About this Guide

This guide describes how to set up and license the VM-Series firewall; it is intended for administrators who want to deploy the VM-Series firewall.

For more information, refer to the following sources:

- For information on the additional capabilities of and instructions for configuring the features on your firewall, refer to https://docs.paloaltonetworks.com.
- For access to the knowledge base, complete documentation set, discussion forums, and videos, refer to https://live.paloaltonetworks.com.
- For contacting support, for information on support programs, to manage your account or devices, or to open a support case, refer to https://www.paloaltonetworks.com/support/tabs/overview.html.
- For the most current PAN-OS 7.1 release notes, go to https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-release-notes.

To provide feedback on the documentation, please write to us at: documentation@paloaltonetworks.com.
Set up the VM-Series Firewall in Azure

VM-Series firewall on Azure brings the security features of Palo Alto Networks next generation firewall as a virtual machine in the Azure public cloud (starting with PAN-OS 7.1.0) and Azure Government Cloud Marketplace (starting with PAN-OS 7.1.1). 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 in Azure
▲ Deployments Supported in Azure
▲ Deploy the VM-Series Firewall in Azure (Solution Template)
▲ Deploy the VM-Series Firewall from the Azure China Marketplace (Solution Template)
▲ Use the ARM Template to Deploy the VM-Series Firewall
▲ Deploy the VM-Series and Azure Application Gateway Template
About the VM-Series Firewall in 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 in both the standard Azure public cloud and in the Azure Government Cloud environments. The VM-Series firewall in the Azure public marketplace supports the Bring Your Own License (BYOL) model and the hourly Pay-As-You-Go (PAYG) option in the usage-based licensing model. In the Azure Government Marketplace and Azure China, the VM-Series firewall is available in the bring your own license (BYOL) option only. To deploy the VM-Series on Azure Government, use the BYOL workflow outlined in the Deploy the VM-Series Firewall in Azure (Solution Template). Azure China has a slightly different workflow that is outlined in Deploy the VM-Series Firewall from the Azure China Marketplace (Solution Template).

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 Networking and VM-Series

The Azure VNets 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.

In 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 VNets 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 in Azure

You can deploy the VM-Series firewall in 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 in Azure (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 in Azure. The 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.

  If you want to use the Azure CLI to locate all the images available from Palo Alto Networks, you need the following details to complete the command (show vm-image list):
  - Publisher: paloaltonetworks
  - Offer: vmseries1
  - SKU: byol, bundle1, bundle2
  - Version: 7.1.1 or latest

To use the ARM templates, see Use the ARM Template to Deploy the VM-Series Firewall.

Minimum System Requirements for the VM-Series in 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 in Azure must meet the following requirements:

- **Azure VMs** of the following types: Standard_D3 (default), Standard_D3_v2, Standard_D4, Standard_D4_v2, Standard_A4.
- Four or eight CPU cores to deploy the firewall; the management plane only uses one CPU core and the additional cores are assigned to the dataplane.
- Up to four network interfaces (NICs). A primary interface is required for management access and up to three 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 three network interfaces. 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 in Azure supports Layer 3 interfaces only.
- Minimum of 4GB of memory for all models except the VM-1000-HV, which needs 5GB. Any additional memory will be used by the management plane only.
- Minimum of 40GB of virtual disk space. 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.

The VM-Series firewall in Azure does not support a high availability configuration; native VM Monitoring capabilities for virtual machines that are hosted in Azure is also not available.
Deployments Supported in Azure

Use the VM-Series firewall in Azure to secure your network users in the following scenarios:

- **Hybrid and VNet to VNet**—The VM-Series firewall in 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 in Azure (Solution Template) and configure the firewall and Azure for your deployment needs, or you can learn about the VM-Series Firewall Templates in 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 in Azure (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.

### Deploy the VM-Series Firewall in Azure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Set up an Azure account.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Create a Microsoft account.</td>
</tr>
<tr>
<td>2.</td>
<td>Log in to the Azure portal (<a href="https://portal.azure.com">https://portal.azure.com</a>) using your Microsoft account credentials.</td>
</tr>
<tr>
<td></td>
<td>If you are using a trial subscription, you may need to open a support request (<a href="#">Help + Support &gt; New Support Request</a>) to increase the quota of allocated VM cores.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Find the VM-Series solution template in the Azure Marketplace.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select <strong>Azure Marketplace &gt; Virtual Machines</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>Search for Palo Alto Networks. The offerings for the VM-Series firewall display. For the differences in the BYOL and PAYG models, see <strong>VM-Series Firewall in Amazon Web Services (AWS)</strong> and <strong>Azure Licenses</strong>.</td>
</tr>
<tr>
<td>3.</td>
<td>Select an offering and click <strong>Create</strong>.</td>
</tr>
</tbody>
</table>
Step 3  Deploy the firewall.

1. Configure basic settings for the firewall.
   a. Enter a **Username** for the firewall administrator.
   b. Enter a **Password** or copy and paste an **SSH public key** for securing administrative access to the firewall.
   c. Select your Azure **Subscription**.
   d. Create a new resource group for holding all the resources associated with the VM-Series firewall for this deployment.
      From the Azure Marketplace, 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.
   e. Select the Azure **Location**. This is the region in which you are deploying the firewall.

2. Configure storage and networking.
   a. Select an existing storage account or create a new one.
   b. 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.
   c. 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.
   d. 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.
   a. Use the default variable (new PublicIP) to assign a **Public IP address** to the management interface (eth0) of the firewall.
   b. 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.
   c. Enter a display name to identify the VM-Series firewall within the resource group.
   d. To select PAN-OS version, use the **VM-Series Version** drop-down.
   e. Select the Azure virtual machine tier and size to meet your needs. See Minimum System Requirements for the VM-Series in 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.
   a. Select **Dashboard >Resource Groups**, select the resource group.
   b. Select **All Settings > Deployments > Deployment History** for detailed status.
Deploy the VM-Series Firewall in Azure (Continued)

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.
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 in the parameters file. You will see a certificate warning; that is okay. Continue to the web page.
### Deploy the VM-Series Firewall in Azure (Continued)

#### 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.**

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**.
     The private IP address assigned in the ARM template will be automatically acquired.
   - 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.
   - 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 a NAT virtual machine, a 3rd party 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 in Azure

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 an 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.

---

**Deploy the VM-Series Firewall on Azure China**

**Step 1** Set up an Azure account.

1. Create a Microsoft account.
2. Log in to the Azure portal (https://portal.azure.cn) 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.

2. Select an offering and click **Immediate deployment of**.
Deploy the VM-Series Firewall from the Azure China Marketplace (Solution Template)

Set up the VM-Series Firewall in Azure

**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.
   - 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.
   - 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.**
   a. Enter the storage account name for an existing account or create a new one.
   b. Enter the name for the blob storage container to which the firewall vhd mage will be copied and saved.
   c. 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.
   d. Enter a **Username** for the firewall administrator.
   e. Enter a **Password** for securing administrative access to the firewall.
   f. Select the Azure virtual machine tier and size to meet your needs. See **Minimum System Requirements for the VM-Series in Azure**.
   g. Enter a **VmName**, which is a display name to identify the VM-Series firewall within the resource group.
   h. 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.
   i. 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.
   j. 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.**
   b. Select **Dashboard >Resource Groups**, select the resource group.
   c. 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).
   - On the **Config** tab, assign the interface to the default router.
   - **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.
<table>
<thead>
<tr>
<th>Step 8</th>
<th>Configure the firewall for your specific deployment.</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Gateway—Deploy a 3rd party load balancer in front of the UnTrust zone.</td>
<td></td>
</tr>
<tr>
<td>• Hybrid and Inter-VNet—Deploy an Azure VPN Gateway or a NAT virtual machine in front the UnTrust zone.</td>
<td></td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td>• GlobalProtect—Deploy a NAT virtual machine in front of the UnTrust zone.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Direct traffic to the VM-Series firewall.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. To ensure that the VM-Series firewall secures all traffic within the Azure resource group, configure static routes on the firewall.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>
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, 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.

**Deploying VM-Series Firewall using the ARM Template**

1. **Step 1** Download the ARM template from the GitHub repository.
   - Download and save the files to a local client: https://github.com/PaloAltoNetworks/azure

---

Copyright © 2007-2017 Palo Alto Networks
### Use the ARM Template to Deploy the VM-Series Firewall

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Create a Resource Group in Azure.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Log in to the Azure CLI using the command: <code>azure login</code> If you need help, refer to the Azure documentation on installing the CLI.</td>
</tr>
<tr>
<td>2.</td>
<td>Switch to Resource Manager mode using the command: <code>azure config mode arm</code></td>
</tr>
<tr>
<td>3.</td>
<td>Create a resource group.</td>
</tr>
</tbody>
</table>

### Step 3  Deploy the ARM template.

| 1.     | Open the Parameters File with a text editor and modify the values for your deployment: |
|        | `azure group create -v -n "<YourResourceGroupName>" -l "<YourAzureLocation>" -d "<GiveASmallDeploymentLabel>" -f azureDeploy.json -e azureDeploy.parameters.json` |
| 2.     | Deploy the template in the resource group you created. |
| 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.  |
| a.     | Select Dashboard > Resource Groups, select the resource group. |
| b.     | 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.
## Use the ARM Template to Deploy the VM-Series Firewall (Continued)

**Step 4** 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`):
   a. Route all outbound traffic through the UnTrust zone, ethernet1/1 to the Azure router at 192.168.1.1.
   b. 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.
   c. 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`).
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.

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

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 \textit{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
Deploy the VM-Series and Azure Application Gateway Template

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. 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.
### Deploy the Template to Azure

**Step 1** Deploy the template.

1. Access the template from [https://github.com/PaloAltoNetworks/azure-application-gateway](https://github.com/PaloAltoNetworks/azure-application-gateway)
2. Click **Deploy to Azure**.
3. Fill in the details for deploying the template. See [VM-Series and Azure Application Gateway Template Parameters](https://github.com/PaloAltoNetworks/azure-application-gateway#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.
   - Select **Dashboard > Resource Groups**, select the resource group.
   - Select **Overview** to review all the resources that have been deployed. The deployment status should display **Succeeded**.
   - 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.
### Deploy the Template to Azure

| 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.  
- **To 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. |
### VM-Series and Azure Application Gateway Template Parameters

The following table lists the required and optional parameters and the default values, if any.

<table>
<thead>
<tr>
<th><strong>Deploy the Template to Azure</strong></th>
<th><strong>To import the sample configuration file:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Download and save the Sample Configuration File to your local client.</td>
</tr>
<tr>
<td></td>
<td>2. Select Device &gt; Setup &gt; Operations, click Import named configuration snapshot, Browse to the sample configuration file that you have saved locally, and click OK.</td>
</tr>
<tr>
<td></td>
<td>3. Click Load named configuration snapshot, select the Name of the sample configuration file you just imported, and click OK.</td>
</tr>
<tr>
<td></td>
<td>4. Change the IP address of the address objects and the static route to match the IP address from the CIDR block you used.</td>
</tr>
<tr>
<td></td>
<td>5. Click Commit to overwrite the running configuration with the sample configuration you just imported. When you commit, the hostname and the administrator user account that you specified when deploying the template will be overwritten. You must create a new admin user account and delete the pandemo admin account that is provided in the template.</td>
</tr>
<tr>
<td></td>
<td>6. Create a new admin user account. Select Device &gt; Administrators and Add a new account.</td>
</tr>
<tr>
<td></td>
<td>7. Modify the Hostname in the General Settings widget in Device &gt; Setup &gt; Management.</td>
</tr>
<tr>
<td></td>
<td>8. Commit your changes, and log out.</td>
</tr>
<tr>
<td></td>
<td>9. Log in to the firewall using the credentials you created, and delete the pandemo admin account.</td>
</tr>
</tbody>
</table>

**Step 4** Log in and configure the other instance of the VM-Series firewall.  
See 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 firewall and view the Traffic logs generated on session start in Monitor > Logs > Traffic.
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource group</td>
<td>Create new or use existing (no default).</td>
</tr>
<tr>
<td>Subscription</td>
<td>The type of Azure subscription you will use to cover the cost of the resources deployed with the template.</td>
</tr>
<tr>
<td>Location</td>
<td>Select the Azure location to which you want to deploy the template (no default).</td>
</tr>
<tr>
<td><strong>Network Security Group</strong></td>
<td></td>
</tr>
<tr>
<td>Network Security Group Name</td>
<td>The network security group limits the source IP addresses from which the VM-Series firewalls and web servers can be accessed. Default: nsg-mgmt</td>
</tr>
<tr>
<td>Network Security Group Inbound Src IP</td>
<td>The source IP addresses that can log in to the management port of the VMs deployed by the template. Default value 0.0.0.0/0 means you can log into the firewall management port from any IP address.</td>
</tr>
<tr>
<td><strong>Storage Account</strong></td>
<td></td>
</tr>
<tr>
<td>Storage Account Name</td>
<td>Create new or enter the name of an existing Storage Account (no default). The name must be globally unique.</td>
</tr>
<tr>
<td>Storage Account Type</td>
<td>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.</td>
</tr>
<tr>
<td><strong>VNet</strong></td>
<td></td>
</tr>
<tr>
<td>Virtual Network</td>
<td>Create new or enter the name of an existing VNet. The default name for the VNet is vnet-FW</td>
</tr>
<tr>
<td>Virtual Network Address Prefix</td>
<td>192.168.0.0/16</td>
</tr>
<tr>
<td><strong>Azure Application Gateway</strong></td>
<td></td>
</tr>
<tr>
<td>App Gateway Name</td>
<td>myAppGw</td>
</tr>
<tr>
<td>App Gateway DNS Name</td>
<td>Enter a globally unique DNS name for the Azure Application Gateway.</td>
</tr>
<tr>
<td>App Gateway Subnet Name and Prefix</td>
<td>Default name is AppGWSubnet and the subnet prefix is 192.168.3.0/24.</td>
</tr>
<tr>
<td><strong>Azure Load Balancer and Web Servers</strong></td>
<td></td>
</tr>
<tr>
<td>Internal Load Balancer Name</td>
<td>myPrivateLB</td>
</tr>
<tr>
<td>Internal Load Balancer Subnet Name and Prefix</td>
<td>Default name is backendSubnet and the subnet prefix is 192.168.4.0/24.</td>
</tr>
<tr>
<td>Backend Vm Size</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Firewalls</strong></td>
<td></td>
</tr>
<tr>
<td>Firewall Model</td>
<td>Choose from BYOL or PAYG (bundle 1 or bundle 2, each bundle includes the VM-300 and a set of subscriptions).</td>
</tr>
</tbody>
</table>
Set up the VM-Series Firewall in Azure

Deploy the VM-Series and Azure Application Gateway Template

### 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.

- **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).
Deploy the VM-Series and Azure Application Gateway Template

Set up the VM-Series Firewall in Azure

- **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-Series 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.