

# ***Auto Scaling the VM-Series Firewall on Azure***

---

## Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

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

## About the Documentation

- To ensure you are viewing the most current version of this document, or to access related documentation, visit the Technical Documentation portal: [docs.paloaltonetworks.com](http://docs.paloaltonetworks.com).
- To search for a specific topic, go to our search page: [docs.paloaltonetworks.com/search.html](http://docs.paloaltonetworks.com/search.html).
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at [documentation@paloaltonetworks.com](mailto:documentation@paloaltonetworks.com).

## Copyright

Palo Alto Networks, Inc.

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

© 2019-2019 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at [www.paloaltonetworks.com/company/trademarks.html](http://www.paloaltonetworks.com/company/trademarks.html). All other marks mentioned herein may be trademarks of their respective companies.

## Last Revised

March 18, 2019

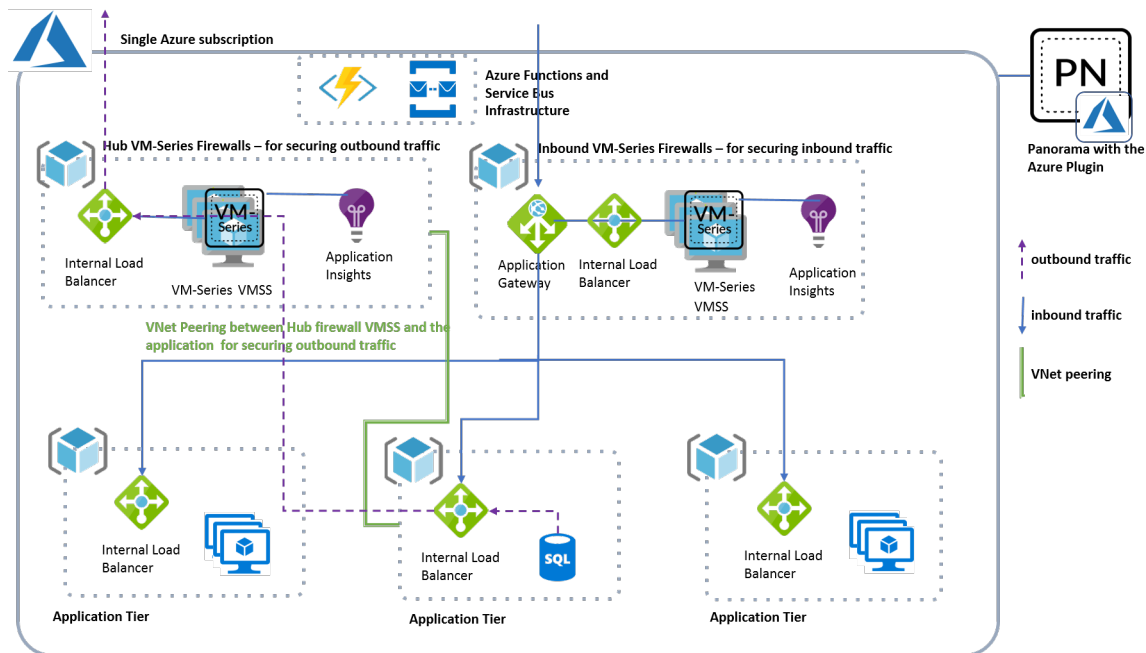
---

# Table of Contents

- Auto Scaling the VM-Series-firewall on Azure..... 4
  - Auto Scaling on Azure - Components and Planning Checklist.....5
    - Plan Your Deployment..... 6
  - Auto Scaling on Azure—How it Works.....8
  - Deploy Azure Auto Scaling Template..... 10
    - Before You Begin..... 10
    - Deploy the Auto Scaling VM-Series Firewalls to Secure Your Applications..... 12
  - Parameters in the Auto Scaling Templates for Azure.....20
    - Infrastructure Template Parameters.....20
    - Inbound Firewall Template Parameters..... 20
    - Hub Template Parameters..... 21
    - Application Template Parameters..... 22
  - Known Issues in Plugin Version 2.0.0..... 23

# Auto Scaling the VM-Series-firewall on Azure

Palo Alto Networks now provides templates to help you deploy an auto-scaling tier of VM-Series firewalls using several Azure services such as Virtual Machine Scale Sets, Application Insights, Azure Load Balancers, Azure functions, Panorama and the Panorama plugin for Azure, and the VM-Series automation capabilities including the PAN-OS API and bootstrapping. The templates allow you to leverage the scalability features on Azure that are designed to manage sudden surges in demand for application workload resources by independently scaling the VM-Series firewalls with the changing workloads.



- [Auto Scaling on Azure - Components and Planning Checklist](#)
- [Deploy Azure Auto Scaling Template](#)
- [Parameters in the Auto Scaling Templates for Azure](#)

---

# Auto Scaling on Azure - Components and Planning Checklist

To deploy VM-Series firewalls in an auto scaling set up where the firewalls can scale with your application workloads and ensure high availability for your services, you need to understand the following concepts:

- **Virtual Machine Scale Sets (VMSS)**— A VMSS is a groups of individual virtual machines (VMs) within the Microsoft Azure public cloud that administrators can configure and manage as a single unit. The firewall templates provided for auto scaling, create and manage a group of identical, load balanced VM-Series firewalls that are scaled up or down based on custom metrics published by the firewalls to Azure Application Insights. The scaling-in and scaling out operation can be based on configurable thresholds.
- **Azure Application Insights**—The VM-Series firewall on Azure can publish custom PAN-OS metrics natively to Azure Application Insights that you can use to monitor the firewalls directly from the Azure portal. These metrics allow you to assess performance and usage patterns that you can use to set alarms and take action to automate events such as launching or terminating instances of the VM-Series firewalls. See [Custom PAN-OS Metrics Published for Monitoring](#) for a description on the metrics that are available.
- **Panorama and the Panorama plugin for Azure**—Panorama is required to enable centralized management of the auto scaling VM-Series firewalls that are deployed in the VMSS. The Azure plugin on Panorama enables you to set up communication between Panorama and the resources within your Azure subscription. The plugin takes care of the interactions required to license, bootstrap and configure the VM-Series firewalls using device groups and template stacks on Panorama. It also programs the Azure static routes and the Azure Application Insights Instrumentation Key to the firewalls in the VMSS.
- **Azure Functions and Service Bus**—Azure Service Bus enables message-based communication between the Azure plugin on Panorama and the Azure resources. The Azure Function is a publicly accessible webhook that publishes messages to the message queue. When you configure the Azure plugin to subscribe to that queue, it can read messages to learn when a new application template is deployed (as long as it has the Panorama managed tag) and when a firewall was scaled in events so that it can contact the Palo Alto Networks licensing server and deactivate the license. The Panorama plugin and the Azure function use a Shared Access Signature (SAS) token to authenticate to the Service Bus and write or read messages from the queue.
- **Templates**—For deploying the auto scaling VM-Series firewalls to secure your application server pool on Azure, four templates are available to you—Inbound firewall template, Hub firewall template, infrastructure template, and the sample app template.
  - **Infrastructure template**—The template deploys the Azure Service Bus and messaging infrastructure to enable message-based communication between the Azure plugin on Panorama and the Azure resources.
  - **Inbound firewall template**—The template deploys an Azure Application Gateway (L7 load balancer), VMSS for the VM-Series firewalls, new VNET with three subnets for the Trust, Untrust, and Management interfaces on the firewall, an Application Insights instance, and storage. The VM-Series firewalls in this template enable you to secure inbound traffic from the Internet to your application.
  - **Hub firewall template**—The template deploys an Standard internal load balancer, VMSS for the VM-Series firewalls, new VNET with three subnets for the Trust, Untrust, and Management interfaces on the firewall, an Application Insights instance, and storage. The VM-Series firewalls that this template deploys enable you to secure outbound traffic (traffic originating from the application servers), and east-west traffic between the application tiers.
  - **App template**—This template is provided as an example to help you can try the VM-Series auto scaling solution on Azure. When deploying this application template, you can choose whether you want to secure inbound traffic only or secure both inbound and outbound traffic. The template deploys an internal load balancer (Standard) and a sample web application. If you opt to secure

---

outbound traffic, it also creates User Defined Routes (UDRs) to forward outgoing traffic from the application server through the hub firewall VMSS.

- **Azure VNet Peering**—Azure VNet peering enables you to connect virtual networks within the Azure public cloud. The traffic between virtual machines in peered virtual networks is routed directly through the Microsoft backbone infrastructure, instead of using a gateway or going over the public internet. In peered VNets, all subnets within the virtual network have routes with next hop type VNet peering for each address space within these networks. If your applications and the VM-Series firewall VMSS are in different VNets, VNet peering between the application and the Inbound and Hub firewall VMSS virtual networks is required to successfully route traffic between them.
- **Azure Load Balancers**—Internal load balancer and the Azure Application gateway to redistribute traffic to the firewall VMSS or to the backend application server pool.
- **Tags**—The firewalls in the VMSS and the sample application have tags that are used for identification. When you deploy the firewall templates—Inbound or Hub—every VM-Series firewall instance has a tag called PanoramaManaged=True. This tag enables Panorama to identify the firewalls in the VMSS so that you can centrally manage them from Panorama.

The sample Application template includes two additional tags. One is PanoramaResourceGroupType=SpokeApp to indicate that both inbound and outbound traffic are secured using the Inbound firewall VMSS and the Hub firewall VMSS. The other tag is PAVMPort = <port no>, which is the port to which the firewall is automatically creates a static route to enable source NAT to the application backend.

- **Sample firewall configuration**— The sample configuration includes a virtual router with eth1/1 (Untrust) and eth1/2 (Trust) interfaces in a zone. You can use this configuration as a starting point so that Panorama can push the static routes that enable the firewalls to forward inbound/outbound traffic through the correct interface on the firewall.

## Plan Your Deployment

Before you begin, use the following checklist to think through your auto scaling deployment and collect the details required to continue with [Deploy Azure Auto Scaling Template](#):

- ❑ The Azure subscription and region in which you want to deploy the applications and the VM-Series firewalls.

The firewalls and the applications must be deployed in the same region and within the same subscription. Cross subscription deployments are not supported in template version 1.0.

- ❑ Panorama appliance running PAN-OS 8.1.x, where x is 6 or later, and [install the Panorama plugin for Azure](#) version 2.0.0.
- ❑ Plan the device groups and templates/template stack on Panorama.

On Panorama, you must assign firewall to a template stack and a device group in order to push network configuration and policies. 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. There is a 1:1 relationship between an Azure subscription and an auto scaling definition on Panorama. For each firewall Resource Group that you want to add to Panorama, you must provide the Resource Group name, Resource Group type - Hub or Inbound, device group name and template stack name with which to associate the firewalls so that Panorama can push the configuration. As a part of the auto scaling definition, you can specify whether you want Panorama to create and pushes the static routes required to forward inbound/outbound traffic through the firewall.



*You must also add a virtual router to the template stack.*

- ❑ Create a storage account on the Azure portal and set up the Azure Files service to contain the folder structure required for the bootstrap package.
- ❑ Gather the information you need as [inputs in the init-cfg.txt](#) file used to bootstrap the VM-Series firewalls. You must include the following:

- 
- Panorama IP address—The IP address of the Panorama appliance that the firewalls must connect with for the license and configuration.
  - VM auth key—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.
  - Auth codes, if using BYOL
  - Device group name
  - Template stack name
- ❑ (If you want to secure an application that you have already deployed) Collect the application details required to configure the Azure Application Gateway in the Inbound firewall template to steer the application traffic to the internal load balancer that fronts the application which you want to secure. Refer to the [Azure Application Gateway](#) documentation for details on the frontend- and backend-server configuration. For an example configuration, see [onboard an app](#).
- Because the inbound firewall VMSS can support multiple applications in the backend pool, you must manually configure the public load balancer to listen for the application. When you use the sample app template, the relevant [tags](#) are automatically defined and the plugin creates the static routes required to redirect traffic through the firewall before it is routed to the application server pool. In this case, you must manually add the tags to the public load balancer that fronts your application server pool.
- ❑ The Azure plugin on Panorama needs an Active Directory application and a Service Principal to execute Azure APIs and access Azure resources. Create the [Active Directory application and Service Principal](#). You must create the Active Directory application and Service Principal and provide the following details from that process as inputs to the Azure plugin on Panorama.
- Application ID
  - Secret key (Copy this key; the secret key is no longer visible after you navigate away from the page)
  - Tenant ID
  - Subscription ID
- ❑ Download the templates and files that enable this auto scaling deployment from the [GitHub repository](#).
- ❑ Record the Service Bus Key Name and Shared Access Signature. After you deploy the infrastructure template, you must gather these details for configuring the auto scaling definition.

---

# Auto Scaling on Azure—How it Works

The primary reason you want to deploy an auto scaling set of VM-Series firewalls is to ensure operational efficiency and to secure traffic to your highly available internet-facing applications when demand spikes, and to maintain cost efficiency when demand drops and the application workloads scale in.

The first step in the process of enabling auto scaling with the VM-Series firewalls is to launch the infrastructure template which provides the messaging infrastructure. The Panorama plugin for Azure uses this infrastructure to learn about the VM-Series firewall VMSS that are deployed when you launch the Hub or Inbound firewall templates and to learn when a new application server pool is added and needs to be secured by the Hub or Inbound firewall templates or both.

Then, you set up the Auto Scaling definition on Panorama to authorize access using the Service Bus name, Service Bus Key Name, the Shared Access Token, and the Service Principal for the Azure subscription. These details enable Panorama to access the metadata on your Azure resources and to read the messages that the Azure function publishes to the Service Bus.

When you deploy the inbound firewall template to secure all inbound traffic to the application server pool, the VMSS for the VM-Series firewalls is launched along with the Azure Application Insights instance to which these firewalls publish the PAN-OS metric that you want to trigger auto scaling. As a part of the template inputs, you choose the PAN-OS scaling metric and threshold values for the Application Insights alarms that trigger the scaling process. The firewalls are automatically bootstrapped using your inputs in the template and added as managed devices to Panorama.

On Panorama, you can now add the Inbound firewall Resource Group details and enable the auto-programming of routes. The Inbound firewall template has three static routes. A default route to forward traffic to the trust interface, and this route is used when a more specific route is not available. A route to send return traffic from the application back to the Application Gateway IP address in the Inbound firewall Resource group, and lastly a route to enable health checks to enable load balancing to the firewall instance.

When the newly launched firewall connects to Panorama, Panorama pushes the device group and template stack configuration which includes the virtual router and policy rules you've defined and the auto programmed static routes. In addition, the Panorama plugin also retrieves that Application Insights instrumentation key and adds it to the template stack to which the firewall are assigned. When the firewall reaches the configured threshold, and a scale out event occurs, a new instance of the VM-Series firewall is launched. The firewall is bootstrapped, connects to Panorama and gets its license and configuration to ensure that it can secure your applications.

When a scale in event occurs, the Panorama plugin deactivates the license on the firewall and manages the lifecycle of the firewall. The IP address of the firewall is removed from the VMSS and the internal load balancer does not route traffic to the firewall.

The flow in the Hub firewall template is similar, with a slight difference in the static routes configuration.

In order to direct traffic through the Inbound firewall or Hub VMSS to the applications, there is some configuration that you need to complete:

To secure inbound application traffic, the application must be connected to the Inbound firewall VMSS (or should I say Resource Group). When you onboard your application, you need to do the following:

- Configure the Application Gateway with the frontend and backend configuration to point to the internal load balancer that fronts the application server pool. Refer to the [Azure Application Gateway documentation](#).
- In the default BackendUDR, add a route with application subnet as the destination, and the next hop IP address as that of the internal load balancer that fronts the firewall VMSS.
- Set up VNet peering between the application VNet and the Inbound firewall VMSS VNet, if they are in different VNets. When you use the sample application template included in the GitHub repository, VNet peering is set up for you.



- 
- Tag the internal load balancer that fronts the application with these name-value pairs.

```
PanoramaManaged=yes
```

```
InboundRG-<Name of the Inbound Firewall Resource Group>
```

To secure both inbound and outbound traffic, the application is connected to the Inbound firewall VMSS and the Hub firewall VMSS, you need to complete the set up above to connect the application to the Inbound firewall VMSS, and the following to connect the Hub firewall VMSS:

- Add a UDR in the route table and associate the application's subnet to the route table. Refer to the [Azure documentation](#).
- On the Azure portal, add a default route (0.0.0.0/0) to forward all traffic to the internal load balancer that fronts the Hub firewall VMSS.
- On Panorama, add a static route to direct return traffic to the application workloads. To enable the firewalls in the Hub VMSS to direct traffic back to the application workloads, you need to configure a static route. Make sure to define the static route on the template stack that manages the configuration of the firewalls in the Hub VMSS.
- Tag the internal load balancer that fronts the application with these name-value pairs.

```
HubRG-<Name of the Hub Firewall Resource Group>
```

---

# Deploy Azure Auto Scaling Template

The Azure auto scaling template leverages multiple components including native Azure services to auto scale the VM-Series firewall to secure your application workloads as they scale in or out to meet the needs of your enterprise. To enable the Azure VM Scale Sets (VMSS) to auto scale VM-Series firewalls, custom firewall metrics are published to Azure Application Insights which allows for firewalls to scale in or scale out based on the monitored thresholds. For this auto scaling mechanism to work, you require Panorama and the Azure plugin on Panorama. For details on all the components you need to secure your application workloads with an auto-scaling tier of VM-Series firewalls, see [Auto Scaling on Azure - Components and Planning Checklist](#).

- [Before You Begin](#)
- [Deploy the Auto Scaling VM-Series Firewalls to Secure Your Applications](#)

## Before You Begin

Get started with the deploying the VM-Series firewalls that auto scale with your application workloads on Azure.

- Review the checklist in [Plan Your Deployment](#).
- Download the templates and files from the [GitHub repository](#).
- [Install the Panorama plugin for Azure](#) version 2.0.0 on Panorama.
- On Panorama create the following:
  1. In a template stack create a virtual router.



*Make sure to add the virtual router to the template stack and not to the template. If you do not create the virtual router in the template stack, the static routes that the inbound firewall template automatically creates will not be added to the virtual router, and your application template may not launch successfully.*

2. In a template, create two interfaces—ethernet1/1(Untrust) and ethernet1/2 (Trust) interfaces. On each interface, **Enable DHCP** and clear **Automatically create default route pointing to default gateway provided by server**.
3. Assign the interfaces to the virtual router.
4. Create a NAT policy rule.
  - Select the device group that you plan to use for the configuration of the Inbound Firewall template, and add a NAT policy rule to direct traffic from the untrust zone to the trust zone, and set the translated packet to use the trust interface (ethernet1/2) IP address so that the return traffic is sent back to the trust interface on the firewall.

NAT Policy Rule

General Original Packet Translated Packet Active/Active HA Binding Target

Any

Source Zone

myUnrust

Destination Zone

myTrust

Destination Interface

any

Service

any

+ Add - Delete

Any

Source Address

+ Add - Delete

Any

Destination Address

+ Add - Delete

OK Cancel

NAT Policy Rule

General Original Packet Translated Packet Active/Active HA Binding Target

Source Address Translation

Translation Type: Dynamic IP And Port

Address Type: Interface Address

Interface: ethernet1/2

None

Destination Address Translation

Translation Type: None

OK Cancel

- Select the device group that you plan to use for the configuration of the Hub Firewall template, and add a NAT policy rule to direct traffic from the trust zone to the untrust zone, and set the translated packet to use the untrust interface (ethernet1/1) IP address so that the return traffic is sent back to the untrust interface on the firewall.

NAT Policy Rule

General Original Packet Translated Packet Active/Active HA Binding Target

Any

Source Zone

myTrust

Destination Zone

myUnrust

Destination Interface

any

Service

any

+ Add - Delete

Any

Source Address

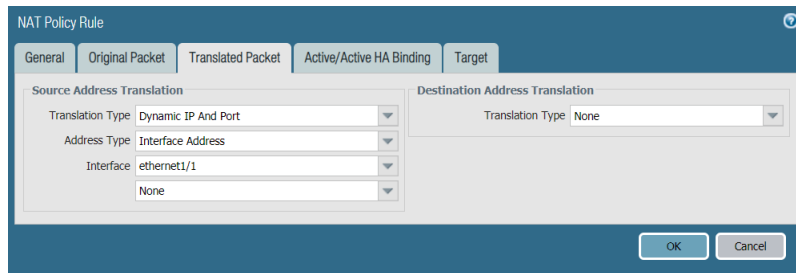
+ Add - Delete

Any

Destination Address

+ Add - Delete

OK Cancel

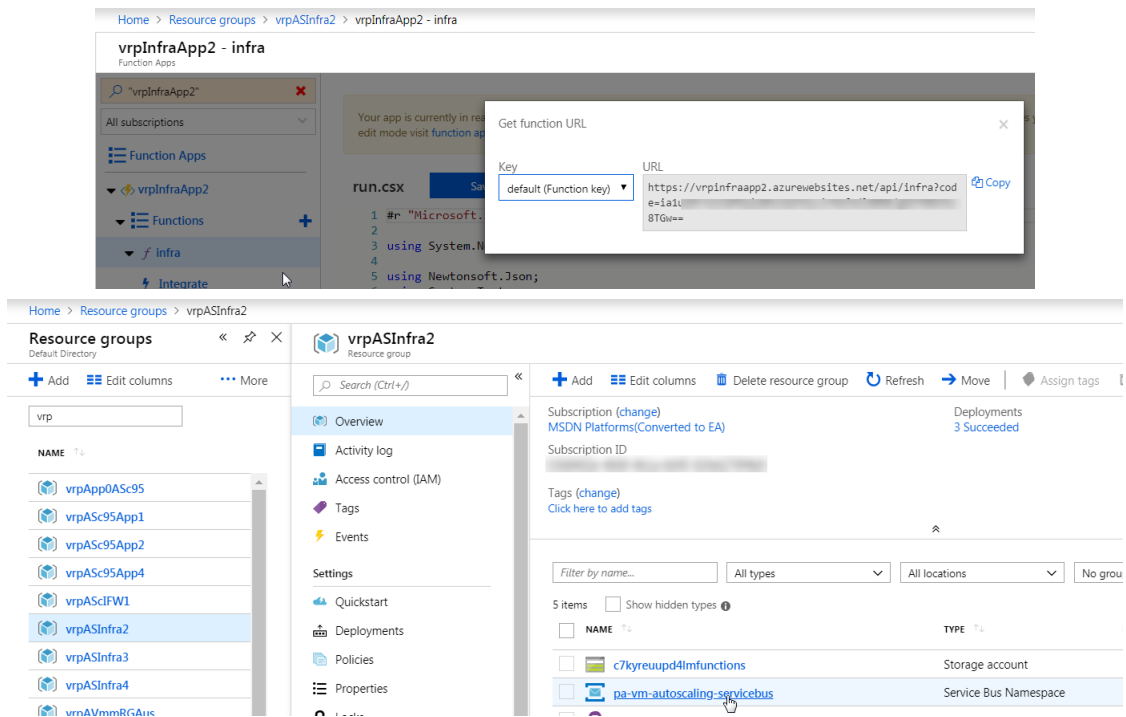


5. Create Security policy rules to allow traffic for the application(s) you are deploying.

## Deploy the Auto Scaling VM-Series Firewalls to Secure Your Applications

### STEP 1 | Launch the infrastructure template.

This allows you to launch the Azure Service Bus and the Azure function. You need to get the SB name, SB credentials (shared access key) for use later on the Panorama Azure plugin. You will also need the Function URL to deploy the firewall template (for inbound and hub).

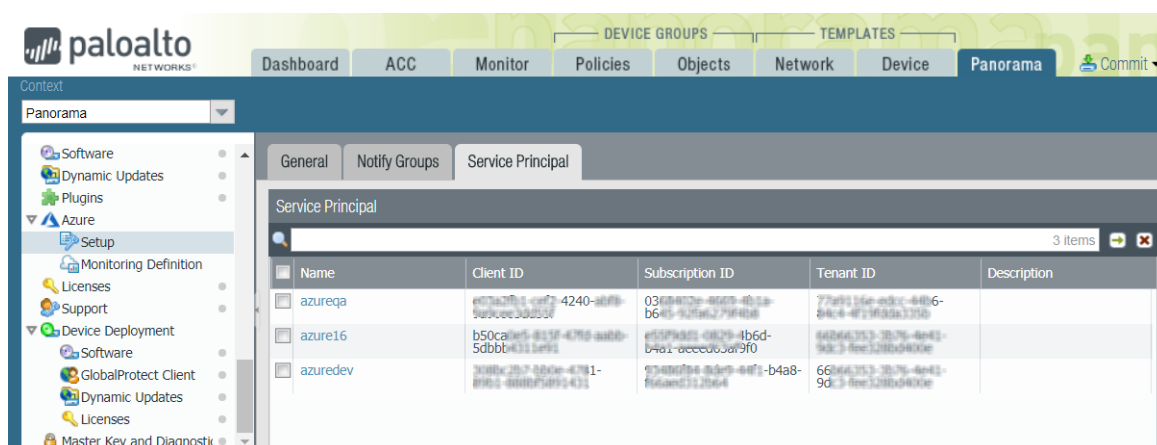


### STEP 2 | Log in to the Panorama, and for every VMSS group of firewalls, create a device group, a template stack and one or more templates.

### STEP 3 | Set up your Service Principal on the Azure plugin on Panorama.

The Service Principal is the service account that you created on the Azure portal. This account is attached to the Azure AD and has limited permissions to access and monitor the resources in your Azure subscription.

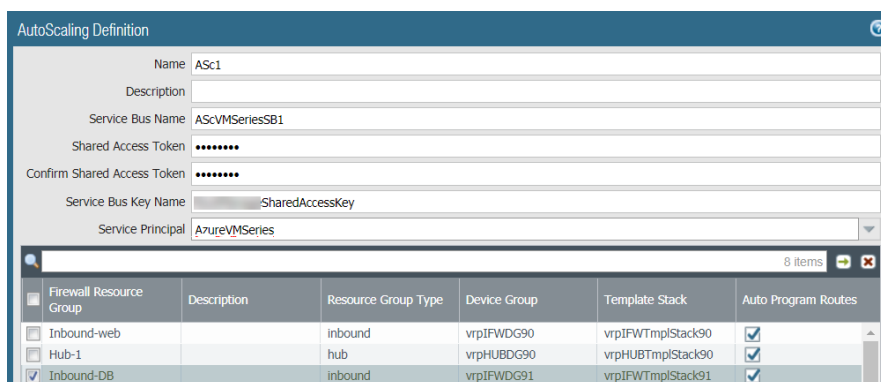
1. Select **Panorama > Plugins > Azure > Setup > Service Principal > Add**.



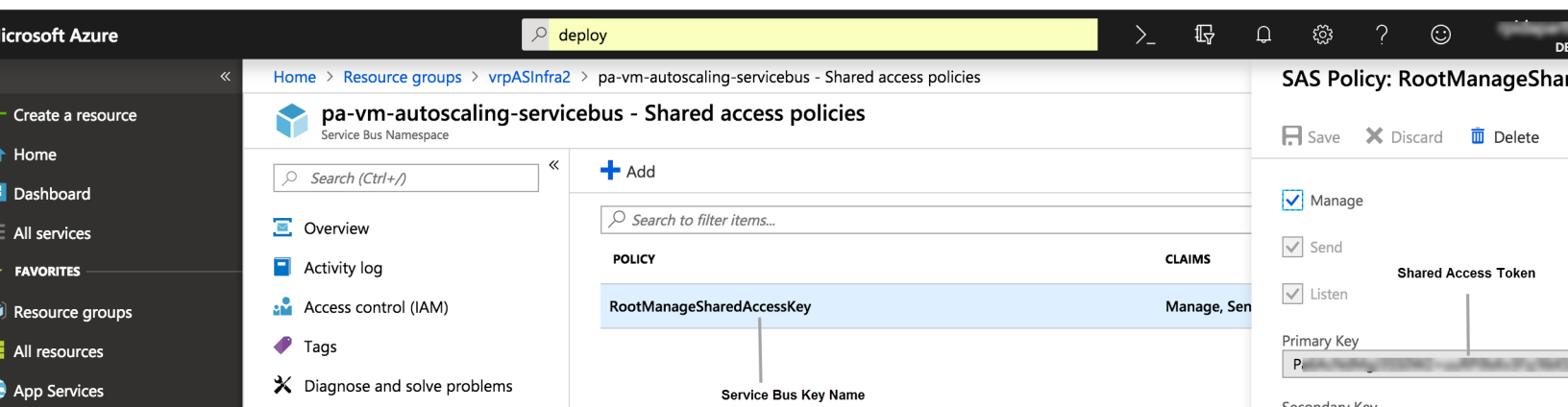
2. Enter a **Name** and optionally a **Description** to identify the service account.
3. Enter the **Subscription ID** for the Azure subscription you want to monitor. You must login to your Azure portal to [get this subscription ID](#).
4. Enter the **Client Secret** and re-enter it to confirm.
5. Enter the **Tenant ID**. The tenant ID is the Directory ID you saved when you set up the Active Directory application.
6. Click **Validate** to verify that the keys and IDs you entered are valid, and Panorama can communicate with the Azure subscription using the API.

#### STEP 4 | Create your Azure auto scaling definition for the Azure subscription.

You can add up to 10 Autoscaling Definitions and each definition can include up to 25 Virtual Machine Scale Sets (VMSS). The firewalls in a VMSS map to one device group and one template stack on Panorama.



1. Select **Panorama > Plugins > Azure > Autoscaling > Add**.
2. Enter a **Name** and **Description** for the auto scaling definition.
3. Add the **Service Bus Name**—Enter the Service Bus Name that you defined when you launched the infrastructure template from the GitHub repository. You must copy this name from the from the Azure portal and paste it here.
4. Add the **Shared Access Token** and **Service Bus Key Name**— You need to get these from the infrastructure template on the Azure portal.



5. Select the **Service Principal** that enables Panorama to authenticate to your Azure subscription.
6. **Add** the firewall Resource Group to Panorama.
  1. Enter a name to identify the **Firewall Resource Group**, and optionally a **Description**.
  2. Select the Resource Group Type: **Hub**—These firewalls secure outbound traffic and east-west traffic between the VMs in your Azure deployment. **Inbound**—These firewalls secure inbound traffic to the application VMs in your Azure deployment.
  3. Select the **Device Group**, and the **Template Stack** that you created for the firewalls deployed within the Resource Group above.
  4. Verify that **Push static routes automatically to the template stack** is enabled. This option is enabled by default, and it enables Panorama to push static routes to the firewalls that belong to the Inbound Firewall VMSS and the Hub Firewall VMSS. In the Inbound Firewall template, the static routes enable the firewalls to direct inbound traffic to the backend application server pool, route return traffic to the client, and route the health probe initiated by the Azure load balancer. In the Hub Firewall template, the static routes enable the firewalls to route the health probe initiated by the Azure load balancer and direct outbound traffic (that is traffic originating from the applications/services) to the internet.

#### STEP 5 | Launch the Azure Inbound Firewall template.

For a description of the input parameters, see [Inbound Firewall Template Parameters](#). And skip to [onboard an app](#), if you do not want to secure outbound traffic (that is secure traffic originating from your application workloads within a Resource Group).

#### STEP 6 | Launch the Azure Hub Firewall template.

You need to deploy this template, only if you want to secure traffic originating from your application workloads within a Resource Group.

1. Launch the Hub autoscaling firewall template. For a description of the input parameters, see [Hub Template Parameters](#).
2. Verify that the auto-programmed routes are in the virtual router on Panorama.


After you deploy the Hub template, a default route and a route for health checks to the managed firewalls is automatically added to the virtual router in the template stack for the VM-Series firewalls launched with the Hub template. And the Azure Application Insights instrumentation key is also automatically available. You need to verify that these routes and the are included so that the firewalls are properly configured and can send metrics for monitoring the autoscaling thresholds. the Synchronizng Config with Azure button. Follow the same procedure if you do not see routes populated for the Hub template stack as well.

1. Log in to Panorama and select **Network**.
2. Select the template stack associated with the Hub firewall VMSS in the **Template** drop-down.

3. Select **Virtual Router** and select the virtual router.
4. Select **Static Routes** and verify that you can see two routes.

Name	Destination	Interface	Type	Value	Admin Distance	Metric	BFD	Route Table
AzurePanPluginDefaultRoute	0.0.0.0/0	ethernet1/1	ip-address	172.16.1.1	default	10	None	unicast
AzurePanPluginAzureHealthCh	168.63.129.16/32	ethernet1/2	ip-address	172.16.2.4	default	10	None	unicast

5. Select **Device > VM-Series** and view the value for the **Azure Instrumentation Key**.

 If you do not see the static routes or the Azure Instrumentation Key, on Panorama > Plugins > Azure > AutoScaling, and click the Synchronizing Config with Azure link that corresponds to the autoscaling definition you want to update.

3. Add a static route to direct return traffic from the internet back to the application.

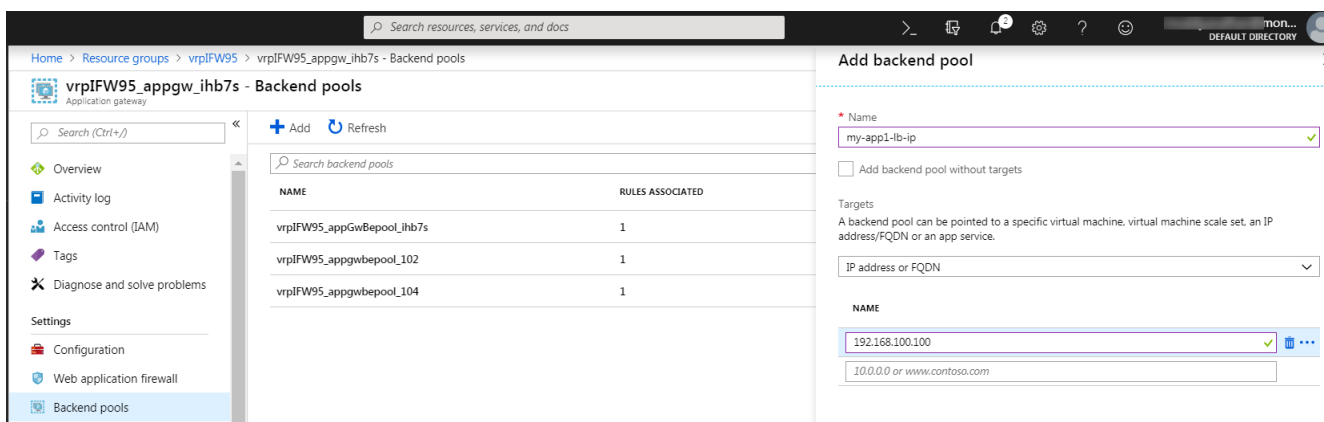
On Panorama, you must add a static route to the virtual router associated with the template stack for the Hub firewall. This route is not automatically added, and is needed to ensure that the application server receives the requested content back from the internet.

1. Log in to Panorama and select **Network**.
2. Select the template stack associated with the Hub firewall VMSS in the **Template** drop-down.
3. Select **Virtual Router** and select the virtual router you are configuring.
4. Select **Static Routes** and add a route with the destination IP address as the subnet for the application, set the outgoing interface as the trust interface on the firewall and the Next Hop IP address for the internal load balancer that fronts your application workloads in the application Resource Group.

Name	Destination	Interface	Type	Value	Admin Distance	Metric	BFD	Route Table
AzurePanPluginDefaultRoute	0.0.0.0/0	ethernet1/1	ip-address	172.16.1.1	default	10	None	unicast
AzurePanPluginAzureHealthCh	168.63.129.16/32	ethernet1/2	ip-address	172.16.2.4	default	10	None	unicast
to-App	10.0.2.0/24	ethernet1/2	ip-address	172.16.2.1	default	10	None	unicast

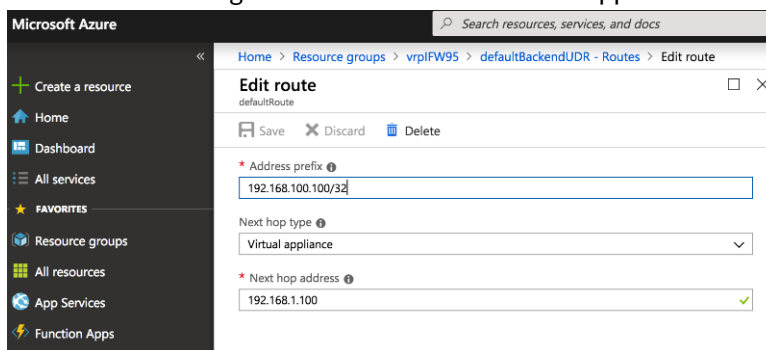
**STEP 7** | To onboard an app, complete the following on the Inbound Firewall Resource Group.


1. Access the Application Gateway.
2. Add the Load balancer IP address for the sample application to the Application Gateway backend pool.



3. Add a route to the defaultBackendUDR to direct traffic through the firewall to the application you want to secure.

You need to add a route that specifies the address prefix of the internal load balancer IP address for the application gateway that was created when you launched the App template, and the next hop IP address should match the IP address of the load balancer that fronts the VM-Series firewall VMSS in the Inbound firewall resource group. This route allows the Application Gateway to send traffic to the Inbound firewall VMSS before routing it to the load balancer in the application resource group.



 If you have your own app and you want to configure it to secure traffic to it using the VM-Series firewalls that you deployed using the hub or the firewall template, you must do the following:

- Set up VNET peering between the application VNet and the VNet in which your firewall VMSS are deployed.

If you are securing inbound and outbound application traffic, on the Azure portal select the virtual network for the application and verify that VNet peering status is connected for the Hub and the Inbound firewall VNets.

NAME	PEERING STATUS	PEER	GATEWAY TRANSIT
jpasaprg-vnet-jpashubrg-vnetvnet-peering	Connected	jpashubrg-vnet	Enabled
jpasaprg-vnet-inbound-fw-vnetvnet-peering	Connected	inbound-fw-vnet	Enabled

- Add the IP address of the internal Load Balancer that fronts the application to the Application gateway configuration in the inbound firewall Resource Group.
- Add a route to the defaultBackend UDR table to direct traffic through the firewall. You need to add a route that specifies the IP address of the load balancer that fronts the application, and specify the IP address load balancer that fronts the firewall VMSS as the next hop. This route allows the Application Gateway to send traffic to the firewall VMSS before routing it to the load balancer in the application resource group.



- Add the following tags to the internal load balancer that fronts your application workloads.
  - HubRG: Enter the name of the Hub firewall Resource Group
  - PanoramaManaged: yes
  - InboundRG: Enter the name of the Inbound firewall Resource Group

Microsoft Azure

Home > Resource groups > vrplApp0ASc95 > myPrivateLB - Tags

**myPrivateLB - Tags**  
Load balancer

Search (Ctrl+/,)

Save Delete all Revert changes

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources. [Learn more](#)

NAME	VALUE
HubRG	:
PanoramaManaged	: yes
InboundRG	: vrplFW95

myPrivateLB (Load balancer)  
No changes

**STEP 8** | To onboard an app, complete the following on the Hub Firewall Resource Group.

1. Access the Application Gateway.
2. Add the Load balancer IP address for the sample application to the Application Gateway backend pool.

Home > Resource groups > vrplFW95 > vrplFW95\_appgw\_ihb7s - Backend pools

**vrplFW95\_appgw\_ihb7s - Backend pools**  
Application gateway

Search (Ctrl+/,)

+ Add Refresh

Search backend pools

NAME	RULES ASSOCIATED
vrplFW95_appgwBepool_ihb7s	1
vrplFW95_appgwBepool_102	1
vrplFW95_appgwBepool_104	1

**Add backend pool**

Name: my-app1-lb-ip ✓

☐ Add backend pool without targets

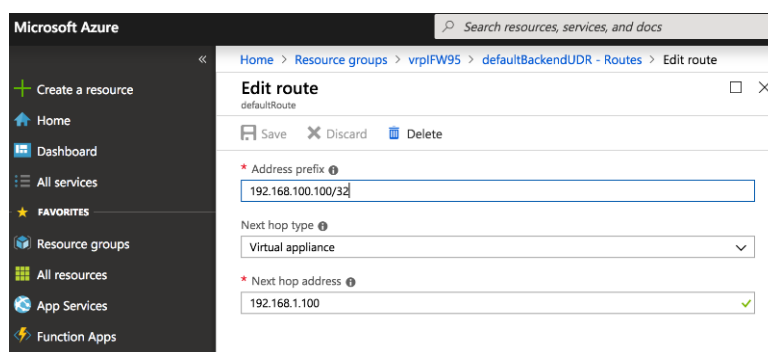
Targets: A backend pool can be pointed to a specific virtual machine, virtual machine scale set, an IP address/FQDN or an app service.

IP address or FQDN: 192.168.100.100 ✓

NAME: 10.0.0.0 or www.contoso.com

3. Add a route to the defaultBackendUDR to direct traffic through the firewall to the application you want to secure.

You need to add a route that specifies the address prefix of the internal load balancer IP address for the application gateway that was created when you launched the App template, and the next hop IP address should match the IP address of the load balancer that fronts the VM-Series firewall VMSS in the Inbound firewall resource group. This route allows the Application Gateway to send traffic to the Inbound firewall VMSS before routing it to the load balancer in the application resource group.



If you have your own app and you want to configure it to secure traffic to it using the VM-Series firewalls that you deployed using the hub or the firewall template, you must do the following:

- Set up VNET peering between the application VNet and the VNet in which your firewall VMSS are deployed.

If you are securing inbound and outbound application traffic, on the Azure portal select the virtual network for the application and verify that VNet peering status is connected for the Hub and the Inbound firewall VNets.

NAME	PEERING STATUS	PEER	GATEWAY TRANSIT
jpasaprg-vnet-jpashubrg-vnetvnet-peering	Connected	jpashubrg-vnet	Enabled
jpasaprg-vnet-inbound-fw-vnetvnet-peering	Connected	inbound-fw-vnet	Enabled

- Add the IP address of the internal Load Balancer that fronts the application to the Application gateway configuration in the inbound firewall Resource Group.
- Add a route to the defaultBackend UDR table to direct traffic through the firewall. You need to add a route that specifies the IP address of the load balancer that fronts the application, and specify the IP address load balancer that fronts the firewall VMSS as the next hop. This route allows the Application Gateway to send traffic to the firewall VMSS before routing it to the load balancer in the application resource group.
- Add the following tags to the internal load balancer that fronts your application workloads.
  - HubRG: Enter the name of the Hub firewall Resource Group
  - PanoramaManaged: yes
  - InboundRG: Enter the name of the Inbound firewall Resource Group

Microsoft Azure

deplo

Home > Resource groups > vrpApp0ASc95 > myPrivateLB - Tags

myPrivateLB - Tags

Load balancer

Search (Ctrl+ /)

Save

Delete all

Revert changes

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Frontend IP configuration

Backend pools

Health probes

Load balancing rules

Inbound NAT rules

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to m

Learn more

NAME	VALUE
HubRG	:
PanoramaManaged	: yes
InboundRG	: vrpIFW95
	:

myPrivateLB (Load balancer)

No changes

## STEP 9 | On Panorama, create Security policy rules.

For securing inbound application traffic, you can specify the source zone and destination zones as any, and add the destination IP addresses as a dynamic address group object and reference it in the Security policy rule.

AUTO SCALING THE VM-SERIES FIREWALL ON AZURE | 19

© Palo Alto Networks, Inc.

---

# Parameters in the Auto Scaling Templates for Azure

This section describes the values you need to provide as input when you deploy the template resources that enable you to auto scale the VM-Series firewalls on Azure with your application workloads.

- [Infrastructure Template Parameters](#)
- [Inbound Firewall Template Parameters](#)
- [Hub Template Parameters](#)
- [Application Template Parameters](#)

## Infrastructure Template Parameters

Inputs for the infrastructure template are as follows:

- Panorama Plugin Message Handler Name—The name of the Azure Function that will pass messages to the Panorama plugin for Azure. The Azure function URL will begin with this name.
- Storage Account Type—Select the type you want to use.
- Repo URL—The URL for the parent GitHub repository that hosts the templates. The location where Palo Alto Networks posts these templates is: <https://github.com/PaloAltoNetworks/azure-autoscaling/Version-1-0>
- Branch—leave as is.
- Service Bus Name—The name of the Service Bus to which Panorama subscribes for notifications from Azure. The value must be between 6 and 50 characters long. This name has to be globally unique, must start and end with a letter or number, and can contain letters, numbers, and hyphens only.

## Inbound Firewall Template Parameters

Inputs for the Inbound Firewall template are as follows:

- Resource Group Name and Location—Create a new Resource group and pick a location.
- App GatewayDns Name—A name
- Network Security Group Inbound Src IP: To restrict inbound access to the firewall management interface. CIDR format for example 199.16.5.122/32.
- Fw Load Balancer IP: Enter an IP address from the Untrust subnet CIDR to assign to the Azure load balancer that fronts the firewall VMSS. The Azure Application Gateway will use this IP address to send traffic onward to the firewall. For example: 192.168.1.4
- virtualNetworkName—The name of the VNet in which you want to deploy the resources in this template.
- virtualNetworkAddressPrefix—For example: 192.168.0.0/21
- mgmtSubnetPrefix—For example: 192.168.0.0/24
- untrustSubnetPrefix—For example: 192.168.1.0/24
- trustSubnetPrefix—For example: 192.168.2.0/24
- appGatewaySubnetPrefix: For example: 192.168.3.0/24
- vmSeriesFirewallModel: BYOL or PAYG bundles
- vmSeriesImageVersion: 8.1
- vmSeriesFirewallVmSize: Standard\_D3\_v2 (default). See [VM instance types](#) for minimum system requirements on the VM-Series firewall on Azure, and refer to [Azure Virtual Machines](#) for a list of instance types available for your region.
- Username—Enter a username for logging in to the firewall web interface.

- Authentication Type: password or SSH key
- Bootstrap Storage Account—Enter the Name of the storage account.
- Bootstrap Storage Account Access Key—Specify the storage account key.
- bootstrapFileShare—The name of the fileshare that holds the bootstrap folder structure.
- bootstrapSharedDir—This directory name is optional.
- VM Scale Set Min Count—Enter a value between 1 and 3. Default is 1
- VM Scale Set Max Count— Enter a value between 1 and 3. Default is 1.
- Auto Scale Metric—Active Sessions (default). To view all the supported metrics, see [Custom PAN-OS metrics](#).
- scaleInThreshold—Enter the threshold for a scaling event. This input can be a number or a percentage based on the scaling metric you selected above.
- scaleOutThreshold—Enter the threshold for a scaling event. This input can be a number or a percentage based on the scaling metric you selected above.
- Panorama Plugin Message Handler URL: This is the name for the Azure Function that entered in the infrastructure template. This URL allows the Service Bus queue and the Panorama plugin for Azure to send messages about your Azure resources. For example: `https://test-asc-function-handler.azurewebsites.net/api/infra?code=IKDDx5U2HddsabcdE==`

## Hub Template Parameters

Inputs for the hub firewall template that enables you to secure outbound traffic and east-west traffic between the application tiers are as follows:

- virtualNetworkName—The name of the VNet in which you want to deploy the resources in this template.
- virtualNetworkAddressPrefix—
- mgmtSubnetPrefix—
- untrustSubnetPrefix—
- trustSubnetPrefix—
- Load Balancer IP—Enter an IP address from the Trust subnet CIDR. The Load balancer will use this IP address to send traffic to the trust interface on the firewall.
- Network Security Group Inbound Src IP: To restrict inbound access to the firewall management interface. CIDR format, for example: 199.16.5.122/32.
- Bootstrap Storage Account—Enter the Name of the storage account.
- Bootstrap Storage Account Access Key—Specify the storage account key.
- bootstrapFileShare—The name of the fileshare that holds the bootstrap folder structure.
- bootstrapSharedDir—This directory name is optional.
- VM Scale Set Min Count—Enter a value between 1 and 3. Default is 1
- VM Scale Set Max Count— Enter a value between 1 and 3. Default is 1.
- Auto Scale Metric—Active Sessions (default). To view all the supported metrics, see [Custom PAN-OS metrics](#).
- scaleInThreshold—Enter the threshold for a scaling event. This input can be a number or a percentage based on the scaling metric you selected above.
- scaleOutThreshold—Enter the threshold for a scaling event. This input can be a number or a percentage based on the scaling metric you selected above.
- Panorama Plugin Message Handler URL: This is the name for the Azure Function that entered in the infrastructure template. This URL allows the Service Bus queue and the Panorama plugin for Azure to send messages about your Azure resources. For example: `https://test-asc-function-handler.azurewebsites.net/api/infra?code=IKDDx5U2HddsabcdE==`

---

## Application Template Parameters

The inputs for the App template are:

- Connect to Hub: yes or no.
- Hub Resource Group Name—Required only if yes. The name of the Resource Group that hosts the resources you deployed with the Hub Firewall template.
- Hub VNET Name—Required only if yes. The name of the VNet that hosts the resources you deployed with the Hub Firewall template.
- Hub Load Balancer IP—Required only if yes. This is the IP address that you had assigned to the load balancer when you launched the Hub Firewall template.
- Application Load Balancer IP—Enter an IP address that belongs to the trust subnet. The application gateway that is in the Inbound Firewall Resource Group will use this IP address to send traffic to the firewall and then on to the application workloads.
- Inbound Firewall Resource Group Name—
- Inbound Firewall VNet Name—
- virtualNetworkAddressPrefix—The CIDR of the VNet in which you want to deploy the resources in this template.
- virtualNetworkName—The name of the VNet in which you want to deploy the resources in this template.
- mgmtSubnetPrefix—
- trustedSubnetPrefix—
- backendSubnetPrefix—The subnet in which your application workloads are deployed.
- username—To log in to the sample application server.
- password—The password for the administrative user you entered above.

# Known Issues in Plugin Version 2.0.0

Issue	Description
PLUG-1344	Upgrade from Panorama plugin for Azure version 1.0.0 to 2.0.0 is not supported. If you are using plugin version 1.0.0, you must remove the configuration and delete plugin version 1.0.0 before you install version 2.0.0.
PLUG-1407	The Azure Application Insights instance that is deployed with the Inbound Firewall or the Hub Firewall template provided for the autoscaling VM-Series firewalls, is in US East region.
PLUG-1444	<p>After you manually delete the Firewall Resource Group in an Autoscaling Definition, you cannot reuse the template stack associated with the managed firewalls to push configuration to firewalls in another Resource Group.</p> <p><b>Workaround</b>—To re-use the template stack, you must first delete the Application Insights instrumentation key on <b>Device &gt; Setup &gt; Operations &gt; Azure Application Insights</b>. You must also delete the static routes that the plugin configured for the firewall resource group, on the virtual router.</p>
PLUG-1466	When using the Azure plugin version 2.0.0, do not configure the VM Monitoring Definition along with the Autoscaling Definition. You can only enable one of the two capabilities.
PLUG-1482	<p>With the Azure PAYG Bundle1 and Bundle2 licenses, Panorama does not remove the firewalls as a managed device. Any firewalls that are scaled-in will display as a managed device and be in a disconnected state on Panorama.</p> <p><b>Workaround</b>—Find the serial number of the disconnected firewalls on <b>Panorama &gt; Managed Device &gt; Summary</b> and manually delete each one from the device group.</p>
PLUG-1582	<p>The Panorama plugin for Azure does not work as expected on Panorama 9.0.</p> <p><b>Workaround</b>—Install the plugin on Panorama 8.1.x, where x is 6 or later.</p>