DEPLOYMENT GUIDE FOR AZURE

Single VNet Design Model (Common Firewall Option)

RELEASE 2
FEBRUARY 2019

Table of Contents

Preface

GUIDE TYPES

Overview guides provide high-level introductions to technologies or concepts.

Reference architecture guides provide an architectural overview for using Palo Alto Networks® technologies to provide visibility, control, and protection to applications built in a specific environment. These guides are required reading prior to using their companion deployment guides.

Deployment guides provide decision criteria for deployment scenarios, as well as procedures for combining Palo Alto Networks technologies with third-party technologies in an integrated design.

DOCUMENT CONVENTIONS

Notes provide additional information.

Cautions warn about possible data loss, hardware damage, or compromise of security.

Blue text indicates a configuration variable for which you need to substitute the correct value for your environment.

In the **IP** box, enter **10.5.0.4/24**, and then click **OK**.

Bold text denotes:

- Command-line commands;

  ```
  # show device-group branch-offices
  ```

- User-interface elements.

  In the **Interface Type** list, choose **Layer 3**.

- Navigational paths.

  Navigate to **Network > Virtual Routers**.

- A value to be entered.

  Enter the password **admin**.

Italic text denotes the introduction of important terminology.

An *external dynamic list* is a file hosted on an external web server so that the firewall can import objects.

Highlighted text denotes emphasis.

```
Total valid entries: 755
```

Purpose of This Guide

This guide provides design and deployment details for Palo Alto Networks® Security Operating Platform on Microsoft Azure. This deployment guide focuses specifically on the common firewall option of the Single Virtual Network (VNet) design model. Details for the Dedicated Inbound option for this design model are included in a separate deployment guide.

This deployment guide:

- Provides architectural guidance and deployment details for using Palo Alto Networks next-generation firewalls to provide visibility, control, and protection to your applications built on Microsoft Azure.
- Requires that you first read the Reference Architecture Guide for Azure. The reference architecture guide provides architectural insight and guidance for your organization to plan linkage of pertinent features with the next-generation firewall in a scalable and highly available design.
- Provides decision criteria for deployment scenarios, as well as procedures for programming features of Microsoft Azure and the Palo Alto Networks VM-Series next-generation firewall in order to achieve an integrated design.

OBJECTIVES

Completing the procedures in this guide, you can successfully deploy a Palo Alto Networks VM-series next-generation firewall in the Azure environment. The main objectives are to enable the following functionality:

- Protection and inspection of flows inbound from the internet, outbound and east-west from private networks and for secure communication with on-premise devices
- Application layer visibility and control for all flows
- Preparing the firewalls to participate in the full Security Operating Platform with WildFire® analytics, URL filtering, identity-based services, and the full Threat Prevention services
- Resilient and scalable operation through integration with Azure load balancer and Azure application gateway
- Panorama™ centralized management using templates and device groups
- Centralized reporting with Palo Alto Networks cloud-delivered Logging Service
- Automatic firewall configuration through bootstrapping

AUDIENCE

This deployment guide is written for technical readers, including system architects and design engineers, who want to deploy the Palo Alto Networks Security Operating Platform within a public cloud datacenter infrastructure. It assumes the reader is familiar with the basic concepts of applications, networking, virtualization, security, and high availability, as well as a basic understanding of network and data center architectures.

To be successful, you must have a working knowledge of networking and policy in PAN-OS®.

RELATED DOCUMENTATION

The following documents support this deployment guide:

- Palo Alto Networks Security Operating Platform Overview—Introduces the various components of the Security Operating Platform and describes the roles they can serve in various designs.
- Reference Architecture Guide for Azure—Presents a detailed discussion of the available design considerations and options for the next-generation VM-Series firewall on Microsoft Azure. If you are unable to access the URL for the reference architecture guide, please ask your account team to assist you.

Deployment Overview

There are many ways to use the concepts discussed in the Reference Architecture Guide for Azure to achieve an architecture that secures applications deployed on Azure. Each of the design models in that guide provide an example architecture that secures inbound access to an application in Azure, the communication between private virtual machines and workloads, and the connection to your on-site networks.

This guide is specific to the common firewall option. The key design considerations for when to choose this option follow.

CHOOSING A DESIGN MODEL OPTION

As discussed in the reference architecture guide, when choosing a design model option, consider the following factors:

- **Scale**—What are the expected number of sessions and bandwidth required for the applications? Is this deployment for a proof-of-concept? Are the traffic profiles for inbound, outbound, east-west and on-premise communication balanced? The common firewall option does not differentiate between traffic flows, and resources consumed by one traffic profile may affect overall performance. The common firewall option provides linear scaling across all traffic profiles by adding additional firewalls to the load-balancer backend pools. To provide increased scale for a specific traffic profile, consider the dedicated inbound and dedicated-inbound/dedicated-backhaul options.
- **Complexity**—Is it more important to keep individual device configuration simple and permit easier troubleshooting, or is it acceptable to take on a somewhat higher administrative workload in order to reduce the total number of deployed devices? The common firewall option combines the configurations for all functions to a single set of devices with uni-directional and bi-directional flows across multiple zones. Careful consideration of any changes is necessary in order to evaluate overall impact, and configuration errors may be more likely. For simplified configuration and/or reduced impact of configuration errors, consider the dedicated inbound and dedicated-inbound/dedicated-backhaul options.
- **Resiliency and high availability**—Are there differentiated availability requirements for different traffic profiles? The common firewall option provides the same level of availability for all profiles. To provide differentiated availability for high priority traffic profiles, consider using the dedicated inbound and dedicated-inbound/dedicated-backhaul options.

Design Models

The design models differ primarily in how the resources are allocated in Azure.

Consider which model best fits your needs and use it as a starting point for your design. The design models in this reference design are the:

- **Single VNet model**—In this model, all functions and resources are allocated within a single VNet, and there are no dependencies on how resources are allocated in other VNets.

  The single VNet design model has several configuration options that differ primarily in how traffic flows are divided amongst VM-Series firewalls while offering you flexibility in the number of firewalls, scale, and operational resiliency. The configuration options for the single VNet model are the:

  - **Common firewall option**—In this model, all traffic flows through a single set of firewalls. The set of firewalls is a shared resource and has limited scale. This model keeps the number of firewalls low and is suitable for small deployments and proof-of-concepts. However, the technical integration complexity is high. This guide describes the deployment details for this option only.
  - **Dedicated inbound option**—This model separates inbound traffic flows onto a dedicated set of firewalls, allowing for greater scaling of inbound-traffic loads. Outbound, east-west, and backhaul traffic flows through a common firewall set that is a shared resource. This design reduces technical integration complexity and increases scale compared to the common firewall model. For deployment details for this option, see the Deployment Guide for Microsoft Azure—Single VNet Design Model (Dedicated Inbound Option).
  - **Dedicated-inbound/dedicated-backhaul option**—Inbound, outbound and east-west, and backhaul traffic are each on dedicated sets of firewalls. This model offers increased operational resiliency and reduces the chances of high bandwidth use from one traffic profile affecting another. This option does not currently have a deployment guide.

- **Transit VNet model**—In this model, the functions and resources are allocated across multiple VNets that are connected into a hub-and-spoke topology. This design model is highly scalable and highly resilient and is suitable for large production deployments.

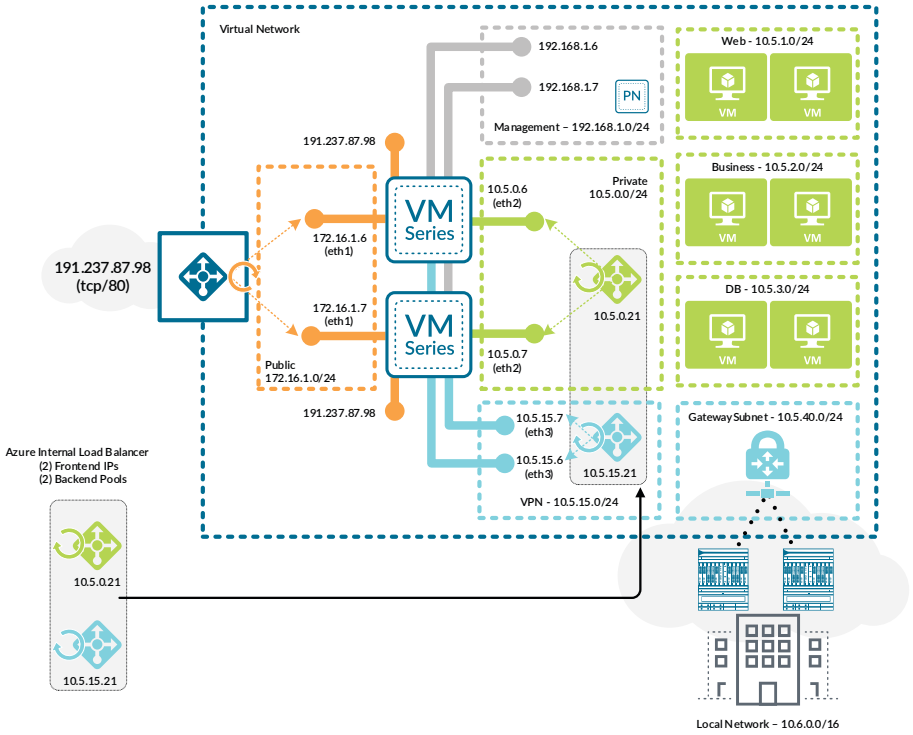
The outbound and backhaul traffic are separated onto a dedicated set of firewalls in a hub or transit VNet that consolidates services for spoke subscribers. East-west traffic between private subnets across different subscribers is controlled by firewalls in the transit VNet. Each subscriber handles its own inbound traffic by using firewall resources within their VNet. This model offers increased scale and operational resiliency and reduces the chances of high bandwidth use from one traffic profile affecting another. This model also reduces the number of locations that must be secured for outbound traffic and allows all backhaul traffic to share a common set of resilient connections. The deployment details for this option are covered in the Deployment Guide for Microsoft Azure—Transit VNet Design Model.

SINGLE VNET MODEL—COMMON FIREWALL OPTION

In the common firewall option, a common set of firewalls provides visibility and control of all traffic profiles (inbound, outbound, east-west, backhaul).

The firewalls are members of an availability set that distributes their virtual machines across the Azure infrastructure to avoid downtime caused by infrastructure maintenance or failure.

Figure 1 Single VNet model—common firewall option



Inbound Traffic

There are two options for inbound traffic:

- **Azure public load balancer**—Choose this option if you require load balancing only at Layer 4 (TCP/UDP). Health probes in this design monitor the firewall resources and are not directly monitoring the health of the web server resources.
- **Azure application gateway**—Choose this option if you require load balancing at Layer 7 (application layer) for HTTP and HTTPS. Capabilities include url path-based routing and SSL offload. Health probes in this design directly monitor the health of the web server resources.

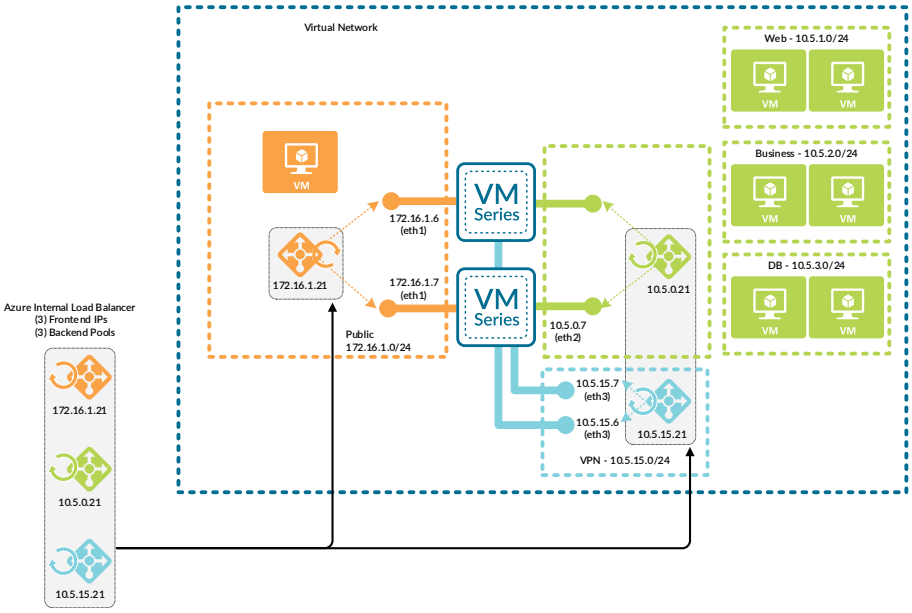
Inbound Traffic with Azure Public Load Balancer

For inbound traffic, a public load-balancer distributes traffic to the firewalls. To simplify firewall configuration, the front-tend public IP address is associated with a DNS name and floating IP is enabled on the load-balancer rules. The public load-balancer's health probes monitor firewall availability through the HTTPS service activated in the interface management profile. Connectivity to the HTTPS service is limited to traffic sourced from the health probe IP address.

User-defined routes direct traffic from the subnet that contains the public interfaces to the other networks in the VNet to the next-hop of *none*. This ensures that only inbound traffic forwarded through the public load balancer can communicate to private resources through the firewall.

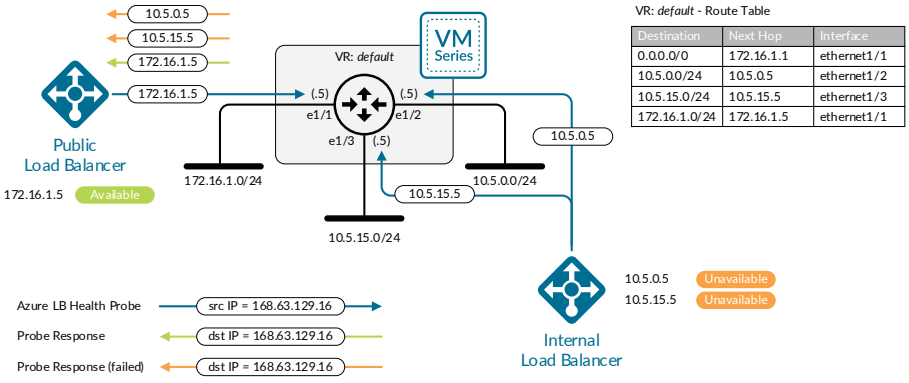
If internal virtual machine resources are deployed in the subnet that contains the public interfaces and these resources require communication to private resources, then a user-defined route directs traffic to the next hop of an internal load balancer in the public subnet.

Figure 2 Inbound internal traffic



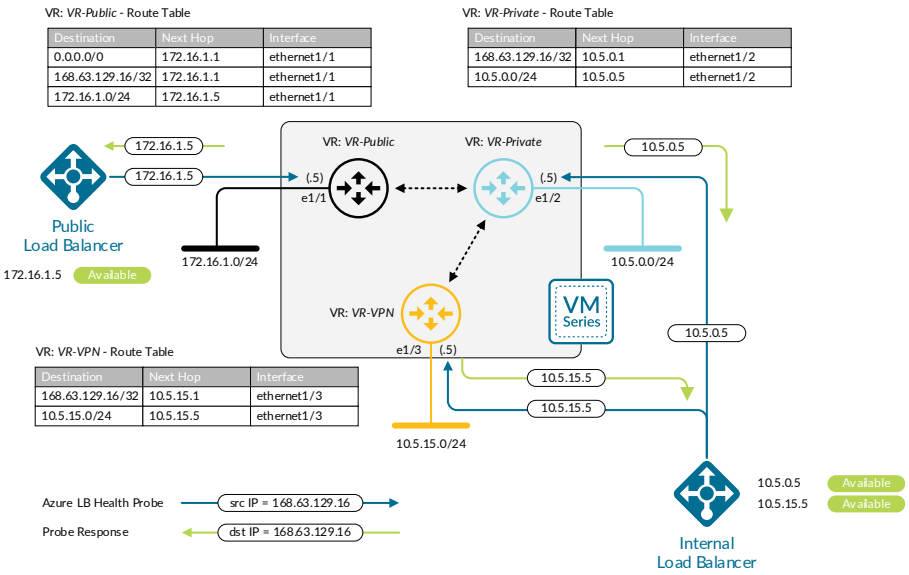
Azure always sources load-balancer health probes from an IP address of 168.63.129.16. This implementation is incompatible with multi-homed devices such as routers or firewalls. Health probes succeed on one interface only and fail on the remaining interfaces, because there is only one active IP route table entry for 168.63.129.16/32. Multiple virtual routers must be configured to support health probes on multiple interfaces.

Figure 3 Health probe failures with single virtual router



The public interface uses a dedicated virtual router. Static routes define a default route and /32 host route for the Azure health probes out the public interface, as well as a route to private networks through the virtual router dedicated to the private interface. Dedicated virtual routers allow the firewall to have the interface that received the health probe to source responses.

Figure 4 Health probes with multiple virtual routers

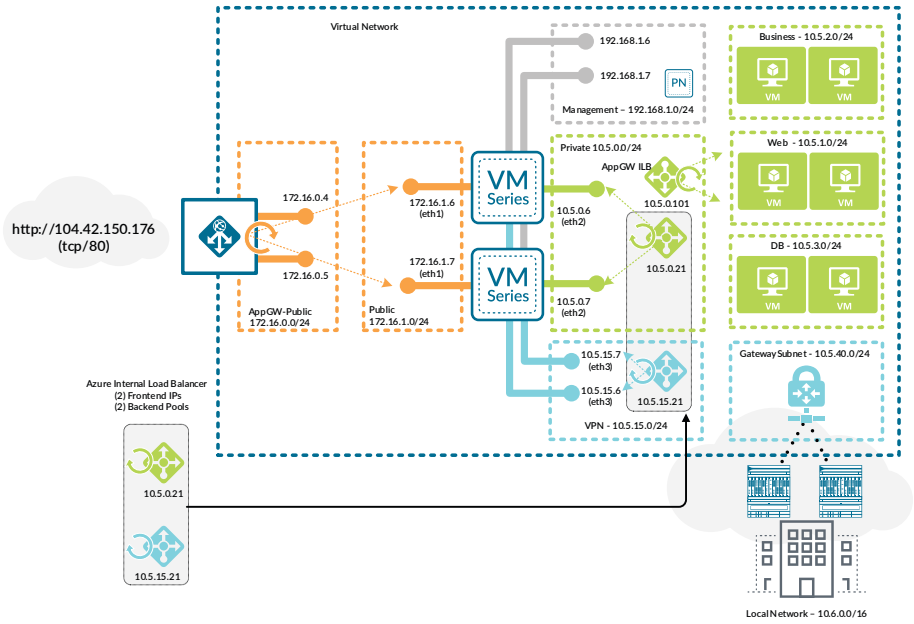


The firewall applies both a destination and source NAT to inbound traffic. Destination NAT translates the FQDN address object associated with the load-balancer public DNS name to the virtual machine or load-balancer on the private network. The source NAT translates the source to be the IP address of the private interface of the firewall, ensuring return traffic flows symmetrically.

The firewall security policy allows appropriate application traffic to the resources in the private network while firewall security profiles prevent known malware and vulnerabilities from entering the network in traffic allowed in the security policy.

Inbound Traffic with Azure Application Gateway

Figure 5 Common firewall option with application gateway



You create an additional public subnet for the application gateway. Specify a minimum of two application gateway instances in order to ensure that the instances are distributed across Azure update and fault domains.

For inbound traffic, an application gateway with a public frontend terminates incoming connections and initiates corresponding new connections to the configured HTTP/HTTPS backends. You must assign unique TCP ports for all backends. All new connections are sourced from the private IP addresses of the application gateway instances and are distributed to the public interfaces of the firewalls, which are configured as the backend pool targets for the application gateway. The application gateway's health probes monitor backend availability on all specified HTTP/HTTPS ports.

Application gateway destination NAT rules on the firewalls are used to map to backend resources directly or through one or more internal load balancers.

Any combination of the following methods is supported:

- **Firewall destination port NAT to backend resource**—No internal load balancer is required; this method uses port-based NAT policy rules associated to the backend resource. Resource mapping parameters are contained entirely within the firewall NAT policy.
- **Internal load balancer with one or more front-end IP addresses**—This method uses port-based NAT policy rules associated to the load balancer front-end IP addresses. Port mapping is also configured on the load balancer. This method uses the load-balancer for resiliency and scaling of the backend resources.
- **Multiple internal load balancers**—This method uses port-based NAT policy rules associated to each load balancer's front-end IP addresses. This option supports more granular separation of both the load balancers and the backend resources.

The firewall also applies a source NAT to inbound traffic. The source NAT translates the source to be the IP address of the private interface of the firewall, ensuring return traffic flows symmetrically.

The firewall security policy allows HTTP/HTTPS application traffic from the application gateway instances to the resources in the private network while firewall security profiles prevent known malware and vulnerabilities from entering the network in traffic allowed in the security policy. To support the use of HTTP/HTTPS backends on ports other than 80/443, security policy rules should have their service configured to include the specific service ports in use instead of *application-default*.

User-defined routes direct traffic from the subnets that contain the public interfaces to the other networks in the VNet to the next hop of *none*. This ensures that only inbound traffic forwarded through the application gateway can communicate to private resources through the firewall.

If internal virtual machine resources are deployed in the subnet that contains the public interfaces and these resources require communication to private resources, then a front-end IP and backend pool for the internal load balancer is deployed. A user-defined route directs traffic to the next hop of an internal load balancer front-end in the public subnet. The public interface only requires a dedicated virtual router if a load balancer is used for internal inbound traffic.

If using a dedicated virtual router, static routes define a default route out the public interface, as well as a route to private networks through the virtual router dedicated to the private interface. Dedicated virtual routers allow the firewall to have the interface that received the health probe to source responses.

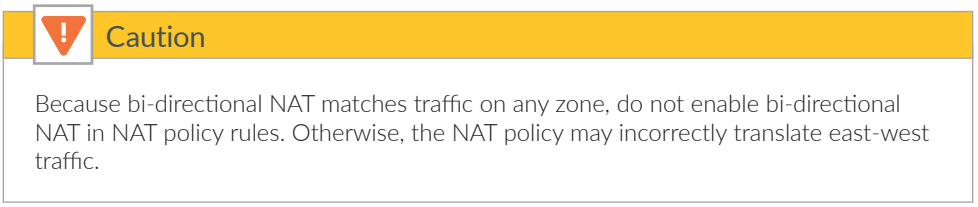
Outbound Traffic

For outbound traffic, an internal load-balancer distributes traffic to the firewalls. User-defined routes on the private subnets direct traffic to the load-balancer's frontend IP address, which shares a subnet with the firewall private interfaces. Load-balancer rules forward all TCP and UDP ports to the firewalls. Common ports required for outbound traffic include UDP/123 (NTP), TCP/80 (HTTP), and TCP/443 (HTTPS). DNS is not needed, because virtual machines communicate to Azure name services directly through the Azure network fabric. The internal load-balancer's health probes monitor firewall availability through the HTTPS service enabled in the interface management profile. Connectivity to

the HTTPS service is limited to traffic sourced from the health probe IP address.

The private interface uses a dedicated virtual router. Static routes are defined for the health probe IP address and private network range out the private interface. Additionally, a static default route forwards traffic to the virtual router dedicated to the public interface.

The firewall applies source NAT to outbound traffic. When the outbound traffic originates from a resource that is associated with a public IP address, source NAT translates outbound traffic to the FQDN address object. For private resources not associated with a public IP address, the firewall translates the source address to its public interface. An Azure public IP address is associated with each firewall's public interface which is required when the interface is also associated with an inbound public load-balancer's backend pool.



The firewall security policy allows appropriate application traffic from the resources in the private network to the internet. You should implement the security policy by using positive security policies (whitelisting). Security profiles prevent known malware and vulnerabilities from entering the network in return traffic allowed in the security policy. URL filtering, file blocking, and data filtering protect against data exfiltration.

East-West Traffic

East-west traffic, or traffic between private subnets, uses the same internal load-balancer to distribute traffic to the firewalls as the outbound traffic. User-defined routes to the private network subnets are applied to the private subnets and direct traffic to the load-balancer's frontend IP address. The existing load-balancer rules for outbound traffic apply to east-west traffic as well, and apply to all TCP and UDP ports.

The firewall should not translate the destination for traffic between private subnets. Like inbound traffic, source NAT is required for return traffic to flow symmetrically. A positive control security policy should allow only appropriate application traffic between private resources and requires that the default intrazone security policy rules be overridden and modified to deny traffic. Security profiles should also be enabled to prevent known malware and vulnerabilities from moving laterally in the private network through traffic allowed in the security policy.

Backhaul and Management Traffic

User-defined routes applied to the gateway subnet direct traffic that has a destination in the private network range to the internal load-balancer with an additional frontend IP dedicated to incoming traffic from the backhaul connection. The load-balancer then distributes traffic to a new backend pool with dedicated interfaces on the firewalls. Dedicated firewall interfaces are used for the backhaul traffic because they allow for enhanced security policies that can take zone into account.

On the firewall, a dedicated virtual router for the backhaul interface and static routes provides reachability to the on-site networks and health probe IP address. Static routes on both the backhaul and private virtual routers provide bi-directional traffic flow between the on-site and private network ranges. Traffic originating in private subnets and destined to on-site networks follows the same path as east-west traffic. All that is required is the addition of user-defined routes that forward on-site network ranges to the outbound/east-west load-balancer frontend.

Traffic from the on-site networks communicates to the management subnet directly. This allows on-site administrators to manage the firewalls even when a misconfiguration occurs in user-defined routing or load-balancers.

User-defined routes blackhole the traffic to the on-site networks from public subnets by sending the traffic to a next-hop of *none*.

Assumptions and Prerequisites

Microsoft Azure:

- Your organization has a valid active subscription associated with your Azure user account.
- Two resource groups are used—one for Panorama and common resources and a separate resource group for dataplane devices
- Uses Standard-SKU IP addresses and load-balancers, except where specifically noted in the guide.
- Only IPv4 networking is used.
- Web servers for inbound traffic are already deployed with their own dedicated load-balancer.
- Business and DB servers are already deployed.
- If you are using the application gateway for SSL, then you must have a web server public certificate with bundled private key.
- If you are using the application gateway for SSL and intend on re-encrypting on the backend from the application gateway to the web servers, you must have a common web server certificate for the servers in the SSL web server backend pool.

Palo Alto Networks next-generation firewalls and Panorama:

- Device configuration is centrally managed with Panorama using templates and device groups.
- Panorama will be deployed on Azure in management-only mode.
- Firewall logging uses the Palo Alto Networks cloud-based Logging Service.
- The PAN-OS version tested in this deployment guide is 8.1.5 for all devices.
- The Cloud services plugin for Panorama is 1.2.0-h2.
- The on-premise firewalls for backhaul traffic are already deployed with a set of interfaces connected to the public and private zones and integrated into the on-premise dynamic routing protocol.

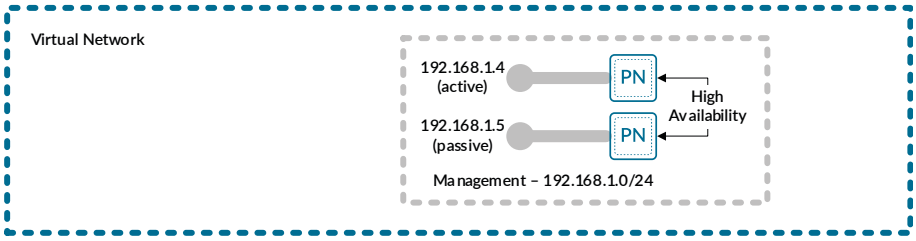
Palo Alto Networks licensing:

- Your organization has a Panorama license for the current and expected number of managed VM-Series firewalls.
- Sufficient VM-Series licensing for the current and expected number of VM-Series firewalls. This guide assumes you are using the BYOL licensing option.
- Requires a bundled auth-key for VM-Series if you intend to use bootstrapping.
- Logging Service instance is provisioned with sufficient storage to support the required data retention period and auth-code has been issued.
- Logging Service region used is americas.

Deployment Details for Panorama

Panorama is deployed in a new dedicated Azure Resource Group which includes the VNet used for the common firewall option. You must complete two complementary procedure groups in order to deploy Panorama. The first procedure group configures the Azure environment. Once Azure is configured, then Panorama may be deployed.

Figure 6 Panorama high-availability mode deployed on Azure



Several of the resources created on Azure are used by procedures later in this guide When the resource already exists, you will be instructed to modify an existing resource rather than create a new resource.

Procedures

Creating and Configuring Azure Common Resources

1.1 Create the Resource Group

1.2 Create the Virtual Network

1.3 Create the Public IP Address for Panorama

1.4 Create and Apply the Network Security Group

1.5 Create Whitelist Network Security Group

1.6 Create the Availability Set

1.7 Create the Storage Account

1.8 Verify Resource Creation Completed

The following procedures are completed using the Azure Resource Manager. Sign in to Azure at https://portal.azure.com.

> **Note**
>
> Some Azure templates provide an option to create a new resource when needed at deployment time and other templates require resources to be created in advance. Where possible, this guide creates the resource in advance and then references the existing resource at deployment time.

This procedure group creates the resources listed in the following table as preparation for deploying Panorama.

Table 1 Azure resources required for deployment

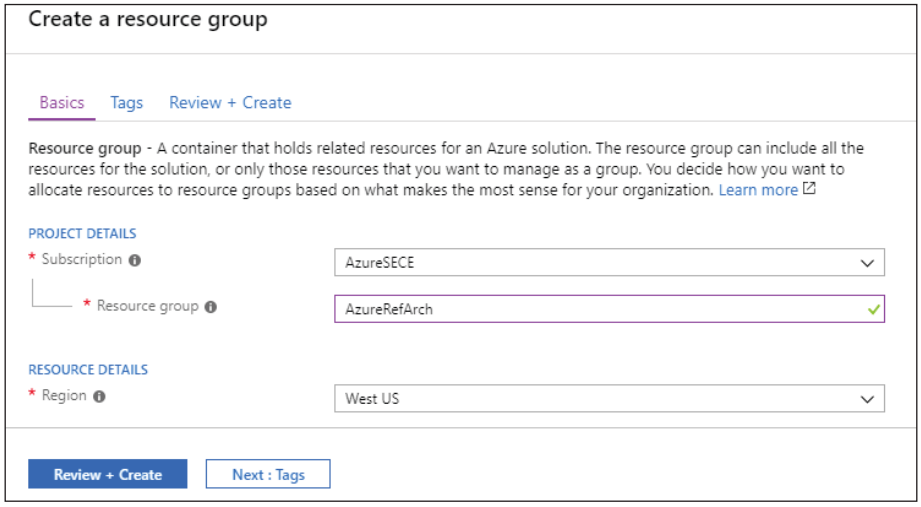
Parameter	Value	Comments
Resource group	AzureRefArch	—
Subscription	<value>	Must have a valid Azure subscription
Resource group location	<location>	Tested in West US
Virtual network	AzureRefArch-VNET	—
Public IP for Panorama management (primary)	Azure-Panorama-1	Panorama, or primary Panorama when using Panorama High Availability
Public IP for Panorama management (secondary)	Azure-Panorama-2	Optional—secondary Panorama when using Panorama High Availability
Availability set	AzureRefArch-AS	Suggested if planning for Panorama High Availability
Diagnostics storage account	azurerefarchv2diag	—

1.1 Create the Resource Group

All resources deployed in this guide should use the same location. The deployment in this guide was tested in **West US**.

Step 1: In **Home > Resource groups**, click **Add**.

Step 2: In the **Resource group** box, enter **AzureRefArch** and select the desired value for the region. Click **Review + Create**.



Step 3: On the next screen, click **Create**.

1.2 Create the Virtual Network

You create the VNet with an initial IP address space and a subnet that must be within the IP address space. You can modify the VNet after creation to add additional IP address space and subnets. Only the first entry in the following table is configured in this procedure.

Table 2 Virtual network IP addressing and subnets

Address space	Subnet	Address range	Comments
192.168.1.0/24	Management	192.168.1.0/24	Initial address space, subnet, and range
172.16.0.0/23	CommonFW-AppGW-Public CommonFW-Public	172.16.0.0/24 172.16.1.0/24	Configured in separate procedures
10.5.0.0/16	CommonFW-Private CommonFW-Web CommonFW-Business CommonFW-DB CommonFW-VPN	10.5.0.0/24 10.5.1.0/24 10.5.2.0/24 10.5.3.0/24 10.5.15.0/24	Configured in separate procedures

Step 1: In **Home > Virtual networks**, click **Add.**

Step 2: In the **Name** box, enter **AzureRefArch-VNET**.

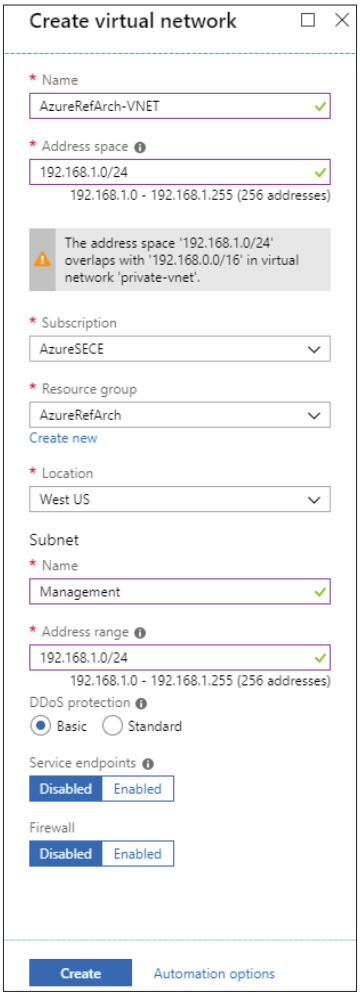
Step 3: In the **Address space** box, enter **192.168.1.0/24**.

> **Note**
>
> Azure Resource Manager provides a warning if the proposed address space overlaps with address space already assigned in another VNet within the same subscription. These warnings can be ignored if communication between these VNets is not required. Otherwise, choose a different non-overlapping address space.

Step 4: In the Resource Group list, select **AzureRefArch**.

Step 5: In the Subnet section's **Name** box, enter **Management**.

Step 6: In the Subnet section's **Address Range** box, enter **192.168.1.0/24**, and then click **Create**.



1.3 Create the Public IP Address for Panorama

The Panorama virtual machines deployed on Azure are managed using public IP addresses unless on-site network connectivity has been established. The process to configure on-site network connectivity is included later in this guide.

This procedure creates a public IP address that is associated with the management interface of the primary Panorama system at deployment time. If necessary, this procedure is repeated to create an additional public IP address for the secondary Panorama system. The parameters listed in Table 1 are used to complete this procedure.

> **Note**
>
> This guide uses Standard-SKU IP addresses in all procedures except where specifically noted.

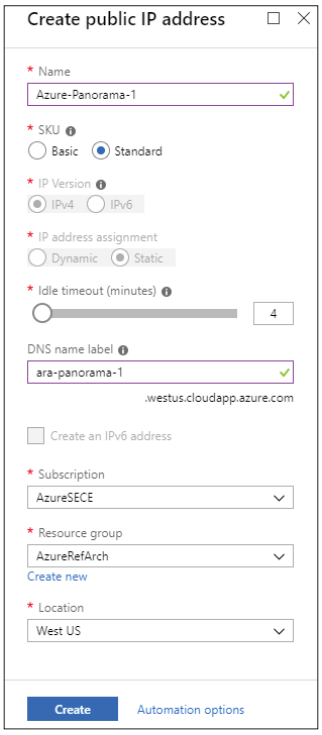
Take note of the fully qualified domain name (FQDN) that is defined by adding the location specific suffix to your DNS name label. We recommend managing your devices by using the DNS name rather than the public IP address, which may change.

Step 1: In **Home > Public IP addresses**, click **Add.**

Step 2: In the **Name** box, enter **Azure-Panorama-1**.

Step 3: Under SKU, select **Standard**.

Step 4: In the **DNS name label** box, enter **ara-panorama-1**. In the **Resource Group** list, select **AzureRefArch**, and then click **Create**.



1.4 Create and Apply the Network Security Group

Azure requires that a network security group (NSG) must be applied on a subnet or NIC of your virtual machine resource or traffic is not permitted to reach the resource when Standard SKU public IP addresses are associated with the resource.

Note

This guide uses Standard-SKU IP addresses in all procedures except where specifically noted.

This procedure creates NSGs for use with the management subnet. Each NSG includes default rules that allow for traffic within the VNET and from the Azure load balancer health probes.

Step 1: In **Home > Network Security groups**, click **Add.**

Step 2: In the **Name** box, enter **AllowManagement-Subnet**.

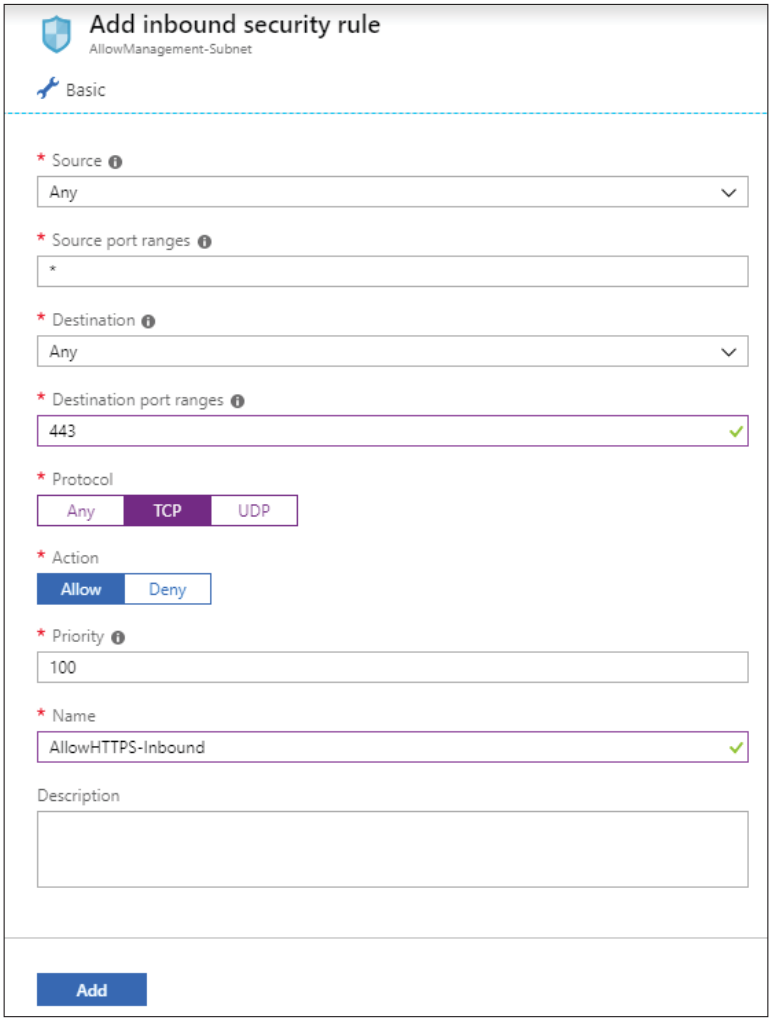
Step 3: In the **Resource Group** list, select **AzureRefArch**.

Step 4: In **Home > Network security groups > AllowManagement-Subnet**, in the Settings section, click **Inbound security rules**, and then click **Add**. The Add inbound security rule pane appears.

Step 5: In the **Destination port ranges** box, enter **443**.

Step 6: In the **Protocol** section, select **TCP**.

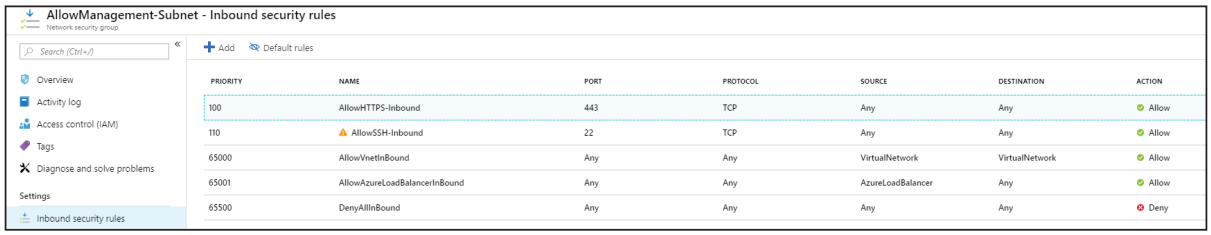
Step 7: In the **Name** box, enter **AllowHTTPS-Inbound**, and then click **Add**.



Step 8: Repeat Step 4 through Step 7, with the following values:

- **Destination port ranges**—**22**
- **Priority**—**110**
- **Name**—**AllowSSH-Inbound**

> **Note**
>
> Azure presents warning messages when the NSG rules expose various ports to the Internet. We advise using more restrictive rules outside of a testing environment.

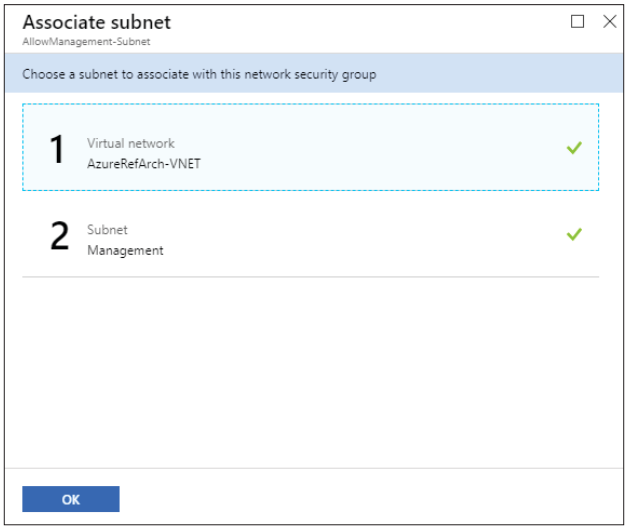


Step 9: In **Home > Network security groups > AllowManagement-Subnet**, in the Settings section, click **Subnets**.

Step 10: In the **AllowManagement-Subnet—Subnets** pane, click **Associate**.

Step 11: Click the **Virtual network—Choose a virtual network** section. From the **Choose virtual network** list, select **AzureRefArch-VNET**.

Step 12: Click the **Subnet—Choose a subnet** section. From the **Choose subnet** list, select **Management**, and then click **OK**.



1.5 Create Whitelist Network Security Group

Some virtual machines require the application of an NSG at deployment time. Because a subnet NSG is already applied, it is not necessary to apply additional rules to the virtual machine NIC. In this procedure, you create a whitelist NSG, which is applied to virtual machines as they are deployed. When NSGs are applied at both the subnet and NIC level, the security rules are merged.

Step 1: In **Home > Network Security groups**, click **Add.**

Step 2: In the **Name** box, enter **AllowAll-NIC**.

Step 3: In the **Resource Group** list, select **AzureRefArch**.

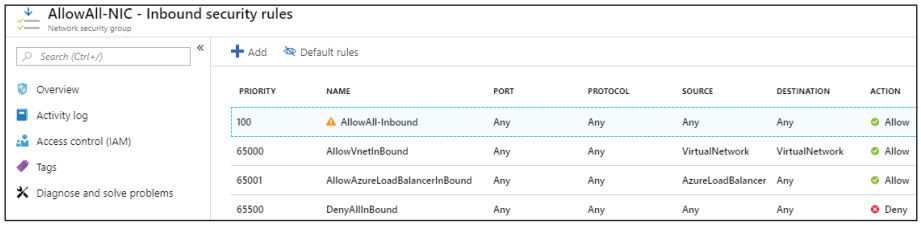
Step 4: In **Home > Network security groups > AllowAll-NIC**, in the Settings section, click **Inbound security rules**, and then click **Add**. The Add inbound security rule pane appears.

Step 5: In the **Destination port ranges** box, enter *.

Step 6: In the **Priority box**, enter **100**.

Step 7: In the **Name** box, enter **AllowAll-Inbound**, and then click **Add**.

> **Note**
>
> Azure presents warning messages when the Network Security Group rules expose various ports to the Internet.



1.6 Create the Availability Set

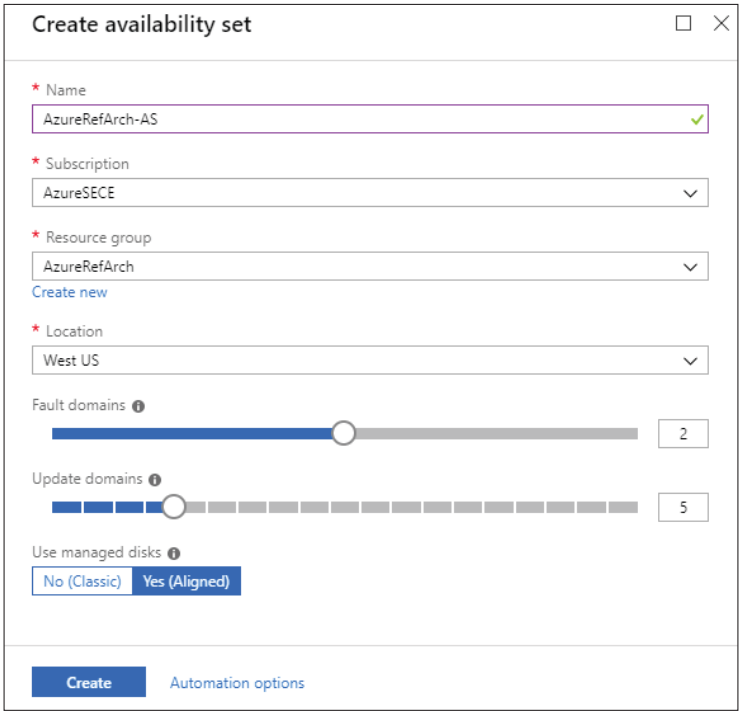
The Panorama high-availability model benefits from the use of an availability set with two fault domains. This ensures that the primary and secondary Panorama systems are deployed on different fault domains.

> **Note**
>
> You can configure an availability set on a virtual machine only during its initial deployment. You can't modify a virtual machine's availability-set configuration after the virtual machine is deployed.

Step 1: In **Home > Availability sets**, click **Add.**

Step 2: In the **Name** box, enter **AzureRefArch-AS**.

Step 3: In the Resource Group section, select **AzureRefArch**, and then click **Create**.



1.7 Create the Storage Account

Panorama and other resources require general purpose storage for diagnostics and bootstrapping.

Step 1: In **Home > Storage accounts**, click **Add.**

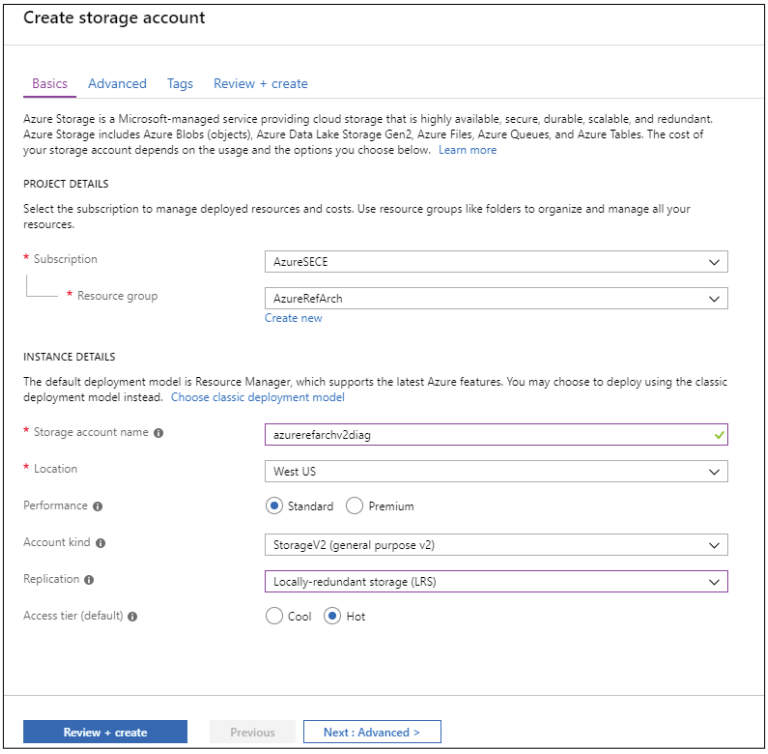
Step 2: In the **Resource Group** list, select **AzureRefArch**.

Step 3: In the **Storage account name** box, enter **azurerefarchv2diag**.

Step 4: In the **Account kind** list, select **StorageV2 (general purpose v2)**.

Step 5: In the **Replication** list, select **Locally-redundant storage (LRS)**.

Step 6: Click **Review + create**.

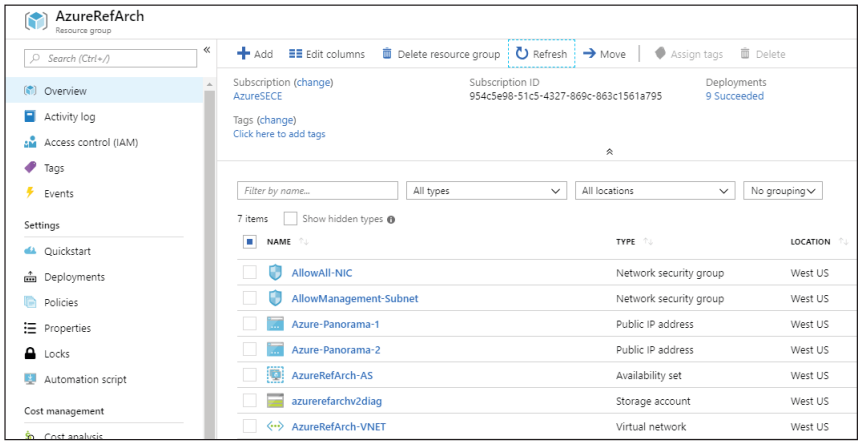


Step 7: On the next screen, after validation passes, click **Create**.

1.8 Verify Resource Creation Completed

Some Azure deployments are time consuming, and if any resources are missing, the deployment fails. It is quicker to verify that all of the necessary resources exist before proceeding with a deployment than waiting until a deployment fails.

Step 1: In **Home > Resource Groups**, select **AzureRefArch**.



Step 2: Verify that the resource group, NSGs, public IP addresses, availability set, storage account, and VNet have been successfully created.

Procedures

Deploying Panorama on Azure

The following procedures use the Azure Resource Manager and the Panorama device portal. Sign in to Azure at https://portal.azure.com. Details on how to access Panorama after deployment are included in the relevant procedures.

This procedure deploys Panorama in management mode. Panorama defaults to management mode when it detects that there is not sufficient log storage capacity to run in Panorama mode.

Table 3 Panorama deployment parameters

Parameter	Value	Comments
Name	Azure-Panorama-1 Azure-Panorama-2	Primary system Secondary system (optional for high availability)
VM disk type	Standard HDD	Required for D3_v2 Standard.
Username	refarchadmin	May not use “admin”
Authentication type	<password>	Complex password required
Subscription	<value>	Must have a valid Azure subscription
Resource group name	Use existing AzureRefArch	—
Location	<location>	Tested in West US
Panorama VM size	D3_v2 Standard	Setup Prerequisites for the Panorama Virtual Appliance

Table continued on next page

Continued from previous page

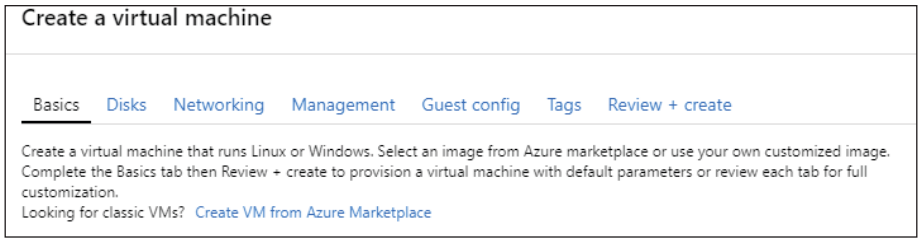
Parameter	Value	Comments
Availability set	AzureRefArch-AS	Recommend to use Availability Set if planning for active/standby Panorama. Cannot change setting after deployment.
Storage Use managed disks	Yes	—
Virtual Network	AzureRefArch-VNET	—
Subnet	Management	—
Public IP	Azure-Panorama-1 Azure-Panorama-2	DNS configured as: ara-panorama-1 DNS configured as: ara-panorama-2
Network security group	AllowAll-NIC	NSG is applied at subnet level
Auto-shutdown	No	—
Monitoring boot diagnostics	On	—
Diagnostics storage account	azurerefarchv2diag	—

2.1 Create Panorama Virtual Machine

Use the parameters in Table 3 to deploy Panorama.

Step 1: In **Home > Virtual machines**, click **Add.**

Step 2: Click **Create VM from Azure Marketplace**.



Step 3: In the **Search compute** box, enter **Panorama**, and then and press Enter to search.

Step 4: In the search results, click **Panorama (BYOL)**.

Step 5: In **Home > Virtual machines > Create a virtual machine > Marketplace > Panorama (BYOL)**, click **Create**.

Step 6: In the **Resource Group** list, select **AzureRefArch**.

Step 7: In the **Virtual machine name** box, enter **Azure-Panorama-1**.

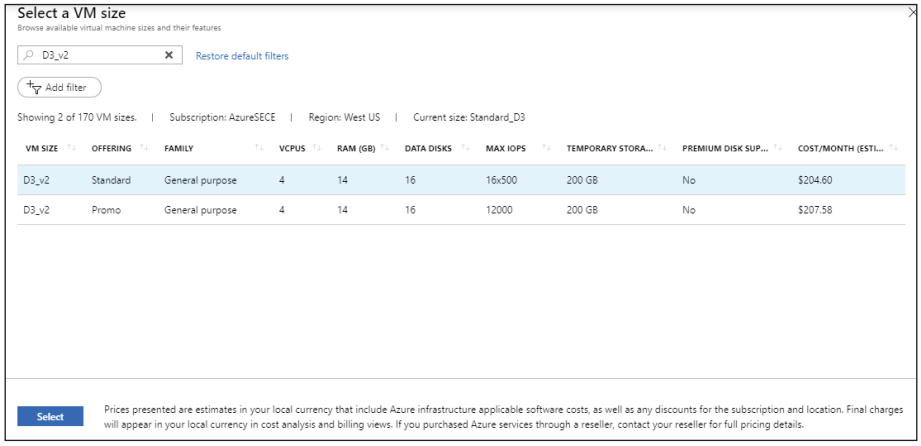
Step 8: In the **Availability options** list, select **Availability set**.

Step 9: In the **Availability set** list, select **AzureRefArch-AS**.

Step 10: In the Size section, click **Change size**.

Step 11: In the Select a VM Size pane, in the **Search** box, enter **D3_v2** to search.

Step 12: Click the **D3_v2 Standard** row, and then click **Select**.

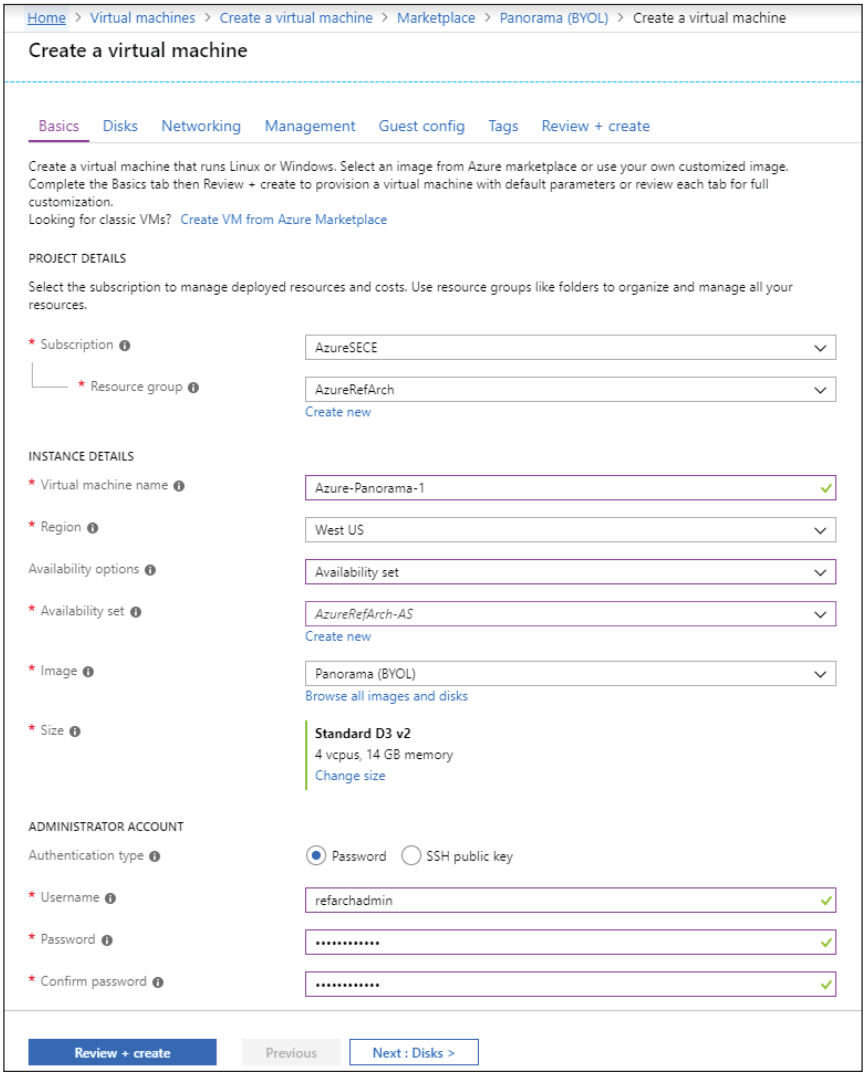


Step 13: For **Authentication type**, select **Password**.

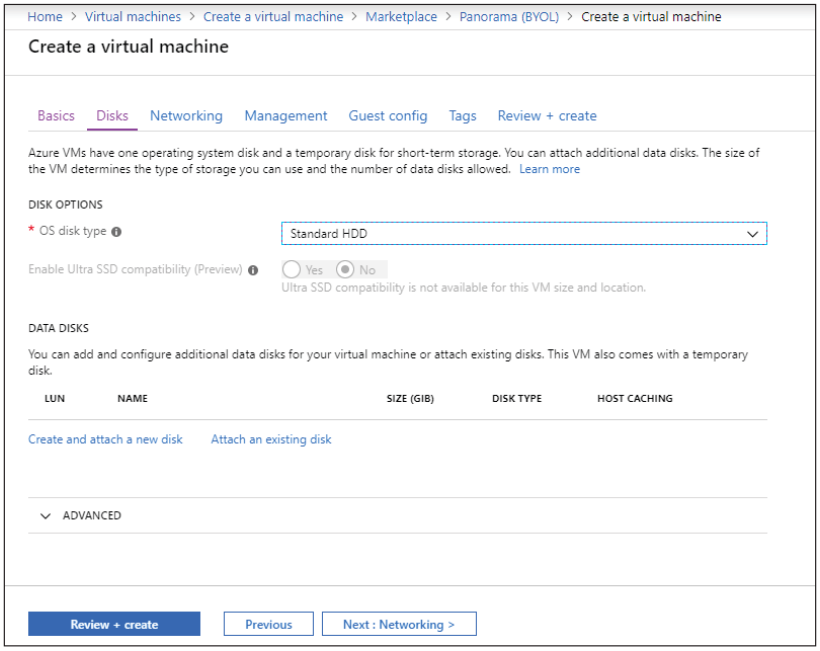
Step 14: In the **Username** box, enter **refarchadmin**.

Step 15: For **Authentication type**, select **Password**.

Step 16: In the **Password** and **Confirm Password** boxes, enter the password, and then click **Next: Disks>**.



Step 17: In the **OS disk type** list, select **Standard HDD**, and then click **Next: Networking>**.



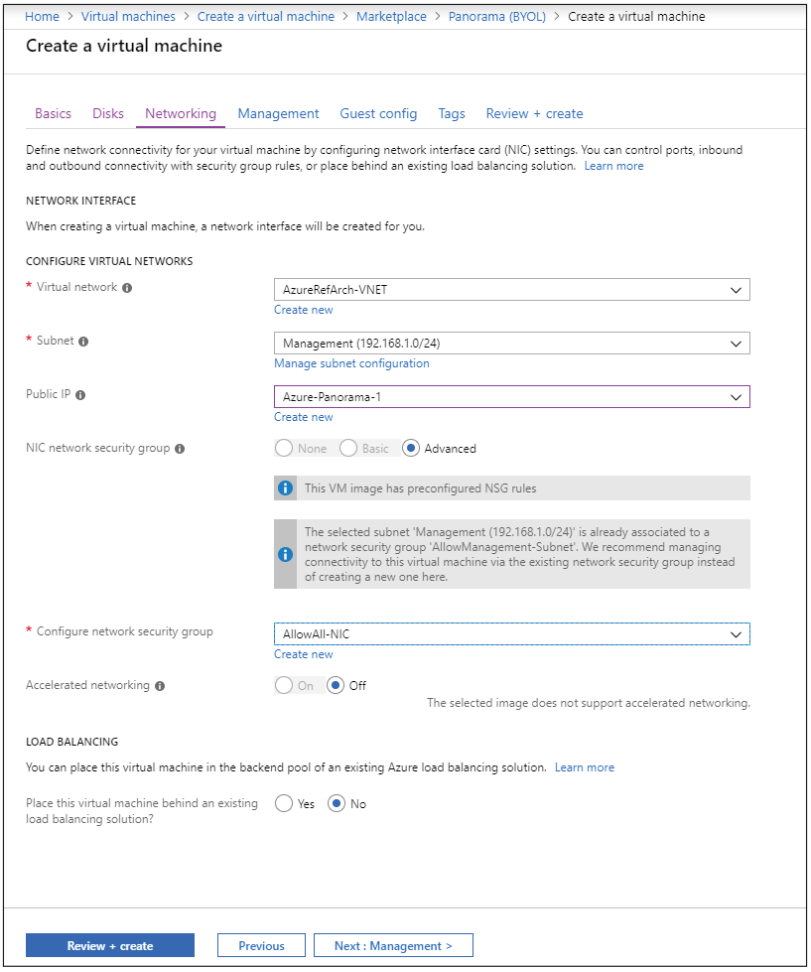
Step 18: In the **Virtual network** list, select **AzureRefArch-VNET**.

Step 19: In the **Subnet** list, select **Management (192.168.1.0/24)**.

Step 20: In the **Public IP** list, select **Azure-Panorama-1**.

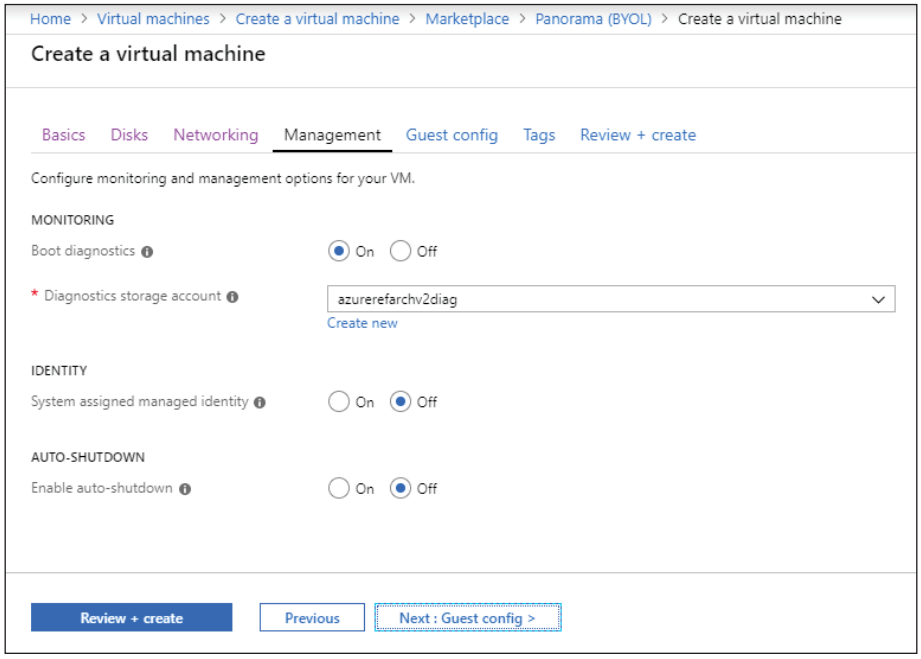
Step 21: In the **Configure network security group** list, select **AllowAll-NIC** for resource group **AzureRefArch**. The subnet already has an associated NSG.

Step 22: Click **Next: Management>**.



Step 23: For Boot diagnostics, select **On**.

Step 24: In the Diagnostics storage account list, select **azurerefarchv2diag**, and then click **Review + create**.



Step 25: After validation passes, review the **Product Details**, **Terms of use** and **Summary** sections. If the information is correct and acceptable, then click **Create**.

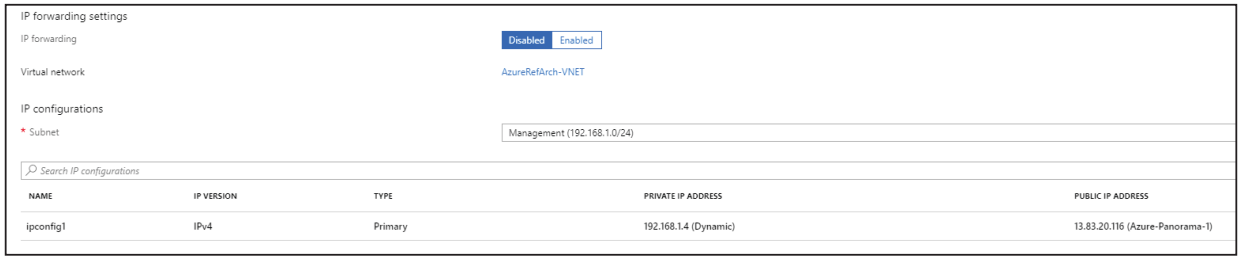
2.2 Change Azure Assigned IP Address from Dynamic to Static

You must configure Panorama with a static IP address. Azure networking provides the IP address to Panorama using DHCP but by default is configured to use dynamic assignment. If the current IP address is acceptable, convert the address assignment to static. To change the IP address, convert the assignment to static and then assign an available address. Any IP address changes require a restart of the Panorama virtual machine.

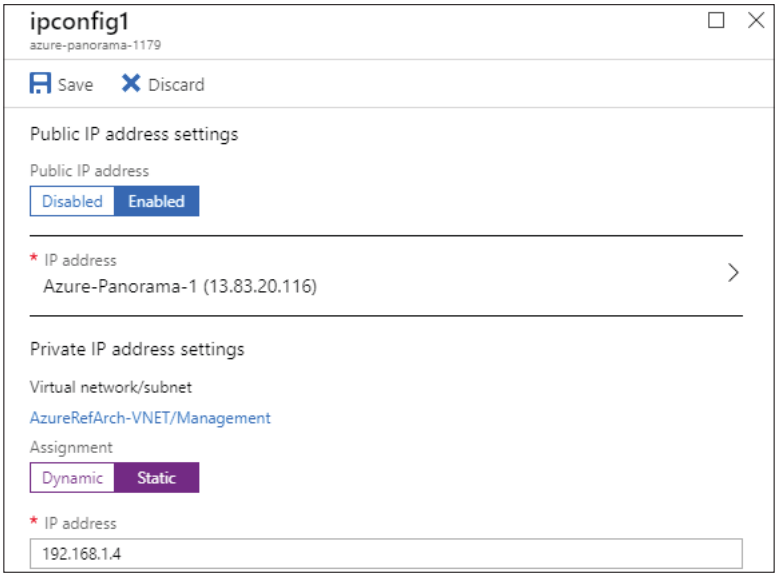
Step 1: In **Home > Virtual machines >** **Azure-Panorama-1**, click **Networking**.

Step 2: Click the **Network interface** name (example: **azure-panorama-1179**).

Step 3: Click **IP configurations**.



Step 4: Click the IP configuration row to edit the settings.



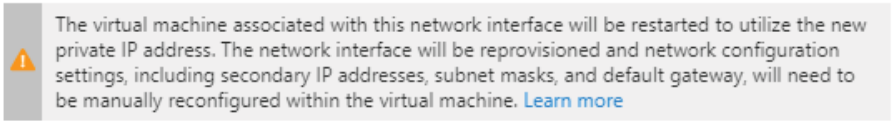
Step 5: In the Private IP address settings section, click **Static** to convert from dynamic to static configuration.

Step 6: If you want to change the static IP address to a preferred value, in the **IP address** box, enter a new IP address. The chosen IP address must be unassigned in Azure.

Caution

Changing an IP address forces a restart of the virtual machine.

Step 7: Click **Save**. If you changed the IP address, the below message appears and the virtual machine restarts.



2.3 License Panorama on Azure

Panorama is now running on Azure but is unlicensed and using a factory default configuration. Based on the size selected for the Panorama virtual machine, the **System Mode** is management-only.

This procedure assumes that you have a valid serial number for your Panorama device(s) and that registration on the customer support portal (https://support.palotaltonetworks.com) is complete.

Step 1: Log in to Panorama (example: https://ara-panorama-1.westus.cloudapp.azure.com)

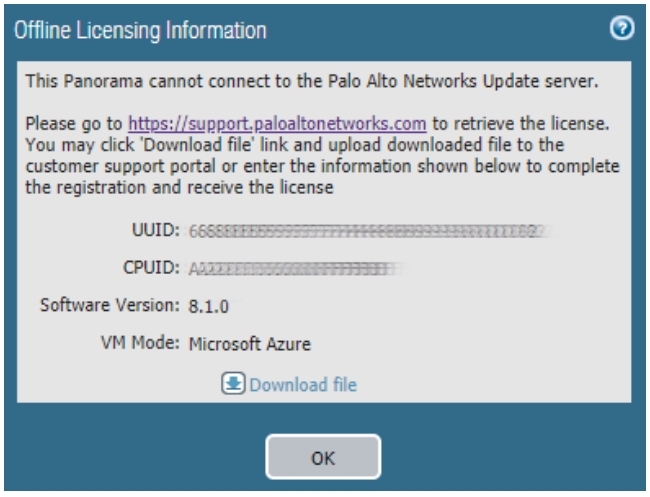
You will see a series of dialog boxes and warnings.

Step 2: On the There are no device groups dialog box, click **OK**.

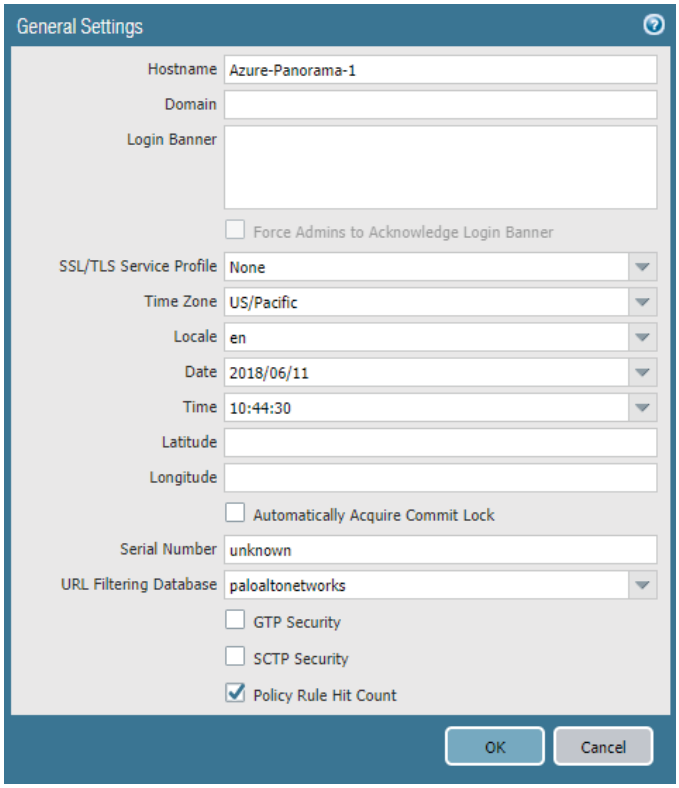
Step 3: On the Retrieve Panorama License dialog box, click **OK** .

Step 4: On the next Retrieve Panorama License dialog box, click **Complete Manually**.

Step 5: On the Offline Licensing Information dialog box, click **OK** .



Step 6: In **Panorama > Setup > Management > General Settings**, click the Edit cog.



Step 7: In the **Domain** box, enter the domain suffix.

Step 8: In the **Time Zone** list, select the appropriate time zone (example: **US/Pacific**).

Step 9: In the **Serial Number** box, enter the serial number from the customer support portal, and then click **OK**.

Step 10: In **Panorama > Setup > Services**, click the Edit cog.

Step 11: In the **Primary DNS Server** box, enter **168.63.129.16.**

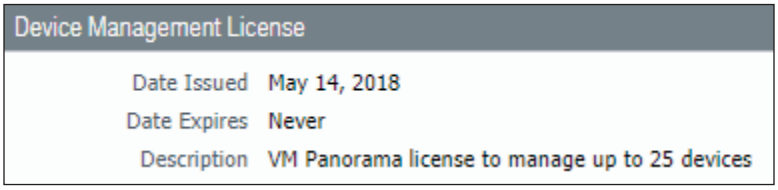
Step 12: On the NTP tab, in the Primary NTP Server section **NTP Server Address** box, enter **0.pool.ntp.org**.

Step 13: In the Secondary NTP Server section **NTP Server Address** box, enter **1.pool.ntp.org, and then** click **OK**.

Step 14: On the **Commit** menu, click **Commit to Panorama**.

Step 15: In **Panorama > Licenses**, click **Retrieve license keys from license server**.

Step 16: Verify **Device Management License** is active.



2.4 Update Panorama Software to Recommended Version

Step 1: Navigate to **Panorama > Software**.

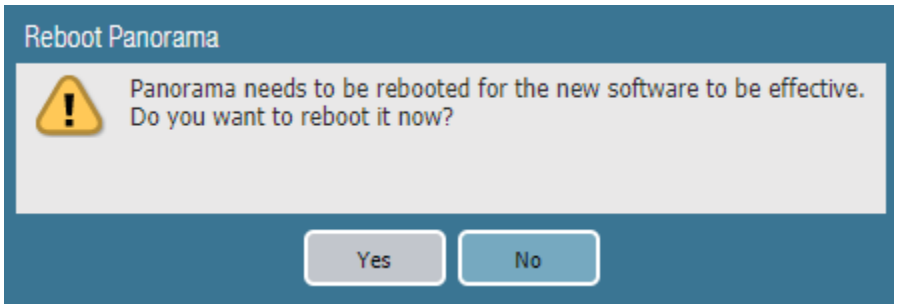
> **Note**
>
> If you receive an **Operation Failed** warning with the message **No update information available**, you may click **Close** to acknowledge. No action is required.

Step 2: In **Panorama > Software**, click **Check Now**.

Step 3: For version **8.1.5**, in the **Actions** column, click **Download**, and when it's complete, click **Close**.

Step 4: After the status in the **Available** column has changed to **Downloaded**, and then in the **Action** column, click **Install**.

Step 5: When prompted to Reboot Panorama, click **Yes**.



2.5 Configure Panorama High Availability

(Optional)

This procedure is necessary only to deploy Panorama in a high availability configuration. Panorama supports an HA configuration in which one peer is the active-primary and the other is the passive-secondary. If a failure occurs on the primary peer, it automatically fails over and the secondary peer becomes active.

The Panorama HA peers synchronize the running configuration each time you commit changes on the active Panorama peer. The candidate configuration is synchronized between the peers each time you save the configuration on the active peer or just before a failover occurs.

Settings that are common across the pair, such as shared objects and policy rules, device group objects and rules, template configuration, and administrative access configuration, are synchronized between the Panorama HA peers.

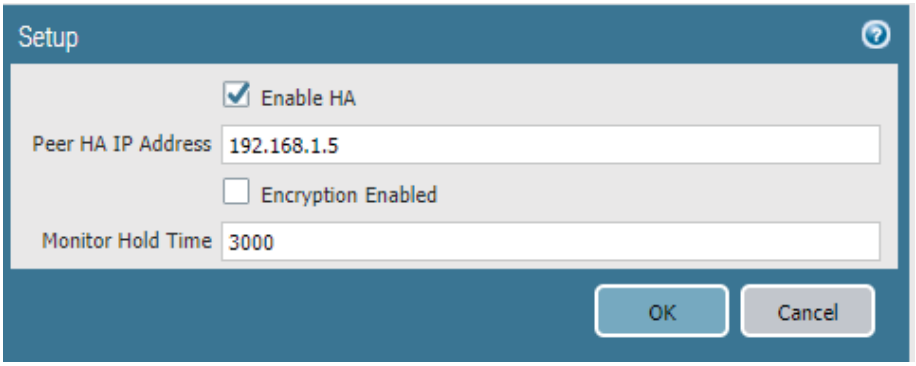
Several conditions must be met in order to configure Panorama high availability. Each Panorama system must run the same software version and have the same firewall management capacity license, and if Panorama plugins are used, the plugins must be the same version.

Perform Step 1 through Step 6 on the primary Panorama.

Step 1: In **Panorama > High Availability > Setup**, click the Edit cog.

Step 2: Select **Enable HA**.

Step 3: In the **Peer HA IP Address** box, enter **192.168.1.5**, and then click OK.



Step 4: In **Panorama > High Availability > Election Settings**, click the Edit cog.

Step 5: In the Priority list, select **primary**, and then click **OK**.

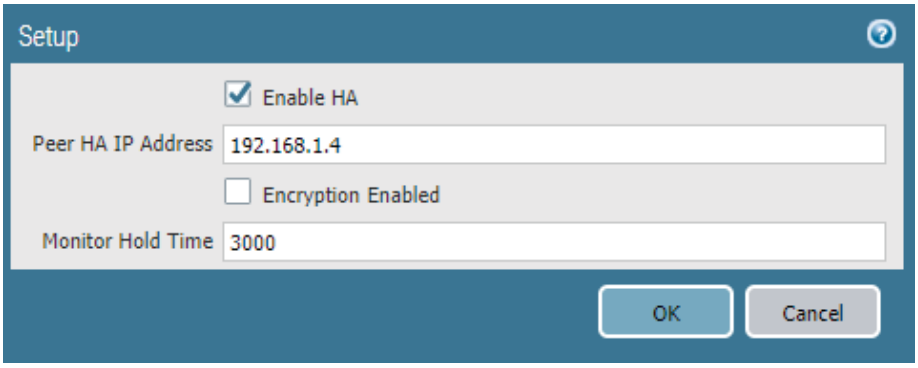
Step 6: On the **Commit** menu, click **Commit to Panorama**.

Perform Step 7 through Step 12 on the secondary Panorama.

Step 7: In **Panorama > High Availability>Setup**, click the Edit cog.

Step 8: Select **Enable HA**.

Step 9: In the **Peer HA IP Address** box, enter **192.168.1.4**, and then click OK.

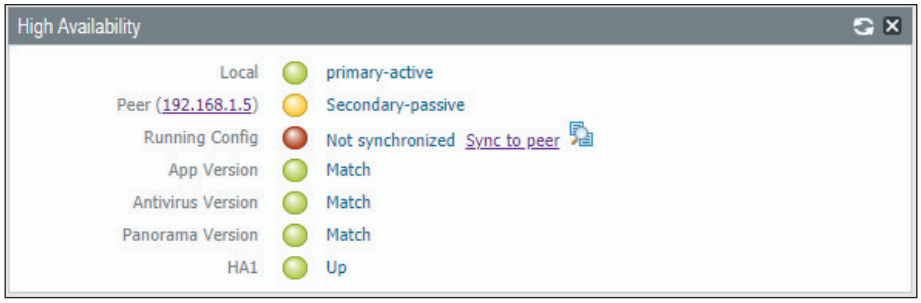


Step 10: In **Panorama > High Availability > Election Settings**, click the Edit cog.

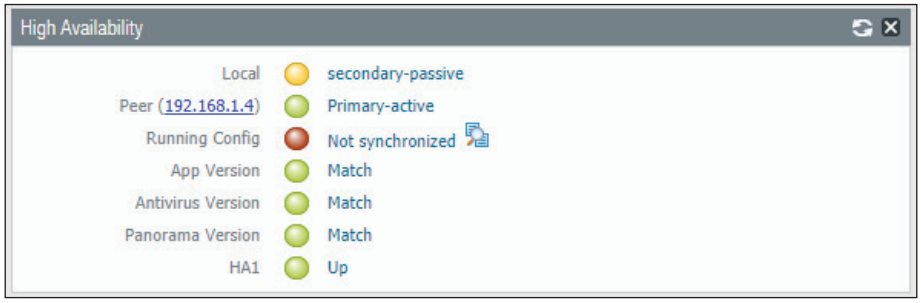
Step 11: In the **Priority** list, select **secondary**, and then click **OK**.

Step 12: On the **Commit** menu, click **Commit to Panorama**.

Step 13: On the primary Panorama, in **Dashboard > Widgets > System**, click **High Availability** to enable the **High Availability** dashboard widget. This adds a dashboard pane that displays the status of the Panorama peers.



Step 14: Repeat Step 13 on the secondary Panorama.



Step 15: On the primary Panorama, in **Dashboard > High Availability**, click **Sync to peer**.

Step 16: Click **Yes** to accept the **Overwrite Peer Configuration** warning and proceed with the synchronization.

2.6 Activate Logging Service

The Logging Service requires an authorization code, which is used to activate the service. This procedure also assumes that you have a valid serial number for your Panorama device(s) and that registration on the customer support portal is complete.

The Logging Service instance is associated with the serial number of the primary Panorama. This procedure is not repeated for the secondary Panorama.

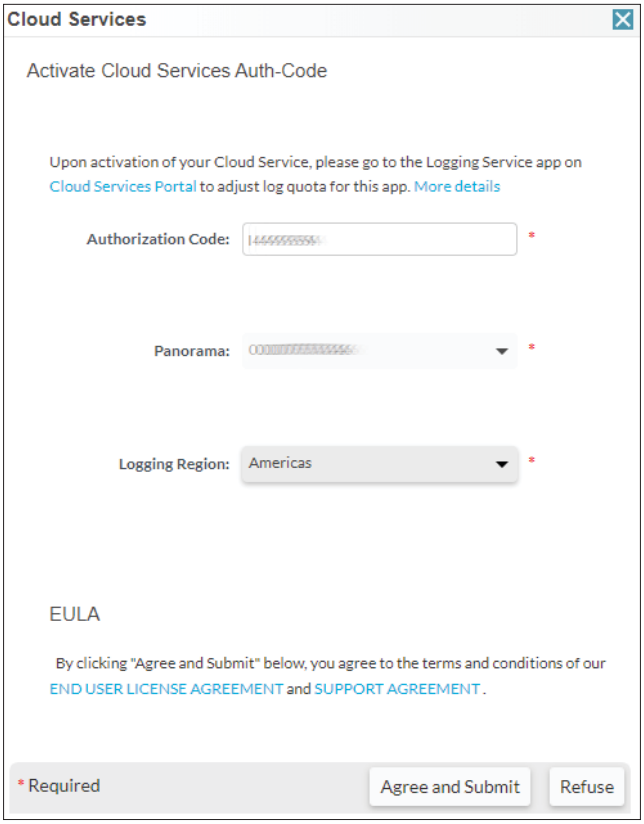
Step 1: Log in to the Customer Support Portal at https://support.paloaltonetworks.com.

Step 2: Select **Assets > Cloud Services**, and then click **Activate Cloud Services Auth-Code**.

Step 3: In the Cloud Services window, in the **Authorization Code** box, enter the authorization code (example: **I7654321**), and then press Tab key to advance. The **Panorama** and **Logging Region** boxes appear.

Step 4: In the Cloud Services window, in the **Panorama** list, select the value that corresponds to the serial number assigned to your primary Panorama.

Step 5: In the Cloud Services window, in the **Logging Region** list, select the value that corresponds to your region (example: **Americas**).



Step 6: Accept the EULA by clicking on **Agree and Submit**.

2.7 Install Cloud Services Plugin

If running Panorama in high availability mode, perform this procedure on the primary Panorama first. Then repeat this procedure for the secondary Panorama.

Step 1: In **Panorama > Plugins**, click **Check Now**.

Step 2: For **cloud_services-1.2.0-h2**, in the **Actions** column, click **Download**.

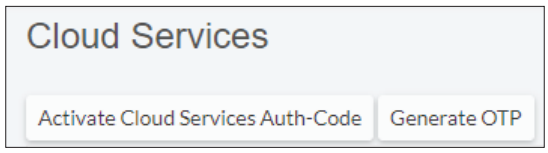
Step 3: After the download is completed, click **Close**.

Step 4: After the status in the **Available** column changes to a check, and then in the **Action** column, click **Install**.

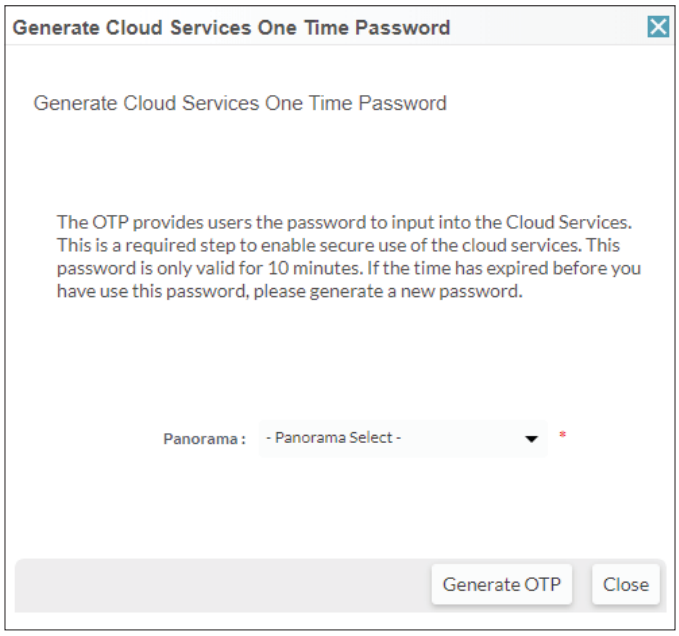
Step 5: Click **OK** to close the dialog box that indicates a successful installation.

Perform Step 6 through Step 8 on the customer support portal (https://support.paloaltonetworks.com) to complete the association of Panorama to the cloud service.

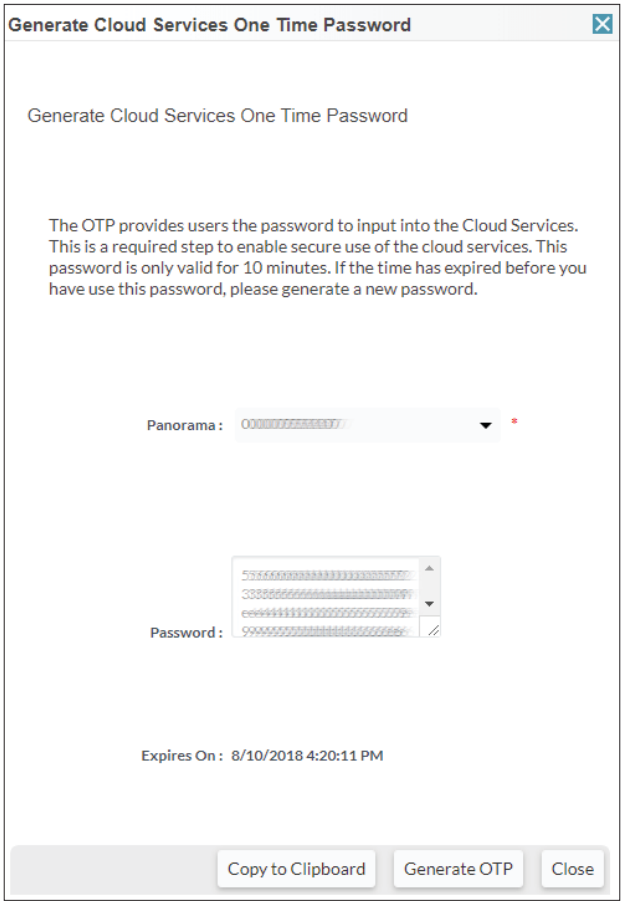
Step 6: In **Assets > Cloud Services**, click **Generate OTP**.



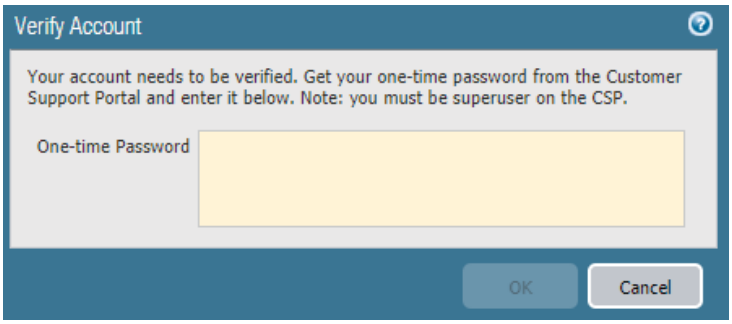
Step 7: In the Generate Cloud Services One Time Password window, in the **Panorama** list, select the serial number for the primary Panorama, and then click **Generate OTP**.



Step 8: In the Generate Cloud Services One Time Password window, click **Copy to Clipboard**.

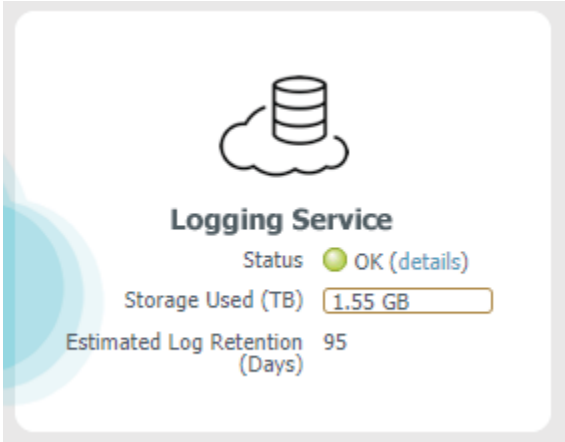


Step 9: On Panorama, navigate to **Panorama > Cloud Services > Status**, and then click **Verify**.



Step 10: In the **One-Time Password** box, paste the OTP that was generated from the Customer Support Portal.

Step 11: In **Panorama > Cloud Service > Status**, verify the status.



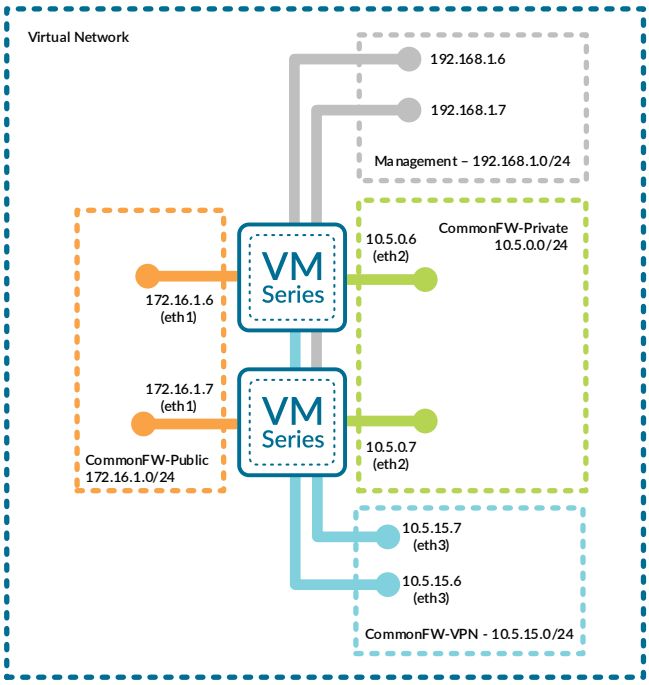
Step 12: If necessary, repeat this procedure for the secondary Panorama.

Deployment Details for VM-Series

You deploy the VM-Series firewalls in a new dedicated Azure Resource Group for the common firewall option. Some Azure resources, such as the VNet, have already been allocated within the Azure Resource Group used for Panorama. You must complete multiple complementary procedure groups in order to deploy and configure the VM-Series.

The first procedure group modifies and configures the Azure environment. After Azure is configured, the second procedure group deploys the VM-Series and minimally configures each device to prepare for central management through Panorama.

Figure 7 Common firewall option—VM-Series deployment parameters



The third procedure group configures the Panorama configuration templates used by the each of VM-Series devices. All template based configuration is common across all VM-Series devices and only takes effect once pushed from Panorama to the VM-Series. After the templates are complete, the fourth procedure group registers the individual VM-Series devices with Panorama, associates them with the templates and placeholder device groups, pushes the configurations, and refreshes the licenses.

Procedures

Creating and Configuring Azure Common Resource for VM-Series

The following procedures are completed using the Azure Resource Manager. Sign in to Azure at https://portal.azure.com.

Azure has removed the option to select an existing resource group for marketplace solutions that enable multiple NICs. To deploy the firewall into an existing resource group, use the ARM template in the GitHub Repository or your own custom ARM template.

This procedure group creates the resources listed in the following table as preparation for deploying the VM-Series firewalls.

Table 4 Azure resources required for deployment

Parameter	Value	Comments
Virtual network	AzureRefArch-VNET	Existing VNet in the AzureRefArch resource group, in which Panorama is already deployed
Resource Group	AzureRefArch-CommonFW	New resource group specifically for the common firewall option
Storage account	azurerefarchv2commonfw	General purpose storage for VM-Series virtual file systems
Availability set	AzureRefArch-CommonFW-AS	New availability set for the VM-Series in the common firewall option
Public IP for VM-Series 1	aracf-vmfw1	Public IP for management interface
Public IP for VM-Series 2	aracf-vmfw2	Public IP for management interface

3.1 Create Whitelist Network Security Group

Azure requires that an NSG must be applied on a subnet or NIC of your virtual machine resource, or traffic is not permitted to reach the resource when Standard SKU public IP addresses are associated with the resource.

> **Note**
>
> This guide uses Standard-SKU IP addresses in all procedures except where specifically noted.

This procedure creates a whitelist NSG for use with testing, which is applied to all dataplane subnets. The intent of this NSG is to simplify the troubleshooting process during early stages of deployment and testing.

> **Caution**
>
> An Allow-ALL NSG permits access to devices with public IP addresses from the Internet. We advise using more restrictive rules outside of a testing environment.

Step 1: In **Home > Network Security groups**, click **Add.**

Step 2: In the **Name** box, enter **AllowAll-Subnet**.

Step 3: In the **Resource Group** list, select **AzureRefArch**, and then click **Create**.

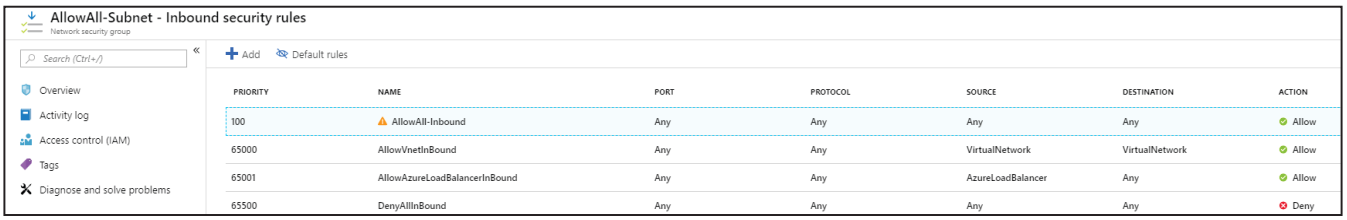
Step 4: In **Home > Network security groups > AllowAll-Subnet**, in the Settings section, click **Inbound security rules**, and then click **Add**. The Add inbound security rule pane appears.

Step 5: In the **Destination port ranges** box, enter *.

Step 6: In the **Priority box**, enter **100**.

Step 7: In the **Name** box, enter **AllowAll-Inbound**, and then click **Add**.

> **Note**
>
> Azure presents warning messages when the Network Security Group rules expose various ports to the Internet.



3.2 Add Address Space and Subnets to the Virtual Network

The existing virtual network (VNet) is modified to add additional IP address space and subnets. The first entry in Table 5 has already been configured in a prior procedure.

Table 5 Virtual network IP addressing and subnets

Address space	Subnet	Address range	Comments
192.168.1.0/24	Management	192.168.1.0/24	Initial address space, subnet and range (already configured).
172.16.0.0/23	CommonFW-AppGW-Public CommonFW-Public	172.16.0.0/24 172.16.1.0/24	New subnet New subnet AppGW subnet required only when using application gateway for inbound traffic
10.5.0.0/16	CommonFW-Private CommonFW-Web CommonFW-Business CommonFW-DB CommonFW-VPN	10.5.0.0/24 10.5.1.0/24 10.5.2.0/24 10.5.3.0/24 10.5.15.0/24	New subnet New subnet New subnet New subnet New subnet

Step 1: In **Home > Virtual networks > AzureRefArch-VNET**, click **Address space.**

Step 2: In the **Add additional address space** box, enter **172.16.0.0/23**. A new box appears below.

Step 3: In the **Add additional address space** box, enter **10.5.0.0/16**, and then click **Save**.

Step 4: In **Home > Virtual networks > AzureRefArch-VNET**, click **Subnets.**

Step 5: Click **Subnet** to add a new subnet.

Step 6: In the **Name** box, enter **CommonFW-Public**.

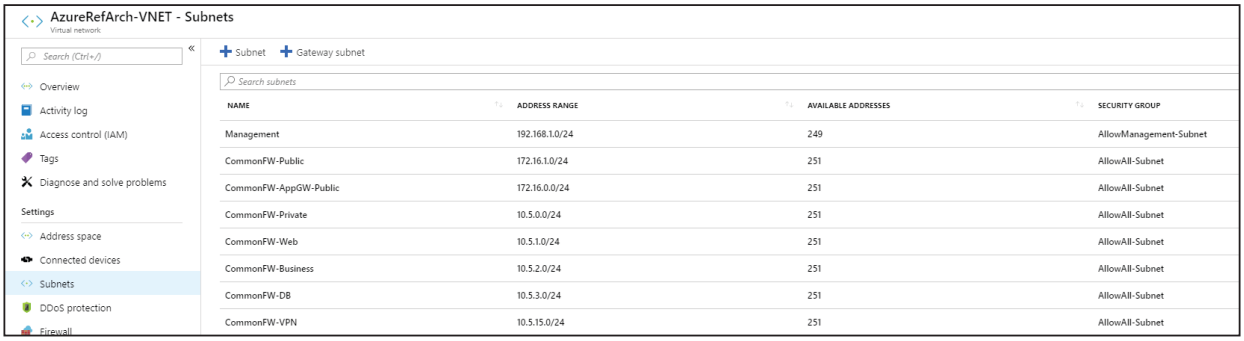
Step 7: In the **Address Range (CIDR block)** box, enter **172.16.1.0/24**.

Step 8: Click in the **Network security group** section. In the **Resource** list, select **AllowAll-Subnet**, and then click **OK**.

> **Caution**
>
> An NSG is not explicitly assigned to newly created subnets. You must assign an NSG to any subnet that uses an Azure Standard SKU public IP address.
>
> Azure documentation states "If you do not have an NSG on a subnet or NIC of your virtual machine resource, traffic is not allowed to reach this resource."
>
> During initial deployment and troubleshooting you may want to configure and use a whitelist "Allow All" NSG to simplify verification.
>
> This guide does not provide further recommendations on how to properly craft and configure the NSGs.

Step 9: Repeat Step 4 through Step 8 for all of the subnets listed as New subnet in Table 5. The CommonFW-AppGW-Public subnet is required only you are using the application gateway option for inbound traffic.

Step 10: Verify that all subnets are created with the correct IP ranges and security group.



3.3 Create the Resource Group for the Common Firewall Option

This guide uses two resource groups, one has already been created for Panorama and common resources. This procedure creates a new resource group which contains all of the VM-Series devices and Azure load balancer resources for the common firewall option.

> **Note**
>
> Resource groups are an administrative concept. Resources and devices in different resource groups can communicate if they are located within a common VNet, or if their VNets are interconnected.

Step 1: In **Home > Resource groups**, click **Add**.

Step 2: In the **Resource group** list, enter **AzureRefArch-CommonFW** and select the desired value for the **Region**. Click **Review + Create**, and then on the next screen, click **Create**.

3.4 Create the Storage Account

The VM-Series firewalls require general purpose storage for their virtual file systems and bootstrapping.

Step 1: In **Home > Storage accounts**, click **Add.**

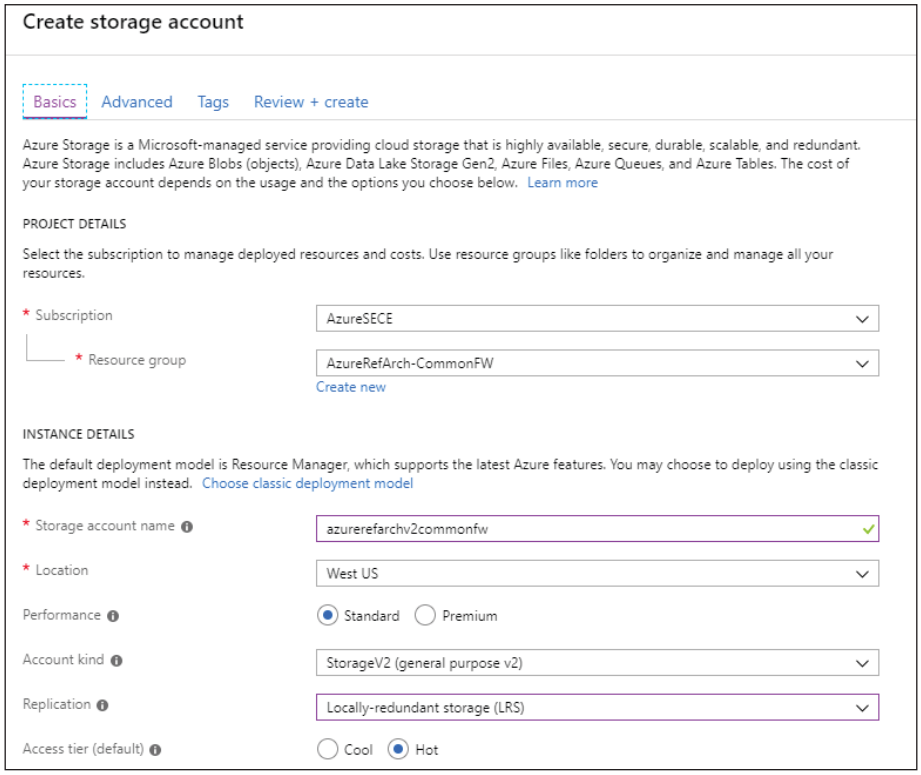
Step 2: In the **Resource Group** list, select **AzureRefArch-CommonFW**.

Step 3: In the **Storage account name** box, enter **azurerefarchv2commonfw**.

Step 4: In the **Account kind** list, select **StorageV2 (general purpose v2)**.

Step 5: In the **Replication** list, select **Locally-redundant storage (LRS)**.

Step 6: Click **Review + create.**



Step 7: On the next screen, after validation passes, click **Create**.

3.5 Create the Availability Set

The VM-Series resiliency model for Azure benefits from the use of an availability set with two fault domains. This ensures that the VM-Series systems are distributed across different fault domains.

> **Note**
>
> You can only configure an availability set on a virtual machine during its initial deployment. You can't modify a virtual machine's availability set configuration after the virtual machine is deployed.

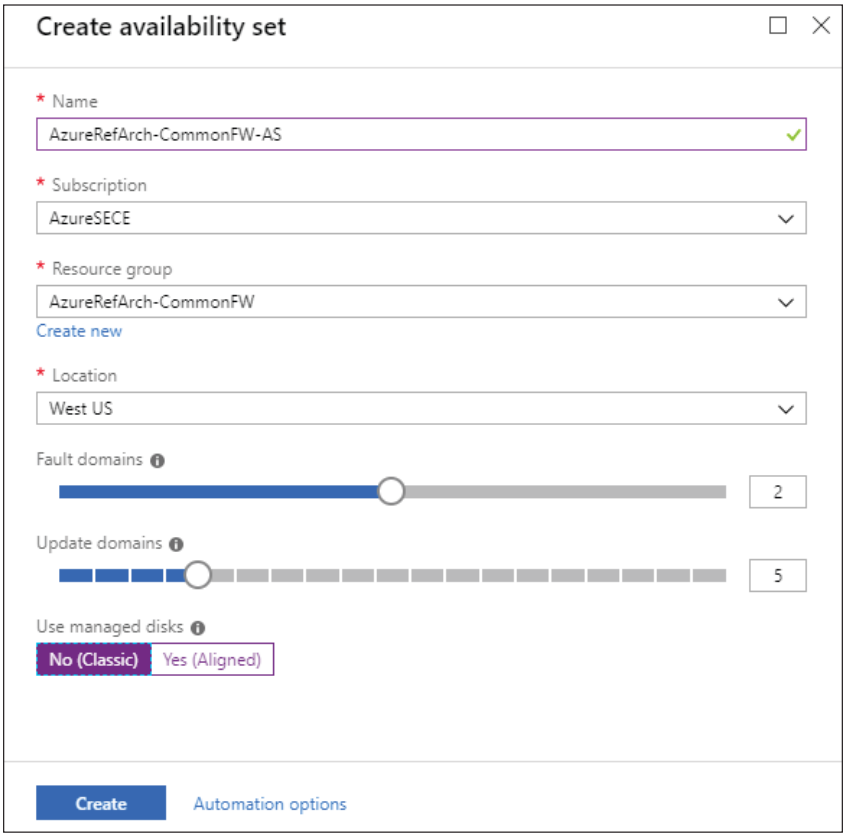
Step 1: In **Home > Availability sets**, click **Add.**

Step 2: In the **Name** box, enter **AzureRefArch-CommonFW-AS**.

Step 3: In the **Resource Group** list, select **AzureRefArch-CommonFW**.

Step 4: In **Use managed disks**, select **No (classic)**. This is required for the ARM template.

Step 5: Click **Create**.



3.6 Create the Public IP Address for VM-Series

The VM-Series devices deployed on Azure are managed using public IP addresses unless on-site network connectivity has been established. The process to configure on-site network connectivity is included later in this guide.

This procedure creates a public IP address that is associated to the management interface of the VM-Series at deployment time. If necessary, this procedure is repeated to create additional public IP addresses for additional VM-Series devices. The parameters listed in Table 4 are used to complete this procedure.

Take note of the FQDN that is defined by adding the location specific suffix to your DNS name label. We recommend managing your devices using the DNS name rather than the public IP address, which may change.

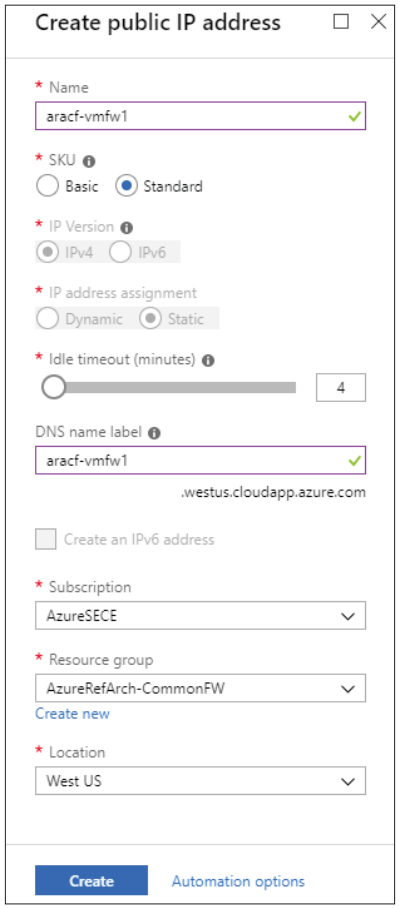
Step 1: In **Home > Public IP addresses**, click **Add.**

Step 2: In the **Name** box, enter **aracf-vmfw1**.

Step 3: Select **Standard** SKU.

Step 4: In the **DNS name label** box, enter **aracf-vmfw1**.

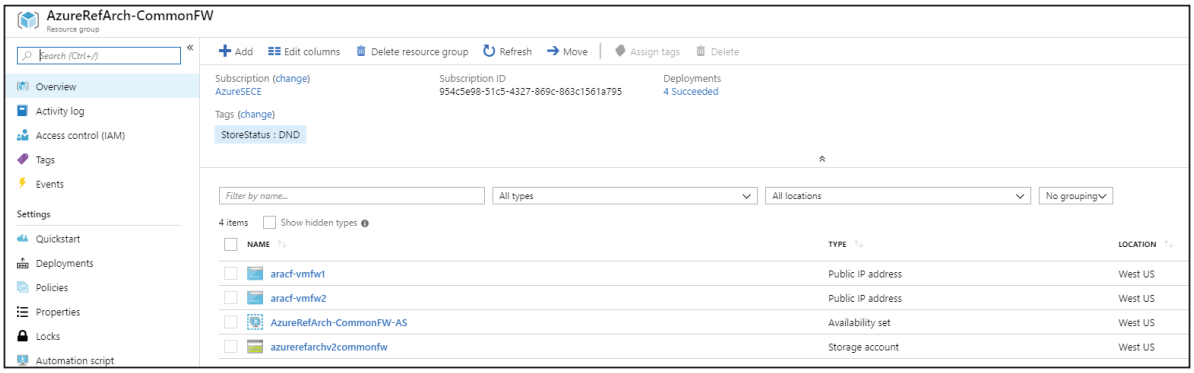
Step 5: In the **Resource Group** list, select **AzureRefArch-CommonFW**, and then click **Create**.



3.7 Verify Resource Creation Completed

Some Azure deployments are time consuming and if any resources are missing, the deployment fails. It is quicker to verify that all of the necessary resources exist before proceeding with a deployment than waiting until a deployment fails.

Step 1: In **Home > Resource Groups**, select **AzureRefArch-CommonFW**.



Step 2: Verify that the resource group, public IP addresses, availability set, and storage account have been successfully created.

Procedures

Deploying VM-Series on Azure

- 4.1 Deploy VM-Series using Custom ARM Template
- 4.2 License VM-Series on Azure
- 4.3 Update Device Software

The following procedures are completed using the Azure Resource Manager deployed from an Azure Resource Manager Template posted at GitHub. If you are already signed in to Azure at https://portal.azure.com, the deployment from GitHub uses the same session authorization.

Table 6 VM-Series deployment parameters

Parameter	Value	Comments
Resource group	AzureRefArch-CommonFW	Existing
Location	—	Tested in West US
VM name	ARACF-VMFW1 ARACF-VMFW2	First device Second device
Storage account name	azurerefarchv2commonfw	—
Storage account existing RG	AzureRefArch-CommonFW	—
Fw Av Set	AzureRefArch-CommonFW-AS	—
VM size	Standard_D3_v2	https://www.paloaltonetworks.com/documentation/80/virtualization/virtualization/set-up-the-vm-series-firewall-on-azure/about-the-vm-series-firewall-on-azure/minimum-system-requirements-for-the-vm-series-on-azure
Public IP type	standard	Standard IP SKU required for use with Azure Standard load-balancer
Image version	latest	—
Image SKU	byol	—
Virtual network name	AzureRefArch-VNET	Uses AzureRefArch-VNET in resource group AzureRefarch
Virtual network address prefix	192.168.1.0/24	Match the initial IP address space from AzureRefArch-VNET
Virtual network existing RG name	AzureRefArch	—
Subnet0Name	Management	—
Subnet1Name	CommonFW-Public	—
Subnet2Name	CommonFW-Private	—
Subnet3Name	CommonFW-VPN	—
Subnet0Prefix	192.168.1.0/24	—
Subnet1Prefix	172.16.1.0/24	—
Subnet2Prefix	10.5.0.0/24	—
Subnet3Prefix	10.5.15.0/24	—
Subnet0Start Address	192.168.1.6 192.168.1.7	First device Second device (start assignment from .6)

Table continued on next page

Continued table

Parameter	Value	Comments
Subnet1Start Address	172.16.1.6 172.16.1.7	First device Second device (start assignment from .6)
Subnet2Start Address	10.5.0.6 10.5.0.7	First device Second device (start assignment from .6)
Subnet3Start address	10.5.15.6 10.5.15.7	First device Second device (start assignment from .6)
Admin username	refarchadmin	—
Admin password	<password>	—
Public IP address name	aracf-vmfw1 aracf-vmfw2	First device Second device
Nsg name	None	NSG is applied at subnet level

4.1 Deploy VM-Series using Custom ARM Template

Repeat this procedure for all VM-Series. This guide assumes that at least two VM-Series devices are created.

The custom Azure Resource Manager template used in this procedure has been developed and validated specifically for this deployment guide.

For template details and features, see : https://github.com/PaloAltoNetworks/ReferenceArchitectures/tree/master/Azure-1FW-4-interfaces-existing-environment.

Use the parameters in Table 6 to deploy each VM-Series.

Step 1: Deploy the VM-Series by clicking on the **Deploy to Azure** button.

Step 2: In the Resource Group list, select **AzureRefArch-CommonFW**.

Step 3: In the **Vm Name** box, enter **ARACF-VMFW1**.

Step 4: In the **Storage Account Name** box, enter **azurerefarchv2commonfw**.

Step 5: In the **Storage Account Existing RG** box, enter **AzureRefArch-CommonFW**.

Step 6: In the **Fw Av Set** box, enter **AzureRefArch-CommonFW-AS**.

Step 7: In the **Vm Size** list, select **Standard_D3_v2**.

Step 8: In the **Public IP Type** list, select **standard**.

Step 9: In the **Image Version** list, select **latest**.

Step 10: In the **Image Sku** list, select **byol**.

Step 11: In the **Virtual Network Name** box, enter **AzureRefArch-VNET**.

Step 12: In the **Virtual Network Address Prefix** box, enter **192.168.1.0/24**.

Step 13: In the **Virtual Network Existing RG Name** box, enter **AzureRefArch**.

Step 14: In the **Subnet0Name** box, enter **Management**.

Step 15: In the **Subnet1Name** box, enter **CommonFW-Public**.

Step 16: In the **Subnet2Name** box, enter **CommonFW-Private**.

Step 17: In the **Subnet3Name** box, enter **CommonFW-VPN**.

Step 18: In the **Subnet0Prefix** box, enter **192.168.1.0/24**.

Step 19: In the **Subnet1Prefix** box, enter **172.16.1.0/24**.

Step 20: In the **Subnet2Prefix** box, enter **10.5.0.0/24**.

Step 21: In the **Subnet3Prefix** box, enter **10.5.15.0/24**.

Step 22: In the **Subnet0Start Address** box, enter **192.168.1.6**.

Step 23: In the **Subnet1Start Address** box, enter **172.16.1.6**.

Step 24: In the **Subnet2Start Address** box, enter **10.5.0.6**.

Step 25: In the **Subnet3Start Address** box, enter **10.5.15.6**.

Step 26: In the **Admin Username** box, enter **refarchadmin**.

Step 27: In the **Admin Password** box, enter the password.

Step 28: In the **Public IP Address Name** box, enter **aracf-vmfw1**.

Step 29: In the **Network Security Group** box, enter **None**.

Step 30: Review the terms and conditions**.** If they are acceptable, select **I agree to the terms and conditions**, and then click **Purchase**.

4.2 License VM-Series on Azure

Your VM-Series is now running on Azure but is unlicensed and using a factory default configuration.

This procedure assumes that you have a valid authorization code for your VM-Series device(s) and have registered the code on the Palo Alto Networks customer support portal (https://support.paloaltonetworks.com).

Step 1: Log in to your VM-Series device (example: https://aracf-vmfw1.westus.cloudapp.azure.com).

Step 2: In **Device > Setup > Management > General Settings**, click the edit cog.

Step 3: In the **Domain** box, enter the domain suffix.

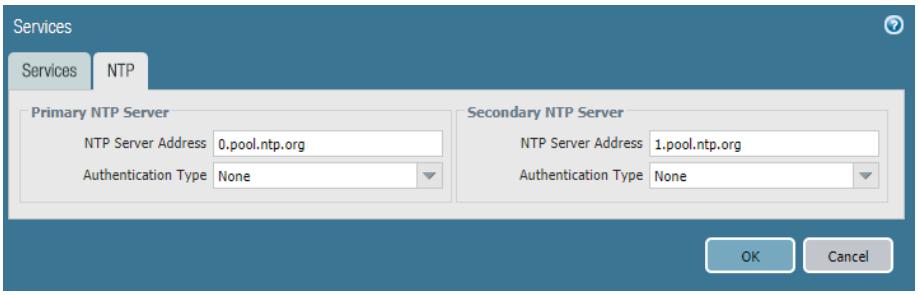
Step 4: In the **Time Zone** list, select the appropriate time zone (example: **US/Pacific**).

Step 5: In **Device > Setup > Services > Services**, click the edit cog.

Step 6: In the **Primary DNS Server** box, enter **168.63.129.16.**

Step 7: On the NTP tab, in the Primary NTP Server section's **NTP Server Address** box, enter **0.pool.ntp.org**.

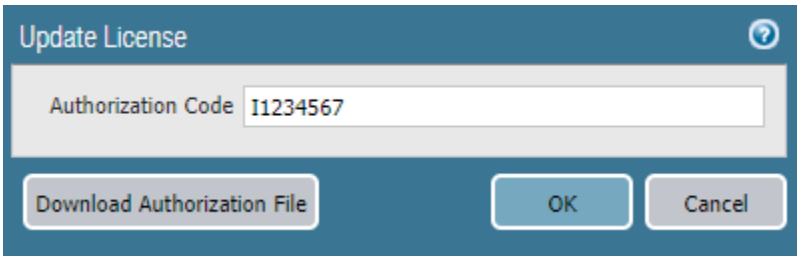
Step 8: In the Secondary NTP Server section's **NTP Server Address** box, enter **1.pool.ntp.org**, and then click **OK**.



Step 9: Click **Commit**.

Step 10: In **Device > Licenses**, click **Activate feature using authorization code**.

Step 11: In the Update License window, in the **Authorization Code** box, enter the authorization code (example: **I1234567**), and then click **OK**.



Step 12: Click **OK** to acknowledge the PAN services restart warning.

> **Note**
>
> The VM-Series services are restarted after the license is installed. Your management session to the VM-Series must be refreshed after the restart; this may take a few minutes.

4.3 Update Device Software

Step 1: Navigate to **Device > Software**.

> **Note**
>
> If you receive an **Operation Failed** warning with the message **No update information available**, you may click **Close** to acknowledge. No action is required.

Step 2: In **Device > Software**, click **Check Now**.

Step 3: For version **8.1.5**, in the Actions column, click **Download,** and then when the download is complete, click **Close**.

Step 4: After the status in the Available column has changed to **Downloaded**, in the **Action** column, click **Install**.

Step 5: When prompted to reboot the device, click **Yes**.

Step 6: After the reboot, in **Device > Dynamic Updates,** click **Check Now**.

This step schedules automatic downloads of the Applications and Threats packages.

Procedures

Preparing VM-Series Firewall Configurations Using Panorama

Panorama provides a number of tools for centralized administration:

- **Hierarchical device groups**—Panorama manages common policies and objects through hierarchical device groups. Multi-level device groups are used to centrally manage the policies across all deployment locations with common requirements
- **Templates/template stacks**—Panorama manages common device and network configuration through templates. You can use templates to manage configuration centrally and then push the changes to all managed firewalls. This approach avoids your making the same individual firewall change repeatedly across many devices. To make things easier, you can stack templates and use them as building blocks for device and network configuration.

5.1 Create Panorama Device Group

This guide uses a single device group specific to the common firewall option. The objects and policies are created in the procedures that require them.

Step 1: Log in to Panorama (example: https://ara-panorama-1.westus.cloudapp.azure.com).

Step 2: In **Panorama > Device Groups**, click **Add**.

Step 3: In the **Name** box, enter **Azure-CommonFW**.

Step 4: In the **Description** box, enter a valid description.

Step 5: In the **Parent Device Group** box, verify the value is set to **Shared**, and then click **OK**.

5.2 Create Panorama Templates

The templates include configuration for all functions that are common across all the VM-Series devices in the common firewall design option.

Two templates are used. The **Azure-3-Zone** template includes firewall networking functions including interfaces, zones, and virtual routers. The **Logging Service** template includes device functions to enable the Logging Service. Both templates are applied to devices using a Panorama template stack, which logically merges the assigned templates and associates them with the relevant devices.

This procedure creates the templates that are used for subsequent procedures in this guide. The specific configurations for these templates are created within the relevant procedures. You create the template stack later in this guide, when associating the first device to the templates.

Step 1: Log in to Panorama (example: https://ara-panorama-1.westus.cloudapp.azure.com).

Step 2: In **Panorama > Templates**, click **Add**.

Step 3: In the **Name** box, enter **Azure-3-Zone**.

Step 4: In the **Description** box, enter a valid description, and then click **OK**.

Step 5: In **Panorama > Templates**, click **Add**.

Step 6: In the **Name** box, enter **Logging Service**.

Step 7: In the **Description** box, enter a valid description, and then click **OK**.

Step 8: On the **Commit** menu, click **Commit to Panorama**.

Step 9: Verify the additional tabs for Device Groups (Policies and Objects) and Templates (Network and Device) are now visible on the Panorama management portal.

Note

You may need to refresh the screen on the secondary Panorama and navigate to a different tab before the additional tabs becomes visible.

5.3 Select Azure-3-Zone Template for Configuration

Step 1: Log in to Panorama (example: https://ara-panorama-1.westus.cloudapp.azure.com).

Step 2: Navigate to **Templates > Device**.

Step 3: In the **Template** list, select **Azure-3-Zone**.

5.4 Configure Device Parameters

This procedure ensures that DNS and NTP are configured consistently across all devices.

Step 1: In **Templates > Device > Setup > Services > Global > Services**, click the Edit cog.

Step 2: In the **Primary DNS Server** box, enter **168.63.129.16**.

Step 3: On the NTP tab, in the Primary NTP Server section's **NTP Server Address** box, enter **0.pool.ntp.org**.

Step 4: In the Secondary NTP Server section's **NTP Server Address** box, enter **1.pool.ntp.org,** and then click **OK**.

5.5 Create Zones and Virtual Routers

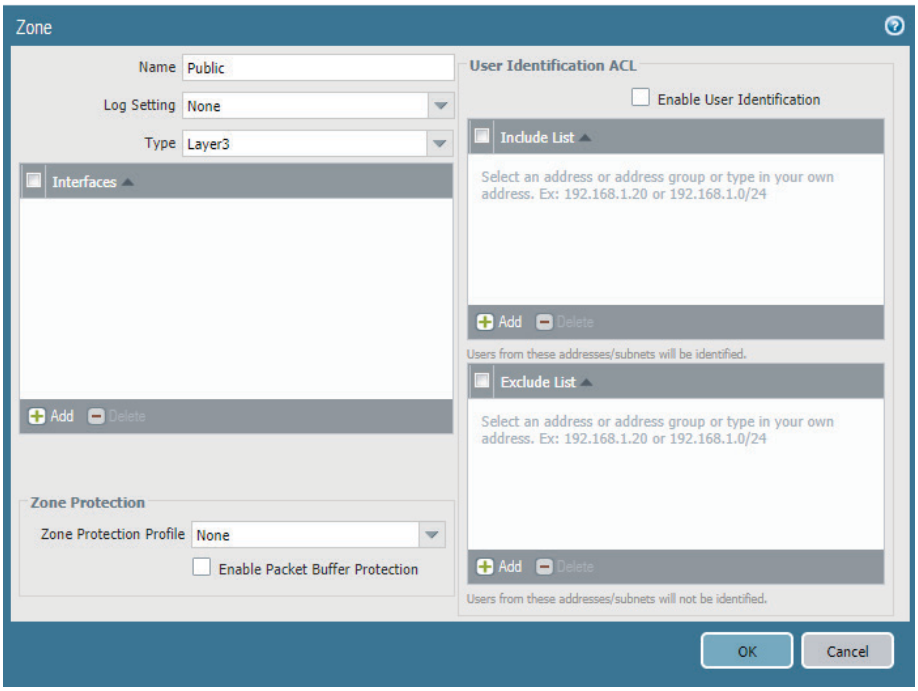
Table 7 Zone and virtual router settings

Zone name	Zone type	Virtual router name
Public	Layer3	VR-Public
Private	Layer3	VR-Private
VPN	Layer3	VR-VPN

Step 1: In **Templates > Network > Zones**, click **Add**. The Zone window appears.

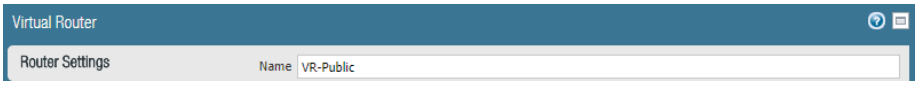
Step 2: In the **Name** box, enter **Public**.

Step 3: In the **Type** list, select **Layer3**, and then click **OK**.



Step 4: In **Templates > Network > Virtual Routers**, click **Add**. The Virtual Router configuration window appears.

Step 5: In the **Name** box, enter **VR-Public**, and then click **OK**.



Step 6: Repeat Step 1 through Step 5 for all rows in Table 7.

5.6 Create Management Profiles

The load-balancer health-checks use HTTPS probes towards the firewall's dataplane interfaces. The firewall blocks responses to these probes by default. Interface management profiles are used to override the default block operation.

> **Note**
>
> A single management profile may be applied to multiple interfaces. We recommend separate management profiles per interface, if required, to allow for different management policies.

The application gateway health probes do not require an interface management profile. If you are using the application gateway option for inbound traffic, only the MP-Private and MP-VPN interface management profiles are required.

> **Note**
>
> If the firewall is configured with a management profile on the public interface for HTTP, HTTPS, SSH or Telnet, then traffic to TCP/80, TCP/443, TCP/22 or TCP/23 does not pass to the backend resources and those ports may not be used for the backend with the application gateway. The health probes may succeed if the application gateway source IPs are permitted in the management profile, but this does not verify health of the backend resources.

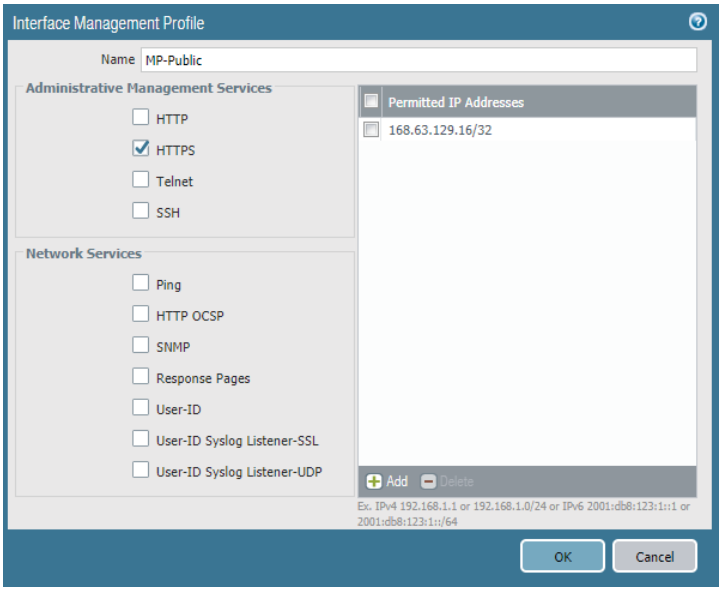
Step 1: In **Templates > Network > Network Profiles > Interface Mgmt,** click **Add**. The Interface Management Profile configuration window appears.

Step 2: In the **Name** box, enter **MP-Public**.

Step 3: In the Administrative Management Services section, select **HTTPS.**

Step 4: In the Permitted IP Addresses pane, click **Add**.

Step 5: Enter **168.63.129.16/32**, and then click **OK**.



Step 6: Repeat Step 1 through Step 5 for **MP-Private** and **MP-VPN**.

5.7 Create Ethernet Interfaces

> **Note**
>
> Although the VM-Series is not a modular hardware platform, assign interfaces to Slot 1 when using Panorama templates for the VM-Series.

Table 8 Azure-3-zone template interface settings

Slot	Interface	Interface type	Virtual router	Security zone	IPv4	Management profile
Slot 1	ethernet1/1	Layer3	VR-Public	Public	DHCP Client	MP-Public
Slot 1	ethernet1/2	Layer3	VR-Private	Private	DHCP Client	MP-Private
Slot 1	ethernet1/3	Layer3	VR-VPN	VPN	DHCP Client	MP-VPN

Step 1: In **Templates > Network > Interfaces > Ethernet,** click **Add Interface**. The Ethernet Interface configuration window appears.

Step 2: In the **Slot** list, select **Slot 1**.

Step 3: In the **Interface Name** list, select **ethernet1/1**.

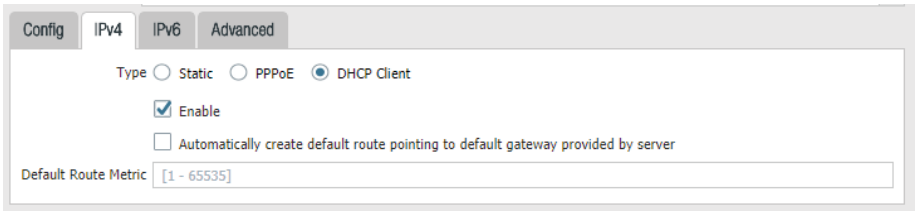
Step 4: In the **Interface Type** list, select **Layer3**.

Step 5: In the **Assign Interface To Virtual Router** list, select **VR-Public**.

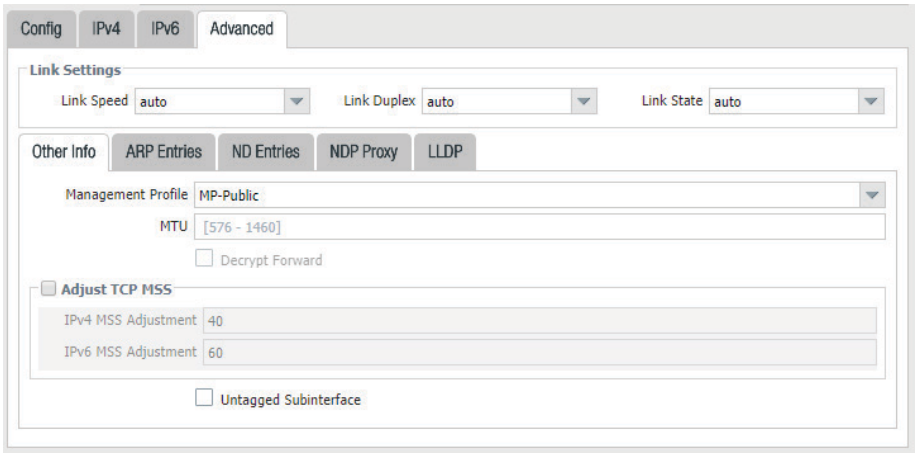
Step 6: In the **Assign Interface To Security Zone** list, select **Public**.

Step 7: On the IPv4 tab, select **DHCP client**.

Step 8: Select **Enable** and clear **Automatically create default route pointing to default gateway provided by server**.



Step 9: On the Advanced tab, in the **Management Profile** list, select **MP-Public**, and then click **OK**.



Step 10: On the warning message, click **Yes**.

Step 11: Repeat Step 1 through Step 10 or all rows in Table 8.

5.8 Add Static Routes to Virtual Routers

Each of the three virtual routers requires static route configuration. Repeat this procedure three times, using the values in the appropriate table:

- When configuring static routes for **VR-Public**, use the values in Table 9.
- When configuring static routes for **VR-Private**, use the values in Table 10.
- When configuring static routes for **VR-VPN**, use the values in Table 11.

Table 9 VR-Public IPv4 static routes

Name	Destination prefix	Interface	Next-hop	Next-hop value
default	0.0.0.0/0	ethernet1/1	IP Address	172.16.1.1
Azure-Probe	168.63.129.16/32	ethernet1/1	IP Address	172.16.1.1
Net-10.5.0.0_16	10.5.0.0/16	None	Next VR	VR-Private

Table 10 VR-Private IPv4 static routes

Name	Destination prefix	Interface	Next-hop	Next-hop value
default	0.0.0.0/0	None	Next VR	VR-Public
Azure-Probe	168.63.129.16/32	ethernet1/2	IP Address	10.5.0.1
Net-10.5.1.0_24	10.5.1.0/24	ethernet1/2	IP Address	10.5.0.1
Net-10.5.2.0_24	10.5.2.0/24	ethernet1/2	IP Address	10.5.0.1
Net-10.5.3.0_24	10.5.3.0/24	ethernet1/2	IP Address	10.5.0.1
Net-10.6.0.0_16	10.6.0.0/16	None	Next VR	VR-VPN

Table 11 VR-VPN IPv4 static routes

Name	Destination prefix	Interface	Next-hop	Next-hop value
Azure-Probe	168.63.129.16/32	ethernet1/3	IP Address	10.5.15.1
Net-10.6.0.0_16	10.6.0.0/16	ethernet1/3	IP Address	10.5.15.1
Net-10.5.0.0_16	10.5.0.0/16	None	Next VR	VR-Private

Step 1: In **Templates > Network > Virtual Routers**, click **VR-Public**. The Virtual Router configuration window appears.

Step 2: On the Static Routes tab, click **Add**. The Virtual Router —Static Route—IPv4 configuration window appears.

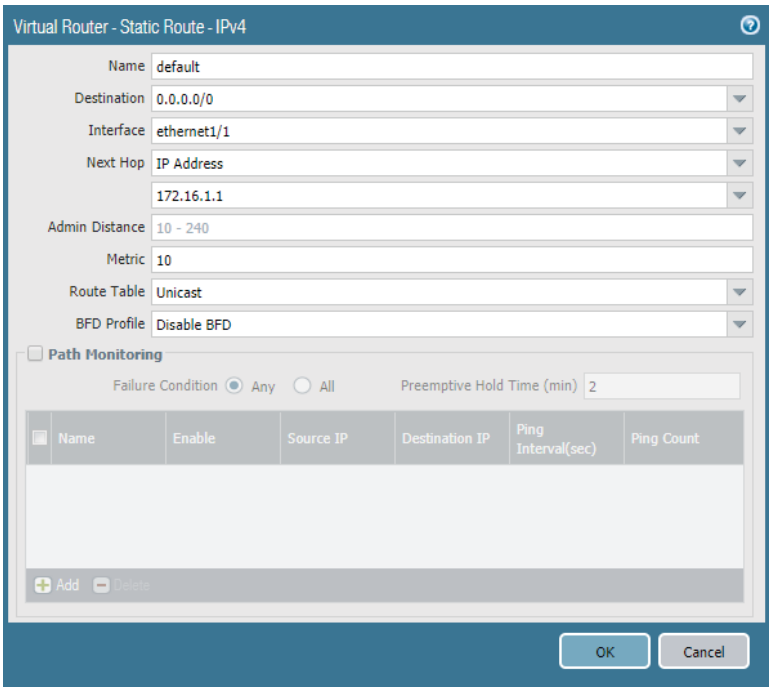
Step 3: In the **Name** box, enter **default**.

Step 4: In the **Destination** box, enter **0.0.0.0/0**.

Step 5: In the **Interface** list, select **ethernet1/1**.

Step 6: In the **Next Hop** list, select **IP Address** and enter **172.16.1.1**, click **OK**, and then click **OK** again.

Step 7: After adding all routes for this virtual router, click **OK** to close the Virtual Router window.



5.9 Commit Changes

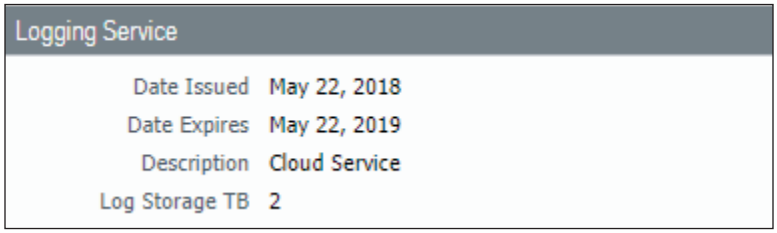
This procedure commits all configuration changes for Procedure 5.1 through Procedure 5.8.

Step 1: On the **Commit** menu, click **Commit to Panorama**.

5.10 Retrieve and Verify Logging Service License

Step 1: In **Panorama > Licenses**, click **Retrieve license keys from license server**.

Step 2: Verify that the Logging Service license is active.



5.11 Configure Logging-Service Template

Step 1: Navigate to **Templates > Device**.

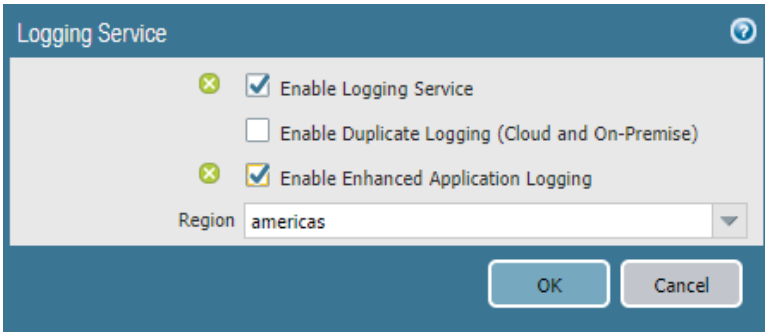
Step 2: In the **Template** list, select **Logging-Service**.

Step 3: In **Templates > Device > Setup > Management > Logging Service**, click the Edit cog.

Step 4: Select **Enable Logging Service**.

Step 5: Select **Enable Enhanced Application Logging**.

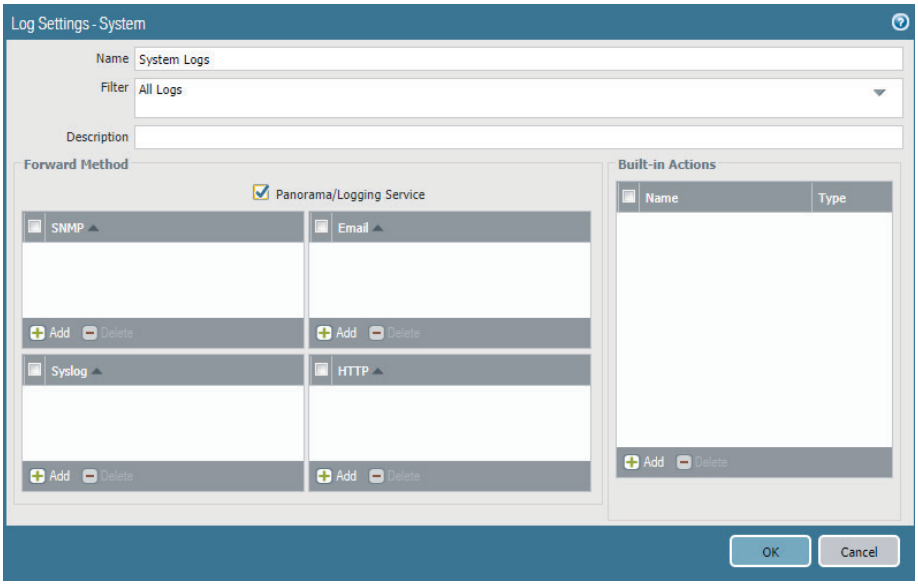
Step 6: In **Region** list, select **americas**, and then click **OK**.



Step 7: In **Templates > Device > Log Settings > System**, click **Add**. The Log Settings—System configuration window appears.

Step 8: In the **Name** box, enter **System Logs**.

Step 9: Select **Panorama/Logging Service**, and then click **OK**.



Step 10: In **Templates > Device > Log Settings > Configuration**, click **Add**. The Log Settings—Configuration window appears.

Step 11: In the **Name** box, enter **Configuration Logs**.

Step 12: Select **Panorama/Logging Service**, and then click **OK**.

Step 13: On the **Commit** menu, click **Commit to Panorama**.

Procedures

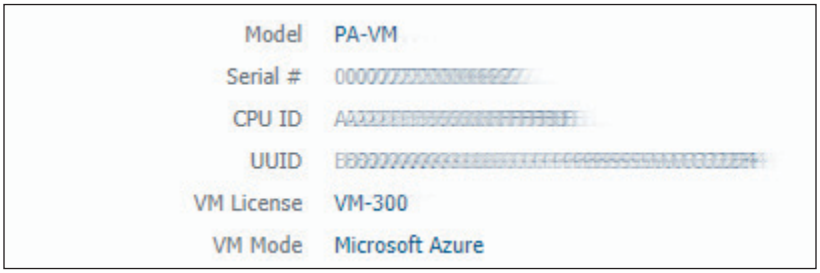
Managing VM-Series with Panorama

6.1 Add VM-Series to Panorama

This procedure is required for each new VM-Series device that is added to Azure. Later in this guide, you perform the procedure to automatically bootstrap the VM-Series to register with Panorama.

Log in to your VM-Series device (example: https://aracf-vmfw1.westus.cloudapp.azure.com).

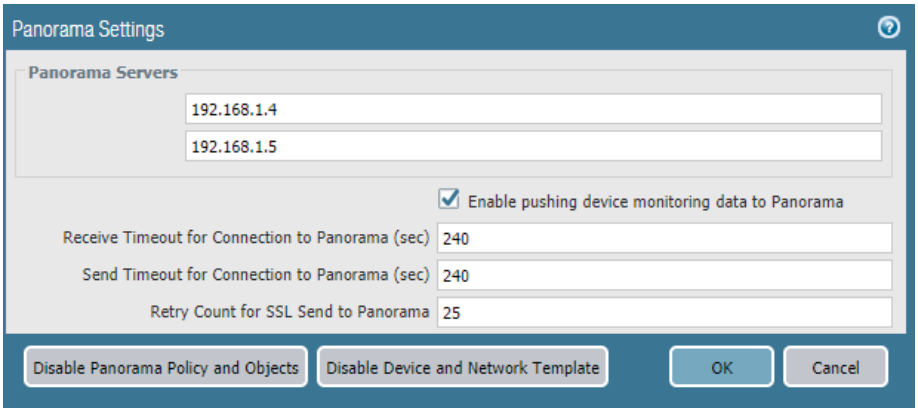
Step 1: In **Dashboard > General Information**, record the **Serial #**.



Step 2: In **Device > Setup > Management > Panorama Settings**, click the edit cog.

Step 3: In the Panorama Servers section, in the top box, enter **192.168.1.4**.

Step 4: If you are using Panorama High Availability, in the bottom **Panorama Servers** box, enter **192.168.1.5**, and then click **OK**.

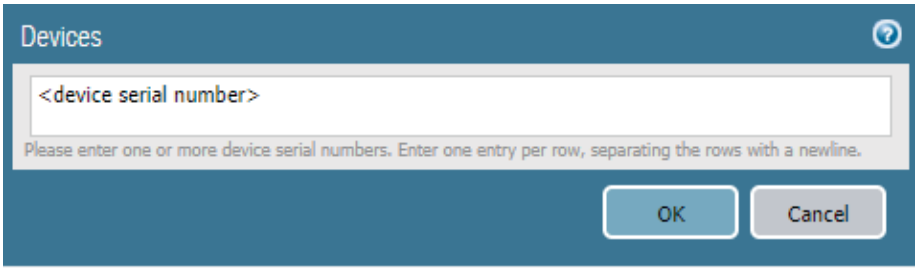


Step 5: Click **Commit**.

Step 6: Log in to Panorama (example: https://ara-panorama-1.westus.cloudapp.azure.com)

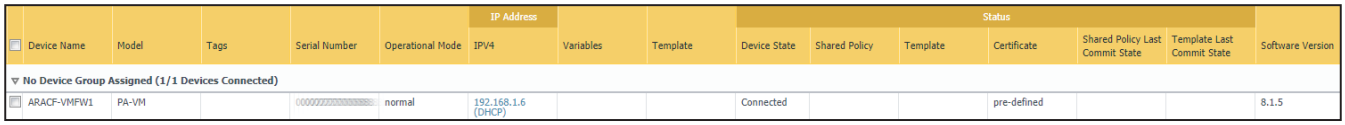
Step 7: In **Panorama > Managed Devices > Summary**, click **Add**.

Step 8: In the **Devices** box, enter the serial number from Step 1, and then click **OK**.



Step 9: On the **Commit** menu, click **Commit to Panorama**.

Step 10: In **Panorama > Managed Devices > Summary**, verify that the device state of the VM-Series is **Connected**. It may take a few minutes for the state to change.



Device Name	Model	Tags	Serial Number	Operational Mode	IP Address: IPV4	Variables	Template	Status: Device State	Shared Policy	Template	Certificate	Shared Policy Last Commit State	Template Last Commit State	Software Version
No Device Group Assigned (1/1 Devices Connected)														
ARACF-VMFW1	PA-VM		[redacted]	normal	192.168.1.6 (DHCP)			Connected			pre-defined			8.1.5

6.2 Add VM-Series to Template Stack and Device Group

In this this procedure, you add devices to the template stack and device groups. The template stack is created and configured only when you add the first VM-Series device.

Option 1: Template stack does not already exist

This option creates a template stack.

Log in to Panorama (example: https://ara-panorama-1.westus.cloudapp.azure.com).

Step 1: In Panorama > Templates, click Add Stack.

Step 2: In the **Name** box, enter **Azure-CommonFW-Option**.

Step 3: In the Templates pane, click **Add**. Enter **Azure-3-Zone**.

Step 4: In the Templates pane, click **Add**. Enter **Logging-Service**.

Option 2: Template stack has already been created

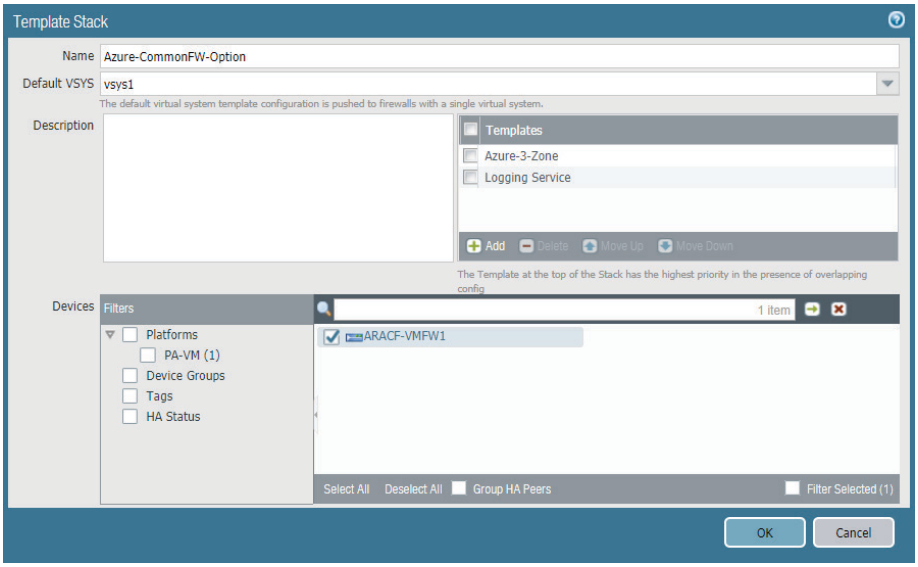
This option modifies the existing template stack.

Step 1: Log in to Panorama (example: https://ara-panorama-1.westus.cloudapp.azure.com).

Step 2: In **Panorama > Templates**, click **Azure-CommonFW-Option**.

Proceed with configuring the template stack.

Step 3: In the Devices pane, select **ARACF-VMFW1** to assign it to the template stack, and then click **OK**.

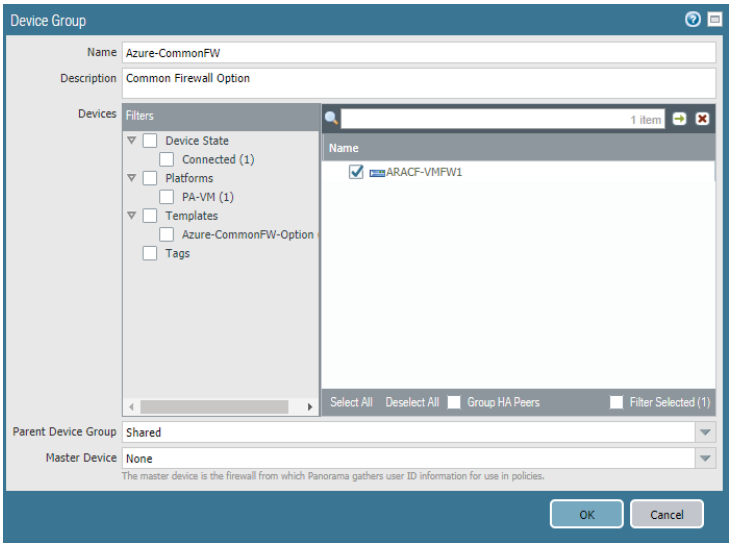


Step 4: On the **Commit** menu, click **Commit and Push**.

The local configuration on each VM-Series should now reflect the template-based configuration that was created on Panorama. This includes interfaces, zones, virtual routers, management profiles, and Logging Service.

Step 5: In **Panorama > Device Groups**, click **Azure-CommonFW**.

Step 6: In the Devices pane, select **ARACF-VMFW1** to assign it to the device group, and then click **OK**.



Step 7: On the **Commit** menu, click **Commit and Push**.

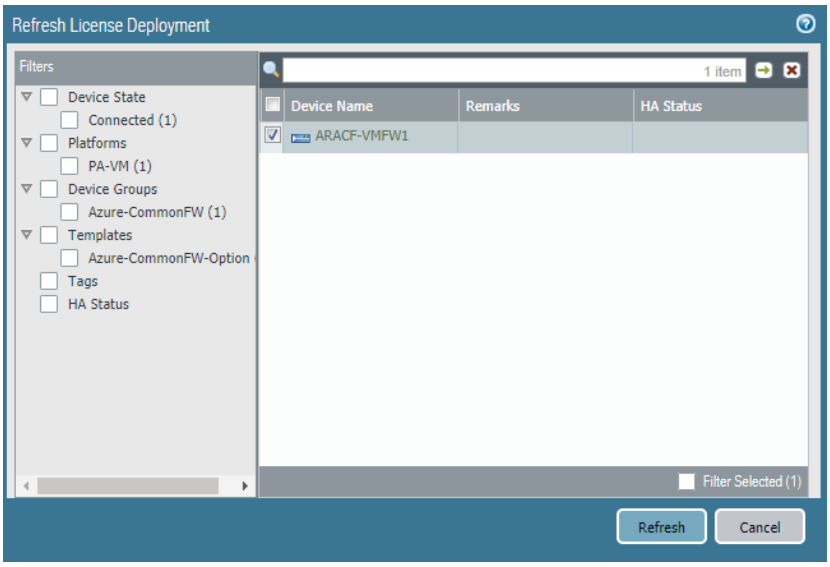
Device group policies and objects are created in procedures later in this guide. The policies and objects for the **Azure-CommonFW** device group are automatically pushed to the local devices from Panorama as they are created.

6.3 Refresh License to Enable Logging Service

Step 1: Log in to Panorama (example: https://ara-panorama-1.westus.cloudapp.azure.com).

Step 2: In **Panorama > Device Deployment > Licenses**, click **Refresh**. The Refresh License Deployment window appears.

Step 3: In the **Device Name** column, select the VM-Series, and then click **Refresh**.



Step 4: Verify the details include **Successfully installed license 'Logging Service,'** and then click **Close**.

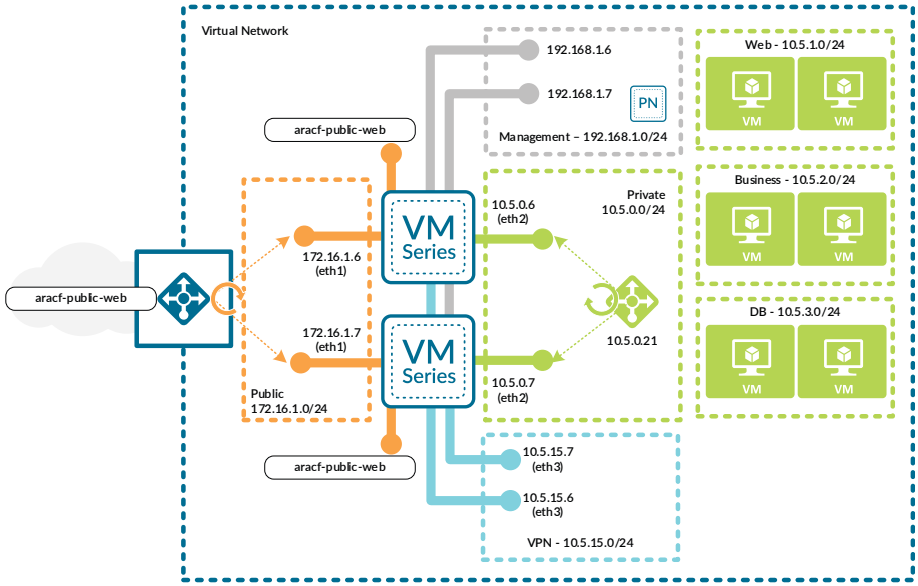
Device Name	Status	Result	Progress	Details
ARACF-VMFW1	Completed	Successful	100%	Successfully installed license 'Threat Prevention' on ARACF-VMFW1. Successfully installed license 'PAN-DB URL Filtering' on ARACF-VMFW1. Successfully installed license 'GlobalProtect Gateway' on ARACF-VMFW1. Successfully installed license 'GlobalProtect Portal' on ARACF-VMFW1. Successfully installed license 'WildFire License' on ARACF-VMFW1. Successfully installed license 'BrightCloud URL Filtering' on ARACF-VMFW1. Successfully installed license 'PA-VM' on ARACF-VMFW1. Successfully installed license 'AutoFocus Device License' on ARACF-VMFW1. Successfully installed license 'Logging Service' on ARACF-VMFW1.

Deployment Details for Azure Networking and Firewall Policies

The VM-Series devices do not actively forward traffic within Azure until they have been integrated into Azure networking and the firewall policies for each traffic profile have been created. You must complete the complementary procedure groups in order support the traffic profiles in the common firewall option.

Resiliency for the traffic profiles is implemented using Azure user-defined routes, Azure load balancer, and Azure application gateway. These procedures are included in the first procedure group. The traffic profiles within the common firewall option each requires a unique firewall policy. A second procedure group configures the policies required for each traffic profile.

Figure 8 Azure networking for common firewall option



Procedures

Configuring Azure Networking and Services

Use Azure Resource Manager to complete these procedures. Sign in to Azure at https://portal.azure.com.

There are two options for inbound traffic that have been previously discussed:

- **Azure public load balancer**—Complete Procedure 7.1 through Procedure 7.3.
- **Azure application gateway**—Complete Procedure 7.4 through Procedure 7.8.

The other procedures in this procedure group are:

- Azure internal load balancer (Outbound traffic)—Complete Procedure 7.9 and Procedure 7.10.
- Azure internal load balancer (Inbound traffic—optional)—Complete Procedure 7.11.
- Configure Azure User Defined Routes (all traffic profiles)—Complete Procedure 7.12 and Procedure 7.13.

7.1 Create the Public IP Address for the Azure Public Load-Balancer

If you have selected the Azure public load balancer option for inbound traffic complete this procedure.

This procedure creates a public IP address that is assigned as the frontend IP address for the Azure public load-balancer for inbound traffic to the web server resources.

Note the FQDN that is defined by adding the location specific suffix to your DNS name label. You use this value in a subsequent procedure when you create Panorama IP address objects for the Inbound Access traffic profile.

Step 1: In **Home > Public IP addresses**, click **Add.**

Step 2: In the **Name** box, enter **ARA-CommonFW-Public-Web**.

Step 3: Select **Standard SKU**.

Step 4: In the **DNS name label** box, enter **aracf-public-web**.

Step 5: In the **Resource Group** list, select **AzureRefArch-CommonFW**, and then click **Create**.

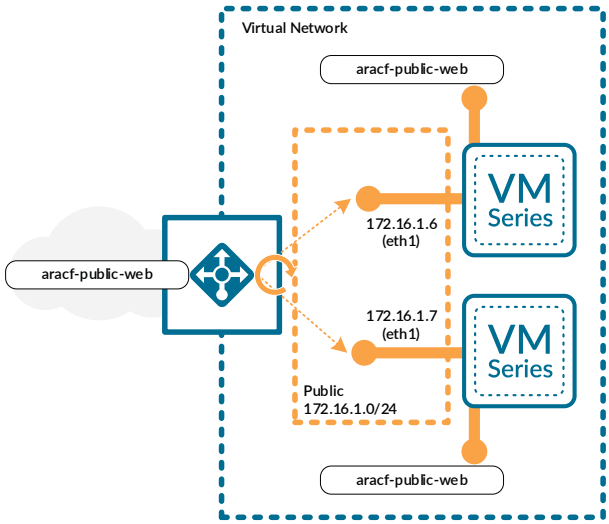
Step 6: Record the value for the FQDN (example: **aracf-public-web.westus.cloudapp.azure.com**).

7.2 Create the Azure Public Load-Balancer

If you have selected the Azure public load balancer option for inbound traffic, complete this procedure.

You create the Azure Public Load-Balancer with a single public frontend IP address and associate it with the public interfaces of a pair of VM-Series firewalls using floating IP.

Figure 9 Azure public load-balancer



Step 1: In **Home > Load Balancers**, click **Add**.

Step 2: In the **Name** box, enter **ARA-CommonFW-LB-Public**.

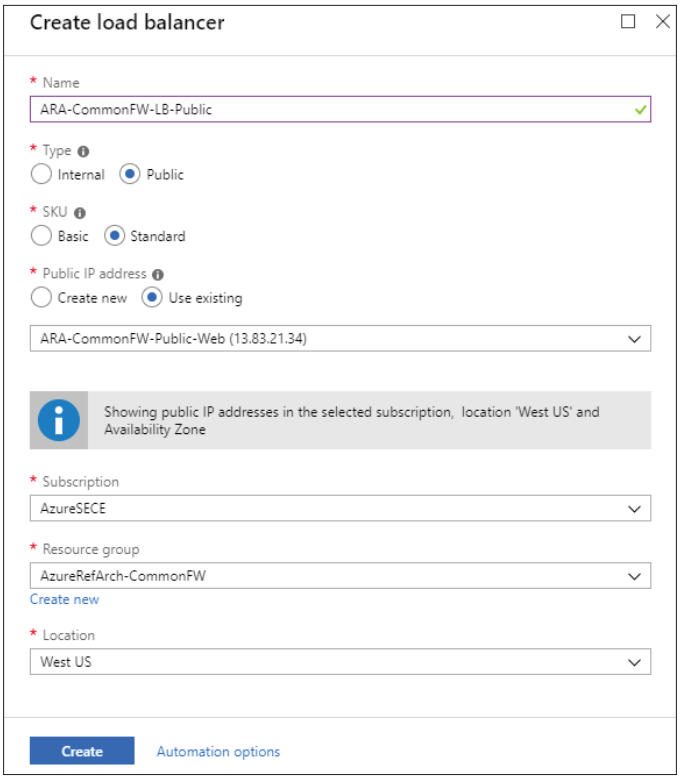
Step 3: In the Type section, select **Public**.

Step 4: In the SKU section, select **Standard**.

Step 5: In the Public IP address section, select **Use Existing**, and then select **ARA-CommonFW-Public-Web**.

This address is associated with the default frontend IP configuration (**LoadBalancerFrontEnd**). You may add additional frontend IP addresses to the load-balancer if necessary after it has been created.

Step 6: In the **Resource Group** list, select **AzureRefArch-CommonFW**, and then click **Create**.



7.3 Configure the Azure Public Load-Balancer

If you have selected the Azure public load balancer option for inbound traffic, complete this procedure.

This procedure assumes that all of the VM-Series firewalls that are to be associated to the load-balancer have already been deployed and does not include the steps to add a new firewall to an existing backend pool.

Step 1: In **Home > Load Balancers > ARA-CommonFW-LB-Public**, click **Health probes**, and then click **Add**.

Step 2: In the **Name** box, enter **HTTPS-Probe**.

Step 3: In the **Port** box, enter **443**, and then click **OK**.

Step 4: In **Home > Load Balancers > ARA-CommonFW-LB-Public**, click **Backend pools**, and then click **Add**.

Step 5: In the **Name** box, enter **Firewall-Layer**.

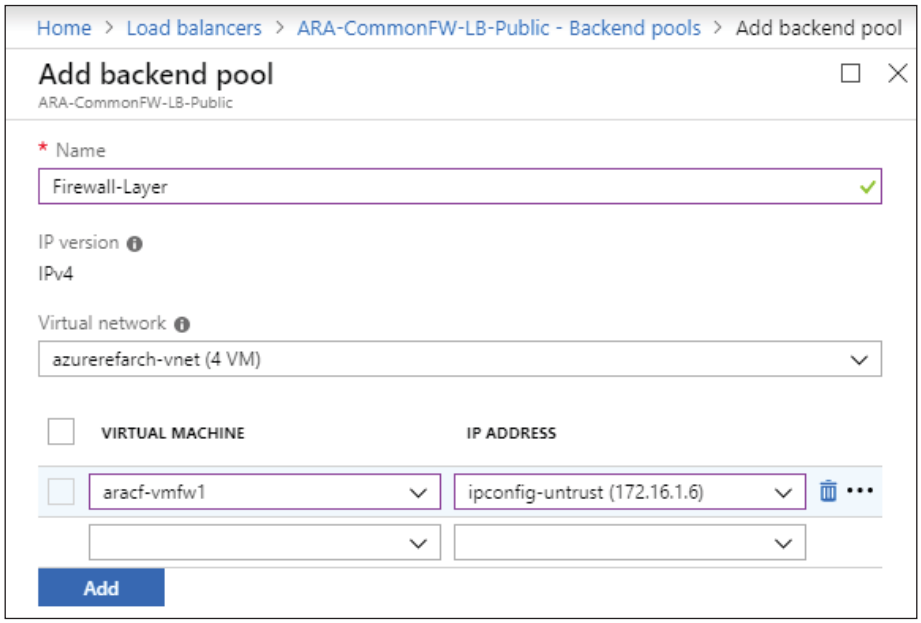
Step 6: In the **Virtual network** list, select **azurerefarch-vnet (X VM)**, where X is the total number of virtual machines already deployed in your VNet.

Step 7: In the **VIRTUAL MACHINE** column, select a VM-Series to be added to this backend pool (example: **aracf-vmfw1**).

Step 8: In the **IP ADDRESS** column, select the **IP configuration** that is associated to the **CommonFW-Public** subnet. (example: **ipconfig-untrust**).

Step 9: Repeat Step 7 and Step 8 for all VM-Series firewalls that are to be assigned to this backend pool.

Step 10: Click **Add**.



Next, you create a load balancing rule for each required TCP port (Example: **TCP/80**, **TCP/443**).

Step 11: In **Home > Load Balancers > ARA-CommonFW-LB-Public**, click **Load balancing rules**, and then click **Add**.

Step 12: In the **Name** box, enter **ARA-CommonFW-LB-Public-Web-80**.

Step 13: In the **Frontend IP address** list, select **LoadBalancerFrontEnd**.

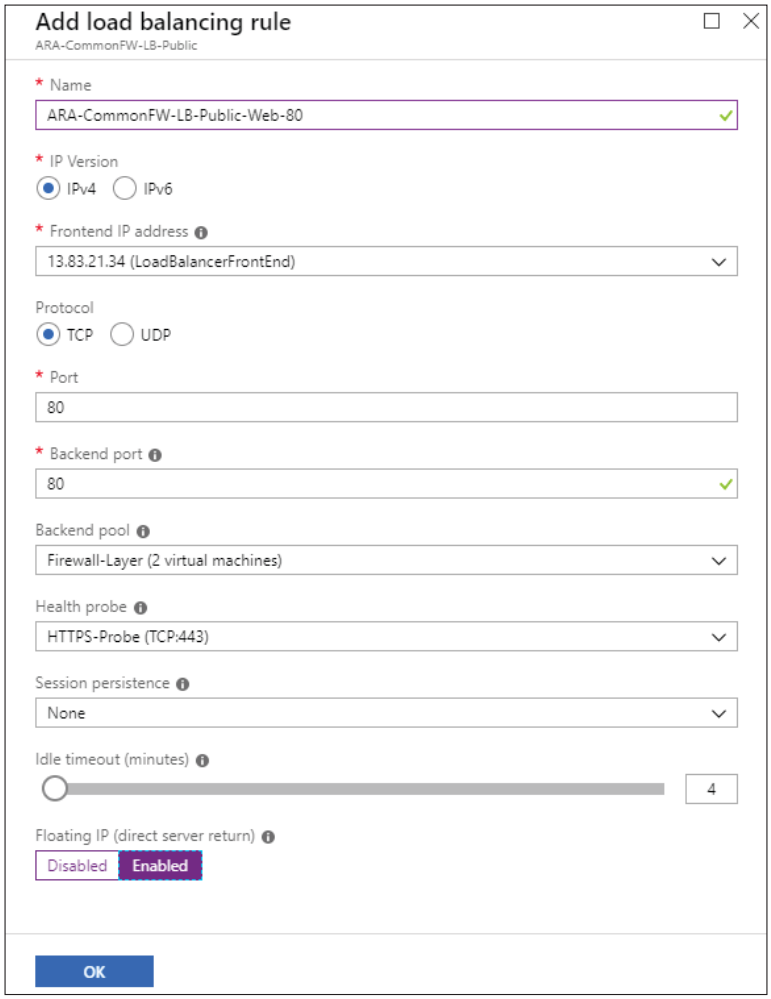
Step 14: In the **Port** box, enter **80**.

Step 15: In the **Backend port** box, enter **80**.

Step 16: In the **Backend pool** list, select **Firewall-Layer**.

Step 17: In the **Health probe** list, select **HTTPS-Probe**.

Step 18: In the **Floating IP (direct server return)** section, select **Enabled**, and then click **OK**.



7.4 Create the Public IP Address for the Azure Application Gateway

If you have selected the Azure application gateway option for inbound traffic, complete this procedure.

Next you create a dynamic public IP address that is assigned as the public frontend IP address for the Azure application gateway for inbound traffic to the web server resources. The IP address is not assigned until the application gateway is created.

Step 1: In **Home > Public IP addresses**, click **Add.**

Step 2: In the **Name** box, enter **ARA-CommonFW-Public-AppGW**.

Step 3: Select **Basic** SKU.

> **Note**
>
> Do not choose a Standard IP SKU for the public IP address of your application gateway. Only the Basic IP SKU is currently supported.

Step 4: In the **DNS name label** box, enter **aracf-public-appgw**.

Step 5: In the **Resource Group** list, select **AzureRefArch-CommonFW**, and then click **Create**.

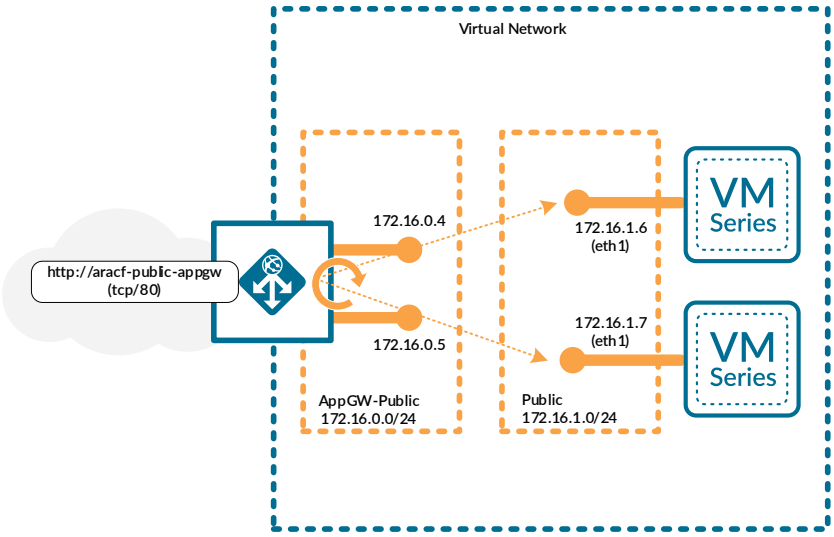
Step 6: Record the value for the FQDN (example: **aracf-public-appgw.westus.cloudapp.azure.com**).

7.5 Create the Azure Application Gateway

If you have selected the Azure application gateway option for inbound traffic, complete this procedure.

This procedure creates an application gateway with a public frontend IP address with an HTTP listener on TCP/80. Additional listeners may be created after the application gateway has been created.

Figure 10 Azure application gateway



Step 1: In **Home > Application gateways**, click **Add**.

Step 2: In the **Name** box, enter **ARA-CommonFW-AppGW**.

Step 3: In the **Tier** box, enter **Standard**.

Step 4: In the **Resource group** list, select **AzureRefArch-CommonFW**, and then click **OK**.

Step 5: In the **Virtual network** section, click **Choose a virtual network**, and then select **AzureRefArch-VNET**.

Step 6: In the **Subnet** list, select **CommonFW-AppGW-Public**.

Step 7: In the **Public IP address** section, select **Use existing**, and then select **ARA-CommonFW-Public-AppGW**, and then click **OK**.

Step 8: Review the Summary, and then if it's acceptable, click **OK**.

7.6 Configure the Azure Application Gateway

If you have selected the Azure application gateway option for inbound traffic, complete this procedure.

This procedure assumes that all of the VM-Series firewalls that are to be associated to the load-balancer have already been deployed and does not include the steps to add a new firewall to an existing backend pool.

A default HTTP backend rule is automatically created mapping HTTP/80 on inbound connections to HTTP/80 on the backend pool targets.

Step 1: In **Home > Application gateways > ARA-CommonFW-AppGW**, click **Backend pools**.

Step 2: Click **appGatewayBackendPool** to add targets to the existing default backend pool.

Step 3: In the **Targets** list, select **Virtual machine**.

Step 4: In the **VIRTUAL MACHINE** column, select a VM-Series to be added to this backend pool (example: **ARACF-VMFW1**).

Step 5: In the **NETWORK INTERFACES** column, select the interface that is associated to the **CommonFW-public** subnet (example: **AFACF-VMFW1-eth1**).

Step 6: Repeat Step 4 and Step 5 for all VM-Series firewalls that are to be assigned to this backend pool.

Step 7: Click **Save**.

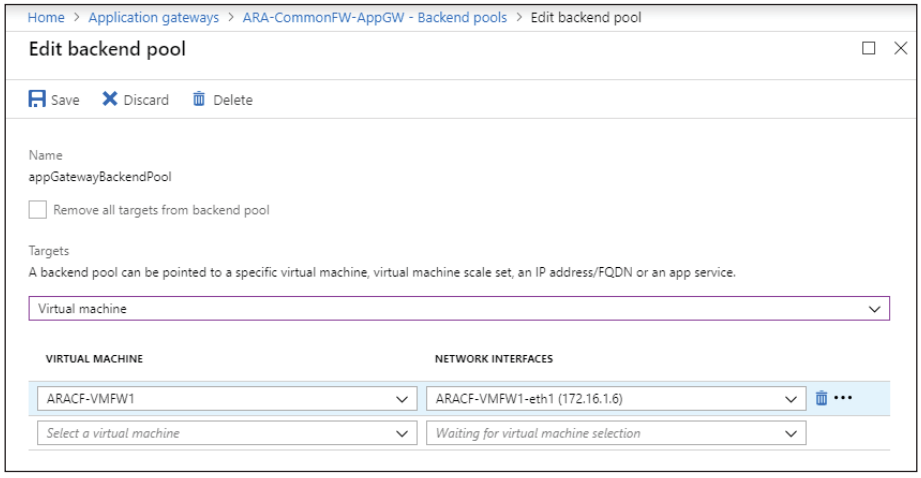


Table 12 Application gateway listeners

Listener name	Frontend name	Frontend port	Protocol	Usage
appGatewayHttpListener	appGatewayFrontendPort	80	HTTP	Default listener
AppGW-Listen-HTTP-8000	HTTP-8000	8000	HTTP	Direct to server. No load-balancer required.
AppGW-Listen-HTTPS-443	HTTPS-443	443	HTTPS	SSL re-encryption and SSL offload

An additional HTTP listener for TCP/8000 is created to show the details for destination NAT only configuration on the firewall that does not require the use of an internal load-balancer.

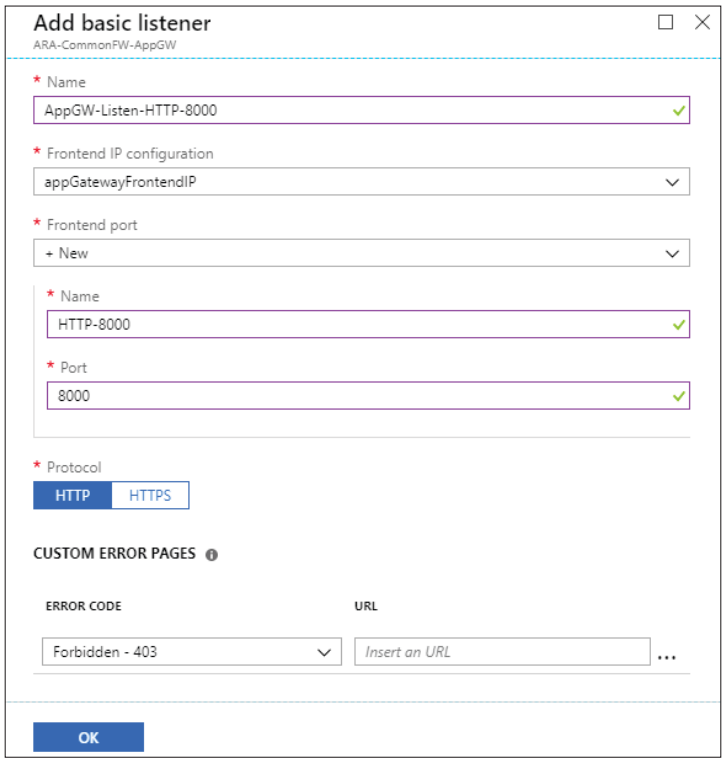
Step 8: In **Home** > **ARA-CommonFW-AppGW**, click **Listeners**, and then click **Basic**.

Step 9: In the **Name** box, enter **AppGW-Listen-HTTP-8000**.

Step 10: In the **Frontend port** list, select **New**.

Step 11: In the **Frontend port Name** box, enter **HTTP-8000**.

Step 12: In the **Frontend port Port** box, enter **8000**, and then click **OK**.



An additional HTTPS listener for TCP/443 is required for SSL. All HTTPS listeners require a X.509 digital certificate with a bundled private key in PKCS #12 format. The certificate must be issued by a trusted certificate authority and the certificate file type must be .PFX.

Note

Certificate creation and management is beyond the scope of this document.

If your application gateway is providing access to https://aracf-public-appgw.westus.cloudapp.azure.com, then you need certificate with a subject alternate name for the FQDN "aracf-public-appgw.westus.cloudapp.azure.com" or a wildcard certificate for " *.westus.cloudapp.azure.com".

Alternatively, if you have a DNS CNAME entry for your domain that maps "web.your-domain.com" to "aracf-public-appgw.westus.cloudapp.azure.com", then you could use a certificate with Subject Alternate Name for the FQDN "web.yourdomain.com" or a wildcard certificate for "*.yourdomain.com".

Step 13: In **Home** > **ARA-CommonFW-AppGW**, click **Listeners**, and then click **Basic**.

Step 14: In the **Name** box, enter **AppGW-Listen-HTTPS-443**.

Step 15: In the **Frontend port** list, select **New**.

Step 16: In the **Frontend port Name** box, enter **HTTPS-443**.

Step 17: In the **Frontend port Port** box, enter **443**.

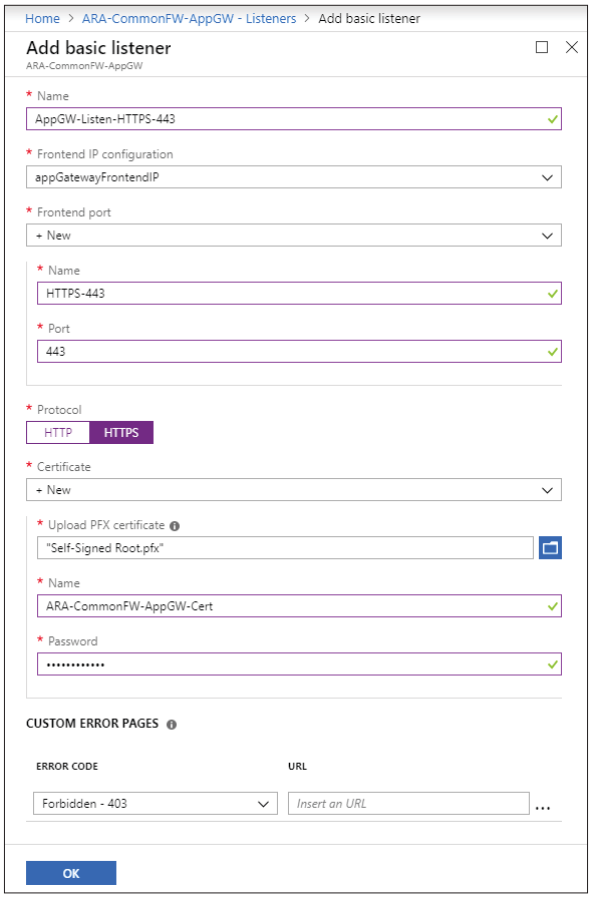
Step 18: In the Protocol section, select **HTTPS**.

Step 19: In the **Certificate** list, select **New**.

Step 20: For the **Upload PFX certificate** box, click the **Browse** icon and select the public web server certificate.

Step 21: In the certificate **Name** box, enter **ARA-CommonFW-AppGW-Cert**.

Step 22: In the certificate **Password** box, enter the certificate password, and then click **OK**.

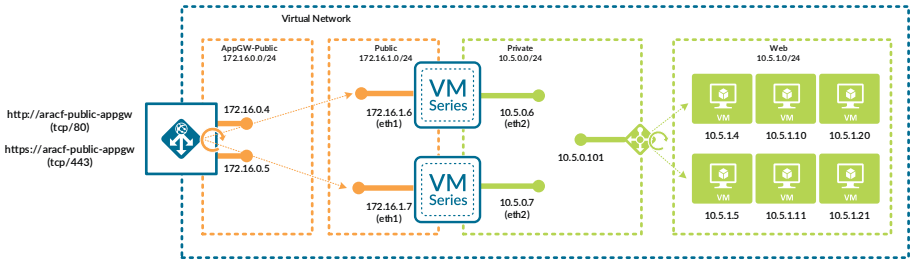


Because the application gateway backend pool includes only the public interfaces of the firewalls, you must use multiple TCP ports to associate to the HTTP/HTTPS backend resources behind the firewalls.

Two options are configured for the application gateway

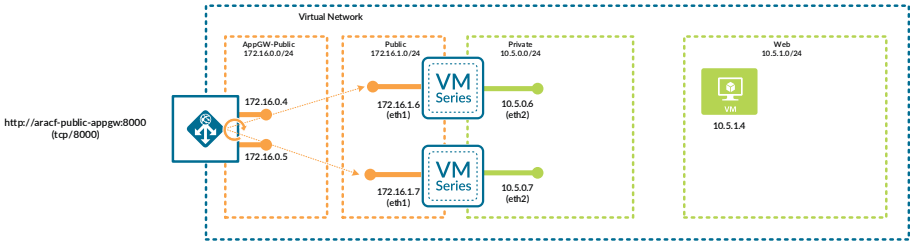
- **Internal load balancer**—You use a load-balancer frontend IP address for the application gateway backends. Port-based NAT policy rules on the firewall translate any traffic from the application gateways to the firewall public interface IP address to the frontend IP of the internal load balancer. Port mapping is also configured on the load balancer to direct traffic to the actual web server resources.

Figure 11 Application gateway with internal load balancer



- **Firewall destination NAT to backend resource**—Web server resources are used for the application gateway backends. Port-based NAT policy rules on the firewall translate any traffic from the application gateways to the firewall public interface IP address to the IP addresses of the web server resources. No internal load balancer is required.

Figure 12 Application gateway direct to web server



An HTTP backend on TCP/80 is created by default when you first deploy the application gateway. Additional HTTP/HTTPS backends are required for any other usages. Example usages and backends are listed in Table 13. The first entry in the table has already been created.

> **Note**
>
> If you are using a public load balancer for inbound traffic with health probes on TCP/443, then you may not also use TCP/443 for an application gateway HTTPS backend.

If you configure the application gateway to re-encrypt SSL traffic to an HTTPS backend, you must provide a DER or Base-64 encoded X.509 digital certificate for the actual server resource saved in .CER format.

> **Note**
>
> Certificate creation and management is beyond the scope of this document.

Table 13 HTTP/HTTPS Backends

Frontend listener (protocol/port)	Path	Usage	HTTP/HTTPS backend	HTTP/HTTPS backend (protocol/port)
HTTP/80	All	Default	appGatewayBackendHTTPSettings	HTTP/80
HTTP/80	/images/*	URL path-based routing	AppGW-Backend-HTTP-8081	HTTP/8081
HTTP/8000	All	Direct to Web Server (no ILB used)	AppGW-Backend-HTTP-8000	HTTP/8000
HTTPS/443	All	Re-encrypt (requires server certificate)	AppGW-Backend-HTTPS-443	HTTPS/443
HTTPS/443	/images/*	SSL offload	AppGW-Backend-HTTP-8443	HTTP/8443

Step 23: In **Home > Application gateways >** **ARA-CommonFW-AppGW**, click **HTTP settings**, and then click **Add**.

Step 24: In the **Name** box, enter **AppGW-Backend-HTTP-8081**.

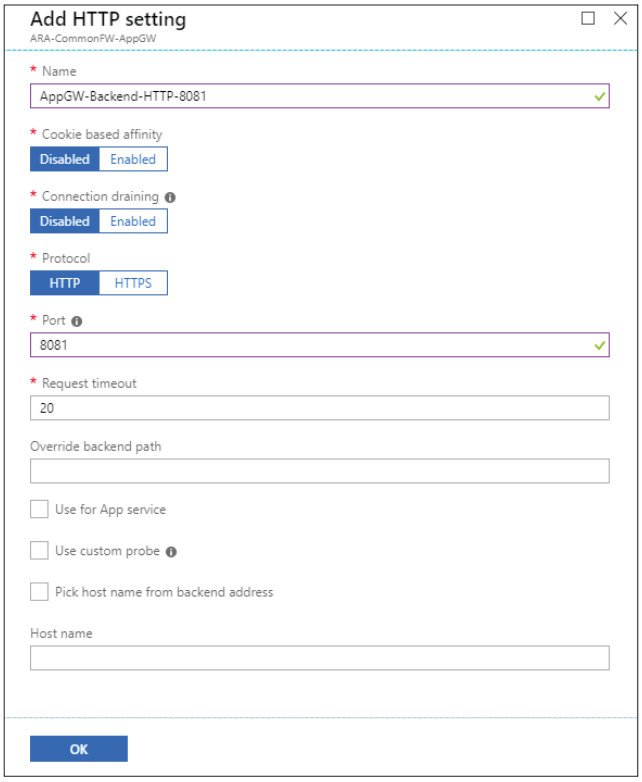
Step 25: In the **Protocol** section, select **HTTP**.

Step 26: If backend protocol is **HTTPS**, then perform the following substeps; otherwise, proceed to Step 27.

- In the **Backend authentication certificates** section, in the **Name** box, enter **WebServer-Authentication-Cert**.
- For the **Upload CER certificate** box, click the **Browse** icon, and then select the web server authentication certificate (example: **Server-Cert.cer**).

Step 27: In the **Port** box, enter **8081**, and then click **OK**.

Step 28: Repeat Step 23 through Step 27 for all rows in Table 13



Application gateway rules are created to associate the frontend listeners with the HTTP/HTTPS backends. Basic rules only allow a single HTTP/HTTPS backend for each listener. Use path-based rules to associate multiple HTTP/HTTPS backends for a listener. A path-based rule includes both basic default settings and additional path-based exceptions within a single rule.

The default rule "rule1" is a Basic rule and is deleted and replaced with a Path-based rule. At least one additional rule must be created before deleting the default rule.

Step 29: In **Home > Application gateways > ARA-CommonFW-AppGW**, click **Rules**.

Step 30: Click **Path-based**.

Step 31: In the **Name** box, enter **HTTPS-Rule-1**.

Step 32: In the **Listener** list, select **AppGW-LISTEN-HTTPS-443**.

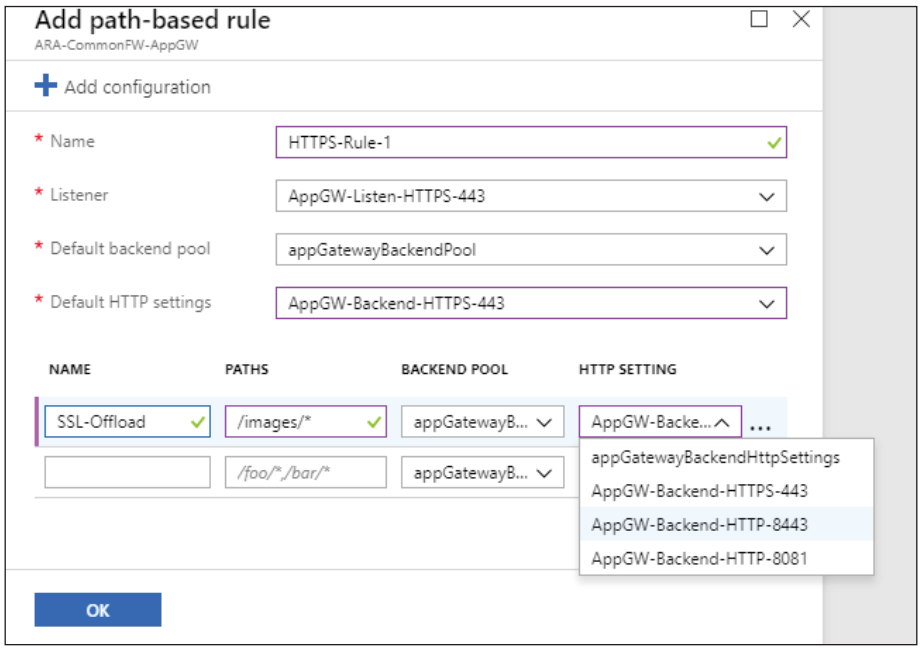
Step 33: In the **Default backend pool** list, select **appGatewayBackendPool**.

Step 34: In the **Default HTTP settings** list, select **AppGW-Backend-HTTPS-443**.

Step 35: In the path-based rule configuration section, perform the following substeps:

- In the **NAME** box, enter **SSL-Offload**.
- In the **PATHS** box, enter **/images/***.
- In the **BACKEND POOL** box, enter **appGatewayBackendPool**.
- In the **HTTP SETTING** section, select **AppGWBackend-HTTP-8443**.

Step 36: Click **OK**.



Step 37: In **Home > Application gateways > ARA-CommonFW-AppGW**, click **Rules**.

Step 38: Right-click on **rule1**, and then click **Delete**.

Step 39: In **Home > Application gateways > ARA-CommonFW-AppGW**, click **Rules**, and then click **Path-based**.

Step 40: In the **Name** box, enter **HTTP-Rule-1**.

Step 41: In the **Listener** list, select **appGatewayHttpListener**.

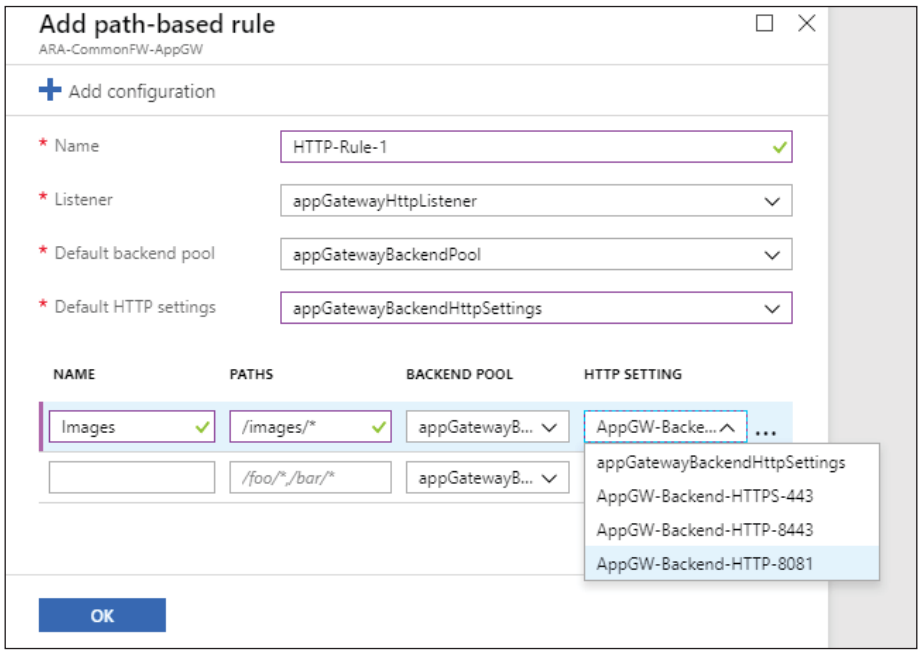
Step 42: In the **Default backend pool** list, select **appGatewayBackendPool**.

Step 43: In the **Default HTTP settings** list, select **appGatewayBackendHttpSettings**.

Step 44: In the path-based rule configuration section, perform the following substeps:

- In the **NAME** box, enter **Images**.
- In the **PATHS** box, enter **/images/***.
- In the **BACKEND POOL** box, enter **appGatewayBackendPool**.
- In the **HTTP SETTING** section, select **AppGWBackend-HTTP-8081**.

Step 45: Click **OK**.



Step 46: In **Home > Application gateways > ARA-CommonFW-AppGW**, click **Rules**, and then click **Basic**.

Step 47: In the **Name** box, enter **HTTP-Rule-2**.

Step 48: In the **Listener** list, select **AppGW-Listen-HTTP-8000**.

Step 49: In the **Default backend pool** list, select **appGatewayBackendPool**.

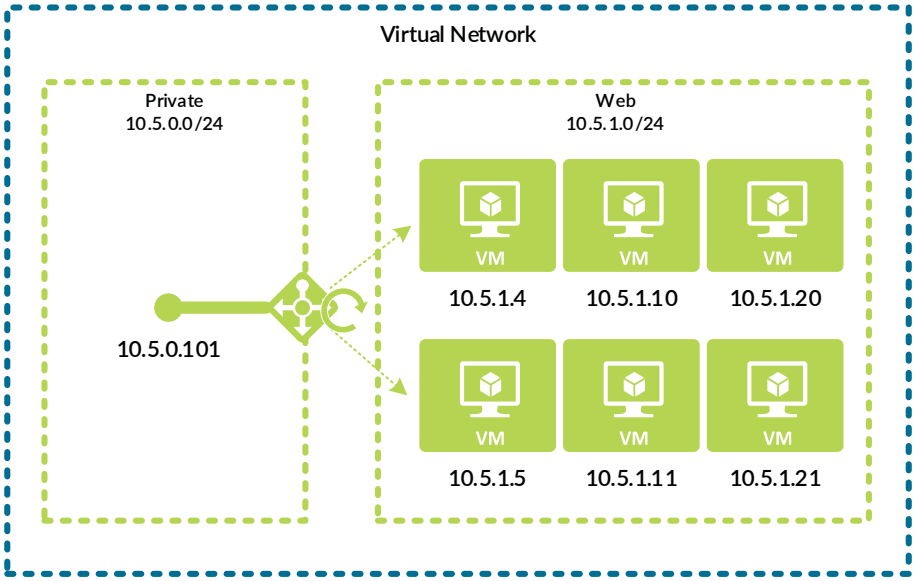
Step 50: In the **Default HTTP settings** list, select **AppGW-Backend-HTTP-8000**, and then click **OK**.

7.7 Create the Azure Inbound Internal Load-Balancer for Application Gateway (optional)

If you have selected the Azure application gateway with the internal load balancer option for inbound traffic, complete this procedure.

This procedure is required in order to add web server resiliency or to provide horizontal web-server scaling. Otherwise each HTTP/HTTPS backend corresponds only to a single web server.

You create the Azure Internal Load-Balancer with a single private frontend IP address and associate it with the web server resources for the application gateway.



You use the frontend IP address as the NAT destination for the application gateway firewall rules.

Step 1: In **Home > Load Balancers**, click **Add**.

Step 2: In the **Name** box, enter **ARA-CommonFW-AppGW-ILB**.

Step 3: In the Type section, select **Internal**.

Step 4: In the SKU section, select **Standard**.

Step 5: Click the **Choose a virtual network** section, and then select **AzureRefArch-VNET**.

Step 6: Click the **Choose a subnet** section, and then select **CommonFW-Private**.

Step 7: In the IP address assignment section, select **Static**.

Step 8: In the **Private IP address** box, enter **10.5.0.101**.

This address is associated with the default frontend IP configuration (**LoadBalancerFrontEnd**), which is used for inbound access.

Step 9: In the Resource Group list, select **AzureRefArch-CommonFW**, and then click **Create**.

7.8 Configure the Azure Inbound Internal Load-Balancer for Application Gateway

Table 14 Example internal load-balancer rules

Rule	Frontend IP	Backend pool	Frontend port	Backend pool	Pool members	Backend port
AppGW-1	10.5.0.101	Web-Pool-1	TCP/80	Web-Pool-1	10.5.1.4 10.5.1.5	TCP/80
AppGW-2	10.5.0.101	Image-Pool-2	TCP/8081	Image-Pool-2	10.5.1.10 10.5.1.11	TCP/80
AppGW-3	10.5.0.101	Image-Pool-2	TCP/8443	Image-Pool-2	10.5.1.10 10.5.1.11	TCP/8443
AppGW-4	10.5.0.101	SSL-Pool-3	TCP/443	SSL-Pool-3	10.5.1.20 10.5.1.21	TCP/443

This example uses separate web server backend pools for each usage: HTTP default, images, and SSL. The backend pool for the image servers is used for both cleartext HTTP access, as well as for SSL offload. In this case, because there are two rules associated with the same backend pool, the pool members must listen on multiple ports (TCP/80 and TCP/8443). Load-balancer health probes are configured for all backend web server ports.

Step 1: In **Home > Load Balancers > ARA-CommonFW-AppGW-ILB**, click **Health probes**, and then click **Add**.

Step 2: In the **Name** box, enter **HTTP-Probe**.

Step 3: In the **Port** box, enter **80**, click **OK**, and then click **Add**.

Step 4: In the **Name** box, enter **HTTP-Probe-8443**.

Step 5: In the **Port** box, enter **8443**, click **OK**, and then click **Add**.

Step 6: In the **Name** box, enter **HTTPS-Probe-443**.

Step 7: In the **Port** box, enter **443**, and then click **OK**.

Step 8: In **Home > Load Balancers > ARA-CommonFW-AppGW-ILB**, click **Backend pools**.

Step 9: For each backend pool listed in Table 14, perform these substeps once:

- Click **Add**.
- In the **Name** box, enter **Web-Pool-1**.
- For each pool member listed for this backend pool in Table 14, repeat the following substeps.
  - In the **Virtual network** list, select **azurerefarch-vnet (X VM)**, where X is the total number of virtual machines already deployed in your VNet.
  - In the **VIRTUAL MACHINE** column, select a web server resource to be added to this backend pool (example: **aracf-web-1**).
  - In the **IP ADDRESS** column, select the **IP configuration** that is associated to the **CommonFW-Private** subnet. (example: **ipconfig1 (10.5.1.4**).
  - Click **Add**.

Step 10: In **Home > Load Balancers > ARA-CommonFW-AppGW-ILB**, click **Load balancing rules**.

Step 11: For each rule listed in Table 14, perform these substeps once:

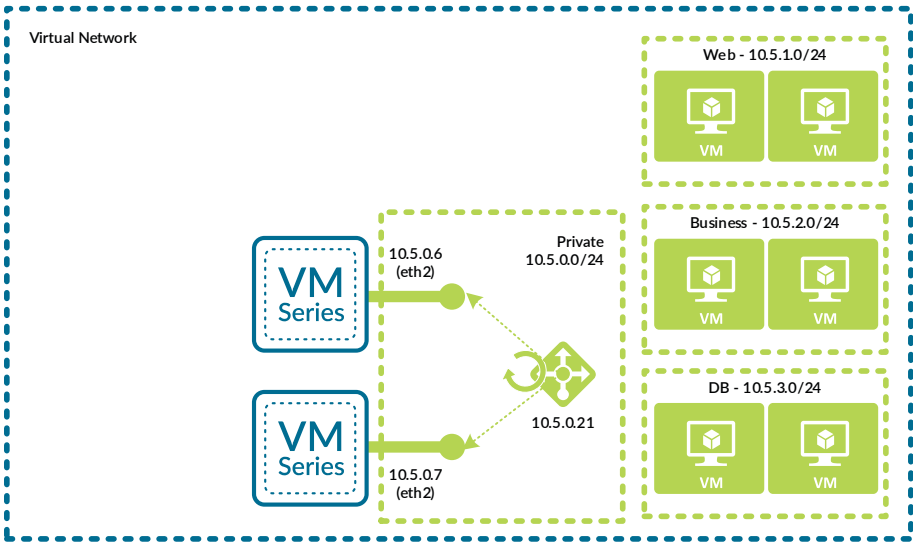
- Click **Add**.
- In the **Name** box, enter **AppGW-1**.
- In the **Frontend IP address** list, select **LoadBalancerFrontEnd**.
- For **Protocol**, select **TCP**.
- In the **Port** box, enter **80**.
- In the **Backend port** box, enter **80**.
- In the **Backend pool** list, select **Web-Pool-1**.
- In the **Health probe** list, select **HTTP-Probe**, and then click **OK**.

7.9 Create the Azure Internal Load-Balancer

An internal load-balancer is required in order to support the outbound, east/west, and backhaul traffic profiles.

You create the Azure Internal Load-Balancer with a single private frontend IP address and associate it with the private interfaces of a pair of VM-Series firewalls.

Figure 13 Azure internal load-balancer for outbound access



You use the frontend IP address as the routing next-hop for destination addresses on the public networks and the internet.

Step 1: In **Home > Load Balancers**, click **Add**.

Step 2: In the **Name** box, enter **ARA-CommonFW-Internal**.

Step 3: In the Type section, select **Internal**.

Step 4: In the SKU section, select **Standard**.

Step 5: Click the **Virtual network** *Choose a virtual network* section, and select **AzureRefArch-VNET**.

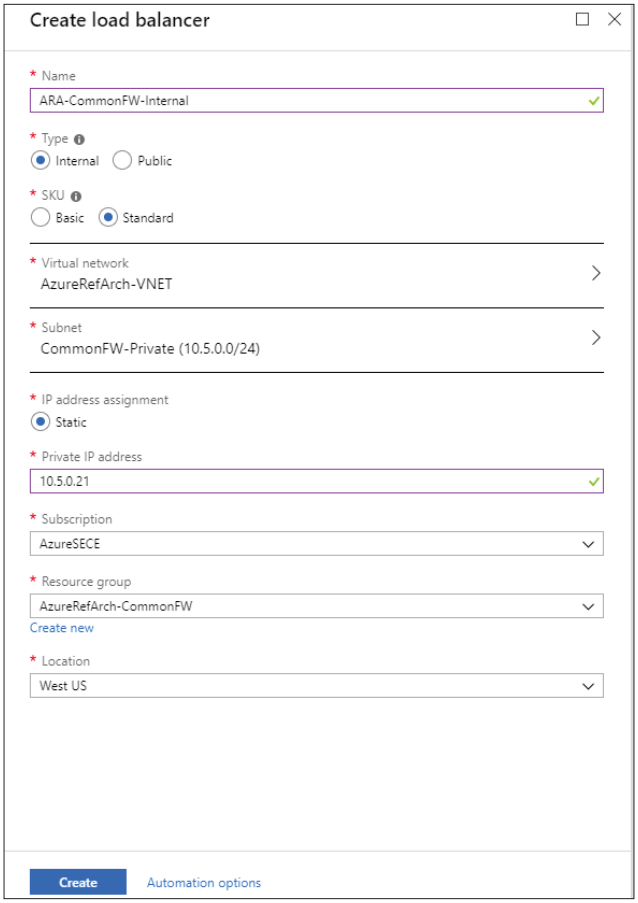
Step 6: Click the **Subnet** *Choose a subnet* section, and select **CommonFW-Private**.

Step 7: In the IP address assignment section, select **Static**.

Step 8: In the **Private IP address** box, enter **10.5.0.21**.

This address is associated with the default frontend IP configuration (**LoadBalancerFrontEnd**), which is used for outbound, east/west and backhaul access. Additional frontend IP addresses may be added to the load-balancer if necessary after it has been created.

Step 9: In the **Resource Group** list, select **AzureRefArch-CommonFW**, and then click **Create**.



7.10 Configure the Azure Internal Load-Balancer for Outbound Traffic

Step 1: In **Home > Load Balancers > ARA-CommonFW-Internal**, click **Health probes**, and then click **Add**.

Step 2: In the **Name** box, enter **HTTPS-Probe**.

Step 3: In the **Port** box, enter **443**, and then click **OK**.

Step 4: In **Home > Load Balancers > ARA-CommonFW-Internal**, click **Backend pools**, and then click **Add**.

Step 5: In the **Name** box, enter **Firewall-Layer-Private**.

Step 6: In the **Virtual network** list, select **azurerefarch-vnet (X VM)**, where X is the total number of virtual machines already deployed in your VNet.

Step 7: In the **VIRTUAL MACHINE** column, select a VM-Series to be added to this backend pool (example: **aracf-vmfw1**).

Step 8: In the **IP ADDRESS** column, select the **IP configuration** that is associated to the **CommonFW-Private** subnet. (example: **ipconfig-trust**).

Step 9: Repeat Step 7 and Step 8 for all VM-Series firewalls that are to be assigned to this backend pool.

Step 10: Click **Add**.

Step 11: In **Home > Load Balancers > ARA-CommonFW-Internal**, click **Load balancing rules**, and then click **Add**.

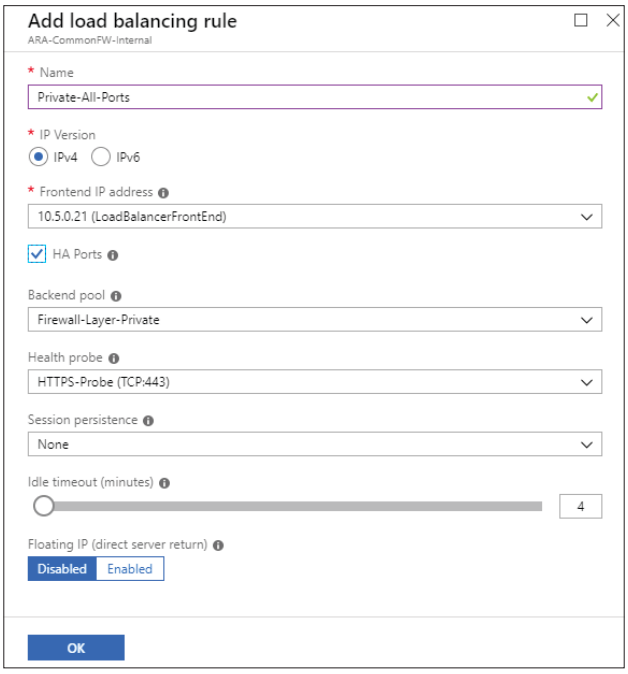
Step 12: In the **Name** box, enter **Private-All-Ports**.

Step 13: In the **Frontend IP address** list, select **LoadBalancerFrontEnd**.

Step 14: Select **HA ports**.

Step 15: In the **Backend pool** list, select **Firewall-Layer-Private**.

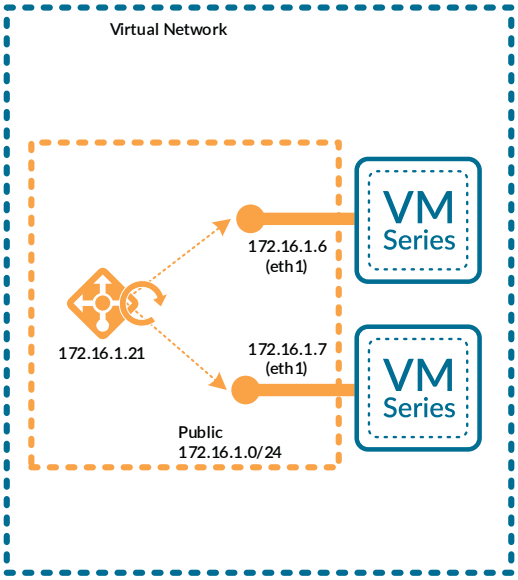
Step 16: In the **Health probe** list, select **HTTPS-Probe**, and then click **OK**.



7.11 Configure the Azure Internal Load-Balancer for Inbound Traffic

This procedure is required only if you have resources in the CommonFW-Public subnet that need access to the private networks. Because this subnet uses Azure internal addressing, you cannot use the public load-balancer but instead use an additional frontend IP address and backend pool on the internal load-balancer.

Figure 14 Azure internal load-balancer for inbound access



The frontend IP address is used as the routing next-hop for destination address on the private networks.

Step 1: In **Home > Load Balancers > ARA-CommonFW-Internal**, click **Frontend IP configuration**, and then click **Add**.

Step 2: In the **Name** box, enter **Internal-Frontend-Public**.

Step 3: In the **Subnet** list, select **CommonFW-Public**.

Step 4: In the Assignment section, select **Static**.

Step 5: In the **IP address** box, enter **172.16.1.21**.

Step 6: In **Home > Load Balancers > ARA-CommonFW-Internal**, click **Backend pools**, and then click **Add**.

Step 7: In the **Name** box, enter **Firewall-Layer-Public**.

Step 8: In the **Virtual network** list, select **azurerefarch-vnet (X VM)**, where X is the total number of virtual machines already deployed in your VNet.

Step 9: In the **VIRTUAL MACHINE** column, select a VM-Series to be added to this backend pool (example: **aracf-vmfw1**).

Step 10: In the **IP ADDRESS** column, select the **IP configuration** that is associated to the **CommonFW-Public** subnet. (example: **ipconfig-untrust**).

Step 11: Repeat Step 9 and Step 10 for all VM-Series firewalls that are to be assigned to this backend pool.

Step 12: Click **Add**.

Step 13: In **Home > Load Balancers > ARA-CommonFW-Internal**, click **Load balancing rules**, and then click **Add**.

Step 14: In the **Name** box, enter **Public-All-Ports**.

Step 15: In the **Frontend IP address** list, select **Internal-Frontend-Public**.

Step 16: Select **HA ports**.

Step 17: In the **Backend pool** list, select **Firewall-Layer-Public**.

Step 18: In the **Health probe** list, select **HTTPS-Probe**, and then click **OK**.

7.12 Configure Azure User Defined Routes

Azure Networking automatically creates system routes for the address space defined in the VNet. Additional system routes are also added to the Azure route table, including a default route to the internet and null routes for RFC-1918 and RFC-6598 ranges.

Override the Azure system routes with user-defined routes (UDRs) in order to isolate subnets and to logically insert virtual devices such as load-balancers and firewalls into the traffic forwarding path.

Note

Data traffic is not forwarded to the firewalls within the VNet until UDRs are created to direct traffic to the firewalls. In a resilient environment, data traffic is directed to load-balancers that act as frontends for the firewalls contained in their backend pools.

Table 15 Azure system routes

Address space	Address prefix	Next-hop type
VNet defined	192.168.1.0/24	Virtual Network
VNet defined	172.16.0.0/23	Virtual Network
VNet defined	10.5.0.0/16	Virtual Network
Default (Azure defined)	0.0.0.0/0	Internet
RFC-1918 (Azure defined)	10.0.0.0/8	None
RFC-1918 (Azure defined)	172.16.0.0/12	None
RFC-1918 (Azure defined)	192.168.0.0/16	None
RFC-6598 (Azure defined)	100.64.0.0/10	None

If you add a UDR with the same prefix and prefix-length as a system route, the UDR becomes the active route, and the state of the original system route changes to an Invalid state.

If you add a UDR with a more specific prefix that falls within the address space of a system route, the UDR becomes an active route, and the original system route also remains in an Active state.

Caution

The use of UDR summary routes may have unexpected consequences. If you apply a UDR summary to a subnet that falls within the summary but does not have a more specific UDR, traffic within the subnet (host to host) is controlled by the UDR.

As an example, if you applied a UDR for 10.5.0.0/16 with a next-hop of 10.5.0.21 (firewall load-balancer) to the 10.5.1.0/24 subnet, then traffic between host 10.5.1.4 and host 10.5.1.5 is routed through the firewall as intrazone traffic. This effectively causes microsegmentation.

Azure networking does not have a concept of equal cost paths; you cannot add multiple UDRs with same prefix and prefix-length with different next-hops to perform traffic load-balancing. The only method by which you may perform load-balancing is by using UDRs to forward traffic to an Azure load-balancing resource.

The effective routing table after adding UDRs is evaluated using traditional routing rules based on longest match of the destination address.

Figure 15 User-defined routes with common firewall option

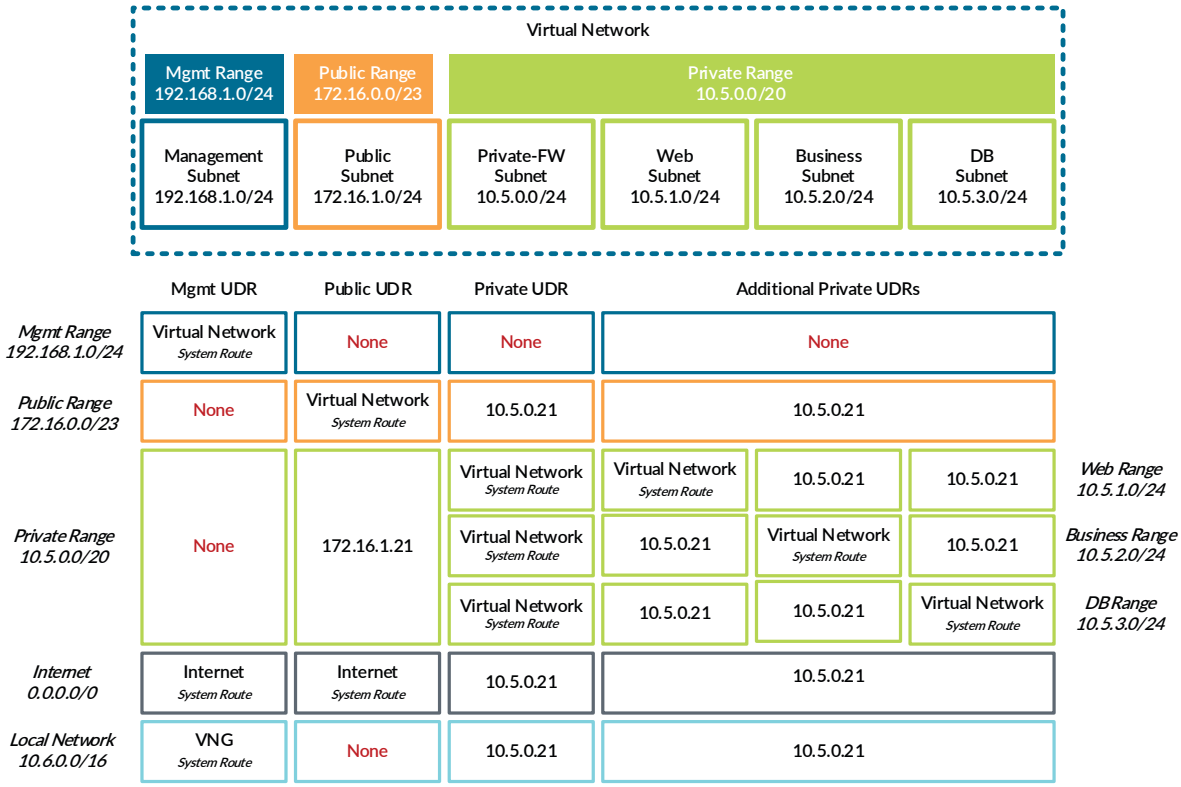


Table 16 Azure route tables

Subnet	Route table name	Resource group	Table of UDRs
Management	ARA-Management	AzureRefArch	Table 17
CommonFW-Public	ARACF-Public	AzureRefArch-CommonFW	Table 18
CommonFW-Private	ARACF-Private	AzureRefArch-CommonFW	Table 19
CommonFW-Web	ARACF-Web	AzureRefArch-CommonFW	Table 20
CommonFW-Business	ARACF-Business	AzureRefArch-CommonFW	Table 21
CommonFW-DB	ARACF-DB	AzureRefArch-CommonFW	Table 22

Table 17 Management subnet UDRs (192.168.1.0/24)

Route name	Address prefix	Next-hop type	Next-hop address	Comments
Blackhole-Public	172.16.0.0/23	None	—	Block traffic to Public IP address space
Blackhole-Private	10.5.0.0/20	None	—	Block traffic to Private IP address space

Table 18 Public subnet UDRs (172.16.1.0/24)

Route name	Address prefix	Next-hop type	Next-hop address	Comments
Blackhole-Management	192.168.1.0/24	None	—	Block traffic to Management IP address space
Net-10.5.0.0_20	10.5.0.0/20	Virtual appliance	172.16.1.21	Frontend IP of load-balancer

Table 19 Private subnet UDRs (10.5.0.0/24)

Route name	Address prefix	Next-hop type	Next-hop address	Comments
Blackhole-Management	192.168.1.0/24	None	—	Block traffic to Management IP address space
Net-172.16.0.0_23	172.16.0.0/23	Virtual appliance	10.5.0.21	Frontend IP of load-balancer
UDR-default	0.0.0.0/0	Virtual appliance	10.5.0.21	Frontend IP of load-balancer. Overrides system route

Table 20 Web subnet UDRs (10.5.1.0/24)

Route name	Address prefix	Next-hop type	Next-hop address	Comments
Blackhole-Management	192.168.1.0/24	None	—	Block traffic to Management IP address space
Net-172.16.0.0_23	172.16.0.0/23	Virtual appliance	10.5.0.21	Frontend IP of load-balancer
UDR-default	0.0.0.0/0	Virtual appliance	10.5.0.21	Frontend IP of load-balancer Overrides system route
Net-10.5.2.0_24 (optional for intrazone)	10.5.2.0/24	Virtual appliance	10.5.0.21	Frontend IP of load-balancer
Net-10.5.3.0_24 (optional for intrazone)	10.5.3.0/24	Virtual appliance	10.5.0.21	Frontend IP of load-balancer

Table 21 Business subnet UDRs (10.5.2.0/24)

Route name	Address prefix	Next-hop type	Next-hop address	Comments
Blackhole-Management	192.168.1.0/24	None	—	Block traffic to Management IP address space
Net-172.16.0.0_23	172.16.0.0/23	Virtual appliance	10.5.0.21	Frontend IP of load-balancer
UDR-default	0.0.0.0/0	Virtual appliance	10.5.0.21	Frontend IP of load-balancer. Overrides system route
Net-10.5.1.0_24 (optional for intrazone)	10.5.1.0/24	Virtual appliance	10.5.0.21	Frontend IP of load-balancer
Net-10.5.3.0_24 (optional for intrazone)	10.5.3.0/24	Virtual appliance	10.5.0.21	Frontend IP of load-balancer

Table 22 DB subnet UDRs (10.5.3.0/24)

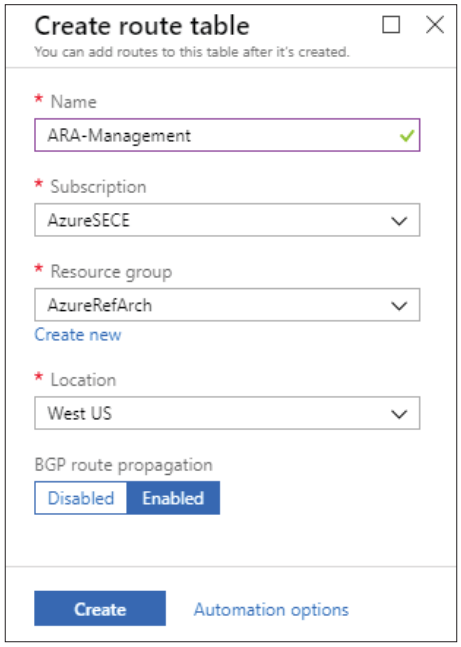
Route name	Address Prefix	Next-hop type	Next-hop address	Comment
Blackhole-Management	192.168.1.0/24	None	—	Block traffic to Management IP address space
Net-172.16.0.0_23	172.16.0.0/23	Virtual appliance	10.5.0.21	Frontend IP of load-balancer
UDR-default	0.0.0.0/0	Virtual appliance	10.5.0.21	Frontend IP of load-balancer. Overrides system route
Net-10.5.1.0_24 (optional for intrazone)	10.5.1.0/24	Virtual appliance	10.5.0.21	Frontend IP of load-balancer
Net-10.5.2.0_24 (optional for intrazone)	10.5.2.0/24	Virtual appliance	10.5.0.21	Frontend IP of load-balancer

Repeat this procedure for each entry in Table 16:

Step 1: In **Home** > **Route** tables, click **Add**.

Step 2: In the **Name** box, enter **ARA-Management**.

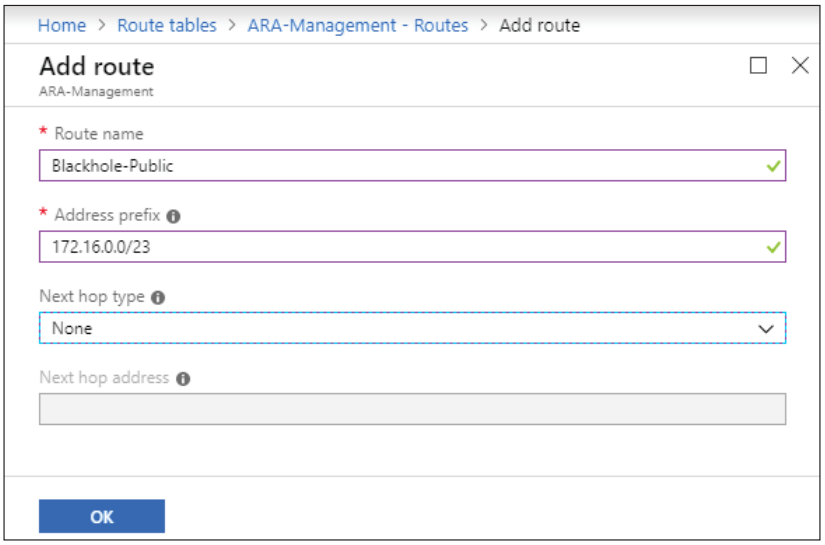
Step 3: In the **Resource Group** list, select **AzureRefArch**, and then click **Create**.



Step 4: In **Home** > **Route tables** > **ARA-Management**, click **Routes**.

Step 5: Repeat these substeps for all entries in the table of UDRs:

- In **Home > Routes tables > ARA-Management—Routes**, click **Add**.
- In the **Route name** box, enter **Blackhole-Public**.
- In the **Address prefix** box, enter **172.16.0.0/23**.
- In the **Next hop type** list, select **None**.
- If the next-hop type is **Virtual appliance**, then enter the **Next hop address** value.
- Click **OK**.



7.13 Apply Route Tables to Subnets

The UDRs take effect only after the route table is associated with the subnet.

Step 1: In **Home > Virtual networks > AzureRefArch-VNET**, click **Subnets**.

Step 2: Click **Management**.

Step 3: Click the **Route table** section, and then in the Resource pane, select **ARA-Management**.

Step 4: Click **Save**, and then click **X** to Close.

Step 5: Repeat Step 2 through Step 4 for each entry in Table 16.

Procedures

Using Panorama to Configure Centralized Security Policy and NAT Policy

This procedure group includes the objects, NAT policy rules, and security policy rules for each of the traffic profiles in the common firewall option:

- Inbound access traffic profile with public load balancer
- Inbound access traffic profile with application gateway
- Outbound access traffic profile
- East/West traffic profile

Each traffic profile is described and configured separately so that you can cover the significant differences in detail and in context.

All procedures and steps in this procedure group are performed on Panorama.

> **Note**
>
> Verify that you have selected the proper device group for the following procedures.

8.1 Create Logging Profile for Logging Service

This procedure creates the log-forwarding profile to send security policy logs to Logging Service. This profile is associated to security policy rules used in each of three traffic profiles. Because the log forwarding profile is referenced in every security policy rule, you must complete this procedure first.

Step 1: Log in to Panorama (example: https://ara-panorama-1.westus.cloudapp.azure.com).

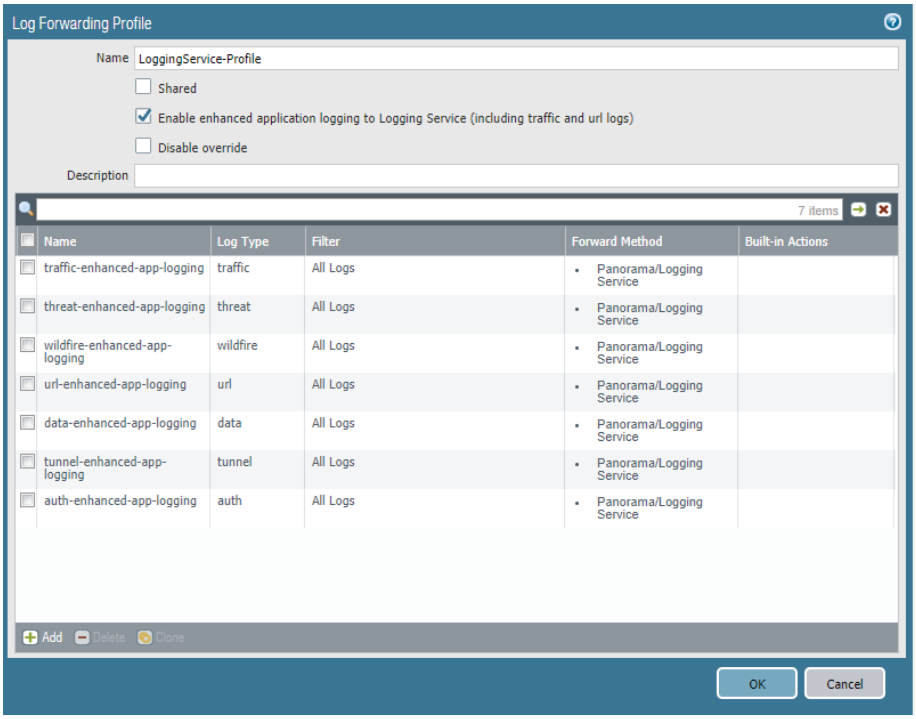
Step 2: Navigate to **Device Groups > Objects**.

Step 3: In the **Device Group** list, select **Azure-CommonFW**.

Step 4: In **Device Groups > Objects > Log Forwarding**, click **Add**.

Step 5: In the **Name** box, enter **LoggingService-Profile**.

Step 6: Select **Enable enhanced application logging to Logging Service (including traffic and url logs),** and then click **OK**.



8.2 All Traffic Profiles—Permit Azure Probes

The health probes from Azure load balancer must be permitted on the firewall interfaces. The probes are sent periodically at 3 second intervals, which generates a significant amount of firewall logs. This procedure creates a security policy rule that explicitly permits the probes and suppresses any logging from matches to the rule.

We recommend the use of an explicit rule to permit the probes instead of relying on the default intrazone rule. This rule is configured in the parent device group with a security Pre Rule and is inherited by the child device groups.

Step 1: Log in to Panorama (example: https://ara-panorama-1.westus.cloudapp.azure.com).

Step 2: Navigate to **Device Groups > Objects**.

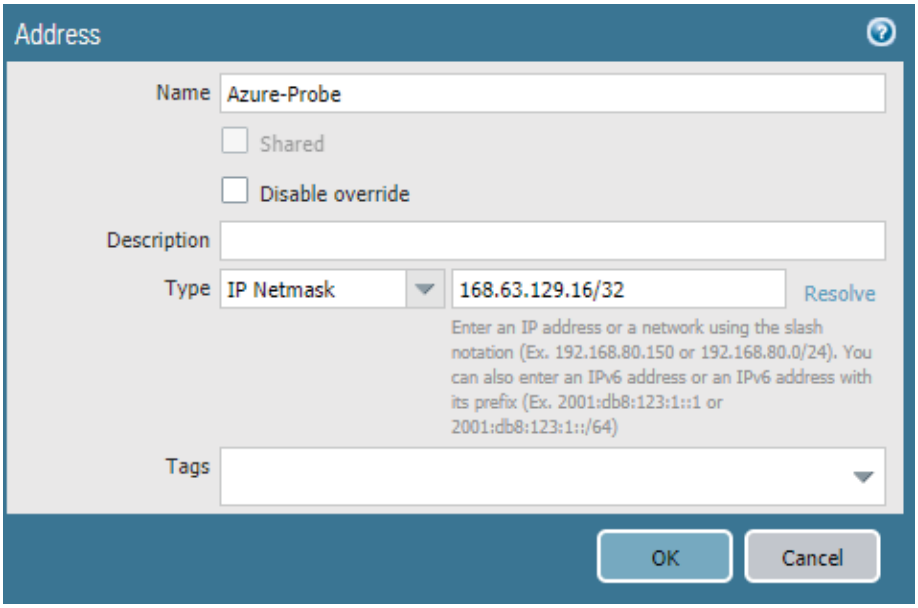
Step 3: In the **Device Group** list, select **Azure-CommonFW**.

Step 4: In **Device Groups > Objects > Addresses**, click **Add**.

Step 5: In the **Name** box, enter **Azure-Probe**.

Step 6: In the **Type** list, select **IP Netmask**.

Step 7: In the **Type value** box, enter **168.63.129.16/32**, and then click **OK**.



Step 8: In **Device Groups > Policies > Security > Pre Rules**, click **Add**.

Step 9: In the **Name** box, enter **Permit Azure Probes and Suppress Logs**.

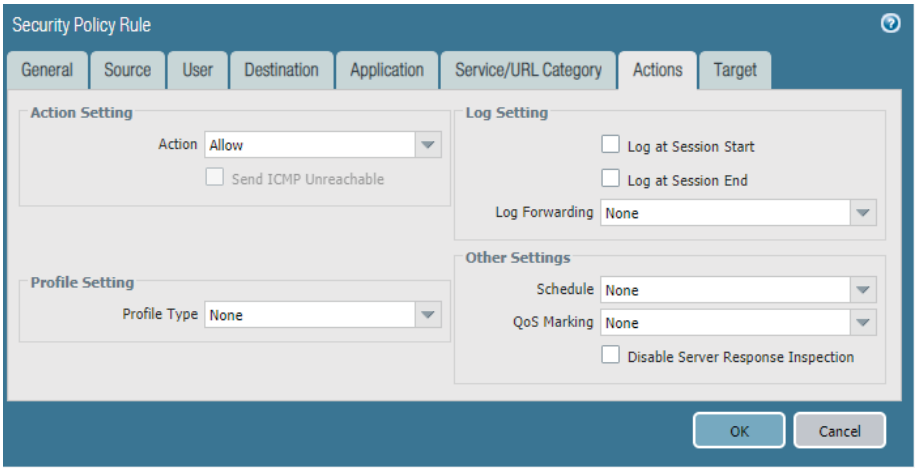
Step 10: In the **Rule Type** list, select **intrazone**.

Step 11: On the Source tab, in the Source Zone pane, select **Any**.

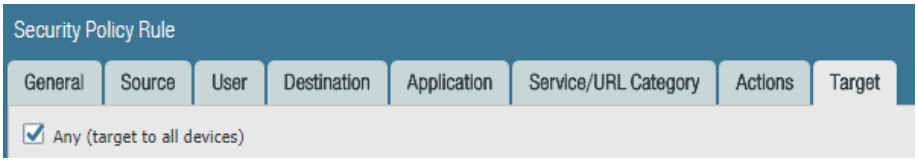
Step 12: In the Source Address pane, click **Add**, and then select **Azure-Probe**.

Step 13: On the Actions tab, in the Action Setting section, in the **Action** list, select **Allow**.

Step 14: In the Log Setting section, clear **Log at Session End**.



Step 15: On the Target tab, verify that **Any (target to all devices)** is selected, and then click **OK**.



Caution

Make sure to target all devices (any) in the device group; otherwise, the policy rule will not be automatically applied to new group members.

					Source			Destination					
	Name	Location	Tags	Type	Zone	Address	User	Zone	Address	Application	Service	Action	Target
1	Permit Azure Probes and Suppress Logs	Azure-CommonFW	none	intrazone	any	Azure-Probe	any	(intrazone)	any	any	application-default	Allow	any

Step 16: On the **Commit** menu, click **Commit and Push**.

8.3 Inbound Access (Public Load Balancer)—Create Address Objects

This procedure assumes that you have already deployed a set of web server resources in the CommonFW-Web subnet. In a resilient web server model, the web servers are in a backend pool of an Azure internal load-balancer. The load-balancer frontend IP is referenced by security and NAT policy rules and should be defined as an address object (example: **10.5.0.20**). This guide does not include the procedures to create this load-balancer or to create the web server resources.

Table 23 Inbound traffic address objects

Object name	Description	Type	Type value
Web-Public-LB-FQDN	FQDN of public web server	FQDN	aracf-public-web.westus.cloudapp.azure.com
Web-Private-LB	IP address of private internal load balancer	IP Netmask	10.5.0.20/32

Step 1: Log in to Panorama (example: https://ara-panorama-1.westus.cloudapp.azure.com).

Step 2: Navigate to **Device Groups > Objects**.

Step 3: In the **Device Group** list, select **Azure-CommonFW**.

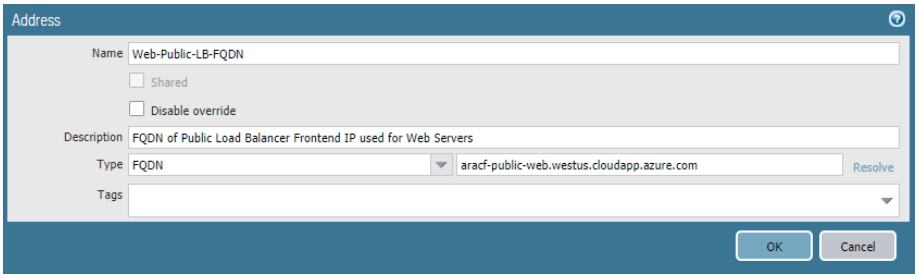
Step 4: In **Device Groups > Objects > Addresses**, click **Add**.

Step 5: In the **Name** box, enter **Web-Public-LB-FQDN**.

Step 6: In the **Type** list, select **FQDN**.

Step 7: In the **Type value** box, enter **aracf-public-web.westus.cloudapp.azure.com**, and then click **OK**.

Step 8: Repeat Step 4 through Step 7 for all rows in Table 23.



8.4 Inbound Access (Public Load Balancer)—Configure NAT Policy

This procedure uses NAT Pre Rules. These rules are logically evaluated prior to local rules and cannot be locally overridden on the local device.

Step 1: Log in to Panorama (example: https://ara-panorama-1.westus.cloudapp.azure.com).

Step 2: Navigate to **Device Groups > Policies**.

Step 3: In the **Device Group** list, select **Azure-CommonFW**.

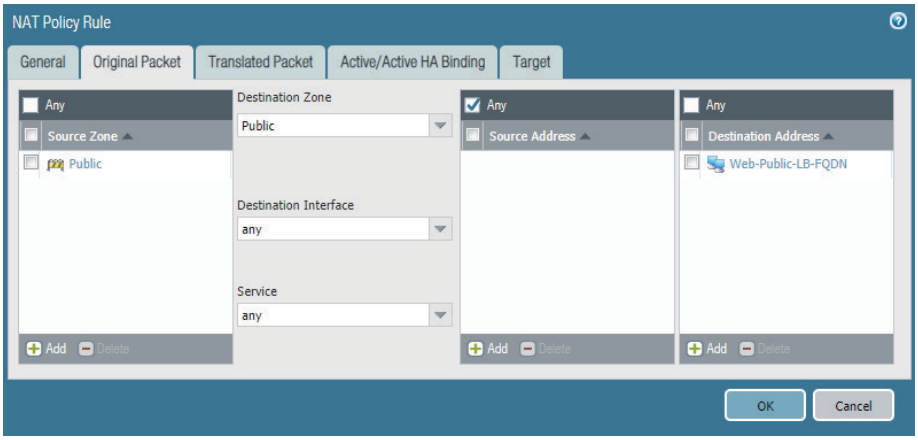
Step 4: In **Device Groups > Policies > NAT > Pre Rules**, click **Add**.

Step 5: In the **Name** box, enter **Inbound-Web**.

Step 6: On the Original Packet tab, in the Source Zone pane, click **Add** and select **Public**.

Step 7: In the **Destination Zone** list, select **Public**.

Step 8: In the Destination Address pane, click **Add**, and then select **Web-Public-LB-FQDN**.



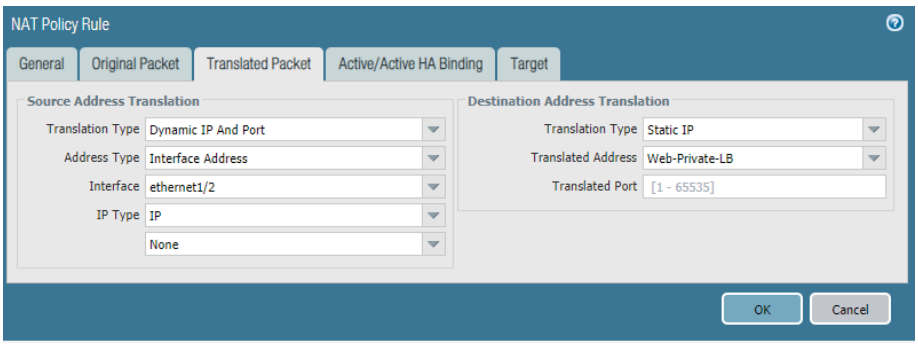
Step 9: On the Translated Packet tab, in the Source Address Translation section, in the **Translation Type** list, select **Dynamic IP And Port**.

Step 10: In the Source Address Translation section, in the **Address Type** list, select **Interface Address**.

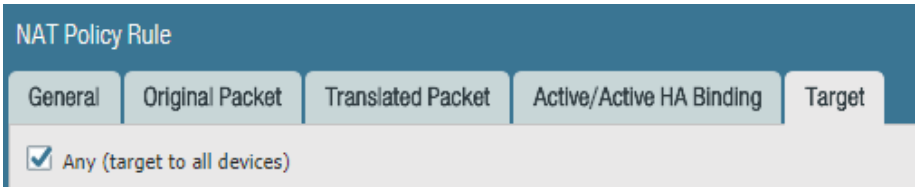
Step 11: In the Source Address Translation section, in the **Interface** list, select **ethernet1/2**.

Step 12: In the Destination Address Translation section, in the **Translation Type** list, select **Static IP**.

Step 13: In the Destination Address Translation section, in the **Translated Address** list, select **Web-Private-LB**.



Step 14: On the Target tab, verify that **Any (target to all devices)** is selected.



Caution

Make sure to target all devices in the device group; otherwise, the policy rule will not be automatically applied to new group members.

8.5 Inbound Access (Public Load Balancer)—Configure Security Policy

This procedure uses security Pre Rules. These rules are logically evaluated prior to local rules and cannot be locally overridden on the local device.

The security policy example for the Inbound Access Profile permits these applications:

- Web browsing (web-browsing)
- SSL (ssl)

Add additional applications to your policy as required.

Step 1: In **Device Groups > Policies > Security > Pre Rules**, click **Add**.

Step 2: In the **Name** box, enter **Inbound-Web**.

Step 3: On the Source tab, in the Source Zone pane, click **Add**, and then select **Public**.

Step 4: On the Destination tab, in the Destination Zone pane, click **Add**, and then select **Private**.

Step 5: In the Destination Address pane, click **Add,** and then select **Web-Public-LB-FQDN**.

Step 6: On the Application tab, in the Applications pane, click **Add**, and then enter/search/select **web-browsing**.

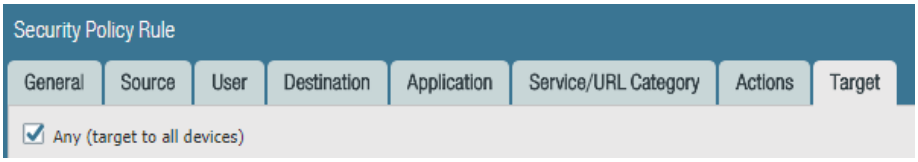
Step 7: In the Applications pane, click **Add**, and then enter/search/select **ssl**.

Step 8: On the Service/URL Category tab, in the Service pane, select **application-default**.

Step 9: On the Actions tab, in the Action Setting section, in the **Action** list, select **Allow**.

Step 10: In the Log Setting section, in the **Log Forwarding** list, select **LoggingService-Profile**.

Step 11: On the Target tab, verify that **Any (target to all devices)** is selected, and then click **OK**.



Caution

Make sure to target all devices (any) in the device group; otherwise, the policy rule will not be automatically applied to new group members.

				Source		Destination					
	Name	Location	Type	Zone	Address	Zone	Address	Application	Service	Action	Target
2	Inbound-Web	Azure-CommonFW	universal	Public	any	Private	Web-Public-LB-FQDN	ssl web-browsing	application-default	Allow	any

Step 12: On the **Commit** menu, click **Commit and Push**.

8.6 Inbound Access (Application Gateway)—Enable XFF

The application gateway is a proxy and masks the original source IP address of incoming connections so that the firewall sees only the source IP addresses of the application gateway instances. The application gateway adds the original source address information to the HTTP packet header, by using the X-Forwarded-For (XFF) HTTP header field. The firewall is configured to extract XFF information from the session and add the original source IP address information to the logs.

Step 1: Log in to Panorama (example: https://ara-panorama-1.westus.cloudapp.azure.com)

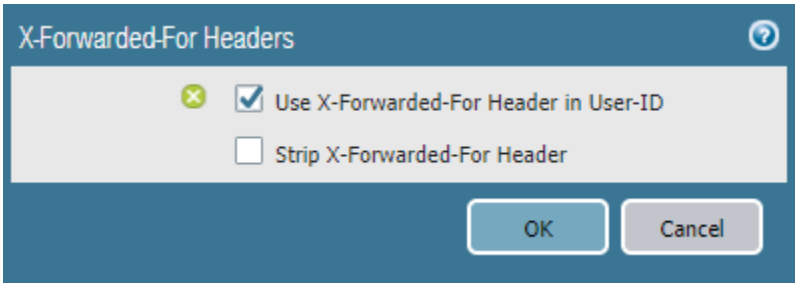
Step 2: Navigate to **Templates > Device**.

Step 3: In the **Template** list, select **Azure-3-Zone**.

Step 4: Navigate to **Templates > Device > Setup > Content-ID.**

Step 5: In the **X-Forwarded-For Headers** section, click the Edit cog.

Step 6: Select **Use X-Forwarded-For Header in User-ID**, and then click **OK**.



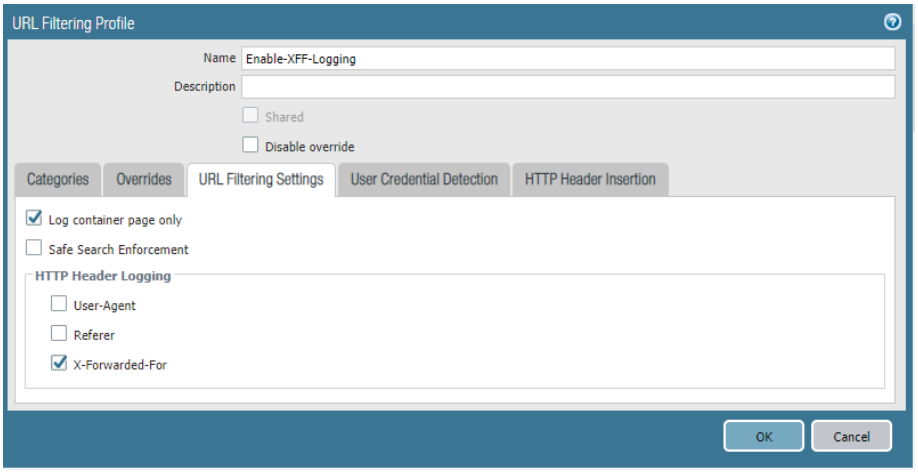
Step 7: Navigate to **Device Groups > Objects**.

Step 8: In the **Device Group** list, select **Azure-CommonFW**.

Step 9: In **Device Groups > Objects > Security Profiles > URL Filtering**, click **Add.**

Step 10: In the URL Filtering Profile pane, in the **Name** box, enter **Enable-XFF-Logging**.

Step 11: On the URL Filtering Settings tab, in the **HTTP Header Logging** section, select **X-Forwarded-For**, and then click **OK**.



8.7 Inbound Access (Application Gateway)—Create Address Objects

This procedure assumes that you have already deployed a set of web server resources in the CommonFW-Web subnet. In a resilient web server model, the web servers are in a backend pool of an Azure internal load-balancer. The load-balancer frontend IP is referenced by security and NAT policy rules and should be defined as an address object (example: **10.5.0.101**).

Table 24 Inbound traffic address objects

Object name	Description	Type	Type value
AppGW-Instance-1	Application gateway (Instance 1)	IP Netmask	172.16.0.4/32
AppGW-Instance-2	Application gateway (Instance 2)	IP Netmask	172.16.0.5/32
AppGW-Internal-LB	IP address of AppGW internal load-balancer	IP Netmask	10.5.0.101/32
Direct-Web	IP address of web server resource (does not require ILB)	IP Netmask	10.5.1.4/32

Step 1: Log in to Panorama (example: https://ara-panorama-1.westus.cloudapp.azure.com).

Step 2: Navigate to **Device Groups > Objects**.

Step 3: In the **Device Group** list, select **Azure-CommonFW**.

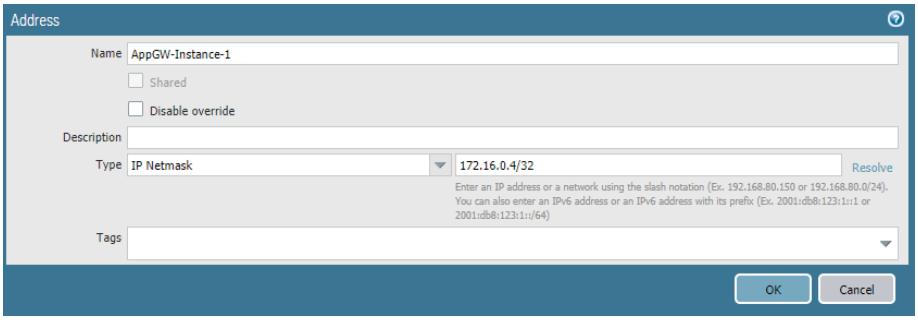
Step 4: In **Device Groups > Objects > Addresses**, click **Add**.

Step 5: In the **Name** box, enter **AppGW-Instance-1**.

Step 6: In the **Type** list, select **IP Netmask**.

Step 7: In the **Type value** box, enter **172.16.0.4/32**, and then click **OK**.

Step 8: Repeat Step 4 through Step 7 for all rows in Table 24.



8.8 Inbound Access (Application Gateway)—Configure NAT Policy

This procedure uses NAT Pre Rules. These rules are logically evaluated prior to local rules and cannot be locally overridden on the local device.

The application gateway is configured to send web traffic on multiple non-standard ports as well as the standard ports (80/443). To simplify the configuration of the NAT and security policies, a custom service is created for each non-standard port that is not predefined. The configuration example in this guide uses the destination ports as listed in Table 25.

> **Note**
>
> Do not use TCP/8080 as a non-standard port; this port is already predefined as service-http. You must manually remove this port from the predefined service and create a new service in order to create an explicit NAT rule using this port.

Table 25 Services for application gateway

Name	Type	Destination port
service-http	Predefined	TCP/80 TCP/8080
service-https	Predefined	TCP/443
service-http-8000	Custom	TCP/8000
service-http-8081	Custom	TCP/8081
service-http-8443	Custom	TCP/8443

Step 1: Log in to Panorama (example: https://ara-panorama-1.westus.cloudapp.azure.com).

Step 2: Navigate to **Device Groups > Objects**.

Step 3: In the **Device Group** list, select **Azure-CommonFW**.

Step 4: In **Device Groups > Objects > Services**, click **Add**.

Step 5: In the **Name** box, enter **service-http-8000**.

Step 6: In the **Destination Port** box, enter **8000**, and then click **OK**.

Step 7: Repeat Step 4 through Step 6 for all rows in Table 25.

Each firewall needs a unique set of NAT policy rules. In each set, the destination address of the original packet is always set to the IP address of the public interface of each firewall. Table 26 lists only two firewalls as targets. If your firewall layer includes additional firewalls, then you must add a new set of rules for each additional firewall.

Each application gateway HTTP/HTTPS backend as specified in Table 13 must have a corresponding NAT translation rule on each firewall. The original packet service (or destination TCP port) is mapped to a translated address and translated port by the firewall that corresponds to an actual backend resource in the private networks. These resources can be either load-balancer front-ends or actual servers. You already created address objects for the backend resources in Procedure 8.7.

Table 26 NAT translation rules for application gateway

Name	Service	Source objects	Destination address	Translated address/ translated port	Target firewall
Inbound-AppGW-FW-1_HTTP-80	service-http	AppGW-Instance-1 AppGW-Instance-2	172.16.1.6/32	AppGW-Internal-LB/80	ARACF-VMFW1
Inbound-AppGW-FW-2_HTTP-80	service-http	AppGW-Instance-1 AppGW-Instance-2	172.16.1.7/32	AppGW-Internal-LB/80	ARACF-VMFW2
Inbound-AppGW-FW-1_HTTP-8000	service-http-8000	AppGW-Instance-1 AppGW-Instance-2	172.16.1.6/32	Direct-Web/80	ARACF-VMFW1
Inbound-AppGW-FW-2_HTTP-8000	service-http-8000	AppGW-Instance-1 AppGW-Instance-2	172.16.1.7/32	Direct-Web/80	ARACF-VMFW2
Inbound-AppGW-FW-1_HTTP-8081	service-http-8081	AppGW-Instance-1 AppGW-Instance-2	172.16.1.6/32	AppGW-Internal-LB/8081	ARACF-VMFW1
Inbound-AppGW-FW-2_HTTP-8081	service-http-8081	AppGW-Instance-1 AppGW-Instance-2	172.16.1.7/32	AppGW-Internal-LB/8081	ARACF-VMFW2
Inbound-AppGW-FW-1_HTTPS-443	service-https	AppGW-Instance-1 AppGW-Instance-2	172.16.1.6/32	AppGW-Internal-LB/443	ARACF-VMFW1
Inbound-AppGW-FW-2_HTTPS-443	service-https	AppGW-Instance-1 AppGW-Instance-2	172.16.1.7/32	AppGW-Internal-LB/443	ARACF-VMFW2
Inbound-AppGW-FW-1_HTTP-8443	service-http-8443	AppGW-Instance-1 AppGW-Instance-2	172.16.1.6/32	AppGW-Internal-LB/8443	ARACF-VMFW1
Inbound-AppGW-FW-2_HTTP-8443	service-http-8443	AppGW-Instance-1 AppGW-Instance-2	172.16.1.7/32	AppGW-Internal-LB/8443	ARACF-VMFW2

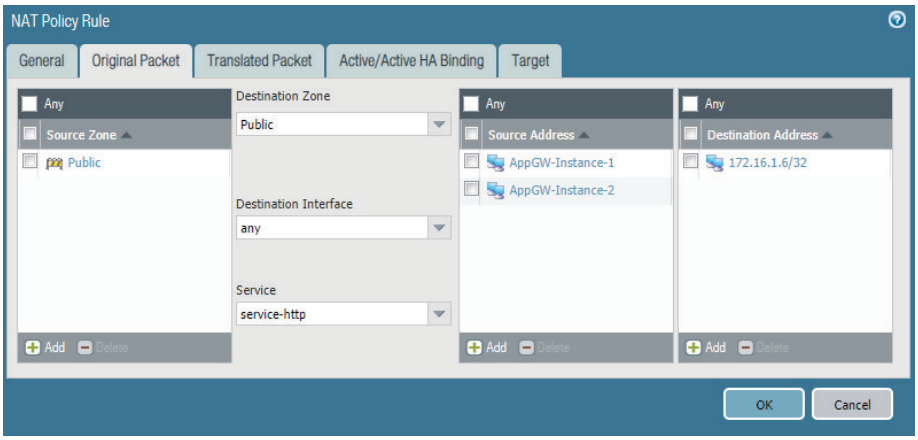
Step 8: Log in to Panorama (example: https://ara-panorama-1.westus.cloudapp.azure.com).

Step 9: Navigate to **Device Groups > Policies**.

Step 10: In the **Device Group** list, select **Azure-CommonFW**.

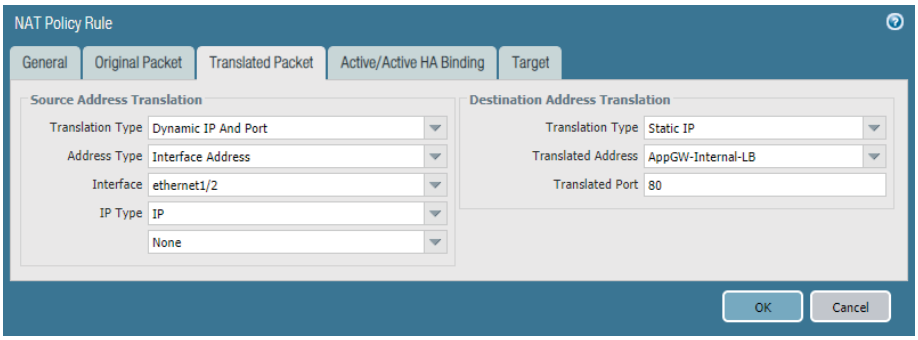
Step 11: For each entry in Table 26, perform the following substeps:

- In **Device Groups > Policies > NAT > Pre Rules**, click **Add**.
- In the **Name** box, enter **Inbound-AppGW-FW-1_HTTP-80**.
- On the Original Packet tab, in the Source Zone pane, click **Add** and select **Public**.
- In the **Destination Zone** list, select **Public**.
- In the Service list, select **service-http**.
- In the Source Address pane, click **Add** and select **AppGW-Instance-1**.
- In the Source Address pane, click **Add** and select **AppGW-Instance-2**.
- In the Destination Address pane, click **Add** and enter **172.16.1.6/32**.

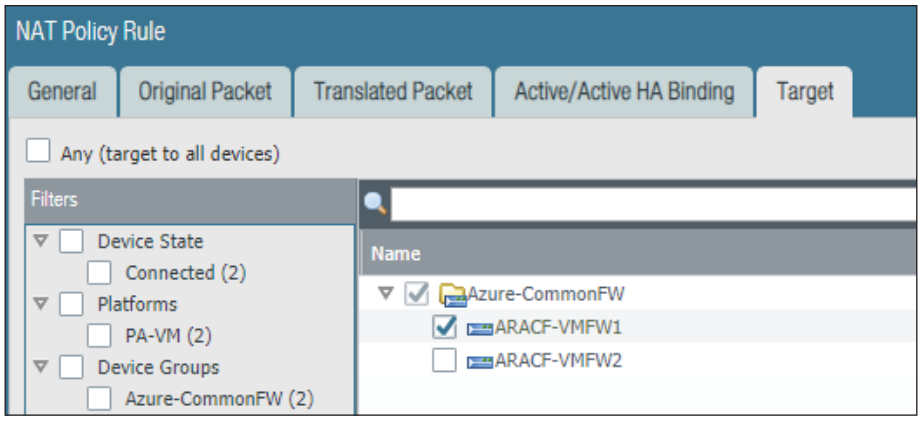


- On the Translated Packet tab, in the Source Address Translation section, in the **Translation Type** list, select **Dynamic IP And Port**.
- In the Source Address Translation section, in the **Address Type** list, select **Interface Address**.
- In the Source Address Translation section, in the **Interface list, select ethernet1/2**.
- In the Destination Address Translation section, in the **Translation Type** list, select **Static IP**.
- In the Destination Address Translation section, in the **Translated Address** list, select **AppGW-Internal-LB**.

- In the Destination Address Translation section, in the Translated Port box, enter **80**.



- On the Target tab, select only the firewall target from the current entry in the table (example: **ARACF-VMFW1**), and then click **OK**.



Your NAT policy rules for the application gateway should look similar to the following. Each firewall has a unique set of rules with similar policy. The target for each set of rules lists only one firewall.

Figure 16 NAT policy rules for first firewall

	Name	Location	Tags	Original Packet						Translated Packet		Active/Active HA Binding	Target
				Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation		
2	Inbound-AppGW-FW-1_HTTP-80	Azure-CommonFW	none	Public	Public	any	AppGW-Instance-1 AppGW-Instance-2	172.16.1.6/32	service-http	dynamic-ip-and-port ethernet1/2	destination-translation address: AppGW-Internal-LB port: 80	none	ARACF-VMFW1
4	Inbound-AppGW-FW-1_HTTP-8000	Azure-CommonFW	none	Public	Public	any	AppGW-Instance-1 AppGW-Instance-2	172.16.1.6/32	service-http-8000	dynamic-ip-and-port ethernet1/2	destination-translation address: Direct-Web port: 80	none	ARACF-VMFW1
6	Inbound-AppGW-FW-1_HTTP-8081	Azure-CommonFW	none	Public	Public	any	AppGW-Instance-1 AppGW-Instance-2	172.16.1.6/32	service-http-8081	dynamic-ip-and-port ethernet1/2	destination-translation address: AppGW-Internal-LB port: 8081	none	ARACF-VMFW1
8	Inbound-AppGW-FW-1_HTTPS-443	Azure-CommonFW	none	Public	Public	any	AppGW-Instance-1 AppGW-Instance-2	172.16.1.6/32	service-https	dynamic-ip-and-port ethernet1/2	destination-translation address: AppGW-Internal-LB port: 443	none	ARACF-VMFW1
10	Inbound-AppGW-FW-1_HTTP-8443	Azure-CommonFW	none	Public	Public	any	AppGW-Instance-1 AppGW-Instance-2	172.16.1.6/32	service-http-8443	dynamic-ip-and-port ethernet1/2	destination-translation address: AppGW-Internal-LB port: 8443	none	ARACF-VMFW1

Figure 17 NAT policy rules for second firewall

				Original Packet						Translated Packet			
	Name	Location	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation	Active/Active HA Binding	Target
3	Inbound-AppGW-FW-2_HTTP-80	Azure-CommonFW	none	Public	Public	any	AppGW-Instance-1 AppGW-Instance-2	172.16.1.7/32	service-http	dynamic-ip-and-port ethernet1/2	destination-translation address: AppGW-Internal-LB port: 80	none	ARACF-VMFW2
5	Inbound-AppGW-FW-2_HTTP-8000	Azure-CommonFW	none	Public	Public	any	AppGW-Instance-1 AppGW-Instance-2	172.16.1.7/32	service-http-8000	dynamic-ip-and-port ethernet1/2	destination-translation address: Direct-Web port: 80	none	ARACF-VMFW2
7	Inbound-AppGW-FW-2_HTTP-8081	Azure-CommonFW	none	Public	Public	any	AppGW-Instance-1 AppGW-Instance-2	172.16.1.7/32	service-http-8081	dynamic-ip-and-port ethernet1/2	destination-translation address: AppGW-Internal-LB port: 8081	none	ARACF-VMFW2
9	Inbound-AppGW-FW-2_HTTPS-443	Azure-CommonFW	none	Public	Public	any	AppGW-Instance-1 AppGW-Instance-2	172.16.1.7/32	service-https	dynamic-ip-and-port ethernet1/2	destination-translation address: AppGW-Internal-LB port: 443	none	ARACF-VMFW2
11	Inbound-AppGW-FW-2_HTTP-8443	Azure-CommonFW	none	Public	Public	any	AppGW-Instance-1 AppGW-Instance-2	172.16.1.7/32	service-http-8443	dynamic-ip-and-port ethernet1/2	destination-translation address: AppGW-Internal-LB port: 8443	none	ARACF-VMFW2

8.9 Inbound Access (Application Gateway)—Configure Security Policy

This procedure uses security Pre Rules. These rules are logically evaluated prior to local rules and cannot be locally overridden on the local device.

The security policy example for the Inbound Access Profile permits these applications:

- Web browsing (web-browsing)
- SSL (ssl)

Each firewall needs a unique security policy rule. The destination address must match the IP address of the public interface of each firewall in Step 7. Table 27 lists only two firewalls as targets. If your firewall layer includes additional firewalls, then you must add a new rule for each additional firewall.

Table 27 Security policy rules for application gateway

Name	Source objects	Destination address	Target firewall
Inbound-AppGW-FW-1	AppGW-Instance-1 AppGW-Instance-2	172.16.1.6/32	ARACF-VMFW1
Inbound-AppGW-FW-2	AppGW-Instance-1 AppGW-Instance-2	172.16.1.7/32	ARACF-VMFW2

Step 1: In **Device Groups > Policies > Security > Pre Rules**, click **Add**.

Step 2: In the **Name** box, enter **Inbound-AppGW-FW-1**.

Step 3: On the Source tab, in the Source Zone pane, click **Add** and select **Public**.

Step 4: In the Source Address pane, click **Add** and select **AppGW-Instance-1**.

Step 5: In the Source Address pane, click **Add** and select **AppGW-Instance-2**.

Step 6: On the Destination tab, in the Destination Zone pane, click **Add** and select **Private**.

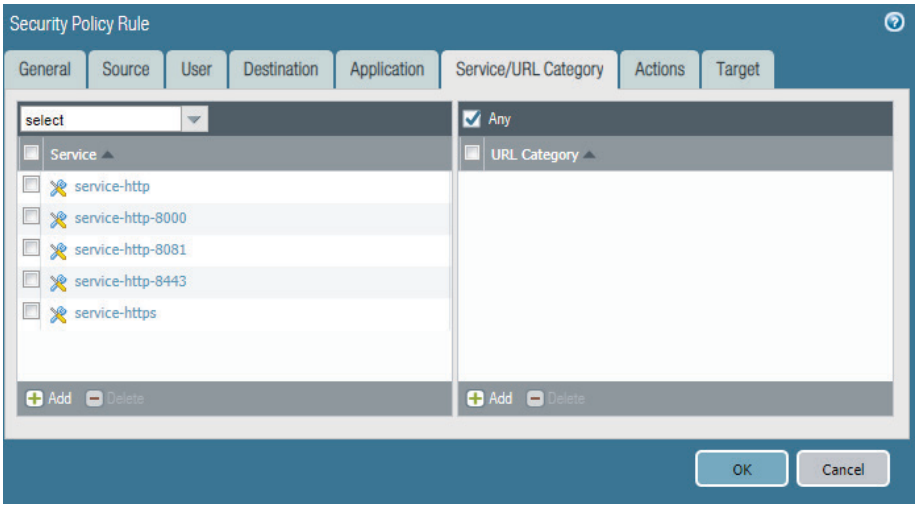
Step 7: In the Destination Address pane, click **Add** and enter **172.16.1.6/32**.

Step 8: On the Application tab, in the Applications pane, click **Add** and enter/search/select **web-browsing**.

Step 9: In the Applications pane, click **Add** and enter/search/select **ssl**.

The application gateway is configured to send web traffic on multiple non-standard ports as well as the standard ports (80/443). The firewall restricts web traffic on non-standard ports when application-default is configured. To permit web traffic on the non-standard ports, each service in use must be explicitly listed.

Step 10: On the Service/URL Category tab, in the Service pane, click **Add** and select each service listed in Table 25.



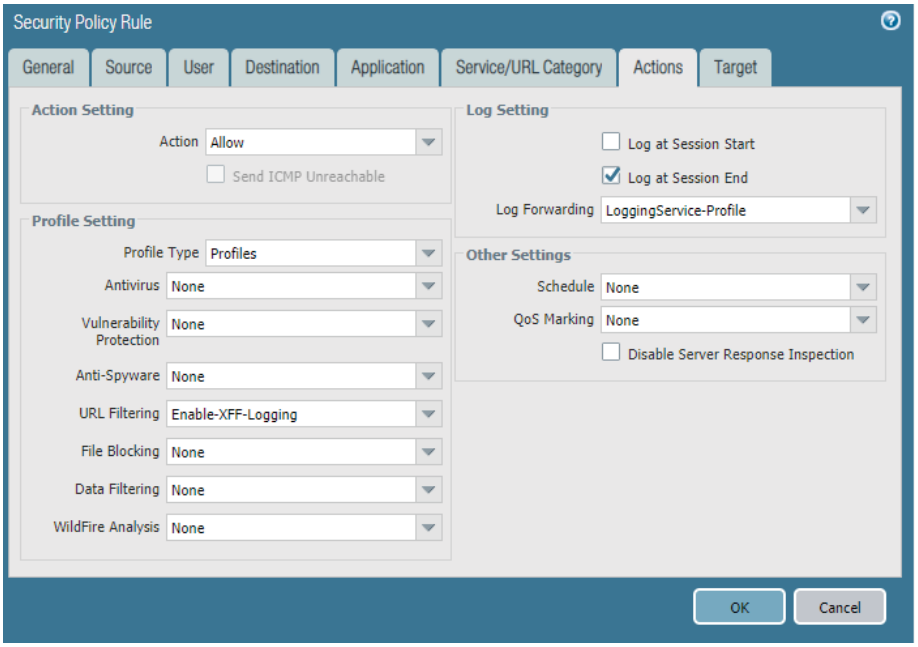
Step 11: On the Actions tab, in the Action Setting section, in the **Action** list, select **Allow**.

> **Note**
>
> To view the XFF header information for sessions, add the X-Forwarded-For column to the firewall's URL filtering log monitor default view.

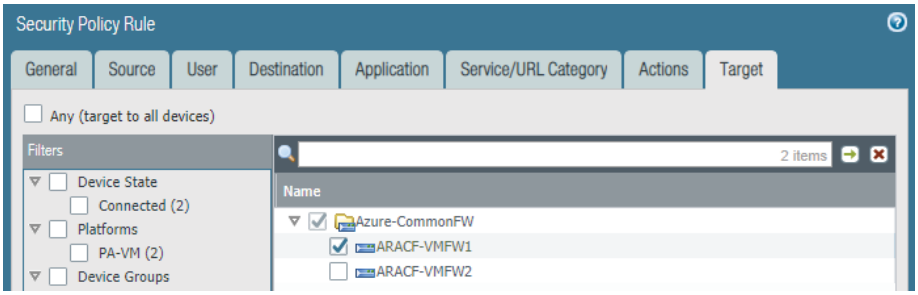
Step 12: In the Profile Setting section, in the **Profile Type** list, select **Profiles**.

Step 13: In the Profile Setting section, in the **URL Filtering** list, select **Enable-XFF-Logging**.

Step 14: In the Log Setting section, in the **Log Forwarding** list, select **LoggingService-Profile**.



Step 15: On the Target tab, select only the firewall target from the current entry in the table (example: **ARACF-VMFW1**), and then click **OK**.



Your security policy rules for the application gateway should look similar to the following. Each firewall has a unique rule with similar policy. The target for each rule lists only one firewall.

	Name	Location	Type	Source		Destination		Application	Service	Action	Target
				Zone	Address	Zone	Address				
3	Inbound-AppGW-FW-1	Azure-CommonFW	universal	Public	AppGW-Instance-1 AppGW-Instance-2	Private	172.16.1.6/32	ssl web-browsing	service-http service-http-8000 service-http-8081 service-http-8443 service-https	Allow	ARACF-VMFW1
4	Inbound--AppGW-FW-2	Azure-CommonFW	universal	Public	AppGW-Instance-1 AppGW-Instance-2	Private	172.16.1.7/32	ssl web-browsing	service-http service-http-8000 service-http-8081 service-http-8443 service-https	Allow	ARACF-VMFW2

Step 16: On the **Commit** menu, click **Commit and Push**.

8.10 Outbound Access—Create Public IP Address and Associate with Firewall

For virtual machines behind the firewall to communicate to devices on the internet, the firewall must translate the source IP address of the outbound traffic to an IP address on the public subnet. The simplest method is to use dynamic IP and port translation to the firewall's public interface IP address.

Azure then translates the source IP address again as the outbound traffic leaves the VNet. Because the firewall's public interface is a member of the Azure public load-balancer backend pool, Azure networking performs translation for only TCP/UDP ports referenced in the active load balancing rules. To support a broad range of services, create a new public IP address for the public interface of each firewall used for outbound access. This method supports all TCP/UDP ports.

Step 1: In **Home > Public IP addresses**, click **Add.**

Step 2: In the **Name** box, enter **ARA-CommonFW-vmfw1-outbound**.

Step 3: Select **Standard** SKU.

Step 4: In the **DNS name label** box, enter **aracf-vmfw1-outbound**.

Step 5: In the **Resource Group** list, select **AzureRefArch-CommonFW**, and then click **Create**.

Step 6: After the address has been successfully created, in **Home > Public IP address > ARA-CommonFW-vmfw1-outbound** , click **Associate**.

Step 7: In the Associate Public IP address pane, in the **Resource type** list, select **Network interface**.

Step 8: In the Choose Network Interface pane, select the public interface of **ARACF-VMFW1** (example: **ARACF-VM-FW1-eth1**), and then click **OK**.

Step 9: Repeat this procedure for any additional firewalls used for outbound access.

8.11 Outbound Access—Create Address Objects

Network objects are created to simplify the creation of NAT and security policy rules.

Table 28 Outbound traffic address objects

Object name	Description	Type	Type value
Net-10.5.1.0_24	Web subnet	IP Netmask	10.5.1.0/24
Net-10.5.2.0_24	Business subnet	IP Netmask	10.5.2.0/24
Net-10.5.3.0_24	DB subnet	IP Netmask	10.5.3.0/24

Step 1: Log in to Panorama (example: https://ara-panorama-1.westus.cloudapp.azure.com).

Step 2: Navigate to **Device Groups > Objects**.

Step 3: In the **Device Group** list, select **Azure-CommonFW**.

Step 4: In **Device Groups > Objects > Addresses**, click **Add**.

Step 5: In the **Name** box, enter **Net-10.5.1.0_24**.

Step 6: In the **Type** list, select **IP Netmask**.

Step 7: In the **Type value** box, enter **10.5.1.0/24**, and then click **OK**.

Step 8: Repeat Step 4 through Step 7 for all rows in Table 28.

8.12 Outbound Access—Configure NAT Policy

This procedure uses NAT Pre Rules. These rules are logically evaluated prior to local rules and cannot be locally overridden on the local device.

Step 1: Log in to Panorama (example: https://ara-panorama-1.westus.cloudapp.azure.com).

Step 2: Navigate to **Device Groups > Policies**.

Step 3: In the **Device Group** list, select **Azure-CommonFW**.

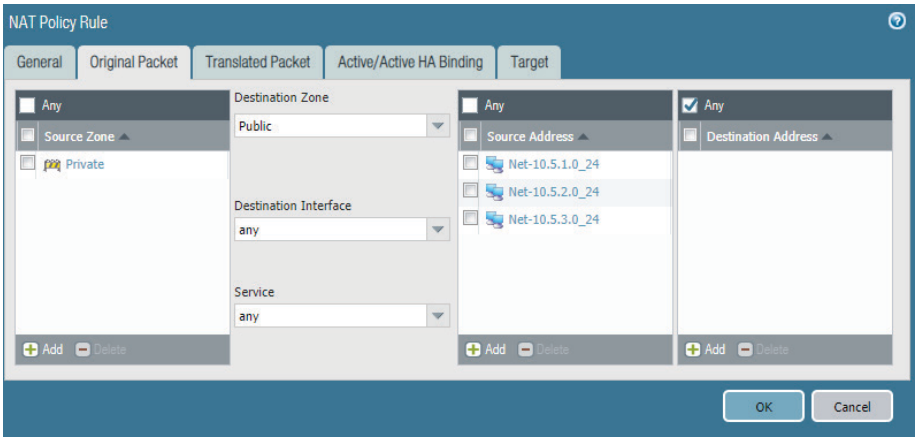
Step 4: In **Device Groups > Policies > NAT > Pre Rules**, click **Add**.

Step 5: In the **Name** box, enter **Outbound-Internet**.

Step 6: On the Original Packet tab, in the Source Zone pane, click **Add** and select **Private**.

Step 7: In the **Destination Zone** list, select **Public**.

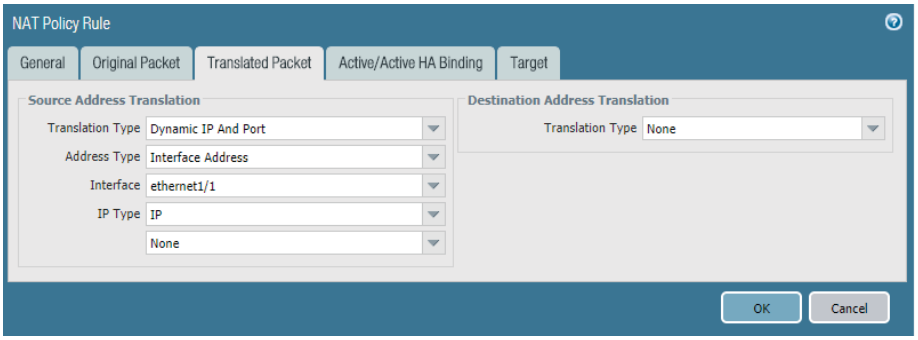
Step 8: In the Source Address pane, click **Add** and select **Net-10.5.1.0_24**. Repeat this step for all objects in Table 28.



Step 9: On the Translated Packet tab, in the Source Address Translation section, in the **Translation Type** list, select **Dynamic IP And Port**.

Step 10: In the Source Address Translation section, in the **Address Type** list, select **Interface Address**.

Step 11: In the Source Address Translation section, in the **Interface box**, select **ethernet1/1**.



Step 12: On the Target tab, verify that **Any (target to all devices)** is selected.

Caution

Make sure to target all devices in the device group. Otherwise, the policy rule will not be automatically applied to new group members.

8.13 Outbound Access—Configure Security Policy

This procedure uses security Pre Rules. These rules are logically evaluated prior to local rules and cannot be locally overridden on the local device. This example uses a common outbound policy for all private subnets. If you wish to use a differentiated policy, create separate rules for each subnet.

The security policy example for the Outbound Access Profile permits these applications:

- Web browsing (web-browsing)
- SSL (ssl)
- Google base (google-base)

Add additional applications to your policy as required.

Step 1: Log in to Panorama (example: https://ara-panorama-1.westus.cloudapp.azure.com).

Step 2: Navigate to **Device Groups > Policies**.

Step 3: In the **Device Group** list, select **Azure-CommonFW**.

Step 4: In **Device Groups > Policies > Security > Pre Rules**, click **Add**.

Step 5: In the **Name** box, enter **Outbound-Internet**.

Step 6: On the Source tab, in the Source Zone pane, click **Add** and select **Private**.

Step 7: In the Source Address pane, click **Add** and select **Net-10.5.1.0_24**. Repeat this step for all objects in Table 28

Step 8: On the Destination tab, in the Destination Zone pane, click **Add** and select **Public**.

Step 9: On the Application tab, in the Applications pane, click **Add** and enter/search/select **web-browsing**.

Step 10: In the Applications pane, click **Add** and enter/search/select **ssl**.

Step 11: In the Applications pane, click **Add** and enter/search/select **google-base**.

Step 12: On the Service/URL Category tab, in the **Service** pane, select **application-default**.

Step 13: On the Actions tab, in the Action Setting section, in the **Action** list, select **Allow**.

Step 14: In the Log Setting section, in the **Log Forwarding** list, select **LoggingService-Profile**.

Step 15: On the Target tab, verify that **Any (target to all devices)** is selected, and then click **OK**.

	Name	Location	Type	Source Zone	Source Address	Destination Zone	Destination Address	Application	Service	Action	Target
5	Outbound-Internet	Azure-CommonFW	universal	Private	Net-10.5.1.0_24 Net-10.5.2.0_24 Net-10.5.3.0_24	Public	any	google-base ssl web-browsing	application-default	Allow	any

Caution

Make sure to target all devices (any) in the device group; otherwise, the policy rule will not be automatically applied to new group members.

Step 16: On the **Commit** menu, click **Commit and Push**.

8.14 East/West Traffic

Traffic that originates from a virtual machine within a private subnet—and is destined to a virtual machine in different private subnet—routes to the firewall through a user-defined route table applied to the virtual machine's subnet. Virtual machines that can communicate to each other without the need for a firewall to protect the traffic can be on the same subnet, and virtual machines that do need traffic protection should be on different subnets.

Because the traffic flow for the East/West Traffic Profile always stays within the Private zone, the firewall security policy uses a Rule Type of **intrazone**.

Because both ends of the communication are within the VNet, the firewall should not apply a NAT policy to traffic between private subnets.

Note

Azure networking does not require the use of source NAT on the firewall to enforce symmetry if both directions of the flow pass through the same Azure internal load-balancer. The private subnets have UDRs directing East/West traffic to the firewall layer, so NAT is not required.

This procedure reuses objects already created in Procedure 8.11. If necessary, create additional objects using the same procedure.

This procedure uses security Pre Rules. These rules are logically evaluated prior to local rules and cannot be locally overridden on the local device. The example policy assumes three subnets with a granular policy with each as a source to the other two destinations.

Table 29 East/West security policy rules (example)

Rule	Source	Destination
Web-to-Business	Net-10.5.1.0_24 (web)	Net-10.5.2.0_24 (business)
Web-to-DB	Net-10.5.1.0_24 (web)	Net-10.5.3.0_24 (DB)
Business-to-Web	Net-10.5.2.0_24 (business)	Net-10.5.1.0_24 (web)
Business-to-DB	Net-10.5.2.0_24 (business)	Net-10.5.3.0_24 (DB)
DB-to-Web	Net-10.5.3.0_24 (DB)	Net-10.5.1.0_24 (web)
DB-Business	Net-10.5.3.0_24 (DB)	Net-10.5.2.0_24 (business)

The example security policy for the East/West Access Profile permits these applications:

- SSH (ssh)
- RDP (ms-rdp)
- Web browsing (web-browsing)
- SSL (SSL)

Add additional required applications to your policy as needed.

Step 1: Log in to Panorama (example: https://ara-panorama-1.westus.cloudapp.azure.com).

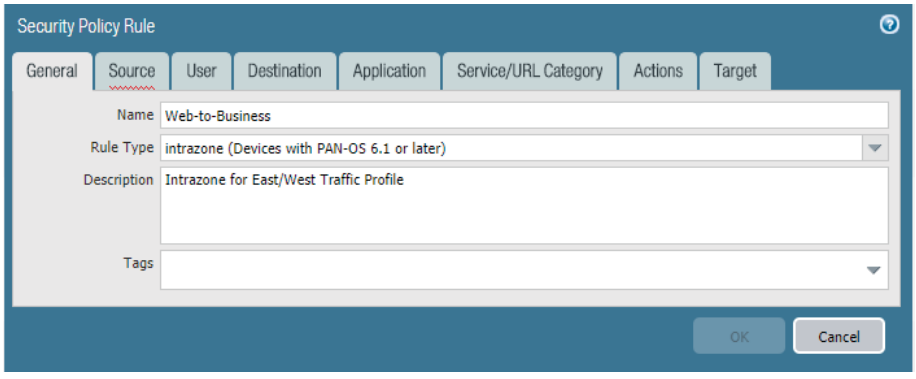
Step 2: Navigate to **Device Groups > Policies**.

Step 3: In the **Device Group** list, select **Azure-CommonFW**.

Step 4: In **Device Groups > Policies > Security > Pre Rules**, click **Add**.

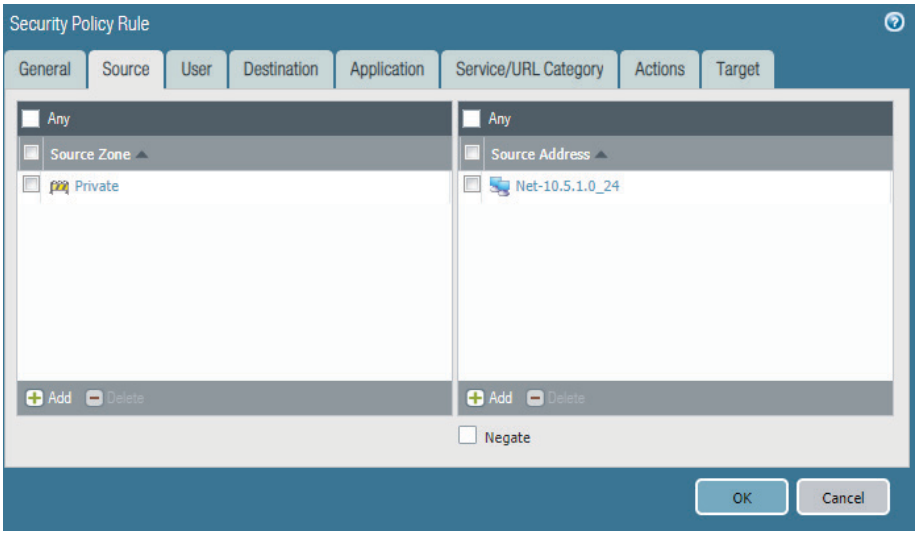
Step 5: In the **Name** box, enter **Web-to-Business**.

Step 6: In the **Rule Type** list, select **intrazone**.

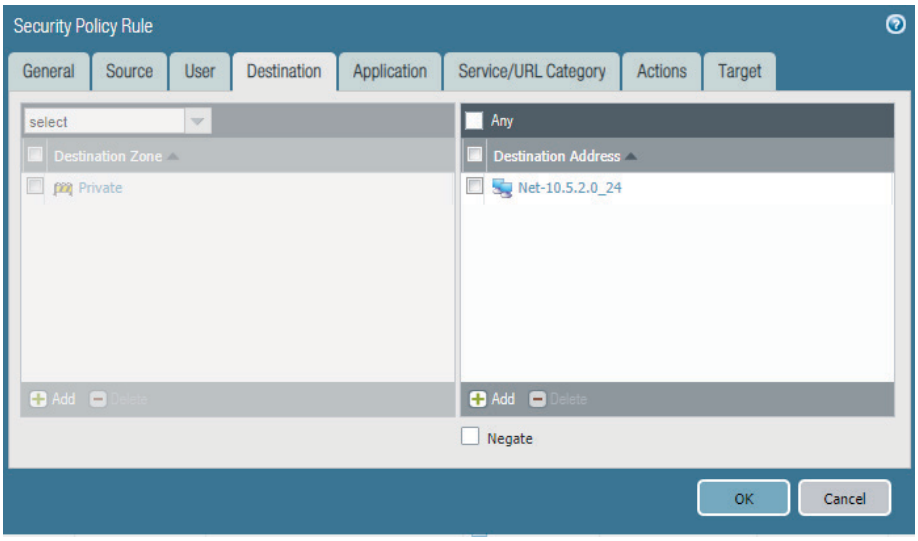


Step 7: On the Source tab, in the Source Zone pane, click **Add** and select **Private**.

Step 8: In the Source Address pane, click **Add** and select **Net-10.5.1.0_24**.



Step 9: On the Destination tab, in the Destination Address pane, click **Add** and select **Net-10.5.2.0_24**.



Step 10: On the Application tab, in the Applications pane, click **Add** and enter/search/select **ssh**.

Step 11: In the Applications pane, click **Add** and enter/search/select **ms-rdp**.

Step 12: In the Applications pane, click **Add** and enter/search/select **web-browsing**.

Step 13: In the Applications pane, click **Add** and enter/search/select **ssl**.

Step 14: On the Service/URL Category tab, in the Service pane, select **application-default**.

Step 15: On the Actions tab, in the Action Setting section, in the **Action** list, select **Allow**.

Step 16: In the Log Setting section, in the **Log Forwarding** list, select **LoggingService-Profile**.

Step 17: On the Target tab, verify that **Any (target to all devices)** is selected, and then click **OK**.

> **Caution**
>
> Make sure to target all devices (any) in the device group; otherwise, the policy rule will not be automatically applied to new group members.

Step 18: Repeat Step 4 through Step 17 for all rows in Table 29.

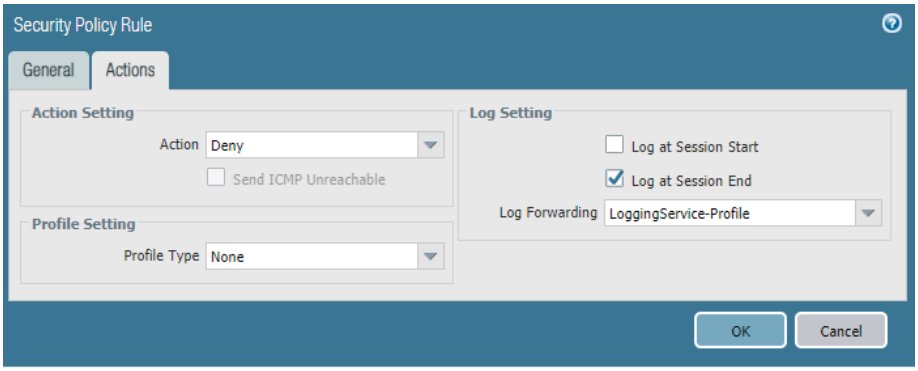
				Source		Destination					
	Name	Location	Type	Zone	Address	Zone	Address	Application	Service	Action	Target
6	Web-to-Business	Azure-CommonFW	intrazone	Private	Net-10.5.1.0_24	(intrazone)	Net-10.5.2.0_24	ms-rdp ssh ssl web-browsing	application-default	Allow	any
7	Web-to-DB	Azure-CommonFW	intrazone	Private	Net-10.5.1.0_24	(intrazone)	Net-10.5.3.0_24	ms-rdp ssh ssl web-browsing	application-default	Allow	any
8	Business-to-Web	Azure-CommonFW	intrazone	Private	Net-10.5.2.0_24	(intrazone)	Net-10.5.1.0_24	ms-rdp ssh ssl web-browsing	application-default	Allow	any
9	Business-to-DB	Azure-CommonFW	intrazone	Private	Net-10.5.2.0_24	(intrazone)	Net-10.5.3.0_24	ms-rdp ssh ssl web-browsing	application-default	Allow	any
10	DB-to-Web	Azure-CommonFW	intrazone	Private	Net-10.5.3.0_24	(intrazone)	Net-10.5.1.0_24	ms-rdp ssh ssl web-browsing	application-default	Allow	any
11	DB-to-Business	Azure-CommonFW	intrazone	Private	Net-10.5.3.0_24	(intrazone)	Net-10.5.2.0_24	ms-rdp ssh ssl web-browsing	application-default	Allow	any

Step 19: In **Device Groups > Policies > Security > Default Rules**, select the row **intrazone-default**, and click **Override**.

Step 20: On the Actions tab, in the Action Setting section, in the **Action** list, select **Deny**.

Step 21: In the Log Setting section, check **Log at Session End**.

Step 22: In the Log Setting section, in the **Log Forwarding** list, select **LoggingService-Profile**, and then click **OK**.

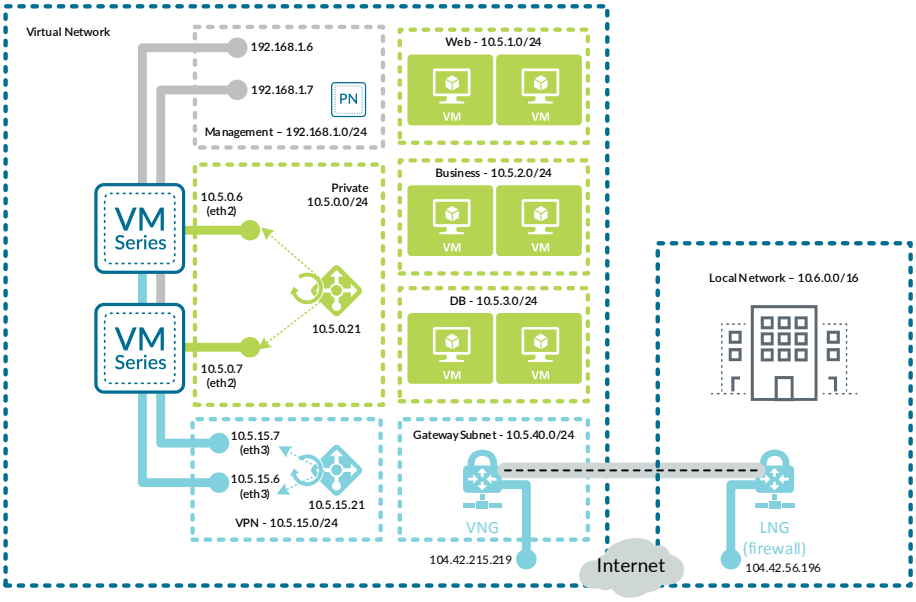


Step 23: On the **Commit** menu, click **Commit and Push**.

Deployment Details for Backhaul Connection

Use the following procedure groups to build an IPSec VPN connection for backhaul between Azure and your on-site network over the internet. The VPN endpoints used are the Azure Virtual Network Gateway (VNG) and an on-site Local Network Gateway (LNG). The LNG used in this guide is a Palo Alto Networks next-generation firewall.

Figure 18 Backhaul connection to on-site network



Note

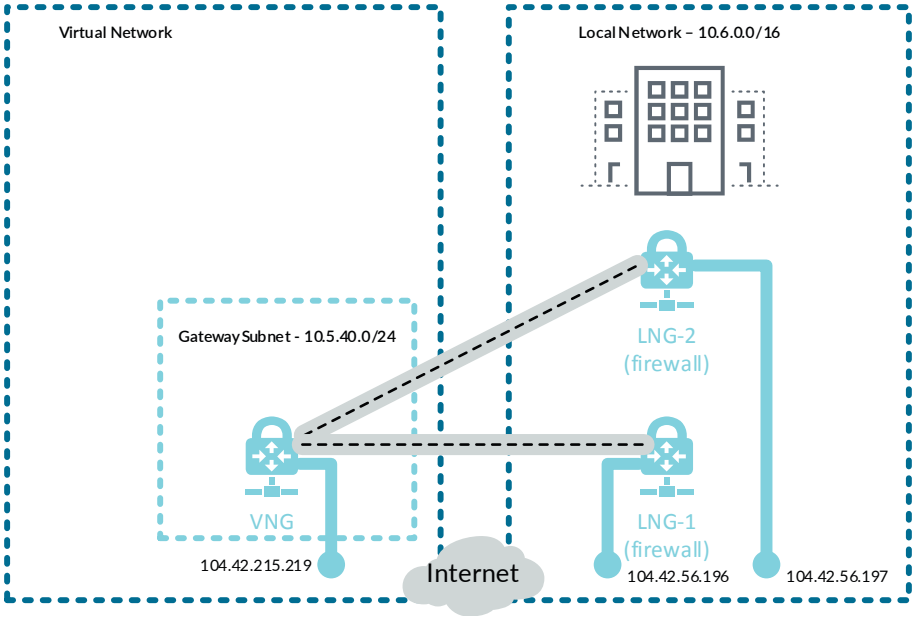
The connection from Azure to the on-site network was tested and validated only with a specific design and includes two options: static routing and BGP routing. Other variants to the backhaul design may work with similar configurations but have not been explicitly tested.

A resilient design for the backhaul uses a pair of connections from Azure to the on-site network and must use BGP routing. An additional LNG is deployed on-site to terminate the second connection from the Azure VNG. Routing will be configured to prefer the first connection as active and the second connection as standby to ensure that traffic is routed symmetrically between the on-site network and Azure.

Note

Every Azure VPN gateway consists of two instances in an active-standby configuration. For any planned maintenance or unplanned disruption that happens to the active instance, the standby instance would take over automatically and resume the VPN connections.

Figure 19 Resilient backhaul connection



Procedures

Configuring Azure Networking for Backhaul Connection

9.1 Configure the Azure Internal Load-Balancer for Backhaul

9.2 Configure Azure User Defined Routes

9.3 Apply Route Tables to Subnets

9.4 Modify Existing Route Tables

9.5 Create the VPN Gateway Subnet.

9.6 Create Public IP for VPN Gateway

9.7 Deploy Virtual Network Gateway on Azure

9.8 Create Local Network Gateway

9.9 Create VPN Connection from VNG to LNG

This procedure group relies on the following assumptions:

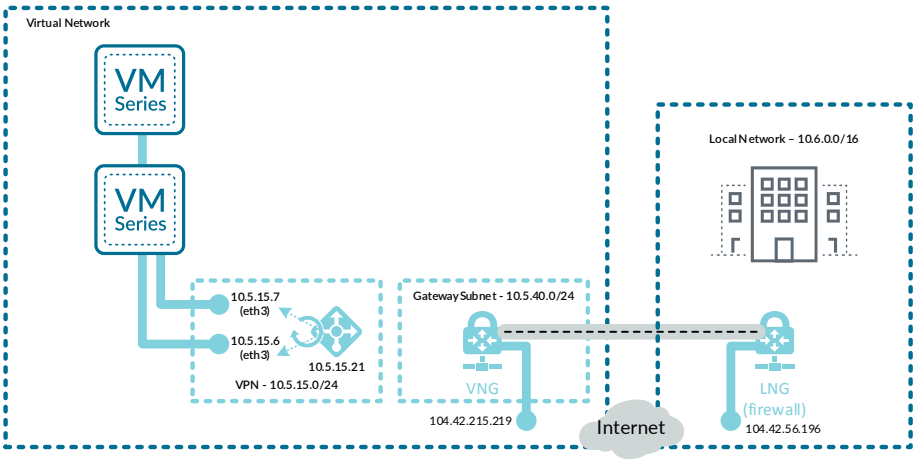
- The on-site local network IP address block is **10.6.0.0/16**.
- The existing on-site firewall must have a statically assigned public IP address.
- The Azure subnet reachable for Panorama and VM-Series management is **192.168.1.0/24**.
- The Azure subnets reachable for in-band access (Web, DB, Business) included within the IP address range are **10.5.0.0/20**.

Use the Azure Resource Manager to complete the following procedures. Sign in to Azure at https://portal.azure.com.

9.1 Configure the Azure Internal Load-Balancer for Backhaul

Because the VPN gateway subnet uses Azure internal addressing, you use an additional frontend IP address and back-end pool on the internal load-balancer.

Figure 20 Azure internal load-balancer for backhaul



The frontend IP address is used as the routing next-hop for destination addresses on the private networks.

Step 1: In **Home > Load Balancers > ARA-CommonFW-Internal**, click **Frontend IP configuration**, and then click **Add**.

Step 2: In the **Name** box, enter **Internal-Frontend-VPN**.

Step 3: In the **Subnet** list, select **CommonFW-VPN**.

Step 4: In the Assignment section, select **Static**.

Step 5: In the **IP address** box, enter **10.5.15.21**, and then click **OK**.

Step 6: In **Home > Load Balancers > ARA-CommonFW-Internal**, click **Backend pools**, and then click **Add**.

Step 7: In the **Name** box, enter **Firewall-Layer-VPN**.

Step 8: In the **Virtual network** list, select **azurerefarch-vnet (X VM)**, where X is the total number of virtual machines already deployed in your VNet.

Step 9: In the **VIRTUAL MACHINE** column, select a VM-Series to be added to this backend pool (example: **aracf-vmfw1**).

Step 10: In the **IP ADDRESS** column, select the **IP configuration** that is associated to the **CommonFW-VPN** subnet. (example: **ipconfig-dmz**).

Step 11: Repeat Step 9 and Step 10 for all VM-Series firewalls that are to be assigned to this backend pool.

Step 12: Click **Add**.

Step 13: In **Home > Load Balancers > ARA-CommonFW-Internal**, click **Load balancing rules**, and then click **Add**.

Step 14: In the **Name** box, enter **VPN-All-Ports**.

Step 15: In the **Frontend IP address** list, select **Internal-Frontend-VPN**.

Step 16: Select **HA ports**.

Step 17: In the **Backend pool** list, select **Firewall-Layer-VPN**.

Step 18: In the **Health probe** list, select **HTTPS-Probe**, and then click **OK**.

9.2 Configure Azure User Defined Routes

This procedure relies on the following assumptions:

- The on-site local network IP address block is **10.6.0.0/16**.
- The existing on-site firewall BGP peer address (assigned to tunnel interface) is **10.6.1.255**.
- The existing on-site firewall must have a statically assigned public IP address.
- The Azure subnet reachable for Panorama and VM-Series management is **192.168.1.0/24**.
- The Azure subnets reachable for in-band access (Web, DB, Business) included within the IP address range are **10.5.0.0/20**.

Table 30 Azure route tables

Subnet	Route table name	Resource group	Table of UDRs
CommonFW-VPN	ARACF-VPN	AzureRefArch-CommonFW	Table 31
GatewaySubnet	ARA-VPNGateway	AzureRefArch	Table 32

Table 31 VPN subnet UDRs (10.5.15.0/24)

Route name	Address prefix	Next-hop type	Next-hop address	Comments
Blackhole-Management	192.168.1.0/24	None	—	Block traffic to Management IP address space
Blackhole-Public	172.16.0.0/23	None	—	Block traffic to Public IP address space

Table 32 VPN gateway subnet UDRs (10.5.40.0/24)

Route name	Address prefix	Next-hop type	Next-hop address	Comments
Blackhole-Public	172.16.0.0/23	None	—	Block traffic to Public IP address space
Net-10.5.0.0_20	10.5.0.0/20	Virtual appliance	10.5.15.21	Frontend IP of load-balancer

Step 1: In **Home** > **Route** tables, click **Add**.

Step 2: In the **Name** box, enter **ARACF-VPN**.

Step 3: In the **Resource Group** list, select **AzureRefArch-CommonFW**, and then click **Create**.

Step 4: In **Home > Route tables > ARACF-VPN**, click **Routes**.

Step 5: Repeat these substeps for all entries in the table of UDRs:

- In **Home > Routes tables > AzureRefArch-VPN—Routes**, click **Add**.
- In the **Route name** box, enter **Blackhole-Management**.
- In the **Address prefix** box, enter **192.168.1.0/24**.
- In the **Next hop type** list, select **None**.
- If the Next-hop type is Virtual appliance, then enter the Next-hop address value, and then click **OK**.

Step 6: Repeat this procedure for each entry in Table 30.

9.3 Apply Route Tables to Subnets

The UDRs take effect only after the route table is associated with the subnet.

Step 1: In **Home > Virtual networks > AzureRefArch-VNET**, click **Subnets**.

Step 2: Click **CommonFW-VPN**.

Step 3: Click the **Route table** section, and in the Resource pane, select **ARACF-VPN**.

Step 4: Click **Save**, and then click **X** to Close.

9.4 Modify Existing Route Tables

Azure networking routes traffic from all subnets to the on-site network range directly to the VNG by default. This design allows implicit access for the Management subnet to support in-band management of Panorama and the VM-Series.

To block the traffic or enforce a firewall policy requires that you create UDRs. Configure the UDRs to explicitly block traffic to the on-site network from the public subnet, unless you are running dynamic BGP routing, in which case you disable BGP route propagation for the public network, instead. Configure the UDRs to redirect traffic from all other subnets to the firewall layer for policy enforcement.

The route tables in Table 33 were originally created in Procedure 7.12. Modify the route tables listed in Table 33 by

adding the additional specified routes. If you have additional on-site prefixes, then each prefix requires a UDR in each routing table.

Caution

When adding additional on-site networks, you must manually update the route tables to block and redirect to the new prefixes as they are added. This procedure is required even when you are running dynamic BGP routing, except where noted. Prefixes must match exactly for the UDR overrides to replace the active routes.

The blackhole UDR is only required with the static routing option.

We suggest that you disable route propagation for all subnets, except for the Management and VPN subnets, as a best practice. This ensures that system routes cannot be used to access the on-site networks. UDR redirection to the load-balancer frontend IPs is still required.

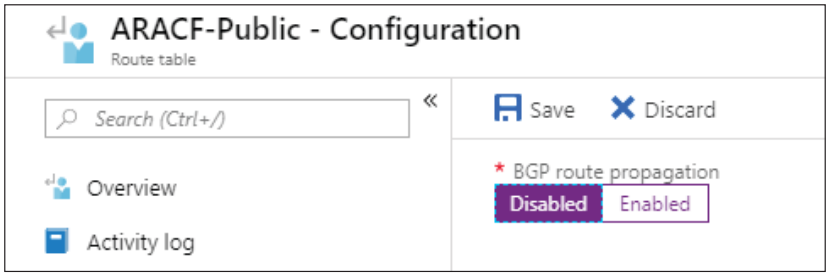
Table 33 Route table modifications for backhaul

Route table name	Route name	Address prefix	Next-hop type	Next-hop address	Comments
ARACF-Public	Blackhole-OnSite	10.6.0.0/16	None	—	Block traffic to On-site IP address space. This is only required if you are using static routing.
ARACF-Private	Net-10.6.0.0_16	10.6.0.0/16	Virtual appliance	10.5.0.21	Frontend IP of load-balancer Access to on-site network through the firewall layer
ARACF-Web	Net-10.6.0.0_16	10.6.0.0/16	Virtual appliance	10.5.0.21	Frontend IP of load-balancer Access to on-site network through the firewall layer
ARACF-Business	Net-10.6.0.0_16	10.6.0.0/16	Virtual appliance	10.5.0.21	Frontend IP of load-balancer Access to on-site network through the firewall layer
ARACF-DB	Net-10.6.0.0_16	10.6.0.0/16	Virtual appliance	10.5.0.21	Frontend IP of load-balancer Access to on-site network through the firewall layer

If you are running BGP, disable BGP route propagation for the public subnet and all other subnets listed in Table 33. This configuration prevents any BGP learned routes from being installed in the active route table for these subnets.

Step 1: For all entries in Table 33, perform these substeps:

- In **Home > Route tables > ARACF-Public**, click **Configuration**.
- In the BGP route propagation section, click **Disabled**, then click **Save**.



9.5 Create the VPN Gateway Subnet.

This procedure adds a new subnet for the VPN Gateway to the existing VNet.

Step 1: In **Home > Virtual networks > AzureRefArch-VNET**, click **Subnets.**

Step 2: Click **Gateway subnet** to add a new gateway subnet.

Step 3: In the **Address Range (CIDR block)** box, enter **10.5.40.0/24**.

Step 4: Click the **Route table** section, select **ARA-VPNGateway**, and then click **OK**.

9.6 Create Public IP for VPN Gateway

Step 1: In **Home > Public IP addresses**, click **Add.**

Step 2: In the **Name** box, enter **ARA-VNG-Public**.

Step 3: Select **Basic** SKU.

> **Note**
>
> Do not choose a Standard IP SKU for the public IP address of your Virtual Network Gateway. The Standard IP SKU uses only static IP address assignment. Azure Resource Manager does not permit this selection and presents the following error: “Static public IP address can only be assigned to load-balancers.”

Step 4: In the IP address assignment section, select **Dynamic**.

> **Note**
>
> In the **DNS name label** box, do not enter a value. Azure does not support dynamic resolution of the FQDN for a VPN gateway.

Step 5: In the **Resource Group** list, select **AzureRefArch**, and then click **Create**.

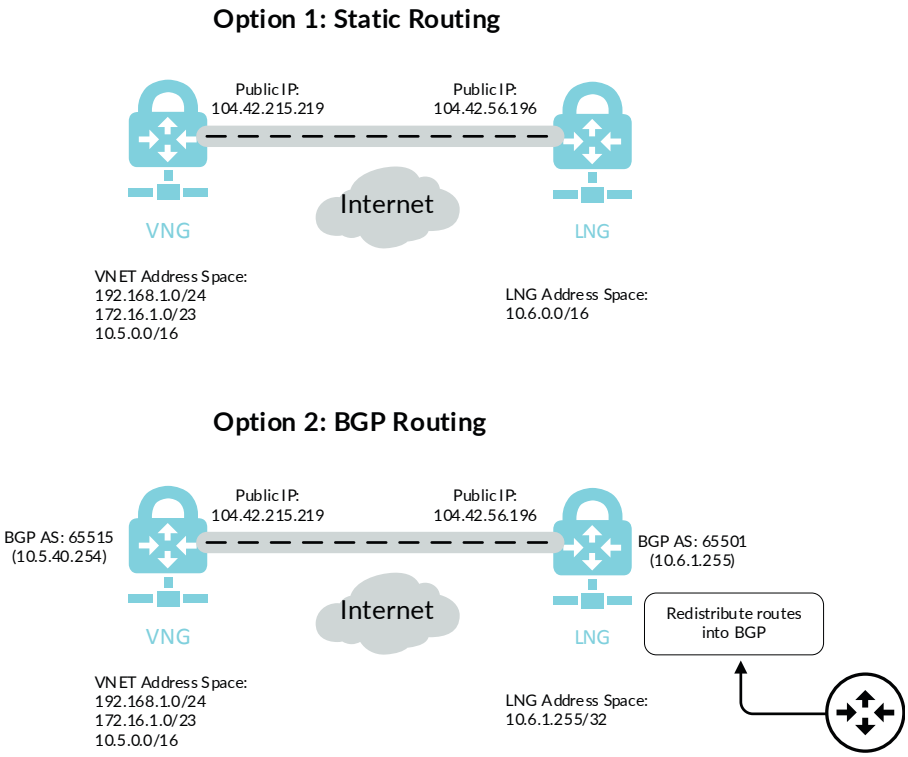
The on-premise firewall requires a peer IP address for the Azure VNG. The actual IP address is not assigned by Azure until the VNG is created and the public IP address is associated.

9.7 Deploy Virtual Network Gateway on Azure

This procedure includes two routing options, static routing and dynamic routing with BGP. The static routing option is simpler to configure but requires manual modification for any routing changes. The BGP option is more complex to initially configure but is easier to operate and maintain in a rapidly changing environment.

Refer to Figure 21 for this and the following procedures.

Figure 21 Backhaul routing options—static and BGP



Step 1: In **Home > Virtual networks gateways**, click **Add.**

Step 2: In the **Name** box, enter **ARA-VNG.**

Step 3: In the Gateway type section, select **VPN**.

Step 4: In the VPN type section, select **Route-based**.

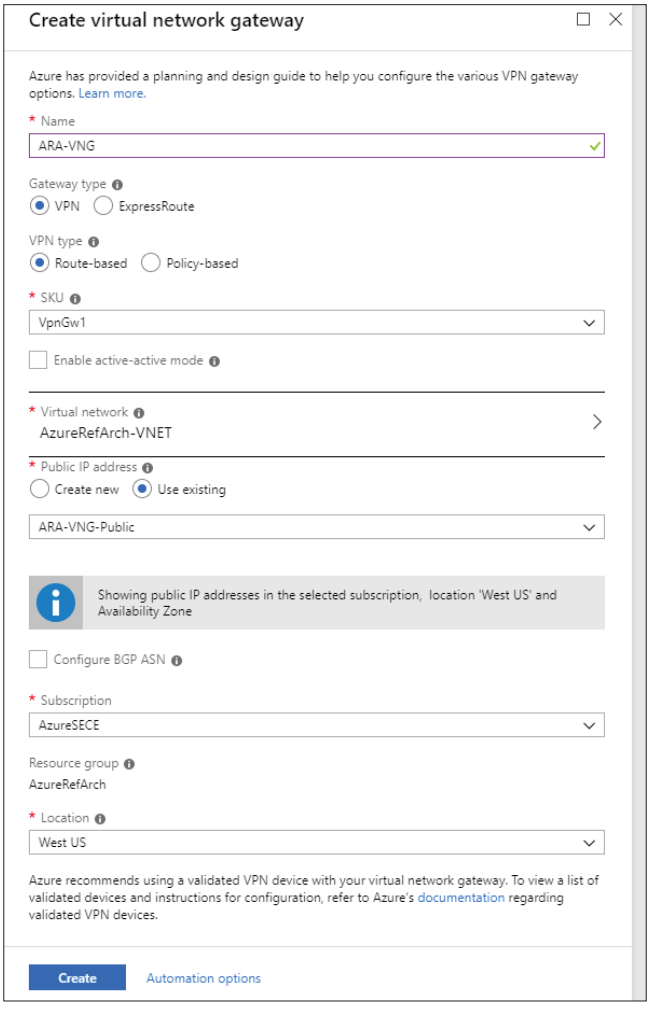
Step 5: In the **SKU** list, select **VpnGw1**. The basic SKU does not support BGP or IKEv2.

Step 6: Click the **Virtual Network** section, and then select **AzureRefArch-VNET**.

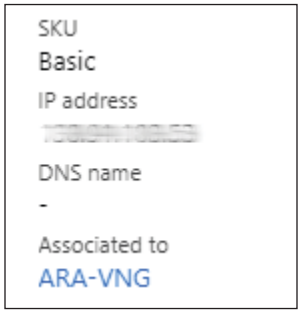
Step 7: Click the **Public IP address** section, select **Use existing**, and then select **ARA-VNG-Public**.

Step 8: If you're configuring dynamic routing with BGP, select **Configure BGP ASN**, and then in the **Autonomous system number (ASN)** box, accept the proposed default value of **65515**.

Step 9: Click **Create**.

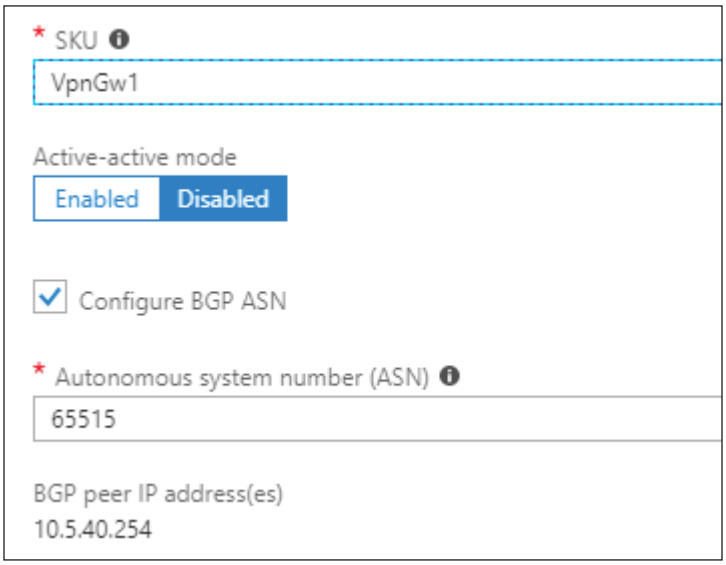


Step 10: In **Home > Public IP addresses > ARA-VNG-Public**, record the IP address (Example: **104.42.215.219**).



Step 11: If you configured BGP, then in **Home > Virtual network gateways > ARA-VNG**, click **Configuration**.

Step 12: Record the **BGP peer IP address** assigned to the virtual network gateway (Example: **10.5.40.254**).



9.8 Create Local Network Gateway

The local network gateway corresponds to the on-premise firewall that terminates the IPSec VPN tunnel from Azure.

Step 1: In **Home > Local network gateways**, click **Add**.

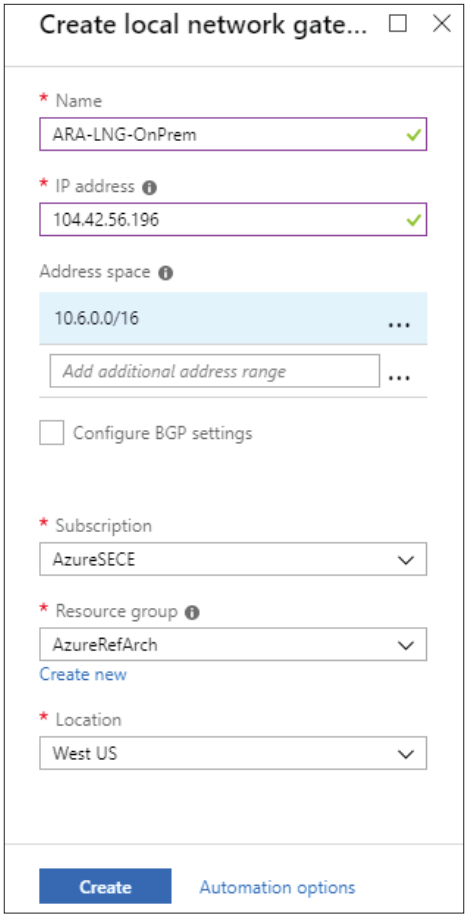
Step 2: In the **Name** box, enter **ARA-LNG-OnPrem**.

Step 3: In the **IP address** box, enter the public IP address of the on-premise IPSec VPN peer (Example: **104.42.56.196**).

Option 1: Static Routing

Step 1: In the **Address space** box, enter the IP prefix that is reachable through the VPN tunnel. (Example: **10.6.0.0/16**). If multiple IP prefixes are reachable, you must add the additional prefixes by repeating this step multiple times.

Step 2: In the **Resource Group** list, select **AzureRefArch**, and then click **Create**.



Option 2: Dynamic Routing with BGP

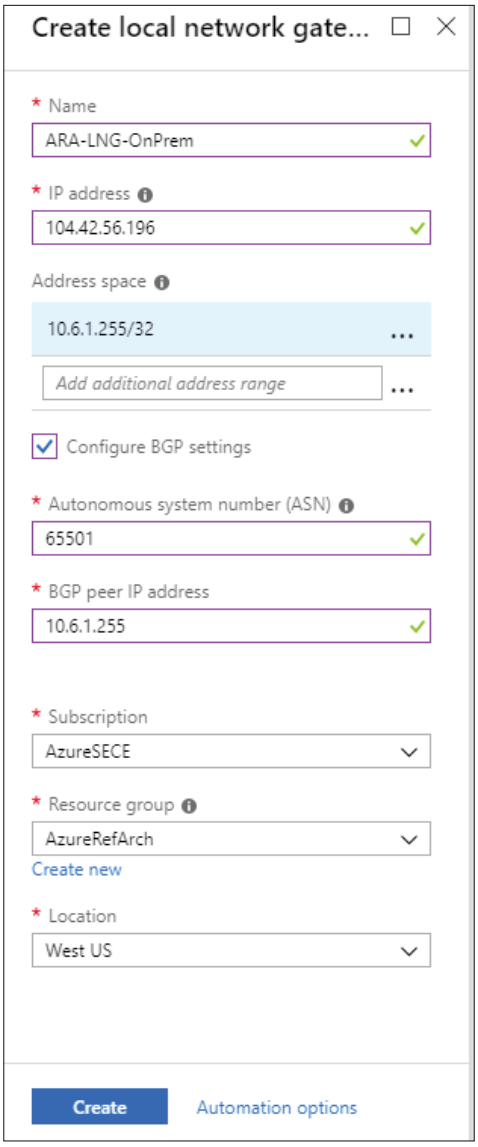
Step 1: In the **Address space** box, enter only the IP prefix for the BGP peer address from the on-premise firewall this LNG corresponds to. (Example: **10.6.1.255/32**)

Step 2: Select **Configure BGP settings**.

Step 3: In the **Autonomous system number (ASN)** box, enter **65501**.

Step 4: In the **BGP peer IP address** box, enter **10.6.1.255**.

Step 5: In the **Resource Group** list, select **AzureRefArch**, and then click **Create**.



9.9 Create VPN Connection from VNG to LNG

Step 1: In **Home > Connections**, click **Add**.

Step 2: In **Home > Connections > Create connection > Basics**, in the **Connection type** list, select **Site-to-site (IPsec)**.

Step 3: In the **Resource Group** list, select **AzureRefArch**, and then click **OK**.

Step 4: In **Home > Connections > Create connection > Settings,** click the **Virtual network gateway** section, and then select **ARA-VNG**.

Step 5: Click the **Local network gateway** section, and then select **ARA-LNG-OnPrem**.

Step 6: In the **Connection name** box, enter **AzureRefArch-to-OnPrem**.

Step 7: In the **Shared key (PSK)** box, enter the value for the pre-shared key (complex password).

Step 8: If you configured BGP, select **Enable BGP**, and then click **OK**.

Step 9: Review the Summary and if it's acceptable, click **OK**.

Procedures

Configuring On-site Firewall for VPN Access to Azure

10.1 Configure Objects and Interfaces

10.2 Configure IKEv2 and IPSec

10.3 Configure Routing

10.4 Configure BGP

These procedures assume the on-site firewall is configured and running with a public interface reachable from the internet and a private interface with access to internal subnets. The firewall is already configured with a default virtual router. DNS and NTP are configured.

The following procedures are completed on the on-site next-generation firewall or VM-Series device. If you are using a second resilient on-site firewall, this procedure group is repeated.

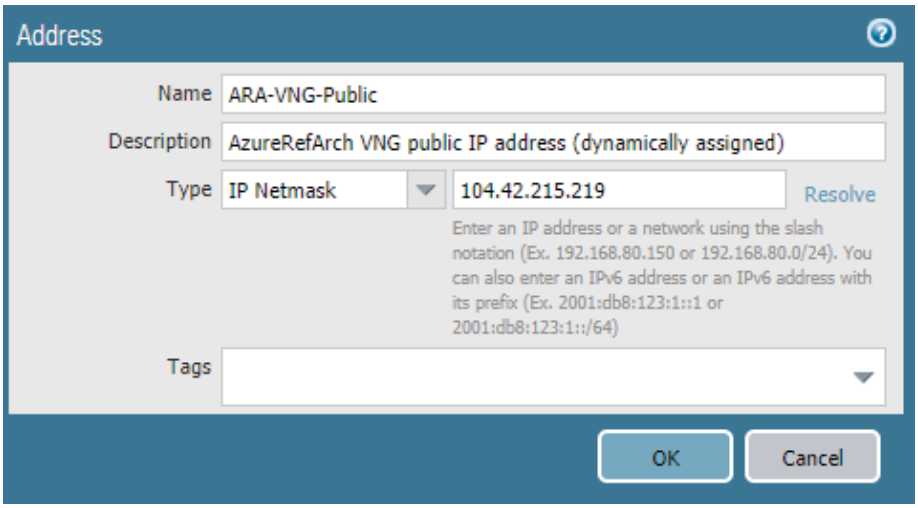
10.1 Configure Objects and Interfaces

Step 1: In **Objects > Addresses**, click **Add**.

Step 2: In the **Name** box, enter **ARA-VNG-Public**.

Step 3: In the **Type** list, select **IP Netmask**.

Step 4: In the **Type value** box, enter the public IP address that was assigned by Azure (Example: 104.42.215.219), and then click **OK**.



Step 5: In **Network > Zones**, click **Add**. The Zone configuration window appears.

Step 6: In the **Name** box, enter **VPN**.

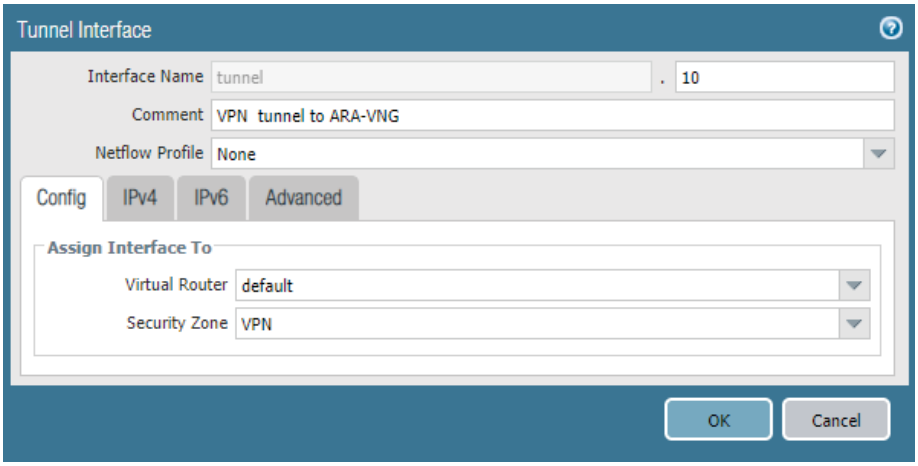
Step 7: In the **Type** list, select **Layer3**, and then click **OK**.

Step 8: In **Network > Interfaces**, change to the Tunnel tab, and then click **Add**. The Tunnel Interface configuration window appears.

Step 9: In the **Interface Name.subinterface** box, enter **10**.

Step 10: In the **Virtual Router** list, select **default**.

Step 11: In the **Security Zone** list, select **VPN**.



Note

If you are configuring the second device for resilient backhaul, use the value of **10.6.1.254/32** in Step 12.

Step 12: If you configured BGP, change to the **IPv4** tab. In the IP pane, click **Add**, enter **10.6.1.255/32**, and then click **OK**.

Step 13: On the Advanced tab, in the **MTU** box, enter **1424**, and then click **OK**.

This value is used to minimize IP packet fragmentation due to the tunnel and IPSec encapsulation overhead.

Step 14: In **Network Interfaces**, click the public-facing Ethernet interface (example: **ethernet1/1**).

Step 15: On the Advanced tab, in the Other Info section, select **Adjust TCP MSS**, and then click **OK**.

This feature is enabled to minimize IP packet fragmentation due to the tunnel and IPSec encapsulation overhead.

10.2 Configure IKEv2 and IPSec

Use the values specified in Table 34 for the steps in this procedure. The firewall can successfully negotiate these values with the Azure VNG without requiring any modification of the Azure default settings. The strongest authentication and encryption values that are compatible with Azure are listed.

Table 34 IKEv2 and IPSec parameters

Parameter	Value	Description
IKEv2 DH group	group2	Diffie-Helman Group 2
IKEv2 authentication	sha256	Secure Hash Algorithm 2 (SHA-2) with 256-bit digest
IKEv2 encryption	aes-256-cbc	Advanced Encryption Standard (AES) Cipher Block Chaining (CBC) with 256-bit key
IKEv2 key lifetime timer	28800 Seconds	—
IKEv2 timer authentication multiple	3	—
IPSec encryption	aes-256-gcm	AES Galois Counter Mode (GCM) with 256-bit key
IPSec authentication	sha512	Secure Hash Algorithm 2 (SHA-2) with 512-bit digest
IPSec DH group	no-pfs	Perfect Forward Secrecy disabled
IPSec lifetime	3600 Seconds	—

Step 1: In **Network > Network Profiles > IKE Crypto**, click **Add**. The IKE Crypto Profile configuration window appears.

Step 2: In the **Name** box, enter **Azure-IKEv2**.

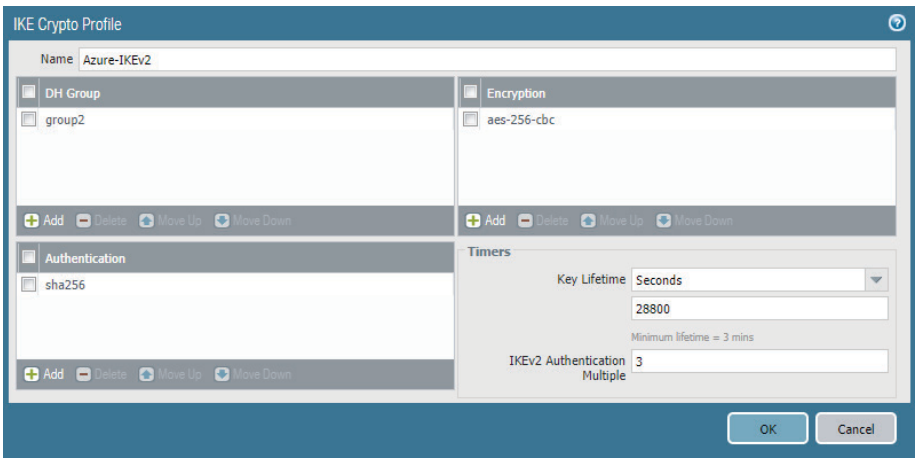
Step 3: In the DH Group pane, click **Add** and select **group2**.

Step 4: In the Authentication pane, click **Add** and select **sha256**.

Step 5: In the Encryption pane, click **Add** and select **aes-256-cbc**.

Step 6: In the Timers section, in the **Key Lifetime** list, select **Seconds** and enter **28800**.

Step 7: In the Timers section, in the **IKEv2 Authentication Multiple** box, enter **3**, and then click **OK**.



Step 8: In **Network > Network Profiles > IPSec Crypto**, click **Add**. The IPSec Crypto Profile configuration window appears.

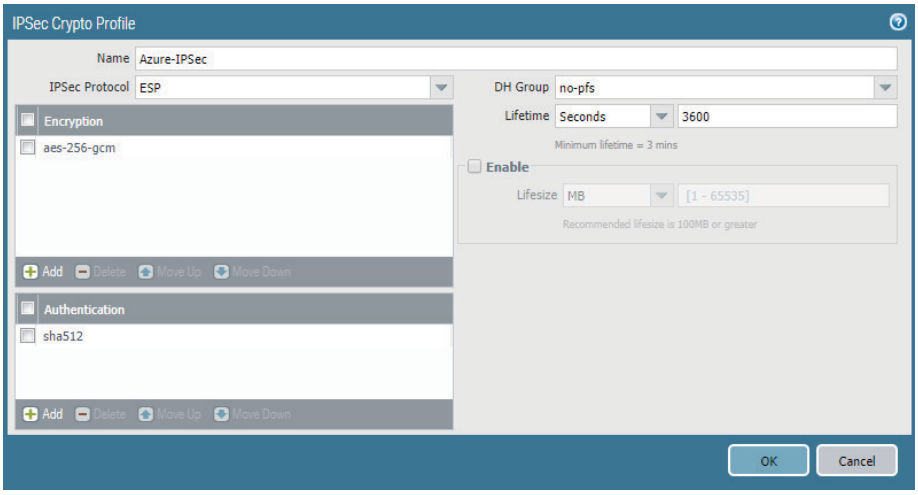
Step 9: In the **Name** box, enter **Azure-IPSec**.

Step 10: In the Encryption pane, click **Add** and select **aes-256-gcm**.

Step 11: In the Authentication pane, click **Add** and select **sha512**.

Step 12: In the **DH Group** list, select **no-pfs**.

Step 13: In the **Lifetime** list, select **Seconds** and enter **3600**, and then click **OK**.



Step 14: In **Network > Network Profiles > IKE Gateways**, click **Add**. The IKE Gateway configuration window appears.

Step 15: In the **Name** box, enter **OnPrem-to-AzureRefArch-IKEv2**.

Step 16: In the **Version** list, select **IKEv2 only mode**.

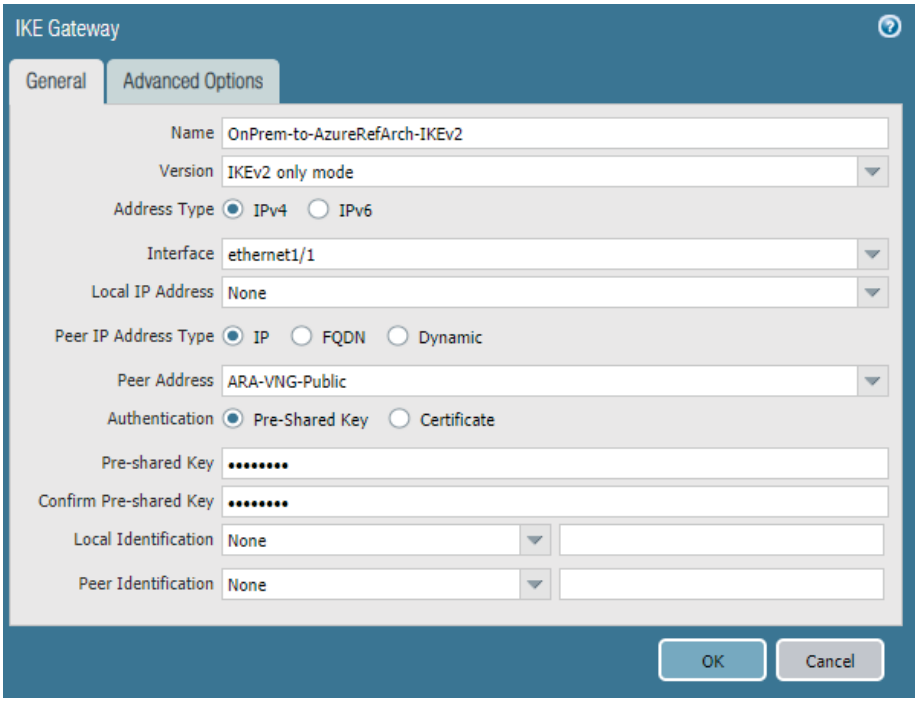
Step 17: In the **Interface** list, select the public interface of the firewall (example: **ethernet1/1**).

Step 18: In the Peer IP Address Type section, select **IP**.

Step 19: In the **Peer Address** list, select **ARA-VNG-Public**.

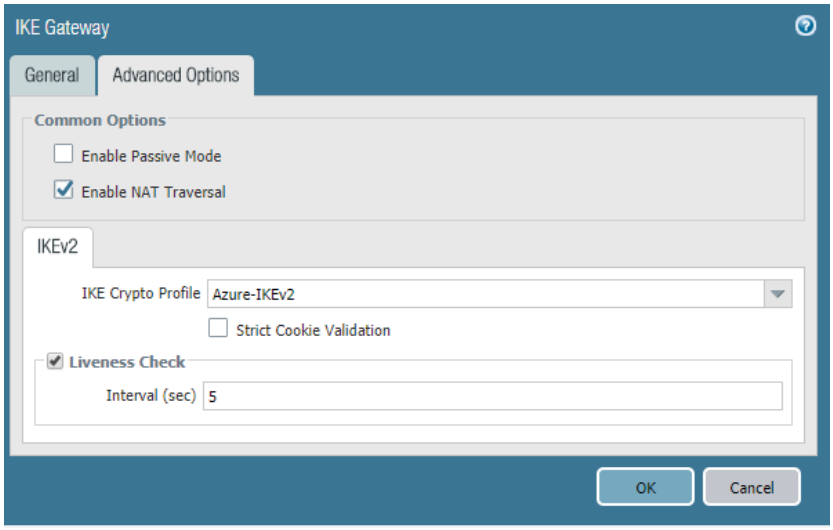
Step 20: In the **Pre-shared Key** box, enter the Shared key (PSK) that matches the VPN connection configured on Azure.

Step 21: In the **Confirm Pre-shared Key** box, re-enter the key.



Step 22: On the Advanced Options tab, select **Enable NAT Traversal**.

Step 23: In the **IKE Crypto Profile** list, select **Azure-IKEv2**, and then click **OK**.



Step 24: In **Network > IPSec Tunnels**, click **Add**.

Step 25: In the **Name** box, enter **OnPrem-to-AzureRefArch**.

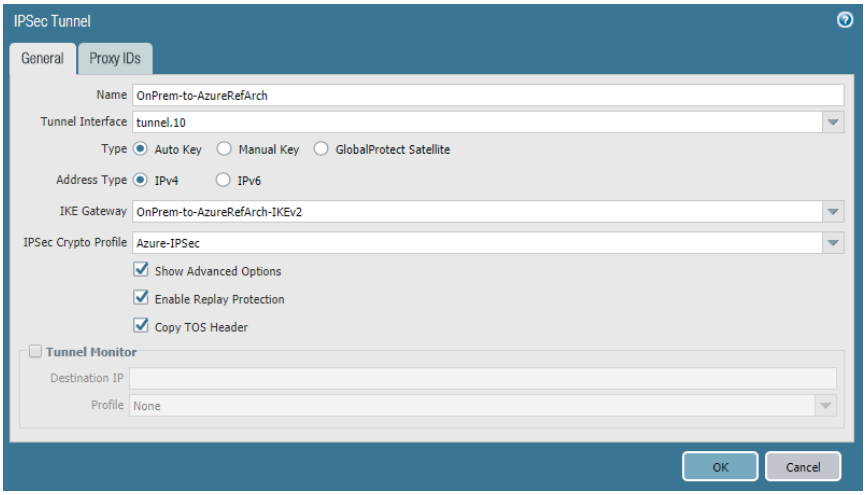
Step 26: In the **Tunnel Interface** list, select **tunnel.10**.

Step 27: In the **IKE Gateway** list, select **OnPrem-to-AzureRefArch-IKEv2**.

Step 28: In the **IPSec Crypto Profile** list, select **Azure-IPSec**.

Step 29: Select **Show Advanced Options**.

Step 30: Select **Copy TOS Header**, and then click **OK**.



10.3 Configure Routing

The static routing option requires the creation of explicit static routes for all Azure destination prefixes. The dynamic routing option requires the creation of a single static route that corresponds to the Azure routing peer prefix. All other destinations are dynamically learned using the routing protocol.

Table 35 Static routes for on premise firewall

Name	Destination prefix	Interface	Next-hop	Next-hop value
Azure-10.5.0.0_16	10.5.0.0/16	tunnel.10	None	—
Azure-192.168.1.0_24	192.168.1.0/24	tunnel.10	None	—

Step 1: In **Network > Virtual Routers**, click **default**. The Virtual Router—default window appears.

Step 2: Change to the **Static Routes** tab.

Option 1: Static Routing

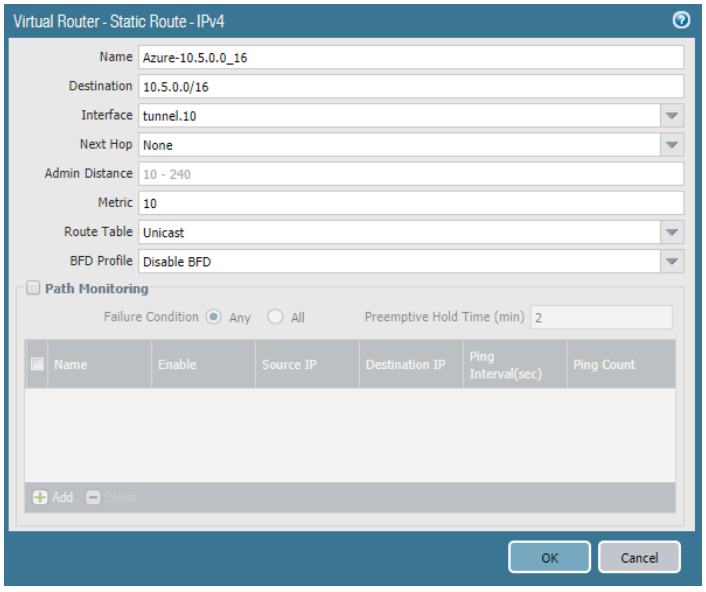
Step 1: Click **Add**. The Virtual Router—Static Route—IPv4 window appears.

Step 2: In the **Name** box, enter **Azure-10.5.0.0_16**.

Step 3: In the **Destination** box, enter **10.5.0.0/16**.

Step 4: In the **Interface** list, select **tunnel.10**.

Step 5: In the **Next Hop** list, select **None**, and then click **OK**.



Step 6: Repeat Step 1 through Step 5 for all static routes in Table 35.

Step 7: After adding all routes for this virtual router, click **OK** to close the Virtual Router window, and then click **Commit**.

Option 2: Dynamic Routing with BGP

The BGP option requires a static host route to reach the Azure BGP peer.

Step 1: Click **Add**. The Virtual Router—Static Route—IPv4 window appears.

Step 2: In the **Name** box, enter **Azure-BGP-Router-ID**.

Step 3: In the **Destination** box, enter **10.5.40.254/32**.

Step 4: In the **Interface** list, select **tunnel.10**.

Step 5: In the **Next Hop** list, select **None**, and then click **OK**.

Step 6: Click **OK** to close the Virtual Router window, and then click **Commit**.

10.4 Configure BGP

(Optional)

If you are using static routing, skip this procedure.

This procedure requires that you have a BGP autonomous system number; the example uses 65501 for the on-site firewall. The BGP peering configuration uses the tunnel interface IP address of the firewall as the BGP Router ID.

Step 1: In **Network > Virtual Routers**, click **default**. The Virtual Router—default window appears.

Step 2: On the Redistribution Profile tab, click **Add**. The Redistribution Profile IPv4 window appears.

Note

This example redistributes the directly connected route for the subnet assigned to the Private zone interface (ethernet1/2). If you are running a dynamic routing protocol in your on-site network and firewall, then redistribute the routes from the routing protocol instead of the connected route.

The use of a dynamic routing protocol is required to ensure symmetric routing when using a resilient backhaul connection.

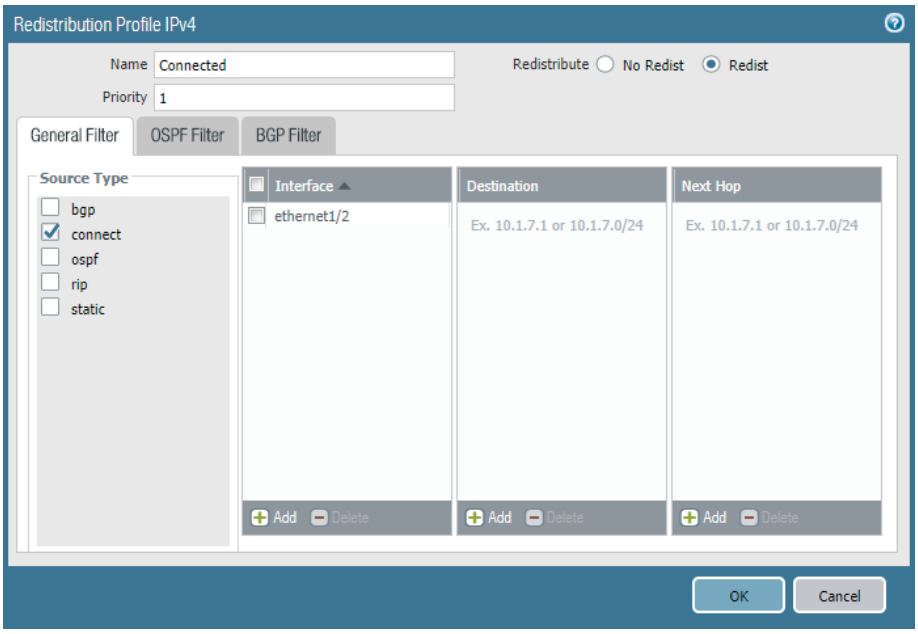
Step 3: In the **Name** box, enter **Connected**.

Step 4: In the Redistribute section, select **Redist**.

Step 5: In the **Priority** box, enter **1**.

Step 6: In the Source Type pane, select **connect**.

Step 7: In the Interface pane, click **Add**, select **ethernet1/2**, and click **OK**.



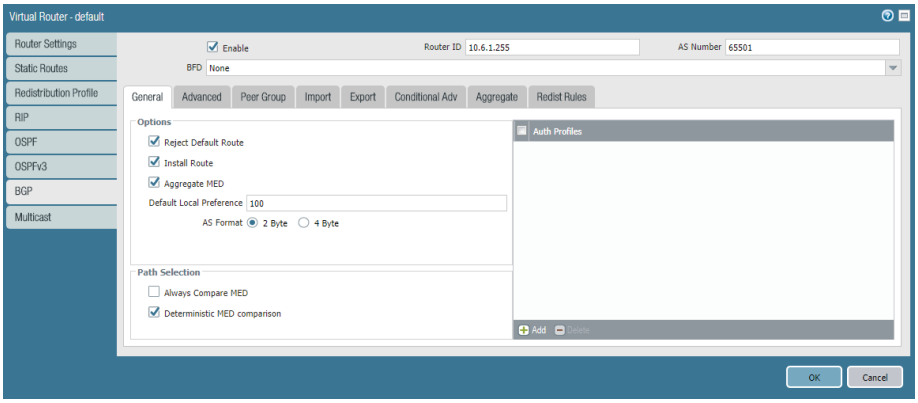
Step 8: On the BGP tab, select **Enable**.

> **Note**
>
> If you are configuring the second device for resilient backhaul, use the value of **10.6.1.254** in Step 9.

Step 9: In the **Router ID** box, enter **10.6.1.255**.

Step 10: In the **AS Number** box, enter **65501**.

Step 11: In the Options pane, select **Install Route**.



Step 12: On the Peer Group tab, click **Add**. The Virtual Router—BGP—Peer Group/Peer window appears.

Step 13: In the **Name** box, enter **Azure**.

Step 14: In the Peer pane, click **Add**. The Virtual Router—BGP—Peer Group—Peer window appears.

Step 15: In the **Name** box, enter **AzureRefArch**.

Step 16: In the **Peer AS** box, enter the autonomous system number assigned to the Azure virtual network gateway. The default is **65515**.

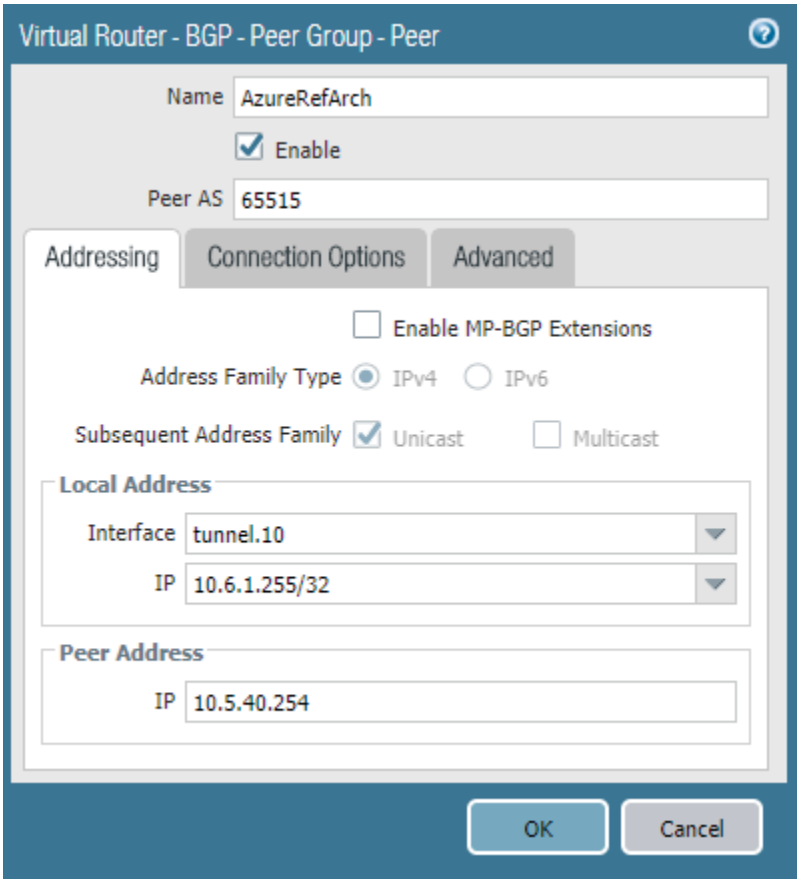
Step 17: In the Local Address pane, in the **Interface** list, select **tunnel.10**.

> **Note**
>
> If you are configuring the second device for resilient backhaul, use the value of **10.6.1.254/32** in Step 18.

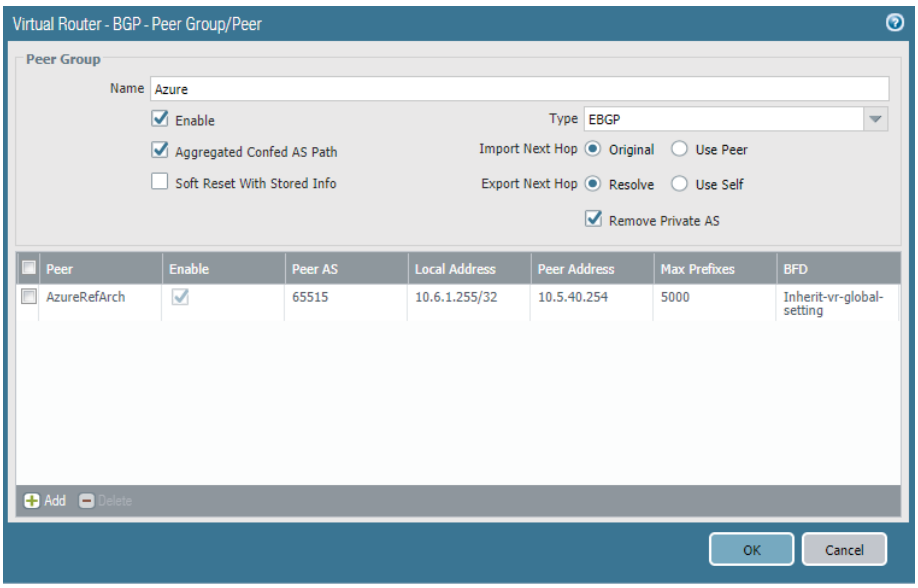
Step 18: In the Local Address pane, in the **IP** list, select **10.6.1.255/32**.

Step 19: In the Peer Address pane, in the **IP** box, enter the BGP peer IP address assigned by Azure to the virtual network gateway (example: **10.5.40.254**).

Step 20: On the Connection Options tab, in the **Multi Hop** box, enter **2**, and then click **OK**.

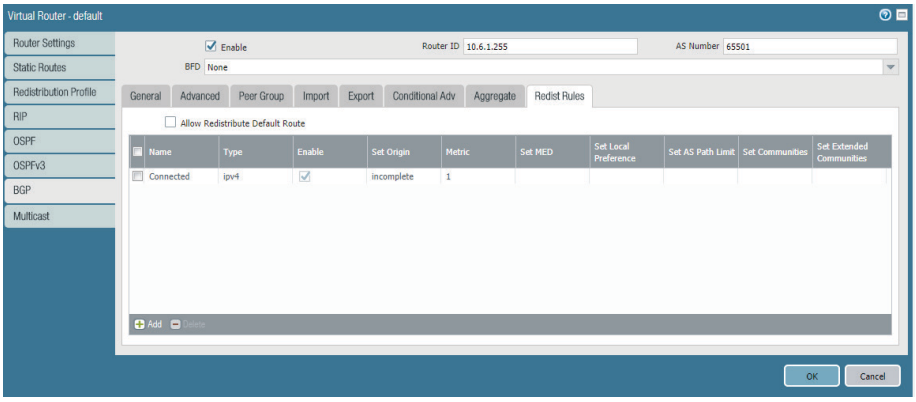


Step 21: Click **OK** to close the Virtual Router—BGP—Peer Group/Peer window.



Step 22: On the Redist Rules tab, click **Add**. The Virtual Router—BGP—Redistribute Rules—Rule window appears.

Step 23: In the **Name** list, select **Connected**, and then click **OK**.



Step 24: Click **OK** to close the Virtual Router—default window, and then click **Commit**.

Procedures

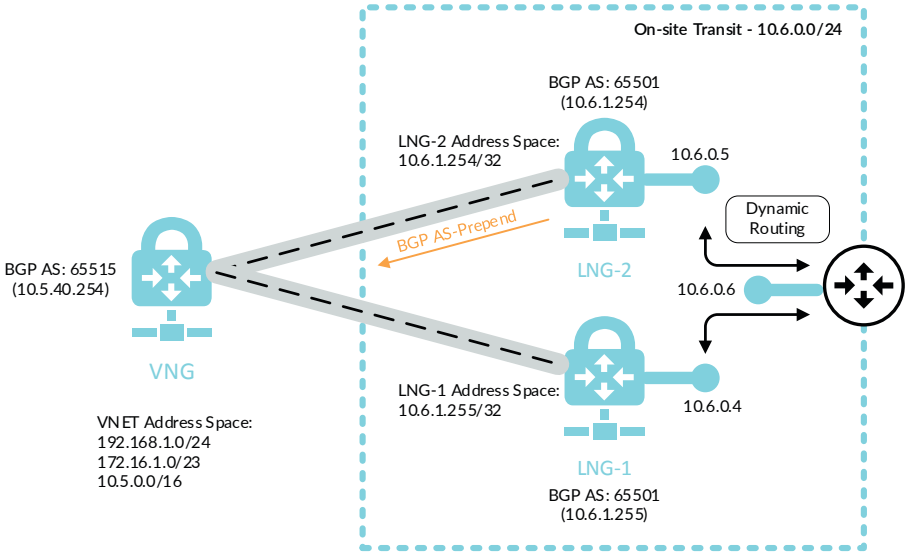
Configuring Resilient Backhaul Connection

This procedure group includes the necessary steps to add a second backhaul connection and configure BGP routing for Azure to prefer the first connection if both LNGs are connected. The first connection must already be configured with the BGP routing option.

This procedure relies on the following assumptions:

- The existing on-site firewall BGP peer address (assigned to tunnel interface) is **10.6.1.254**.
- The second existing on-site firewall must have a statically assigned public IP address.
- The on-site network is configured to use dynamic routing between the on-site firewalls and the internal private network. The downstream router learns the Azure routes from both on-site firewalls and is configured to use routing metrics to select the preferred path through the first connection.
- BGP AS-Prepend is used to make the second connection less preferred.

Figure 22 Resilient routing for backhaul connection



11.1 Create the Second Local Network Gateway

The local network gateway corresponds to the second on-premise firewall that terminates the resilient IPSec VPN tunnel from Azure.

Step 1: In **Home > Local network gateways**, click **Add**.

Step 2: In the **Name** box, enter **ARA-LNG-OnPrem-2**.

Step 3: In the **IP address** box, enter the public IP address of the on-premise IPSec VPN peer (Example: **104.42.56.197**).

Step 4: In the **Address space** box, enter only the IP prefix for the BGP peer address from the on-premise firewall this LNG corresponds to. (Example: **10.6.1.254/32**)

Step 5: Select **Configure BGP settings**.

Step 6: In the **Autonomous system number (ASN)** box, enter **65501**.

Step 7: In the **BGP peer IP address** box, enter **10.6.1.254**.

Step 8: In the **Resource Group** list, select **AzureRefArch**, and then click **Create**.

11.2 Create VPN Connection from VNG to LNG-2

Step 1: In **Home > Connections**, click **Add**.

Step 2: In **Home > Connections > Create connection > Basics**, in the **Connection type** list, select **Site-to-site (IPsec)**.

Step 3: In the **Resource Group** list, select **AzureRefArch**, and then click **OK**.

Step 4: In **Home > Connections > Create connection > Settings,** click the **Virtual network gateway** section, and then select **ARA-VNG**.

Step 5: Click the **Local network gateway** section, and then select **ARA-LNG-OnPrem-2**.

Step 6: In the **Connection name** box, enter **AzureRefArch-to-OnPrem-2**.

Step 7: In the **Shared key (PSK)** box, enter the value for the pre-shared key (complex password).

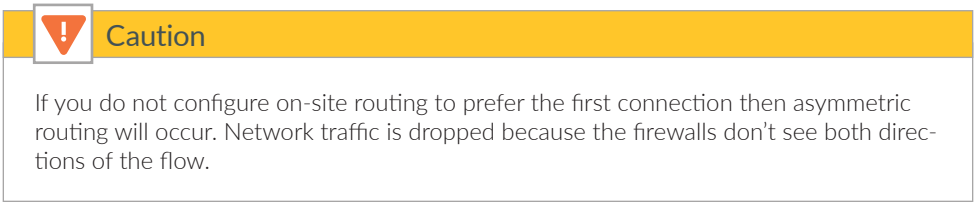
Step 8: Select **Enable BGP**, click **OK**.

Step 9: Review the Summary and if acceptable, click **OK**.

11.3 Configure additional on-site firewall

This procedure configures a second on-site firewall to be used for the resilient backhaul connection. After this firewall is configured by repeating earlier procedures, then BGP is configured to make the second connection less preferred.

The BGP configuration prepends a second AS number to the routes advertised from the second firewall. Azure receive all prefixes from both LNGs and uses the AS-path length to make its routing decision. This routing configuration ensures that Azure chooses the first connection when both are available when sending traffic from Azure to the on-site networks. This does not influence the path section in the opposite direction.



Step 1: Repeat Procedure 10.1 through Procedure 10.4 to configure the second firewall using new values as specified in the notes.

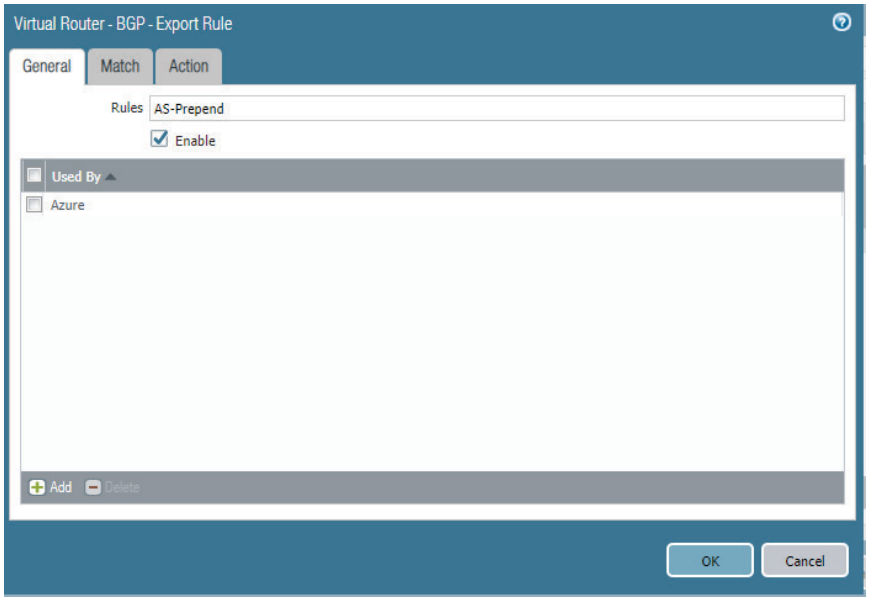
Step 2: In **Network > Virtual Routers**, click **default**. The Virtual Router—default window appears.

Step 3: On the BGP tab, change to the **Export** tab.

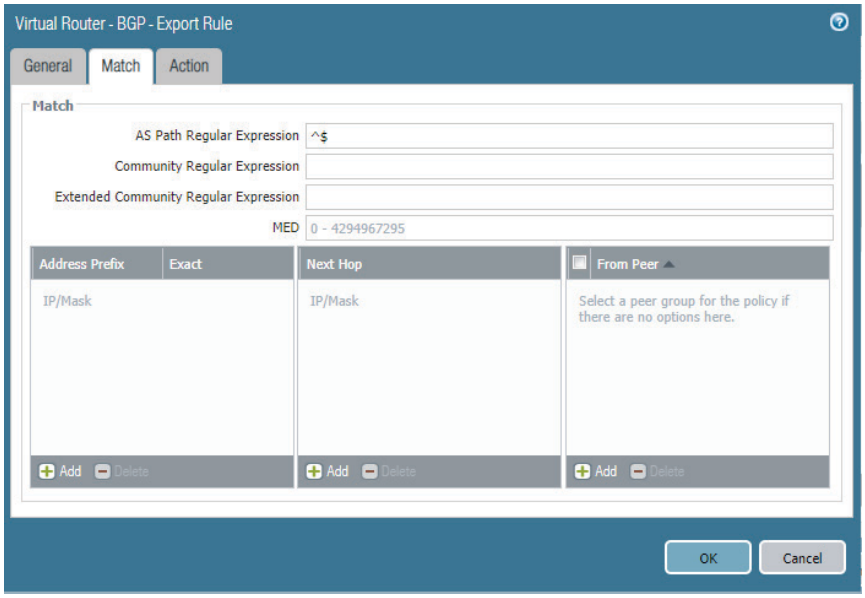
Step 4: Click **Add**, The Virtual Router—BGP—Export Rule window appears.

Step 5: In the **Rules** box, enter **AS-Prepend**.

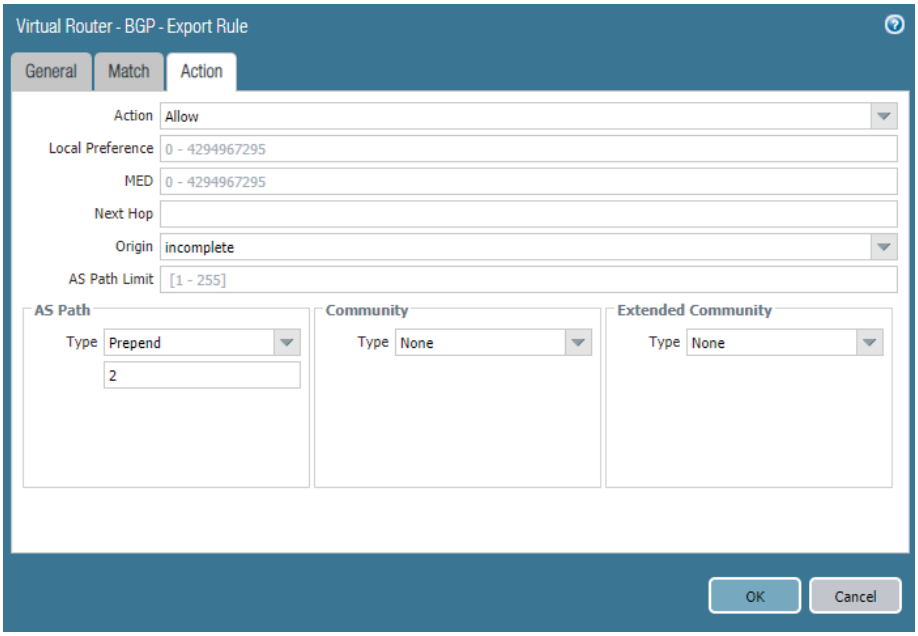
Step 6: In the Used By pane, click **Add**, and select **Azure**.



Step 7: On the Match tab, in the **AS Path Regular Expression** box, enter **^$**. This regular expression matches all prefixes that are local to this autonomous system.



Step 8: On the Action tab, in the AS Path section, in the **Type** list, select **Prepend**. In the **Type value** box, enter **2**.



Step 9: Click **OK** to close the Virtual Router—BGP—Export Rule window.

Step 10: Click **OK** to close the Virtual Router—default window, and then click **Commit**.

Procedures

Using Panorama to Configure Security and NAT for Backhaul Connection

12.1 Backhaul Connection—Create Address Objects

12.2 Backhaul Connection—Configure Security Policy

The security policy for the backhaul connection is enforced at multiple locations. The on-site firewall that terminates the VPN tunnel to Azure can use security policy rules between the private zone and the VPN zone. The VM-Series firewalls on Azure can use security policy rules between the VPN zone and the private zone.

NAT is not required for the backhaul traffic. If the destination traffic is within the Azure VNet, then the load balancer maintains session state to ensure that return traffic to the resource enters through the firewall that processed the out-going traffic.

Only the VM-Series policy is included in this guide.

12.1 Backhaul Connection—Create Address Objects

This procedure reuses objects already created in Procedure 8.11. If necessary, create additional objects using the same procedure. The table of objects (Table 28) is repeated here.

Table 36 Outbound traffic address objects

Object name	Description	Type	Type value
Net-10.5.1.0_24	Web subnet	IP Netmask	10.5.1.0/24
Net-10.5.2.0_24	Business subnet	IP Netmask	10.5.2.0/24
Net-10.5.3.0_24	DB subnet	IP Netmask	10.5.3.0/24

Step 1: Log in to Panorama (example: https://ara-panorama-1.westus.cloudapp.azure.com).

Step 2: Navigate to **Device Groups > Objects**.

Step 3: In the **Device Group** list, select **Azure-CommonFW**.

Step 4: In **Device Groups > Objects > Addresses**, click **Add**.

Step 5: In the **Name** box, enter **Net-10.6.0.0_16**.

Step 6: In the **Type** list, select **IP Netmask**.

Step 7: In the **Type value** box, enter **10.6.0.0/16**, and then click **OK**.

12.2 Backhaul Connection—Configure Security Policy

This procedure uses Security Pre Rules. These rules are logically evaluated prior to local rules and cannot be locally overridden on the local device.

The security policy example for the Backhaul Connection Profile permits these applications:

- SSH (ssh)
- RDP (ms-rdp)
- Web browsing (web-browsing)

This policy permits access to Azure private resources from connections initiated from devices from on-site networks. Add additional required applications to your policy as needed.

Step 1: In **Device Groups > Policies > Security > Pre Rules**, click **Add**.

Step 2: In the **Name** box, enter **VPN-to-Private**.

Step 3: On the Source tab, in the Source Zone pane, click **Add** and select **VPN**.

Step 4: In the Source Address pane, click **Add** and select **Net-10.6.0.0_16**.

Step 5: On the Destination tab, in the Destination Zone pane, click **Add** and select **Private**.

Step 6: In the Destination Address pane, click **Add** and select **Net-10.5.1.0_24**. Repeat this step for all objects in Table 36.

Step 7: On the Application tab, in the Applications pane, click **Add** and enter/search/select **ssh**

Step 8: In the Applications pane, click **Add** and enter/search/select **ms-rdp**.

Step 9: In the Applications pane, click **Add** and enter/search/select **web-browsing**.

Step 10: On the Service/URL Category tab, in the Service pane, select **application-default**.

Step 11: On the Actions tab, in the Action Setting section, in the **Action** list, select **Allow**.

Step 12: In the Log Setting section, in the **Log Forwarding** list, select **LoggingService-Profile**.

Step 13: On the Target tab, verify that **Any (target to all devices)** is selected, and then click **OK**.

> **Caution**
>
> Make sure to target all devices (any) in the device group; otherwise, the policy rule will not be automatically applied to new group members.

				Source		Destination					
	Name	Location	Type	Zone	Address	Zone	Address	Application	Service	Action	Target
12	VPN-to-Private	Azure-CommonFW	universal	VPN	Net-10.6.0.0_16	Private	Net-10.5.1.0_24 Net-10.5.2.0_24 Net-10.5.3.0_24	ms-rdp ssh web-browsing	application-default	Allow	any

Step 14: On the **Commit** menu, click **Commit and Push**.

Deployment Details for Automated Bootstrapping

Procedures

This procedure group provides an alternate deployment method to Procedure 4.1. In addition to deploying the VM-Series using the ARM template, the automated bootstrap process licenses the VM-Series and registers the VM-Series device with Panorama with the designated templates and device group. This option would not typically be chosen to deploy the initial devices, but it is an effective option for scaling performance by adding additional firewalls after the first pair have been deployed.

After deployment using the bootstrap, a new VM-Series is added to the backend pools for the Azure load-balancers and Azure application gateways to complete the integration and make the VM-Series active.

13.1 Create the Bootstrap Package

Step 1: Generate VM Auth Key on Panorama.

The next step requires the use of the command line. (You can also do it via API, but that option is not covered by this guide.)

Step 2: Using SSH, log in to the Panorama command line.

Step 3: Request the VM auth key by using the following command. The lifetime of the key can vary between 1 hour and 8760 hours (1 year). After the specified time, the key expires. Panorama does not register VM-Series firewalls without a valid auth-key in the connection request.

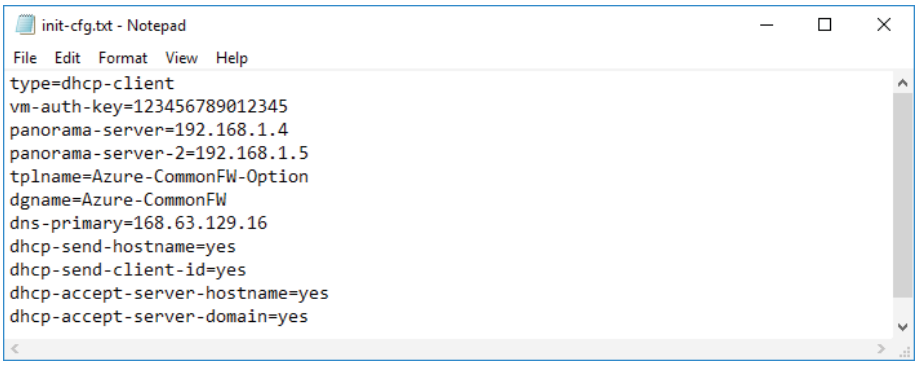
```
request bootstrap vm-auth-key generate lifetime 8760

VM auth key 123456789012345 generated. Expires at: 2019/06/07 14:15:56
```

Step 4: Create init-cfg.txt file.

The following table includes the parameters required for successful bootstrap on Azure. The VM-Series registers with Panorama and is assigned to the listed template stack and device group. Create the file by using a text editor and save as init-cfg.txt

Table 37 Required parameters for Azure bootstrap

Description	Parameter	Value
Type of management IP address	type	dhcp-client
Virtual machine authentication key	vm-auth-key	(generated on Panorama)
Panorama IP address	panorama-server	192.168.1.4
Panorama IP address (secondary)	panorama-server-2 (optional for H/A only)	192.168.1.5 (optional for H/A only)
Template stack name	tplname	Azure-CommonFW-Option
Device group name	dgname	Azure-CommonFW



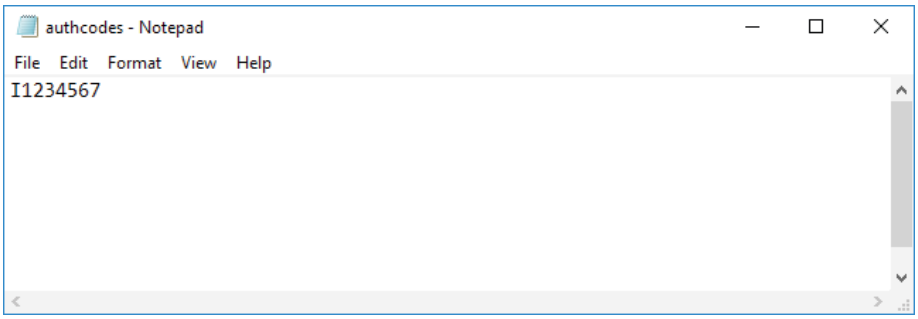
Step 5: If you are using BYOL, create the authcodes file. An auth code bundle includes all of the VM-Series feature licenses with a single auth code.

Example: **I1234567**

Caution

The filename for the authcodes file must not include any extension such as .txt. If you save the file with an extension, the bootstrap process fails.

Create the file using a text editor and save as **authcodes**.

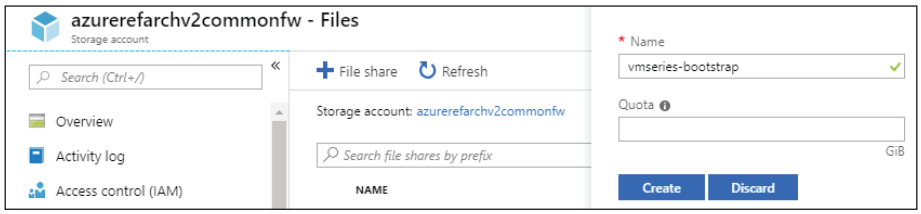


13.2 Deploy the Bootstrap Package to Azure Storage

This procedure creates a new file share for the bootstrap package in an existing storage account. Each bootstrap package is located within a unique directory within the file share.

Step 1: In **Home > Storage accounts > azurerefarchv2commonfw > File service > Files**, click **File share**.

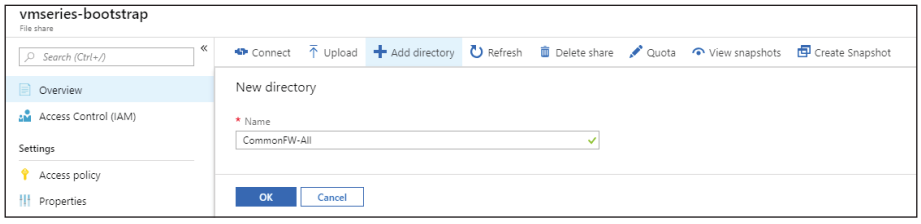
Step 2: In the **Name** box, enter **vmseries-bootstrap**, and click **Create**.



Step 3: In **Home > Storage accounts > azurerefarchv2commonfw > FILE SERVICE > Files**, click **vmseries-bootstrap**.

Step 4: Click **Add directory.**

Step 5: In the Name box, enter **CommonFW-All**, and then click **OK**.



Step 6: In **Home > Storage accounts > azurerefarchv2commonfw - Files > vmseries-bootstrap**, click **CommonFW-All**.

Table 38 Bootstrap package structure

Directory name	File
config	init-cfg.txt
content	—
license	authcodes
software	—

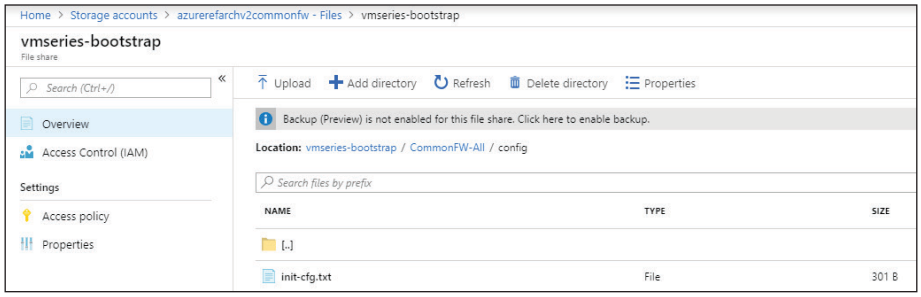
Step 7: Click **Add directory**.

Step 8: In the **Name** box, enter **config**, and then click **OK**.

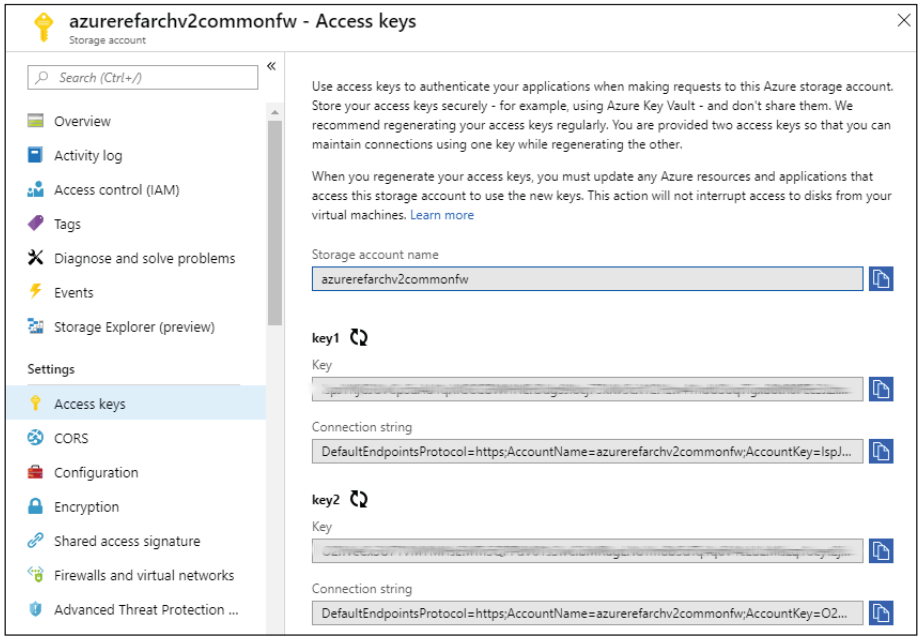
Step 9: If a **File** is listed for a corresponding directory in Step 6, then complete these substeps for the file:

- Click **config**.
- Click **Upload**.
- In the Upload files pane, browse to your local filesystem and select **init-cfg.txt**.
- Click **Upload**.

Step 10: Repeat Step 7 through Step 9 for each entry in Step 6.



Step 11: In **Home > Storage accounts > azurerefarchv2commonfw > Settings > Access keys**, record the access key for the storage account (either key1 or key2) by using **Click to copy**.



Note

You will need to provide the Storage Account, valid Storage Account access key, and File Share, and File Share Directory at deployment time.

Example:

Storage Account Name: azurerefarchv2commonfw
Access Key: <key>
File Share Name: vmseries-bootstrap
File Share Directory: CommonFW-All

13.3 Create the Public IP Address for VM-Series

This procedure is identical to Procedure 3.6. It is repeated here for completeness.

The VM-Series devices deployed on Azure are managed using public IP addresses unless on-site network connectivity has been established. The process to configure on-site network connectivity is included later in this guide.

This procedure creates a public IP address that is associated to the management interface of the VM-Series at deployment time. If necessary, this procedure is repeated to create additional public IP addresses for additional VM-Series devices. The parameters listed in Table 4 are used to complete this procedure.

Take note of the fully qualified domain name (FQDN) that is defined by adding the location specific suffix to your DNS name label. We recommend managing your devices using the DNS name rather than the public IP address, which may change.

Step 1: In **Home > Public IP addresses**, click **Add.**

Step 2: In the **Name** box, enter **aracf-vmfw3**.

Step 3: Select **Standard** SKU.

Step 4: In the **DNS name label** box, enter **aracf-vmfw3**.

Step 5: In the **Resource Group** list, select **AzureRefArch-CommonFW**, and then click **Create**.

Procedures

The following procedures are completed using the Azure Resource Manager deployed from an Azure Resource Manager Template posted at GitHub. If you are already signed in to Azure at https://portal.azure.com, then the deployment from GitHub uses the same session authorization.

14.1 Deploy the VM-Series

This procedure is essentially identical to Procedure 4.1, with additional steps to provide the bootstrap information.

Table 39 VM-Series bootstrap deployment parameters

Parameter	Value	Comments
Resource group	AzureRefArch-CommonFW	Existing
Location	—	Tested in West US
VM name	ARACF-VMFW3	First bootstrap device. Assumes two firewalls already deployed
Storage account name	azurerefarchv2commonfw	—
Storage account existing RG	AzureRefArch-CommonFW	—
Fw Av set	AzureRefArch-CommonFW-AS	—
VM size	Standard_D3_v2	https://www.paloaltonetworks.com/documentation/80/virtualization/virtualization/set-up-the-vm-series-firewall-on-azure/about-the-vm-series-firewall-on-azure/minimum-system-requirements-for-the-vm-series-on-azure
Public IP type	standard	Standard IP SKU required for use with Azure Standard load-balancer
Image version	latest	—
Image Sku	byol	—
Bootstrap firewall	yes	—
Bootstrap storage account	azurerefarchv2commonfw	The bootstrap storage account may be in any resource group within the same Azure subscription and location.
Storage account access key	<key>	Use value recorded from Procedure 13.2, Step 11
Storage account file share	vmseries-bootstrap	Created in Procedure 13.2
Storage account file share directory	CommonFW-All	Created in Procedure 13.2
Virtual network name	AzureRefArch-VNET	Uses AzureRefArch-VNET in resource group AzureRefarch
Virtual network address prefix	192.168.1.0/24	Match the initial IP address space from AzureRefArch-VNET
Virtual network existing RG name	AzureRefArch	—
Subnet0Name	Management	—
Subnet1Name	CommonFW-Public	—

Table continued on next page

Continued from previous page

Parameter	Value	Comments
Subnet2Name	CommonFW-Private	—
Subnet3Name	CommonFW-VPN	—
Subnet0Prefix	192.168.1.0/24	—
Subnet1Prefix	172.16.1.0/24	—
Subnet2Prefix	10.5.0.0/24	—
Subnet3Prefix	10.5.15.0/24	—
Subnet0Start Address	192.168.1.8	First bootstrap device
Subnet1Start Address	172.16.1.8	First bootstrap device
Subnet2Start Address	10.5.0.8	First bootstrap device
Subnet3Start Address	10.5.15.8	First bootstrap device.
Admin username	refarchadmin	—
Admin password	<password>	—
Public IP address name	aracf-vmfw3	First bootstrap device
Nsg name	None	NSG is applied at the subnet level

The custom Azure Resource Manager template used in this procedure has been developed and validated specifically for this deployment guide.

For template details and features, see: https://github.com/PaloAltoNetworks/ReferenceArchitectures/tree/master/Azure-1FW-4-interfaces-existing-environment-BS.

Use the parameters in Table 39 to deploy each VM-Series with bootstrap configuration.

Step 1: Deploy the VM-Series by clicking **Deploy to Azure**.

Step 2: In the **Resource Group** list, select **AzureRefArch-CommonFW**.

Step 3: In the **Vm Name** box, enter **ARACF-VMFW3**.

Step 4: In the **Storage Account Name** box, enter **azurerefarchv2commonfw**.

Step 5: In the **Storage Account Existing RG** box, enter **AzureRefArch-CommonFW**.

Step 6: In the **Fw Av Set** box, enter **AzureRefArch-CommonFW-AS**.

Step 7: In the **Vm Size** list, select **Standard_D3_v2**.

Step 8: In the **Public IP Type** list, select **standard**.

Step 9: In the **Image Version** list, select **latest**.

Step 10: In the **Image Sku** list, select **byol**.

Step 11: In the **Bootstrap Firewall** list, select **yes**.

Step 12: In the **Bootstrap Storage Account** box, enter **azurerefarchv2commonfw**.

Step 13: In the **Storage Account Access Key** box, enter the key value.

Step 14: In the **Storage Account File Share** box, enter **vmseries-bootstrap**.

Step 15: In the **Storage Account File Share Directory** box, enter **CommonFW-All**.

Step 16: In the **Virtual Network Name** box, enter **AzureRefArch-VNET**.

Step 17: In the **Virtual Network Address Prefix** box, enter **192.168.1.0/24**.

Step 18: In the **Virtual Network Existing RG Name** box, enter **AzureRefArch**.

Step 19: In the **Subnet0Name** box, enter **Management**.

Step 20: In the **Subnet1Name** box, enter **CommonFW-Public**.

Step 21: In the **Subnet2Name** box, enter **CommonFW-Private**.

Step 22: In the **Subnet3Name** box, enter **CommonFW-VPN**.

Step 23: In the **Subnet0Prefix** box, enter **192.168.1.0/24**.

Step 24: In the **Subnet1Prefix** box, enter **172.16.1.0/24**.

Step 25: In the **Subnet2Prefix** box, enter **10.5.0.0/24**.

Step 26: In the **Subnet3Prefix** box, enter **10.5.15.0/24**.

Step 27: In the **Subnet0Start Address** box, enter **192.168.1.8**.

Step 28: In the **Subnet1Start Address** box, enter **172.16.1.8**.

Step 29: In the **Subnet2Start Address** box, enter **10.5.0.8**.

Step 30: In the **Subnet3Start Address** box, enter **10.5.15.8**.

Step 31: In the **Admin Username** box, enter **refarchadmin**.

Step 32: In the **Admin Password** box, enter the password.

Step 33: In the **Public IP Address Name** box, enter **aracf-vmfw3**.

Step 34: In the **Network Security Group** box, enter **None**.

Step 35: Review the terms and conditions**.** If they are acceptable, select **I agree to the terms and conditions**.

Step 36: Click **Purchase**.

After deployment, the device registers with Panorama by using the provided bootstrap information. The device is automatically licensed using the bundled auth-code in the bootstrap package. After the services are restarted, the device receives template and device group configuration from Panorama and is ready to be managed.

The software should be upgraded to the same version as other VM-Series firewalls. This procedure is identical to Procedure 4.3 in this guide.

14.2 Add VM-Series to Load-Balancer Backend Pools

You already created the public and private load-balancers in Procedure 7.2 and Procedure 7.4, as well as performing other configurations and updates throughout the guide. Now you integrate additional firewall resources into the design by adding the VM-Series devices to the load-balancer backend pools.

This procedure only includes the steps to add an additional VM-Series device to existing backend pools. Repeat this procedure for each VM-Series device as required.

Step 1: In **Home > Load Balancers > ARA-CommonFW-LB-Public** , click **Backend pools**.

Step 2: Click **Firewall-Layer**.

Step 3: In the **VIRTUAL MACHINE** column, in the first blank row, select a VM-Series to be added to this backend pool (example: **aracf-vmfw3-bs**).

Step 4: In the **IP ADDRESS** column, select the **IP configuration** that is associated to the **CommonFW-Public** subnet. (example: **ipconfig-untrust**).

Step 5: Click **Save**, and then click **X** to exit.

Step 6: In **Home > Load Balancers > ARA-CommonFW-Internal**, click **Backend pools**.

Step 7: Click **Firewall-Layer-Private**.

Step 8: In the **VIRTUAL MACHINE** column, in the first blank row, select a VM-Series to be added to this backend pool (example: **aracf-vmfw3-bs**).

Step 9: In the **IP ADDRESS** column, select the **IP configuration** that is associated to the **CommonFW-Private** subnet. (example: **ipconfig-trust**).

Step 10: Click **Save**, and then click **X** to exit.

Step 11: If you have additional backend pools for your internal load-balancer for Inbound Access and Backhaul and Management traffic, then repeat Step 6 through Step 10 for the **Firewall-Layer-Public** backend pool on the **Common-FW-Public** subnet and the **VPN-Firewall-Layer** backend pool on the **CommonFW-VPN** subnet.

14.3 Outbound Access—Create Public IP Address and Associate with Firewall

This procedure is identical to Procedure 8.10. It is repeated here for completeness.

For virtual machines behind the firewall to communicate to devices on the internet, the firewall must translate the source IP address of the outbound traffic to an IP address on the public subnet. The simplest method is to use dynamic IP and port translation to the firewall's public interface IP address.

Azure then translates the source IP address again as the outbound traffic leaves the VNet. Because the firewall's public interface is a member of the Azure public load-balancer backend pool, Azure networking performs translation for only TCP/UDP ports referenced in the active load balancing rules. To support a broad range of services, create a new public IP address for the public interface of each firewall used for outbound access. This method supports all TCP/UDP ports.

Step 1: Repeat Procedure 8.10 for each additional VM-Series device.

What's New in This Release

Palo Alto Networks made the following changes since the last version of this guide:

- The PAN-OS version tested in this deployment guide is 8.1.5 for all devices.
- The Cloud services plugin for Panorama is 1.2.0-h2.
- The *Shared design mode*l has been renamed the *Single VNet design model—common firewall option* throughout the guide.
- The Azure application gateway has been added as an additional option for the Inbound Access traffic profile. New procedures to deploy the application gateway and configure the firewalls have been added.
- Made minor changes to improve readability and technical accuracy.

You can use the feedback form to send comments about this guide.

Headquarters

Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054, USA
www.paloaltonetworks.com

Phone: +1 (408) 753-4000
Sales: +1 (866) 320-4788
Fax: +1 (408) 753-4001
info@paloaltonetworks.com

B-000116P-19A-1 02/19