridge) or PCI devices (PCI-passthrough or SR-IOV capable adapter) for connectivity to the VM-Series firewall, the VM-Series firewall treats the interface as a PCI device. The assignment of an interface on the VM-Series firewall is based on PCI-ID which is a value that combines the bus, device or slot, and function of the interface. The interfaces are ordered starting at the lowest PCI-ID, which means that the management interface (eth0) of the firewall is assigned to the interface with the lowest PCI-ID.

Let's say you assign four interfaces to the VM-Series firewall, three virtual interfaces of type virtio and e1000 and the fourth is a PCI device. To view the PCI-ID for each interface, enter the command **virsh dumpxml $ domain <name of the VM-Series firewall>** on the Linux host to view the list of interfaces attached to the VM-Series firewall. In the output, check for the following networking configuration:

```
<interface type='bridge'>
      <mac address='52:54:00:d7:91:52'/>
      <source bridge='mgmt-br'/>
      <model type='virtio'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
 function='0x0'/>
    </interface>

   <interface type='bridge'>
      <mac address='52:54:00:f4:62:13'/>
      <source bridge='br8'/>
      <model type='e1000'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x10'
 function='0x0'/>
    </interface>

   <interface type='bridge'>
      <mac address='52:54:00:fe:8c:80'/>
      <source bridge='br8'/>
      <model type='e1000'/>
```

```
      <address type='pci' domain='0x0000' bus='0x00' slot='0x06'
function='0x0'/>
   </interface>

  <hostdev mode='subsystem' type='pci' managed='yes'>
     <source>
       <address domain='0x0000' bus='0x08' slot='0x10' function='0x1'/>
     </source>
     <address type='pci' domain='0x0000' bus='0x00' slot='0x07'
function='0x0'/>
   </hostdev>
```

In this case, the PCI-ID of each interface is as follows:

- First virtual interface PCI-ID is 00:03:00
- Second virtual interface PCI-ID is 00:10:00
- Third virtual interface PCI-ID is 00:06:00
- Fourth interface PCI-ID is 00:07:00

Therefore, on the VM-Series firewall, the interface with PCI-ID of 00:03:00 is assigned as eth0 (management interface), the interface with PCI-ID 00:06:00 is assigned as eth1 (ethernet1/1), the interface with PCI-ID 00:07:00 is eth2 (ethernet1/2) and the interface with PCI-ID 00:10:00 is eth3 (ethernet1/3).

Use an ISO File to Deploy the VM-Series Firewall

If you want to pass a script to the VM-Series firewall at boot time, you can mount a CD-ROM with an ISO file. The ISO file allows you to define a bootstrap XML file that includes the initial configuration parameters for the management port of the firewall. The VM-Series firewall on first boot checks for the **bootstrap-networkconfig.xml** file, and uses the values defined in it.

If a single error is encountered in parsing the bootstrap file, the VM-Series firewall will reject all the configuration in this file and boot with default values.

STEP 1 | Create the XML file and define it as a virtual machine instance.

For a sample file, see Sample XML file for the VM-Series Firewall.

In this example, the VM-Series firewall is called PAN_Firewall_DC1.

For example:

```
user-PowerEdge-R510:~/kvm_script$ sudo vi /etc/libvirt/qemu/
PAN_Firewall_DC1.xml
user-PowerEdge-R510:~/kvm_script$ sudo virsh define/etc/libvirt/qemu/
PAN_Firewall_DC1.xml
Domain PAN_Firewall_DC1_bootstp defined from /etc/libvirt/qemu/
PAN_Firewall_DC1.xml
user-PowerEdge-R510:~/kvm_script$ sudo virsh -q attach-interface
 PAN_Firewall_DC1_bootstp bridge br1 --model=virtio --persistent
user-PowerEdge-R510:~/kvm_script$ virsh list --all
 Id    Name                           State
----------------------------------------------
 -    PAN_Firewall_DC1_bootstp     shut off
```

STEP 2 | Create the bootstrap XML file.

You can define the initial configuration parameters in this file and name it bootstrap-networkconfig.

If you do not want to include a parameter, for example panorama-server-secondary. Delete the entire line from the file. If you leave the IP address field empty, the file will not be parsed successfully.

Use the following example as a template for the bootstrap-networkconfig file. The bootstrap-networkconfig file can include the following parameters only:

```
<vm-initcfg>
<hostname>VM_ABC_Company</hostname>
<ip-address>10.5.132.162</ip-address>
<netmask>255.255.254.0</netmask>
<default-gateway>10.5.132.1</default-gateway>
<dns-primary>10.44.2.10</dns-primary>
<dns-secondary>8.8.8.8</dns-secondary>
<panorama-server-primary>10.5.133.4</panorama-server-primary>
<panorama-server-secondary>10.5.133.5</panorama-server-secondary>
</vm-initcfg>
```

STEP 3 | Create the ISO file. In this example, we use mkisofs.

Save the ISO file in the images directory (/var/lib/libvirt/image) or the qemu directory (/etc/libvirt/qemu) to ensure that the firewall has read access to the ISO file.

For example:

```
# mkisofs -J -R -v -V "Bootstrap" -A "Bootstrap" -ldots -l -allow-lowercase
 -allow-multidot -o <iso-filename> bootstrap-networkconfig.xml
```

STEP 4 | Attach the ISO file to the CD-ROM.

For example:

```
# virsh -q attach-disk <vm-name> <iso-filename> sdc --type cdrom --mode
 readonly –persistent\
```

Sample XML file for the VM-Series Firewall

```
<?xml version="1.0"?>
<domain type="kvm">
<name>PAN_Firewall_DC1</name>
<memory>4194304</memory>
<currentMemory>4194304</currentMemory>
<vcpu placement="static">2</vcpu>
<os>
<type arch="x86_64">hvm</type>
<boot dev="hd"/>
</os>
<features>
<acpi/>
<apic/>
<pae/>
</features>
<clock offset="utc"/>
<on_poweroff>destroy</on_poweroff>
<on_reboot>restart</on_reboot>
```

```
<on_crash>restart</on_crash>
<devices>
<emulator>/usr/libexec/qemu-kvm</emulator>
<disk type="file" device="disk">
<driver type="qcow2" name="qemu"/>
<source file="/var/lib/libvirt/images/panos-kvm.qcow2"/>
<target dev="vda" bus="virtio"/>
</disk>
<controller type="usb" index="0"/>
<controller type="ide" index="0"/>
<controller type="scsi" index="0"/>
<serial type="pty">
<source path="/dev/pts/1"/>
<target port="0"/>
<alias name="serial0"/>
</serial>
<console type="pty" tty="/dev/pts/1">
<source path="/dev/pts/1"/>
<target type="serial" port="0"/>
<alias name="serial0"/>
</console>
<input type="mouse" bus="ps2"/>
<graphics type="vnc" port="5900" autoport="yes"/>
</devices>
</domain>
```

*To modify the number of vCPUs assigned on the VM-Series firewall, change the value **2** to **4** or **8** vCPUs in this line of the sample XML file:*

```
<vcpu placement="static">2</vcpu>
```

Performance Tuning of the VM-Series for KVM

The VM-Series firewall for KVM is a high-performance appliance but may require tuning of the hypervisor to achieve the best results. This section describes some best practices and recommendations for facilitating the best performance of the VM-Series firewall.

By default, KVM uses a linux bridge for VM networking. However, the best performance in a virtual environment is realized with dedicated I/O interfaces (PCI passthrough or SR-IOV). If a virtual switch is required, use a performance-optimized virtual switch (such as Open vSwitch with DPDK).

Install KVM and Open vSwitch on Ubuntu 16.04.1 LTS

For ease of installation, Ubuntu 16.04.1 LTS is recommended for use as the KVM hypervisor platform.

STEP 1 | Install KVM and OVS.

1. Log in to the Ubuntu CLI.
2. Execute the following commands:

```
$ sudo apt-get install qemu-kvm libvirt-bin ubuntu-vm-builder bridge-
utils
$ sudo apt-get install openvswitch-switch
```

STEP 2 | Check and compare the versions of relevant packages.

Execute the following commands:

```
$ virsh --version 1.3.1
$ libvirtd --version
libvirtd (libvirt) 1.3.1
$ /usr/bin/qemu-system-x86_64 --version
QEMU emulator version 2.5.0 (Debian
1:2.5+dfsg-5ubuntu10.6), Copyright (c) 2003-2008
Fabrice Bellard
$ ovs-vsctl --version
ovs-vsctl (Open vSwitch) 2.5.0
Compiled Mar 10 2016 14:16:49
DB Schema 7.12.1
```

Enable Open vSwitch on KVM

Enable OVS by modifying the guest XML definition network settings.

Modify the guest XML definition as follows.

```
[...]
    <interface type='bridge'>
```

```
      <mac address='52:54:00:fb:00:01'/>
      <source bridge='ovsbr0'/>
      <virtualport type='openvswitch'/>
      <model type='virtio'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
 function='0x0'/>
   </interface>
[...]
```

Integrate Open vSwitch with DPDK

To integrate Open vSwitch (OVS) with DPDK, you must install the required components and then configure OVS. DPDK is enabled by default on the VM-Series firewall for KVM.

- Install QEMU, DPDK, and OVS on Ubuntu
- Configure OVS and DPDK on the Host
- Edit the VM-Series Firewall Configuration File

Install QEMU, DPDK, and OVS on Ubuntu

Before you can enable DPDK on OVS, you must install QEMU 2.5.0, DPDK 2.2.0, and OVS 2.5.1. Complete the following procedures to install the components.

STEP 1 | Log in to the KVM host CLI.

STEP 2 | Install QEMU 2.5.0 by executing the following commands:

```
apt-get install build-essential gcc pkg-config glib-2.0 libglib2.0-dev
 libsdl1.2-dev
libaio-dev libcap-dev libattr1-dev libpixman-1-dev
apt-get build-dep qemu
apt-get install qemu-kvm libvirt-bin
wget http://wiki.qemu.org/download/qemu-2.5.0.tar.bz2
tar xjvf qemu-2.5.0.tar.bz2
cd qemu-2.5.0
./configure
make
make install
```

STEP 3 | Install dpdk-2.2.0.

1. Execute the following commands:

```
wget http://dpdk.org/browse/dpdk/snapshot/dpdk-2.2.0.tar.gz
tar xzvf dpdk-2.2.0.tar.gz
cd dpdk-2.2.0
vi config/common_linuxapp
```

2. Change `CONFIG_RTE_APP_TEST=y` to **`CONFIG_RTE_APP_TEST=n`**
3. Change `CONFIG_RTE_BUILD_COMBINE_LIBS=n` to **`CONFIG_RTE_BUILD_COMBINE_LIBS=y`**
4. Execute the following command:

```
vi GNUmakefile
```

5. Change `ROOTDIRS-y := lib drivers app` to **`ROOTDIRS-y := lib drivers`**
6. Execute the following command:

```
make install T=x86_64-native-linuxapp-gcc
```

STEP 4 | Install OVS 2.5.1 by executing the following commands:

```
wget http://openvswitch.org/releases/openvswitch-2.5.1.tar.gz
tar xzvf openvswitch-2.5.1.tar.gz
cd openvswitch-2.5.1
./configure –with-dpdk=”/root/dpdk-2.2.0/x86_64-native-linuxapp-gcc/”
make
make install
```

Configure OVS and DPDK on the Host

After installing the necessary components to support OVS and DPDK, you must configure the host to use OVS and DPDK.

STEP 1 | Log in to the KVM host CLI.

STEP 2 | If you are replacing or reconfiguring an existing OVS-DPDK setup, execute the following commands to reset any previous configuration. Repeat the command for each interface.

```
rm /usr/local/var/run/openvswitch/<interface-name>
```

STEP 3 | Configure initial huge pages for OVS.

```
echo 16384 > /sys/kernel/mm/hugepages/hugepages-2048kB/nr_hugepages
```

STEP 4 | Mount huge pages for QEMU:

```
mkdir /dev/hugepages
mkdir /dev/hugepages/libvirt
mkdir /dev/hugepages/libvirt/qemu
mount -t hugetlbfs hugetlbfs /dev/hugepages/libvirt/qemu
```

STEP 5 | Use the following command to kill any currently existing OVS daemon.

```
killall ovsdb-server ovs-vswitchd
```

STEP 6 | Create directories for the OVS daemon.

```
mkdir -p /usr/local/etc/openvswitch
mkdir -p /usr/local/var/run/openvswitch
```

STEP 7 | Clear old directories.

```
rm -f /var/run/openvswitch/vhost-user*
rm -f /usr/local/etc/openvswitch/conf.db
```

STEP 8 | Initialize the configuration database.

```
ovsdb-tool create /usr/local/etc/openvswitch/conf.db\
/usr/local/share/openvswitch/vswitch.ovsschema
```

STEP 9 | Create an OVS DB server.

```
ovsdb-server --remote=punix:/usr/local/var/run/openvswitch/db.sock \
--remote=db:Open_vSwitch,Open_vSwitch,manager_options \
--private-key=db:Open_vSwitch,SSL,private_key \
--certificate=db:Open_vSwitch,SSL,certificate \
--bootstrap-ca-cert=db:Open_vSwitch,SSL,ca_cert \
--pidfile --detach
```

STEP 10 | Initialize OVS.

```
ovs-vsctl --no-wait init
```

STEP 11 | Start the database server.

```
export DB_SOCK=/usr/local/var/run/openvswitch/db.sock
```

STEP 12 | Install the igb_uio module (network device driver) for DPDK.

```
cd ~/dpdk-2.2.0/x86_64-native-linuxapp-gcc/kmod
modprobe uio
insmod igb_uio.ko
cd ~/dpdk-2.2.0/tools/
```

STEP 13 | Enable DPDK on interfaces using PCI-ID or interface name.

```
./dpdk_nic_bind.py --bind=igb_uio <your first data interface>
./dpdk_nic_bind.py --bind=igb_uio <your second data interface>
```

STEP 14 | Start the OVS daemon in DPDK mode. You can change the number of cores for ovs-vswitchd. By changing -c 0x1 to -c 0x3, you can have two core run this daemon.

```
ovs-vswitchd --dpdk -c 0x3 -n 4 -- unix:$DB_SOCK --pidfile --detach
echo 50000 > /sys/kernel/mm/hugepages/hugepages-2048kB/nr_hugepages
```

STEP 15 | Create the OVS bridge and attach ports to the OVS bridge.

```
ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0 datapath_type=netdev
ovs-vsctl add-port ovs-br0 dpdk0 -- set Interface dpdk0 type=dpdk
ovs-vsctl add-br ovs-br1 -- set bridge ovs-br1 datapath_type=netdev
ovs-vsctl add-port ovs-br1 dpdk1 -- set Interface dpdk1 type=dpdk
```

STEP 16 | Create DPDK vhost user ports for OVS.

```
ovs-vsctl add-port ovs-br0 vhost-user1 -- set Interface vhost-user1
 type=dpdkvhostuser
ovs-vsctl add-port ovs-br1 vhost-user2 -- set Interface vhost-user2
 type=dpdkvhostuser
```

STEP 17 | Set the number of hardware queues of the NIC used by the host.

```
ovs-vsctl set Open_vSwitch . other_config:n-dpdk-rxqs=8
ovs-vsctl set Open_vSwitch . other_config:n-dpdk-txqs=8
```

STEP 18 | Set the CPU mask used for OVS.

```
ovs-vsctl set Open_vSwitch . other_config:pmd-cpu-mask=0xffff
```

STEP 19 | Set the necessary permissions for DPDK vhost user ports. In the example below, 777 is used to give read, write, and executable permissions.

```
chmod 777 /usr/local/var/run/openvswitch/vhost-user1
chmod 777 /usr/local/var/run/openvswitch/vhost-user2
chmod 777 /dev/hugepages/libvirt/qemu
```

Edit the VM-Series Firewall Configuration File

Edit the VM-Series firewall XML configuration file to support OVS and DPDK. You can access the XML configuration file or after deploying the VM-Series firewall. If you do this after deploying the firewall, be sure to shut down the firewall before making any changes. The values below are examples, your values for each parameter will vary based on your VM-Series model.

STEP 1 | Log in to the KVM host CLI.

STEP 2 | Edit the XML configuration file of your VM-Series firewall.

1. Open the XML config file using **virsh edit $<*your-vm-series-name*>**.
2. Sets the memory backing for the hugepage. Ensure that you provide enough memory to support the VM-Series firewall model you are deploying on the host. See VM-Series System Requirements for more information.

```
<memory unit='KiB'>12582912</memory>
  <currentMemory unit='KiB'>6291456</currentMemory>
  <memoryBacking>
    <hugepages/>
```

3. Set the necessary CPU flags for VM.

```
<cpu mode='host-model'>
```

4. Enable memory sharing between the VM and the host.

```
<numa>
      <cell id='0' cpus='0,2,4,6' memory='6291456' unit='KiB'
 memAccess='shared'/>
```

```
      <cell id='1' cpus='1,3,5,7' memory='6291456' unit='KiB'
 memAccess='shared'/>
    </numa>
```

5. Set the DPDK vhost user ports as the VM -series firewall's network interfaces. Additionally, set the number of virtio virtual queues provided to the VM-Series firewall by the host.

```
<interface type='vhostuser'>
      <mac address='52:54:00:36:83:70'/>
      <source type='unix' path='/usr/local/var/run/openvswitch/vhost-
user1' mode='client'/>
<model type='virtio'/>
<driver name='vhost' queues='8'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x04'
 function='0x0'/>
    </interface>
    <interface type='vhostuser'>
      <mac address='52:54:00:30:d7:94'/>
      <source type='unix' path='/usr/local/var/run/openvswitch/vhost-
user2' mode='client'/>
<model type='virtio'/>
<driver name='vhost' qeueus='8'>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x05'
 function='0x0'/>
    </interface>
```

Enable SR-IOV on KVM

Single root I/O virtualization (SR-IOV) allows a single PCIe physical device under a single root port to appear to be multiple separate physical devices to the hypervisor or guest. To enable SR-IOV on a KVM guest, define a pool of virtual function (VF) devices associated with a physical NIC and automatically assign VF devices from the pool to PCI IDs.

For SR-IOV with Intel 10GB network interfaces (ixgbe driver), the driver version must be 4.2.5 or later to support multiple queues for each NIC interface.

STEP 1 | Define a network for a pool of VFs.

1. Generate an XML file with text similar to the following example. Change the value of pf dev to the ethdev corresponding to you SR-IOV device's physical function.

```
<network>
   <name>passthrough</name>
   <forward mode='hostdev' managed='yes'>
     <pf dev='eth3'/>
   </forward>
</network>
```

2. Save the XML file.
3. Execute the following commands:

```
$ virsh net-define <path
to network XML file>
$ virsh net-autostart passthrough
$ virsh net-start passthrough
```

STEP 2 | After the defining and starting the network, modify the guest XML definition to specify the network.

```
<interface type='network'>
    <source network='passthrough'>
</interface>
```

When the guest starts, a VF is automatically assigned to the guest.

STEP 3 | Add the multicast MAC address to the host.

When SR-IOV is enabled, multicast traffic is filtered by the PF. This filtering causes applications that rely on multicast, such as OSPF, to fail. To prevent this filtering, you must manually add the multicast MAC address to the host using the following command:

```
#ip
maddress add <multicast-mac> dev <interface-name>
```

Enable Multi-Queue Support for NICs on KVM

Modify the guest XML definition to enable multi-queue virtio-net. Multi-queue virtio-net allows network performance to scale with the number of vCPUs and allows for parallel packet processing by creating multiple TX and RX queues.

Modify the guest XML definition. Insert a value from 1 to 256 for N to specify the number of queues. For the best results, match the number of queues with number of dataplane cores configured on the VM.

```
<interface type='network'>
      <source network='default'/>
      <model type='virtio'/>
      <driver name='vhost' queues='N'/>
</interface>
```

Isolate CPU Resources in a NUMA Node on KVM

You can improve performance of VM-Series on KVM by isolating the CPU resources of the guest VM to a single non-uniform memory access (NUMA) node. On KVM, you can view the NUMA topology **virsh**. The following example is from a two-node NUMA system:

STEP 1 | View the NUMA topology. In the example below, there are two NUMA nodes (sockets), each with a four-core CPU with hyperthreading enabled. All the even-numbered CPU IDs belong to one node and all the odd-numbered CPU IDs belong to the other node.

```
% virsh capabilities
<…>
  <topology>
    <cells num='2'>
      <cell id='0'>
        <memory unit='KiB'>33027228</memory>
        <pages unit='KiB' size='4'>8256807</pages>
        <pages unit='KiB' size='2048'>0</pages>
        <distances>
```

```
          <sibling id='0' value='10'/>
          <sibling id='1' value='20'/>
        </distances>
        <cpus num='8'>
          <cpu id='0' socket_id='1' core_id='0' siblings='0,8'/>
          <cpu id='2' socket_id='1' core_id='1' siblings='2,10'/>
          <cpu id='4' socket_id='1' core_id='2' siblings='4,12'/>
          <cpu id='6' socket_id='1' core_id='3' siblings='6,14'/>
          <cpu id='8' socket_id='1' core_id='0' siblings='0,8'/>
          <cpu id='10' socket_id='1' core_id='1' siblings='2,10'/>
          <cpu id='12' socket_id='1' core_id='2' siblings='4,12'/>
          <cpu id='14' socket_id='1' core_id='3' siblings='6,14'/>
        </cpus>
      </cell>
      <cell id='1'>
        <memory unit='KiB'>32933812</memory>
        <pages unit='KiB' size='4'>8233453</pages>
        <pages unit='KiB' size='2048'>0</pages>
        <distances>
          <sibling id='0' value='20'/>
          <sibling id='1' value='10'/>
        </distances>
        <cpus num='8'>
          <cpu id='1' socket_id='0' core_id='0' siblings='1,9'/>
          <cpu id='3' socket_id='0' core_id='1' siblings='3,11'/>
          <cpu id='5' socket_id='0' core_id='2' siblings='5,13'/>
          <cpu id='7' socket_id='0' core_id='3' siblings='7,15'/>
          <cpu id='9' socket_id='0' core_id='0' siblings='1,9'/>
          <cpu id='11' socket_id='0' core_id='1' siblings='3,11'/>
          <cpu id='13' socket_id='0' core_id='2' siblings='5,13'/>
          <cpu id='15' socket_id='0' core_id='3' siblings='7,15'/>
        </cpus>
    </cell>
</cells>
```

STEP 2 | Pin vCPUs in a KVM guest to specific physical vCPUs, use the **cpuset** attribute in the guest xml definition. In this example, all 8 vCPUs are pinned to physical CPUs in the first NUMA node. If you do not wish to explicitly pin the vCPUs, you can omit the **cputune** block, in which case, all vCPUs will be pinned to the range of CPUs specified in cpuset, but will not be explicitly mapped.

```
<vcpu cpuset='0,2,4,6,8,10,12,14'>8</vcpu>
<cputune>
  <vcpupin vcpu='0' cpuset='0'/>
  <vcpupin vcpu='1' cpuset='2'/>
  <vcpupin vcpu='2' cpuset='4'/>
  <vcpupin vcpu='3' cpuset='6'/>
  <vcpupin vcpu='4' cpuset='8'/>
  <vcpupin vcpu='5' cpuset='10'/>
  <vcpupin vcpu='6' cpuset='12'/>
  <vcpupin vcpu='7' cpuset='14'/>
</cputune>
```

Set Up the VM-Series Firewall on Hyper-V

The VM-Series firewall can be deployed on a server running Microsoft Hyper-V. Hyper-V is packaged as a standalone hypervisor or as an add-on/role for Windows Server.

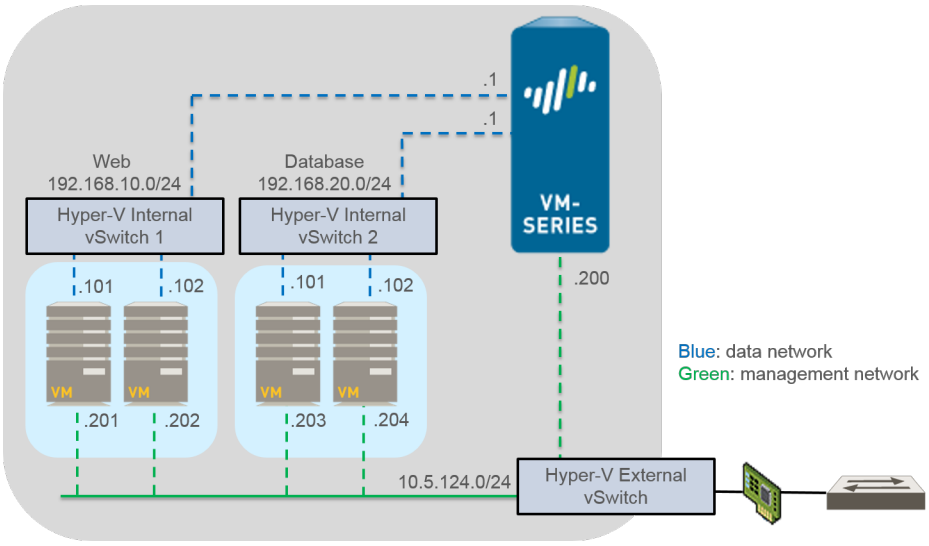
Supported Deployments on Hyper-V

You can deploy one or more instances of the VM-Series on hosts running Hyper-V. Where you place the VM-Series firewall depends on your network topology. VM-Series supports tap, virtual wire, Layer 2, and Layer 3 interface deployments.

- Secure Traffic on a Single Hyper-V Host
- Secure Traffic Across Multiple Hyper-V Hosts

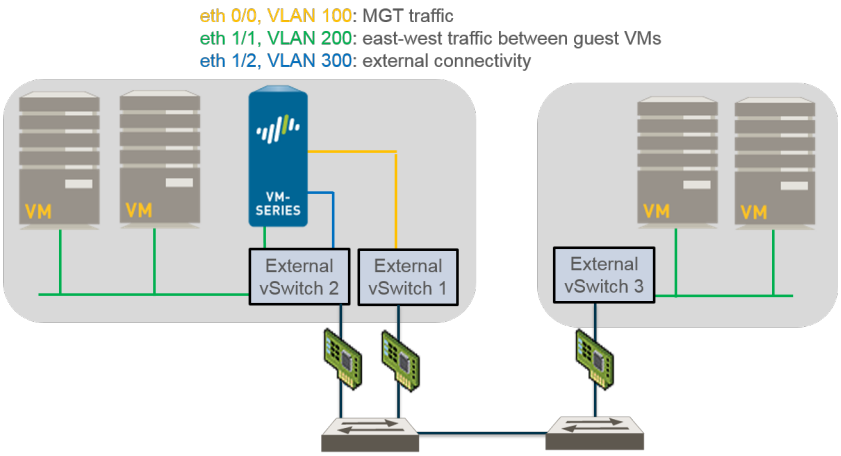
Secure Traffic on a Single Hyper-V Host

The VM-Series firewall is deployed on a single Hyper-V host along with other guest VMs. In the example below, the VM-Series firewall has a Layer 3 interfaces and the VM-Series and other guest VMs are connected by Hyper-V vSwitches. All traffic between the web servers and database servers is routed through the firewall. Traffic across the database servers only or across the web servers only is processed by the external vSwitch and not routed through the firewall.



Secure Traffic Across Multiple Hyper-V Hosts

You can deploy your VM-Series firewall to secure the traffic of multiple Hyper-V hosts. In the example below, the VM-Series is deployed in Layer 2 mode protecting traffic to and from the guest VMs. A single VM-Series firewall protects traffic between four guest VMs spread across two Hyper-V hosts. VLAN tagging is used to logically isolate traffic and direct it to the firewall. Additionally, management traffic is decoupled from all other traffic by placing it on its own external vSwitch.



System Requirements on Hyper-V

The VM-Series requires a minimum resource allocation on the Hyper-V host, so make sure to conform to the requirements listed below to ensure optimal performance.

- The host CPU must be a 64-bit x86-based Intel or AMD CPU with virtualization extension.
- See VM-Series System Requirements for the minimum hardware requirements for your VM-Series model.
- Minimum of two network adapters. The VM-Series firewall supports synthetic network adapters, which provide better performance than emulated network adapters. Hyper-V supports up to eight synthetic network adapters.
- Refer to the Compatibility matrix for the Windows Server versions supported.

  Hyper-V Server does not have a native graphical user interface; all configuration is done through PowerShell. However, you can use Hyper-V Manager running on a remote machine to manage the firewall.If you use the Hyper-V role add-on, you can manage the firewall using Hyper-V Manager or PowerShell.
- The VM-Series does not support Legacy Network Adapter or SR-IOV/PCI-Passthrough.

Linux Integration Services

Linux Integration Services (LIS) is a package of drivers and services that enhance the performance of Linux-based virtual machines on Hyper-V. The VM-Series firewall supports the following services to improve the integration between the host and the virtual machine:

- **Graceful Shutdown**—Allows you to perform a graceful shutdown of the VM-Series firewall from the Hyper-V management interface without having to log into the guest.
- **Heartbeat to Hyper-V Manager**—Provides heartbeat monitoring of the running status of guest VMs from the Hyper-V management interface.
- **Firewall Management IP Address Visibility**—Allows you to use Hyper-V Manager to view the IP address assigned to the management interface on the firewall.

Install the VM-Series Firewall on Hyper-V

Use the instructions in this section to deploy your VM-Series firewall on a Hyper-V host. A Palo Alto Networks support account and a valid VM-Series license are required to download the VHDX image file and install the VM-Series on the Hyper-V host. If you have not already registered the capacity auth-code that you received with the order fulfillment email, with your support account, see Register the VM-Series Firewall. After completing the registration continue to the following tasks:

- Before You Begin
- Performance Tuning of the VM-Series Firewall on Hyper-V
- Provision the VM-Series Firewall on a Hyper-V host with Hyper-V Manager
- Provision the VM-Series Firewall on a Hyper-V host with PowerShell
- Perform Initial Configuration on the VM-Series Firewall

Before You Begin

Before installing and configuring your VM-Series firewall, know and account for the following items as needed when you configure your VM-Series firewall:

- Virtual Switch Types
- MAC Address Spoofing

Virtual Switch Types

Before installing the VM-Series, you must create the vSwitches required for providing external connectivity for management access and for routing traffic from and to the virtual machines that the firewall will secure. Hyper-V allows you to create three types of vSwitches:

- **External vSwitch**—binds to a physical network adapter and provides the vSwitch access to a physical network.
- **Internal vSwitch**—passes traffic between the virtual machines and the Hyper-V host. This type of vSwitch does not provide connectivity to a physical network connection.
- **Private vSwitch**—passes traffic between the virtual machines on the Hyper-V host only.

An external vSwitch is required for management of the VM-Series firewall. Other vSwitches connected to the VM-Series firewall can be of any type and will depend on your network topology.

MAC Address Spoofing

If you are deploying the VM-Series firewall with interfaces enabled in Layer 3 mode, make sure to enable use of hypervisor assigned MAC addresses so that the hypervisor and the firewall can properly handle packets. Alternatively, use the Hyper-V Manager to enable MAC address spoofing on the virtual network adapter for each dataplane interface on the firewall. For more information, see Hypervisor Assigned MAC Addresses.

If you are deploying the VM-Series firewall with interfaces enabled in Layer 2 mode or virtual-wire mode, you must enable MAC address spoofing on the virtual network adapter in Hyper-V for each dataplane interface on the firewall. This setting is required to ensure that packets sent by the VM-Series are not dropped by the virtual network adapter if the source MAC address does not match the outgoing interface MAC address.

Performance Tuning of the VM-Series Firewall on Hyper-V

The VM-Series firewall for Hyper-V is a high-performance appliance but may require tuning of the hypervisor to achieve the best results. This section describes some best practices and recommendations for facilitating the best performance of the VM-Series firewall.

- Disable Virtual Machine Queues
- Isolate CPU Resources in a NUMA Node

Disable Virtual Machine Queues

Palo Alto Networks recommends disabling virtual machine queues (VMQ) for all NICs on the Hyper-V host. This option is prone to misconfiguration and can cause reduced network performance when enabled.

STEP 1 | Login to Hyper-V Manager and select your VM.

STEP 2 | Select **Settings** > **Hardware** > **Network Adapter** > **Hardware Acceleration**.

STEP 3 | Under Virtual machine queue, uncheck **Enable virtual machine queue**.

STEP 4 | Click **Apply** save your changes and **OK** to exit the VM settings.

Isolate CPU Resources in a NUMA Node

You can improve performance of VM-Series for Hyper-V by isolating the CPU resources of the guest VM to a single non-uniform memory access (NUMA) node. You can view the NUMA settings of your VM in Hyper-V Manager by selecting **Settings** > **Hardware** > **Processor** > **NUMA**.

Provision the VM-Series Firewall on a Hyper-V host with Hyper-V Manager

Use these instructions to deploy the VM-Series firewall on Hyper-V using Hyper-V Manager.

STEP 1 | Download the VHDX file.

Register your VM-Series firewall and obtain the VHDX file.

1. Go to https://www.paloaltonetworks.com/services/support.
2. Filter by **PAN-OS for VM-Series Base Images** and download the VHDX file. For example, PA-VM-HPV-7.1.0.vhdx.

STEP 2 | Set up any vSwitch(es) that you will need.

To create a vSwitch:

1. From Hyper-V Manager, select the host and select **Action** > **Virtual Switch Manager** to open the Virtual Switch Manager window.
2. Under **Create virtual switch**, select the type of vSwitch (external, internal, or private) to create and click **Create Virtual Switch**.

STEP 3 | Install the firewall.

1. On the Hyper-V Manager, select the host and select **Action** > **New** > **Virtual Machine.** Configure the following settings in the New Virtual Machine Wizard:
    1. Choose a **Name** and **Location** for the VM-Series firewall. The VM-Series firewall stores the VHDX file at the specified location.

2. Choose **Generation 1**. This is the default option and the only version supported.
3. For **Startup Memory**, assign the memory based on the VM-Series System Requirements of your VM-Series model.

   Do not enable dynamic memory; the VM-Series firewall requires static memory allocation.

4. Configure **Networking**. Select an external vSwitch to connect the management interface on the firewall.
5. To connect the **Virtual Hard Disk**, select **Use an existing virtual hard disk** and browse to the VHDX file you downloaded earlier.
6. Review the summary and click **Finish**.

2. Assign virtual CPUs to the firewall.
   1. Select the VM you created and navigate to **Action** > **Settings**.
   2. Select **Processor** and enter the minimum number of CPUs based on the VM-Series System Requirements of your VM-Series model..
   3. Click **OK**.

STEP 4 | Connect at least one network adapter for the dataplane interface on the firewall.

1. Select **Settings** > **Hardware** > **Add Hardware** and select the **Hardware type** for your network adapter.

   Legacy Network Adapter and SR-IOV are not supported. If selected, the VM-Series firewall will boot into maintenance mode.

2. Click **OK**.

STEP 5 | (Optional) Enable MAC address spoofing on Hyper-V if you are not using Layer 3 with hypervisor assigned MAC address.

1. Double click the dataplane virtual network adapter and click **Advanced Settings**.
2. Click the **Enable MAC address spoofing** check box and click **Apply**.

STEP 6 | Power on the firewall.

Select the firewall from the list of **Virtual Machines** and navigate to **Action** > **Start** to power on the firewall.

Provision the VM-Series Firewall on a Hyper-V host with PowerShell

Use these instructions to deploy the VM-Series firewall on Hyper-V using PowerShell.

STEP 1 | Download the VHDX file.

Register your VM-Series firewall and obtain the VHDX file.

1. Go to https://www.paloaltonetworks.com/services/support.
2. Filter by **PAN-OS for VM-Series Base Images** and download the VHDX file. For example, PA-VM-HPV-7.1.0.vhdx.

STEP 2 | Set up any vSwitch(es) that you will need.

Create a vSwitch by using the following commands. Give the vSwitch a name and choose the switch type.

```
> New-VMSwitch -Name <"switch-name"> -SwitchType <switch-type>
```

STEP 3 | Install the VM-Series firewall.

1. Create the new virtual machine and set the memory based on the VM-Series System Requirements of your VM-Series model.

```
> NEW-VM -Name <vm-name> -MemoryStartupBytes 4GB -VHDPath <file-path-to-vhdx>
```

2. Set processor count based on the VM-Series System Requirements of your VM-Series model.

```
> SET-VMProcessor –VMName <vm-name> –Count 2
```

STEP 4 | Connect at least one network adapter for the management interface on the firewall.

Connect the default network adapter created during VM creation to management vSwitch.

```
> connect-VMNetworkAdapter -vmname <vm-name> -Name <"network-adapter-name">
 -SwitchName <"management-vswitch">
```

STEP 5 | (Optional) Enable MAC address spoofing on Hyper-V if you are not using Layer 3 with hypervisor assigned MAC address.

```
> Set-VMNetworkAdapter -vmname <vm-name> -Name <"network-adapter-name"> -
MacAddressSpoofing On
```

STEP 6 | Power on the firewall.

For example:

```
> Start-VM -vmname <vm-name>
```

Perform Initial Configuration on the VM-Series Firewall

Use these instructions to perform the initial configuration of your VM-Series firewall. By default, the VM-Series firewall uses DHCP to obtain an IP address for the management interface. However, you can assign a static IP address. After completing the initial configuration, access the web interface to complete further configurations tasks. If you have Panorama for central management, refer to the Panorama Administrator's Guide for information on managing the device using Panorama.

If you are using bootstrapping to perform the configuration of your VM-Series firewall on Hyper-V, refer to Bootstrap the VM-Series Firewall on Hyper-V. For general information about bootstrapping, see Bootstrap the VM-Series Firewall.

STEP 1 | Gather the required information from your network administrator.

- Management port IP address
- Netmask
- Default gateway
- DNS server IP address

STEP 2 | Access the console of the VM-Series firewall.

1. In Hyper-V Manager, select the VM-Series firewall and click **Connect** from the Actions list.
2. Log in to the firewall with the default username and password: **admin/admin**
3. Enter configuration mode using the following command: **configure**

STEP 3 | Configure the network access settings for the management interface. You should restrict access to the firewall and isolate the management network. Additionally, do not make the allowed network larger than necessary and never configure the allowed source as 0.0.0.0/0.

Enter the following commands:

```
set deviceconfig system type static
```

```
set deviceconfig system ip-address <Firewall-IP> netmask <netmask>
default-gateway <gateway-IP> dns-setting servers primary <DNS-IP>
```

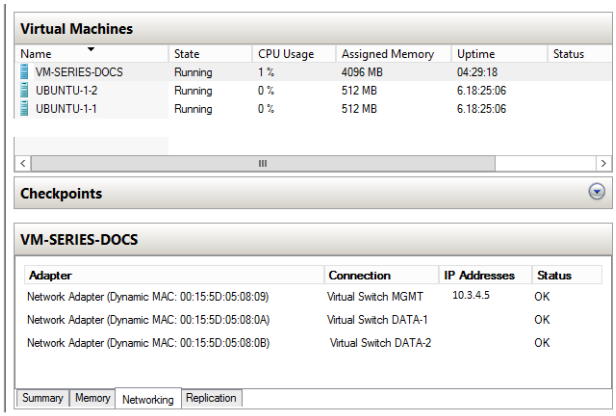
where *<Firewall-IP>* is the IP address you want to assign to the management interface, *<netmask>* is the subnet mask, *<gateway-IP>* is the IP address of the network gateway, and *<DNS-IP>* is the IP address of the DNS server.

STEP 4 | Commit your changes and exit the configuration mode.

1. Enter **commit**.
2. Enter **exit**.

STEP 5 | Verify that you can view the management interface IP address from the Hyper-V Manager.

1. Select the VM-Series firewall from the list of **Virtual Machines**.
2. Select **Networking**. The first network adapter that displays in the list is used for management access to the firewall; subsequent adapters in the list are used as the dataplane interfaces on the firewall.



STEP 6 | Verify network access to external services required for firewall management, such as the Palo Alto Networks Update Server.

1. Use the ping utility to verify network connectivity to the Palo Alto Networks Update server as shown in the following example. Verify that DNS resolution occurs and the response includes the IP address for the Update server; the update server does not respond to a ping request.

```
admin@PA-200 > ping host updates.paloaltonetworks.com
```

```
PING updates.paloaltonetworks.com (10.101.16.13) 56(84) bytes of data.
From 192.168.1.1 icmp_seq=1 Destination Host Unreachable
From 192.168.1.1 icmp_seq=2 Destination Host Unreachable
From 192.168.1.1 icmp_seq=3 Destination Host Unreachable
From 192.168.1.1 icmp_seq=4 Destination Host Unreachable
```

After verifying DNS resolution, press Ctrl+C to stop the ping request.

2. Use the following CLI command to retrieve information on the support entitlement for the firewall from the Palo Alto Networks update server:

```
request support
check
```

If you have connectivity, the update server will respond with the support status for your firewall.

STEP 7 | (Optional) Verify that your VM-Series jumbo frame configuration does not exceed the maximum MTU supported on Hyper-V.

The VM-Series has a default MTU size of 9216 bytes when jumbo frames are enabled. However, the maximum MTU size supported by the physical network adapter on the Hyper-V host is 9000 or 9014 bytes depending on the network adapter capabilities. To verify the configured MTU on Hyper-V:

1. In Windows Server 2012 R2, open the **Control Panel** and navigate to N**etwork and Internet** > **Network and Sharing Center** > **View network status and tasks**.
2. Click on a network adapter or virtual switch from the list.
3. Click **Properties**.
4. Click **Configure**.
5. On the Advanced tab, select **Jumbo Packet** from the list.
6. Select 9000 or 9014 bytes from the Value drop-down menu.
7. Click **OK**.

If you have enabled jumbo frames on Hyper-V, Enable Jumbo Frames on the VM-Series Firewall and set the MTU size to match that configured on the Hyper-V host.

STEP 8 | Access the web interface of the VM-Series firewall and configure the interfaces and define security rules and NAT rules to safely enable the applications you want to secure.

Refer to the PAN-OS Administrator's Guide.

Set up the VM-Series Firewall on Azure

VM-Series firewall on Azure brings the security features of Palo Alto Networks next generation firewall as a virtual machine in the Azure Marketplace. On Azure, the VM-Series firewall is available in the bring your own license (BYOL) model or in the pay-as-you-go (PAYG) hourly model. Microsoft Azure allows you to deploy the firewall to secure your workloads within the virtual network in the cloud, so that you can deploy a public cloud solution or you can extend the on-premises IT infrastructure to create a hybrid solution.

About the VM-Series Firewall on Azure

The VM-Series firewall on Azure must be deployed in a virtual network (VNet) using the Resource Manager deployment mode. You can deploy the VM-Series firewall on the following Azure geographies: Standard Azure public cloud, Azure China, Azure Germany, and Azure Government.

Marketplace	VM-Series Offering
Standard Azure public cloud	On standard Azure public cloud, the VM-Series firewall is available in both the Bring Your Own License (BYOL) model and the hourly Pay-As-You-Go (PAYG) option (usage-based licensing). For licensing details, see License Types—VM-Series Firewalls, and refer to the list of supported Azure regions in which you can deploy the VM-Series firewall.
Azure Government	VM-Series firewall is available in the BYOL option. To deploy the VM-Series on Azure Government, use the BYOL workflow outlined in the Deploy the VM-Series Firewall from the Azure Marketplace (Solution Template).
Azure China	VM-Series firewall is available in the BYOL option. Azure China has a slightly different workflow that is outlined in Deploy the VM-Series Firewall from the Azure China Marketplace (Solution Template)
Azure Germany	VM-Series firewall is available in the BYOL and ELA options. Unlike other Azure regions, on Azure Germany only the VM-Series VHD/image is published to the Marketplace. You will need to reference this VHD image within your custom ARM templates, or deploy it on the Azure CLI, Azure PowerShell or Azure ARM API. To locate the image, you the need the following details to complete the command (show vm-image list): • Publisher: paloaltonetworks • Offer: vmseries1 • SKU: byol • Version: 8.0.7 or latest To test the VM-Series firewall on Azure Germany, try the sample ARM template that deploys the firewall with three network interfaces. This sample template is under the community-support policy and is available in the GitHub repository at: https://github.com/PaloAltoNetworks/azure-germany

- Azure Networking and VM-Series
- VM-Series Firewall Templates on Azure
- Minimum System Requirements for the VM-Series on Azure
- Support for High Availability on VM-Series on Azure

Azure Networking and VM-Series

The Azure VNet infrastructure does not require virtual machines to have a network interface in each subnet. The architecture includes an internal route table (called system routes) that directly connects all

virtual machines within a VNet such that traffic is automatically forwarded to a virtual machine in any subnet. For a destination IP address that is not within the VNet, the traffic is sent to the default Internet gateway or to a VPN gateway, if configured. In order to route traffic through the VM-Series firewall, you must create user defined routes (UDRs) that specify the next hop for traffic leaving a subnet. This route forces traffic destined to another subnet to go to the VM-Series firewall instead of using the system routes to directly access the virtual machine in the other subnet. For example, in a two-tiered application with a web tier and a database tier, you can set up UDRs for directing traffic from the web subnet to the DB subnet through the VM-Series firewall.

On Azure, UDRs are for traffic leaving a subnet only. You cannot create user defined routes to specify how traffic comes into a subnet from the Internet or to route traffic to virtual machines within a subnet.

For documentation on Microsoft Azure, refer to https://azure.microsoft.com/en-us/documentation/.

The solution templates for deploying the VM-Series firewall that are available in the Azure Marketplace, have three network interfaces. Because the VNet infrastructure does not require virtual machines to have a network interface in each subnet, three network interfaces are sufficient for most deployments. If you want to customize the template, use the ARM templates that are available in the GitHub repository.

VM-Series Firewall Templates on Azure

You can deploy the VM-Series firewall on Azure using templates. Palo Alto Networks provides two kinds of templates:

- **Solution Templates in the Azure Marketplace** —The solution templates that are available in the Azure Marketplace allow you to deploy the VM-Series firewall using the Azure portal. You can use an existing resource group and storage account (or create them new) to deploy the VM-Series firewall with the following default settings for all regions except Azure China:
  - VNet CIDR 192.168.0.0/16; you can customize the CIDR to a different private IP address range.
  - Three subnets— 192.168.0.0/24 (management), 192.168.1.0/24 (untrust), 192.168.2.0/24 (trust)
  - Three network interfaces, one in each subnet. If you customize the VNet CIDR, the subnet ranges map to your changes.

  To use the solution template, see Deploy the VM-Series Firewall from the Azure Marketplace (Solution Template) for Azure China, see Deploy the VM-Series Firewall from the Azure China Marketplace (Solution Template).
- **ARM Templates in the GitHub Repository**—In addition to Marketplace based deployments, Palo Alto Networks provides Azure Resource Manager templates in the GitHub Repository to simplify the process of deploying the VM-Series firewall on Azure.
  - Use the ARM Template to Deploy the VM-Series Firewall—The basic ARM template includes two JSON files (a Template file and a Parameters File) to help you deploy and provision all the resources within the VNet in a single, coordinated operation. These templates are provided under an as-is, best effort, support policy.

    If you want to use the Azure CLI to locate all the images available from Palo Alto Networks, you the need the following details to complete the command (show vm-image list):

    - *Publisher: paloaltonetworks*
    - *Offer: vmseries1*
    - *SKU: byol, bundle1, bundle 2*
    - *Version: 8.0.0, 7.1.1 or latest*

- Deploy the VM-Series and Azure Application Gateway Template to support a scale out security architecture that protects your internet-facing web applications using two VM-Series firewalls between a pair of (external and internal) Azure load balancers VM-Series and Azure Application Gateway. This template is currently not available for Azure China.

Minimum System Requirements for the VM-Series on Azure

You must deploy the VM-Series firewall in the Azure Resource Manager (ARM) mode only; the classic mode (Service Management based deployments) is not supported. The VM-Series firewall on Azure must meet the following requirements:

- Azure Linux VMs of the following types:
  - Standard_D3_v2 (default)
  - Standard_D4_v2
  - Standard_D5_v2
  - Standard_D4_v3
  - Standard_D16_v3
  - Standard_DS3_v2
  - Standard_DS4_v2
  - Standard_DS5_v2
- For memory, disk and CPU cores required to deploy the VM-Series firewall, see VM-Series System Requirements.

  You can add additional disk space of 40GB to 8TB for logging purposes. The VM-Series firewall does not utilize the temporary disk that Azure provides.
- Up to seven network interfaces (NICs). A primary interface is required for management access and up to six interfaces for data traffic.

  On Azure, because a virtual machine does not require a network interface in each subnet, you can set up the VM-Series firewall with just two network interfaces (one for management traffic and one for dataplane traffic). To create zone-based policy rules on the firewall, in addition to the management interface, you need at least two dataplane interfaces so that you can assign one dataplane interface to the *trust* zone, and the other dataplane interface to the *untrust* zone.

  Because the Azure VNet is a Layer 3 network, the VM-Series firewall on Azure supports Layer 3 interfaces only.

Support for High Availability on VM-Series on Azure

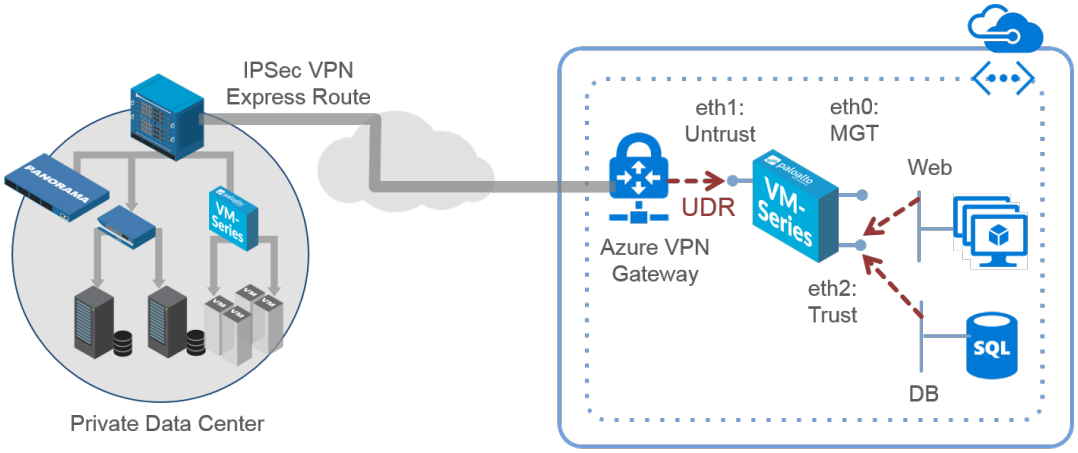
For high availability with VM-Series on Azure, use a scale out architecture using cloud-native load balancers such as the Azure Application Gateway or Azure Load Balancer to distribute traffic across a set of healthy instances of the firewall. For details, For details, see Deploy the VM-Series and Azure Application Gateway Template.

If you want the traditional active/passive high availability with session synchronization, upgrade to PAN-OS 9.0 and refer to Set up Active/Passive HA on Azure.

Deployments Supported on Azure

Use the VM-Series firewall on Azure to secure your network users in the following scenarios:

- **Hybrid and VNet to VNet**—The VM-Series firewall on Azure allows you to securely extend your physical data center/private cloud into Azure using IPSec and ExpressRoute. To improve your data center security, if you have segmented your network and deployed your workloads in separate VNets, you can secure traffic flowing between VNets with an IPSec tunnel and application whitelisting policies.

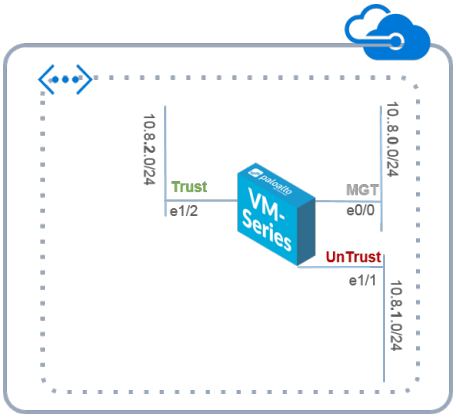


- **Inter-Subnet** —The VM-Series firewall can front your servers in a VNet and protects against lateral threats for inter-subnet traffic between applications in a multi-tier architecture.
- **Gateway**—The VM-Series firewall serves as the VNet gateway to protect Internet-facing deployments in the Azure Virtual Network (VNet). The VM-Series firewall secures traffic destined to the servers in the VNet and it also protects against lateral threats for inter-subnet traffic between applications in a multi-tier architecture.
- **GlobalProtect**—Use the Azure infrastructure to quickly and easily deploy the VM-Series firewall as GlobalProtect™ and extend your gateway security policy to remote users and devices, regardless of location.

You can continue with Deploy the VM-Series Firewall from the Azure Marketplace (Solution Template) and configure the firewall and Azure for your deployment needs, or you can learn about the VM-Series Firewall Templates on Azure that you can use to deploy the firewall. For information on bootstrapping, see Bootstrap the VM-Series Firewall in Azure.

Deploy the VM-Series Firewall from the Azure Marketplace (Solution Template)

The following instructions show you how to deploy the solution template for the VM-Series firewall that is available in the Azure Marketplace. To use the customizable ARM templates available in the GitHub repository, see Use the ARM Template to Deploy the VM-Series Firewall.



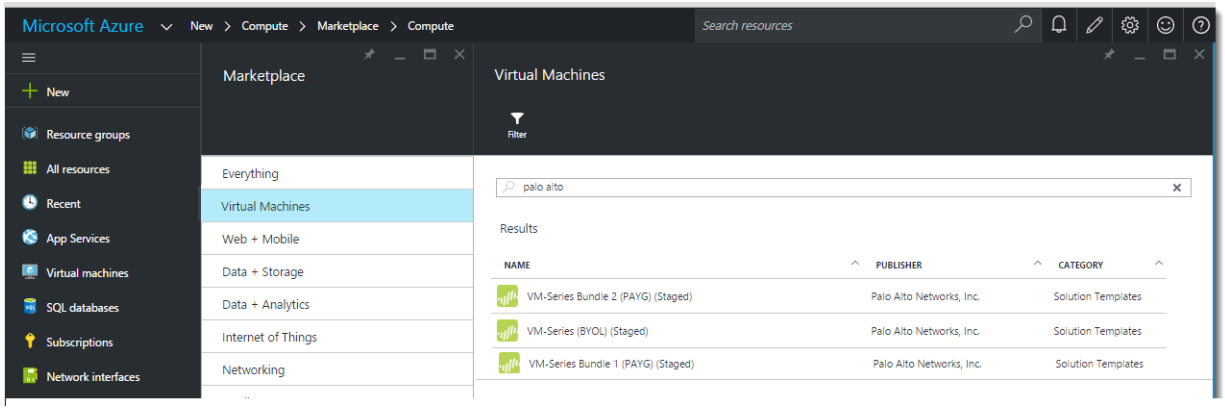
STEP 1 | Set up an Azure account.

1. Create a Microsoft account.
2. Log in to the Azure portal (**`https://portal.azure.com`**) using your Microsoft account credentials.

If you are using a trial subscription, you may need to open a support request (Help + Support > New Support Request) to increase the quota of allocated VM cores.

STEP 2 | Find the VM-Series solution template in the Azure Marketplace.

1. Select **Azure Marketplace** > **Virtual Machines**.
2. Search for Palo Alto Networks. The offerings for the VM-Series firewall display. For the differences in the BYOL and PAYG models, see VM-Series Firewall in Amazon Web Services (AWS) and Azure Licenses.

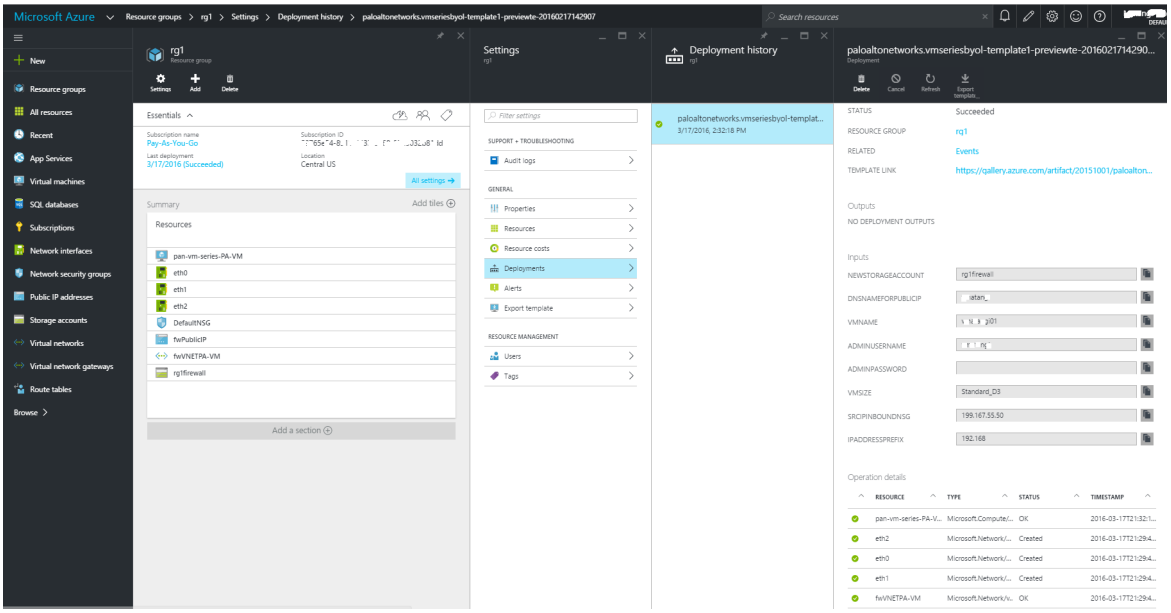


3. Select an offering and click **Create**.

STEP 3 | Deploy the firewall.

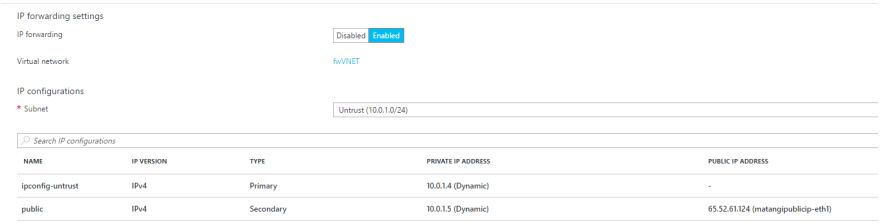
1. Configure basic settings for the firewall.
    1. Enter a **Username** for the firewall administrator.
    2. Enter a **Password** (of up to 31 characters) or copy and paste an **SSH public key** for securing administrative access to the firewall.
    3. Select your Azure **Subscription**.
    4. Create a new resource group for holding all the resources associated with the VM-Series firewall for this deployment.

        Azure has removed the option to select an existing resource group for Marketplace solutions that enable multiple NICs. To deploy the firewall into an existing resource group, use the ARM template in the GitHub Repository or your own custom ARM template.
    5. Select the Azure **Location**. This is the region in which you are deploying the firewall.
2. Configure storage and networking.
    1. Select an existing storage account or create a new one.
    2. Select an existing VNet or create a new one, and enter the IP address space for the VNet. By default the CIDR is 10.0.0.0/16.
    3. Configure the subnets for the network interfaces. If you use an existing VNet, you must have defined three subnets, one each for the management, trust and untrust interfaces. If you create a new VNet, verify or change the prefixes for each subnet. The default subnets are 10.0.0.0/24 for the management subnet, 10.0.1.0/24 for the untrust subnet, and 10.0.2.0/24 for the trust subnet.
    4. Enter the source IP address or IP range (include CIDR) that can access the VNet. **Network Security Group: inbound source IP** allows you to restrict inbound access to the Azure VNet.
3. Define management access to the firewall.
    1. Use the default variable (new PublicIP) to assign a **Public IP address** to the management interface (eth0) of the firewall.
    2. Enter a prefix to access the firewall using a DNS name. You must combine the prefix you enter with the suffix displayed on screen for example <yourname>centralus.cloudapp.azure.com to access the web interface of the firewall.
    3. Enter a display name to identify the VM-Series firewall within the resource group.
    4. Select the Azure virtual machine tier and size to meet your needs. See Minimum System Requirements for the VM-Series on Azure.
4. Review the summary, accept the terms of use and privacy policy, and click **Create** to deploy the firewall.
5. Verify that you have successfully deployed the VM-Series firewall.
    1. Select **Dashboard** > **Resource Groups**, select the resource group.
    2. Select **All Settings** > **Deployments** > **Deployment History** for detailed status



STEP 4 | Attach a public IP address for the untrust interface of the VM-Series firewall. When you create a new public IP address you get one from the block of IP addresses Microsoft owns, so you can't choose a specific one. The maximum number of public IP addresses you can assign to an interface is based on your Azure subscription.

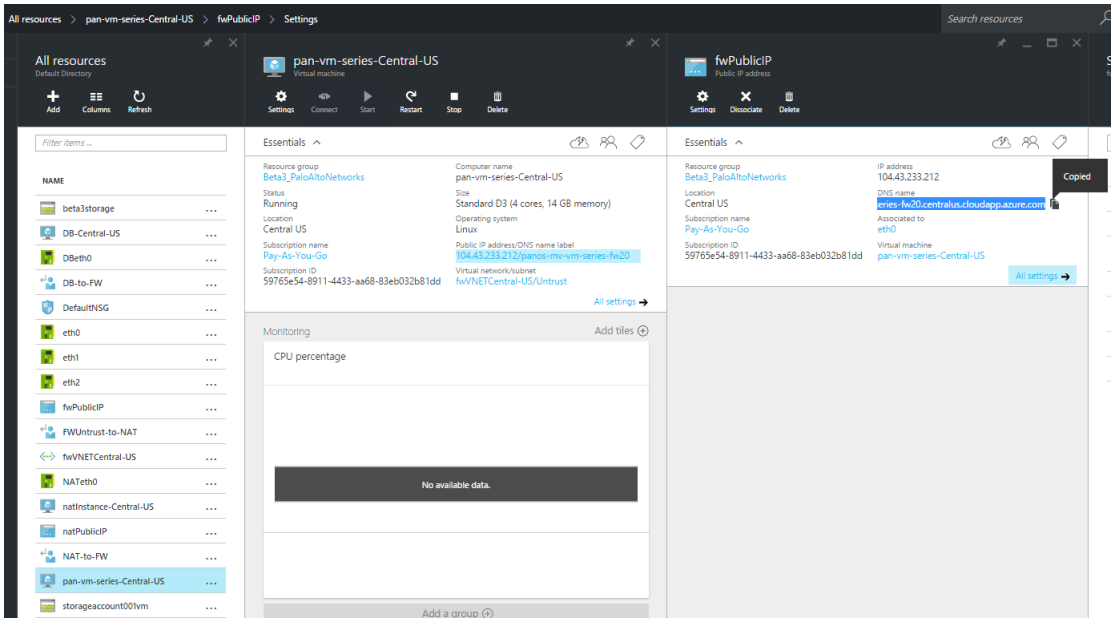
1. On the Azure portal, select the network interface for which you want to add a public IP address. For example the eth1 interface.
2. Select **IP Configurations** > **Add** and for Public IP address, select **Enabled**. Create a new public IP address or select one that you have available.
3. Verify that you can view the secondary IP address associated with the interface.



When you attach a secondary IP address to a network interface, the VM-Series firewall does not automatically acquire the private IP address assigned to the interface. You will need to manually configure the private IP address using the VM-Series firewall web interface. See Configure the dataplane network interfaces as Layer 3 interfaces on the firewall.

STEP 5 | Log in to the web interface of the firewall.

1. On the Azure portal, in **All Resources**, select the VM-Series firewall and view the full DNS name for the firewall.



1. Using a secure connection (https) from your web browser, log in to the DNS name for the firewall.
2. Enter the username/password you defined in the parameters file. You will see a certificate warning; that is okay. Continue to the web page.

STEP 6 | Activate the licenses on the VM-Series firewall.

For the BYOL version

1. Create a Support Account.
2. Register the VM-Series Firewall (with auth code).
3. On the firewall web interface, select **Device** > **Licenses** and select **Activate feature using authentication code**.
4. Enter the capacity auth-code that you registered on the support portal. The firewall will connect to the update server (updates.paloaltonetworks.com), and download the license and reboot automatically.
5. Log back in to the web interface and confirm the following on the **Dashboard**:
   - A valid serial number displays in **Serial#**.

     If the term Unknown displays, it means the device is not licensed. To view traffic logs on the firewall, you must install a valid capacity license.
   - The **VM Mode** displays as Microsoft Azure.

For the PAYG version

1. Create a Support Account.
2. Register the Usage-Based Model of the VM-Series Firewall in AWS and Azure (no auth code).

STEP 7 | Configure the dataplane network interfaces as Layer 3 interfaces on the firewall.

If you are hosting multiple websites or services with different IP addresses and SSL certificates on a single server, you might need to configure more than one IP address on the VM-Series firewall interfaces.

With the support for multiple public IP address for the firewall interfaces, the NAT VM is no longer required. If you have an existing deployment that uses the NAT VM, reassign

the public IP address from the NAT VM to the untrust interface on the firewall, and then delete the NAT VM, the UDR, and subnet.

1. Select **Network** > **Interfaces** > **Ethernet**.
2. Click the link for **ethernet 1/1** and configure as follows:
   - **Interface Type**: Layer3 (default).
   - 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 called UnTrust, and then click OK.
   - On the **IPv4** tab, select **DHCP Client** if you plan to assign only one IP address on the interface. The private IP address assigned in the ARM template will be automatically acquired. If you plan to assign more than one IP address select **Static** and manually enter the primary and secondary IP addresses assigned to the interface on the Azure portal.
   - Clear the **Automatically create default route to default gateway provided by server** check box. Disabling this option ensures that traffic handled by this interface does not flow directly to the default gateway in the VNet.
3. Click the link for **ethernet 1/2** and configure as follows:
   - Set **Interface Type** to Layer3 (default).
   - **Security Zone**: Trust
   - **IP address**: Select **DHCP Client** or **Static**.
   - Clear the **Automatically create default route to default gateway provided by server** check box. Disabling this option ensures that traffic handled by this interface does not flow directly to the default gateway in the VNet.
4. Click **Commit**. Verify that the link state for the interfaces is up.
5. Add a stati c route on the virtual router of the VM-Series firewall for any networks that the firewall needs to route.

   For example, to add a default route to the destination subnets for the servers that the firewall secures:
   - Select **Network** > **Virtual Router** > **default** >
   - Select **Static Routes** > **IPv4**, and add the next hop IP address for the destination servers. You can set x.x.x.1 as the next hop IP address for all traffic (destined to 0.0.0.0/0 from interface ethernet1/1).

STEP 8 | Configure the firewall for your specific deployment.

- Gateway—Deploy a 3rd party load balancer in front of the UnTrust zone.
- Hybrid and Inter-VNet—Deploy an Azure VPN Gateway or a NAT virtual machine in front the UnTrust zone.
- Inter-Subnet—On the VM-Series firewall, add an intra-zone security policy rule to allow traffic based on the subnets attached to the Trust interface.
- GlobalProtect—Deploy a NAT virtual machine in front of the UnTrust zone.

STEP 9 | Direct traffic to the VM-Series firewall.

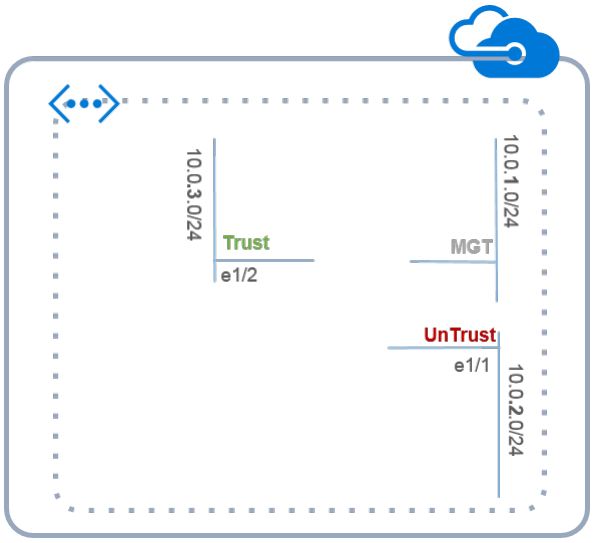
1. To ensure that the VM-Series firewall secures all traffic within the Azure resource group, configure static routes on the firewall.
2. Configure UDRs to direct all traffic through the interfaces on the VM-Series firewall. Refer to the Azure documentation on UDRs for details.

   The UDRs on the internal subnets must send all traffic through the Trust interface. The UDRs on the UnTrust side direct all traffic from the Internet through the UnTrust interface on the VM-Series firewall. The traffic from the Internet may be coming from an Azure Application Gateway or Azure

Load Balancer, or through the Azure VPN Gateway in case of a hybrid deployment that connects your on-premises network with the Azure cloud.

Deploy the VM-Series Firewall from the Azure China Marketplace (Solution Template)

The following instructions show you how to deploy the solution template for the VM-Series firewall that is available in the Azure China Marketplace. The Azure China Marketplace supports only the BYOL model of the VM-Series firewall. You can deploy the firewall in a existing resource group that is empty or into a new resource group. The default VNet in the template is 10.0.0.0/16, and it deploys a VM-Series firewall has 3 network interfaces, one management and two dataplane interfaces as shown below. To use the customizable ARM templates available in the GitHub repository, see Use the ARM Template to Deploy the VM-Series Firewall.



STEP 1 | Set up an Azure account.

1. Create a Microsoft account.
2. Log in to the Azure portal (**`https://portal.azure.com`**) using your Microsoft account credentials.

If you are using a trial subscription, you may need to open a support request (Help + Support > New Support Request) to increase the quota of allocated VM cores.

STEP 2 | Find the VM-Series solution template in the Azure Marketplace.

1. Search for Palo Alto Networks on the Azure China marketplace (https://market.azure.cn/zh-cn). The offering for the different PAN-OS versions of the VM-Series firewalls displays.

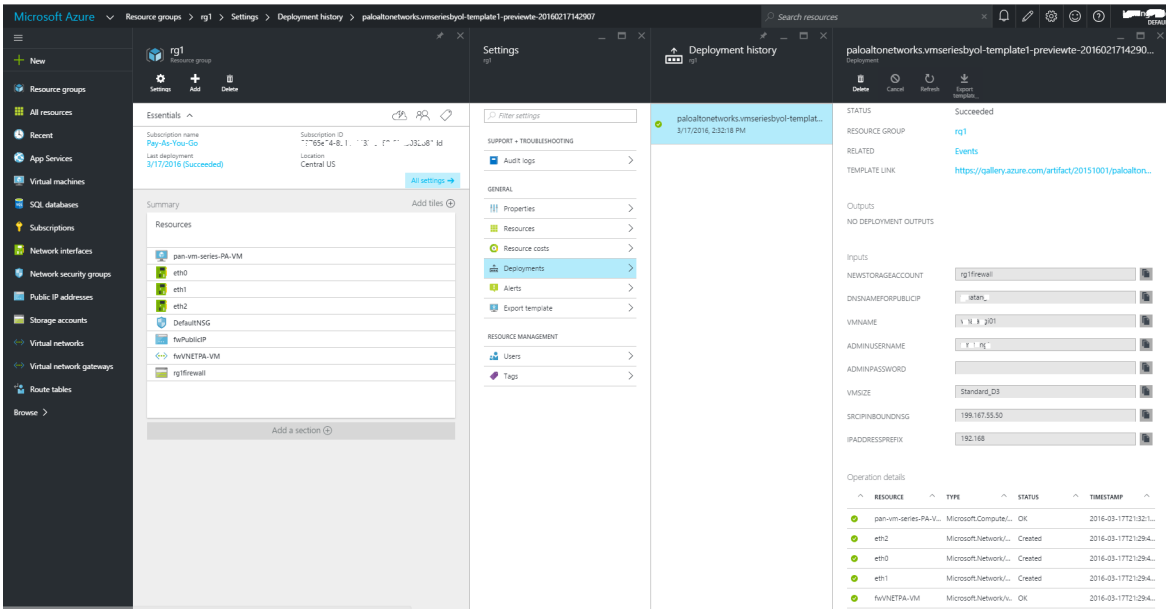
2. Select an offering and click **Immediate deployment of**.

STEP 3 | Deploy the firewall.

1. Select your Azure **Subscription**.
2. Select a resource group for holding all the resources associated with the VM-Series firewall in this deployment.

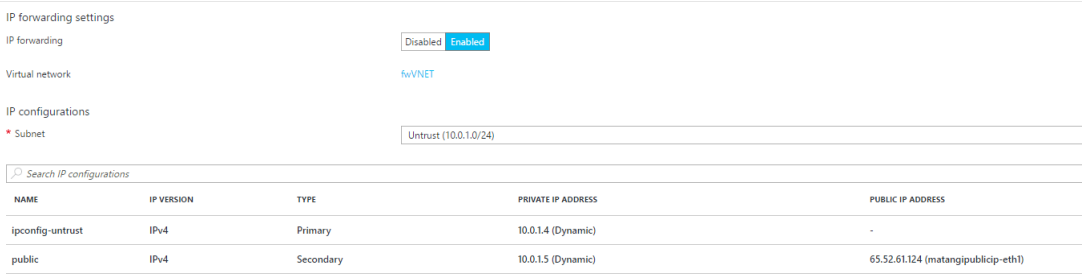
   You can deploy the VM-Series firewall into a new Resource Group, or an existing Resource Group that is empty. To deploy the firewall into an existing resource group that has other resources, use the ARM template in the GitHub Repository or your own custom ARM template. Ensure that the existing resources match the parameter values you provide in the ARM template.

   1. If you create a new resource group, enter a name for the resource group and select the Azure China region where you want to deploy the firewall.
   2. If you select an existing resource group, select the Azure China region for this resource group, and select complete deployment.
3. Configure basic settings for the firewall.
   1. Enter the storage account name for an existing account or create a new one.
   2. Enter the name for the blob storage container to which the firewall vhd image will be copied and saved.
   3. Enter a DNS name for accessing the Public IP address on the management interface (eth0) of the firewall. To access the web interface of the firewall, you must combine the prefix you enter with the suffix, for example: <*yourDNSname*><*china_region*>.cloudapp.azure.com
   4. Enter a **Username** for the firewall administrator.
   5. Enter a **Password** for securing administrative access to the firewall.
   6. Select the Azure virtual machine tier and size to meet your needs. See Minimum System Requirements for the VM-Series on Azure.
   7. Enter a **VmName**, which is a display name to identify the VM-Series firewall within the resource group.
   8. Use a **PublicIPAddressName** to label the firewall management interface within the resource group. Microsoft Azure binds the DNS name that you defined with this name so that you can access the management interface on the firewall from the public internet.
   9. Enter a **VirtualNetworkName** to identify your VNet. The default IP **Address Prefix** for the VNet is 10.0.0.0/16. You can change this to meet your IP addressing needs.
   10. Configure the subnets for the network interfaces. If you use an existing VNet, you must have defined three subnets, one each for the management, trust and untrust interfaces. If you create a new VNet, verify or change the prefixes for each subnet. The default subnets are 10.0.1.0/24, 10.0.2.0/24, and 10.0.3.0/24. You can allocate these subnets to the management, trust, and untrust interfaces as you would like.
4. Review the summary, accept the terms of use and privacy policy, and click **Immediate deployment** to deploy the firewall. The deployment maybe take 20 minutes and you can use the link on the page to verify progress.
5. Verify that you have successfully deployed the VM-Series firewall.
   1. Log in to the Azure China portal (https://portal.azure.cn) using your Microsoft account credentials.
   2. Select **Dashboard** > **Resource Groups**, select the resource group.
   3. Select **All Settings** > **Deployments** > **Deployment History** for detailed status



STEP 4 | Attach a public IP address for the untrust interface of the VM-Series firewall. This allows you to access the interface from the public internet and is useful for any internet-facing application or service.

1. On the Azure portal, select the network interface for which you want to add a public IP address. For example the eth1 interface.
2. Select **IP Configurations** > **Add** and for Public IP address, select **Enabled**. Create a new public IP address or select one that you have available.
3. Verify that you can view the secondary IP address associated with the interface.

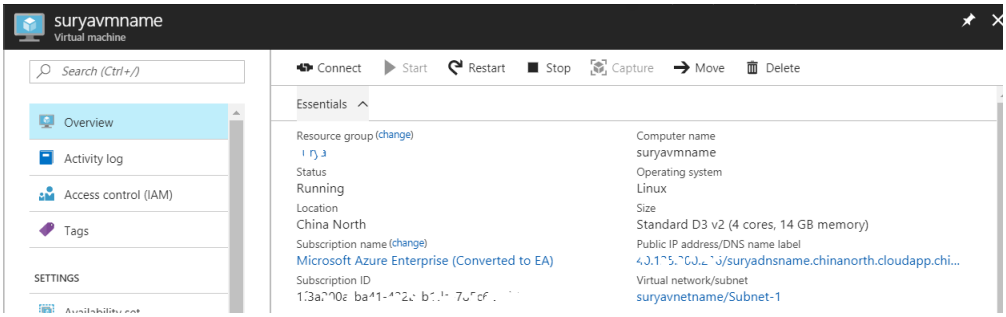


When you attach a secondary IP address to a network interface, the VM-Series firewall does not automatically acquire the private IP address assigned to the interface. You will need to manually configure the private IP address using the VM-Series firewall web interface. See Configure the dataplane network interfaces as Layer 3 interfaces on the firewall.

Each interface on the VM-Series firewall on Azure can have one dynamic (default) or static private IP address, and multiple public IP addresses (static or dynamic) associated with it. The maximum number of public IP addresses you can assign to an interface is based on your Azure subscription. When you create a new public IP address you get one from the block of IP addresses Microsoft owns, so you can't choose a specific one.

STEP 5 | Log in to the web interface of the firewall.

1. On the Azure portal, in **All Resources**, select the VM-Series firewall and view the full DNS name for the firewall.



2. Using a secure connection (https) from your web browser, log in to the DNS name for the firewall.
3. Enter the username/password you defined earlier. You will see a certificate warning; that is okay. Continue to the web page.

STEP 6 | Activate the licenses on the VM-Series firewall.

1. Create a Support Account.
2. Register the VM-Series Firewall (with auth code).
3. On the firewall web interface, select **Device** > **Licenses** and select **Activate feature using authentication code**.
4. Enter the capacity auth-code that you registered on the support portal. The firewall will connect to the update server (updates.paloaltonetworks.com), and download the license and reboot automatically.
5. Log back in to the web interface and confirm the following on the **Dashboard**:
   - A valid serial number displays in **Serial#**.

     If the term Unknown displays, it means the device is not licensed. To view traffic logs on the firewall, you must install a valid capacity license.
   - The **VM Mode** displays as Microsoft Azure.

STEP 7 | Configure the dataplane network interfaces as Layer 3 interfaces on the firewall.

If you are hosting multiple websites or services with different IP addresses and SSL certificates on a single server, you might need to configure more than one IP address on the VM-Series firewall interfaces.

1. Select **Network** > **Interfaces** > **Ethernet**.
2. Click the link for **ethernet 1/1** and configure as follows:
   - **Interface Type**: Layer3 (default).
   - 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 called UnTrust, and then click OK.
   - On the **IPv4** tab, select **DHCP Client** if you plan to assign only one IP address on the interface. The private IP address assigned in the ARM template will be automatically acquired. If you plan to assign more than one IP address select **Static** and manually enter the primary and secondary IP addresses assigned to the interface on the Azure portal.
   - Clear the **Automatically create default route to default gateway provided by server** check box. Disabling this option ensures that traffic handled by this interface does not flow directly to the default gateway in the VNet.
3. Click the link for **ethernet 1/2** and configure as follows:
   - Set **Interface Type** to Layer3 (default).
   - **Security Zone**: Trust
   - **IP address**: Select **DHCP Client** or **Static**.

- Clear the **Automatically create default route to default gateway provided by server** check box. Disabling this option ensures that traffic handled by this interface does not flow directly to the default gateway in the VNet.

4. Click **Commit**. Verify that the link state for the interfaces is up.

STEP 8 | Configure the firewall for your specific deployment.

- Gateway—Deploy a 3rd party load balancer in front of the UnTrust zone.
- Hybrid and Inter-VNet—Deploy an Azure VPN Gateway or a NAT virtual machine in front the UnTrust zone.
- Inter-Subnet—On the VM-Series firewall, add an intra-zone security policy rule to allow traffic based on the subnets attached to the Trust interface.
- GlobalProtect—Deploy a NAT virtual machine in front of the UnTrust zone.

STEP 9 | Direct traffic to the VM-Series firewall.

1. To ensure that the VM-Series firewall secures all traffic within the Azure resource group, configure static routes on the firewall.
2. Configure UDRs to direct all traffic through the interfaces on the VM-Series firewall. Refer to the Azure documentation on UDRs for details.

   The UDRs on the internal subnets must send all traffic through the Trust interface. The UDRs on the UnTrust side direct all traffic from the Internet through the UnTrust interface on the VM-Series firewall. The traffic from the Internet may be coming from an Azure Application Gateway or Azure Load Balancer, or through the Azure VPN Gateway in case of a hybrid deployment that connects your on-premises network with the Azure cloud.

Use the ARM Template to Deploy the VM-Series Firewall

In addition to Marketplace based deployments, Palo Alto Networks provides a GitHub repository which hosts sample ARM templates that you can download and customize for your needs. ARM templates are JSON files that describe the resources required for individual resources such as network interfaces, a complete virtual machine or even an entire application stack with multiple virtual machines. ARM templates are for advanced users; refer to the Microsoft documentation on ARM Templates.

To simplify the deployment of all the required resources, the template includes two json files:

- **Template File**—The azureDeploy.json is the main resources file that deploys all the components within the resource group.
- **Parameters File**—The azureDeploy.parameters.json is the file that includes the parameters required to successfully deploy the VM-Series firewall in the VNet. It includes details such as the virtual machine tier and size, username and password for the firewall, the name of the storage container for the firewall. You can customize this file for your Azure VNet deployment.

To help you deploy the firewall as a gateway for Internet-facing applications, the template provisions the VM-Series firewall, a database server, and a web server. The VNet uses the private non-routable IP address space 192.168.0.0/16. You can modify the template to use 172.16.0.0/12, or 10.0.0.0/8.

The ARM template also provides the necessary user-defined rules and IP forwarding flags to enable the VM-Series firewall to secure the Azure resource group. For the five subnets—Trust, Untrust, Web, DB, and NAT—included in the template, you have five route tables, one for each subnet with user defined rules for routing traffic to the VM-Series firewall and the NAT virtual machine.

For the four subnets—Trust, Untrust, Web, and DB—included in the template, you have four route tables, one for each subnet with user defined rules for routing traffic to the VM-Series firewall.

ARM templates are for advanced users. Palo Alto Networks provides the ARM template under the community supported policy.

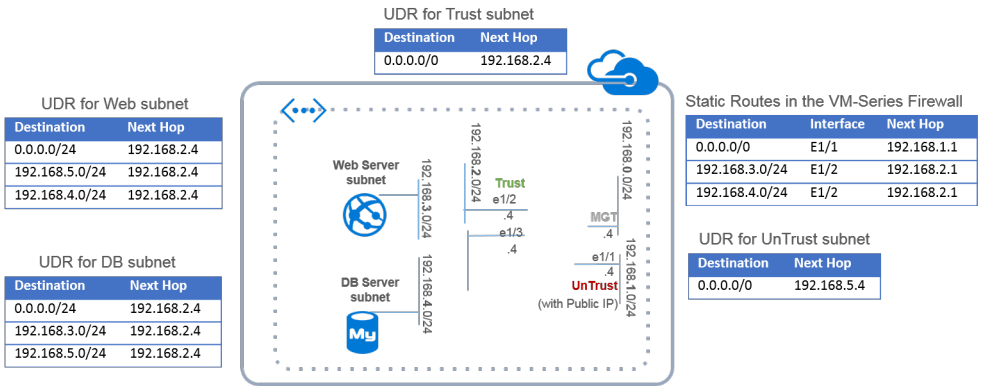


Figure 12: Deploying VM-Series Firewall using the ARM Template

STEP 1 | Download the ARM template from the GitHub repository.

Download and save the files to a local client: https://github.com/PaloAltoNetworks/azure

For Azure China: github.com/PaloAltoNetworks/Azure-China

STEP 2 | (Only for Azure China) Copy the VHD image for the VM-Series firewall to your Azure storage account.

Get the image from https://paloaltonetworks.blob.core.chinacloudapi.cn/vm-series/PA-VM-AZR-8.0.0.vhd.

STEP 3 | Create a Resource Group on Azure.

1. Log in to the Azure CLI using the command: **`azure login`**

   If you need help, refer to the Azure documentation on installing the CLI, or for details on how to access the CLI on Azure Government or Azure China.
2. Switch to Resource Manager mode using the command: **`azure config mode arm`**
3. Create a resource group.

STEP 4 | Deploy the ARM template.

1. Open the Parameters File with a text editor and modify the values for your deployment:

   In Azure China, you must edit the path for the storage account that hosts the VHD image required to deploy the VM-Series firewall. In the variables section of the template file, find the parameter called userImageNameURI and replace the value with the location where you saved the VHD image.
2. Deploy the template in the resource group you created.

```
azure group create -v -n "YourResourceGroupName"
-l "YourAzureLocation" -d "GiveASmallDeploymentLabel"
-f azureDeploy.json -e azureDeploy.parameters.json
```

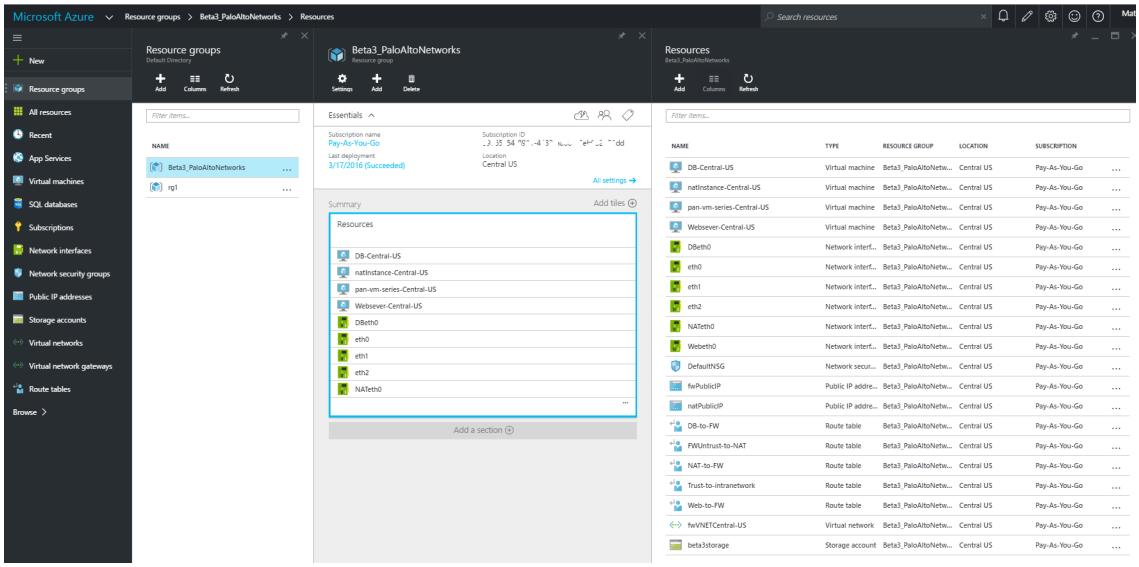
3. Check the progress/status of the deployment from the Azure CLI:

```
azure group deployment show "YourResourceGroupName" "YourDeploymentLabel"
```

   When the template is successfully deployed the `ProvisioningState is Running`.

   If the `ProvisioningState is Failed`, you must check for errors on the Azure portal at Resource Group > Events. Filter for only events in the last one hour, select the most recent events, and drill down to find the errors.
4. Verify that you have successfully deployed the VM-Series firewall.
   1. Select **Dashboard** > **Resource Groups**, select the resource group.
   2. Select **All Settings** > **Deployments** > **Deployment History** for detailed status.



The address space within the VNet uses the prefix 192.168, which is defined in the ARM template.

5. Attach a public IP address to the untrust interface on the firewall.

STEP 5 | Configure the firewall as a VNet gateway to protect your Internet-facing deployment.

1. Log in to the management interface IP address on the firewall.
2. Configure the dataplane network interfaces as Layer 3 interfaces on the firewall (**Network** > **Interfaces** > **Ethernet**).
3. Add static rules to the virtual router on the firewall. To route traffic through the firewall in this example, you need three static routes on the firewall (**Network** > **Virtual Routers**, select the router and click **Static Routes**):
    1. Route all outbound traffic through the UnTrust zone, ethernet1/1 to the Azure router at 192.168.1.1.
    2. Route all inbound traffic destined to the web server subnet through the Trust zone, ethernet1/2 to the Azure router at 192.168.2.1.
    3. Route all inbound traffic destined to the database server subnet through the Trust zone, ethernet1/2 to the Azure router at 192.168.2.1.
4. Create security policy rules (**Policies** > **Security**) to allow inbound and outbound traffic on the firewall. You also need security policy rules to allow appropriate traffic from the web server subnet to the database server subnet and vice versa.
5. **Commit** the changes on the firewall.
6. Verify that the VM-Series firewall is securing traffic (**Monitor** > **Logs** > **Traffic**).

VM Monitoring on Azure

VM Monitoring of Microsoft® Azure® resources enables you to dynamically update security policy rules to consistently enforce Security policy across all assets deployed within your Azure subscription. The VM Monitoring solution on Azure uses a VM Monitoring script that runs on a virtual machine within the Azure public cloud. This script collects the IP address-to-tag mapping for all your Azure assets and uses the API to push the VM information to your Palo Alto Networks® firewall(s).

About VM Monitoring on Azure

As you deploy or terminate virtual machines in the Azure public cloud, you can use the VM Monitoring solution for Azure to consistently enforce security policy rules on these workloads.

The VM Monitoring solution on Azure uses a VM Monitoring script that runs on a virtual machine in the Azure public cloud environment. The operating system of the virtual machine that the script runs on, must be Red Hat Enterprise Linux (RHEL) 7.4 with Python version 2.7.5. The script collects the IP address to tag mappings for all your Azure assets and uses the Azure and PAN-OS APIs to register the VM information—IP address to tag mapping—on the firewalls you specify. You can specify one or more virtual systems on the firewall to which you want to register the VM information.

The solution, which is posted on GitHub, is released under the official support policy of Palo Alto Networks through the support options that you've purchased. The GitHub repository includes two files:

- Parameters file—The parameters file is named **parameters.json**. This file allows you to specify details on your Azure subscription, how to authenticate to it, which Azure resources to monitor, and to which firewalls you want to publish the IP address to tag mapping information that the script collects.
- VM Monitoring script—The VM Monitoring script uses Python and is named **run.py**. This script collects the IP address-to-tag mapping information for the Azure deployment that you want to monitor and pushes the information to the specified firewalls using the PAN-OS API. The script registers new IP address to tag mapping on the firewalls, and unregisters IP addresses and tags that are deprovisioned in your Azure deployment from the firewall. To prevent overwriting the VM information, make sure that a virtual system receives IP address and tag information from one instance of the script only.

  You must use the management interface on the firewall to communicate with the virtual machine (RHEL instance) that runs the script.

  The script generates 2 sets of log files. The audit log includes all messages, including the API calls and the responses. The error log includes error messages only. The log files require about 30 GB on the hard disk of the virtual machine. The log file is rotated at 1 GB, and a maximum of 30 logs files are stored on disk. If you want persistent log storage, make sure to export or archive the log files to an external location.

You can deploy one or more instances of the virtual machine (RHEL instance) to run the VM Monitoring script that monitors your Azure subscription. Because the script is designed to execute as a cron task, the script executes only when it detects that the process isn't already running. Therefore, a new cron task does not execute when one is running, and you cannot have multiple instances of the VM Monitoring script run on a single virtual machine (RHEL instance).

Gather the Resources Required for VM Monitoring on Azure

The following table lists the resources needed to deploy this VM Monitoring solution for Microsoft® Azure®.

What you need	Description
❑ System Requirements for the virtual machine. *Only one instance of the VM Monitoring script can run on a virtual machine instance.*	The VM Monitoring solution on Azure requires a system with: • **Operating System**—Red Hat Enterprise Linux (RHEL) 7.4 • **Python Version**—2.7.5 • **Disk Size**—60GB minimum
❑ Set up the Active Directory application and a Service Principal to enable API access for the VM Monitoring script.	Because the VM Monitoring script uses the Azure API to collect the attributes for your Azure deployment, you need to set up an Active Directory application and a Service Principal to assign permissions. When you follow the instructions in the preceding link, you must assign an IAM role with a minimum privilege of **reader** when prompted to **Assign application to role**. The workflow will provide you with various keys and IDs that are required to generate an Azure Bearer Token used in the header of the API call. Ensure that you collect the following information, which you must enter as input in the parameters.json file: • **Application ID**— • **Authentication Key**—Make sure to jot down this secret key. You cannot view this key again. • **Directory ID**— • Subscription ID—

❑ Collect the details required for the parameters.json file that the script invokes to monitor your Azure deployment.
 	
`{"parameters":{"clientId":{"value":"e12a3fb1-cef2-0000-abf8-7a9cee0dd55f"},`
`"clientSecret":{"value":"jEWXJcNswGWv9VmpJCR80S2GQl/eDQq3W6Yu7yjN2/c="},`
`"tenantId":{"value":"77a9116e-edcc-44b6-84c4-4f19fdda335b"},`
`"subscriptionId":{"value":"0123402e-4559-4b1a-b645-92fa1234f4b8"},`
`"targetIps":{"value":"172.30.161.201, 172.30.161.202"},`
`"resourceGroupName":{"value":"vmscript5RG",`
	You must have the following information to fill out the parameters.json file:
	• **Client ID**—The Application ID that you copied earlier.
	• **Secret Key**—The authentication key you copied earlier when you set up the Active Directory application. To to log in as the application, the key value with the Application ID are required.
	• **Tenant ID**—The Directory ID you copied earlier.

What you need	Description

<pre>"vnetName":{"value": "vpn5vnet5"},
"targetApiKeys":{"value":"LUFRPT14MW5xOEo
1R09KVlBZNnpnemh0VHRBOWl6TGM9bXcwM
JHUGVhRlNiY0dCR0srNERUQT09,00000000
000ZNnpnemh0VHRBOWl6TGM9bXcwM3JHUG
hRlNiY0dCR0sra"},
"targetVsys":{"value": "vsys1,vsys3"}}}</pre>
	• **Azure Subscription ID**—The Azure subscription you want to monitor.
	• **Target IPs**—A comma separated list of IP addresses of the next-gen firewalls to which you want to register the IP address-to-tag mapping. You can then configure the firewalls that receive the VM information to enforce policy.
	If the firewalls are in an HA configuration, include the IP address for both HA peers. The script will register tags to the active peer only.
	• **Vsys**—The virtual system that you want to set as the destination for registering the IP address-to-tag mapping that the script retrieves.
	• **Resource Group Name**—(Optional, but recommended if you have overlapping IP addresses across your Resource groups and VNets within your subscription) Enter (only) one resource group name that you want to monitor.
	• **VNet Name**—(Optional, but recommended if you have overlapping IP addresses in your resource group) Enter the name of a single VNet that you want to monitor.
	• **API Keys**—Comma separated list of the API keys for the administrative user account on each firewall.
	For all comma separated values—Target IPs, API keys, and Vsys—you should not have space between the comma and the value.

Set Up VM Monitoring on Azure

This workflow guides you through deployment of the RHEL virtual machine and configuration of the VM monitoring script to run as a cron task on this RHEL instance so that the script can collect the virtual

machine attributes within your Azure subscription. You can then use this information to proactively enforce policy using your Palo Alto Networks firewalls.

There is no default interval or frequency at which the script will execute, so you must configure the script to run at a specific interval at which the script collects the IP address-to-tag mapping and publishes the information to a target virtual system on your next-gen firewalls. The script registers new IP addresses and associated tags on the firewall, and unregisters IP addresses and tags for assets that were deleted or terminated within your Azure environment.

STEP 1 | Make sure that you first Gather the Resources Required for VM Monitoring on Azure.

STEP 2 | Deploy a Red Hat Enterprise Linux 7.4 OS with at least 60GB hard disk space on the Azure public cloud.

The virtual machine must have network connectivity to the management interface of the firewalls to which you are registering the IP address-to-tag information.

STEP 3 | Use an SSH client to log in to the virtual machine and verify the python version with the command **`python -V`**.

Authenticate to the RHEL virtual machine using the option —password or SSH key— you selected when deploying the instance.

STEP 4 | Copy the files from the GitHub repository to the virtual machine.

The VM Monitoring solution includes two files— parameters.json and run.py.

```
git clone https://github.com/PaloAltoNetworks/azure-vm-monitoring
```

STEP 5 | Edit the parameters.json file and specify the resources you want to monitor within your Azure subscription.

```
vi parameters.json
```

STEP 6 | Set up the cron task to run the VM Monitoring script at a specified frequency.

The minimum frequency you can set is one minute. The amount of time the script takes to retrieve the IP address-to-tag information in your environment and register it on the firewall varies based on the number of virtual machines in your deployment.

1. To set up the cron task, enter the following command:

   ```
   sudo crontab -e
   ```

   This will open up an editor where you can enter the interval and specify the absolute path for the directory in which to save the log files. For example:

   ```
   */5 * * * * /usr/bin/python/home/vmMonitoring/run.py -f
   /home/vmMonitoring/parameters.json -l /vmagentlogs
   ```

2. Verify that the cron task is set up properly with the command **`sudo crontab -l`**

*To execute the VM Monitoring script on demand, use the command **`python run.py -f parameters.json -l <log-directory>`**, where log directory is the absolute path where you want to save the log files.*

STEP 7 | Open the audit log file to confirm that the script was executed successfully and to view the IP address-to-tag mapping that it retrieved.

```
vi <log-directory>/audit.log
```

```
</entry><count>7</count></result></response>2018-03-20 17:24:31.822
+0000 VM Monitoring log INFO: : Get Tags: retrieved 7 tags2018-03-20
17:24:31.822 +0000 VM Monitoring log INFO: : Get Tags: Retrieved total
of 7 tags2018-03-20 17:24:32.167 +0000 VM Monitoring log INFO: : Get
Tags: <response status="success"><result>Session target vsys changed to
none</result></response>2018-03-20 17:24:32.168 +0000 VM Monitoring log
INFO: : current: ['10.155.1.1', '10.155.1.2', '10.155.1.3', '10.155.2.1',
'10.155.2.2', '10.155.3.3', '10.155.3.4']2018-03-20 17:24:32.168 +0000
VM Monitoring log INFO: : new: ['10.155.1.1', '10.155.1.2', '10.155.1.6',
'10.155.2.1', '10.155.2.2', '10.155.3.5', '10.155.3.6']2018-03-20
17:24:32.168 +0000 VM Monitoring log INFO: : Script completed normally.
```

STEP 8 | Log in to the CLI on the firewall and verify that you can view the IP address and tags that the script published.

You can quickly confirm that the registered VM count on the firewall matches the audit log:

On a hardware-based firewall, you must specify the target virtual system on which you are registering the VM information using the following command:

```
admin@PA500> set system setting target-vsys vsys1

Session target vsys changed to vsys1

admin@PA5000vsys1>show object registered-ip all
```

```
registered IP                          Tags
10.155.2.5                           #"azure-tag.vm-name.vrpn5server"
                                     "azure-tag.resource-group.vrpn5RG”
                                     "azure-tag.subnet.vrpn5Untrust"
                                     "azure-tag.vnet.vrpn5vnet0"
                                     "azure-tag.region.eastus2"
                                     "azure-tag.vm-size.Standard_D2s_v3”
                                     "azure-tag.os-type.Linux"
                                     "azure-tag.os-publisher.Canonical"
                                     "azure-tag.os-offer.UbuntuServer"
                                     "azure-tag.os-sku.16.04-LTS"
```

STEP 9 | Set up Dynamic Address Groups and use them in Security policy.

Attributes Monitored on Azure

The VM Monitoring script allows you to gather the following set of metadata elements or attributes on the virtual machines in your Microsoft® Azure® deployment.

Attributes Monitored	Example
VM Name	azure-tag.vm-name.web_server1
VM Size	azure-tag.vm-size.standard_ds2_v2
OS Type	azure-tag.os-type.Linux
OS Publisher	azure-tag.os-publisher.Canonical
OS Offer	azure-tag.os-offer.UbuntuServer

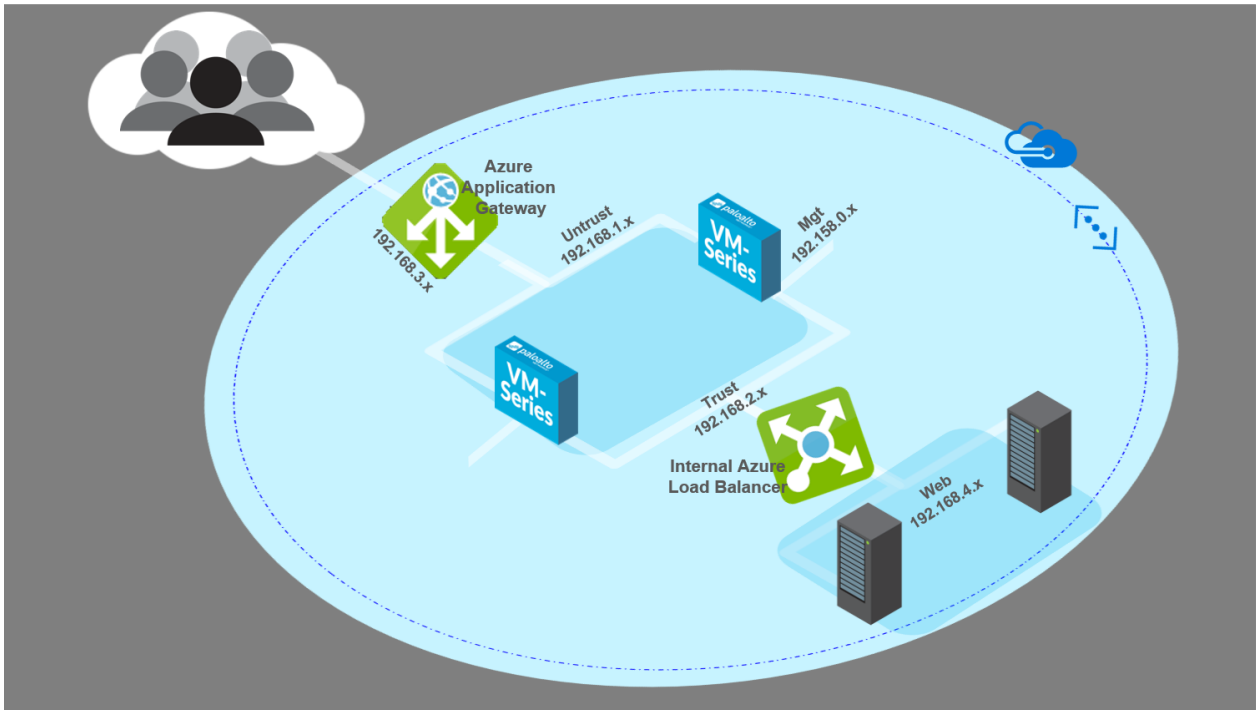
Attributes Monitored	Example
OS SKU	azure-tag.os-sku.14.04.5-LTS
Subnet	azure-tag.subnet.webtier
VNet	azure-tag.vnet.untrustnet
Azure Region	azure-tag.region.east-us
Resource Group Name	azure-tag.resource-group.myResourceGroup
User Defined Tags	azure-tag.mytag.value

Deploy the VM-Series and Azure Application Gateway Template

The VM-Series and Azure Application Gateway template is a starter kit that you can use to deploy VM-Series firewalls to secure web workloads for internet-facing deployments on Microsoft Azure (currently not available for Azure China).

This template deploys two VM-Series firewalls between a pair of (external and internal) Azure load balancers. The external load balancer is an Azure Application Gateway, which is an HTTP (Layer 7) load balancer that also serves as the internet-facing gateway, which receives traffic and distributes it through the VM-Series firewall on to the internal load balancer. The internal load balancer is an Azure Load Balancer (Layer 4) that fronts a pair of web servers. The template supports the BYOL and the Azure Marketplace versions of the VM-Series firewall.

As demand on your web workloads increases and you increase capacity for the web server tier you can manually deploy additional VM-Series firewalls to secure your web server tier.

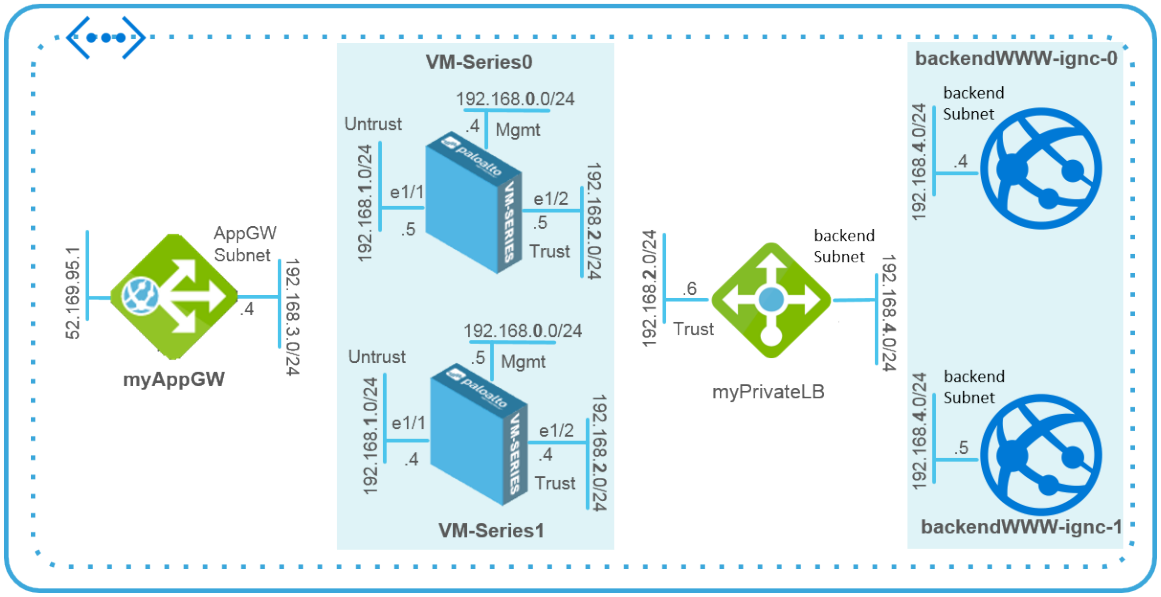


- VM-Series and Azure Application Gateway Template
- Start Using the VM-Series & Azure Application Gateway Template

VM-Series and Azure Application Gateway Template

The VM-Series and Azure Application Gateway template launches an Azure Application Gateway (Layer 7 load balancer) and an Azure (Layer 4) load balancer. Nested between the Application gateway and the load balancer are a pair of VM-Series firewalls in an Availability Set, and a pair of sample web servers running

Apache2 on Ubuntu in another Availability Set. The Availability Sets provide protection from planned and unplanned outages. The following topology diagram shows the resources that the template deploys:



You can use a new or an existing storage account and resource group in which to deploy all the resources for this solution within an Azure location. It does not provide default values for the resource group name and storage account name, you must enter a name for them. While you can create a new or use an existing VNet, the template creates a default VNet named *vnet-FW* with the CIDR block 192.168.0.0/16, and allocates five subnets (192.168.1.0/24 - 192.168.5.0/24) for deploying the Azure Application Gateway, the VM-Series firewalls, the Azure load balancer and the web servers. Each VM-Series firewall is deployed with three network interfaces—ethernet0/1 in Mgmt subnet (192.168.0.0/24), ethernet1/1 in Untrust subnet (192.168.1.0/24), and ethernet1/2 in Trust subnet(192.168.2.0/24).

The template creates a Network Security Group (NSG) that allows inbound traffic from any source IP address on ports 80,443, and 22. It also deploys the pair of VM-Series firewalls and the web server pair in their respective Availability Sets to ensure that at least one instance of each is available during a planned or unplanned maintenance window. Each Availability Set is configured to use three fault domains and five update domains.

The Azure Application Gateway acts as a reverse-proxy service, which terminates a client connection and forwards the requests to back-end web servers. The Azure Application Gateway is set up with an HTTP listener and uses a default health probe to test that the VM-Series firewall IP address (for ethernet1/1) is healthy and can receive traffic.

The template does not provide an auto-scaling solution; you must plan your capacity needs and then deploy additional resources to Adapt the Template *for your deployment.*

The VM-Series firewalls are not configured to receive and secure web traffic destined to the web servers. Therefore, at a minimum, you must configure the firewall with a static route to send traffic from the VM-Series firewalls to the default router, configure destination NAT policy to send traffic back to the IP address of the load balancer, and configure Security policy rules. The NAT policy rule is also required for the firewall to send responses back to the health probes from the HTTP listener on the Azure Application Gateway. To assist you with a basic firewall configuration, the GitHub repository includes a sample configuration file called *appgw-sample.xml* that you can use to get started.

Start Using the VM-Series & Azure Application Gateway Template

The VM-Series & Azure Application Gateway template launches all the resources you need to deploy and secure your web workloads for Internet facing deployments on Microsoft Azure, excluding Azure China. This section provides details on how to deploy the template, configure the firewalls to route and secure traffic destined to the web servers, and extend the capabilities and resources that this template provides to accommodate your deployment needs.

- Deploy the Template to Azure
- VM-Series and Azure Application Gateway Template Parameters
- Sample Configuration File
- Adapt the Template

Deploy the Template to Azure

Use the following instructions to deploy the template to Azure.

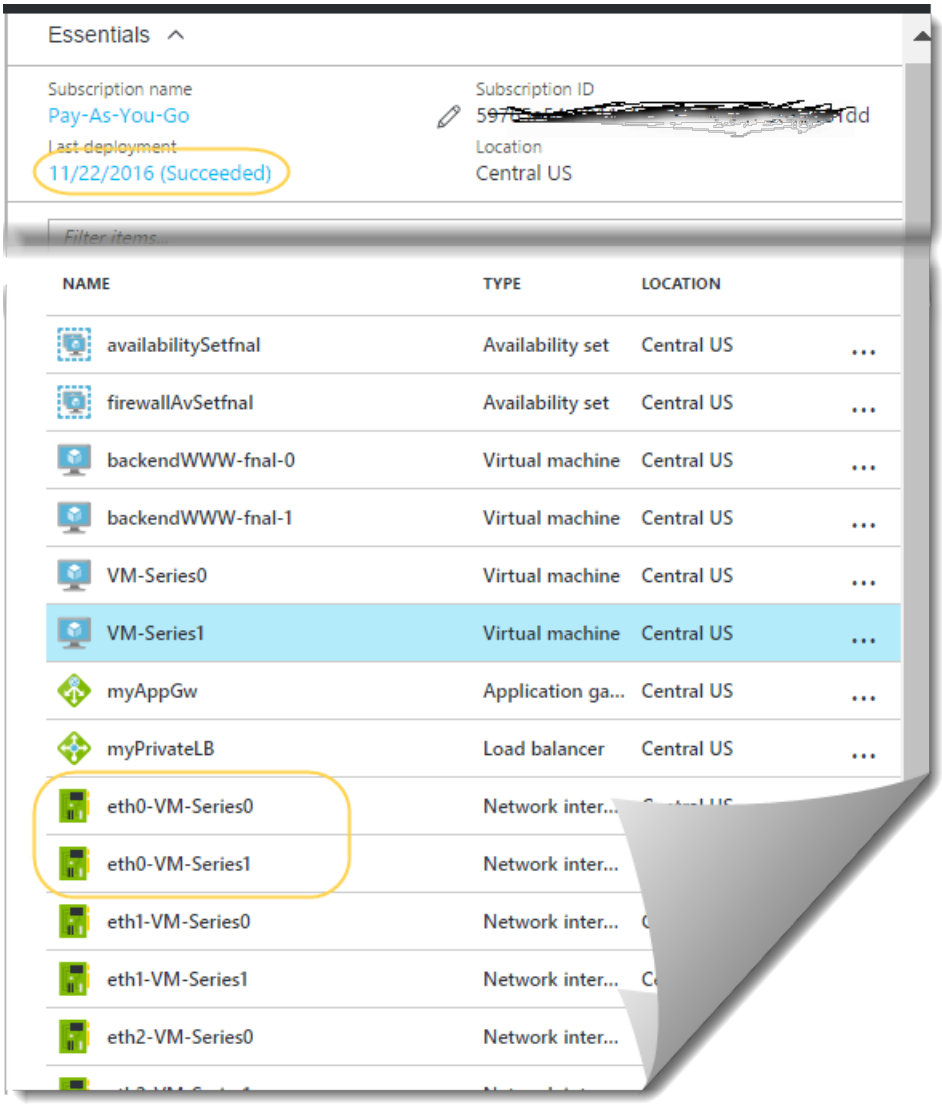
STEP 1 | Deploy the template.

Currently not available for deploying in Azure China.

1. Access the template from https://github.com/PaloAltoNetworks/azure-applicationgateway
2. Click **Deploy to Azure**.
3. Fill in the details for deploying the template. See VM-Series and Azure Application Gateway Template Parameters for a description and the default values, if any, for each parameter.

   At a minimum, you have to pick the **Azure Subscription**, **Resource Group**, **Location**, **Storage Account Name**, and a **Username/password** or **SSH Key** for the administrative account on the VM-Series firewalls.
4. Click **Purchase** to accept the terms and conditions and deploy the resources.

   If you have validation errors, click to view the details and fix your errors.
5. On the Azure portal, verify that you have successfully deployed the template resources, including the VM-Series firewalls.
   1. Select **Dashboard** > **Resource Groups**, select the resource group.
   2. Select **Overview** to review all the resources that have been deployed. The deployment status should display **Succeeded**.



3. Note the Public IP address or the DNS name assigned to **eth0-VM-Series0** and **eth0-VM-Series1** to access the management interface of the VM-Series firewalls.

STEP 2 | Log in to the firewalls.

1. Using a secure connection (https) from your web browser, log in to the IP address for eth0-VM-Series0 or the DNS name for the firewall.
2. Enter the username/password you defined in the parameters file. You will see a certificate warning; that is okay. Continue to the web page.

STEP 3 | Configure the VM-Series firewall.

You can either configure the firewall manually or import the Sample Configuration File provided in the GitHub repository and customize it for your security needs.

- **Configure the firewall manually**—You must do the following at a minimum:

1. Configure the dataplane network interfaces as Layer 3 interfaces on the firewall (**Network** > **Interfaces** > **Ethernet**).

2. Add a static rule to the virtual router on the firewall. This static rule specifies the firewall's untrust interface IP address as the nexthop address for any traffic destined for ethernet1/1. (**Network** > **Virtual Routers**, select the router and click **Static Routes**).
3. Create security policy rules (**Policies** > **Security**) to allow inbound and outbound traffic on the firewall.
4. Add NAT policies (**Policies** > **NAT**). You must create destination NAT and source NAT rules on the firewall to send traffic to the web servers and back out to the client who initiated the request.

   The destination NAT rule is for all traffic that arrives on the firewall's untrust interface. This rule is required to translate the destination IP address on the packet to that of the internal load balancer so that all traffic is directed to the internal load balancer and on to the backend web servers.

   The source NAT rule is for all traffic from the backend web server and destined to the untrust interface on the firewall. This rule translates the source address to the IP address of the trust interface on the firewall
5. **Commit** your changes.

   - **Import the sample configuration file:**
6. Download and save the Sample Configuration File to your local client.
7. Select **Device** > **Setup** > **Operations**, click **Import named configuration snapshot**, **Browse** to the sample configuration file that you have saved locally, and click **OK**.
8. Click **Load named configuration snapshot**, select the **Name** of the sample configuration file you just imported, and click **OK**.
9. Change the IP address of the address objects and the static route to match the IP address from the CIDR block you used. Update address objects to use the private IP addresses for eth1-VM-Series0 and eth1-VM-Series1.
10. Important! Create a new admin user account. Select **Device** > **Administrators** and **Add** a new account.
11. Modify the **Hostname** in the General Settings widget in **Device** > **Setup** > **Management**.
12. **Commit** your changes, and log out. The commit overwrites the running configuration with the sample configuration file and updates you just made. On commit, the hostname and the administrator user account that you specified when deploying the template are overwritten. You will now need to log in using the new admin user account and password.

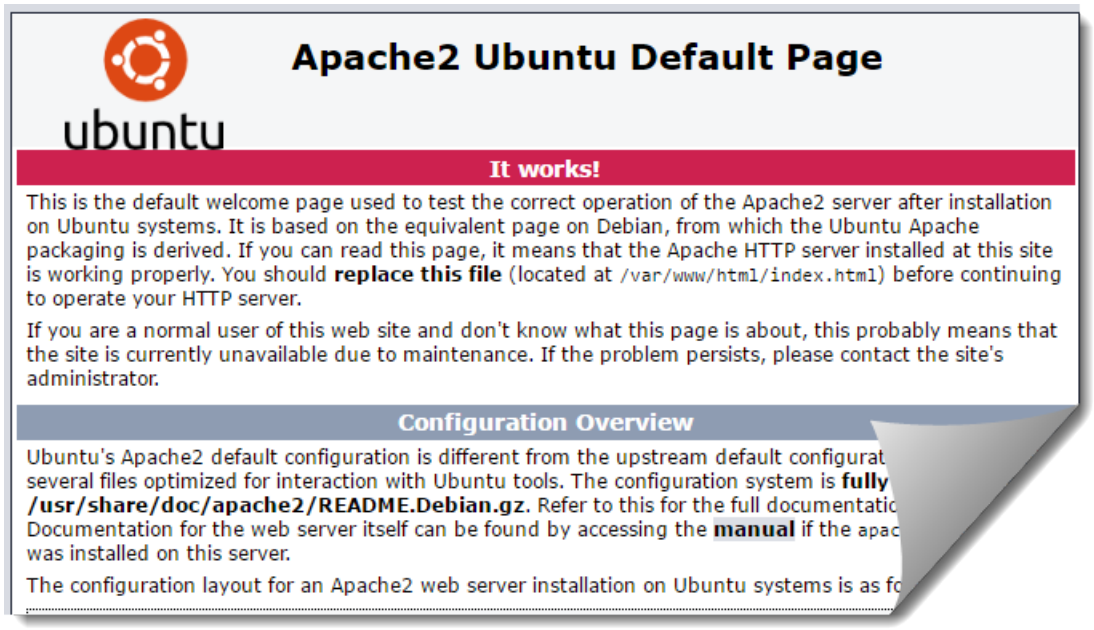
    - **Log in to the firewall**—Use the credentials you created and delete the pandemo administrative account imported as part of the sample configuration file.

STEP 4 | Log in and configure the other instance of the VM-Series firewall.

See step Configure the VM-Series firewall.

STEP 5 | Verify that you have configured the firewalls properly.

From your web browser, use http to access the IP address or DNS name for the app gateway. You should be able to view the default Apache 2 Ubuntu web page.



If you have used the sample configuration firewall, log in to the fireewall and view the Traffic logs generated on session start in **Monitor** > **Logs** > **Traffic**.

VM-Series and Azure Application Gateway Template Parameters

The following table lists the required and optional parameters and the default values, if any.

Parameter	Description
Resource group	Create new or use existing (no default).
Subscription	The type of Azure subscription you will use to cover the cost of the resources deployed with the template.
Location	Select the Azure location to which you want to deploy the template (no default).
Network Security Group	
Network Security Group Name	The network security group limits the source IP addresses from which the VM-Series firewalls and web servers can be accessed. Default: nsg-mgmt
Network Security Group Inbound Src IP	The source IP addresses that can log in to the management port of the VMs deployed by the template. The default value 0.0.0.0/0 means you can log into the firewall management port from any IP address.
Storage Account	

Parameter	Description
Storage Account Name	Create new or enter the name of an existing Storage Account (no default). The name must be globally unique.
Storage Account Type	Choose between standard and premium storage and your data replication needs for local redundancy, geo-redundancy, and read-access geo-redundancy. The default option is Locally Redundant Storage (LRS). The other options are Standard GRS, Premium LRS, and Standard RAGRS.
VNet	
Virtual Network	Create new or enter the name of an existing VNet. The default name for the VNet is vnet-FW
Virtual Network Address Prefix	192.168.0.0/16
Azure Application Gateway	
App Gateway Name	myAppGw
App Gateway DNS Name	Enter a globally unique DNS name for the Azure Application Gateway.
App Gateway Subnet Name and Prefix	Default name is AppGWSubnet and the subnet prefix is 192.168.3.0/24.
Azure Load Balancer and Web Servers	
Internal Load Balancer Name	myPrivateLB
Internal Load Balancer Subnet Name and Prefix	Default name is backendSubnet and the subnet prefix is 192.168.4.0/24.
Backend Vm Size	The default size is Standard tier D1 Azure VM. Use the drop-down in the template to view the other Azure VM options available for the backend web servers.
Firewalls	
Firewall Model	Choose from BYOL or PAYG (bundle 1 or bundle 2, each bundle includes the VM-300 and a set of subscriptions).
Firewall Vm Name and Size	The default name for the firewall is VM-Series, and the default size is Standard tier D3 Azure VM. Use the drop-down in the template to view the other Azure VM options available for the VM-Series firewalls
Mgmt Subnet Name and Prefix	The management subnet for the VM-Series firewalls and the web servers deployed in this solution.

Parameter	Description
	Default name is Mgmt and the subnet prefix is 192.168.0.0/24.
Mgmt Public IP Address Name	Enter a hostname to access the management interface on each firewall. The names must be globally unique.
Trusted Subnet Name and Prefix	The subnet to which eth1/1 on the VM-Series firewall is connected; this subnet connects the VM-Series firewall to the Azure Application gateway. The firewall receives web traffic destined to the web servers on eth1/1. Default name is Trust and the subnet prefix is 192.168.2.0/24.
Untrusted Subnet Name	The subnet to which eth1/2 on the VM-Series firewall is connected. The firewall receives return and outbound web traffic on this interface. Default name is Untrust and the subnet prefix is 192.168.1.0/24. The name must be globally unique.
Username	Enter the username for the administrative account on the VM-Series firewalls and the web servers.
Authentication Type	You must either enter a password for authentication or use an SSH public key (no default).

Sample Configuration File

To help you get started, the GitHub repository contains a sample configuration file named *appgw-sample.xml* that includes the following rules/objects:

- **Address objects**—Two address objects, `firewall-untrust-IP` and `internal-load-balancer-IP`, which you will need to modify to match the IP addresses in your setup. You need to modify these address objects to use the private IP addresses assigned to eth1-VM-Series0 and eth1-VM-Series1 on the Azure portal.
- **Static route**—The default virtual router on the firewall has a static route to 192.168.1.1, and this IP address is accurate if you use the default template values. If you have changed the Untrust subnet CIDR, you'll need to update the IP address to match your setup. All traffic coming from the backend web servers, destined for the application gateway, uses this IP address as the next hop for delivering packets to the untrust interface on the firewall.
- **NAT Policy Rule**—The NAT policy rule enables destination NAT and source NAT.
  - The destination NAT rule is for all traffic that arrives on the firewall's untrust interface (ethernet1/2), which is the firewall-untrust-IP address object. This rule translates the destination IP address on the packet to that of the internal load balancer so that all traffic is directed to the internal load balancer and thus to the backend web servers.
  - The source NAT rule is for all traffic from the backend web server and destined to the untrust network interface on the firewall. This rule translates the source address to the IP address of the trust interface on the firewall (ethernet1/2).
- **Security Policy Rule**—Two Security policy rules are defined in the sample configuration file. The first rule allows all inbound web-browsing traffic and generates a log at the start of a session on the firewall. The second rule blocks all other traffic and generates a log at the start and end of a session on the firewall. You can use these logs to monitor all traffic to the web servers in this deployment.
- **Administrative User Credentials**— The sample configuration file includes a username and password for logging in to the firewall, which is set to pandemo/demopassword. After you import the sample

configuration, you must either change the password and set it to a strong, custom password or create a new administrator account and delete the pandemo account.

Adapt the Template

As your needs evolve, you can scope your capacity needs and extend the template for your deployment scenario. Here are some ways you can build on the starter template to meet your planned capacity needs:

- Deploy additional VM-Series firewalls behind the Azure Application Gateway. You can manually install more VM-Series firewalls into the same Availability Set or launch a new Availability Set and manually deploy additional VM-Seri es firewalls.
- Configure the VM-Series firewalls beyond the basic configuration provided in the sample configuration file in the GitHub repository.
- Enable HTTPS load balancing (SSL offload) on the Azure Application Gateway. Refer to the Azure documentation for details.
- Add or replace the sample web servers included with the template.

Set Up the VM-Series Firewall on OpenStack

The VM-Series firewall for OpenStack allows you to deploy the VM-Series firewall in your OpenStack environment to provide secure application delivery along with network security, performance and visibility. This solution deploys the VM-Series firewall on a KVM/Ubuntu hypervisor in a Mirantis OpenStack environment that uses Contrail for virtualized networking functions.

VM-Series Deployments in OpenStack

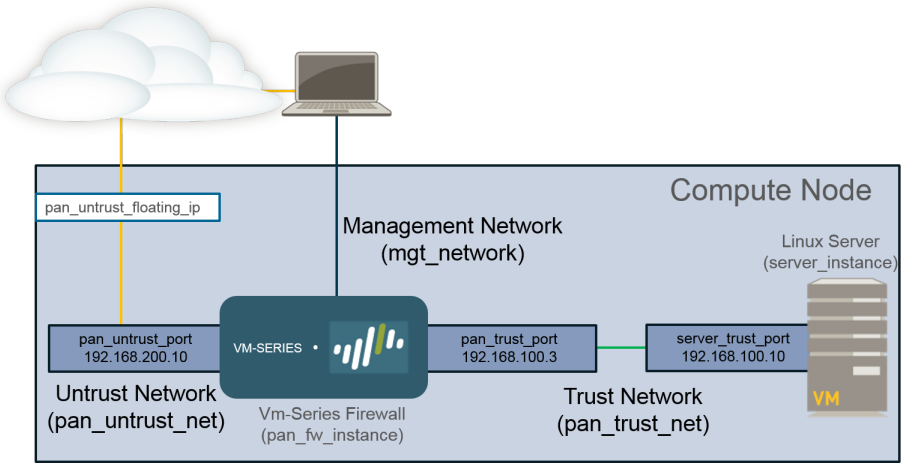
The Heat Orchestration templates provided by Palo Alto Networks allow you to deploy the VM-Series firewall individually, through service chaining, or dynamically with service scaling.

- Basic Gateway
- Service Chaining and Service Scaling

Basic Gateway

The VM-Series firewall for OpenStack allows you to deploy the VM-Series firewall on the KVM hypervisor running on a compute node in your OpenStack environment. This solution uses Heat Orchestration Templates and bootstrapping to deploy the VM-Series firewall and a Linux server. The VM-Series firewall protects the deployed Linux server by inspecting the traffic going in and out of the server. The sample bootstrap files allow the VM-Series firewall to boot with basic configuration for handling traffic.

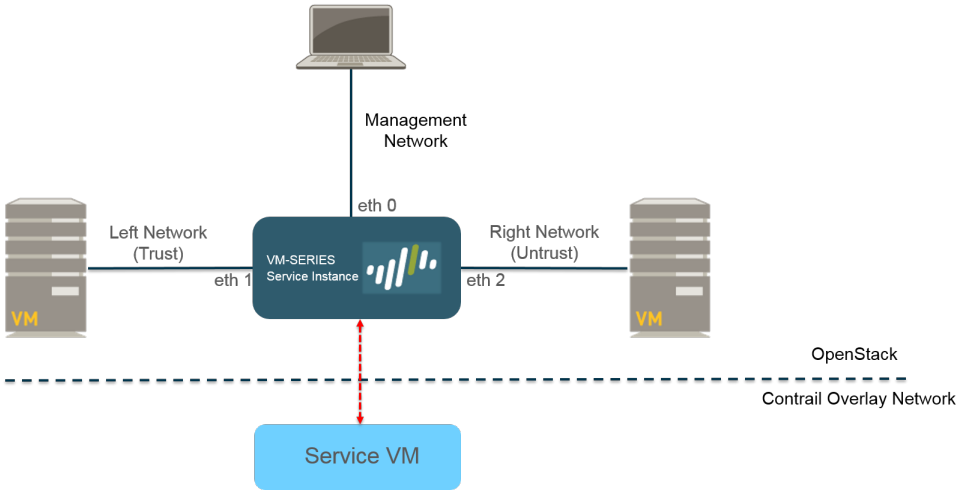
These heat template files and the bootstrap files combine to create two virtual machines, the VM-Series firewall and Linux server, in a network configuration similar to that shown below.



Service Chaining and Service Scaling

Service chaining is a Contrail feature that deploys a VM-Series firewall as a service instance in your OpenStack environment. A service chain is a set of service virtual machines, such as firewalls or load balancers, and each virtual machine in the service chain is a service instance. Service scaling allows you to dynamically deploy additional instances of the VM-Series firewall. Using CPU utilization or incoming bytes per second metrics gathered by Ceilometer, OpenStack deploys or shuts down additional instances of the VM-Series firewall to meet the current needs of your network.

The VM-Series firewall in OpenStack solution leverages heat orchestration templates to configure and deploy the components required for service chaining and service scaling. The heat templates provided by Palo Alto networks create a service template, service instance, and service policy (to direct traffic to the VM-Series firewall) to deploy two Linux servers and the VM-Series firewall service instance between them.



Components of the VM-Series for OpenStack Solution

The VM-Series firewall in an OpenStack environment has been tested with the following components.

Component	Description
Software	• Hypervisor: KVM/Ubuntu 14.04 • Networking: Contrail 3.0.2 • OpenStack Distro: Mirantis 8.0 (Liberty) • Telemetry: Ceilometer (service scaling only) • Orchestration: OpenStack Heat Templates (Version 2015-10-15 or higher) • VM-Series for KVM PAN-OS 8.0 or later
VM-Series Hardware Resources	See VM-Series System Requirements for the minimum hardware requirements for your VM-Series model. In OpenStack, flavors define the CPU, memory, and storage capacity of a compute instance. When setting up your Heat template, choose the compute flavor that meets or exceeds the hardware requirements for the VM-Series model.
Fuel Master	Fuel is a web UI-driven deployment and management tool for OpenStack.
OpenStack Controller	This node runs most of the shared OpenStack services, such API and scheduling. Additionally, the Horizon UI runs on this node.
OpenStack Compute	The compute node contains the virtual machines, including the VM-Series firewall, in the OpenStack deployment. The compute node that houses the VM-Series must meet the following criteria: • Instance type OS::Nova::Server • Allow configuration of at least three interfaces • Accept the VM-Series qcow2 image • Accept the compute flavor parameter *Install the OpenStack compute node on a bare-metal server because the VM-Series firewall does not support nested virtualization.*
Contrail Controller	The Contrail controller node is a software-defined networking controller used for management, control, and analytics for the virtualized network. It provides routing information to the compute and gateway nodes. Additionally, the Contrail controller provides the necessary support for service chaining and service scaling.
Contrail Gateway	The Contrail gateway node provides IP connectivity to external networks from virtual networks. MPLS over GRE tunnels from the virtual machines

Component	Description
	terminate at the gateway node, where packets are decapsulated and sent to their destinations on IP networks.
Ceilometer (OpenStack Telemetry)	In the case of the VM-Series firewall for OpenStack, Ceilometer monitors CPU utilization for service scaling. When CPU utilization meets the defined thresholds, a new service instance of the VM-Series firewall is deployed or shut down.
Heat Orchestration Template Files	Palo Alto Networks provides a sample Heat template for deploying the VM-Series firewall. This template is made up of a main template and an environment template. These files instantiate one VM-Series instance with one management interface and two data interfaces. In a basic gateway deployment, the template instantiates a Linux server with one interface. The interface of the server attaches to the private network created by the template. In a service chaining or service scaling deployment, the templates instantiate two Linux servers with one server attached to each data interface of the firewall.
VM-Series Firewall Bootstrap Files	The VM-Series firewall bootstrap files consist of a init-cfg.txt file, bootstrap.xml file, and VM-Series auth codes. Along with the Heat template files, Palo Alto Networks provides a sample init-cfg.txt and bootstrap.xml files. You must provide your own auth codes to license your VM-Series firewall and activate any subscriptions. See Bootstrap the VM-Series Firewall for more information about VM-Series bootstrap files.

Heat Template for a Basic Gateway Deployment

The heat template file includes the following four files to help you launch the VM-Series firewall on KVM in OpenStack. All four files are required to deploy the VM-Series firewall and Linux server.

- **pan_basic_gw.yaml**—Defines the resources created to support the VM-Series firewall and Linux server on the compute node, such as interfaces and IP addresses.
- **pan_basic_gw_env.yaml**—Defines the environment that the VM-Series firewall and Linux server exist in. Many parameters in the pan_basic_gw.yaml file reference the parameters defined in this file, such as flavor for the VM-Series and the Linux server.
- **init-cfg.txt**—Includes the operational command to enable DHCP on the firewall management interface.
- **bootstrap.xml**—Provides basic configuration for the VM-Series firewall. The bootstrap.xml file configures the data interfaces and IP addresses. These values must match the corresponding values in the pan_basic_gw.yaml file.

  Additionally, the bootstrap.xml file includes a NAT rule called untrust2trust. This rule translate the trust port on the server to the untrust port of the VM-Series firewall.

The table below describes resources that the pan_basic_gw.yaml template file creates and provides the default value, if applicable.

Resource	Description
pan_fw_instance	VM-Series firewall with a management interface and two data interfaces.
server_instance	A Linux server with a single interface.
pan_trust_net	A connection to the internal network to which the trust interface of the firewall and trust interface of the server are attached.
pan_trust_subnet	Subnet attached to the trust interface on the firewall (pan_trust_net) and has a CIDR value of 192.168.100.0/24.
pan_untrust_net	Untrust network to which the untrust port of the firewall is attached.
pan_untrust_subnet	Subnet attached to the untrust interface of the firewall (pan_untrust_net) and has a CIDR value of 192.168.200.0/24.
allow_ssh_https_icmp_secgroup	Security group that allows TCP on ports 22 and 443 and ICMP traffic.
pan_untrust_port	The untrust port of the VM-Series firewall deployed in Layer 3 mode. The Heat template provides a default IP address of 192.168.200.10 to this port. If you change this IP address in the heat template, you must change the IP address in the bootstrap.xml file.
pan_untrust_floating_ip	A floating IP address assigned from the public_network.

Resource	Description
pan_untrust_floating_ip_assoc	This associates the pan_untrust_floating_ip to the pan_untrust_port.
pan_trust_port	The trust port of the VM-Series firewall Layer 3 mode.
server_trust_port	The trust port of the Linux server Layer 3 mode. The Heat template provides a default IP address of 192.168.100.10 to this port. If you change this IP address in the heat template, you must change the IP address in the bootstrap.xml file.

The pan_basic_gw.yaml file references the pan_basic_gw_env.yaml for many of the values needed to create the resources need to deploy the VM-Series firewall and Linux server. The heat template environment file contains the following parameters.

Parameter	Description
mgmt_network	The VM-Series firewall management interface attaches to the network specified in this parameter. The template does not create the management network; you must create this before deploying the heat templates. The default value is mgmt_ext_net. You should restrict access to the firewall and isolate the management network. Additionally, do not make the allowed network larger than necessary and never configure the allowed source as 0.0.0.0/0.
public_network	Addresses that the OpenStack cluster and the virtual machines in the cluster use to communicate with the external or public network. The public network provides virtual IP addresses for public endpoints, which are used to connect to OpenStack services APIs. The template does not create the public network; you must create this before deploying the heat templates. The default value is public_net.
pan_image	This parameter specifies the VM-Series base image used by the Heat template when deploying the VM-Series firewall. The default value is pa-vm-7.1.4.
pan_flavor	This parameter defines the hardware resources allocated to the VM-Series firewall. The default value is m1.medium. This value meets the VM-Series on KVM System Requirements described in the Set Up the VM-Series Firewall on KVM chapter.
server_image	This parameter tells the Heat template which image to use for the Linux server. The default value is Ubuntu-14.04.
server_flavor	This parameter defines the hardware resources allocated to the Linux server. The default value is m1.small.
server_key	The server key is used for accessing the Linux server through ssh. The default value is server_key. You can change this value by entering a new server key in the environment file.

Heat Templates for Service Chaining and Service Scaling

The heat template environment file defines the parameters specific to the VM-Series firewall instance deployed through service chaining or service scaling. The parameters defined in the environment file are divided into sections described below. There are two versions of the heat templates for service chaining—vwire and L3— and one for service scaling.

Service chaining requires the heat template files and two bootstrap files to launch the VM-Series firewall service instance and two Linux servers in the left and right networks.

- **Template files**—This template defines the resources created to support the VM-Series firewall and two Linux servers, such as interfaces and IP addresses.
  - service_chaining_template_vm.yaml for vwire deployments.
  - service_chaining_template_L3.yaml for L3 deployments.
  - service_scaling_template.yaml for service scaling deployments.
- **Environment file**—This environment file defines the environment that the VM-Series firewall and Linux servers exist in. Many parameters in the template reference the parameters defined in this file, such as flavor for the VM-Series and the names of the Linux servers.
  - service_chaining_env_vm.yaml for vwire deployments.
  - service_chaining_env_L3.yaml for L3 deployments.
  - service_scaling_env.yaml for service scaling deployments.
- **service_instance.yaml**—(Service Scaling only) This is a nested heat template that is reference by Service_Scaling_template.yaml to deploy the service instance. It provides the necessary information to deploy service instances for scaling events.
- **init-cfg.txt**—Provides the minimum information required to bootstrap a VM-Series firewall. The init-cfg.txt provided only includes the operational command to enable DHCP on the firewall management interface.
- **<file_name>_bootstrap.xml**—Provides basic configuration for the VM-Series firewall. The bootstrap.xml file configures the data interfaces. These values must match the corresponding values in the heat templates files.

For more information about the init-cfg.txt and bootstrap.xml files, see Bootstrap Configuration Files.

The following tables describe the parameters of the environment file.

Virtual Network

The virtual network configuration paramaters in the heat template environment file define the virtual network that connects the VM-Series firewall and the two Linux servers deployed by the heat template.

Virtual Network (VN Config)	
management_network	The VM-Series firewall management interface attaches to the network specified in this parameter. You should restrict access to the firewall and isolate the management network. Additionally, do not make the allowed network larger than necessary and never configure the allowed source as 0.0.0.0/0.
left_vn or left_network	Name of the left virtual network.
right_vn or right_network	Name of the right virtual network.
left_vn_fqdn	Fully qualified domain name of the left virtual network.
right_vn_fqdn	Fully qualified domain name of the right virtual network
route_target	Edit this value so route target configuration matches that of your external gateway.

Virtual Machine

The virtual machine parameters define the left and right Linux servers. The name of the port tuple is defined here and referenced by the heat template. In Contrail, a port tuple is an ordered set of virtual network interfaces connected to the same virtual machine. With a port tuple, you can create ports and pass that information when creating a service instance. The heat template creates the left, right, and management ports and adds them to the port tuple. The port tuple is then linked to the service instance. When you launch the service instance using the heat templates, the port tuple maps the service virtual machine to the virtual machine deployed in OpenStack.

Virtual Machine (VM Config)	
flavor	The flavor of the left and right virtual machines. The default value is m1.small.
left_vm_image or right_vm_image or image	The name of the software image for the left and right virtual machines. Change this value to match the file name of the image you uploaded. The default is TestVM, which is a default image provided by OpenStack.
svm_name	The name applied to the VM-Series firewall.
left_vm_name and right_vm_name	The name of the left and right virtual machines.
port_tuple_name	The name of the port tuple used by the two Linux servers and the VM-Series firewall.
server_key	The server key is used for accessing virtual machines through SSH. The default value is server_key. You can change this value by entering a new server key in the environment file.

Service Template

The service template defines the parameters of the service instance, such as the software image, virtual machine flavor, service type, and interfaces. Service templates are configured within the scope of a domain and can be used on all projects within the specified domain.

Service Template (ST Config)	
S_Tmp_name	The name of the service template.
S_Tmp_version	The service template version. The default value is 2. Do not change this parameter because service template version 2 is required to support port tuples.
S_Tmp_service_mode	Service mode is the network mode used by the VM-Series firewall service instance. For the L3 network template, the default value is in-network. For the virtual wire template, the default value is transparent.
S_Tmp_service_type	The type of service being deployed by the template. The default value is firewall and should not be changed when deploying the VM-Series firewall.
S_Tmp_image_name	This parameter specifies the VM-Series base image used by the Heat template when deploying the VM-Series firewall. Edit this parameter to match the name of the VM-Series firewall image uploaded to your OpenStack environment.
S_Tmp_flavor	This parameter defines the hardware resources allocated to the VM-Series firewall. The default value is m1.large.
S_Tmp_interface_type_mgmt S_Tmp_interface_type_left S_Tmp_interface_type_right	The parameters define the interface type for management, left, and right interfaces.
domain	The domain where this service template is tied to. The default value is default-domain.

Service Instance

The service instance portion of the heat template environment file provides the name of the individual instance deployed by the heat template and service template.

Service Instance (SI Config)	
S_Ins_name	The service instance name. This is the name of the VM-Series firewall instance in Contrail.
S_Ins_fq_name	The fully qualified name of the service instance.

IPAM

IP address management (IPAM) provides the IP address information for the interfaces of the service instance. Changes these parameters to best suit your environment.

IPAM (IPAM Config)	
NetIPam_ip_prefix_mgmt	The IP prefix of the management interface on the VM-Series firewall. The default value is 172.2.0.0.
NetIPam_ip_prefix_len_mgmt	The IP prefix length of the management interface on the VM-Series firewall. The default value is /24.
NetIPam_ip_prefix_left	The IP prefix of the left interface on the VM-Series firewall. The default value is 10.10.1.0.
NetIPam_ip_prefix_len_left	The IP prefix length of the left interface on the VM-Series firewall. The default value is /24.
NetIPam_ip_prefix_right	The IP prefix of the right interface on the VM-Series firewall. The default value is 10.10.2.0.
NetIPam_ip_prefix_len_right	The IP prefix length of the right interface on the VM-Series firewall. The default value is /24.
NetIPam_addr_from_start_this	This parameter determines how IP addresses are assigned to VMs on the subnets described above. If true, any new VM takes the next available IP address. If false, any new VM is assigned an IP address at random. The default value is true.

Service Policy

The service policy defines the traffic redirection rules and policy that point traffic passing between the left and right virtual machines to the VM-Series firewall service instance.

Service Policy (Policy Config)	
policy_name	The name of the service policy in Contrail that redirects traffic through the VM-Series firewall. For the L3 template, the default value is PAN_SVM_policy-L3. For the virtual wire template, the default value is PAN_SVM_policy-vw.
policy_fq_name	The fully qualified name of the service policy.
simple_action	The default action Contrail applies to traffic going to the VM-Series firewall service instance. The default value is pass because the VM-Series firewall will apply its own security policy to the traffic.
protocol	The protocols allowed by Contrail to pass to the VM-Series firewall. The default value is any.

Service Policy (Policy Config)	
src_port_end and src_port_start	Use this parameter to specify source port(s) that should be associated with the policy rule. You can enter a single port, a list of ports separated with commas, or a range of ports in the form of <port>-<port>. The default value is -1 in the provided heat templates; meaning any source port.
direction	This parameter defines the direction of traffic that is allowed by Contrail to pass to the VM-Series firewall. The default value is <> or bidirectional traffic.
dst_port_end and dst_port_start	Use this parameter to specify destination port(s) that should be associated with the policy rule. You can enter a single port, a list of ports separated with commas, or a range of ports in the form of <port>-<port>. The default value is -1 in the provided heat templates; meaning any destination port.

Alarm

The alarm parameters are used in service scaling and are not included in the service chaining environment files. These parameters define the thresholds used by Contrail to determine when scaling should take place. This set of parameters is only used the service scaling heat template.

The default time configured under the cooldown parameters is intended to allow the firewall enough time to boot up. If you change the cooldown values, leave sufficient time for each new firewall instance to boot up.

Alarm	
meter_name	The metric monitored by Ceilometer and used by contrail to determine when an additional VM-Series firewall should be deployed or brought down. The heat template uses CPU utilization or bytes per second as metrics for service scaling.
cooldown_initial	The amount time Contrail waits before launching a additional service instance after the initial service instance is launched. The default is 1200 seconds.
cooldown_scaleup	The amount of time Contrail waits between launching additional service instance after the first scale up service instance launch. The default is 1200 seconds.
cooldown_scaledown	The amount of time Contrail waits between shutting down additional service instances after the first scale up service instance shut down. The default is 1200 seconds.
period_high	The interval during which the average CPU load is calculated as high before triggering an alarm. The default value is 300 seconds.
period_low	The interval during which the average CPU load is calculated as low before triggering an alarm. The default value is 300 seconds.

Alarm	
threshold_high	The value of CPU utilization in percentage or bytes per second that Contrail references before launching a scale up event. The default is 40% CPU utilization or 2800 bytes per second.
threshold_low	The value of CPU utilization in percentage or bytes per second that Contrail references before launching a scale down event. The default is 20% CPU utilization or 12000 bytes per second.

Install the VM-Series Firewall in a Basic Gateway Deployment

Complete the following steps to prepare the heat templates, bootstrap files, and software images needed to deploy the VM-Series firewall in OpenStack. After preparing the files, deploy the VM-Series firewall and Linux server.

STEP 1 | Download the Heat template and bootstrap files.

Download the Heat template package from the GitHub repository.

STEP 2 | Download the VM-Series base image.

1. Login in to the Palo Alto Networks Customer Support Portal.
2. Select **Software Updates** and choose **PAN-OS for VM-Series KVM Base Images** from the **Filter By** drop-down.
3. Download **PA-VM-KVM-8.0.0.qcow2**.

STEP 3 | Download Ubuntu 14.04 and upload the image to the OpenStack controller.

The Heat template needs an Ubuntu image for launching the Linux server.

1. Download Ubuntu 14.04.
2. Log in to the Horizon UI.
3. Select **Project** > **Compute** > **Images** > **Create Image**.
4. **Name** the image Ubuntu 14.04 to match the parameter in the pan_basic_gw_env.yaml file.
5. Set Image Source to **Image File**.
6. Click **Choose File** and navigate to your Ubuntu image file.
7. Set the Format to match the file format of your Ubuntu image.
8. Click **Create Image**.

STEP 4 | Upload the VM-Series for KVM base image to the OpenStack controller.

1. Log in to the Horizon UI.
2. Select **Project** > **Compute** > **Images** > **Create Image**.
3. **Name** the image pa-vm-8.0.0.
4. Set Image Source to **Image File**.
5. Click **Choose File** and navigate to your VM-Series image file.
6. Set the Format to **QCOW2-QEMU Emulator**.
7. Click **Create Image**.

STEP 5 | Upload the bootstrap files.

You can upload the init-cfg.txt, bootstrap.xml, and your VM-Series auth codes to your OpenStack controller or a web server that the OpenStack controller can access.

STEP 6 | Edit the pan_basic_gw.yaml template to point to the bootstrap files and auth codes.
Under Personality, specify the file path or web server address to the location of your files. Uncomment whichever lines you are not using.

```
pan_fw_instance:
  type: OS::Nova::Server
  properties:
```

```
      image: { get_param: pan_image }
      flavor: { get_param: pan_flavor }
      networks:
        - network: { get_param: mgmt_network }
        - port: { get_resource: pan_untrust_port }
        - port: { get_resource: pan_trust_port }
      user_data_format: RAW
      config_drive: true
      personality:
        /config/init-cfg.txt: {get_file: "/opt/pan_bs/init-cfg.txt"}
#        /config/init-cfg.txt: { get_file: "http://web_server_name_ip/
pan_bs/init-cfg.txt" }
        /config/bootstrap.xml: {get_file: "/opt/pan_bs/bootstrap.xml"}
#        /config/bootstrap.xml: { get_file: "http://web_server_name_ip/
pan_bs/bootstrap.xml" }
        /license/authcodes: {get_file: "/opt/pan_bs/authcodes"}
#        /license/authcodes: {get_file: "http://web_server_name_ip/pan_bs/
authcodes"}
```

STEP 7 | Edit the pan_basic_gw_env.yaml template environment file to suit your environment. Make sure that the management and public network values match those that you created in your OpenStack environment. Set the pan_image to match the name you assigned to the VM-Series base image file. You can also change your server key here.

```
root@node-2:~# cat basic_gateway/pan_basic_gw_env.yaml
parameters:
  mgmt_network: mgmt_ext_net
  public_network: public_net
  pan_image: pa-vm-8.0.0
  pan_flavor: m1.medium
  server_image: Ubuntu-14.04
  server_flavor: m1.small
  server_key: server_key
```

STEP 8 | Deploy the Heat template.

1. Execute the command **source openrc**
2. Execute the command **heat stack-create <*stack-name*> -f <*template*> -e ./<*env-template*>**

```
root@node-2:~# heat stack-create stack1 -f pan_basic_gw.yaml -e pan_basic_gw_env.yaml
+--------------------------------------+------------+--------------------+----------------------+--------------+
| id                                   | stack_name | stack_status       | creation_time        | updated_time |
+--------------------------------------+------------+--------------------+----------------------+--------------+
| ebe40f9d-2781-4bb2-b246-f15c761f9045 |   stack1   | CREATE_IN_PROGRESS | 2017-01-25T13:36:59 | None         |
+--------------------------------------+------------+--------------------+----------------------+--------------+
```

STEP 9 | Verify that your VM-Series firewall is deployed successfully.

You can use the following commands to check the creation status of the stack.

- Check the stack status with **heat stack-list**
- View a detailed list of events that occurred during stack creation with **heat event-list**
- View details about your stack with **heat stack-show**

STEP 10 | Verify that the VM-Series firewall is bidirectionally inspecting traffic accessing the Linux server.

1. Log in to the firewall.
2. Select **Monitor** > **Logs** > **Traffic** to view the SSH session.

Install the VM-Series Firewall with Service Chaining or Scaling

Complete the following steps to prepare the heat templates, bootstrap files, and software images needed to deploy the VM-Series firewall. After preparing the files, deploy the VM-Series firewall service and two Linux servers.

STEP 1 | Download the Heat template and bootstrap files.

Download the Heat template package from the GitHub repository.

STEP 2 | Download the VM-Series base image.

1. Login in to the Palo Alto Networks Customer Support Portal.
2. Select **Software Updates** and choose **PAN-OS for VM-Series KVM Base Images** from the **Filter By** drop-down.
3. Download **PA-VM-KVM-8.0.0.qcow2**.

STEP 3 | Download Ubuntu 14.04 and upload the image to the OpenStack controller.

For service chaining, you can use the default image provided by OpenStack called TestVM. Skip this step when using TestVM. An Ubuntu image is required for service scaling.

1. Download Ubuntu 14.04.
2. Log in to the Horizon UI.
3. Select **Project** > **Compute** > **Images** > **Create Image**.
4. **Name** the image Ubuntu 14.04 to match the parameter in the pan_basic_gw_env.yaml file.
5. Set Image Source to **Image File**.
6. Click **Choose File** and navigate to your Ubuntu image file.
7. Set the Format to match the file format of your Ubuntu image.
8. Click **Create Image**.

A server key is required when using an Ubuntu image. Ensure that the server key is added to the environment file.

STEP 4 | Upload the VM-Series for KVM base image to the OpenStack controller.

1. Log in to the Horizon UI.
2. Select **Project** > **Compute** > **Images** > **Create Image**.
3. **Name** the image pa-vm-8.0.0.
4. Set Image Source to **Image File**.
5. Click **Choose File** and navigate to your VM-Series image file.
6. Set the Format to **QCOW2-QEMU Emulator**.
7. Click **Create Image**.

STEP 5 | Upload the bootstrap files. The files must be uploaded to the folder structure described here. The heat template uses this folder structure to locate the bootstrap files.

1. Log in to your OpenStack controller.
2. Create the following folder structure:

   /root/bootstrap/config/

   /root/bootstrap/license/

3. Using SCP or FTP, add the init-cfg.txt and bootstrap.xml files to the config folder and add your VM-Series auth codes to the license folder.

STEP 6 | Edit the template environment file to suit your environment. Verify that the image names in the environment file match the names you gave the files when you uploaded them.

```
parameters:
# VN config
  management_network: 'mgmt_net'
  left_vn: 'left_net'
  right_vn: 'right_net'
  left_vn_fqdn: 'default-domain:admin:left_net'
  right_vn_fqdn: 'default-domain:admin:right_net'
  route_target: "target:64512:20000"
# VM config
  flavor: 'm1.small'
  left_vm_image: 'TestVM'
  right_vm_image: 'TestVM'
  svm_name: 'PAN_SVM_L3'
  left_vm_name: 'Left_VM_L3'
  right_vm_name: 'Right_VM_L3'
  port_tuple_name: 'port_tuple_L3'
#ST Config
  S_Tmp_name: PAN_SVM_template_L3
  S_Tmp_version: 2
  S_Tmp_service_mode: 'in-network'
  S_Tmp_service_type: 'firewall'
  S_Tmp_image_name: 'PA-VM-8.0.0'
  S_Tmp_flavor: 'm1.large'
  S_Tmp_interface_type_mgmt: 'management'
  S_Tmp_interface_type_left: 'left'
  S_Tmp_interface_type_right: 'right'
  domain: 'default-domain'
# SI Config
  S_Ins_name: PAN_SVM_Instance_L3
  S_Ins_fq_name: 'default-domain:admin:PAN_SVM_Instance_L3'
#IPAM Config
  NetIPam_ip_prefix_mgmt: '172.2.0.0'
  NetIPam_ip_prefix_len_mgmt: 24
  NetIPam_ip_prefix_left: '10.10.1.0'
  NetIPam_ip_prefix_len_left: 24
  NetIPam_ip_prefix_right: '10.10.2.0'
  NetIPam_ip_prefix_len_right: 24
  NetIPam_addr_from_start_true: true
#Policy Config
  policy_name: 'PAN_SVM_policy-L3'
  policy_fq_name: 'default-domain:admin:PAN_SVM_policy-L3'
  simple_action: 'pass'
  protocol: 'any'
  src_port_end: -1
  src_port_start: -1
  direction: '< >'
  dst_port_end: -1
  dst_port_start: -1
```

STEP 7 | Edit the template files to point to the bootstrap files and auth codes. Under Personality, specify the file path to the location of your files. Uncomment whichever lines you are not using.

```
Pan_Svm_instance:
```

```
    type: OS::Nova::Server
    depends_on: [ mgmt_InstanceIp, left_InstanceIp, right_InstanceIp ]
    properties:
      name: {get_param: svm_name }
      image: { get_param:  S_Tmp_image_name }
      flavor: { get_param: S_Tmp_flavor }
      networks:
        - port: { get_resource: mgmt_VirtualMachineInterface }
        - port: { get_resource: left_VirtualMachineInterface }
        - port: { get_resource: right_VirtualMachineInterface }
      user_data_format: RAW
      config_drive: true
      personality:
        /config/init-cfg.txt: {get_file: "/root/bootstrap/config/init-
cfg.txt"}
#        /config/init-cfg.txt: { get_file: "http://10.4.1.21/op_test/config/
init-cfg.txt" }
        /config/bootstrap.xml: {get_file: "/root/bootstrap/config/
Service_Chaining_bootstrap_L3.xml"}
#        /config/bootstrap.xml: { get_file: "http://10.4.1.21/op_test/
config/Service_Chaining_bootstrap_L3.xml" }
#        /license/authcodes: {get_file: "/root/bootstrap/license/authcodes"}
#        /license/authcodes: {get_file: "http://10.4.1.21/op_test/license/
authcodes"}
```

STEP 8 | Upload the heat template files.

1. Log in to your OpenStack Controller.
2. Use SCP or FTP to add the heat template file and environment file.

STEP 9 | Deploy the Heat template.

1. Execute the command **`source openrc`**
2. Execute the command **`heat stack-create <stack-name> -f <template> -e ./<env-template>`**

STEP 10 | Verify that your VM-Series firewall is deployed successfully.

You can use the following commands to check the creation status of the stack.

- Check the stack status with **`heat stack-list`**
- View a detailed list of events that occurred during stack creation with **`heat event-list`**
- View details about your stack with **`heat stack-show`**

STEP 11 | Verify that the VM-Series firewall is bidirectionally inspecting traffic between the Linux servers.

1. Log in to the firewall.
2. Select **Monitor** > **Logs** > **Traffic** to view the SSH session.

Set Up a Firewall in Cisco ACI

Palo Alto Networks integrates as a service with Cisco Application-Centric Infrastructure (ACI). ACI is a software-defined networking (SDN) solution for easily deploying new workloads and network services. Using an SDN controller called the Cisco Application Policy Infrastructure Controller (APIC), you deploy the firewall service between Endpoint Groups (EPGs). EPGs act as a container for applications or application tiers. When you place a firewall between EPGs, security policy configured on the firewall secures the traffic between the EPGs.

Cisco ACI Integration Models

There are two models for integrating the firewall into Cisco ACI—Network Policy mode and Service Manager mode.

Network Policy Mode

In network policy mode, traffic is sent to the firewall with a policy-based redirect (PBR). Additionally, configuration of the firewall and configuration of the APIC are completely separate. Network policy mode does not rely on a device package or any ant configuration integration between the firewall and the APIC, so it provides greater flexibility of configuration and deployment of the firewall.

For East-West traffic, define a bridge domain and subnet in the ACI fabric for the firewall. Configure contracts between EPGs that send traffic to the firewall using a PBR. The PBR forwards traffic to the firewall based on policy containg the firewall's IP and MAC address. The firewall interfaces are always in Layer 3 mode and traffic is received and routed back to the ACI fabric. You can configure separate interfaces for consumer and provider connections or a single interface for ingress and egress traffic. The procedure in this document uses a single interface because it simplifies the integration; you do not need to configure as many interfaces, IP addresses, or VLANs. However, when using a single interface, you cannot uses zone information in defining security policy and you must modify the default intra-zone policy on the firewall to deny traffic.

For North-South traffic, you must use a dedicated policy called an L3Out. An L3Out contains the information required for the tenant to connect to external routing devices and access external networks. L3Out connections contain an external network EPG that represent the networks accessible through the L3Out policy. Just as the L3Out can group all external networks into a single EPG, you can use a vzAny object ACI to represent all EPGs in a VRF. Using a vzAny object simples the application of the outbound traffic contract because, whenever a new EPG is added to the VRF, the contract is automatically applied. In this scenario, the external network provides the contract and the vzAny object (all internal EPGs) consume it.

Service Manager Mode

Service manager mode allows you to use the Cisco APIC as a single point of configuration for your ACI fabric as well as your Palo Alto Networks firewalls and Panorama.

The following components are required to integrate the Palo Alto Networks firewall into your Cisco ACI environment in service manager mode.

- Panorama—Panorama is required to deploy security policy and objects on the firewall using the APIC. This document assumes that you are using Panorama. You can deploy the firewall without Panorama and APIC will deploy the context (vsys), high availability, and network interface configuration to the firewall but any security policy must be configured directly on the firewall.

  Panorama acts as a single point of connection between the APIC and the firewalls. Cisco ACI deploys security policy and objects from Panorama to its managed firewalls. The APIC sets devices groups for firewalls based on the APIC configuration and then commits the device groups configuration to the firewall, including security policy, NAT policy, threat profiles, and address objects.

  Cisco ACI integration supports physical and virtual versions of Panorama.
- Palo Alto Networks Firewall—Cisco ACI integration supports physical firewall appliances and the VM-Series firewall for VMware ESXi (standalone version).

Cisco ACI integration supports physical firewalls divided into contexts that the APIC manages as individual firewalls. On hardware-based firewalls, these contexts are the virtual systems (vsys) on the firewalls; each firewall is licensed to support a certain number of vsys instances. When deploying a multi-vsys firewall in ACI, you must configure a chassis manager in the tenant and assign it to the firewall service.

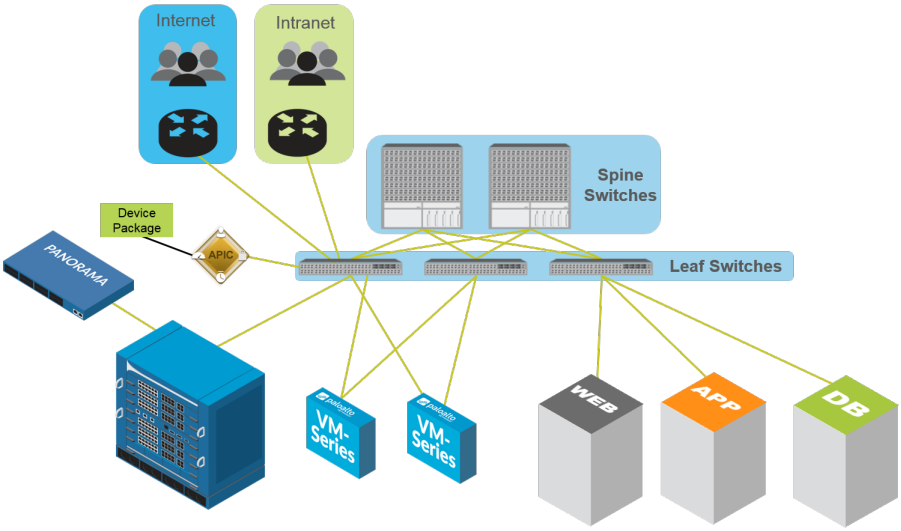
- Cisco APIC—The APIC is your interface for managing your ACI environment. From here, you will create the firewall service, insert the firewall service between endpoint groups, and direct traffic to the firewall.
- Device Package—A device package allows and manages communication between the APIC and Panorama and firewalls. It allows you to configure high availability, networking, and interfaces for the firewall in the APIC and push it to Panorama and the firewalls. Once deployed in ACI, you complete your security configuration through Panorama or the individual firewalls.

The Palo Alto Networks device package version 1.3 requires PAN-OS 8.0 and Cisco ACI 2.3.

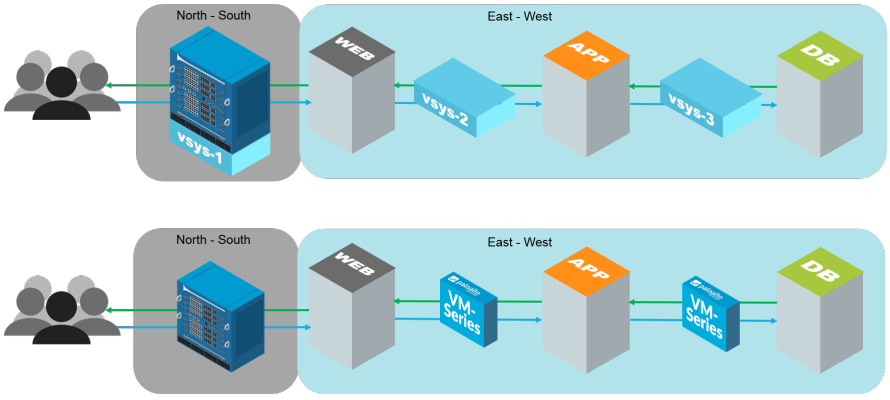
Palo Alto Firewall Integration with Cisco ACI Overview

Palo Alto Networks integration with Cisco ACI allows you to insert a firewall between EPGs as a Layer 4 to Layer 7 service. The firewall then secures the east-west traffic between the application tiers within those EPGs or north-south traffic between users and the applications.

The figure below shows an example of a physical ACI deployment that includes integrated Palo Alto Network firewalls. All the entities in the ACI Fabric are connected to leaf switches and those leaf switches are connected to larger spine switches. As users access the application, the ACI fabric moves the traffic to the correct destination. To secure the traffic between the application tiers, the network administrator inserts the Palo Alto Networks firewalls as L4 to L7 services between each EPG and creates a service graph to define what services the L4 to L7 device provides.



After the firewall services have been deployed, traffic now flows logically as shown below. Traffic to and from the end users and each tier in the application regardless of where or how each entity is physically connected to the network.



The following section provide additional details about components and concepts that make up the integration between the Next-Generation Firewall and Cisco ACI.

- Service Graph Templates
- High Availability in Cisco ACI with the Device Package

- Multi-Context Deployments
- Firewall Policy Based on Endpoint Group, Tenant, or Application

Service Graph Templates

Regardless of you deployment mode, your firewalls are deployed in Cisco ACI through service graphs. A service graph allows you to integrate Layer 4 - Layer 7 devices, such as a firewall, into the flow of traffic without the need for the L4-L7 device to be the default gateway for the servers in the ACI fabric.

Firewalls are represented in the ACI fabric as an L4-L7 device that you configure in the APIC as a device cluster. A single firewall or two firewalls deployed as an HA pair are configured as a device cluster. Each device cluster has one or more logical interfaces that describe the interface information of the device cluster and map the path of the member firewall with a VLAN from the physical or virtual machine monitor (VMM) domain.

Service graph templates define the firewall device cluster that you insert into the traffic flow between EPGs. Additionally, the service graph template defines the how the firewall is integrated and the logical interfaces that are assigned to the consumer and provider EPGs. After creating your service graph template, you assign it to EPGs and contracts. Because the service graph template is not tied to a specific EPG or contract, you can reuse it between multiple EPGs. The APIC then deploys the service graph template by connecting it to the bridge domain between EPGs.

You have three options when using a service graph template to integrate the firewall into the traffic between EPGs.

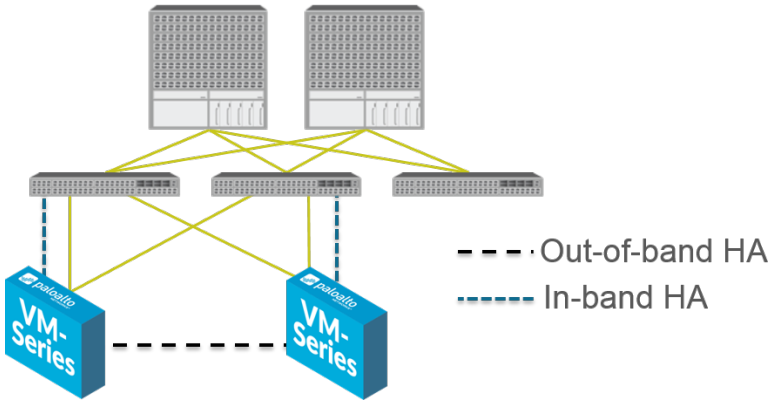
- Policy-Based Redirect—Traffic is routed directly to the firewall. This option is used when deploying the firewall in network policy mode.
- GoTo—The firewall routes traffic between bridge domains. Use this option when deploying a Layer 3 firewall in service manager mode.
- GoThrough—The firewall bridge traffic between to bridge domains. Use this option when deploying a Layer 2 firewall in service manager mode.

High Availability in Cisco ACI with the Device Package

Firewalls integrated into an ACI fabric supports an active-passive high availability configuration. Any interface can be used for the HA link, including the HA1 and HA2 interfaces, management interfaces, or data interfaces. Additionally, the dedicated HA1 and HA2 interfaces can be directly connected between the firewalls for out-of-band HA or use static EPG binding to connect in-band through the ACI switches.

Because virtual firewalls do not have dedicated HA ports, the management port is used as HA1 by default and the HA2 must be specified.

HA on physical firewalls can be combined with a Link Aggregation/Virtual Port Channel to create redundant links between the firewalls and switches. This provides protection against a scenario where the active firewall is up but the link to the firewall or the leaf it connects to have failed. The firewall then switches to the redundant link and leaf node. Link aggregation supports static aggregation mode only.



Multi-Context Deployments

Cisco ACI integration supports physical firewalls divided into contexts that are managed by ACI as individual firewalls. On the firewall, these contexts are the virtual systems (vsys) on the firewalls and each firewall is licensed to support a certain number of vsys instances. When deploying a multi-vsys firewall in ACI, you must configure a chassis manager in the tenant and assign it to the firewall service.

Firewall Policy Based on Endpoint Group, Tenant, or Application

You can create firewall security policy referencing Cisco ACI attributes such as EPG, tenants, and application profile through the use of dynamic address groups. When an endpoint is added to an EPG, the APIC notifies the firewall that a new endpoint has joined the EPG. The firewall then adds that endpoint's IP address to the corresponding dynamic address group.

To enable the use of dynamic address groups, you must enable Attachment Notifications on the Function Connectors in the tenant's Service Graph on the APIC. Additionally, an endpoint must be in an EPG to see any EPG, tenant, or application profile tags on the firewall. To use EPG. tenant, or application profile tags in dynamic address groups on Panorama, you must type the tags into the match criteria field manually; the tags are only suggested on the firewall, not Panorama. After the dynamic address groups are attached to policy and pushed to the firewall(s), the IP addresses are mapped.

Prepare Your ACI Environment for Integration

Before you can integrate the firewall with a device package, you must complete the following steps to prepare your Cisco ACI environment.

STEP 1 | Deploy Panorama.

STEP 2 | Deploy the firewall.

- Physical Firewall—Connect the firewall's out-of-band management port to one leaf switch port and connect at least one firewall data interface to the switch. Firewall interfaces on a physical firewall are configured with VLANs to ensure connectivity to the correct networks. Deploy the firewall according to the platform-specific installation guide.
- VM-Series Firewall—When configuring the virtual hardware for the VM-Series firewall, set the port-group for the management interface. Each VM-Series firewall connected to the network requires its own virtual NIC. Deploy the VM-Series firewall based on your hypervisor.

STEP 3 | Configure the management IP address on each firewall and Panorama.

Perform initial configuration on:

- Hardware-based firewall
- VM-Series firewall
- Panorama

STEP 4 | Add your firewall(s) to Panorama as a managed device.

STEP 5 | Install feature licenses on your firewall(s).

- Register and activate licenses on your physical firewall.
- Register and activate licenses on your VM-Series firewall.
- Manage firewall licenses using Panorama.

STEP 6 | Establish Cisco ACI fabric and management connectivity.

As part of this configuration, create a physical domain and VLAN namespace. Ensure that data interfaces of any physical firewalls are part of the physical domain.

STEP 7 | (VM-Series only) Create a Cisco ACI VMM domain profile.

If you are using virtual machines or the VM-Series firewall, create a virtual machine monitor (VMM) domain profile for the VMware vSphere environment. The VMM domain specifies the connectivity policy between vSphere and the ACI fabric.

STEP 8 | Install the Palo Alto Networks device package for Cisco ACI if you are using Service Manager mode. Do not install this when using Network Policy mode.

1. Login to the APIC.
2. Select **L4-L7 Services** > **Packages** > **L4-L7 Service Device Types**.
3. Select **Actions** > **Import Device Package**.
4. Click **Browse** and locate the Palo Alto Networks Device Package.
5. Click **Open**.
6. Click **Submit**.

Integrate the Firewall with Cisco ACI in Network Policy Mode

In network policy mode, you integrate a pair of firewalls in high availability (HA) into the east-west or north-south traffic by using a policy-based redirect to a single logical HA interface. The firewall and ACI fabric are configured separately and address objects on the firewall are mapped to EPGs in the ACI fabric.

You can use network policy mode to deploy a Palo Alto Networks firewall to secure East-West or North-South traffic.

- Deploy the Firewall to Secure East-West Traffic in Network Policy Mode
- Deploy the Firewall to Secure North-South Traffic in Network Policy Mode

Deploy the Firewall to Secure East-West Traffic in Network Policy Mode

The following procedure describes how to deploy a Palo Alto Networks firewall to secure East-West traffic in the your Cisco ACI environment using unmanaged mode with policy-based redirect. This procedure assumes that you have completed the following:

- Firewalls are operational and connected to a leaf switch in your Cisco ACI environment. Additionally, the management interface of each firewall must be reachable by the APIC.
- Firewalls are deployed in active/passive HA mode. This procedure does not cover HA network setup and assumes you have completed this in advance.

To secure East-West traffic, define a bridge domain and subnet in the ACI fabric for the firewall. Configure contracts between EPGs that send traffic to the firewall using a PBR. The PBR forwards traffic to the firewall based on policy containg the firewall's IP and MAC address. The firewall interfaces are always in Layer 3 mode and traffic is received and routed back to the ACI fabric. You can configure separate interfaces for consumer and provider connections or a single interface for ingress and egress traffic. The procedure in this document uses a single interface because it simplifies the integration; you do not need to configure as many interfaces, IP addresses, or VLANs. However, when using a single interface, you cannot uses zone information in defining security policy and you must modify the default intra-zone policy on the firewall to deny traffic.

This procedure deploys the firewall in one-arm mode. In one-arm mode, the traffic enters and exits the firewall through a single interface. This common firewall interface is used for both consumer and provider interfaces in the service graph template. Using a single interface simplifies integration with the firewall by reducing the number IP addresses, VLANs, and interfaces that you must configure. However, a one-arm deployment model is intrazone, so you cannot use zone information to define security policy.

On the firewall:

- Create a Virtual Router and Security Zone
- Configure the Network Interfaces
- Configure a Static Default Route
- Create Address Objects for the EPGs
- Create Security Policy Rules

On the Cisco APIC:

- Create a VLAN Pool and Domain
- Configure an Interface Policy for LLDP and LACP for East-West Traffic
- Establish the Connection Between the Firewall and ACI Fabric

- Create a VRF and Bridge Domain
- Create an L4-L7 Device
- Create a Policy-Based Redirect
- Create and Apply a Service Graph Template

Create a Virtual Router and Security Zone

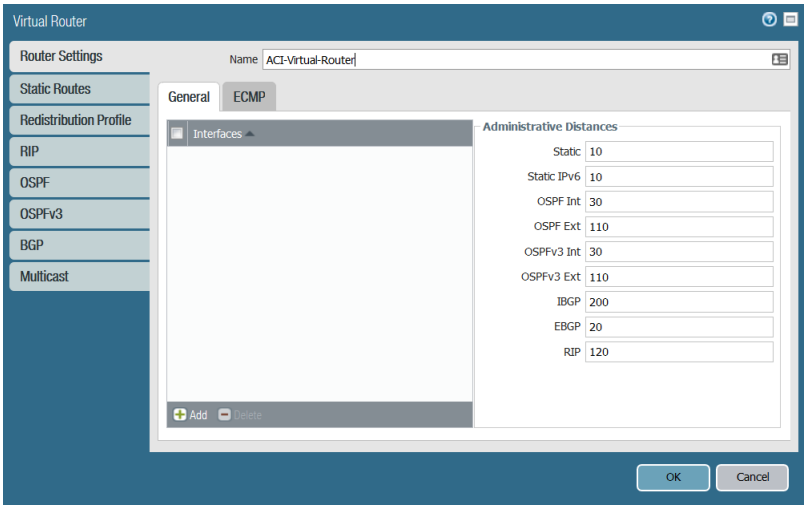
Configure a virtual router and zone on the firewall for each VRF in the tenant.

STEP 1 | Log in to the firewall.

STEP 2 | Select **Network** > **Virtual Routers** and click **Add**.

STEP 3 | Give the virtual router a descriptive **Name**.

STEP 4 | Click **OK**.

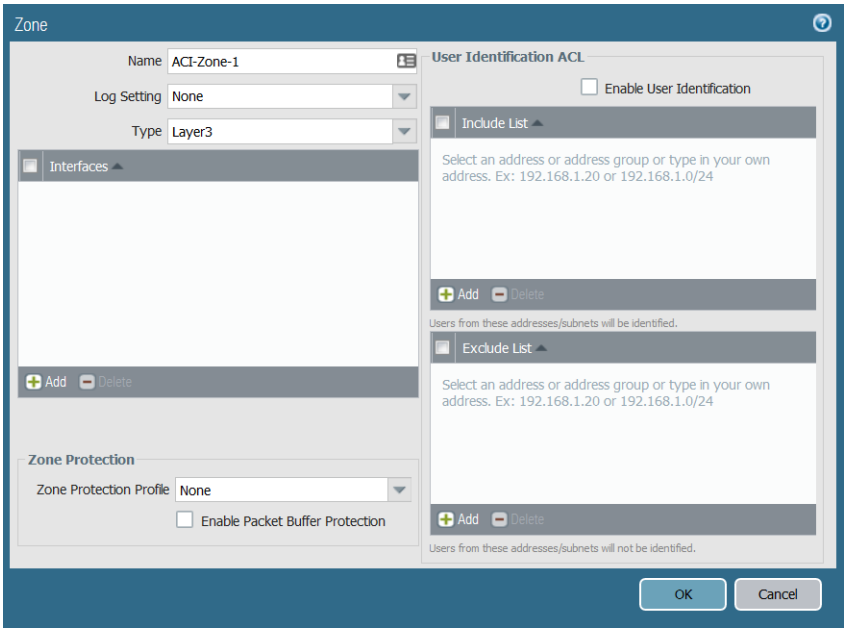


STEP 5 | Select **Network** > **Zones** and click **Add**.

STEP 6 | Give the zone a descriptive **Name**.

STEP 7 | Choose Layer 3 from the **Type** drop-down.

STEP 8 | Click **OK**.



STEP 9 | **Commit** your changes.

Configure the Network Interfaces

Configure the Ethernet interfaces that connect the firewall to the ACI leaf switches. The VLAN ID number used in this configuration should be a member of the VLAN pool assigned to the firewalls in ACI.

The VM-Series firewall does not support aggregate Ethernet groups.

STEP 1 | Select **Network** > **Interfaces** > **Ethernet** and click **Add Aggregate Group**.

STEP 2 | Enter a number for the aggregate group in the second **Interface Name** field.

STEP 3 | Select Layer 3 from the **Interface Type** drop-down.

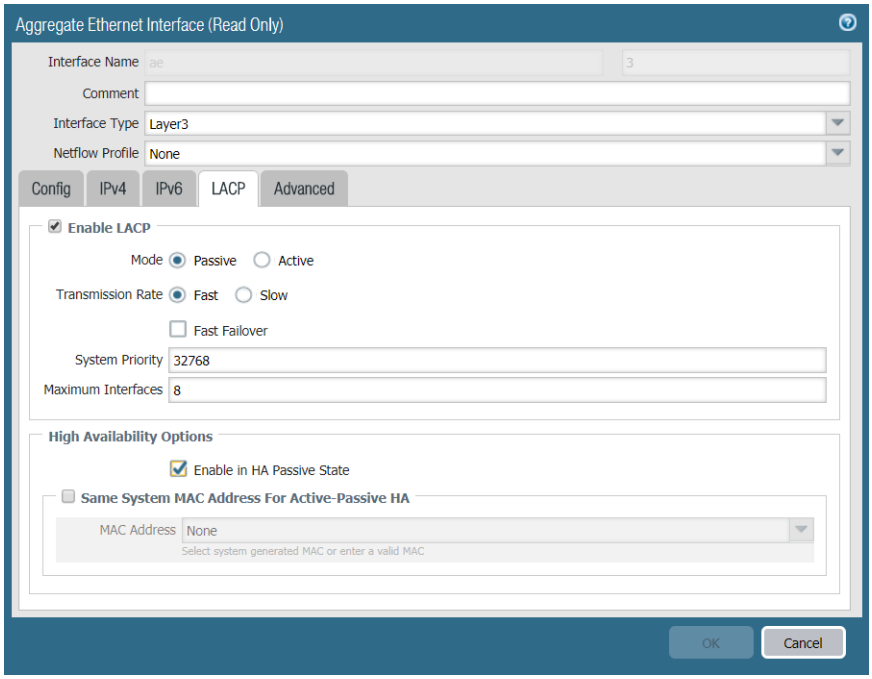
STEP 4 | Select the **LACP** tab and click **Enable LACP**.

STEP 5 | Select **Fast** as the **Transmission Rate**.

STEP 6 | Under High Availability Options, select **Enable in HA Passive State**.

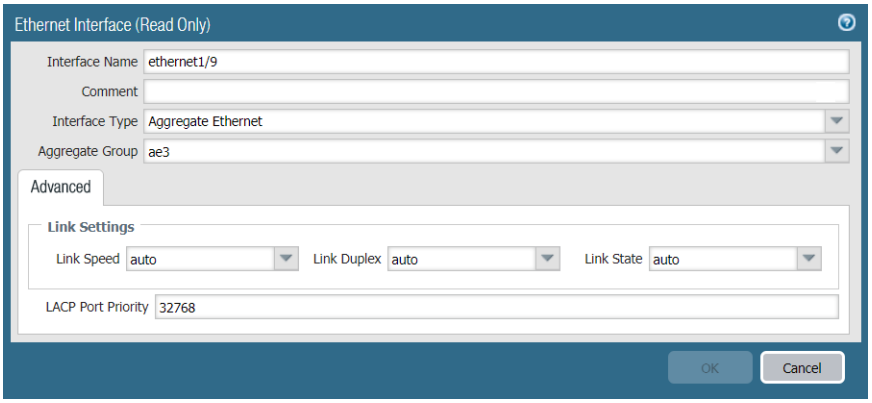
Do not select Same System MAC Address for Active-Passive HA. This option makes the firewall pair appear as a single device to the switch, so traffic will flow to both firewalls instead of just the active firewall.

STEP 7 | Click **OK**.



STEP 8 | Click on the name of an Ethernet interface to configure it and add it to the aggregate group.

1. Select **Aggregate Ethernet** from the Interface Type drop-down.
2. Select the interface you defined in the aggregate Ethernet group configuration.
3. Click **OK**.
4. Repeat this step for each other member interface of the aggregate Ethernet group.



STEP 9 | Add a subinterface on the aggregate Ethernet interface for the tenant and VRF.

1. Select the row of your aggregate Ethernet group and click **Add Subinterface**.
2. In the second **Interface Name** field, enter a numerical suffix to identify the subinterface.
3. In the **Tag** field, enter the VLAN tag of the subinterface.
4. Select the virtual router you configured previously from the **Virtual Router** drop-down.
5. Select the zone you configured previously from the **Zone** drop-down.
6. Select the **IPv4** tab.
7. Select the **Static** Type.
8. Click **Add** and enter the subinterface IP address and network mask in CIDR notation.
9. Click **OK**.

Configure a Static Default Route

Configure a static default route to direct traffic from the Ethernet subinterfaces to the subnet router.

STEP 1 | Select **Network** > **Virtual Routers** and click on the virtual router you created previously in this procedure.

STEP 2 | Select **Static Routes** > **IPv4** and click **Add**.

STEP 3 | Enter a descriptive **Name**.

STEP 4 | Enter 0.0.0.0/0 in the **Destination** field.

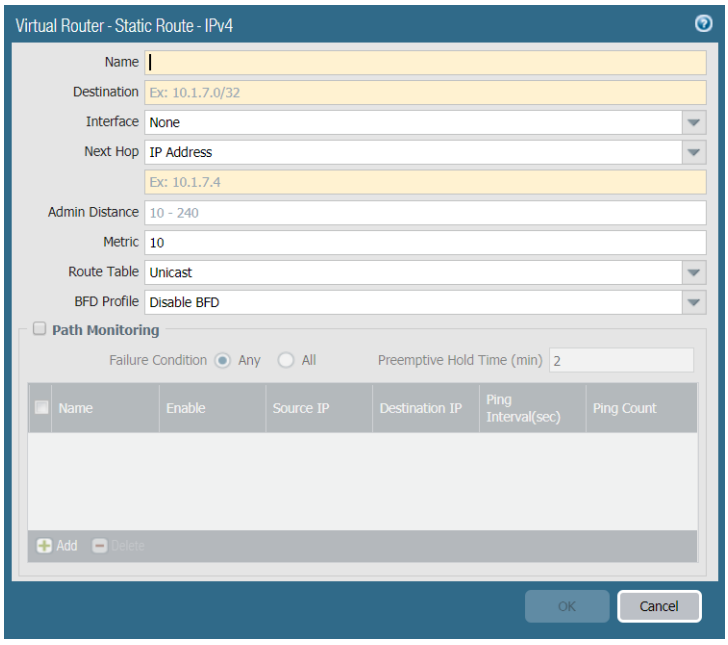
STEP 5 | From the **Interface** drop-down, select the aggregate Ethernet group you created previously in this procedure.

STEP 6 | Select IP Address from the **Next Hop** drop-down and enter the IP address of the next hop router.

STEP 7 | Click **OK**.

STEP 8 | Click **OK** again.

STEP 9 | **Commit** your changes.



Create Address Objects for the EPGs

You must define address objects and map them to endpoint groups (EPGs) to be used in security policy. Address groups are the best way map security groups to a group of servers using an endpoint IP address range. Create one address object for each of your EPGs.

STEP 1 | Select **Objects** > **Address** and click **Add**.

STEP 2 | Enter a descriptive name for your address object.

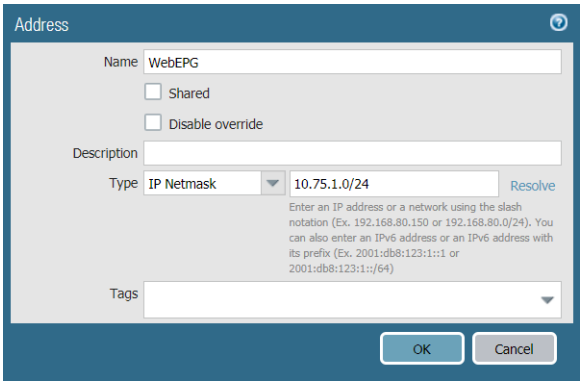
STEP 3 | Select IP Netmask from the **Type** drop-down.

STEP 4 | Enter the IP Netmask.

STEP 5 | Click **OK**.

STEP 6 | Repeat this process for each EPG.

STEP 7 | **Commit** your changes.



Create Security Policy Rules

Create security policy rules to control the traffic moving between your EPGs. By default, the firewall allows all intrazone traffic. Therefore, because the EPGs are in the same zone, all between those EPGs is allowed. Before creating a new rules, you will change the default intrazone rule from allow to deny.

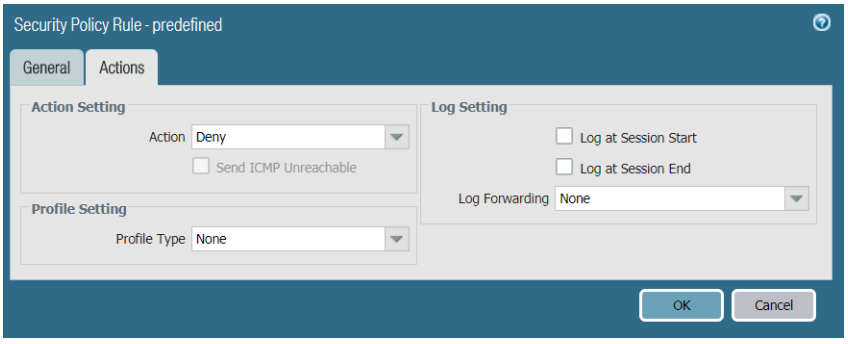
STEP 1 | Select **Policies** > **Security**.

STEP 2 | Click on intrazone-default to highlight the row and click **Override**.

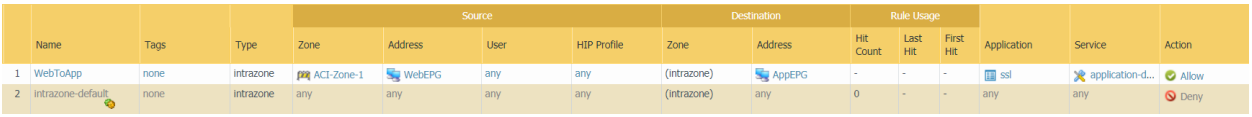
STEP 3 | Select the **Action** tab.

STEP 4 | Select Deny from the **Action** drop-down.

STEP 5 | Click **OK**.



STEP 6 | Configure additional security policy rules based on your needs using the address objects and zone you created for your EPG.



	Name	Tags	Type	Source				Destination		Rule Usage			Application	Service	Action
				Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit			
1	WebToApp	none	intrazone	ACI-Zone-1	WebEPG	any	any	(intrazone)	AppEPG	-	-	-	ssl	application-d...	Allow
2	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	0	-	-	any	any	Deny

Create a VLAN Pool and Domain

Configure the VLAN pool that will be used to allocate VLANs to the firewall when you attach interfaces to the ACI infrastructure for EPGs. The firewall's VLAN pull should have a static VLAN range.

Configure a dedicated domain for the firewall. A domain for the firewall is required to map the VLANs to the EPGs. Create a physical domain for a physical firewall and create a VMM domain for a VM-Series firewall.

STEP 1 | Create a VLAN pool.

1. Log in to your APIC.
2. Select **Fabric** > **Access Policies** > **Pools** > **VLAN**.
3. Right-click **VLAN** and select **Create VLAN Pool**.
4. Enter a descriptive **Name** for your VLAN pool.
5. Select **Dynamic Allocation** for Allocation Mode.
6. Click the plus (+) button to the right of **Encap Blocks**.
7. Enter your VLAN range in the **VLAN Range** field.
8. Select **Static Allocation** form the Allocation Mode drop-down.
9. Click **OK**.
10. Click **Submit**.

STEP 2 | (Physical firewall only) Create a physical domain.

1. Select **Fabric** > **Access Policies** > **Physical and External Domains** > **Physical Domains**.
2. Right-click **Physical Domain** and select **Create Physical Domain**.
3. Enter a descriptive **Name** for your physical domain.
4. Select the VLAN pool you created in the previous procedure from the VLAN Pool list.
5. Click **Submit**.

STEP 3 | (VM-Series firewall only) Create a VMM domain.

1. Select **Virtual Networking** > **VMM Domains** > **VMware**.
2. Right-click **VMware** and select **Create vCenter Domain**.
3. Enter a descriptive **Name** for your VMM domain.
4. Select **VMware vSphere Distributed Switch** from the **Virtual Switch** drop-down.
5. Select **VLAN** from the **Encapsulation** drop-down.
6. Select your VLAN pool from the **VLAN Pool** drop-down.
7. Click the plus (+) button to the right of **vCenter Credentials**.
8. Enter a descriptive **Profile Name** and your vCenter login information.
9. Click the plus (+) button to the right of **vCenter**.
10. Enter a descriptive **Name**.
11. Select vCenter from the Type drop-down.
12. Enter your vCenter IP address under **IP/Hostname**.
13. Select the vCenter Credentials profile you just created from the **Associated Credential** drop-down.
14. Click **Submit**.

Configure an Interface Policy for LLDP and LACP for East-West Traffic

Create policy that enables LLDP and LACP on the ACI interfaces that connect to your firewall.

LLDP is necessary for forwarding to work correctly in the ACI environment; ACI does not deploy a subnet router interface on a leaf switch unless it detects an endpoint on the switch that requires one. LLDP helps determine if a subnet router interface is required.

LACP provides greater resiliency and recovery speed on a link failure.

STEP 1 | Create an LLDP Interface Policy.

1. Select **Fabric** > **Access Policies** > **Interface Policies** > **Policies** > **LLDP Interface**.
2. Right-click on **LLDP Interface** and select **Create LLDP Interface Policy**.
3. Enter a descriptive **Name** for your LLDP interface policy.
4. Select **Enabled** for **Receive State**.
5. Select **Enabled** for **Transmit State**.
6. Click **Submit**.

STEP 2 | Create a Port Channel policy to enable LACP.

1. Select **Fabric** > **Access Policies** > **Interface Policies** > **Policies** > **Port Channel**.
2. Right-click on **Port Channel** and select **Create Port Channel Policy**.
3. Enter a descriptive **Name** for your port channel policy.
4. Select **LACP Active** from the **Mode** drop-down.
5. Click **Submit**.

Establish the Connection Between the Firewall and ACI Fabric

Attach your firewall to the leaf switch through a VPC connection using the Ethernet interface (or aggregate Ethernet group) you configured on your firewall earlier in this procedure. Connect the interface or interfaces to the same ports on the leaf switches.

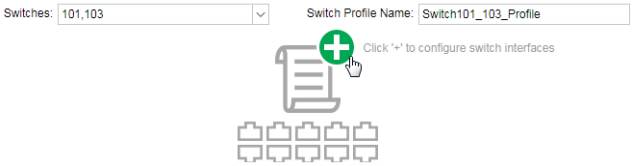
STEP 1 | Select **Fabric** > **Access Policies** > **Quick Start**.

STEP 2 | Click **Configure an interface, PC, and VPC**.

STEP 3 | Click the green and white plus (+).

STEP 4 | Select the leaf switch or switches to which you firewall is connected from the **Switches** drop-down.

STEP 5 | Click the green and white plus (+).



STEP 6 | Select VPC as the **Interface Type**.

STEP 7 | In the **Interfaces** field, enter the number of the interface your firewall uses to connect to the leaf switch.

STEP 8 | Enter a descriptive name into the **Interface Selector Name** field.

STEP 9 | Select **LLDP-Enabled** from the **LLDP Policy** drop-down.

STEP 10 | Select **LACP Active** from the **Port Channel Policy** drop-down.

STEP 11 | Select **Bare Metal** for a physical firewall or **ESX Hosts** for the VM-Series from the **Attached Device Type** drop-down.

STEP 12 | Select **Choose One** for **Domain**.

STEP 13 | Select the physical domain or VMM domain you created previously in this procedure from the **Domain** drop-down.

STEP 14 | Click **Save**.

STEP 15 | Click **Save** and then **Submit**.

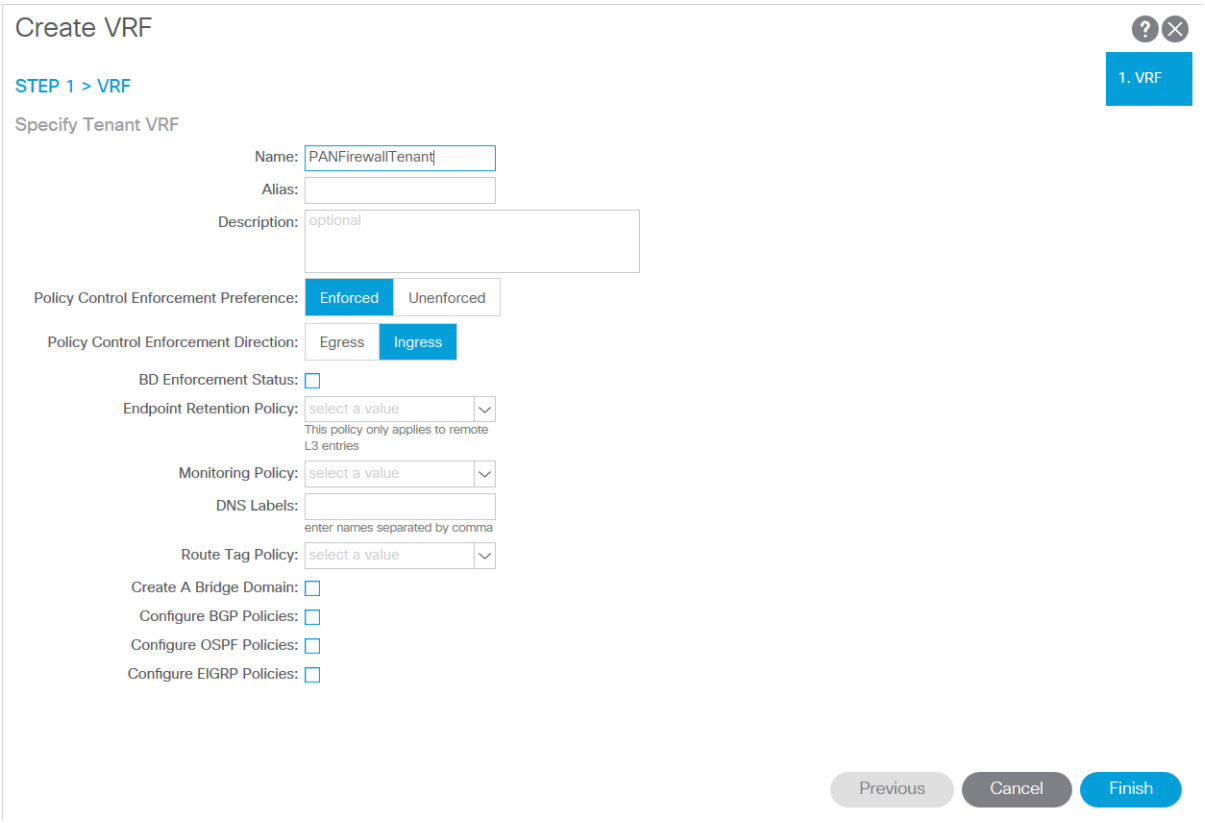
STEP 16 | Repeat this procedure for the second firewall in your HA pair.

Create a VRF and Bridge Domain

A tenant requires a VRF for all bridge domains and subnets. In this example, you will create a single, common VRF for the firewall and endpoints. Then configure a dedicated bridge domain for your firewall and disable dataplane learning. Disabling dataplane learning is required to use Policy Based Redirect in a bridge domain.

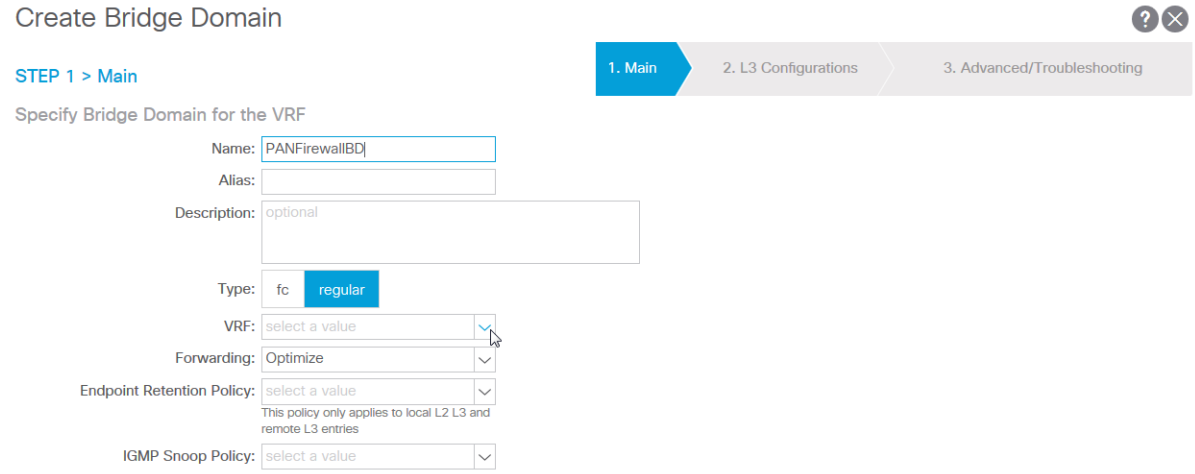
STEP 1 | Create a VRF.

1. On the **Tenants** tab, double-click on the name of your tenant.
2. Select **Networking** > **VRFs**.
3. Right-click **VRFs** and select **Create VRF**.
4. Enter a descriptive **Name** for your VRF.
5. Clear the **Create A Bridge Domain** check box.
6. Click **Finish**.



STEP 2 | Create a bridge domain for the firewall.

1. On the **Tenants** tab, double-click on the name of your tenant.
2. Select **Networking** > **Bridge Domains**.
3. Right-click **Bridge Domains** and select **Create Bridge Domain**.
4. Enter a descriptive **Name** for your bridge domain.
5. Select the VRF you created in the previous procedure from the **VRF** drop-down.
6. Click **Next**.



Create an L4-L7 Device

You must define the firewall as an L4-L7 device in the APIC so ACI can insert it into the traffic flow. You configure L4-L7 devices in the APIC as a device cluster, which is a construct that represents a single firewall or a firewall HA pair acting as a single device. Device clusters have one or more logical interfaces, which define the path of the member firewalls with a VLAN from the physical domain.

STEP 1 | On the **Tenants** tab, double-click on the name of your tenant.

STEP 2 | Select **Services** > **L4-L7** > **Devices**.

STEP 3 | Right-click **Devices** and select **Create L4-L7 Device**.

STEP 4 | Clear the **Managed** check box.

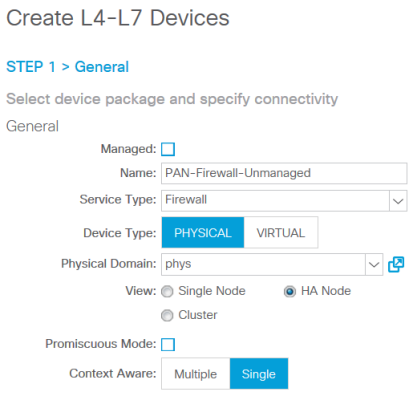
STEP 5 | Enter a descriptive **Name** for your L4-L7 Device.

STEP 6 | Select **Firewall** from the **Service Type** drop-down.

STEP 7 | Select **Physical** for a physical firewall or **Virtual** for a VM-Series firewall from the **Device Type** drop-down.

STEP 8 | Select the physical or VMM domain you created previously from the **Domain** drop-down.

STEP 9 | Select HA Node for **View**.



STEP 10 | Under **Device 1**, click the plus (+) icon to the right of **Device Interfaces**.

STEP 11 | Enter a descriptive **Name** for this interface.

STEP 12 | Under **Path**, select the path to the primary firewall in your HA pair.

STEP 13 | Click **Update**.

STEP 14 | Under **Device 2**, click the plus (+) icon to the right of **Device Interfaces**.

STEP 15 | Enter a descriptive **Name** for this interface.

STEP 16 | Under **Path**, select the path to the secondary firewall in your HA pair.

STEP 17 | Click **Update**.

STEP 18 | Under **Cluster**, click the plus (+) icon to the right of **Cluster Interfaces**.

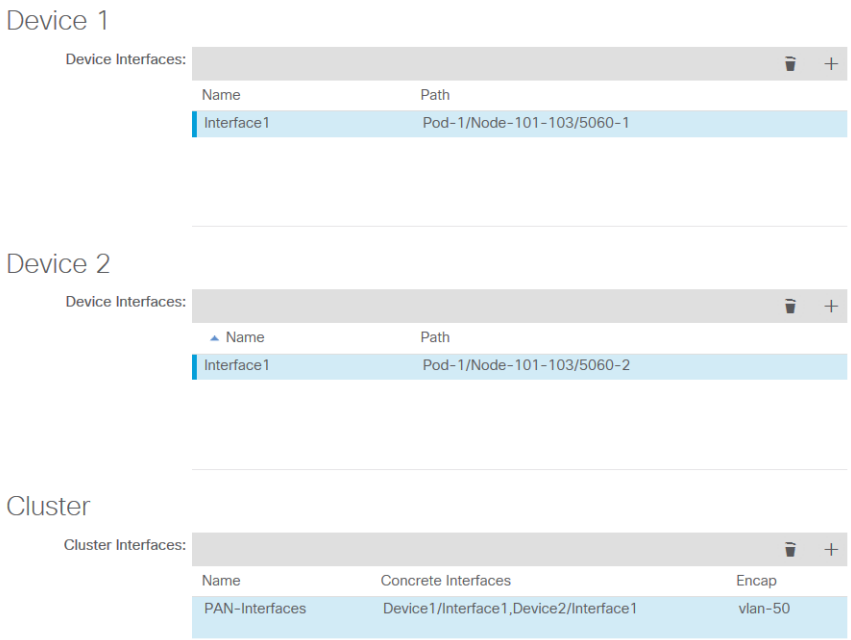
STEP 19 | Enter a descriptive **Name** for the cluster.

STEP 20 | Select the two interfaces you configured above from the list under **Concrete Interfaces**. The APIC requires that you configure two interfaces. However, because there is only one connection between the firewall and the ACI fabric, only one of the interfaces is used.

STEP 21 | Under **Encap**, enter a VLAN from the from the static VLAN pool you created earlier. Traffic will be redirected to the firewall on the VLAN assigned here.

STEP 22 | Click **Update**.

STEP 23 | Click **Finish**.



Create a Policy-Based Redirect

Configure the policy based redirect that sends the traffic between your EPGs to the firewall. Policy based redirect leverages the MAC address of the interface on the firewall. Before configuring the PBR setting on the APIC, you must get the MAC address from the firewall.

STEP 1 | Get the MAC address of the firewall.

1. Log into the firewall CLI.
2. Use the **`command show interface all`** to display the MAC addresses of your configured interfaces.
3. Copy the MAC address of the interface that will receive the redirected traffic.

STEP 2 | Create the L4-L7 Policy-Based Redirect.

1. Log into the APIC.
2. On the **Tenants** tab, double-click on the name of your tenant.
3. Select **Policies** > **Protocol** > **L4-L7 Policy Based Redirect**.
4. Right-click **L4-L7 Policy Based Redirect** and select **Create L4-L7 Policy Based Redirect**.

5. Enter a descriptive **Name** for your Policy Based Redirect.
6. Click the plus (+) icon to the right of **Destinations**.
7. In the **IP** field, enter the IP address of the interface that will receive the redirected traffic.
8. In the **MAC** field, enter the MAC address that you copied from the firewall CLI.
9. Click **OK**.
10. Click **Submit**.

Create and Apply a Service Graph Template

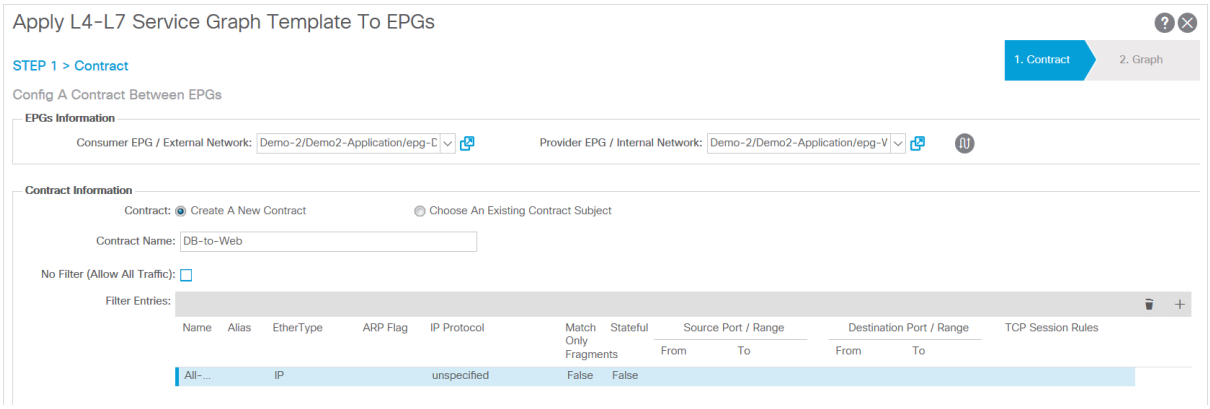
Create a service graph template that uses the device cluster representing the firewall in a policy-based redirect integration. After creating the service graph, you must apply it to EPGs to protect traffic. A contract and contract filter rules define the traffic that can be forwarded to the firewall.

STEP 1 | Create a service graph template.

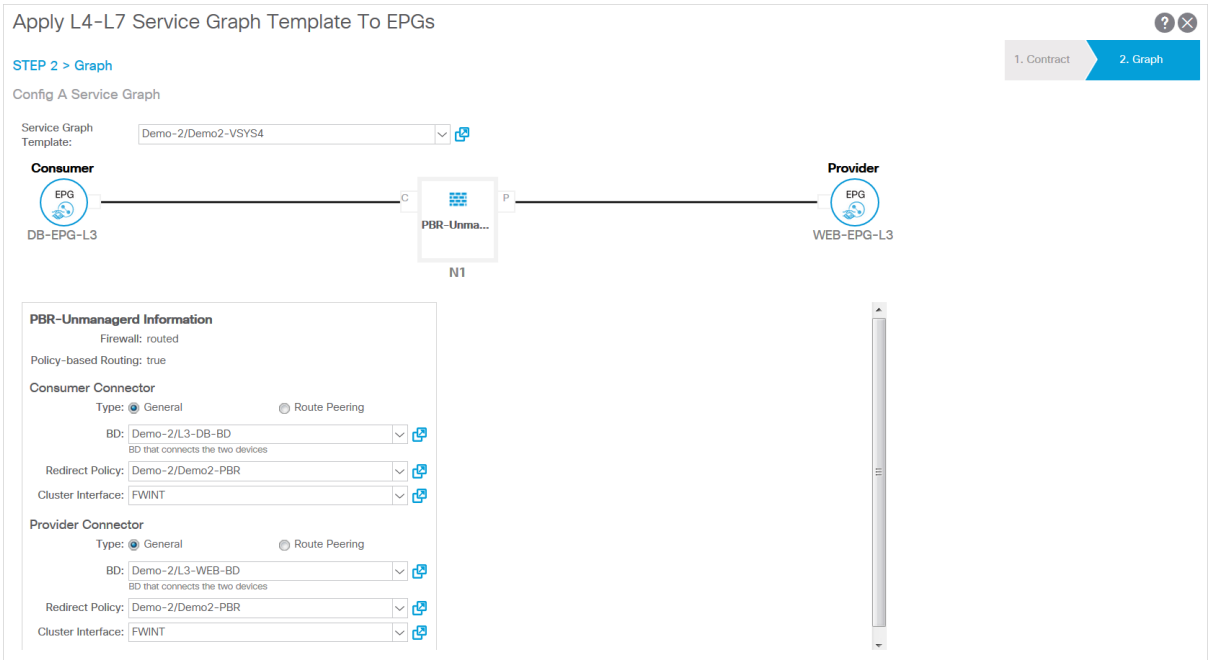
1. On the **Tenants** tab, double-click on the name of your tenant.
2. Select **Services** > **L4-L7** > **L4-L7 Service Graph Templates**.
3. Right-click **L4-L7 Service Graph Template** and select **Create L4-L7 Service Graph Template**.
4. Enter a descriptive **Graph Name** for your service graph template.
5. Select **Create a New One** for **Graph Type**.
6. Click and drag the L4-L7 device you created in the previous procedure bewteen the consumer and provider EPGs.
7. Select **Routed** for **Firewall**.
8. Select **Routed Redirect**.
9. Click **Submit**.

STEP 2 | Apply the service graph template.

1. On the **Tenants** tab, double-click on the name of your tenant.
2. Select **Services** > **L4-L7**.
3. In the **EPGs Information** pane, select your consumer and provider EPGs from the **Consumer EPG** and **Provider EPG** drop-downs.
4. Select **Create a New Contract**.
5. Enter a descriptive **Contract Name**.
6. Clear No Filter **(Allow All Traffic)**. Using this option is not recommended. To allow all traffic between the EPGs to be redirected to the firewall, it is recommended that you create a filter to do this.
7. Click the plus (+) icon to the right of **Filter Entries**.
8. Create a rule (or rules) to define what traffic is allowed to pass between the EPGs and redirected to the firewall.
9. Click **Next**.



10. Select the service graph template you created in the previous procedure from the **Service Graph Template** drop-down.
11. In the consumer and provider pane, select the bridge domain containing your firewall from the **BD** drop-downs.
12. Select the policy based redirect you created previously from the **Redirect Policy** drop-downs.
13. Select the cluster interface you created with you L4-L7 device from the **Cluster Interface** drop-downs.



Deploy the Firewall to Secure North-South Traffic in Network Policy Mode

Use network policy mode to secure North-South traffic entering and exiting your data center using unmanaged mode with policy-based redirect. This procedure assumes that you have completed the following:

- Firewalls are operational and connected to a leaf switch in your Cisco ACI environment. Additionally, the management interface of each firewall must be reachable by the APIC.
- Firewalls are deployed in active/passive HA mode. This procedure does not cover HA network setup and assumes you have completed this in advance.

To establish external connectivity to networks outside of your ACI fabric, you must configure an L3Out. And L3Out is a dedicated policy that contains the parameters required to connect external routing devices to a tenant. Additionally, an L3Out contain an external EPG (called an external network in the APIC UI) that represents networks accessible through the L3Out. The external EPG is not dynamically populated and follows a zero-trust model, so you must define the networks in the EPG. To make configuration easier, you can configure a network of 0.0.0.0/0 to assign all networks to the external EPG.

To secure inbound traffic, connect your firewall or firewalls in an HA pair to your border-leaf switches. Border-leaf switches are leaf switches that provide Layer 3 connections to external routers. The firewalls peer with the border-leaf switches using the open shortest path first (OSPF) protocol that is configured on each leaf switch in the vPC pair and communicates with the firewalls using a switch virtual interface (SVI). On the firewall, you configure a virtual router dedicated to the interfaces that connect to your data center. Additionally, this procedure includes

For outbound traffic, the firewall advertises the external networks to the border-leaf switches using OSPF. Additionally, the external network EPG is configured to allow all networks advertised by the firewall into that EPG. You create a contract between a vzAny managed object and the external networks EPG to allow traffic from any EPG within the VRF to reach the external networks through the firewall. The vzAny managed object allows you to consolidate all EPGs in a VRF to one or more contracts instead of creating a separate contracts for each EPG. The EPGs collected in the vzAny managed object consume the contact provided by the external EPG.

Unlike in service manager mode, management if the ACI infrastructure and the firewalls is completed separately.

On the APIC—

- Create a VLAN Pool and External Routed Domain
- Configure an Interface Policy for LLDP and LACP for North-South Traffic
- Create an External Routed Network
- Configure Subnets to Advertise to the External Firewall
- Create an Outbound Contract
- Create an Inbound Web Contract
- Apply Outbound and Inbound Contracts to the EPGs

On the firewall—

- Create a Virtual Router and Security Zone for North-South Traffic
- Configure the Network Interfaces
- Configure Route Redistribution and OSPF
- Configure NAT for External Connections

Create a VLAN Pool and External Routed Domain

Create a VLAN pool to allocate VLANs to the firewall as you attach interfaces to the infrastructure to support the EPGs in your ACI fabric. You should use a static VLAN range for the firewall.

Additionally, you must create a physical domain to map the VLANs to the EPGs. The following procedure creates a physical domain dedicated to the firewall.

STEP 1 | Create a VLAN pool.

1. Log in to your APIC.
2. Select **Fabric** > **Access Policies** > **Pools** > **VLAN**.
3. Right-click **VLAN** and select **Create VLAN Pool**.
4. Enter a descriptive **Name** for your VLAN pool.
5. Select **Dynamic Allocation** for Allocation Mode.
6. Click the plus (+) button to the right of **Encap Blocks**.

7. Enter your VLAN range in the **VLAN Range** field.
8. Select **Static Allocation** form the Allocation Mode drop-down.
9. Click **OK**.
10. Click **Submit**.

STEP 2 | Create an external routed domain.

1. Select **Fabric** > **Access Policies** > **Physical and External Domains** > **External Domains**.
2. Right-click **External Routed Domain** and select **Create Layer 3 Domain**.
3. Enter a descriptive **Name** for your physical domain.
4. Select the VLAN pool you created in the previous procedure from the VLAN Pool list.
5. Click **Submit**.

Configure an Interface Policy for LLDP and LACP for North-South Traffic

Create policy that enables LLDP and LACP on the ACI interfaces that connect to your firewall.

LLDP is necessary for forwarding to work correctly in the ACI environment; ACI does not deploy a subnet router interface on a leaf switch unless it detects an endpoint on the switch that requires one. LLDP helps determine if a subnet router interface is required.

LACP provides greater resiliency and recovery speed on a link failure.

STEP 1 | Create an LLDP Interface Policy.

1. Select **Fabric** > **Access Policies** > **Interface Policies** > **Policies** > **LLDP Interface**.
2. Right-click on **LLDP Interface** and select **Create LLDP Interface Policy**.
3. Enter a descriptive **Name** for your LLDP interface policy.
4. Select **Enabled** for **Receive State**.
5. Select **Enabled** for **Transmit State**.
6. Click **Submit**.

STEP 2 | Create a Port Channel policy to enable LACP.

1. Select **Fabric** > **Access Policies** > **Interface Policies** > **Policies** > **Port Channel**.
2. Right-click on **Port Channel** and select **Create Port Channel Policy**.
3. Enter a descriptive **Name** for your port channel policy.
4. Select **LACP Active** from the **Mode** drop-down.
5. Click **Submit**.

Create an External Routed Network

The firewalls pass IP routing information to the ACI ovar a Layer 3 OSPF network. ACI uses a switch virtual interface (SVI) on the leaf switches with an IP address on each switch for connection resilience. Create a Layer 3 routed network to peer with the firewall using OSPF.

STEP 1 | On the **Tenants** tab, double-click on the name of your tenant.

STEP 2 | Select **Networking** > **External Routed Networks**.

STEP 3 | Right-click **External Routed Networks** and select **Create Routed Outside**.

STEP 4 | Enter a descriptive **Name** for your **External Routed Network**.

STEP 5 | Select your VRF with external connectivity from the **VRF** drop-down.

STEP 6 | Select the external routed domain you created previously form the **External Routed Domain** drop-down.

STEP 7 | Select **OSPF**.

STEP 8 | Enter an **OSPF Area ID**. The Area ID can be expressed in decimal number or dotted decimal form. For example, Area 1 is the same as Area 0.0.0.1 or Area 271 is the same as Area 0.0.1.15. The Area ID range is 0 (0.0.0.0) to 4294967295 (255.255.255.255).

STEP 9 | Select **Regular Area** for the **OSPF Area Type**.

STEP 10 | Click the plus (+) button to the right of **Nodes and Interface Profiles** to create a Node Profile with a node that for the border-leaf switches that connect to the firewall.

STEP 11 | Enter a descriptive **Name** for your **Node Profile**.

STEP 12 | Attach nodes to your Node Profile.

1. Click the plus (+) button to the right of **Nodes**. This opens the **Select Node** window.
2. Select the node that your firewall is connected to from the **Node ID** drop-down.
3. Enter the IP address of the router attached to the leaf switch in **Router ID**.
4. Click **OK**.
5. Click the plus (+) button to the right of **Nodes and Interface Profiles**.
6. Enter a descriptive **Name** for your **Node Profile**.
7. Click the plus (+) button to the right of **Nodes**. This opens the **Select Node** window.
8. Select the node that your secondary HA firewall is connected to from the **Node ID** drop-down.
9. Enter the IP address of the router attached to the second leaf switch in **Router ID**.
10. Click **OK**.

STEP 13 | Attach an OSPF Interface Profile for your Node Profile.

1. Enter a descriptive **Name** for your OSPF Interface Profile.
2. Click **Next**.
3. Select **Create OSPF Interface Policy** from the OSPF Policy drop-down.
4. Enter a descriptive **Name** for your OSPF Interface Policy.
5. Select **MTU Ignore**.
6. Click **Submit**.
7. Click **Next**.
8. Click **SVI**.
9. Click the plus (+) button to the right of **SVI Interfaces**. This opens the **Select SVI** window.
10. Click **Virtual Port Channel**.
11. Select the Path to the port and port channel interface where the firewall connects to the leaf switch.
12. In **Encap**, enter the VLAN encapsulation used for your layer 3 outside profile.
13. Select **Trunk** for Mode.
14. In the **Side A IPv4 Primary Address** field, enter the primary IP address of the path attached to the layer 3 outside profile.
15. In the **Side B IPv4 Primary Address** field, enter the secondary IP address of the path attached to the layer 3 outside profile.
16. Click **OK**.

STEP 14 | Click **OK** to close the Create Interface Profile window.

STEP 15 | Click **OK** to close the Create Node Profile window.

STEP 16 | Click **Next**.

STEP 17 | Click the plus (+) button to the right of **External EPG Networks**. This opens the **Create Routed Outside** window.

STEP 18 | Enter a descriptive **Name** for you External Network.

STEP 19 | Add a subnet to you External Network.

1. Click the plus (+) button to the right of **Subnets**.
2. Enter the IP address and mask of the subnet's default gateway.
3. Select **Export Route Control Subnet**.
4. Select **External Subnets for External EPG**.
5. Click **OK**.

STEP 20 | Click **Finish**.

Configure Subnets to Advertise to the External Firewall

By default, subnets in the ACI fabric are not advertised to external networks. You must configure the subnets to be advertised externally.

STEP 1 | On the **Tenants** tab, double-click on the name of your tenant.

STEP 2 | Select **Networking** > **Bridge Domains** > **<your bridge domain>**.

STEP 3 | Click **L3 Configurations**.

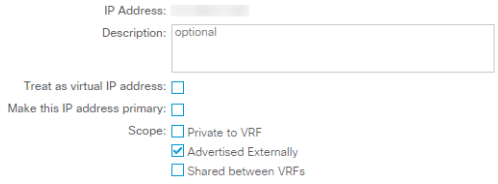
STEP 4 | Click the plus (+) button to the right of **Associated L3 Outs**.

STEP 5 | Select the Layer 3 external routed network connection you created in the previous procedure from the **L3 Out** drop-down.

STEP 6 | Click **Update**.

STEP 7 | Select **Networking** > **Bridge Domains** > **<your bridge domain>** > **Subnets** > **<externally advertised subnet>**.

STEP 8 | Set the Scope to **Advertised Externally**.



STEP 9 | Click **Submit**.

Create an Outbound Contract

Create a contract with a filter that allows DNS, NTP, HTTP, and HTTPS traffic. You will use this contract to allow all endpoints in the VRF to reach the external networks but limits the traffic sent to the firewall.

STEP 1 | On the **Tenants** tab, double-click on the name of your tenant.

STEP 2 | Select **Contracts** > **Filters**

STEP 3 | Right-click on **Filters** and select **Create Filter**.

STEP 4 | Enter a descriptive **Name** for the filter.

STEP 5 | Create a filter entry for UDP traffic.

1. Click the plus (+) button to the right of **Entries**.
2. Enter a descriptive **Name** for the **UDP** filter.
3. Select **IP** from the **EtherType** drop-down.
4. Select **udp** from the **IP Protocol** drop-down.
5. Select **dns** from the **Destination Port From** drop-down.
6. Click **Update**.

STEP 6 | Create a filter entry for TCP traffic.

1. Click the plus (+) button to the right of **Entries**.
2. Enter a descriptive **Name** for the **TCP** filter.
3. Select **IP** from the **EtherType** drop-down.
4. Select **tcp** from the **IP Protocol** drop-down.
5. Select **dns** from the **Destination Port From** drop-down.
6. Click **Update**.

STEP 7 | Create a filter entry for NTP traffic.

1. Click the plus (+) button to the right of **Entries**.
2. Enter a descriptive **Name** for the **NTP** filter.
3. Select **IP** from the **EtherType** drop-down.
4. Select **udp** from the **IP Protocol** drop-down.
5. In the **Destination Port From** field, enter 123.
6. Click **Update**.

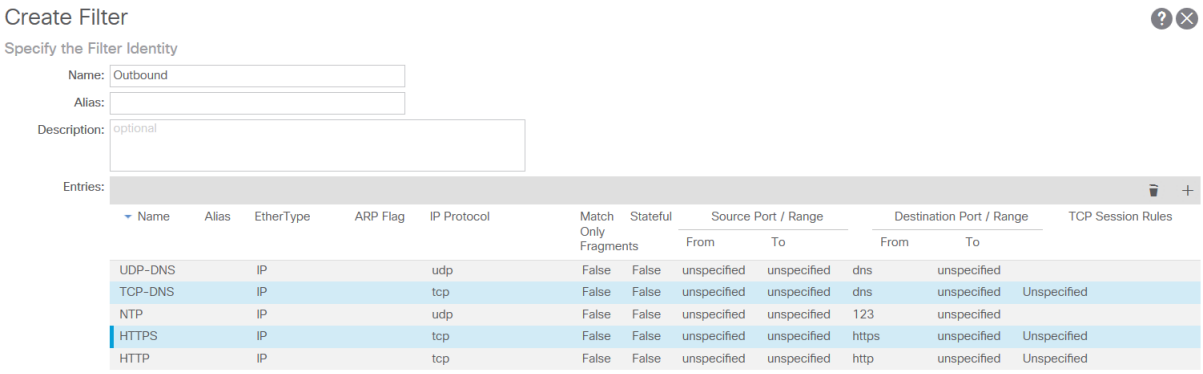
STEP 8 | Create a filter entry for HTTP traffic.

1. Click the plus (+) button to the right of **Entries**.
2. Enter a descriptive **Name** for the **HTTP** filter.
3. Select **IP** from the **EtherType** drop-down.
4. Select **tcp** from the **IP Protocol** drop-down.
5. Select **http** from the **Destination Port From** drop-down.
6. Click **Update**.

STEP 9 | Create a filter entry for HTTPS traffic.

1. Click the plus (+) button to the right of **Entries**.
2. Enter a descriptive **Name** for the **HTTP** filter.
3. Select **IP** from the **EtherType** drop-down.
4. Select **tcp** from the **IP Protocol** drop-down.
5. Select **https** from the **Destination Port From** drop-down.
6. Click **Update**.

STEP 10 | Click **Submit**.



STEP 11 | Create a contract for outbound traffic.

1. On the **Tenants** tab, double-click on the name of your tenant and select **Contracts**.
2. Right-click on **Contracts** and select **Create Contract**.
3. Enter a descriptive **Name** for your **Contract**.
4. Click the plus (+) button to the right of **Subjects**.
5. Enter a descriptive **Name** for you **Subject**.
6. Under Filter Chain, click the plus (+) button to the right of **Filters**.
7. Select the filter you created previously from the drop-down.
8. Click **OK**.

STEP 12 | Click **Submit**.

Create an Inbound Web Contract

You must also create a contract and filters to allow inbound traffic to reach the servers behind the firewall. The following procedure describes the process of creating a contract and filters that allows HTTP and HTTPS web traffic to access resources behind the firewall.

STEP 1 | On the **Tenants** tab, double-click on the name of your tenant.

STEP 2 | Select **Contracts** > **Filters**

STEP 3 | Right-click on **Filters** and select **Create Filter**.

STEP 4 | Enter a descriptive **Name** for the filter.

STEP 5 | Create a filter entry for HTTP traffic.

1. Click the plus (+) button to the right of **Entries**.
2. Enter a descriptive **Name** for the **HTTP** filter.
3. Select **IP** from the **EtherType** drop-down.
4. Select **tcp** from the **IP Protocol** drop-down.
5. Select **http** from the **Destination Port From** drop-down.
6. Click **Update**.

STEP 6 | Create a filter entry for HTTPS traffic.

1. Click the plus (+) button to the right of **Entries**.
2. Enter a descriptive **Name** for the **TCP** filter.
3. Select **IP** from the **EtherType** drop-down.
4. Select **tcp** from the **IP Protocol** drop-down.

5. Select **https** from the **Destination Port From** drop-down.
6. Click **Update**.

STEP 7 | Click **Submit**.

STEP 8 | Create a contract for inbound web traffic.

1. On the **Tenants** tab, double-click on the name of your tenant and select **Contracts**.
2. Right-click on **Contracts** and select **Create Contract**.
3. Enter a descriptive **Name** for your **Contract**.
4. Click the plus (+) button to the right of **Subjects**.
5. Enter a descriptive **Name** for you **Subject**.
6. Under Filter Chain, click the plus (+) button to the right of **Filters**.
7. Select the filter you created previously from the drop-down.
8. Click **OK**.

STEP 9 | Click **Submit**.

Apply Outbound and Inbound Contracts to the EPGs

Now you must apply the inbound and outbound contracts to the appropriate EPGs.

For all the EPGs (EPG collection) within a VRF to send traffic to an external destination, each internal EPG must contract with the external EPG. Typically, you would need to create a separate contract between each internal EPG and the external EPG. However, using a vzAny object you can apply the same contract to all EPGs dynamically. The EPG collection consumes the contract and the external EPG provides the contract. You can configure specific traffic profiles in the contract or send all traffic to the firewall and allow it to control the traffic leaving the datacenter. Additionally, any new EPG that joins the VRF will automatically has the contract applied to it.

Apply the inbound contract so the internal EPG is the provider and the external EPG is the consumer. Traffic flowing to the internal EPG is fist checked against the contract and any allowed traffic is then secured further by the firewall as necessary.

STEP 1 | Apply the outbound contract to all EPGs in the VRF.

1. On the **Tenants** tab, double-click on the name of your tenant.
2. Select **Networking** > **VRFs** > **<you VRF>** > **EPG Collection for VRF**.
3. Click the plus (+) button to the right of **Consumed Contracts**.
4. Select your outbound contract from the **Name** drop-down.
5. Click **Update**.
6. Select **Networking** > **External Routed Networks** > **<your external routed network>** > **Networks** > **External**.
7. Click the plus (+) button to the right of **Provided Contracts**.
8. Select your outbound contract from the **Name** drop-down.
9. Click **Update**.

STEP 2 | Apply the inbound contract so an internal EPG provides it to the external EPG.

1. On the **Tenants** tab, double-click on the name of your tenant.
2. Select **Application Profiles** > **<your application profile>** > **Application EPGs** > **<your application EPG>** > **Contracts**.
3. Right-click on **Contracts** and select **Add Provided Contract**.
4. Select your inbound contract from the **Contract** drop-down.
5. Click **Submit**.

6. On the same tenant, select **Networking** > **External Routed Networks** > **<your external routed network>** > **Networks** > **External**.
7. On the Contracts tab, click the plus (+) button to the right of **Consumed Contracts**.
8. Select your inbound contract from the **Name** drop-down.
9. Click **Update**.

Create a Virtual Router and Security Zone for North-South Traffic

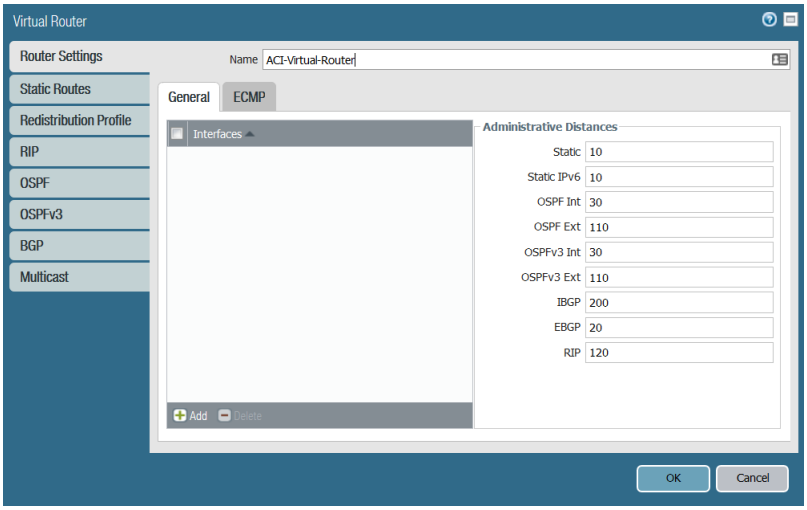
Create a virtual router and security zone on the firewall to match the tenant and VRF on ACI.

STEP 1 | Log in to the firewall.

STEP 2 | Select **Network** > **Virtual Routers** and click **Add**.

STEP 3 | Give the virtual router a descriptive **Name**.

STEP 4 | Click **OK**.

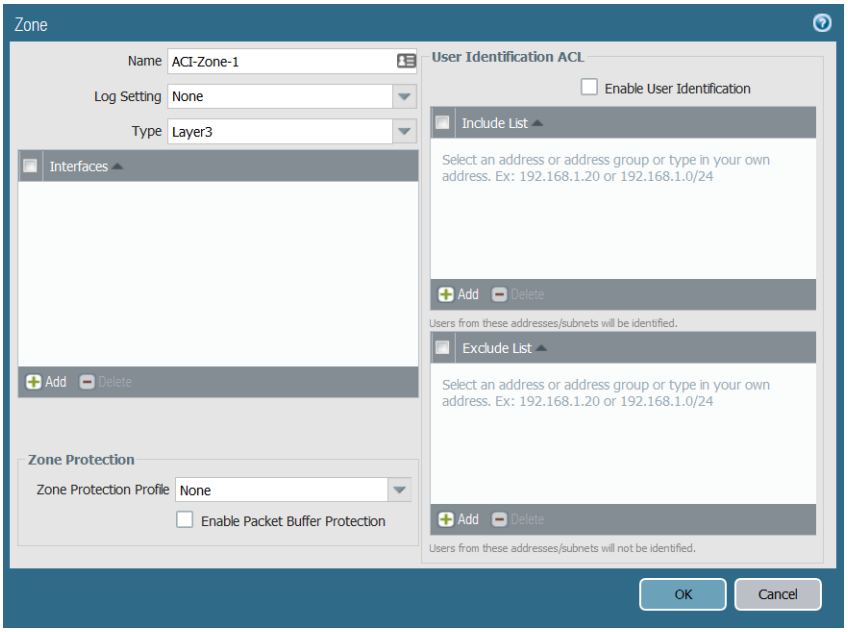


STEP 5 | Select **Network** > **Zones** and click **Add**.

STEP 6 | Give the zone a descriptive **Name**.

STEP 7 | Choose Layer 3 from the **Type** drop-down.

STEP 8 | Click **OK**.



STEP 9 | **Commit** your changes.

Configure the Network Interfaces

Configure an aggregate Ethernet interface, member interfaces, and subinterface that your firewall uses to connect to the ACI leaf switches. If you are using a VM-Series firewall, use discreet interfaces instead of aggregate interfaces.

The VM-Series firewall does not support aggregate Ethernet groups.

STEP 1 | Select **Network** > **Interfaces** > **Ethernet** and click **Add Aggregate Group**.

STEP 2 | Enter a number for the aggregate group in the second **Interface Name** field.

STEP 3 | Select Layer 3 from the **Interface Type** drop-down.

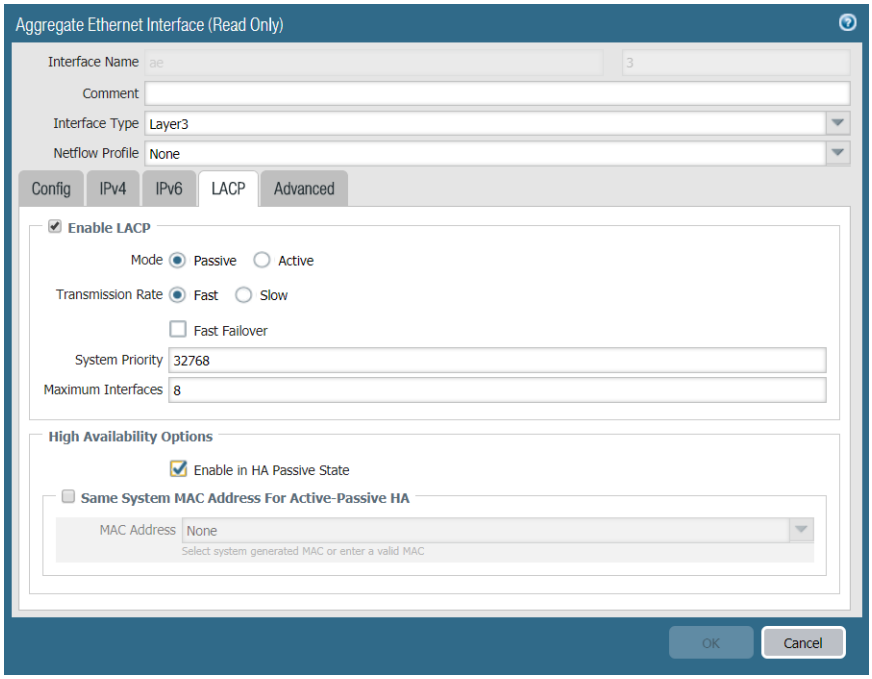
STEP 4 | Select the **LACP** tab and click **Enable LACP**.

STEP 5 | Select **Fast** as the **Transmission Rate**.

STEP 6 | Under High Availability Options, select **Enable in HA Passive State**.

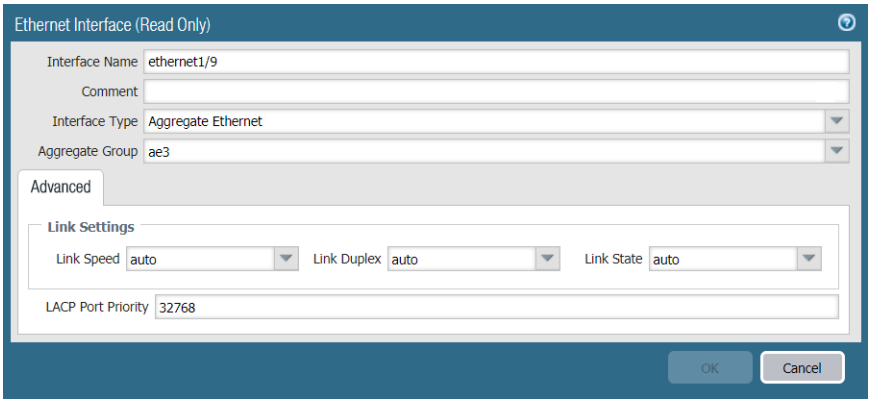
Do not select Same System MAC Address for Active-Passive HA. This option makes the firewall pair appear as a single device to the switch, so traffic will flow to both firewalls instead of just the active firewall.

STEP 7 | Click **OK**.



STEP 8 | Click on the name of an Ethernet interface to configure it and add it to the aggregate group.

1. Select **Aggregate Ethernet** from the Interface Type drop-down.
2. Select the interface you defined in the aggregate Ethernet group configuration.
3. Click **OK**.
4. Repeat this step for each other member interface of the aggregate Ethernet group.



STEP 9 | Add a subinterface on the aggregate Ethernet interface for the tenant and VRF.

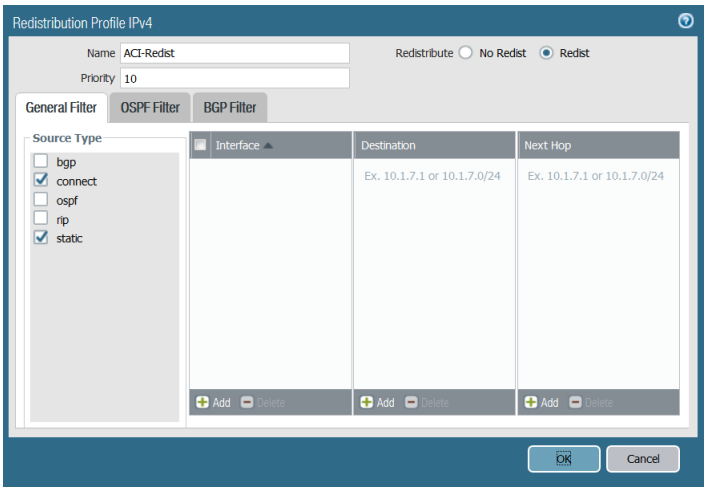
1. Select the row of your aggregate Ethernet group and click **Add Subinterface**.
2. In the second **Interface Name** field, enter a numerical suffix to identify the subinterface.
3. In the **Tag** field, enter the VLAN tag of the subinterface.
4. Select the virtual router you configured previously from the **Virtual Router** drop-down.
5. Select the zone you configured previously from the **Zone** drop-down.
6. Select the **IPv4** tab.
7. Select the **Static** Type.
8. Click **Add** and enter the subinterface IP address and network mask in CIDR notation.
9. Click **OK**.

Configure Route Redistribution and OSPF

Configure route redistribution to make routing information from the firewall available to the external-facing routers attached to your leaf switches. Then configure OSPF on the firewall and assign a router-id, area number, and interface to form adjacencies.

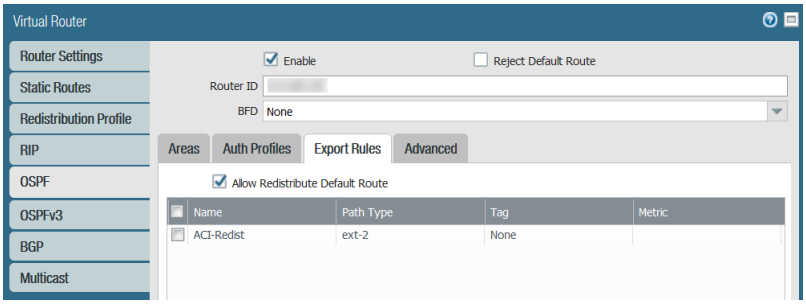
STEP 1 | Configure route redistribution.

1. Select **Network** > **Virtual Routers** and click on the virtual router you created earlier.
2. Select **Redistribution Profile** > **IPv4** > **Add**.
3. Enter a descriptive **Name** for your redistribution profile.
4. Enter a priority.
5. For **Redistribute**, select **Redist**.
6. Check **connect** and **static** under **General Filters**.
7. Click **OK**.



STEP 2 | Configure OSPF.

1. Select **Network** > **Virtual Routers** and click on the virtual router you created earlier.
2. Select **Router Settings** > **ECMP** and select **Enable**.
3. Select **OSPF** and choose **Enable**.
4. Enter the OSPF **Router ID**.
5. Under **Area**, click **Add**.
6. Enter the **Area ID**. This value must match the value you assigned when you created the external routed network on the APIC. On the firewall, this must be entered in dotted decimal form. For example, if you entered an Area ID of 10 in the APIC, the equivalent on the firewall is 0.0.0.10.
7. Select **Interface** > **Add**.
8. Enter the interface that connects to your external network EPG and click **OK**.
9. Select **Export Rules** > **Add**.
10. Select the Redistribution Profile you created above from the **Name** drop-down and click **OK**.
11. Select **Allow Redistribute Default Route**.
12. Click **OK**.

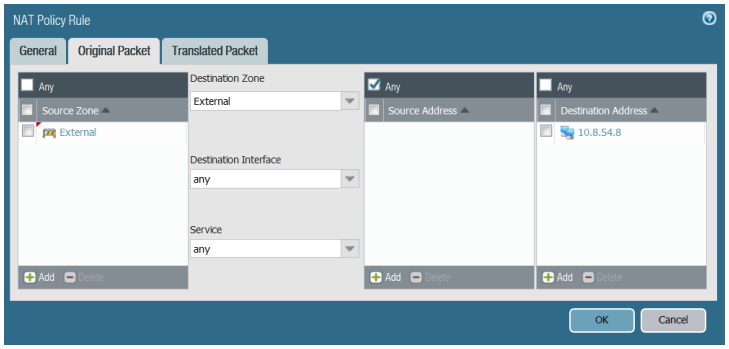


Configure NAT for External Connections

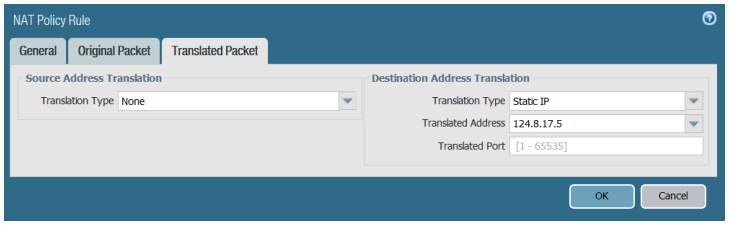
You only need to configure NAT if the firewall has an external interface used for connecting to networks outside of your data center. While NAT is not required, you can use this procedure to translate private IP addressing in your data center to public IP addressing outside. Begin setting up NAT by configuring address translation for traffic entering server inside an EPG in your data center. Then configure a NAT policy that translates the source address of outbound traffic from any EPG to the external interface IP address.

STEP 1 | Configure address translation for traffic entering an EPG in your data center.

1. Select **Policies** > **NAT** and click **Add**.
2. Enter a descriptive **Name** for your NAT policy rule.
3. Select **Original Packet** and click **Add** under **Source Zone**.
4. Select the source zone from the drop-down.
5. Select the destination zone from the **Destination Zone** drop-down.
6. Select **Any** for the **Source Address**.
7. Click **Add** under **Destination Address** and enter the external IP address.



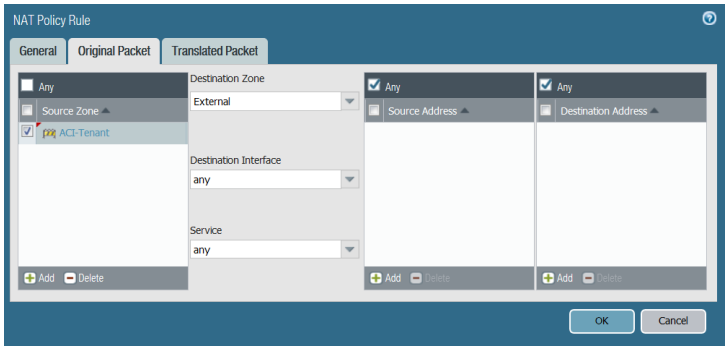
8. On the **Translated Packet** tab, select the **Translation Type** under **Destination Address Translation**.
9. Select an address from the **Translated Address** drop-down.
10. Click **OK**.



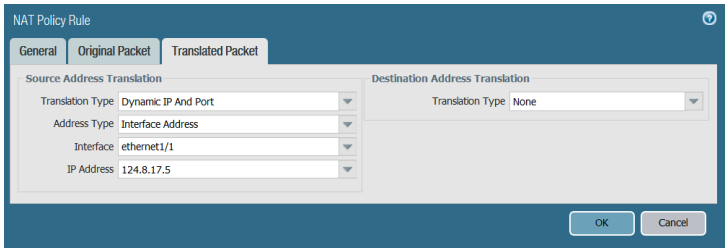
STEP 2 | Configure address translation for outbound traffic.

1. Select **Policies** > **NAT** and click **Add**.
2. Enter a descriptive **Name** for your outbound NAT policy.
3. Select **Original Packet** and click **Add** under **Source Zone**.

4. Select the zone that matches your ACI tenant and VRF.
5. Select the external zone from the **Destination Zone** drop-down.



6. On the **Translated Packet** tab, select the **Translation Type** under **Source Address Translation**.
7. Enter additional required address information.
8. Click **OK**.



STEP 3 | **Commit** your changes.

Integrate a Palo Alto Networks Firewall with Cisco ACI Using the Device Package

This section describes the creation of a tenant, application profile, and firewall service in Cisco ACI.

- Create a Tenant and Application Profile
- Create an L4-L7 Service
- Create and Deploy a Service Graph Template

Components of Cisco ACI Integration Using the Device Package

The following components are required to integrate the Palo Alto Networks firewall into your Cisco ACI environment using the Palo Alto Networks Device Package.

- Panorama—Panorama is required to deploy security policy and objects on the firewall using the APIC. This document assumes that you are using Panorama. You can deploy the firewall without Panorama and APIC will deploy the context (vsys), high availability, and network interface configuration to the firewall but any security policy must be configured directly on the firewall.

  Panorama acts as a single point of connection between the APIC and the firewalls. Cisco ACI deploys security policy and objects from Panorama to its managed firewalls. The APIC sets devices groups for firewalls based on the APIC configuration and then commits the device groups configuration to the firewall, including security policy, NAT policy, threat profiles, and address objects.

  Cisco ACI integration supports physical and virtual versions of Panorama.
- Palo Alto Networks Firewall—Cisco ACI integration supports physical firewall appliances and the VM-Series firewall for VMware ESXi (standalone version).

  Cisco ACI integration supports physical firewalls divided into contexts that the APIC manages as individual firewalls. On hardware-based firewalls, these contexts are the virtual systems (vsys) on the firewalls; each firewall is licensed to support a certain number of vsys instances. When deploying a multi-vsys firewall in ACI, you must configure a chassis manager in the tenant and assign it to the firewall service.
- Cisco APIC—The APIC is your interface for managing your ACI environment. From here, you will create the firewall service, insert the firewall service between endpoint groups, and direct traffic to the firewall.
- Device Package (Service Manager Mode only)—A device package allows and manages communication between the APIC and Panorama and firewalls. It allows you to configure high availability, networking, and interfaces for the firewall in the APIC and push it to Panorama and the firewalls. Once deployed in ACI, you complete your security configuration through Panorama or the individual firewalls.

The Palo Alto Networks device package version 1.3 requires PAN-OS 8.0 and Cisco ACI 2.3.

Create a Tenant and Application Profile

You must create a tenant to contain the application and firewall service. The tenant contains the virtual routing and forwarding (VRF) object, endpoint groups, and application profile.

STEP 1 | Create a tenant, VRF, and two bridge domain.

1. Login to the APIC UI.
2. Select **Tenant** > **Add Tenant**.
3. Enter a **Name** for your tenant.
4. Enter a **VRF Name** for you VRF.
5. Verify that **Take me to this tenant when I click finish** is checked.

6. Click **Submit**. You will be redirected to **Tenant** > **<your-tenant>** > **Networking** where you will add bridge domains.
7. Click and drag the bridge domain (BD) icon next to the icon of the VRF you named previously. This action opens the Create Bridge Domain window.
8. Enter a **Name** for your bridge domain.
9. Click **Submit**.
10. Repeat steps g, h, and i for you second bridge domain.

STEP 2 | Create an Application Profile with two endpoint groups (EPG). Each EPG must correspond to one of the bridge domains you created previously.

1. In the APIC UI, select **Tenants** and double click on the tenant you created previously.
2. Right click on **Application Profiles** and select **Create Application Profile**.
3. Enter a **Name** for you Application Profile.
4. Click the plus (+) icon under EPGs to and EPG.
5. Enter a **Name** for your EPG.
6. Select a bridge domain.
7. Select a domain for the EPG.

   If you choose a virtual domain (VMM), you do not need to provide any further information for the EPG. However, if you choose a physical domain, you need to specify a static path.

   The static path is the physical port on a leaf switch that the firewall is connected to. This mapping was determined when you created you ACI Fabric and deployed the firewall.

STEP 3 | Create a Device Manager. The device manager is your Panorama.

1. Select **L4-L7 Services**.
2. Right click **Device Managers** and select **Create Device Manager**.
3. Enter a **Name** for the device manager.
4. From the Device Manager Type drop-down, select the option that corresponds the with the Palo Alto Networks device package you installed.
5. Click the plus (+) icon under Management and enter the management IP address of Panorama and port 443 because HTTPS is used to connect to Panorama.
6. Click **Update**.
7. Enter the username and password for Panorama.
8. Click **Submit**.

STEP 4 | (Optional) Create a Chassis. A chassis is required to deploy multi-context firewalls (vsys). Without a chassis, the APIC always configures the default vsys (vsys1).

1. Select **L4-L7 Services**.
2. Right click **Chassis** and select **Create Chassis**.
3. Enter a **Name** for the chassis.
4. Enter a username and password and confirm the password.
5. Enter the chassis host IP address and port.

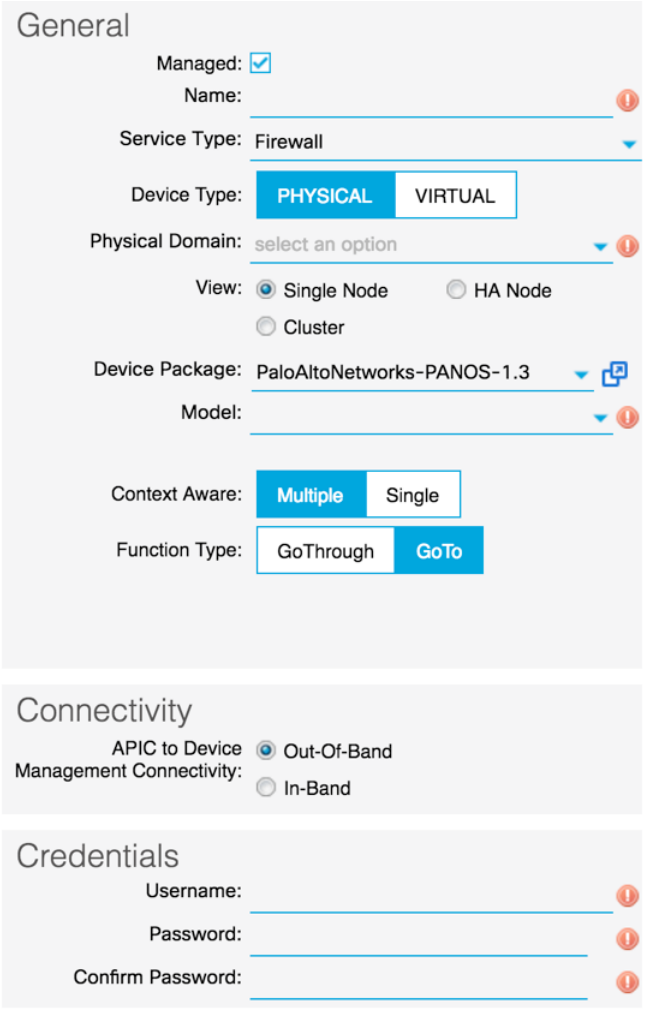
   APIC never uses the username and password entered for the chassis, so the values entered are irrelevant but requested by the APIC. The chassis must exist and is set as the chassis for the firewall device. This instructs APIC to use a vsys other than the default vsys (vsys1).

Create an L4-L7 Service

Now that you have created your tenant with an application profile containing two EPGs, you must configure the firewall as a L4-L7 Service and insert that service between the EPGs. The firewall service then secures the traffic between the EPGs.

STEP 1 | Enter general information about the firewall.

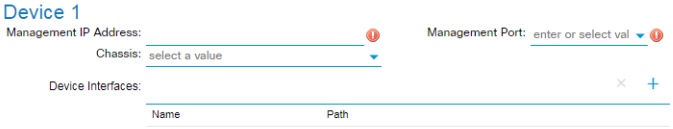
1. Right click **L4-L7 Devices** and select **Create L4-L7 Devices**.
2. Enter a **Name** for your firewall service.
3. Select **Firewall** from the Service Type drop-down.
4. Under Device Type, select **Physical** or **Virtual** depending on the firewall you deployed.
5. Select the Physical or VMM Domain. This is the same domain you chose when creating the application profile.
6. Under View, select Single Node for a single firewall or HA Node for firewalls in an HA pair.
7. Select the Device Package.
8. Select the Model of the firewall you deployed. The device package comes preset with several Palo Alto Networks firewall models.
9. Set **Context Aware** to **Multiple** for multi-vsys deployments.
10. Under Function Type, select GoThrough for L2 and GoTo for L3.
11. Choose a connectivity mode for the APIC to device management connection. This setting defines how Cisco APIC connects to the firewall and to Panorama management interfaces. Choose the setting most appropriate for your environment. If the management interfaces if the firewall and Panorama have nit been added to an EPG, then you would typically choose **Out-Of-Band**. Out-Of-Band management is recommended.
12. Enter the login credentials for the firewall.



STEP 2 | Configure device 1 (the firewall).

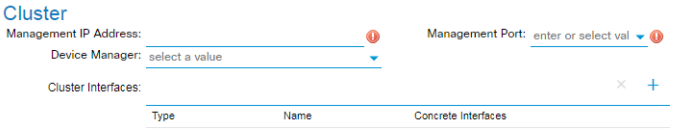
1. Enter the firewall management IP address and select HTTPS as the management port.
2. (VM-Series only) Under VM, select the VM-Series firewall you deployed. All virtual machines connected to the ACI fabric are listed here.
3. (Physical firewall only) Select a Chassis. This directs the firewall to create a new vsys and apply the configuration from the APIC there. Without a chassis select, APIC applies its network configuration to vsys1 and potentially overrides any configuration that already exists on vsys1.
4. Click the plues (+) icon under Device Interfaces to add your interfaces.

   For the VM-Series firewall, select ethernet 1/1 as the first data port and Network adapter 2 as the vNIC. vNIC network adapter 1 is reserved for the firewall management port.
5. For physical firewalls, in addition to select the ethernet port, you must also specify a path. The path is the physical port on a leaf switch that the firewall is connected to. This mapping was determined when you created you ACI Fabric and deployed your firewall.



STEP 3 | Configure the cluster. A cluster is a group of up to two identically configure L4 to L7 devices. The firewall(s) within the cluster are called concrete devices.

1. Enter the Management IP Address. This is the same IP address as device 1.
2. Set the Management Port to HTTPS.
3. Set the Device Manager to Panorama.
4. Set the Cluster Interfaces. The cluster interfaces define which side of the firewall and which side is external.
    1. Set the Type of the first interface to consumer (typically external) and give it a **Name**.
    2. Set a Concrete Interface from the drop-down. You defined the interfaces on the list when you configured in the interfaces for device 1.
    3. Set the Type of the second interface to provider (typically internal) and give it a **Name**.
    4. Select a Concrete Interface from the drop-down.
5. Click **Next** to proceed to the Basic parameters tab.



STEP 4 | Configure basic parameters of the firewall. In a single, non-HA firewall deployment, only the Basic Parameters under Device Settings are required.

1. Expand the **Device Settings** folder.
2. Click **DNS Server (primary)** and enter a Name in the Name column and an IP address in the Value column.
3. Click **Update**.
4. Click **Firewall Hostname** and enter a hostname in the Value column. APIC automatically populates the Name column with **hostname**.
5. Click **Update**.
6. Click **Finish**.

The parameters under All Parameters are optional.

STEP 5 | Verify that your L4-L7 Device was deployed successfully.

1. Select **Tenants** > **<your-tenant>** > **L4-L7 Services** > **L4-L7 Devices** and select the cluster you created.
2. Under Configuration State, the Device State proceeds through several states including **init**, **verificationPending**, **auditPending**, and finally **stable**.

   If the Device State does not reach stable state or shows any state not listed above, select **Faults** to determine the problem and follow the presented directions to resolve the problem.

Create and Deploy a Service Graph Template

After creating Panorama and your firewall, you must create a service graph template. A service graph defines the service that the L4-L7 device (the firewall) provides. Complete the following procedure to create and apply a service graph.

STEP 1 | Create a Service Graph Template.

1. Select **Tenants** > **<your-tenant>** > **L4-L7 Services** and right click on **L4-L7 Service Graph Templates**.
2. Click **Create L4-L7 Service Graph Template**.

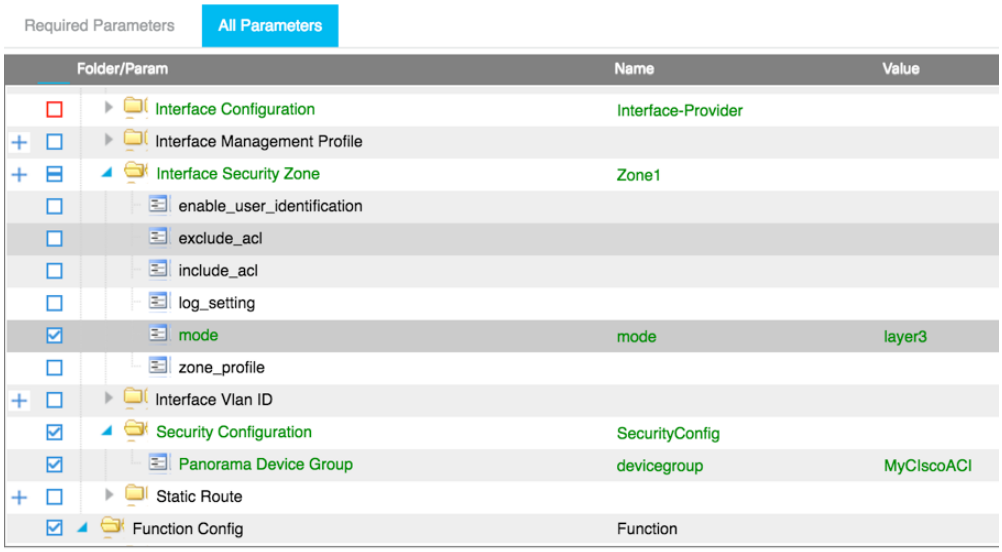
3. Enter a **Graph Name**.
4. Click and drag a device cluster from Device Cluster table and place it between the two EPGs to create a service node.
5. Set the firewall function to Routed (L3/GoTo) or Transparent (L2/GoThrough) depending on how you configured your device.
6. Select the profile that matches the device package and function you configured previously.
7. Click **Submit**.

STEP 2 | Apply the Service Graph Template.

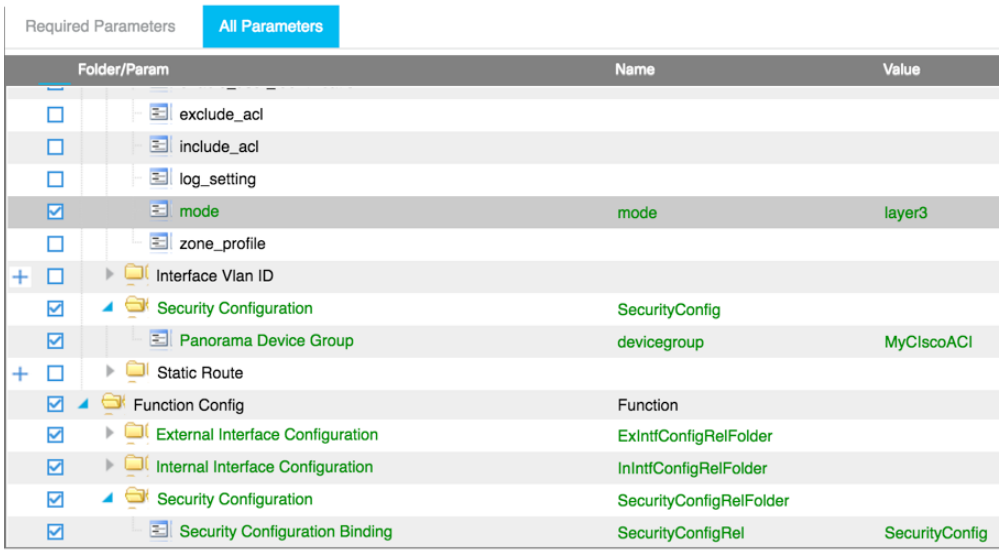
Parameters indicated with red box are required.

1. Select **Tenants** > **<your-tenant>** > **L4-L7 Services** and right click on the service graph template you created above.
2. Click **Apply L4-L7 Service Graph Template**.
3. Select a consumer EPG from the Consumer EPG/External Network drop-down.
4. Select a provider EPG from the Provider EPG/Internal Network drop-down.
5. Enter a **Contract Name**.
6. Click **Next**.
7. Click **Next** again on Step 2 of the wizard.
8. Click on **All Parameters**. This displays all the parameters that APIC will send to the firewall.
9. Create two zones.
    1. Click the plus (+) icon next to Interface Security Zone.
    2. Enter a **Name** for the zone.
    3. Set the **Mode** to Layer 2 or Layer 3
    4. Repeat these steps for the second zone.
10. Configure two data interfaces for the firewall.
    1. Expand **Interface Configuration**.
    2. Select and expand **Layer 2 Interface** or **Layer 3 Interface** based on your deployment.
    3. Enter the interface's IP address with subnet mask.
    4. Click **Security Zone** and specify one the security zones you created previously.
    5. Repeat these steps for the second interface.
11. Create a Panorama device.
    1. Expand **Security Configuration**.
    2. Enter a **Name** for the device group.
    3. Select **Function Config** > **Security Configuration**.
    4. In Security Configuration Binding, set the **SecurityConfigRel** value to **SecurityConfig**.
12. Click Finish. The APIC is now deploying the configuration to the firewall and Panorama. Use Panorama or the firewall web UI to verify the deployment of the network interface configuration and device group configuration.

    The device is now inserted in the network, configured, and ready to pass traffic.



RED indicators parameters needed to be updated and GREEN indicates parameters will be summitted to the provider EPG.



RED indicators parameters needed to be updated and GREEN indicates parameters will be summitted to the provider EPG.

Bootstrap the VM-Series Firewall

Bootstrapping allows you to create a repeatable and streamlined process of deploying new VM-Series firewalls on your network because it allows you to create a package with the model configuration for your network and then use that package to deploy VM-Series firewalls anywhere. You can bootstrap the VM-Series firewall off an external device (such as a virtual disk, a virtual CD-ROM or an AWS S3 bucket) to complete the process of configuring and licensing the VM-Series firewall. You can either bootstrap the firewall with basic initial configuration and licenses so that the firewall can register with Panorama and then retrieve its full configuration from Panorama, or you can bootstrap the complete configuration so that the firewall is fully configured on boot up.

VM-Series Firewall Bootstrap Workflow

After you familiarize yourself with the Bootstrap Package and assess whether you will want to fully configure the firewall or use Panorama to manage the bootstrapped firewall, use the following workflow to bootstrap your VM-Series firewall.

- For security reasons, you can only bootstrap a firewall when it is in factory default state. If you want to bootstrap a VM-Series firewall that has been previously configured, Reset the Firewall to Factory Default Settings.
- Generate the VM Auth Key on Panorama, if you want to use Panorama to manage the VM-Series firewalls being bootstrapped. You must include this key in the basic configuration (init-cfg.txt) file, when you prepare the bootstrap package.
- Prepare the Licenses for Bootstrapping.
- Create the init-cfg.txt File and optionally Create the bootstrap.xml File if you are not using Panorama to manage the firewall configuration.
- Prepare the Bootstrap Package.
- Place the bootstrap package in the format required by your hypervisor and bootstrap the VM-Series firewall.
  - Bootstrap the VM-Series Firewall on ESXi
  - Bootstrap the VM-Series Firewall on Hyper-V
  - Bootstrap the VM-Series Firewall on KVM
  - Bootstrap the VM-Series Firewall in AWS
  - Bootstrap the VM-Series Firewall in Azure
- Verify Bootstrap Completion.

Bootstrap Package

The bootstrap process is initiated only on first boot when the firewall is in a factory default state. When you attach the virtual disk, virtual CD-ROM, or AWS S3 bucket to the firewall, the firewall scans for a bootstrap package and, if one exists, the firewall uses the settings defined in the bootstrap package. If you have included a Panorama server IP address in the file, the firewall connects with Panorama. If the firewall has Internet connectivity, it contacts the licensing server to update the UUID and obtain the license keys and subscriptions. The firewall is then added as an asset in the Palo Alto Networks Support Portal. If the firewall does not have Internet connectivity, it either uses the license keys you included in the bootstrap package or it connects to Panorama, which retrieves the appropriate licenses and deploys them to the managed firewalls.

The bootstrap package that you create must include the following four folders, even if empty:

- **/config folder**—Contains the configuration files. The folder can hold two files: init-cfg.txt and the bootstrap.xml. For details see Bootstrap Configuration Files.

  If you intend to pre-register VM-Series firewalls with Panorama with bootstrapping, you must generate a VM auth key on Panorama and include the generated key in the init-cfg file. See Generate the VM Auth Key on Panorama.
- **/license folder**—Contains the license keys or auth codes for the licenses and subscriptions that you intend to activate on the firewalls. If the firewall does not have Internet connectivity, you must either manually obtain the license keys from the Palo Alto Networks Support portal or use the Licensing API to obtain the keys and then save each key in this folder. For details, see Prepare the Licenses for Bootstrapping.

  You must include an auth code bundle instead of individual auth codes so that the firewall or orchestration service 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.
- **/software folder**—Contains the software images required to upgrade a newly provisioned VM-Series firewall to the desired PAN-OS version for your network. You must include all intermediate software versions between the Open Virtualization Format (OVF) version and the final PAN-OS software version to which you want to upgrade the VM-Series firewall.
- **/content folder**—Contains the application and threat updates, WildFire updates, and the BrightCloud URL filtering database for the valid subscriptions on the VM-Series firewall. You must include the minimum content versions required for the desired PAN-OS version, without the minimum required content version associated with the PAN-OS version, the VM-Series firewall cannot complete the software upgrade.

The file type used to deliver the bootstrap package to the VM-Series firewall varies based on your hypervisor. Use the table below to determine the file type your hypervisor supports.

External Device for Bootstrapping (Bootstrap Package Format)	ESXi	KVM	Hyper-V	AWS	Azure	KVM in OpenStack
CD-ROM (ISO image)	Yes	Yes	Yes	—	—	—
Virtual Hard Disk (vhd)	—	—	—	—	Yes	—
S3 Bucket (ISO image)	—	—	—	Yes	—	—

External Device for Bootstrapping (Bootstrap Package Format)	ESXi	KVM	Hyper-V	AWS	Azure	KVM in OpenStack
config-drive	—	—	—	—	—	Yes
Block Storage Device	Yes	Yes	Yes	—	—	—

Bootstrap Configuration Files

The bootstrap package must include the basic configuration contained in the init-cfg.txt file in the /config folder; the complete configuration (contained in bootstrap.xml file in the /config folder) is optional. When you include both files in the bootstrap package, the firewall merges the configurations of those files and, if any configuration settings overlap between the two files, the firewall uses the setting defined in the init-cfg.txt file.

- Basic Configuration—The init-cfg.txt file is a text file that contains basic initial configuration information. You can name this file generically as init-cfg.txt, or you can prepend the UUID or Serial number of each firewall to the filename to be more specific (for example: 0008C100105-init-cfg.txt). This file must include basic information for configuring the management interface on the firewall, such as the IP address type (static or DHCP), IP address (IPv4 only or both IPv4 and IPv6), netmask, and default gateway. The DNS server IP address, Panorama IP address and device group and template parameters are optional. When the firewall boots, it searches for a text file that matches its UUID or serial number and, if none is found, it searches using the generic filename. For a sample file, see Create the init-cfg.txt File.

  For the VM-Series firewalls that you want to manage using Panorama, you must generate a VM auth key on Panorama and include the key in the init-cfg.txt file. For more information, see Generate the VM Auth Key on Panorama.
- Complete Configuration—The bootstrap.xml file allows you to fully configure the firewall. The bootstrap.xml file is optional and is only required if you are not using Panorama for centrally managing your firewall. You can either define this manually or export the running configuration from an existing firewall and save the file as bootstrap.xml. If you include the bootstrap.xml file, make sure to export the XML file from a firewall of the same platform or hypervisor. If you provide the init-cfg.txt file and the bootstrap.xml file, the firewall merges the files into a running configuration as part of the bootstrap process and, if any settings overlap, the firewall will use the setting from the basic configuration file. See Create the bootstrap.xml File.

Generate the VM Auth Key on Panorama

If you want to use Panorama to manage the VM-Series firewalls that you are bootstrapping, you must generate a VM auth key on Panorama and include the key in the basic configuration (init-cfg.txt) file. The VM auth key allows Panorama to authenticate the newly bootstrapped VM-Series firewall. So, to manage the firewall using Panorama, you must include the IP address for Panorama and the VM auth key in the basic configuration file as well as the license auth codes in the /license folder of the bootstrap package. The firewall can then provide the IP address, serial number, and the VM auth key in its initial connection request to Panorama so that Panorama can verify the validity of the VM auth key and add the firewall as a managed device. If you provide a device group and template in the basic configuration file, Panorama will assign the firewall to the appropriate device group and template so that you can centrally configure and administer the firewall using Panorama.

The lifetime of the key can vary between 1 hour and 8760 hours (1 year). After the specified time, the key expires and Panorama will not register VM-Series firewalls without a valid auth-key in this connection request.

STEP 1 | Log in to the Panorama CLI or access the API:

- In the CLI, use the following operational command:

  ```
  request bootstrap vm-auth-key generate lifetime <1-8760>
  ```

  For example to generate a key that is valid for 24 hrs, enter the following:

  ```
  request bootstrap vm-auth-key generate lifetime 24
  VM auth key 755036225328715 generated. Expires at: 2015/12/29 12:03:52
  ```

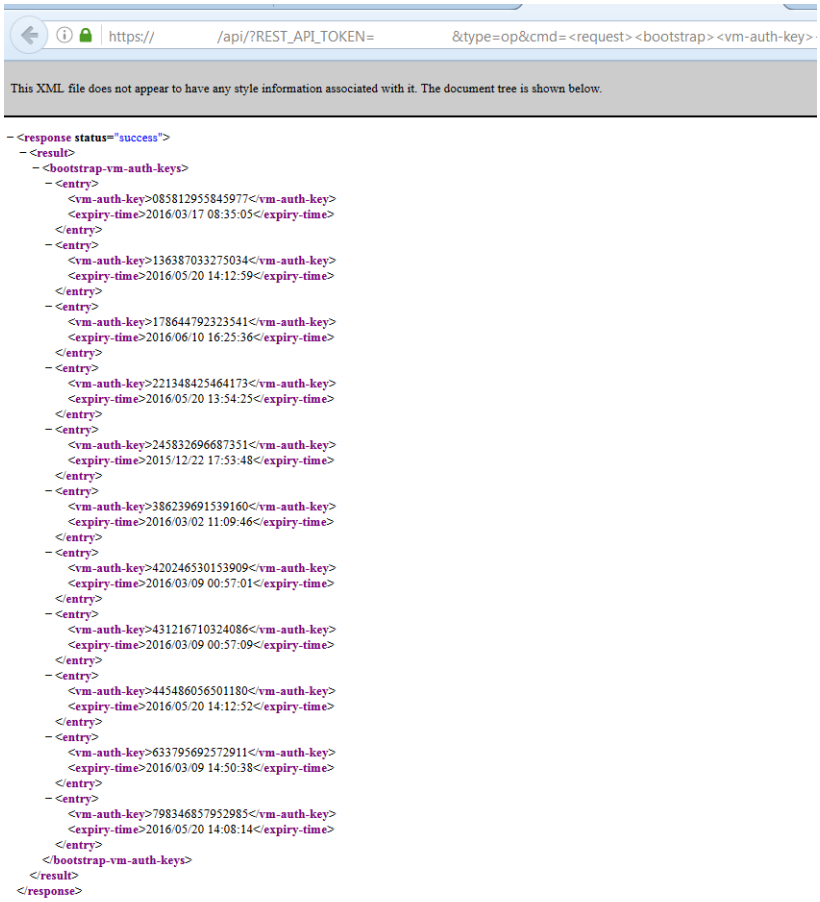
- In the API, use the following URL:

  ```
  https://<Panorama_IP_address>/api/?type=op&cmd=<request><bootstrap><vm-auth-key><generate><lifetime><number-of-hours></lifetime></generate></vm-auth-key></bootstrap></request>
  ```

  where the lifetime is the number of hours for which the VM auth key is valid.

STEP 2 | Verify the validity term of the VM auth key(s) you generated on Panorama. Make sure that the validity term allows enough time for the firewall(s) to register with Panorama.

```
https://<Panorama_IP_address>/api/?type=op&cmd=<request><bootstrap><vm-auth-key><show></show></vm-auth-key></bootstrap></request>
```



STEP 3 | Add the generated VM auth key to the basic configuration (init-cfg.txt) file. See Create the init-cfg.txt File

Create the init-cfg.txt File

The init-cfg.txt file is required to bootstrap the VM-Series firewall. It provides the basic information the firewall needs to connect to you network.

- init-cfg.txt File Components
- Sample init-cfg.txt File

Complete the following procedure to create the init-cfg.txt file.

STEP 1 | Create a new text file.

Use a text editor such as Notepad, EditPad, or other plain-text editors to create a text file.

STEP 2 | Add the basic network configuration for the management interface on the firewall.

If any of the required parameters are missing in the file, the firewall exits the bootstrap process and boots up using the default IP address, 192.168.1.1. You can view the system log on the firewall to detect the reason for the bootstrap failure. For errors, see Licensing API.

There are no spaces between the key and value in each field. Do not add spaces as they could cause failures during parsing on the mgmtsrvr side.

- To configure the management interface with a static IP address, you must specify the IP address, type of address, default gateway, and netmask. An IPv4 address is required, IPv6 address is optional. For syntax, see Sample init-cfg.txt File.
- To configure the management interface as a DHCP client, you must specify only the type of address. If you enable the DHCP client on the management interface, the firewall ignores the IP address, default gateway, netmask, IPv6 address, and IPv6 default gateway values defined in the file. For syntax, see Sample init-cfg.txt File.

When you enable DHCP on the management interface, the firewall takes the DHCP assigned IP address and is accessible over the network. You can view the DHCP assigned IP address on the General Information widget on the Dashboard or with the CLI command **`show system info`**. However, the default static management IP address 192.168.1.1 is retained in the running configuration (**`show config running`**) on the firewall. This static IP address ensures that you can always restore connectivity to your firewall, in the event you lose DHCP access to the firewall.

STEP 3 | Add the VM auth key to register a VM-Series firewall with Panorama.

To add a VM-Series firewall on Panorama, you must add the VM auth key that you generated on Panorama to the basic configuration (init-cfg.txt) file. For details on generating a key, see Generate the VM Auth Key on Panorama.

STEP 4 | Add details for accessing Panorama.

- Add IP addresses for the primary and secondary Panorama servers.
- Specify the template and the device group to which you want to assign the firewall.

Starting in 8.0.4, you can specify a template stack.

STEP 5 | (Optional) Include additional parameters for the firewall.

- Add IP address for the primary and secondary DNS servers.
- Add the hostname for the firewall.
- Enable either jumbo frames or multiple-virtual systems (or both)
- Enable swapping of the management interface (mgmt) and the dataplane interface (ethernet 1/1) on the VM-Series firewall in AWS. For more information on changing the management interface, see Management Interface Mapping for Use with Amazon ELB.
- Enable or disable DPDK.

init-cfg.txt File Components

The following table describes the fields in the init-cfg.txt file. The type, ip-address, default-gateway, and netmask are required.

Field	Description
type=	Type of management IP address: static or dhcp-client. This field is required.
ip-address=	IPv4 address. This field is ignored if the type is dhcp-client. If the type is static, an IPv4 address is required; the ipv6-address field is optional and can be included. You cannot specify the management IP address and netmask configuration for the VM-Series firewall in AWS and Azure. If defined, the firewall ignores the values you specify.
default-gateway=	IPv4 default gateway for the management interface. This field is ignored if the type is dhcp-client. If the type is static, and ip-address is used, this field is required.
netmask=	IPv4 netmask. This field is ignored if the type is dhcp-client. If the type is static, and ip-address is used, this field is required.
ipv6-address=	(Optional) IPv6 address and /prefix length of the management interface. This field is ignored if the type is dhcp-client. If the type is static, this field can be specified along with the ip-address field, which is required.
ipv6-default-gateway=	IPv6 default gateway for the management interface. This field is ignored if the type is dhcp-client. If the type is static and ipv6-address is used, this field is required.
hostname=	Host name for the firewall.
panorama-server=	IPv4 or IPv6 address of the primary Panorama server. This field is not required but recommended for centrally managing your firewalls.
panorama-server-2=	IPv4 or IPv6 address of the secondary Panorama server. This field is not required but recommended.
tplname=	Panorama template name. If you add a Panorama server IP address, as a best practice create a template on Panorama and enter the template name in this field so that you can centrally manage and push configuration settings to the firewall.

Field	Description
	Starting in 8.0.4, you can specify a template stack in this field.
dgname=	Panorama device group name. If you add a Panorama server IP address, as a best practice create a device group on Panorama and enter the device group name in this field so that you can group the firewalls logically and push policy rules to the firewall.
dns-primary=	IPv4 or IPv6 address of the primary DNS server.
dns-secondary=	IPv4 or IPv6 address of the secondary DNS server.
vm-auth-key=	Virtual machine authentication key. (This field is ignored when bootstrapping hardware firewalls.)
op-command-modes=	The following values are allowed: multi-vsys, jumbo-frame, mgmt-interface-swap. If you enter multiple values, use a space or a comma to separate the entries. • multi-vsys—(Hardware-based firewalls only) Enables multiple virtual systems. • jumbo frames—Enables the default MTU size for all Layer 3 interfaces to be set at 9192 bytes. • mgmt-interface-swap—(VM-Series firewall in AWS only) Allows you to swap the management interface (MGT) with the dataplane interface (ethernet 1/1) when deploying the firewall. For details, see Management Interface Mapping for Use with Amazon ELB.
dhcp-send-hostname=	The value of yes or no comes from the DHCP server. If yes, the firewall will send its hostname to the DHCP server. This field is relevant only if type is dhcp-client.
dhcp-send-client-id=	The value of yes or no comes from the DHCP server. If yes, the firewall will send its client ID to the DHCP server. This field is relevant only if type is dhcp-client.
dhcp-accept-server-hostname=	The value of yes or no comes from the DHCP server. If yes, the firewall will accept its hostname from the DHCP server. This field is relevant only if type is dhcp-client.
dhcp-accept-server-domain=	The value of yes or no comes from the DHCP server. If yes, the firewall will accept its DNS server from the DHCP server. This field is relevant only if type is dhcp-client.
op-cmd-dpdk-pkt-io= PAN-OS 8.0.5 and later	The value on or off allows you to enable or disable Data Plane Development Kit (DPDK) in environments where the firewall supports DPDK. DPDK allows the host to process packets faster by bypassing the Linux kernel; interactions with the NIC are performed using drivers and the DPDK libraries.

Sample init-cfg.txt File

The following sample basic configuration (init-cfg.txt) files shows all the parameters that are supported in the file; required parameters are in bold.

Sample init-cfg.txt file (Static IP Address)	Sample init-cfg.txt file (DHCP Client)
type=static	**type=dhcp-client**
ip-address=10.5.107.19	ip-address=
default-gateway=10.5.107.1	default-gateway=
netmask=255.255.255.0	netmask=
ipv6-address=2001:400:f00::1/64	ipv6-address=
ipv6-default-gateway=2001:400:f00::2*	ipv6-default-gateway=
hostname=Ca-FW-DC1	hostname=Ca-FW-DC1
vm-auth-key=755036225328715	vm-auth-key=755036225328715
panorama-server=10.5.107.20	panorama-server=10.5.107.20
panorama-server-2=10.5.107.21	panorama-server-2=10.5.107.21
tplname=FINANCE_TG4	tplname=FINANCE_TG4
dgname=finance_dg dns-primary=10.5.6.6	dgname=finance_dg
dns-secondary=10.5.6.7	dns-primary=10.5.6.6
op-command-modes=jumbo-frame, mgmt-interface-swap**	dns-secondary=10.5.6.7
op-cmd-dpdk-pkt-io=***	op-command-modes=jumbo-frame, mgmt-interface-swap**
dhcp-send-hostname=no	op-cmd-dpdk-pkt-io=***
dhcp-send-client-id=no	dhcp-send-hostname=yes
dhcp-accept-server-hostname=no	dhcp-send-client-id=yes
dhcp-accept-server-domain=no	dhcp-accept-server-hostname=yes
	dhcp-accept-server-domain=yes

You cannot specify the management IP address and netmask configuration for the VM-Series firewall in AWS. If defined, the firewall ignores the values you specify because AWS uses a back-end metadata file to assign the management IP address and netmask.

**The IPv6 default gateway is required if you include an IPv6 address.*

***The `mgmt-interface-swap` operational command pertains only to a VM-Series firewall in AWS.*

****The `op-cmd-dpdk-pkt-io=off` is for disabling DPDK on the VM-Series firewall on ESXi and KVM, DPDK is enabled by default.This parameter is supported in PAN-OS 8.0.5 and later.*

Create the bootstrap.xml File

Use these instructions to create the optional bootstrap.xml file.

STEP 1 | Export a configuration from a firewall.

1. Select **Device** > **Setup** > **Operations**.
2. Select the configuration file you want to export.
   - To export the running configuration, in the Configuration Management section, **Export named configuration snapshot** and select **running config.xml** from the drop-down.
   - To export a previous version of a firewall configuration, in the Configuration Management section, **Export configuration version** and select the appropriate configuration version in the drop-down.

STEP 2 | Rename the configuration file as bootstrap.xml.

1. Rename the file as bootstrap.xml.

   For the bootstrap process to be successful, the filename must be an exact (case-sensitive) match.
2. Save the bootstrap.xml file in the same location as the init-cfg.txt file.

Prepare the Licenses for Bootstrapping

To license the firewall during the bootstrapping process, you must purchase the auth codes and register the licenses and subscriptions on the Palo Alto Networks Support portal before you begin bootstrapping.

For the VM-Series firewalls running BYOL (not applicable for usage-based licensing—PAYG), you must have an auth code bundle that includes the capacity auth code, support subscription, and any other subscriptions you require. The process of preparing the licenses for bootstrapping depends on whether the firewall has internet access when bootstrapping:

- Direct Internet access—The firewall is connected directly to the Internet.
- Indirect Internet access—The firewall is managed by Panorama, which has direct Internet access and the ability to fetch the license keys on behalf of the firewall.
- No Internet access—The firewall uses an orchestration service or a custom script to fetch the license keys on behalf of the firewall.

- For VM-Series firewalls with Internet access.

  Enter the auth code in the /license folder when you Prepare the Bootstrap Package.

- For VM-Series firewalls with indirect Internet access.
  1. Register the auth code on the Palo Alto Networks Support portal.
     1. Go to support.paloaltonetworks.com, log in, and select **Assets** > **Register New Device** > **Register device using Serial Number or Authorization Code**.
     2. Follow the steps to Register the VM-Series Firewall.
     3. Click **Submit**.
  2. Activate the auth codes on the Palo Alto Networks Support portal to generate license keys.
     1. Go to support.paloaltonetworks.com, log in, and select the **Assets** tab.
     2. For each S/N, click the **Action** link.
     3. Select the **Activate Auth-Code** button.
     4. Enter the **Authorization code**, click **Agree**, and **Submit**.
     5. Download the license keys and save it to a local folder.
     6. Continue to Prepare the Bootstrap Package; you must add the license keys that you downloaded to the `\license` folder in the bootstrap package.

- For a custom script or an orchestration service that can access the Internet on behalf of firewalls.

  The script or service must fetch the CPU ID and the UUID from the hypervisor on which the firewall is deployed and access the Palo Alto Networks Support portal with CPU ID, UUID, API key and the auth code to obtain the required keys. See Licensing API.

Prepare the Bootstrap Package

Use the following procedure to prepare the bootstrap package.

STEP 1 | Create the top-level directory structure for the bootstrap package.

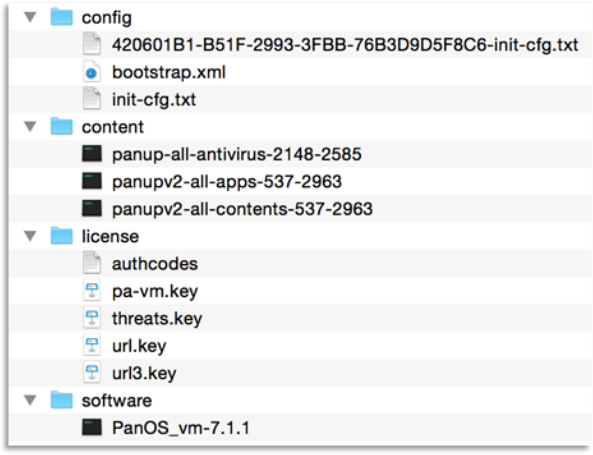
On your local client or laptop, create the following folders:

```
/config
/license
/software
/content
```

You can leave a folder empty, but you must have all four folders.

STEP 2 | Add content within each folder.

For an overview of the process, see Bootstrap Package. For details on the files in the /config folder, see Bootstrap Configuration Files.




```
/config
0008C100105-init-cfg.txt
0008C100107-init-cfg.txt
bootstrap.xml

/content
panupv2-all-contents-488-2590
panup-all-antivirus-1494-1969
panup-all-wildfire-54746-61460

/software
PanOS_vm-7.1.1
PanOS_vm-7.1.4

/license
```

If you save the keys to this folder, you can use a file naming convention that works for you but keep the .key extension in the filename.

```
0001A100105-authcodes
0001A100110-url3.key
0001A100110-threats.key
0001A100110-url3-wildfire.key
```

Use an auth code bundle instead of individual auth codes so that the firewall or orchestration service 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 3 | Create the bootstrap package.

For VM-Series firewalls, create the image in the appropriate format for your hypervisor.

Bootstrap the VM-Series Firewall on ESXi

You can bootstrap the VM-Series firewall using an ISO image or a virtual hard disk.

- Bootstrap the VM-Series Firewall on ESXi with an ISO
- Bootstrap the VM-Series Firewall on ESXi with a Block Storage Device

Bootstrap the VM-Series Firewall on ESXi with an ISO

Use these instructions to bootstrap the VM-Series firewall on an ESXi server using an ISO.

STEP 1 | Create an ISO image and upload it to a Virtual Machine File System (VMFS) datastore or to a Network File System (NFS) volume.

1. Prepare the Bootstrap Package.
2. Create an ISO image. The tool you use to create the image varies based on your client operating system.
3. Upload the ISO image to a VMFS datastore or to an NFS volume that is accessible to the ESX/ESXI host.

STEP 2 | Deploy the firewall.

1. Provision the VM-Series Firewall on an ESXi Server.

   By default, the firewall is deployed with two network interfaces— one for management traffic and one data traffic. Make sure that the first ethernet interface on the firewall, which is its management interface, is connected to the virtual switch port-group assigned for device management.
2. Do not power on the firewall.

STEP 3 | Attach the bootstrap image to the firewall.

1. Select the VM-Series firewall from the **Inventory** list.
2. Click **Edit Settings** and select **Virtual Hardware**.
3. Select **Datastore iso file** in the **CD DVD drive** drop-down, and **browse** for the ISO image.
4. Power on the firewall. The firewall will begin with the bootstrapping process, which will take several minutes. The status messages on the success or failure of the process will display on the console.
5. Verify Bootstrap Completion.

Bootstrap the VM-Series Firewall on ESXi with a Block Storage Device

Use these instructions to bootstrap the VM-Series firewall on an ESXi server using a block storage device.

STEP 1 | Create the bootstrap package and the virtual hard disk.

1. Create the bootstrap package.
2. Deploy a Linux virtual machine.
3. On the Linux machine, Prepare the Bootstrap Package. You can leave the folder empty, but you must have all four folders.
4. Attach a new data disk less than 39 GB to the Linux virtual machine.
5. Partition the disk and format the file system as ext3.
6. Make a directory for the new file system and mount the disk to the Linux virtual machine.
7. Copy the contents of your bootstrap package to the disk.
8. Unmount the disk.

9. Detach the disk from the Linux virtual machine. Take note of the Disk File describing the bootstrap disk you created; it shows the datastore name and path to the disk. Additionally, do not check the Delete Files From Datastore check box; doing so deletes the disk.

STEP 2 | Deploy the firewall.

1. Provision the VM-Series Firewall on an ESXi Server.
2. Do not power on the firewall.

STEP 3 | Attach the bootstrap package to the firewall.

1. Select the VM-Series firewall from the Inventory list.
2. Click **Edit Settings** and select **Virtual Hardware**.
3. From the New Device drop-down, select **Existing Hard Disk**. Select the bootstrap disk according to the datastore and path noted previously.
4. Power on the firewall. The firewall will begin with the bootstrapping process, which will take several minutes. The status messages on the success or failure of the process will display on the console.
5. Verify Bootstrap Completion.

Bootstrap the VM-Series Firewall on Hyper-V

You can bootstrap the VM-Series firewall using an ISO image or a virtual hard disk.

- Bootstrap the VM-Series Firewall on Hyper-V with an ISO
- Bootstrap the VM-Series Firewall on Hyper-V with a Block Storage Device

Bootstrap the VM-Series Firewall on Hyper-V with an ISO

Use these instructions to bootstrap the VM-Series firewall on a Hyper-V server with an ISO.

STEP 1 | Create an ISO image.

1. Prepare the Bootstrap Package.
2. Create an ISO image. The tool you use to create the image varies based on your client operating system.
3. Upload the ISO image to a location accessible to the Hyper-V host.

STEP 2 | Deploy the firewall.

1. Provision the VM-Series Firewall on a Hyper-V host with Hyper-V Manager.

   By default, the firewall is deployed with two network interfaces— one for management traffic and one data traffic. Make sure that the first ethernet interface on the firewall, which is its management interface, is connected to the vSwitch assigned for device management.
2. Do not power on the firewall.

STEP 3 | Attach the bootstrap image to the firewall.

1. In Hyper-V Manager, select the VM-Series firewall from the **Virtual Machines** list.
2. Click **Settings** > **Hardware** > **IDE Controller** > **DVD Drive**.
3. Under Media, click the **Image file** radio button.
4. Click **Browse** and select your uploaded ISO image.
5. Click **Apply** and **Ok** to exit the virtual machine settings.
6. Power on the firewall. The firewall will begin with the bootstrapping process, which will take several minutes. The status messages on the success or failure of the process will display on the console.
7. Verify Bootstrap Completion.

Bootstrap the VM-Series Firewall on Hyper-V with a Block Storage Device

Use these instructions to bootstrap the VM-Series firewall on a Hyper-V server with a block storage device.

STEP 1 | Create the bootstrap package and the virtual hard disk.

1. Deploy a Linux virtual machine.
2. On the Linux machine, Prepare the Bootstrap Package. You can leave the folder empty, but you must have all four folders.
3. Attach a new data disk less than 39 GB to the Linux virtual machine.
   1. Power of the Linux virtual machine.
   2. In Hyper-V, select the Linux virtual machine from the Virtual Machines list.
   3. Select **Settings** > **Hardware** > **IDE Controller**.
   4. Select **Hard Drive** and click **Add**.
   5. Select **Virtual Hard Disk** and click **New**.

6. Follow the on-screen instructions to create a new VHD. Note the name and path of the new VHD.
7. Click **Apply** then **OK** to exit the virtual machine settings.
8. Power on the Linux virtual machine.

4. Connect to the CLI of the Linux virtual machine.
5. Partition the disk and format the file system as ext3.
6. Make a directory for the new file system and mount the disk to the Linux virtual machine.
7. Copy the contents of your bootstrap package to the disk.
8. Unmount the disk.
9. Detach the disk from the Linux virtual machine.
    1. Power of the Linux virtual machine.
    2. Select the Linux virtual machine from the Virtual Machines list.
    3. Select **Settings** > **Hardware** > **IDE Controller**.
    4. Select the VHD you created.
    5. Click **Remove**. This detaches the VHD but does not delete it.

STEP 2 | Deploy the firewall.

1. Provision the VM-Series Firewall on a Hyper-V host with Hyper-V Manager.
2. Do not power on the firewall.

STEP 3 | Attach the bootstrap disk image to the firewall.

1. Select the firewall from the Virtual Machines list.
2. Select **Settings** > **Hardware** > **IDE Controller**.
3. Select **Hard Drive** and click **Add**.
4. Select **Virtual Hard Disk** and click **Browse**.
5. Browse to the bootstrap VHD you created, select it, and click **Open**.
6. Click **Apply** and **OK** to exit the Virtual Machine settings.
7. Power on the firewall. The firewall will begin with the bootstrapping process, which will take several minutes. The status messages on the success or failure of the process will display on the console.
8. Verify Bootstrap Completion.

Bootstrap the VM-Series Firewall on KVM

You can bootstrap the VM-Series firewall on KVM using an ISO image or a virtual hard disk. Additionally, you can bootstrap the VM-Series firewall on KVM in an OpenStack environment using a config-drive.

- Bootstrap the VM-Series Firewall on KVM with an ISO
- Bootstrap the VM-Series Firewall on KVM With a Block Storage Device
- Bootstrap the VM-Series Firewall on KVM in OpenStack

Bootstrap the VM-Series Firewall on KVM with an ISO

Use these instructions to bootstrap the VM-Series firewall on a KVM server using an ISO.

STEP 1 | Create an ISO image.

1. Prepare the Bootstrap Package.
2. Create an ISO image. The tool you use to create the image varies based on your client operating system.
3. Upload the ISO image to a location accessible to the KVM host.

STEP 2 | Deploy the firewall.

1. Install the VM-Series Firewall on KVM.

   By default, the firewall is deployed with two network interfaces— one for management traffic and one data traffic. Make sure that the first ethernet interface on the firewall, which is its management interface, is connected to the virtual switch port-group assigned for device management.
2. Do not power on the firewall.

STEP 3 | Attach the bootstrap image to the firewall.

1. In virt-manager, double-click on the VM-Series firewall to open the console.
2. View the VM hardware details by navigating to **View** > **Details**.
3. Open the Add New Virtual Hardware menu by clicking **Add Hardware**.
4. Change the device type to IDE CDROM.
5. Click the **Select managed or other existing storage** radio button and click **Browse**. Locate the ISO image you created and click **Choose Volume**.
6. Click **Finish** to exit the Add New Virtual Hardware menu.
7. Power on the firewall by navigating to **Virtual Machine** > **Run**. The firewall will begin with the bootstrapping process, which will take several minutes. The status messages on the success or failure of the process will display on the console.
8. Verify Bootstrap Completion.

Bootstrap the VM-Series Firewall on KVM With a Block Storage Device

Use these instructions to bootstrap the VM-Series firewall on a KVM server with a block storage device.

STEP 1 | Create the bootstrap package and the virtual hard disk.

1. Create the bootstrap package.
2. Create a new disk image less than 39 GB in size and partition the disk and format the file system as ext3. The tools used to complete this process vary based on your client operating system.
3. Mount the disk image file and copy the prepared bootstrap package to the disk image files.

4. Copy the contents of your bootstrap package to the disk.
5. Unmount the disk image.
6. Upload the disk image file to a location accessible to the KVM host.

STEP 2 | Deploy the firewall.

1. Install the VM-Series Firewall on KVM.
2. Do not power on the firewall.

STEP 3 | Attach the bootstrap disk image to the firewall.

1. In virt-manager, double click on the VM-Series firewall to open the console.
2. View the VM hardware details be selecting **View** > **Details**.
3. Open the Add New Virtual Hardware menu by clicking **Add Hardware**.
4. Select **Storage** and the select **Select or create custom storage**.
5. Click the **Manage** button to open the **Choose Storage Volume** dialog, and select the disk image file that you previously created.
6. Click Choose Volume.
7. Ensure that the device type is Disk Device and do not change the Bus Type.
8. Click Finish.
9. Power on the firewall. The firewall will begin with the bootstrapping process, which will take several minutes. The status messages on the success or failure of the process will display on the console.
10. Verify Bootstrap Completion.

Bootstrap the VM-Series Firewall on KVM in OpenStack

You can bootstrap the KVM edition of the VM-Series firewall in an OpenStack environment with:

- Red Hat OpenStack Platform 5 or OpenStack Platform 7 running on Red Hat Enterprise Linux 7.2 or Mirantis 7.0 running on Ubuntu 14.04.
- Support for OpenStack CLI only; the UI is not supported.
- Minimum PAN-OS version is PAN-OS 7.1.4.
- ISO9660 or VFAT configuration drive formats.

The KVM edition of the VM-Series firewall in an OpenStack environment reads the bootstrap package from a config-drive that attaches to the instance when it boots. The config-drive is limited to a maximum size of 64MB. Therefore, only /config and /license of the Bootstrap Package can have content; /software and /content must remain empty.

PAN-OS supports two methods for passing the bootstrap package to the config-drive:

- file: passes the bootstrap package as cleartext files
- user-data: passes the bootstrap package in a compressed tar ball (.tgz file) with base64 encoding

To use the user-data method, ensure that your version of OpenStack Platform 5 (Icehouse-based) has been patched with a fix for this Icehouse issue. Without the patch, use of a tar ball with the user-data method causes the nova boot command to fail.

You can use both methods concurrently in deployments where some files in the bootstrap package are static across all VM-Series instances while other files are unique to each firewall. If you include files using both methods, the compute node unpacks the tar ball first and any files passed by the `--file` command overwrite duplicate files from the tar ball.

STEP 1 | Place the bootstrap package in your OpenStack environment.

When using macOS to create your tar ball, you must create the tar ball using a GNU version of tar. The BSD version of tar that is built in to macOS generates an invlaid tar ball and cannot be read by the VM-Series firewall.

1. Prepare the Bootstrap Package.
2. Access the OpenStack CLI.
3. Save the bootstrap package and PAN-OS image in a location accessible by the OpenStack controller node.
4. If using the **--user-data** method to pass the bootstrap package to the config-drive, you can use the following command to create the tar ball:

```
tar -cvzf <file-name>.tgz config/
license software content
```

5. If using the **--user-data** method, encode the tar ball (.tgz file) with base64.

```
base64 -i <in-file> -o <outfile>
```

STEP 2 | Retrieve the network UUID(s).

To attach a NIC to the VM-Series firewall instance with the --nic net-id= argument, you need the network UUID. You can retrieve the network UUID through the OpenStack CLI by using the following command:

```
neutron net-list
```

STEP 3 | Deploy the firewall.

There are three methods for populating a config-drive with the bootstrap package and attaching it to the host VM. Complete the command sequence of your choice on the OpenStack controller node. See the following table for descriptions of the arguments required for bootstrapping.

- --user-data

```
nova
boot --config-drive true --image <pan-os-image-file-name> --
flavor <flavor> --user-data <tgz
location and filename> --security-groups <security-group> --nic
net-id=<mgmt nic net-id> --nic net-id=<eth1
nic net-id> --nic net-id=<eth2 nic net-id>
<vm-series name>
```

- --file

```
nova boot --config-drive
true --image <pan-os-image-file-name> --flavor <flavor> --file /license/
authcodes=<source-path> --file /config/init-cfg.txt=<source-path> --
security-groups <security-group> --nic
net-id=<mgmt nic net-id> --nic net-id=<eth1
nic net-id> --nic net-id=<eth2 nic net-id>
<vm-series name>
```

- --user-data and --file

```
nova
boot --config-drive true --image <pan-os-image-file-name> --
flavor <flavor> --file /config/init-cfg.txt=<source-path>--user-data <tgz
location and filename> --security-groups <security-group> --nic
net-id=<mgmt nic net-id> --nic net-id=<eth1
nic net-id> --nic net-id=<eth2 nic net-id>
<vm-series name>
```

STEP 4 | Verify Bootstrap Completion.

The nova boot command and the following arguments are required to Bootstrap the VM-Series Firewall on KVM in OpenStack.

Arguments	Description
nova boot	Used to boot a new compute instance.
--config-drive true	Enables the config-drive.
--image	Specifies the PAN-OS image file. Only the image name is required. This base image file is required to launch the VM-Series firewall. You can view a list of images available in your OpenStack environment with the following command: `nova image-list`
--flavor	The VM instance type. Ensure that you select a flavor that provides the hardware resources required for your VM-Series firewall. You can view a list of available flavors and their hardware resources with the following command: `nova flavor-list` See VM-Series on KVM— Requirements and Prerequisites for minimum hardware resources required by the KVM VM-Series firewall.
--user-data	Used to pass the tar ball containing the bootstrap package to the config-drive.

--file	Used to pass the init-cfg.txt file and license file as cleartext files to the config-drive.
	For the bootstrap process to succeed, you must include the /config/init-cfg.txt= argument and either the /license/license.key or /license/authcodes argument. Optionally, bootstrap.xml files are also supported.
	`--file /config/init-cfg.txt=`
	`--file /config/bootstrap.xml=`

Arguments	Description

	`--file /license/license.key=`
	`--file /license/authcodes=`
	
	The Server Personality defines the maximum number of files that can be passed using the **`--file`** command. Use the **`nova absolute-limits`** command to view the limit. In the example below, the Personality limit is five. Therefore, the maximum number of files is limited to five.
	
	`nova absolute-limits`
	`+--------------------+-------+--------+`
	`| Name | Used | Max |`
	`+--------------------+-------+--------+`
	`| Cores | 18 | 240 |`
	`| FloatingIps | 0 | 10 |`
	`| ImageMeta | - | 128 |`
	`| Instances | 12 | 1000 |`
	`| Keypairs | - | 100 |`
	`| Personality | - | 5 |`
	`| Personality Size | - | 65536 |`
	`| RAM | 32256 | 393216 |`
	`| SecurityGroupRules | - | 20 |`
	`| SecurityGroups | 1 | 10 |`
	`| Server Meta | - | 128 |`
	`| ServerGroupMembers | - | 10 |`
	`| ServerGroups | 0 | 10 |`
	`+--------------------+-------+--------+`
	
	Exceeding this limit generates an error message. If you need to pass more files than this limit allows, use the user-data method or the combined user-data and file method.

--nic net-id <network UUID>	Creates a NIC on the VM-Series firewall with the specified UUID. You should create at least two NICs: one for a management port and one for a data port.
--security-group	You can provide a comma-separated list of security groups to provide access to the VM-Series firewall. If you do not specify a security group, the VM is placed in the default security group.

Bootstrap the VM-Series Firewall on AWS

To perform bootstrapping, you must be familiar with AWS S3 and IAM permissions required for completing this process. For detailed instructions on creating policy, refer to the AWS documentation on Creating Customer Managed Polices.

The management interface of the VM-Series firewall must be able to access the S3 bucket to complete bootstrapping. You can either assign a public IP address or an elastic IP address to the management interface so that the S3 bucket can be accessed over the Internet. Or, create a AWS VPC endpoint in the same region as the S3 bucket, if you prefer to create a private connection between your VPC and the S3 bucket and do not want to enable internet access on the firewall management interface. For more information refer to the AWS documentation on setting up VPC endpoints.

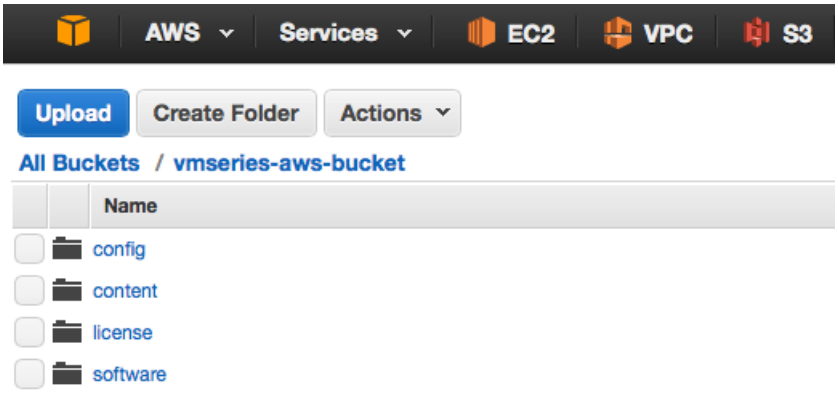
STEP 1 | On the AWS console, create an Amazon Simple Storage Service (S3) bucket at the root-level. The S3 bucket in this example, vmseries-aws-bucket is at the All Buckets root folder level. Bootstrap will fail if you nest the folder because you cannot specify a path to the location of the bootstrap files.

STEP 2 | Create an IAM role with inline policy to enable read access to the S3 bucket [ListBucket, GetObject]. For detailed instructions on creating an IAM role, defining which accounts or AWS services can assume the role, defining which API actions and resources the application can use upon assuming the role, refer to the AWS documentation on IAM Roles for Amazon EC2. When launching the VM-Series firewall, you must attach this role to enable access to the S3 bucket and the objects included in the bucket for bootstrapping successfully.

```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": ["s3:ListBucket"],
"Resource": ["arn:aws:s3:::<bucketname>"]
},
{
"Effect": "Allow",
"Action": [
"s3:GetObject"
],
"Resource": ["arn:aws:s3:::<bucketname>/*"]
}
]
}
```

STEP 3 | Create the folders within the S3 bucket.

- Create the top-level directory structure for the bootstrap package. Create the structure directly in this S3 bucket.



- Add content within each folder. You can leave a folder empty, but you must have all the four folders.

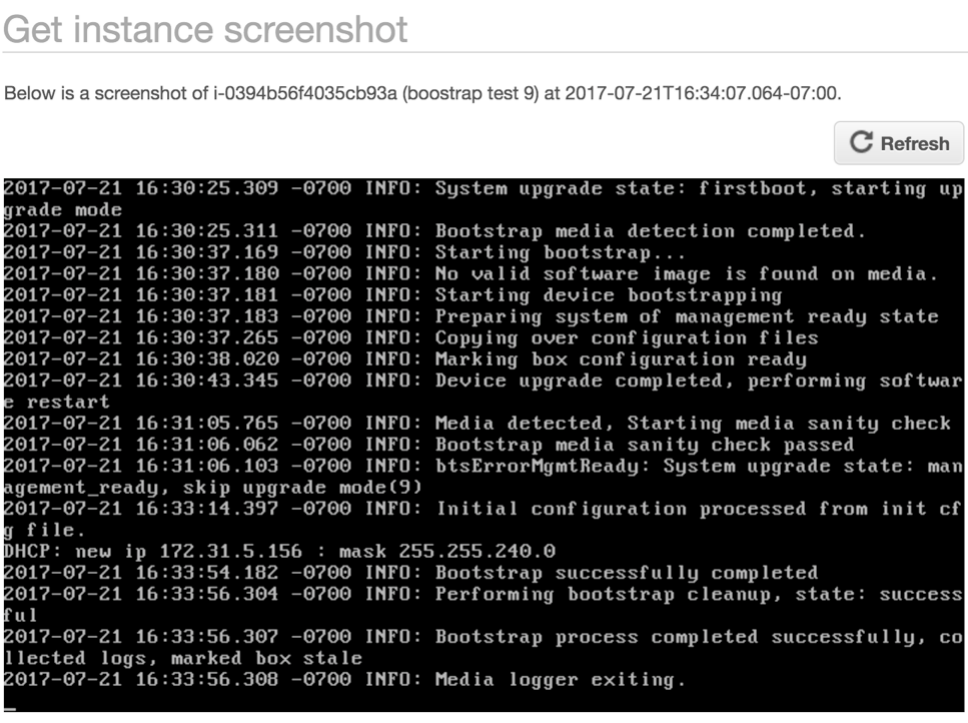
If you have enabled logging in Amazon S3, a Logs folder is automatically created in the S3 bucket. The Logs folder helps troubleshoot issues with access to the S3 bucket.

STEP 4 | Launch the VM-Series Firewall on AWS. When launching the firewall as an EC2 instance, attach the IAM role you created in step 2 and in the user data field (Advanced section), specify the following S3 keyvalue:

```
vmseries-bootstrap-aws-s3bucket=<bucketname>
```

STEP 5 | Verify Bootstrap Completion. Select the firewall instance on the AWS Management console and choose **Actions** > **Instance Settings** > **Get Instance Screenshot**.

- On successful bootstrap, you will see the following message.



- If the S3 bucket does not have the correct permissions or you do not have all four folders in the S3 bucket the following error message displays.

Bootstrap the VM-Series Firewall in Azure

To perform bootstrapping, you must be familiar with the process of creating a VHD and must know about storage accounts and containers in Azure, and how to attach the VHD to a virtual machine.

STEP 1 | Create the VHD. Use the Azure documentation for the commands required to complete the process of creating a VHD.

1. On the Azure portal, deploy a Linux virtual machine.
2. On the Linux virtual machine, **Add a data disk** ranging between 1 to 39 GB. Make sure to save the disk to the same storage account that you will use for the VM-Series firewall.
3. Connect to the console or CLI of the Linux virtual machine.
4. Partition the disk and format the file system as ext3.
5. Create the top-level directory structure for the bootstrap package. and Add content within each folder. You can leave a folder empty, but you must have all the four folders.
6. Copy the contents of the bootstrap package you created above to the disk.
7. Unmount the disk.
8. Detach the disk from the Azure portal. The disk is stored as a page blob.
9. Store the disk as a page blob within the same storage account that you will use for the VM-Series firewall.

STEP 2 | Customize the ARM template to point to the VHD so that the firewall can access the disk on first boot. For example, you need to add the following object in the **`virtualMachine`** resource in the Template file:

```
"storageProfile": {                "imageReference": {
          "publisher": "[parameters('imagePublisher')]",
          "offer": "[parameters('imageOffer')]",
  "sku": "[parameters('imageSku')]",                    "version":
 "latest"                },                 "dataDisks": [
         {                    "name": "datadisk1",
 "diskSizeGB": "[parameters('BootstrapUriSizeGB')]",
   "lun": 0,                   "vhd": {                        "uri":
 "[parameters('BootstrapUri')]"                  },
  "caching": "ReadOnly",                   "createOption": "Attach"
              }                ],                 "osDisk": {
            "name": "osdisk",                    "vhd": {
           "uri": "[concat('http://', parameters('storageAccountName'),
 '.blob.core.windows.net/vhds/', parameters('vmName'), '-',
 parameters('imageOffer'), '-', parameters('imageSku'), '.vhd')]"
          },                    "caching": "ReadWrite",
 "createOption": "FromImage"                }            },
```

STEP 3 | Verify Bootstrap Completion.

Verify Bootstrap Completion

You can see basic status logs on the console during the bootstrap and you can verify that the process is complete.

STEP 1 | If you included panorama-server, tplname, and dgname in your init-cfg.txt file, check Panorama managed devices, device group, and template name.

STEP 2 | Verify the general system settings and configuration. Access the web interface and select **Dashboard** > **Widgets** > **System** or use the CLI operational commands **`show system info`** and **`show config running`**.

STEP 3 | Verify the license installation. Select **Device** > **Licenses** or use the CLI operational command **`request license info`**.

STEP 4 | If you have Panorama configured, manage the content versions and software versions from Panorama. If you do not have Panorama configured, use the web interface to manage content versions and software versions.

Bootstrap Errors

If you receive an error message during the bootstrapping process, refer to the following table for details.

Error message (Severity)	Reasons
Boot image error (high)	• No external device was detected with the bootstrap package. Or • A critical error happened while booting from the image on the external device. The bootstrap process was aborted.
No bootstrap config file on external device (high)	The external device did not have the bootstrap configuration file.
Bad or no parameters for mandatory networking information in the bootstrap config file (high)	The networking parameters required for bootstrapping were either incorrect or missing. The error message lists the value—IP address, netmask, default gateway—that caused the bootstrap failure.
Failed to install license key for file <license-key-filename> (high)	The license key could not be applied. This error indicates that the license key used was invalid. The output includes the name of the license key that could not be applied.
Failed to install license key using authcode <authcode> (high)	The license auth code could not be applied. This error indicates that the license auth code used was invalid. The output includes the name of the authcode that could not be applied.
Failed content update commits (high)	The content updates were not successfully applied.
USB media prepared successfully using given bundle (informational)	The bootstrap image has been successfully complied on the USB flash device. <username>: Successfully prepared the USB using bundle <bundlename>
Successful bootstrap (informational)	The firewall was successfully provisioned with the bootstrap configuration file. The output includes the license keys installed and the filename of the bootstrap configuration. On the VM-Series firewalls only, the PAN-OS version and content update version are also displayed.

Read about the Bootstrap Package and how to Prepare the Bootstrap Package.