Deployment Guide for Azure

Transit VNet Design Model

JANUARY 2020

paloalto NETWORKS®

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

ABOUT PROCEDURES

These guides sometimes describe other companies' products. Although steps and screen-shots were up-to-date at the time of publication, those companies might have since changed their user interface, processes, or requirements.

GETTING THE LATEST VERSION OF GUIDES

We continually update reference architecture and deployment guides. You can access the latest version of this and all guides at this location:

https://www.paloaltonetworks.com/referencearchitectures

WHAT'S NEW IN THIS RELEASE

Palo Alto Networks made the following changes since the last version of this guide:

- Modified the Transit VNet design model to include configuration options for inbound traffic to use a public load balancer or application gateway
- Changed *Logging Service* to *Cortex™ Data Lake*
- Changed Azure VNet IP space allocation to use a single block per VNet
- Updated the design model to use a single front-end IP and single back-end pool with Azure Load Balancer
- Removed the requirement to use source NAT to ensure symmetric routing when using Azure Load Balancer
- Made minor changes to improve readability and technical accuracy

Comprehensive revision history

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 Transit Virtual Network (VNet) design model. Details for the Common Firewall design model option 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 outbound and east-west from private networks and for secure communication with on-premises 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
- Panorama™ centralized management using templates and device groups
- Centralized reporting with Palo Alto Networks cloud-delivered Cortex Data Lake (formerly *Logging Service*)

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 data center 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.
- Deployment Guide for Panorama on Azure—Provides architectural guidance and deployment details for using a Palo Alto Networks Panorama management system, deployed on Microsoft Azure, to provide a single location from which you can create network configurations and security policies that enable visibility, control, and protection to your applications built in an Azure public cloud. The *Deployment Guide for Panorama on Azure* is a prerequisite for this guide.
- Deployment Guide for Azure—Transit VNet Design Model (Common Firewall Option)—Details deployment scenarios and step-by-step guidance for the common firewall option of the Transit VNet design model on Azure.

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 provides 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-premises networks.

This guide is specific to the Transit VNet design model. 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-premises communication balanced? The Transit VNet model allows you to scale inbound access independently based on business need. The outbound, east-west, and backhaul performance provided from the transit VNet scales linearly by adding additional firewalls to the load-balancer back-end pools.
- **Complexity**—Is it more important to keep individual device configuration simple and permit easier trouble-shooting, or is it acceptable to take on a somewhat higher administrative workload in order to reduce the total number of deployed devices? The Transit VNet model uses one set of devices for outbound, east-west, and backhaul traffic profiles and a separate set of devices for inbound traffic profiles. The proper function of each subscriber VNet depends on the transit VNet, so careful consideration of any changes is necessary in order to evaluate overall impact.
- **Resiliency and high availability**—Are there differentiated availability requirements for different traffic profiles? The transit VNet model provides the same level of availability for the outbound, east-west, and backhaul traffic profiles. The Transit VNet model allows you to inherently provide a differentiated level of availability for inbound traffic flows, which have dedicated firewall resources.

Design Models

The primary difference between the design models is resource allocation 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:

- **Transit VNet model**—In this model, you allocate the functions and resources across multiple VNets that are connected in a hub-and-spoke topology. The hub of the topology, or *transit VNet*, is the central point of connectivity for all inbound, outbound, east-west, and backhaul traffic. The spokes isolate workloads in their own VNets. This design model is highly scalable and highly resilient and is suitable for large-production deployments.

  The 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. You deploy all firewalls in the transit VNet.

  This model consolidates resources that multiple workloads can share. This model also offers increased scale and operational resiliency and reduces the chances of high bandwidth use from the inbound access traffic profile affecting other traffic profiles. Palo Alto Networks recommends this model for your production deployments. This guide covers the deployment details for this model.

- **Transit VNet model (Common Firewall Option)**—This option is identical to the Transit VNet model, except that in this option, all traffic flows through a single set of firewalls. The set of firewalls is a shared resource and has limited scale. This option keeps the number of firewalls low and is suitable for small deployments and proof-of-concepts. However, the technical integration complexity is high. For deployment details for this option, see Deployment Guide for Microsoft Azure—Transit VNet Design Model (Common Firewall Option).

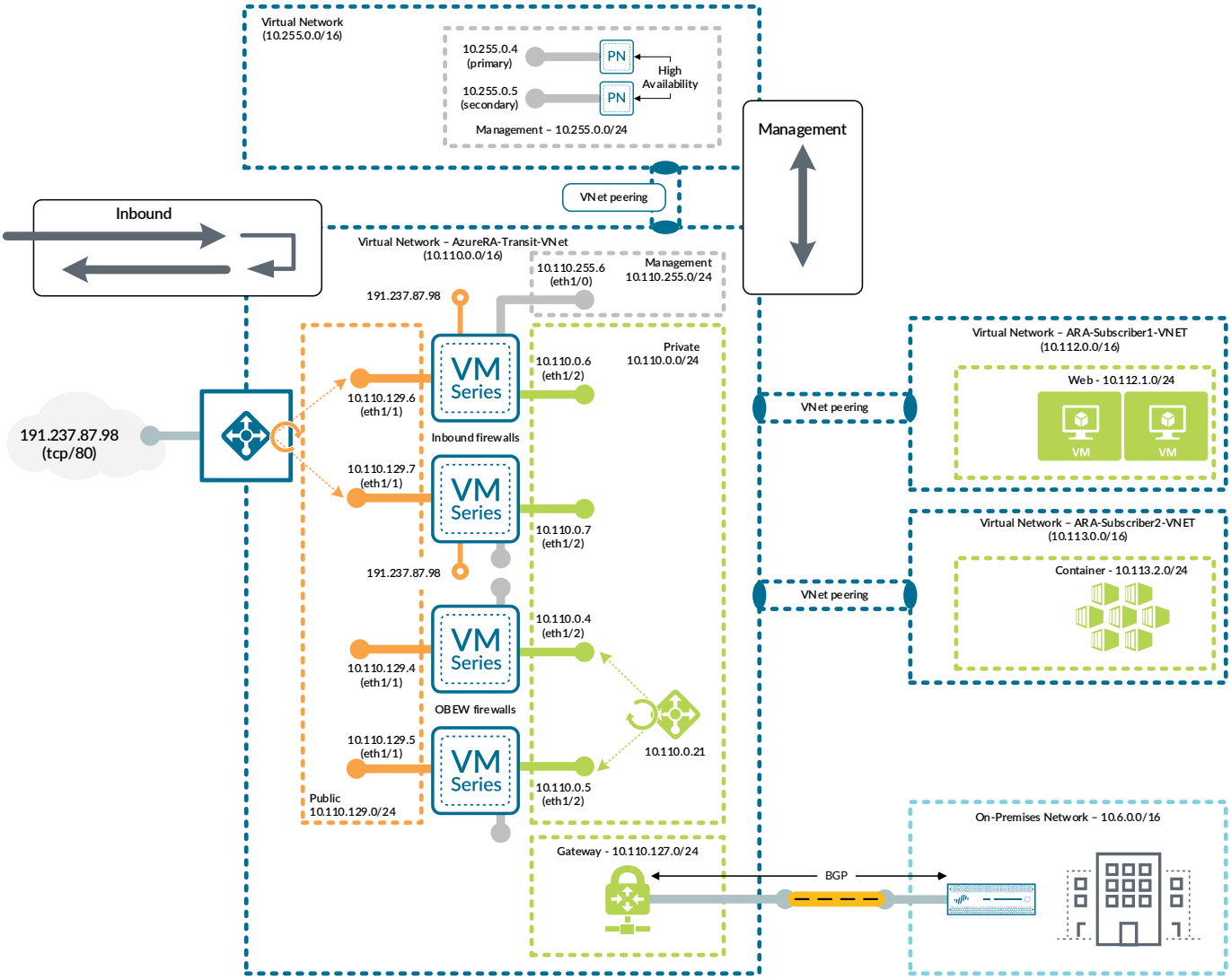
TRANSIT VNET MODEL

The Transit VNet model distributes the various traffic profiles across resources in multiple VNets and is highly scalable. This design model is composed of a single transit VNet and one or more subscriber VNets. The transit VNet does not typically contain any virtual compute resources and acts as a hub for interconnecting the subscriber (or *spoke*) VNets. A transit VNet provides inbound, outbound, and backhaul access for subscriber VNets as a shared service. The transit VNet also controls east-west traffic between subscribers.

A dedicated set of firewalls services inbound traffic from the internet. Another set of firewalls provides visibility and control of all other traffic profiles (outbound, east-west, and backhaul). The firewalls are members of availability sets that distribute their virtual machines across the Azure infrastructure in order to avoid downtime caused by infrastructure maintenance or failure. The separation of functions allows inbound traffic volume to scale independently and simplifies the configuration of the inbound firewalls. You manage the firewalls in the transit VNet from Panorama deployed in a peered VNet.

This model requires that you establish a VNet peer connection between each subscriber VNet and the transit VNet. You cannot use overlapping IP address space within the set of peered VNets.

Figure 1 Transit VNet model



Inbound Traffic

There are two options for inbound traffic:

- **Azure public load balancer**—Choose this option if you require load balancing at Layer 4 only (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

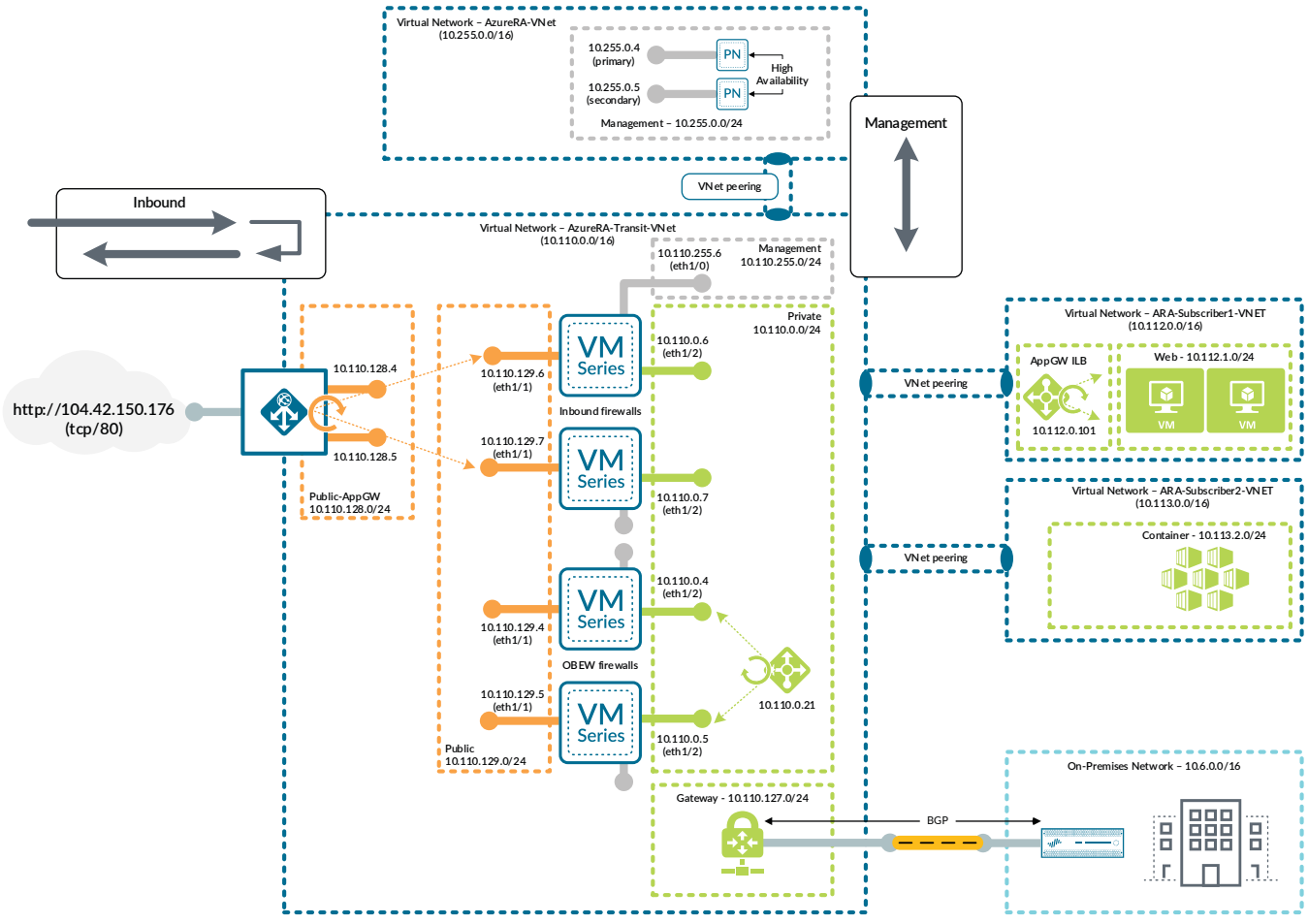
For inbound traffic, a public load balancer distributes traffic to the inbound firewalls. To simplify firewall configuration, the front-end public IP address is associated with a DNS name, and floating IP is enabled on the load-balancer rules. Load-balancer rules forward the required web service ports to the firewalls. Common ports required for inbound traffic include TCP/80 (HTTP) and TCP/443 (HTTPS). The public load balancer's health probes monitor firewall availability through the HTTPS or SSH services activated in the interface management profile. Only traffic sourced from the health probe IP address can connect to the HTTPS or SSH services.

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.

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 subscriber 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 by the security policy.

Inbound Traffic with Azure Application Gateway

Figure 2 Transit VNet model 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 you distribute the instances across Azure update and fault domains.

For inbound traffic, an application gateway with a public front end terminates incoming connections and initiates corresponding new connections to the configured HTTP/HTTPS back ends. You assign unique TCP ports for all back ends. The application gateway sources all new connections from the private IP addresses of the application gateway instances and distributes the connections to the public interfaces of the inbound firewalls, which you have configured as the back-end pool targets for the application gateway. The application gateway's health probes monitor back-end availability on all specified HTTP/HTTPS ports.

You use application gateway destination NAT rules on the firewalls to map to back-end resources directly or through one or more internal load balancers.

This model supports any combination of the following methods:

- **Firewall destination port NAT to back-end resource**—No internal load balancer required, uses port-based NAT policy rules associated to the back-end resource. The firewall NAT policy contains all resource-mapping parameters.
- **Internal load balancer with one or more front-end IP addresses**—Uses port-based NAT policy rules associated to the load balancer's front-end IP addresses. You also configure port mapping on the load balancer. This option uses the load balancer for resiliency and scaling of the back-end resources.
- **Multiple internal load balancers**—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 back-end 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.

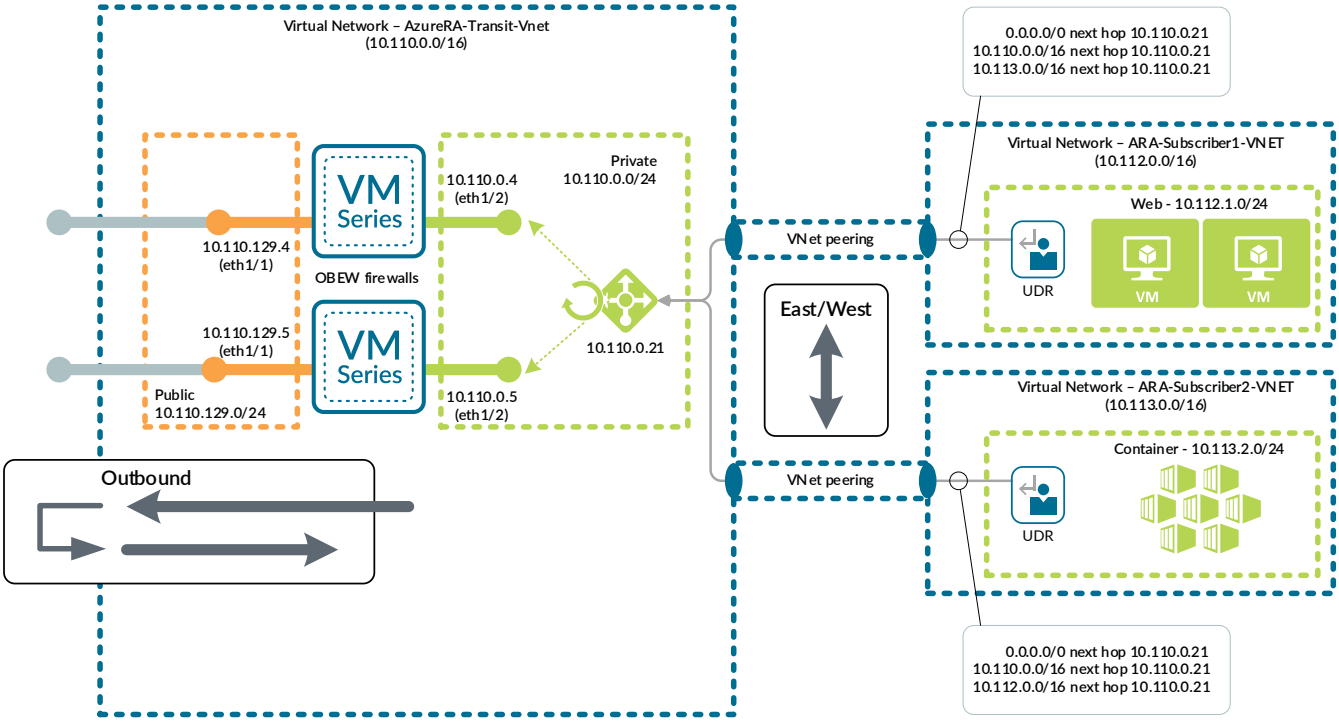
The firewall security policy allows HTTP/HTTPS application traffic from the application gateway instances to the resources in the private network, and firewall security profiles prevent known malware and vulnerabilities from entering the network in traffic allowed by the security policy. To support the use of HTTP/HTTPS back ends on ports other than 80/443, you should configure the service for security policy rules 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 destined for 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.

Outbound Traffic

User-defined routes on the private subnets in the subscriber VNets direct traffic to the load balancer's front-end IP address, which shares a subnet with the firewall private interfaces. The internal load balancer in the transit VNet distributes traffic to the set of firewalls. Load-balancer rules forward all TCP and UDP ports to the firewalls. The internal load balancer's health probes monitor firewall availability through the HTTPS service enabled in the interface management profile. Only traffic sourced from the health probe IP address can connect to the HTTPS service.

Figure 3 Outbound and east-west traffic



You define static routes for the health probe IP address and for the private network range out of the private interface because that is the interface that is receiving the health probes. Additionally, a static default route forwards traffic out the public interface.

The firewall applies source NAT to outbound traffic. The firewall translates the source address to its public interface. Azure automatically translates the interface IP address to the public IP address associated to the firewalls public interface when the traffic leaves the VNet.

The firewall security policy allows appropriate application traffic from the resources in the subscriber private networks 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 by the security policy. URL filtering, file blocking, and data filtering protect against data exfiltration.

East-West Traffic

The same internal load balancer that distributes outbound traffic to the firewalls also distributes the spoke-to-spoke *east-west* traffic, which is the traffic between private subnets within different subscribers. You apply user-defined routes for the private network subnets to the private subnets and direct traffic to the transit VNet's internal load balancer's front-end IP address. The existing load-balancer rules for outbound traffic apply to east-west traffic, as well, and apply to all TCP/UDP ports.

The firewall should not translate the destination for traffic between private subnets. A positive control security policy should allow only appropriate application traffic between private resources and requires that you create corresponding security policy rules to permit specific traffic. You must then override the default intrazone security policy rule and modify it 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 by the security policy.

Backhaul and Management Traffic

The same internal load balancer that distributes outbound and east-west traffic to the firewall also distributes traffic from on-premises networks. User-defined routes applied to the gateway subnet direct traffic that has a destination in the private network range to the internal load balancer. The existing load-balancer rules for outbound traffic apply to backhaul and to all TCP and UDP ports.

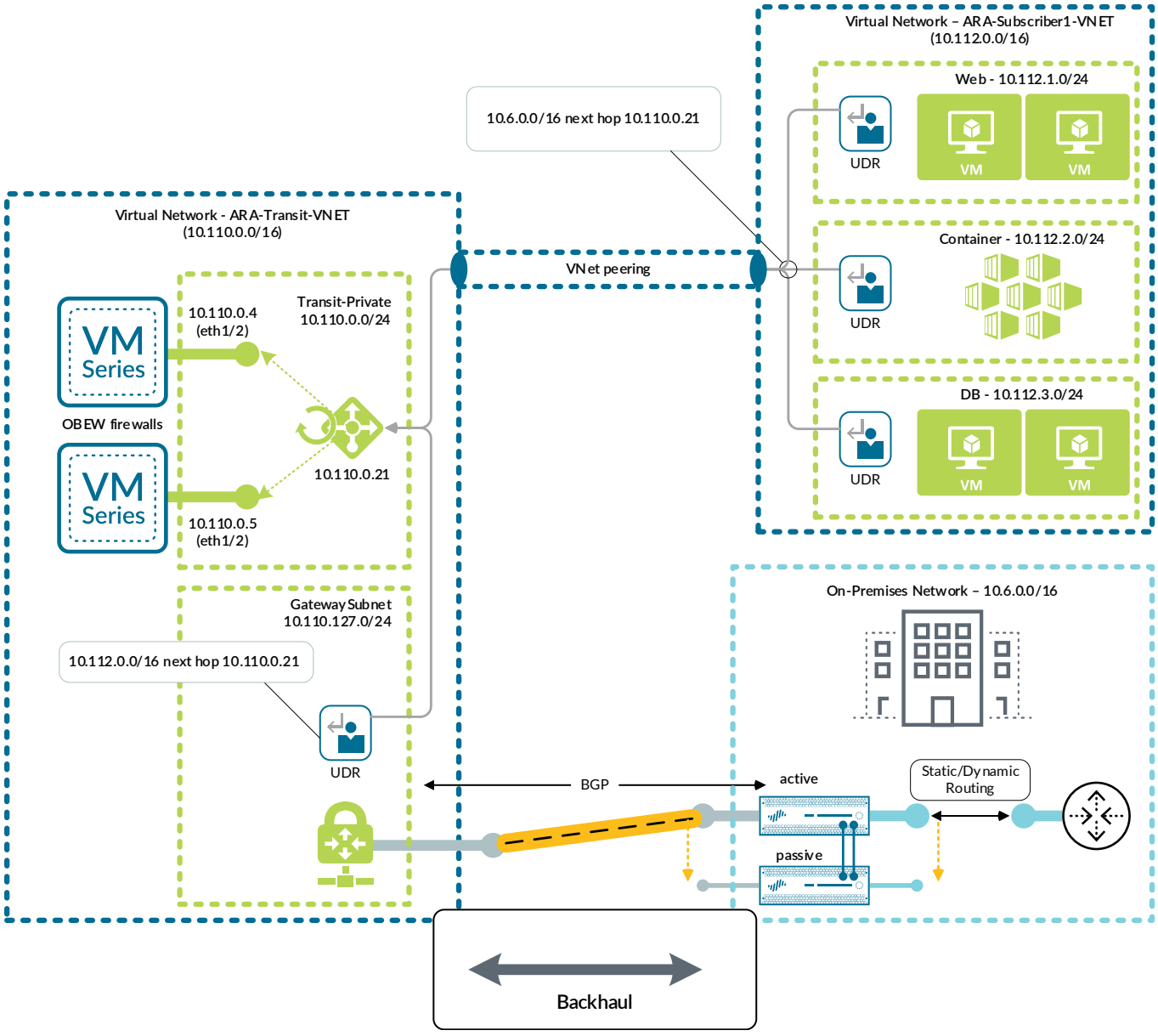
Traffic originating in private subnets and destined to on-premises networks follows the same path as outbound and east-west traffic. The only additional requirement is that you apply user-defined routes that forward on-premises network ranges to the internal load-balancer front end.

A VNG deployed in the transit VNet connects the Azure virtual networks to the on-premises networks. Enable BGP dynamic routing to the on-premises networks. Disable BGP route-propagation for public subnets. This eliminates the need for user-defined routes to discard the traffic to the on-premises networks.

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

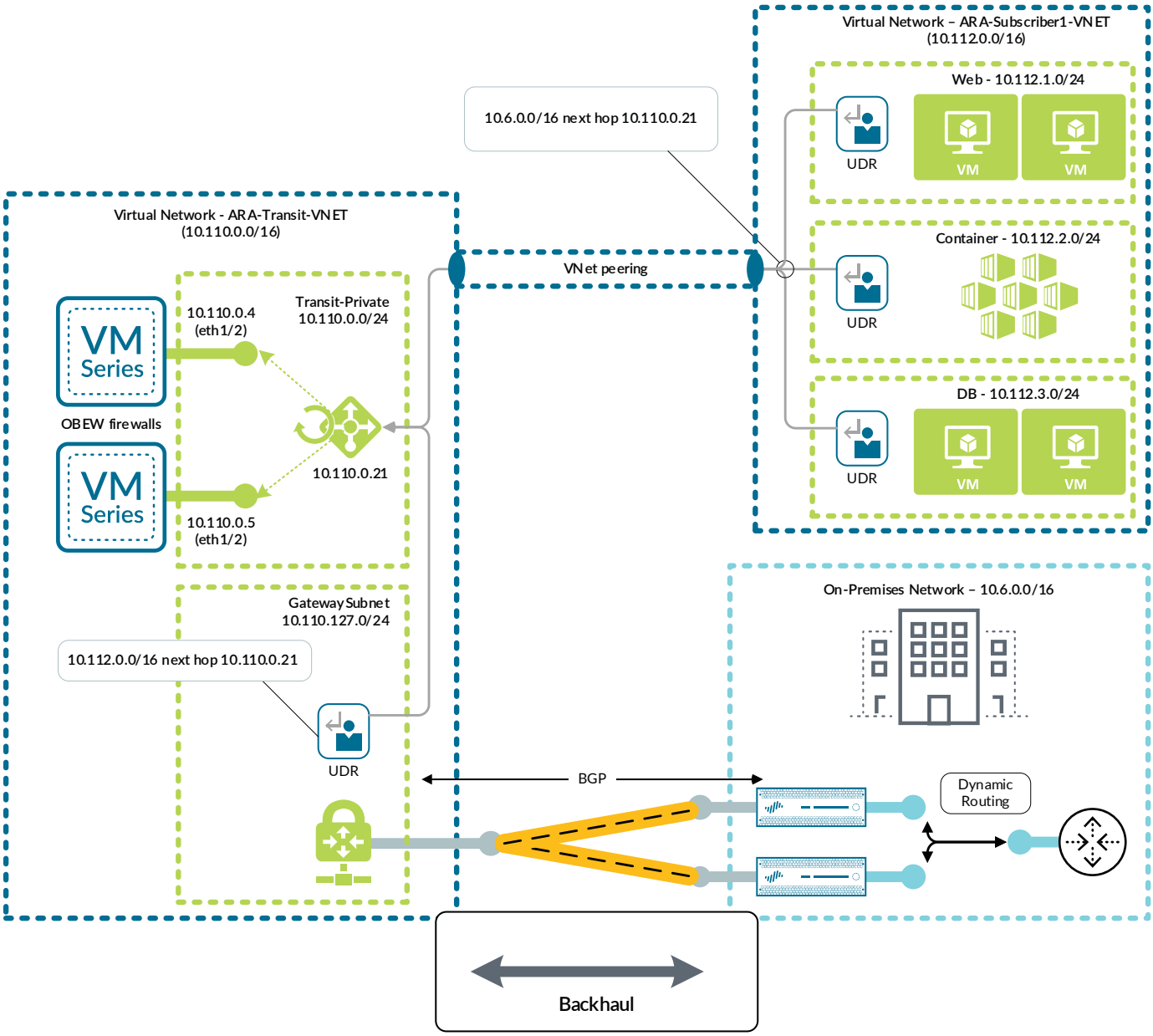
Deploy an active/passive firewall pair at your on-premises network and configure a single VPN tunnel from the VNG to the firewall pair. The high availability features of the firewall provide resiliency for this topology. If the active firewall fails, the passive firewall becomes active. In this configuration, only a single firewall is forwarding traffic.

Figure 4 Transit VNet with active/passive firewall pair



If you prefer to rely on dynamic routing protocols for resiliency, then deploy an active/active firewall pair at your on-premises networks and configure a VPN tunnel from the VNG to each firewall. You configure BGP to prefer one tunnel as the active path and the other tunnel as a backup path. If the firewall with the active path fails, BGP reroutes traffic to the backup path through the other active firewall. Traffic only flows over a single tunnel in both directions to ensure route symmetry.

Figure 5 Transit VNet with active/active firewall pair



Assumptions and Prerequisites

Microsoft Azure:

- Your organization has a valid active subscription associated with your Azure user account.
- A resource group and VNet for Panorama already exist.
- A new resource group for the transit VNet already exists.
- One or more subscriber VNets with their own resource groups already exist.
- Azure uses standard-SKU IP addresses and load balancers, except where specifically noted in the guide.
- Only IPv4 networking is used.
- This deployment was tested predominantly in the US West region, although deploying this design should be possible in any Azure region.

Palo Alto Networks next-generation firewalls and Panorama:

- You have already deployed Panorama and completed all procedures in the Deployment Guide for Panorama on Azure.
- Device configuration is centrally managed with Panorama by using templates and device groups.
- Firewall logging uses the Palo Alto Networks Cortex Data Lake.
- The tested PAN-OS version in this deployment guide is 8.1.11 for all devices.
- The on-premises firewalls for backhaul traffic are already deployed, and they have a set of interfaces connected to the public and private zones and integrated into the on-premises dynamic routing protocol.

Palo Alto Networks licensing:

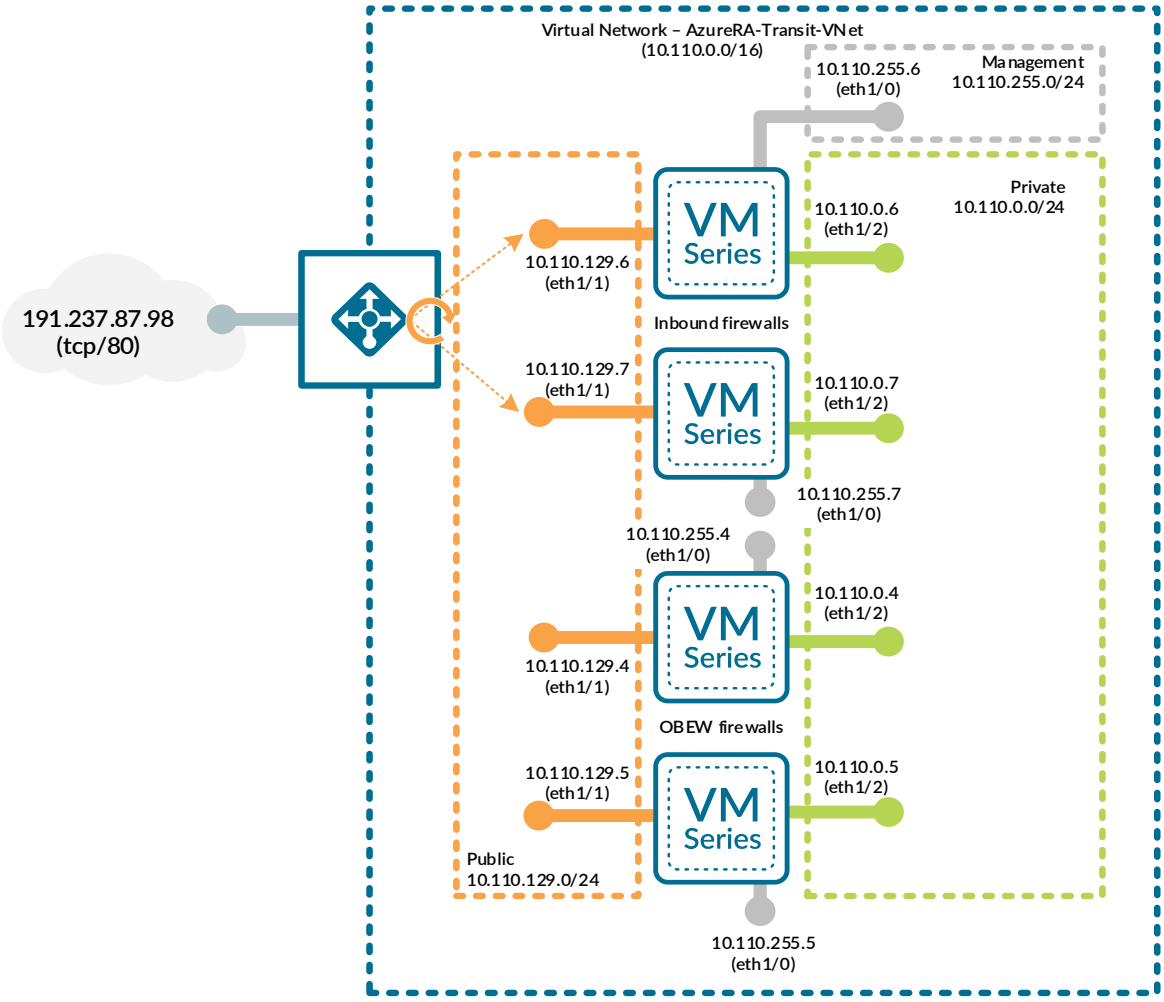
- Your organization has a Panorama license for the current and expected number of managed VM-Series firewalls.
- Sufficient VM-Series licensing for the current and expected number of VM-Series firewalls. This guide assumes you are using the BYOL licensing option.
- The Cortex Data Lake instance is provisioned with sufficient storage to support the required data retention period, and a Cortex Data Lake auth-code has been issued.
- The Cortex Data Lake instance used in this guide is hosted in the Americas region.

Deployment Details for VM-Series Firewalls

For the Transit VNet model, you deploy the VM-Series firewalls in a new dedicated Azure Resource Group and VNet. You configure a VNet peering connection between the transit VNet and the Panorama management VNet in order to enable centralized management. You must complete multiple complementary groups of procedures in order to deploy and configure the VM-Series firewalls.

The first section modifies and configures the Azure environment. After you configure Azure, the second section deploys the VM-Series firewalls and minimally configures each device to prepare for central management through Panorama.

Figure 6 Transit VNet model—VM-Series deployment parameters



The third section 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 after being pushed from Panorama to the VM-Series devices. After the templates are complete, the fourth section 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 Resources for VM-Series Firewalls

You use Azure Resource Manager (ARM) to complete these procedures. 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 network interface cards (NICs). To deploy the firewall into an existing resource group, use the ARM template in the GitHub Repository or your own custom ARM template.

Note

Some Azure templates provide an option to create a new resource when needed at deployment time, and other templates require that you create the resources in advance. Where possible, this guide uses the method of creating the resource in advance and then referencing the existing resource at deployment time.

Using these procedures, you create the resources listed in the following table as preparation for deploying Panorama.

Table 1 Azure resources required for deployment

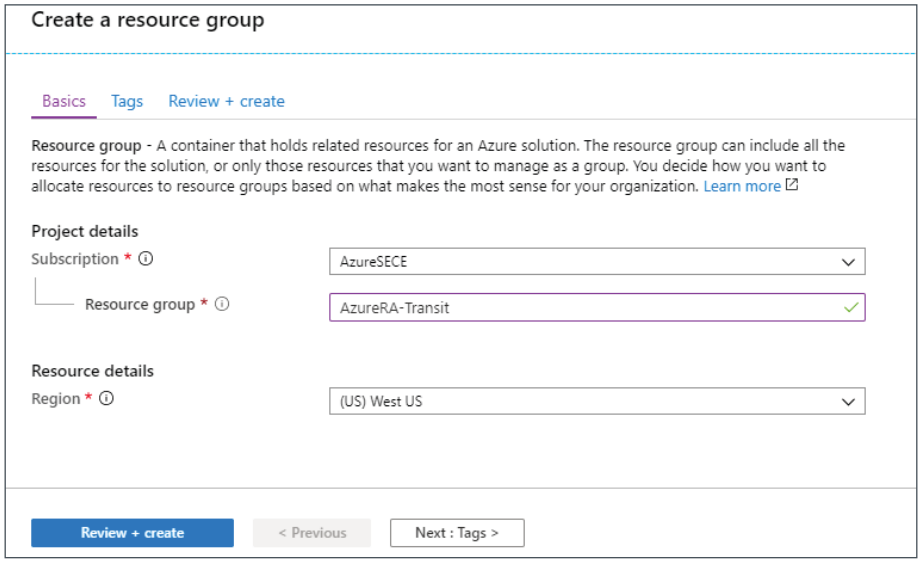
Parameter	Value	Comments
Resource group	AzureRA-Transit	—
Subscription	<value>	Must have a valid Azure subscription
Resource group region	<region>	Tested in West US
Network security groups	AllowManagement-Subnet AllowAll-Subnet	—
Virtual network	AzureRA-Transit-VNet	—
Storage account	azurerav2transit	General purpose storage for VM-Series virtual file systems
Availability set (OBEW)	ARA-Transit-OBEW-AS	Availability set for the VM-Series for the *outbound and east-west* (OBEW) firewall set
Availability set (Inbound)	ARA-Transit-Inbound-AS	Availability set for the VM-Series for the inbound firewall set
Public IP for VM-Series 1 (OBEW)	aratrv-vmfw1	Public IP for management interface
Public IP for VM-Series 2 (OBEW)	aratrv-vmfw2	Public IP for management interface
Public IP for VM-Series 3 (Inbound)	aratrv-vmfw3	Public IP for management interface
Public IP for VM-Series 4 (Inbound)	aratrv-vmfw4	Public IP for management interface

1.1 Create the Resource Group

You should use the same location for all resources you deploy by using this guide. Palo Alto Networks tested the deployment in this guide in **West US**.

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

Step 2: In the **Resource group** box, enter **AzureRA-Transit**, and then in the **Region** list, choose the desired value. Click **Review + create**.



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

1.2 Create the Network Security Group for the Management Subnet

Azure requires that you apply a network security group (NSG) on a subnet or NIC of your virtual machine resource. If you associate the resource with a standard-SKU public IP address and you do not apply this NSG, traffic is not permitted to reach the resource.

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

In this procedure, you create an NSG 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, choose **AzureRA-Transit**, and then click **Create**.

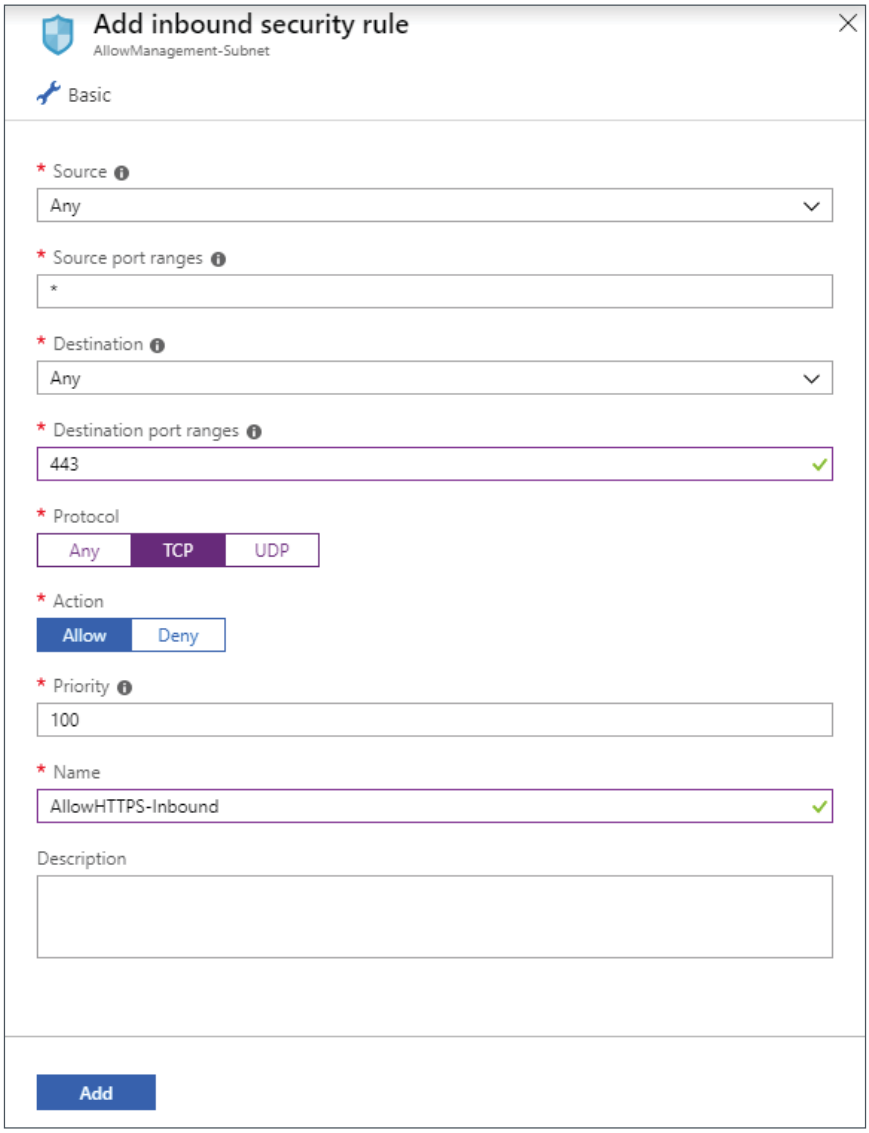
Step 4: In **Home > Network security groups > AllowManagement-Subnet**, in the Settings section, click **Inbound security rules**.

Step 5: Click **Add**. The Add inbound security rule pane appears.

Step 6: In the **Destination port ranges** box, enter **443**.

Step 7: In the Protocol section, select **TCP**.

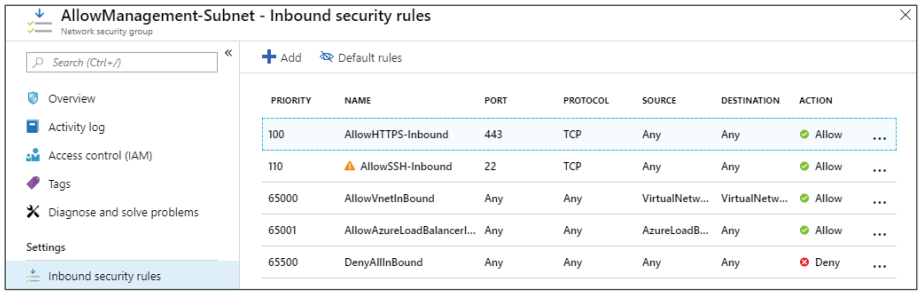
Step 8: In the **Name** box, enter **AllowHTTPS-Inbound**, and then click **Add**.



Step 9: Repeat Step 5 through Step 8 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. Palo Alto Networks advises using more restrictive rules outside of a testing environment.



1.3 Create the Whitelist Network Security Group

Azure requires that you apply a network security group (NSG) on a subnet or NIC of your virtual machine resource. If you associate the resource with a standard-SKU public IP address and you do not apply this NSG, traffic is not permitted to reach the resource.

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

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

> **Caution**
>
> A whitelist NSG permits access from the internet to devices with public IP addresses. Palo Alto Networks advises 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, choose **AzureRA-Transit**, and then click **Create**.

Step 4: In **Home > Network security groups > AllowAll-Subnet**, in the Settings section, click **Inbound security rules**.

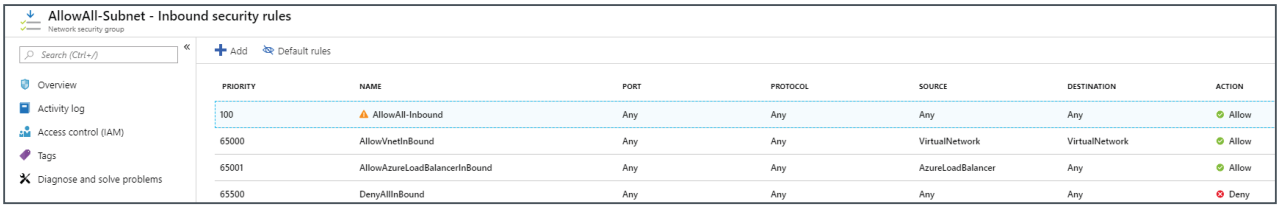
Step 5: Click **Add**. The Add inbound security rule pane appears.

Step 6: In the **Destination port ranges** box, enter *.

Step 7: In the **Priority** box, enter **100**.

Step 8: 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.



1.4 Create the Virtual Network

You create the VNet with an 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 spaces and subnets.

Table 2 Virtual network IP addressing and subnets

Address space	Subnet	IP address range	Create time
10.110.0.0/16	Transit-Management	10.110.255.0/24	Initial subnet
10.110.0.0/16	Transit-Private	10.110.0.0/24	Additional subnet
10.110.0.0/16	Transit-Public	10.110.129.0/24	Additional subnet

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

Step 2: In the **Name** box, enter **AzureRA-Transit-VNet**.

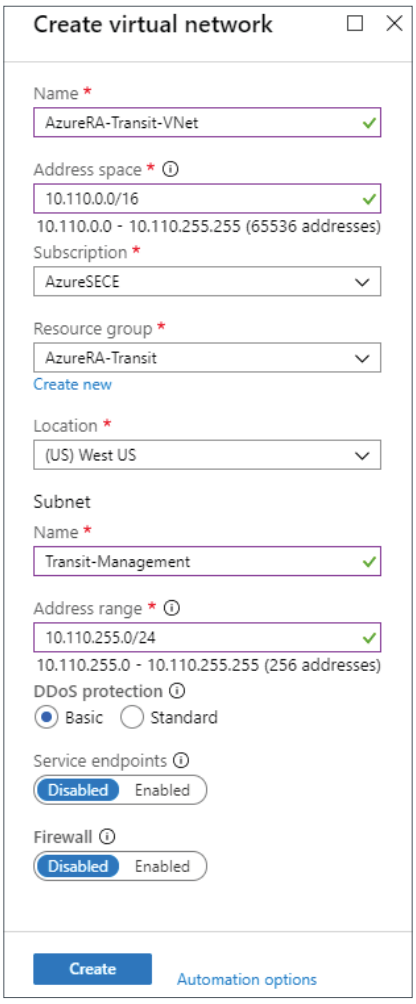
Step 3: In the **Address space** box, enter **10.110.0.0/16**.

> **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. You can ignore this warning if communication between these VNets is not required. Otherwise, choose a different, non-overlapping address space.

Step 4: In the Resource Group list, choose **AzureRA-Transit**.

Step 5: In the Subnet section **Name** box, enter **Transit-Management**.

Step 6: In the Subnet section **Address Range** box, enter **10.110.255.0/24**, and then click **Create**.

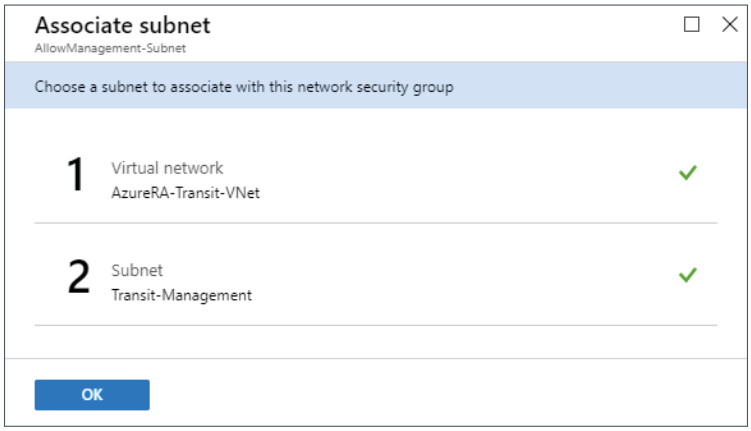


Step 7: In **Home** > **Network security groups** > **AllowManagement-Subnet**, in the Settings section, click **Subnets**.

Step 8: In the **AllowManagement-Subnet—Subnets** pane, click **Associate**.

Step 9: Click **Virtual network — Choose a virtual network**, and then in the **Choose virtual network** list, choose **AzureRA-Transit-VNet**.

Step 10: Click **Subnet — Choose a subnet**, and then in the **Choose subnet** list, choose **Transit-Management**. Click **OK**.



Step 11: In **Home > Virtual networks > AzureRA-Transit-VNet**, click **Subnets**.

Step 12: Click **Subnet**. This creates a new subnet.

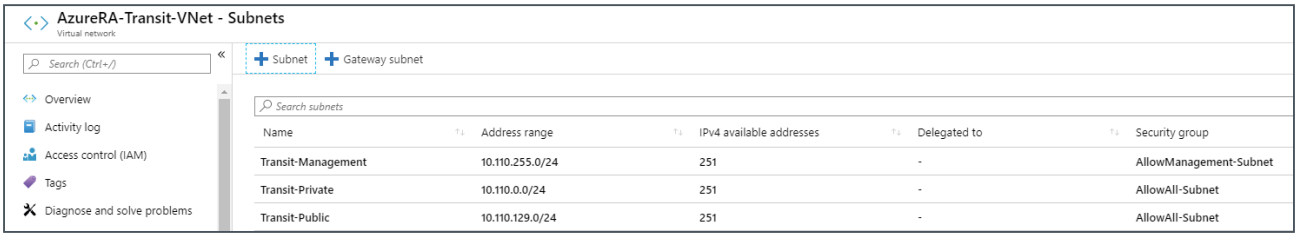
Step 13: In the **Name** box, enter **Transit-Private**.

Step 14: In the **Address Range (CIDR block)** box, enter **10.110.0.0/24**.

Step 15: In the **Network security group** list, choose **AllowAll-Subnet**, and then click **OK**.

Step 16: Repeat Step 11 through Step 15 for all remaining additional subnets in Table 2.

Step 17: Verify that you created all subnets with the correct IP address range and security group.



1.5 Create the Storage Account

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

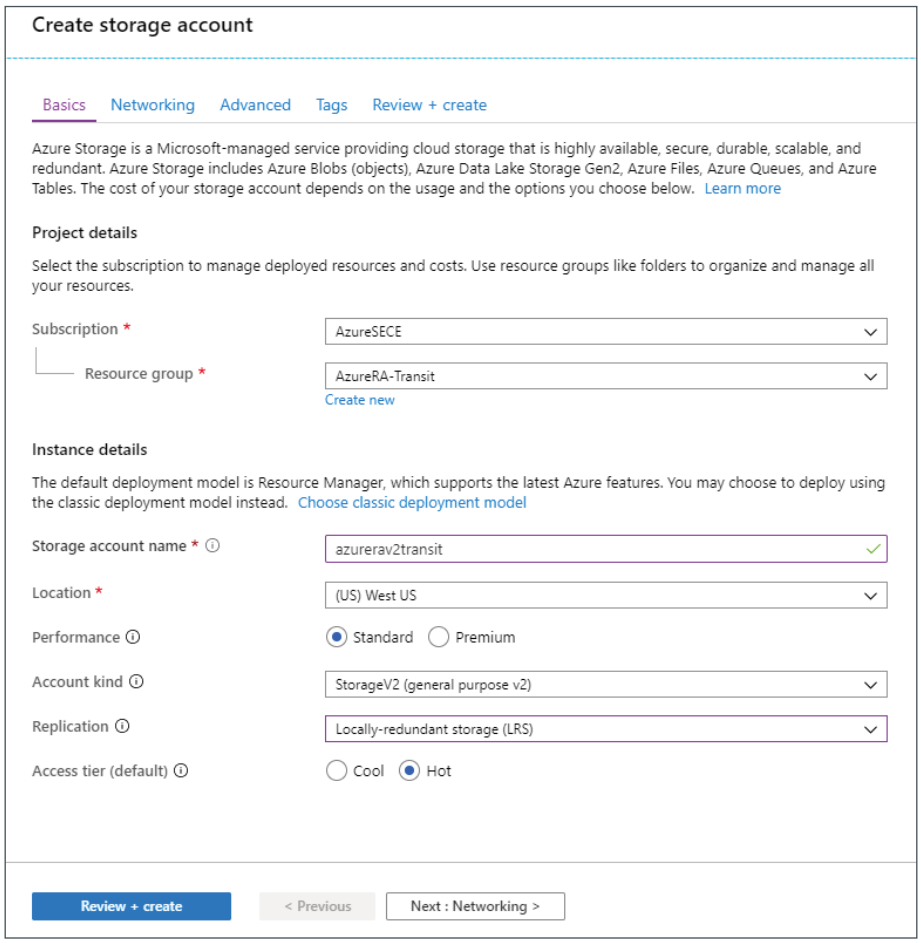
Step 1: In **Home > Storage accounts**, click **Add**.

Step 2: In the **Resource Group** list, choose **AzureRA-Transit**.

Step 3: In the **Storage account name** box, enter **azureav2transit**.

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

Step 5: In the **Replication** list, choose **Locally-redundant storage (LRS)**, and then click **Review + create**.



Step 6: On the next screen, after validation passes, click **Create**.

1.6 Create the Availability Sets

The VM-Series resiliency model for Azure benefits from the use of an availability set with two fault domains. This distributes the VM-Series systems across different fault domains. The Transit VNet design model uses two firewall sets, one for inbound and another for east-west, outbound, and backhaul traffic. To increase the resiliency of the design, each firewall set uses a dedicated Azure availability set.

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.

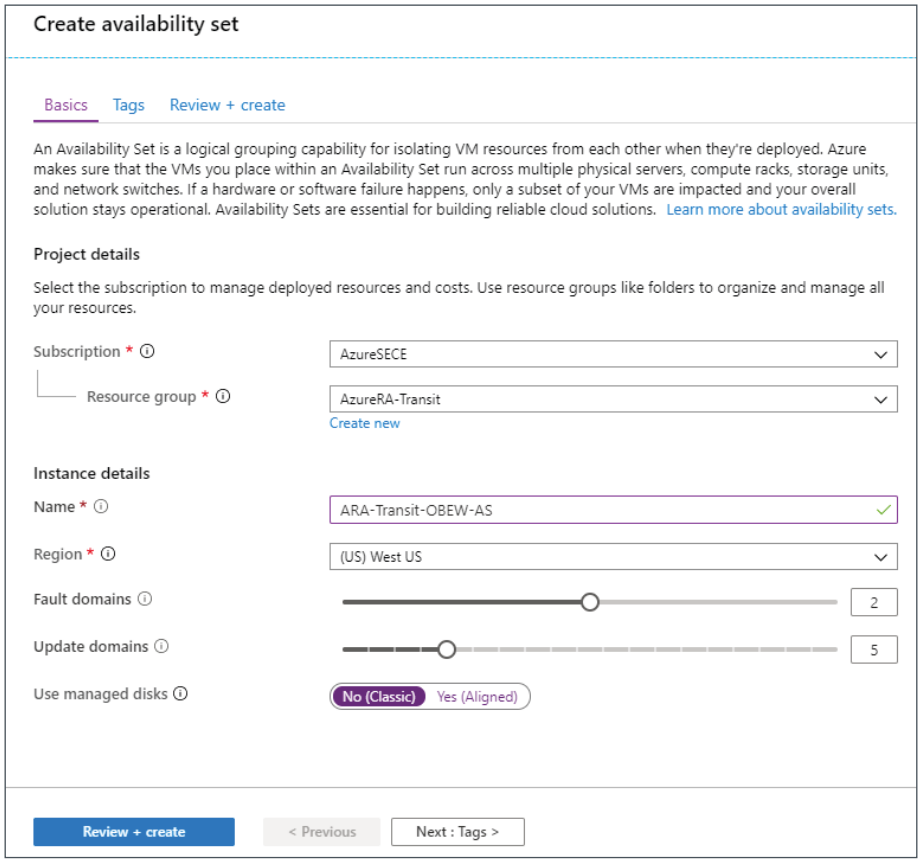
Step 1: In **Home > Availability sets**, click **Add**.

Step 2: In the **Resource Group** list, choose **AzureRA-Transit**.

Step 3: In the **Name** box, enter **ARA-Transit-OBEW-AS**.

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

Step 5: Click **Review + create**.



Step 6: On the next screen, after validation passes, click **Create**.

Step 7: Repeat this procedure to create a second availability set named **ARA-Transit-Inbound-AS**.

1.7 Create the Public IP Address for VM-Series Firewalls

Unless on-premises network connectivity has been established, you manage the VM-Series devices deployed on Azure by using public IP addresses. The process to configure on-premises network connectivity is included later in this guide.

In this procedure, you create a public IP address that is associated to the management interface of the VM-Series device at deployment time. If necessary, you repeat this procedure to create additional public IP addresses for additional VM-Series devices. Use the parameters listed in Table 1 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. Palo Alto Networks recommends managing your devices by using the DNS name rather than the public IP address, which might change.

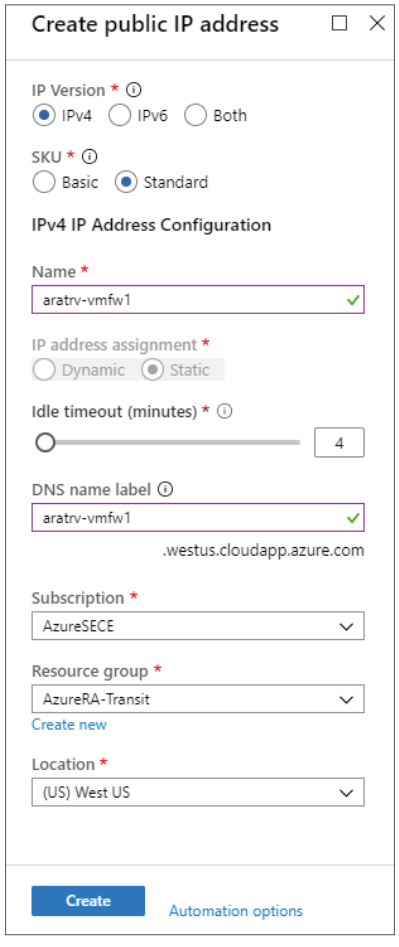
Step 1: In **Home > Public IP addresses**, click **Add**.

Step 2: In the SKU section, select **Standard**.

Step 3: In the **Name** box, enter **aratrv-vmfw1**.

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

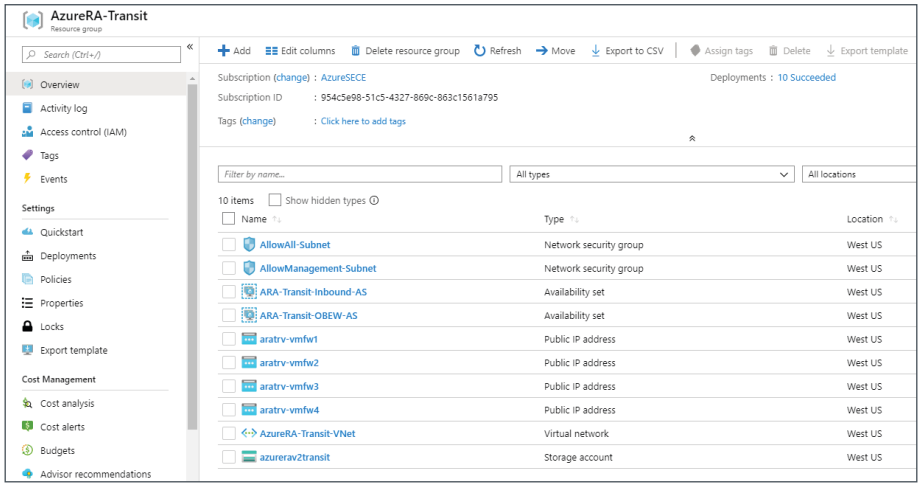
Step 5: In the **Resource Group** list, choose **AzureRA-Transit**, and then click **Create**.



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 it is to wait until a deployment fails.

Step 1: In **Home > Resource Groups**, select **AzureRA-Transit**.

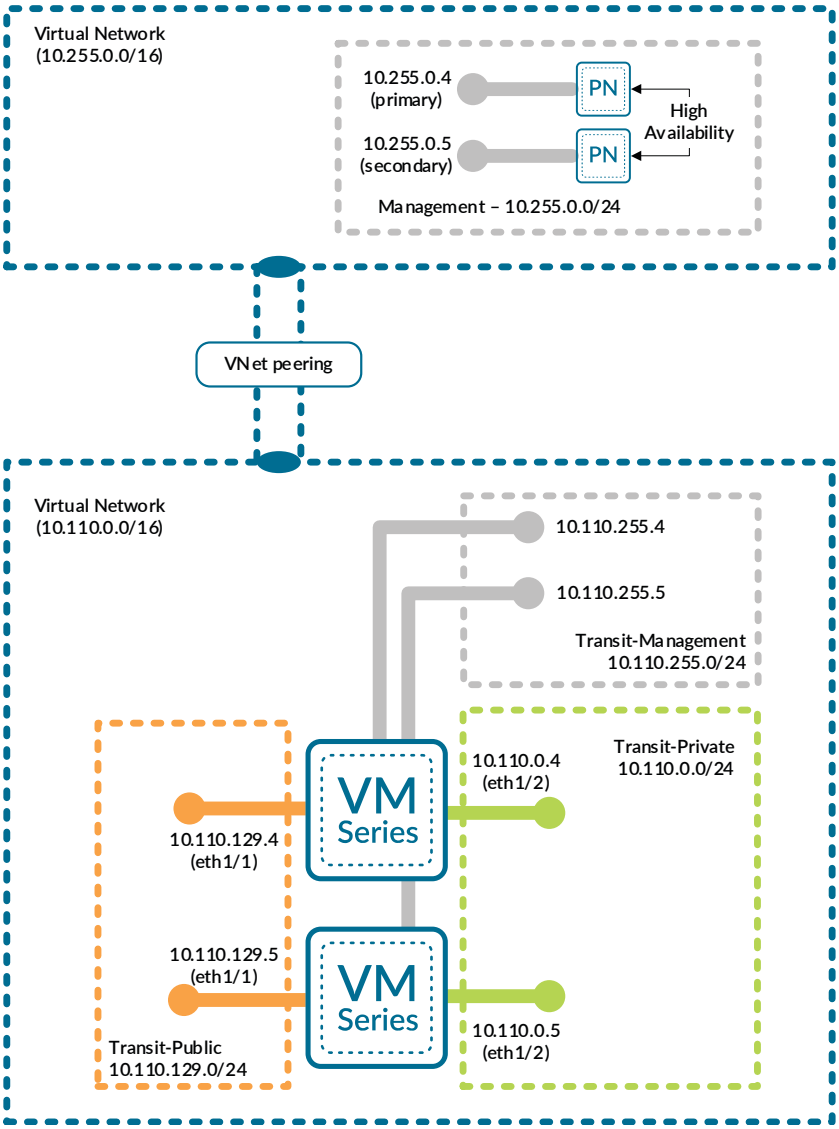


Step 2: Verify that you have successfully created the resource group, NSGs, VNet, public IP addresses, availability sets, and storage account.

1.9 Create Peering between Transit VNet and Panorama Management VNet

This guide assumes that Panorama has already been deployed in high-availability mode in a dedicated resource group and VNet. In order to manage devices deployed in the transit VNet, you must create a VNet peer connection between the transit VNet and the Panorama management VNet.

Figure 7 Peer connection to Panorama management VNet



You need to configure the peering relationship from only a single VNet. Azure then makes the necessary configuration updates on both VNet peers.

Note

In the Configure forwarded traffic settings section, do not enable traffic forwarding from the Panorama management VNet to the transit VNet. The Panorama management VNet does not include any devices configured for forwarding.

Enable traffic forwarding from the transit VNet to the Panorama management VNet. This model assumes that traffic from on-premises networks will access the Panorama management VNet through the transit VNet.

Panorama deployment details:

- Resource Group—**AzureRA**
- VNet—**AzureRA-VNet**

Step 1: In **Home > Virtual networks > AzureRA-Transit-VNet**, click **Peerings**, and then click **Add**.

Step 2: In the **Name of the peering from AzureRA-Transit-VNet to remote virtual network** box, enter **VNet-Peer_AzureRA-VNet**.

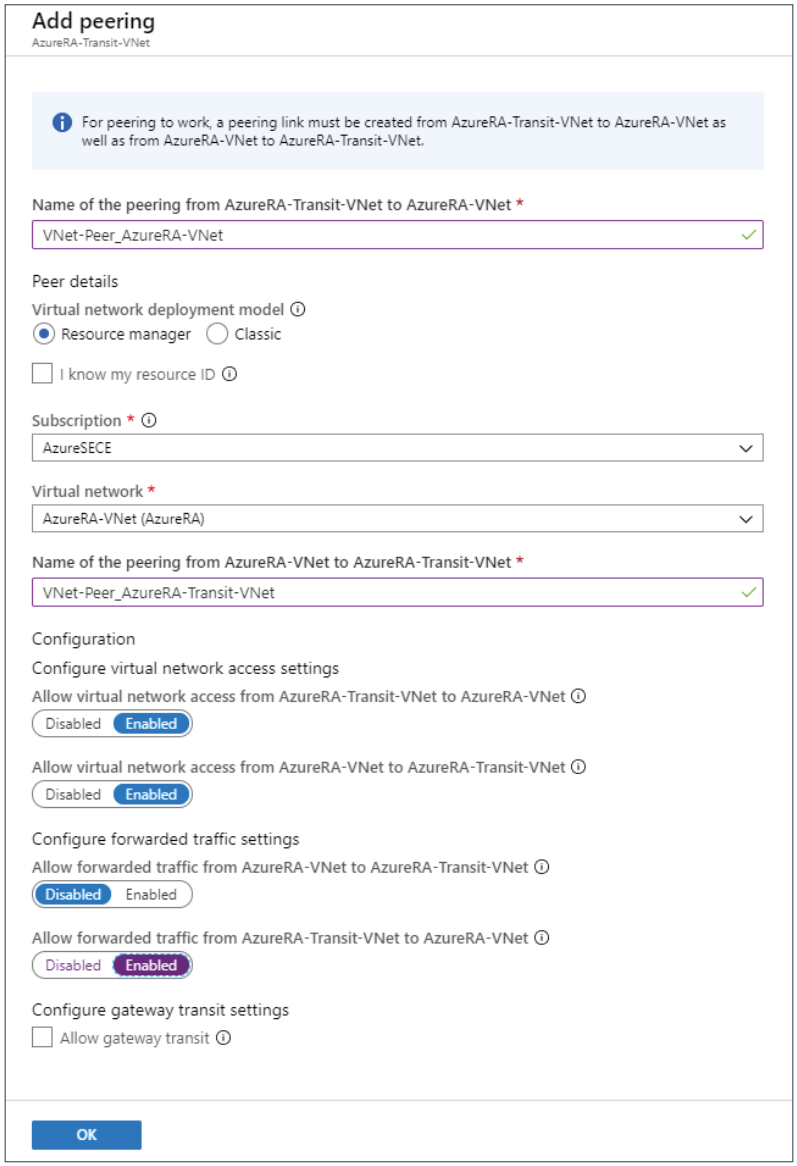
Step 3: In the **Virtual network** list, choose **AzureRA-VNET (AzureRA)**, and then click **OK**.

Step 4: In the **Name of the peering from AzureRA-VNet to AzureRA-Transit-VNet** box, enter **VNet-Peer_AzureRA-Transit-VNet**.

Step 5: For **Allow forwarded traffic from AzureRA-Transit-VNet to AzureRA-VNet**, select **Enabled**.

This setting allows the traffic forwarded from the transit VNet (traffic not originating from inside the peer virtual network) into the Panorama management VNet.

Step 6: Click **OK**.



Procedures

Deploying VM-Series Firewalls on Azure

2.1 Deploy VM-Series Firewall by Using a Custom ARM Template

2.2 License a VM-Series Firewall on Azure

2.3 Update the Device Software

To complete these procedures, you use the 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 3 VM-Series deployment parameters

Parameter	Value	Comments
Resource group	AzureRA-Transit	—
Location	—	Tested in West US
VM name	ARATRV-VMFW1 ARATRV-VMFW2 ARATRV-VMFW3 ARATRV-VMFW4	First device (OBEW) Second device (OBEW) Third device (inbound) Fourth device (inbound)
Storage account name	azurerav2transit	—
Storage account existing RG	AzureRA-Transit	—
Fw Av Set	ARA-Transit-OBEW-AS	Use for all OBEW firewalls
Fw Av Set	ARA-Transit-Inbound-AS	Use for all Inbound firewalls
VM size	Standard_D3_v2	For more information, see Minimum System Requirements for the VM-Series on Azure
Public IP type	standard	Standard-SKU IP addressing required for use with Azure Standard load balancer
Image version	8.1.0	—
Image SKU	byol	—
Virtual network name	AzureRA-Transit-VNet	—
Virtual network address prefix	10.110.0.0/16	Match the IP address space from AzureRA-Transit-VNet
Virtual network existing RG name	AzureRA-Transit	—
Subnet0Name	Transit-Management	—
Subnet1Name	Transit-Public	—
Subnet2Name	Transit-Private	—
Subnet0Prefix	10.110.255.0/24	—
Subnet1Prefix	10.110.129.0/24	—
Subnet2Prefix	10.110.0.0/24	—
Subnet0Start Address	10.110.255.4 10.110.255.5 10.110.255.6 10.110.255.7	First device (OBEW) Second device (OBEW) Third device (inbound) Fourth device (inbound) (start assignment from .4)

Table continued on next page

Continued from previous page

Parameter	Value	Comments
Subnet1Start Address	10.110.129.4 10.110.129.5 10.110.129.6 10.110.129.7	First device (OBEW) Second device (OBEW) Third device (inbound) Fourth device (inbound) (start assignment from .4)
Subnet2Start Address	10.110.0.4 10.110.0.5 10.110.0.6 10.110.0.7	First device (OBEW) Second device (OBEW) Third device (inbound) Fourth device (inbound) (start assignment from .4)
Admin username	refarchadmin	—
Admin password	<password>	—
Public IP address name	aratrv-vmfw1 aratrv-vmfw2 aratrv-vmfw3 aratrv-vmfw4	First device (OBEW) Second device (OBEW) Third device (inbound) Fourth device (inbound)
Nsg name	None	NSG is applied at the subnet level

2.1 Deploy VM-Series Firewall by Using a Custom ARM Template

Repeat this procedure for all VM-Series firewalls. This guide assumes that you have created at least two VM-Series devices for OBEW traffic and at least two VM-Series devices for inbound traffic.

The custom Azure Resource Manager template used in this procedure has been developed and validated specifically to support the Reference Architecture for Azure.

For template details and features, see:
https://github.com/PaloAltoNetworks/ReferenceArchitectures/tree/master/Azure-1FW-3-interfaces-existing-environment-BS

Use the parameters in Table 3 to deploy each VM-Series firewall.

Step 1: On the template, click **Deploy to Azure**. This deploys the VM-Series firewall.

Step 2: In the **Resource Group** list, choose **AzureRA-Transit**.

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

Step 4: In the **Storage Account Name** box, enter **azurerav2transit**.

Step 5: In the **Storage Account Existing RG** box, enter **AzureRA-Transit**.

Step 6: In the **Fw Av Set** box, enter **ARA-Transit-OBEW-AS**.

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

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

Step 9: In the **Image Version** list, choose **8.1.0**.

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

Step 11: In the **Bootstrap Firewall** list, choose **no**.

Step 12: In the **Virtual Network Name** box, enter **AzureRA-Transit-VNet**.

Step 13: In the **Virtual Network Address Prefix** box, enter **10.110.0.0/16**.

Step 14: In the **Virtual Network Existing RG Name** box, enter **AzureRA-Transit**.

Step 15: In the **Subnet0Name** box, enter **Transit-Management**.

Step 16: In the **Subnet1Name** box, enter **Transit-Public**.

Step 17: In the **Subnet2Name** box, enter **Transit-Private**.

Step 18: In the **Subnet0Prefix** box, enter **10.110.255.0/24**.

Step 19: In the **Subnet1Prefix** box, enter **10.110.129.0/24**.

Step 20: In the **Subnet2Prefix** box, enter **10.110.0.0/24**.

Step 21: In the **Subnet0Start Address** box, enter **10.110.255.4**.

Step 22: In the **Subnet1Start Address** box, enter **10.110.129.4**.

Step 23: In the **Subnet2Start Address** box, enter **10.110.0.4**.

Step 24: In the **Admin Username** box, enter **refarchadmin**.

Step 25: In the **Admin Password** box, enter the password.

Step 26: In the **Public IP Address Name** box, enter **aratrv-vmfw1**.

Step 27: In the **Nsg Name** box, enter **None**.

Step 28: Review the terms and conditions. If they are acceptable, select **I agree to the terms and conditions**, and then click **Purchase**.

Step 29: Repeat this procedure for all VM-Series firewalls.

2.2 License a VM-Series Firewall on Azure

Your VM-Series firewall 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 devices 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://aratrv-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 (example: **example.com**).

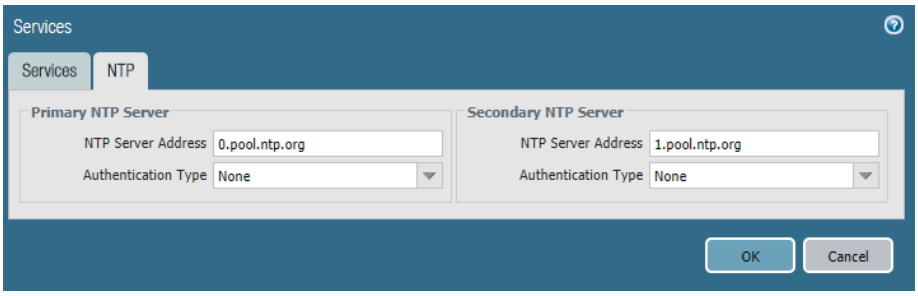
Step 4: In the **Time Zone** list, choose the appropriate time zone (example: **US/Pacific**), and then click **OK**.

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, in the **NTP Server Address** box, enter **0.pool.ntp.org**.

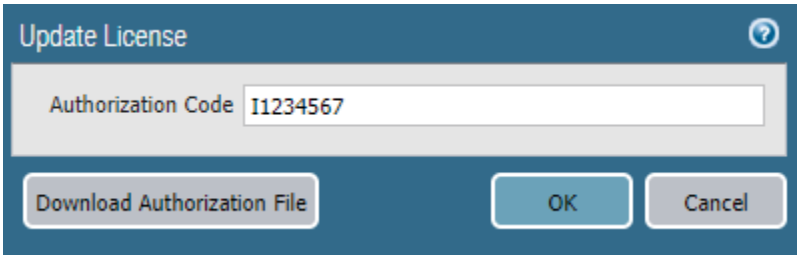
Step 8: In the Secondary NTP Server section, in the **NTP Server Address** box, enter **1.pool.ntp.org**, and then click **OK**.



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: On the warning about restarting PAN services, click **OK**.

> **Note**
>
> The VM-Series services restart after the license is installed. After the restart, you must refresh your management session to the VM-Series firewall. This takes a few minutes.

Step 13: Repeat this procedure for all VM-Series firewalls.

2.3 Update the Device Software

Step 1: Navigate to **Device > Software**, and then click **Check Now**.

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

Step 2: For version **8.1.11**, in the **Action** column, click **Download**.

Step 3: 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 schedules automatic downloads of the Applications and Threats packages.

Step 7: Repeat this procedure for all VM-Series firewalls.

Procedures

Preparing VM-Series Firewall Configurations Using Panorama

Panorama provides the following tools for centralized administration:

- **Hierarchical device groups**—Panorama manages common policies and objects through hierarchical device groups. You can use multi-level device groups in order to centrally manage the policies across all deployment locations with common requirements
- **Templates and 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 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.

The following procedures assume that you have already deployed Panorama in a peered VNet following the procedures in *Deployment Guide for Panorama on Azure*. In that guide, you created an example device group and templates on Panorama. This guide repeats those procedures for continuity.

- **Device group**—VMFW-LogForwarding
- **Template**—VMFW-Baseline

3.1 Create the Panorama Device Groups

This guide uses three device groups. The first device group is the parent device group and includes the log-forwarding object required for log forwarding to Cortex Data Lake. The other two device groups are each specific to a traffic profile in the Transit VNet design model. The Transit-VNet-OBEW device group includes objects and policies for the outbound, backhaul, and east-west firewalls. The Transit-VNet-Inbound device group includes objects and policies for the inbound firewalls.

You will first create the device groups. You must specify the parent device group to properly inherit device group settings from other Panorama device groups. You create the objects and policies in the procedures that require them.

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

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

Step 3: In the **Name** box, enter **Transit-VNet**.

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**.

Step 6: In **Panorama > Device Groups**, click **Add**.

Step 7: In the **Name** box, enter **Transit-VNet-OBEW**.

Step 8: In the **Description** box, enter a valid description.

Step 9: In the **Parent Device Group** list, choose **Transit-VNet**, and then click **OK**.

Step 10: In **Panorama > Device Groups**, click **Add**.

Step 11: In the **Name** box, enter **Transit-VNet-Inbound**.

Step 12: In the **Description** box, enter a valid description.

Step 13: In the **Parent Device Group** list, choose **Transit-VNet**, and then click **OK**.

Name	Description
Shared	
Transit-VNet	Parent device group (includes log forwarding profile for Cortex Data Lake)
Transit-VNet-Inbound	Child device group (includes objects and policies for inbound firewalls)
Transit-VNet-OBEW	Child device group (includes objects and policies for outbound, east-west and backhaul firewalls)

3.2 Configure the Parent Device Group

All child device groups inherit their configuration from this device group. Initially, you create the log-forwarding profile to send security policy logs to Cortex Data Lake (formerly *Logging Service*). This profile is associated to any security policy rules that you create that use Cortex Data Lake. Later in this guide, you add other common objects and policies to this device group.

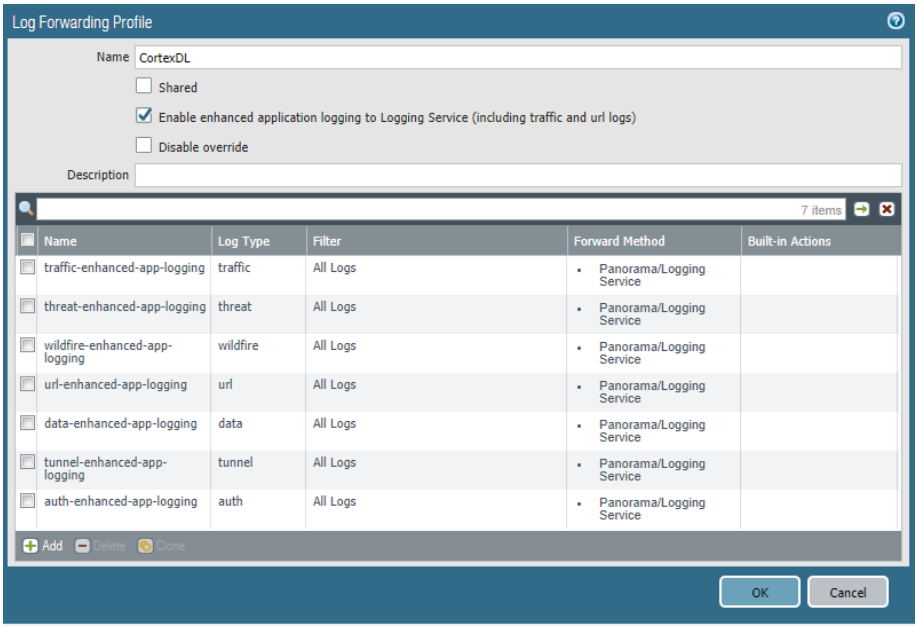
Step 1: In Panorama, navigate to the **Objects** tab.

Step 2: In the **Device Group** list, choose **Transit-VNet**.

Step 3: In **Objects > Log Forwarding**, click **Add**.

Step 4: In the **Name** box, enter **CortexDL**.

Step 5: Select **Enable enhanced application logging to Logging Service (including traffic and url logs),** and then click **OK**.



3.3 Create the Panorama Templates

The templates include configuration for all functions that are common across all the VM-Series devices in the Transit VNet design model.

You create the following Panorama templates in this procedure:

- **VMFW-Baseline**—Includes basic networking services including DNS and NTP and also includes device functions that enable the log forwarding to Cortex Data Lake.
- **Transit-2-Zone-OBEW**—Includes firewall networking functions for the outbound, backhaul, and east-west firewalls, including interfaces, zones, and the virtual router.
- **Transit-2-Zone-Inbound**—Includes firewall networking functions for the inbound firewalls, including interfaces, zones, and the virtual router.

You apply templates to devices by using Panorama template stacks, which logically merges the assigned templates and associates them with the relevant devices.

You create the specific configurations for the templates within the relevant procedures. You create the template stack later in this guide, when associating the first device to the templates.

Step 1: In Panorama, navigate to **Panorama > Templates**, and then click **Add**.

Step 2: In the **Name** box, enter **VMFW-Baseline**.

Step 3: In the **Description** box, enter a valid description, and then click **OK**.

Step 4: In **Panorama > Templates**, click **Add**.

Step 5: In the **Name** box, enter **Transit-2-Zone-OBEW**.

Step 6: In the **Description** box, enter a valid description, and then click **OK**.

Step 7: In the **Name** box, enter **Transit-2-Zone-Inbound**.

Step 8: In the **Description** box, enter a valid description, and then click **OK**.

Name	Description	Type
VMFW-Baseline	Baseline parameters for all VM-Series firewalls	template
Transit-2-Zone-OBEW	Interface, zone and virtual router configuration for OBEW firewalls	template
Transit-2-Zone-Inbound	Interface, zone and virtual router configuration for Inbound firewalls	template

3.4 Configure the Baseline Device Parameters

Performing this procedure configures DNS and NTP consistently across all devices and ensures all devices forward logs to the Cortex Data Lake (formerly *Logging Service*).

Step 1: In Panorama, navigate to the **Device** tab.

Step 2: In the **Template** list, choose **VMFW-Baseline**.

Step 3: In **Device > Setup > Services > Global > Services**, click the edit cog.

Step 4: In the **Primary DNS Server** box, enter **168.63.129.16**.

Step 5: On the NTP tab, in the Primary NTP Server section, in the **NTP Server Address** box, enter **0.pool.ntp.org**.

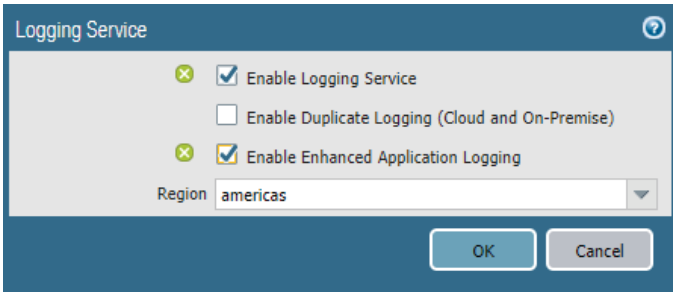
Step 6: In the Secondary NTP Server section, in the **NTP Server Address** box, enter **1.pool.ntp.org**, and then click **OK**.

Step 7: In **Device > Setup > Management > Logging Service**, click the edit cog.

Step 8: Select **Enable Logging Service**.

Step 9: Select **Enable Enhanced Application Logging**.

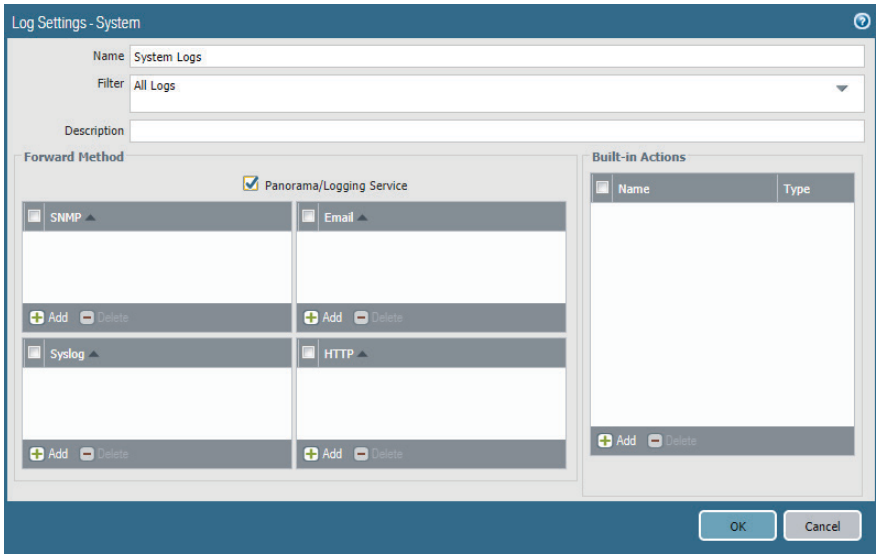
Step 10: In **Region** list, choose **americas**, and then click **OK**.



Step 11: In **Device > Log Settings > System**, click **Add**. The Log Settings—System window appears.

Step 12: In the **Name** box, enter **System Logs**.

Step 13: Select **Panorama/Logging Service**, and then click **OK**.



Step 14: In **Device** > **Log Settings** > **Configuration**, click **Add**. The Log Settings—Configuration window appears.

Step 15: In the **Name** box, enter **Configuration Logs**.

Step 16: Select **Panorama/Logging Service**, and then click **OK**.

3.5 Create Zones and Virtual Router for the OBEW Firewalls

Table 4 Zone and virtual router settings

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

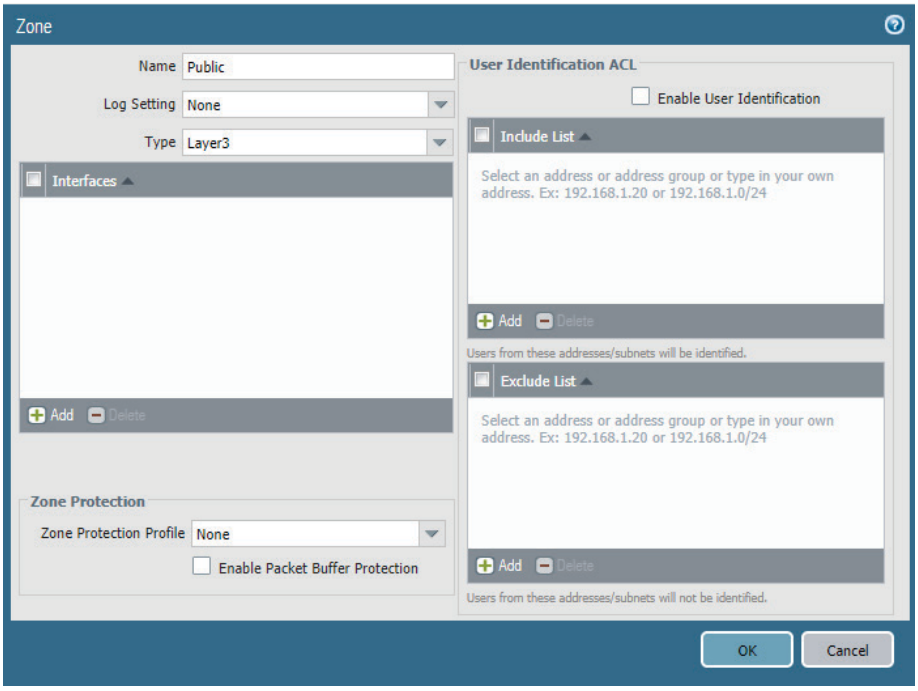
Step 1: In Panorama, navigate to the **Network** tab.

Step 2: In the **Template** list, choose **Transit-2-Zone-OBEW**.

Step 3: In **Network** > **Zones**, click **Add**. The Zone window appears.

Step 4: In the **Name** box, enter **Public**.

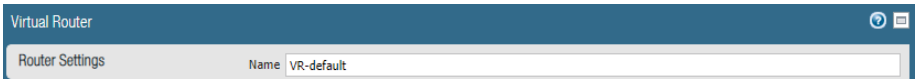
Step 5: In the **Type** list, choose **Layer3**, and then click **OK**.



Step 6: Repeat Step 3 through Step 5 for all rows in Table 4.

Step 7: In **Network > Virtual Routers**, click **Add**. The Virtual Router window appears.

Step 8: In the **Name** box, enter **VR-default**, and then click **OK**.



3.6 Create the Management Profile for the OBEW Firewalls

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

> **Note**
>
> You can apply a single management profile to multiple interfaces. Palo Alto Networks recommends separate management profiles per interface, if required, to allow for different management policies.

Step 1: In Panorama, navigate to the **Network** tab.

Step 2: In the **Template** list, choose **Transit-2-Zone-OBEW**.

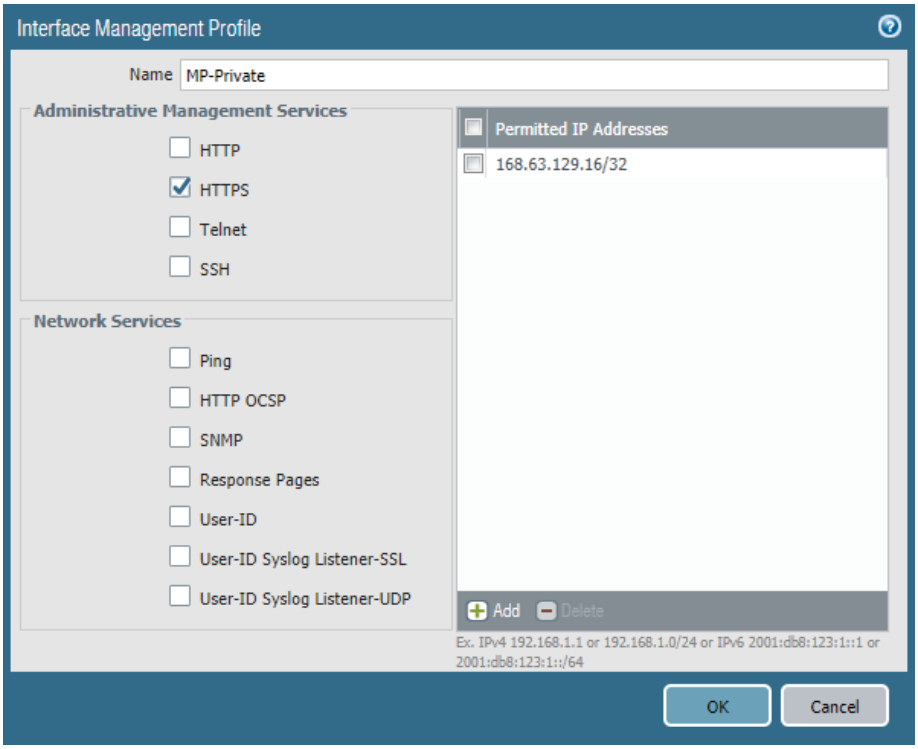
Step 3: In **Network > Network Profiles > Interface Mgmt,** click **Add**. The Interface Management Profile window appears.

Step 4: In the **Name** box, enter **MP-Private**.

Step 5: In the Administrative Management Services section, select **HTTPS**.

Step 6: In the Permitted IP Addresses pane, click **Add**.

Step 7: Enter **168.63.129.16/32**, and then click **OK**.



3.7 Create Ethernet Interfaces for the OBEW Firewalls

Note

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

Table 5 Template interface settings for Transit-2-Zone-OBEW

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

Step 1: In Panorama, navigate to the **Network** tab.

Step 2: In the **Template** list, choose **Transit-2-Zone-OBEW**.

Step 3: In **Network > Interfaces > Ethernet,** click **Add Interface**. The Ethernet Interface window appears.

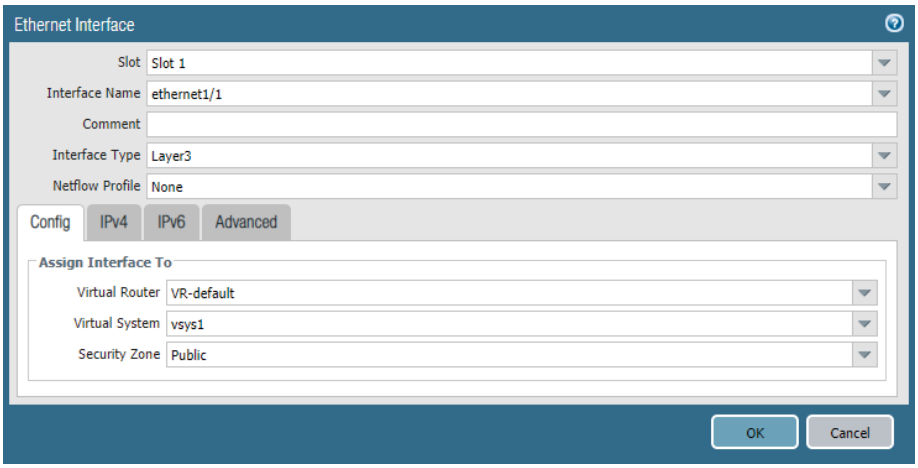
Step 4: In the **Slot** list, choose **Slot 1**.

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

Step 6: In the **Interface Type** list, choose **Layer3**.

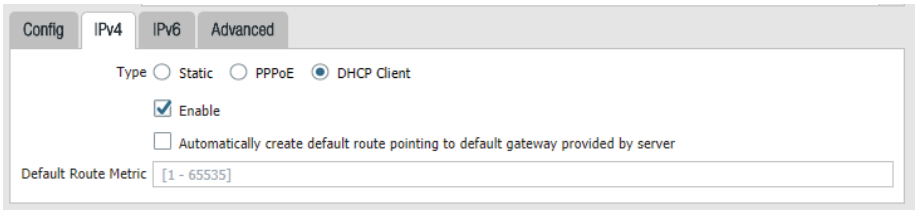
Step 7: In the **Assign Interface To Virtual Router** list, choose **VR-default**.

Step 8: In the **Assign Interface To Security Zone** list, choose **Public**.



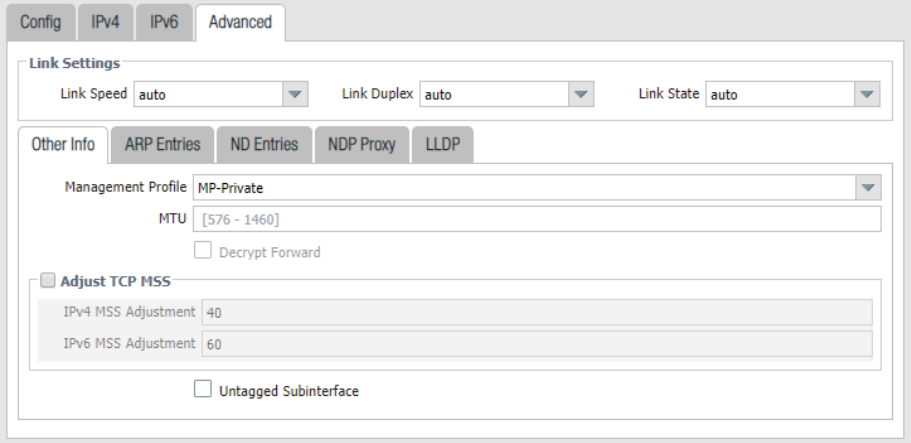
Step 9: On the IPv4 tab, select **DHCP client**.

Step 10: Select **Enable** and clear **Automatically create default route pointing to default gateway provided by server**.



Step 11: Click the **Advanced** tab.

Step 12: If a management profile is listed in Table 5, in the **Management Profile** list, choose **MP-Private**, and then click **OK**.



Step 13: On the warning, click **Yes** to accept and continue.

Step 14: Repeat Step 3 through Step 13 for all rows in Table 5.

Interface	Interface Type	Management Profile	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Virtual System	Security Zone
Slot 1								
ethernet1/1	Layer3		Dynamic-DHCP Client	VR-default	Untagged	none	vsys1	Public
ethernet1/2	Layer3	MP-Private	Dynamic-DHCP Client	VR-default	Untagged	none	vsys1	Private

3.8 Add Static Routes to the Virtual Router for the OBEW Firewalls

The virtual router requires static route configuration. Use the values in Table 6.

Note

The route table include prefixes that are associated with the on-premises network and subscriber VNets. These prefixes are not reachable until you create connections and enable security policies according to procedures later in this guide.

Table 6 VR-default IPv4 static routes for OBEW firewalls

Name	Destination prefix	Interface	Next-hop	Next-hop value
default	0.0.0.0/0	ethernet1/1	IP Address	10.110.129.1
Net-10.110.128.0_23	10.110.128.0/23	ethernet1/1	IP Address	10.110.129.1
Azure-Probe	168.63.129.16/32	ethernet1/2	IP Address	10.110.0.1
Net-10.110.0.0_17	10.110.0.0/17	ethernet1/2	IP Address	10.110.0.1
Net-10.112.0.0_16	10.112.0.0/16	ethernet1/2	IP Address	10.110.0.1
Net-10.113.0.0_16	10.113.0.0/16	ethernet1/2	IP Address	10.110.0.1
Net-10.6.0.0_16	10.6.0.0/16	ethernet1/2	IP Address	10.110.0.1

Step 1: In Panorama, navigate to the **Network** tab.

Step 2: In the **Template** list, choose **Transit-2-Zone-OBEW**.

Step 3: In **Network > Virtual Routers**, click **VR-default**. The Virtual Router window appears.

Step 4: On the Static Routes tab, click **Add**. The Virtual Router —Static Route—IPv4 window appears.

Step 5: In the **Name** box, enter **default**.

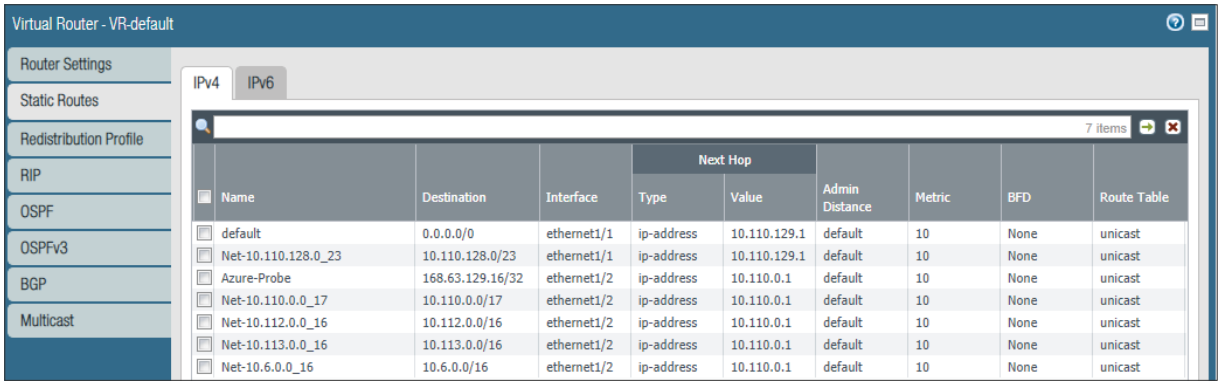
Step 6: In the **Destination** box, enter **0.0.0.0/0**.

Step 7: In the **Interface** list, choose **ethernet1/1**.

Step 8: In the **Next Hop** list, choose **IP Address**, enter **10.110.129.1**, and then click **OK**.

Step 9: Repeat Step 4 through Step 8 for the remaining routes in Table 6.

Step 10: After adding all routes for the virtual router, on the Virtual Router window, click **OK**.



3.9 Create Zones and Virtual Router for the Inbound Firewalls

Table 7 Zone and virtual router settings

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

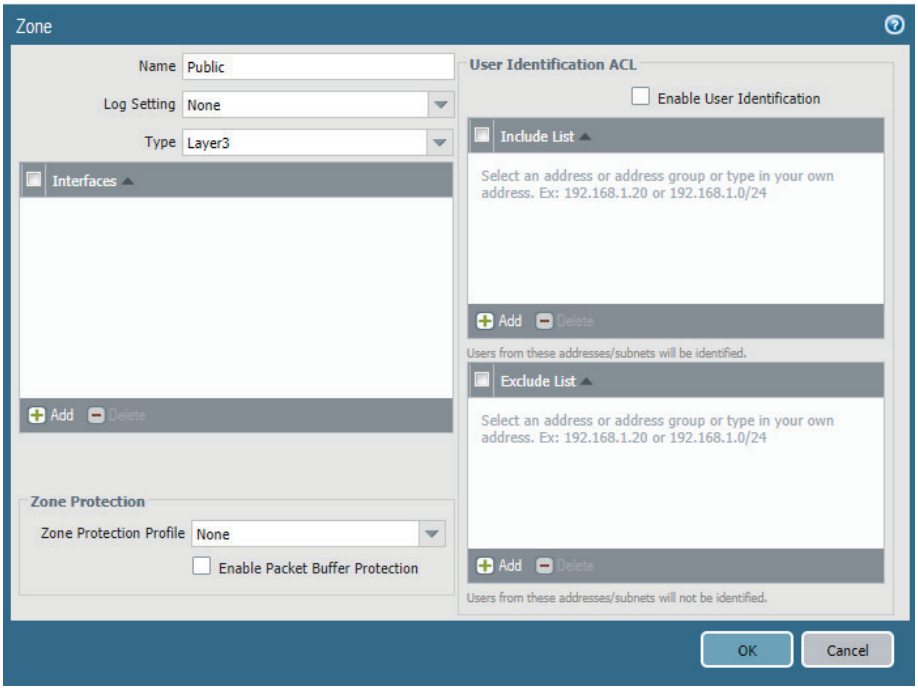
Step 1: In Panorama, navigate to the **Network** tab.

Step 2: In the **Template** list, choose **Transit-2-Zone-Inbound**.

Step 3: In **Network > Zones**, click **Add**. The Zone window appears.

Step 4: In the **Name** box, enter **Public**.

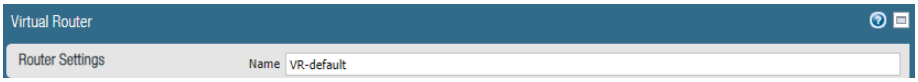
Step 5: In the **Type** list, choose **Layer3**, and then click **OK**.



Step 6: Repeat Step 3 through Step 5 for all rows in Table 7.

Step 7: In **Network > Virtual Routers**, click **Add**. The Virtual Router window appears.

Step 8: In the **Name** box, enter **VR-default**, and then click **OK**.



3.10 Create the Management Profile for the Inbound Firewalls

The load-balancer health-checks use SSH probes towards the firewall's dataplane interfaces. The firewall blocks responses to these probes by default. You use interface management profiles to override the default block operation.

> **Note**
>
> You can apply a single management profile to multiple interfaces. Palo Alto Networks recommends 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, skip to the next procedure.

Step 1: In Panorama, navigate to the **Network** tab.

Step 2: In the **Template** list, choose **Transit-2-Zone-Inbound**.

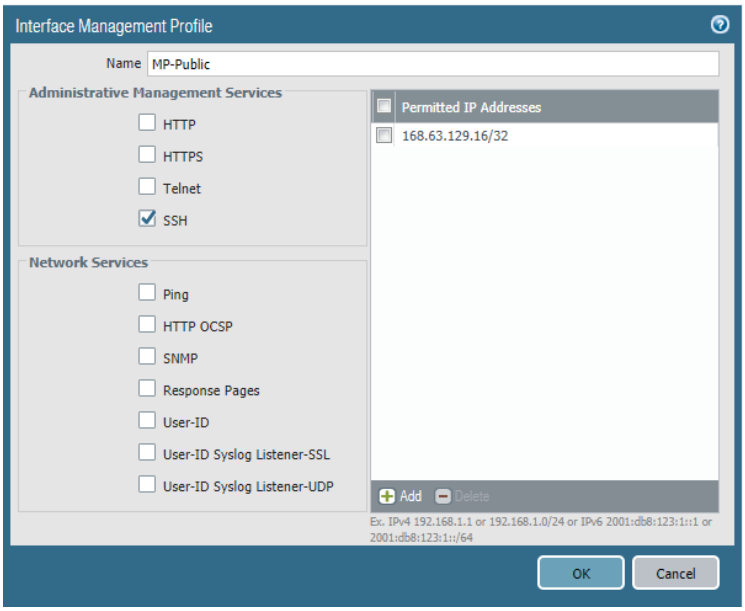
Step 3: In **Network > Network Profiles > Interface Mgmt,** click **Add**. The Interface Management Profile window appears.

Step 4: In the **Name** box, enter **MP-Public**.

Step 5: In the Administrative Management Services section, select **SSH**. If you intend on using the application gateway for inbound access, Palo Alto Networks suggests you use SSH instead of HTTPS for Azure load-balancer health probes.

Step 6: In the Permitted IP Addresses pane, click **Add**.

Step 7: Enter **168.63.129.16/32**, and then click **OK**.



3.11 Create Ethernet Interfaces for the Inbound Firewalls

Note

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

Table 8 Template interface settings for Transit-2-Zone-Inbound

Slot	Interface	Interface type	Virtual router	Security zone	IPv4	Management profile
Slot 1	ethernet1/1	Layer3	VR-default	Public	DHCP Client	MP-Public (not required if using application gateway)
Slot 1	ethernet1/2	Layer3	VR-default	Private	DHCP Client	—

Step 1: In Panorama, navigate to the **Network** tab.

Step 2: In the **Template** list, choose **Transit-2-Zone-Inbound**.

Step 3: In **Network > Interfaces > Ethernet,** click **Add Interface**. The Ethernet Interface window appears.

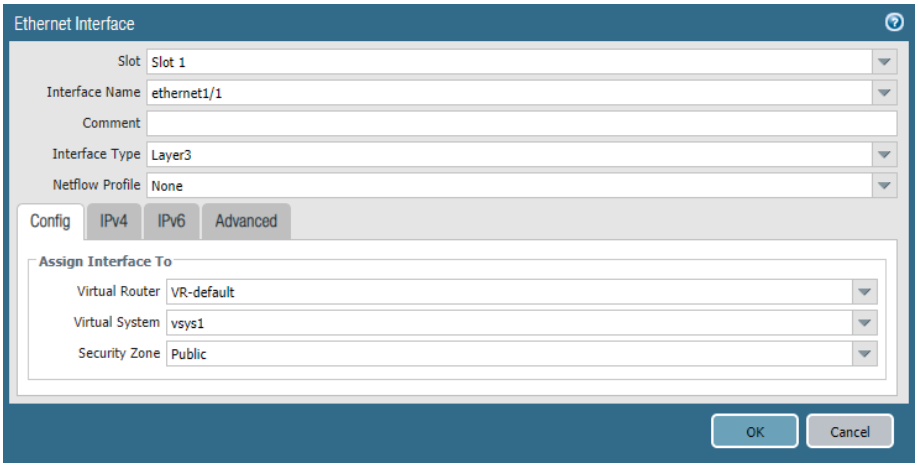
Step 4: In the **Slot** list, choose **Slot 1**.

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

Step 6: In the **Interface Type** list, choose **Layer3**.

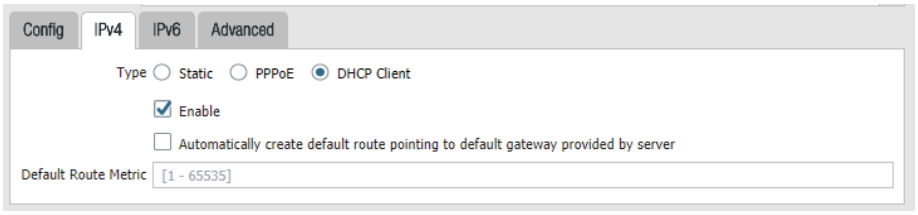
Step 7: In the **Assign Interface To Virtual Router** list, choose **VR-default**.

Step 8: In the **Assign Interface To Security Zone** list, choose **Public**.



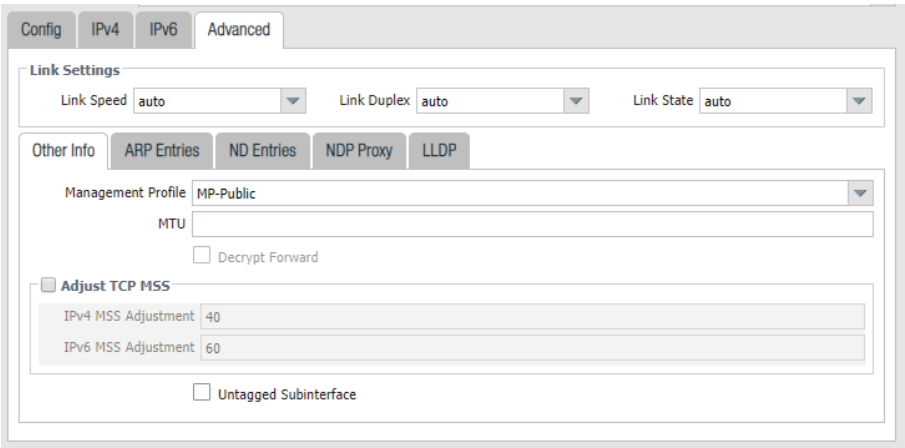
Step 9: On the IPv4 tab, select **DHCP client**.

Step 10: Select **Enable** and clear **Automatically create default route pointing to default gateway provided by server**.



Step 11: Click the **Advanced** tab.

Step 12: If a management profile is listed in Table 8 and is required, in the **Management Profile** list, choose **MP-Public**, and then click **OK**.



Step 13: On the warning, click **Yes** to accept and continue.

Step 14: Repeat Step 3 through Step 13 for all rows in Table 8.

Interface	Interface Type	Management Profile	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Virtual System	Security Zone
Slot 1								
ethernet1/1	Layer3	MP-Public	Dynamic-DHCP Client	VR-default	Untagged	none	vsys1	Public
ethernet1/2	Layer3		Dynamic-DHCP Client	VR-default	Untagged	none	vsys1	Private

3.12 Add Static Routes to the Virtual Router for the Inbound Firewalls

The virtual router requires static route configuration. Use the values in Table 9.

Note

The route table include prefixes that are associated with the on-premises network and subscriber VNets. These prefixes are not reachable until you create connections and enable security policies according to procedures later in this guide.

Table 9 VR-default IPv4 static routes for inbound firewalls

Name	Destination prefix	Interface	Next-hop	Next-hop value
default	0.0.0.0/0	ethernet1/1	IP Address	10.110.129.1
Azure-Probe	168.63.129.16/32	ethernet1/1	IP Address	10.110.129.1
Net-10.110.128.0_23	10.110.128.0/23	ethernet1/1	IP Address	10.110.129.1
Net-10.110.0.0_17	10.110.0.0/17	ethernet1/2	IP Address	10.110.0.1
Net-10.112.0.0_16	10.112.0.0/16	ethernet1/2	IP Address	10.110.0.1
Net-10.113.0.0_16	10.113.0.0/16	ethernet1/2	IP Address	10.110.0.1

Step 1: In Panorama, navigate to the **Network** tab.

Step 2: In the **Template** list, choose **Transit-2-Zone-Inbound**.

Step 3: In **Network > Virtual Routers**, click **VR-default**. The Virtual Router window appears.

Step 4: On the Static Routes tab, click **Add**. The Virtual Router —Static Route—IPv4 window appears.

Step 5: In the **Name** box, enter **default**.

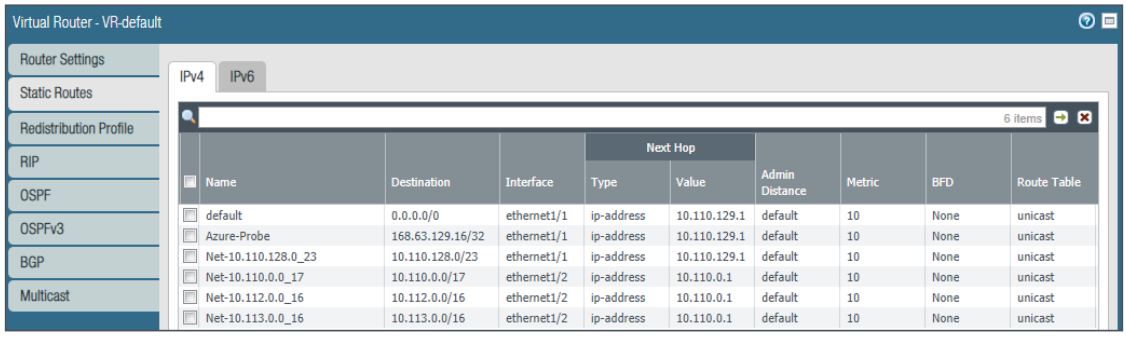
Step 6: In the **Destination** box, enter **0.0.0.0/0**.

Step 7: In the **Interface** list, choose **ethernet1/1**.

Step 8: In the **Next Hop** list, choose **IP Address**, enter **10.110.129.1**, and then click **OK**.

Step 9: Repeat Step 4 through Step 8 for the remaining routes in Table 9.

Step 10: After adding all routes for the virtual router, on the Virtual Router window, click **OK**.



3.13 Commit the Changes

Now you commit all of the configuration changes for Procedure 3.1 through Procedure 3.12.

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

Procedures

Managing VM-Series Firewalls with Panorama

4.1 Add a VM-Series Device to Panorama

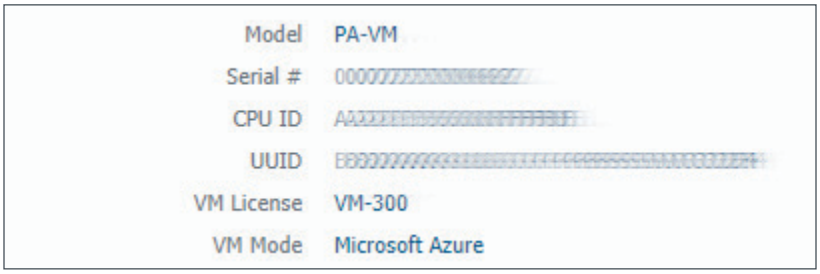
This procedure is required for each new VM-Series device that is added to Azure.

Panorama is already deployed in a different VNet with the following addresses:

- Panorama (primary)—**10.255.0.4**
- Panorama (secondary)—**10.255.0.5**

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

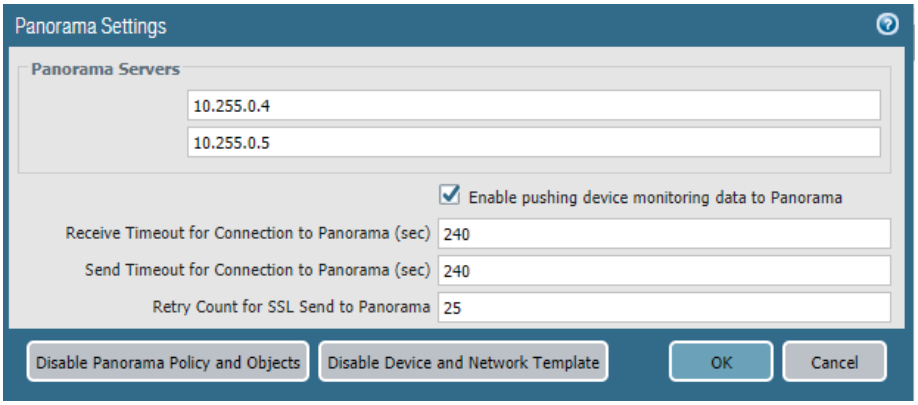
Step 2: In **Dashboard > General Information**, record the **Serial #**.



Step 3: In **Device > Setup > Management > Panorama Settings**, click the edit cog.

Step 4: In the Panorama Servers section, in the top box, enter **10.255.0.4**.

Step 5: If you are using Panorama in a high-availability configuration, in the bottom box, enter **10.255.0.5**, and then click **OK**.

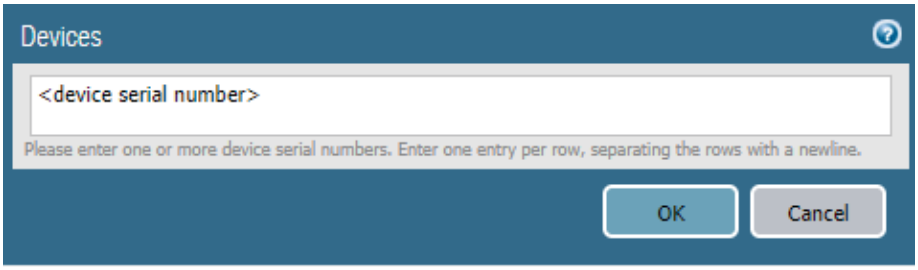


Step 6: Click **Commit**.

Step 7: Log in to Panorama (example: https://azurera-panorama-1.westus.cloudapp.azure.com)

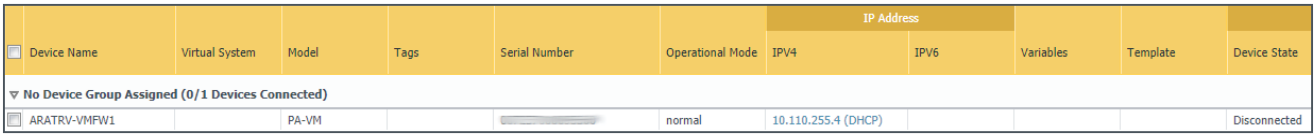
Step 8: In **Panorama > Managed Devices > Summary**, click **Add**.

Step 9: In the **Devices** box, enter the serial number from Step 2, and then click **OK**.



Step 10: On the **Commit** menu, click **Commit to Panorama**.

Step 11: In **Panorama > Managed Devices > Summary**, verify that the VM-Series device state is **Connected**. It might take a few minutes for the state to change.



Step 12: Repeat this procedure for any additional VM-Series devices that you have deployed.

4.2 Add VM-Series Devices to a Template Stack and Device Group for OBEW Firewalls

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

The following templates have already been created on Panorama:

- VMFW-Baseline—This includes DNS and NTP information common across all Azure deployments and includes Cortex Data Lake configuration.
- Transit-2-Zone-OBEW—This includes interface, zone, and virtual router configuration for OBEW firewalls.

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

Step 2: If the **Transit-VNet-OBEW** template stack already exists, in **Panorama > Templates**, click **Transit-VNet-OBEW**, and then skip to Step 7 in order to begin adding devices to the template stack.

If the **Transit-VNet-OBEW** template stack does not yet exist, complete Step 3 through Step 6 in order to create the template stack.

Step 3: In **Panorama > Templates**, click **Add Stack**.

Step 4: In the **Name** box, enter **Transit-VNet-OBEW**.

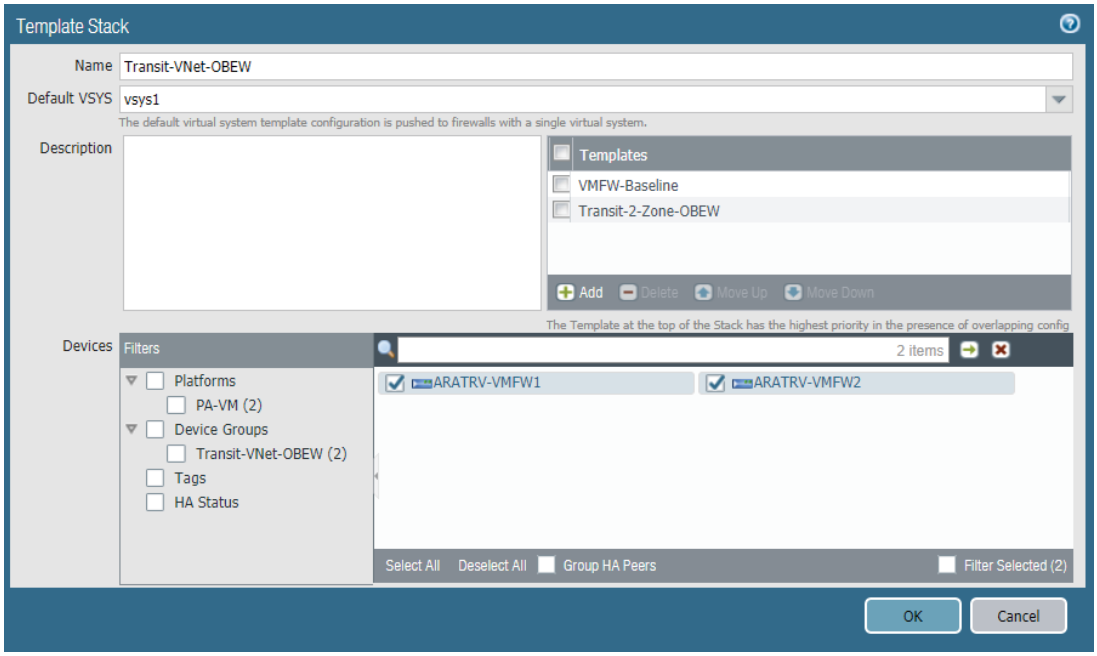
Step 5: In the Templates pane, click **Add**, and then select **VMFW-Baseline**.

Step 6: In the Templates pane, click **Add**, and then select **Transit-2-Zone-OBEW**.

Proceed with adding devices to the template stack.

Step 7: In the Devices pane, select the device you are adding to the template stack (example: **ARATRV-VMFW1**).

Step 8: If necessary, repeat Step 7 for any additional OBEW firewalls, and then click **OK**.



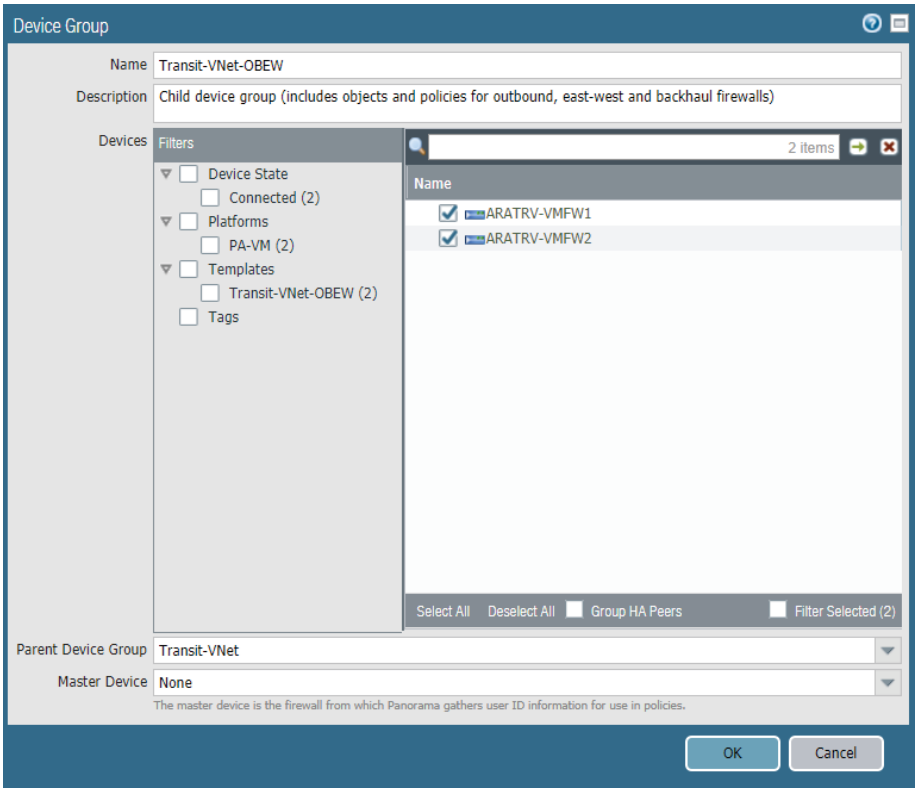
Step 9: On the **Commit** menu, click **Commit and Push**.

The local configuration on each VM-Series device should now reflect the template-based configuration that you created on Panorama. This includes interfaces, zones, virtual routers, management profiles, and Cortex Data Lake.

Step 10: In **Panorama > Device Groups**, click **Transit-VNet-OBEW**.

Step 11: In the Devices pane, select the device you are adding to the device group (example: **ARATRV-VMFW1**).

Step 12: If necessary, repeat Step 11 for any additional OBEW firewalls, and then click **OK**.



Step 13: On the **Commit** menu, click **Commit and Push**.

The local configuration on each VM-Series device should now reflect the device-group-based configuration that you created on Panorama. This includes the log-forwarding profile for Cortex Data Lake.

You create additional device group policies and objects later in this guide. Creating the policies and objects for the **Transit-VNet-OBEW** device group automatically pushes them to the local devices from Panorama.

4.3 Add VM-Series Devices to a Template Stack and Device Group for Inbound Firewalls

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

The following templates have already been created on Panorama:

- **VMFW-Baseline**—This includes DNS and NTP information common across all Azure deployments and includes Cortex Data Lake configuration.
- **Transit-2-Zone-Inbound**—This includes interface, zone, and virtual router configuration for inbound firewalls.

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

Step 2: If the **Transit-VNet-Inbound** template stack already exists, in **Panorama > Templates**, click **Transit-VNet-Inbound**, and then skip to Step 7 in order to begin adding devices to the template stack.

If the **Transit-VNet-Inbound** template stack does not yet exist, complete Step 3 through Step 6 in order to create the template stack.

Step 3: In **Panorama > Templates**, click **Add Stack**.

Step 4: In the **Name** box, enter **Transit-VNet-Inbound**.

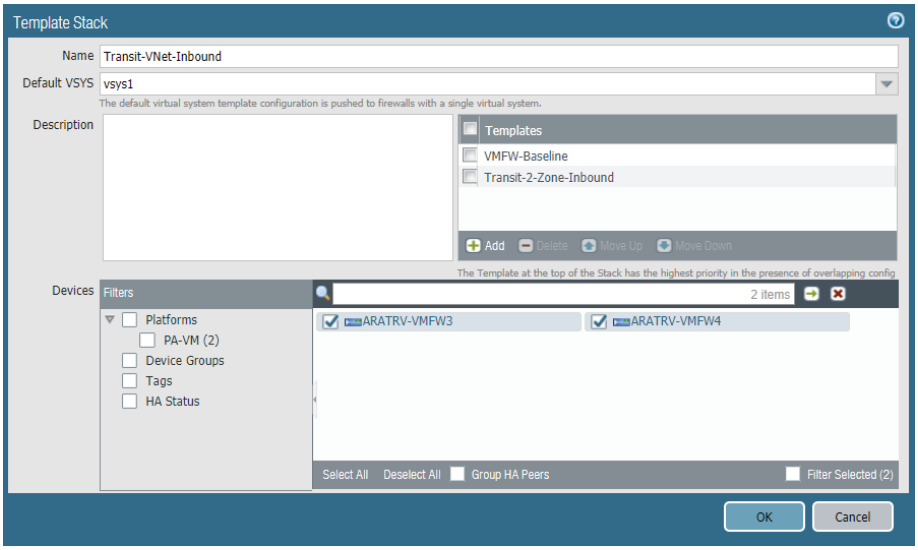
Step 5: In the Templates pane, click **Add**, and then select **VMFW-Baseline**.

Step 6: In the Templates pane, click **Add**, and then select **Transit-2-Zone-Inbound**.

Proceed with adding devices to the template stack.

Step 7: In the Devices pane, select the device you are adding to the template stack (example: **ARATRV-VMFW3**).

Step 8: If necessary, repeat Step 7 for any additional inbound firewalls, and then click **OK**.



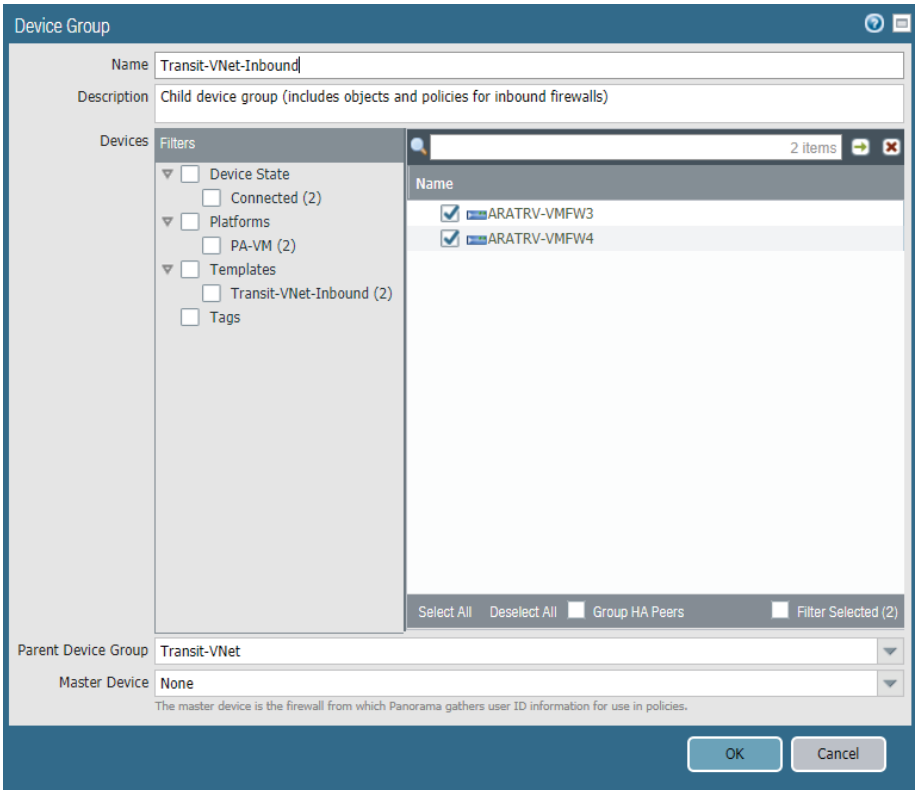
Step 9: On the **Commit** menu, click **Commit and Push**.

The local configuration on each VM-Series device should now reflect the template-based configuration that you created on Panorama. This includes interfaces, zones, virtual routers, management profiles, and Cortex Data Lake.

Step 10: In **Panorama > Device Groups**, click **Transit-VNet-Inbound**.

Step 11: In the Devices pane, select the device you are adding to the device group (example: **ARATRV-VMFW3**).

Step 12: If necessary, repeat Step 11 for any additional inbound firewalls, and then click **OK**.



Step 13: On the **Commit** menu, click **Commit and Push**.

The local configuration on each VM-Series device should now reflect the device-group-based configuration that you created on Panorama. This includes the log-forwarding profile for Cortex Data Lake.

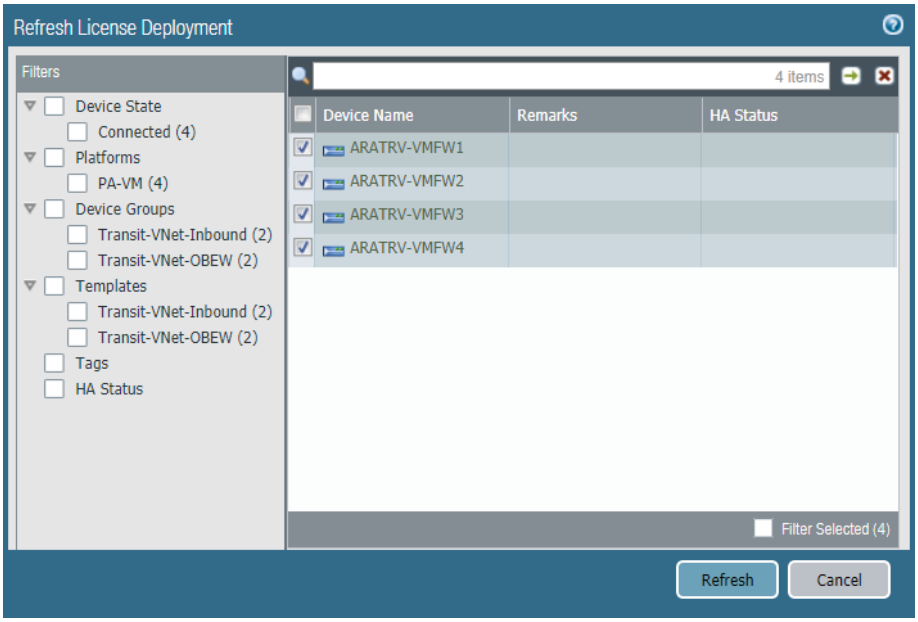
You create additional device group policies and objects later in this guide. Creating the policies and objects for the **Transit-VNet-Inbound** device group automatically pushes them to the local devices from Panorama.

4.4 Refresh License to Enable Log Forwarding to Cortex Data Lake

Step 1: Log in to Panorama (example: https://azurera-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 each VM-Series device, and then click **Refresh**.



Step 4: Verify the details for each VM-Series device include **Successfully installed license 'Logging Service,'** and then click **Close**.

Deployment Details for Azure Networking and Firewall Policies

The VM-Series devices do not actively forward traffic within Azure until you integrate them into Azure networking and create the firewall policies for each traffic profile. You must complete the complementary groups of procedures in order support the traffic profiles in the Transit VNet model.

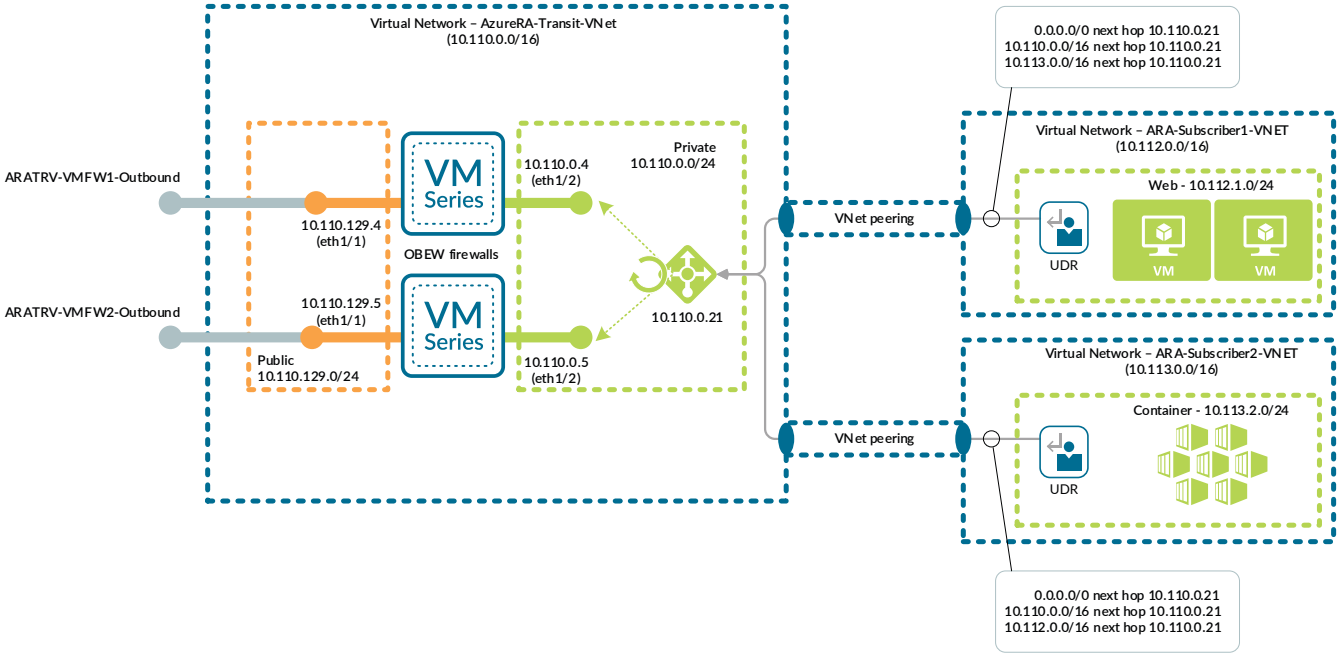
You implement resiliency for the traffic profiles by using Azure user-defined routes, Azure Load Balancer, and Azure Application Gateway, and these procedures are included in the first section of this chapter. The traffic profiles within the Transit VNet model each require a unique firewall policy. The second section of this chapter includes the procedures used to configure the policies required for each traffic profile.

CONFIGURING AZURE NETWORKING AND SERVICES

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

The Transit VNet supports inbound, outbound, and east-west traffic profiles for virtual machines in subscriber VNets. The procedures in this section are organized by traffic profile. First, you will complete the procedures to support the outbound and east-west traffic profiles. Next, you will complete the procedures to support the inbound access traffic profile.

Figure 8 Azure networking for outbound and east-west traffic profiles



There are two options for inbound traffic in the Transit VNet model, a public load balancer or an application gateway. Choose the inbound traffic option that is appropriate for your organization. Palo Alto Networks tested this guide with both options configured concurrently.

Procedures

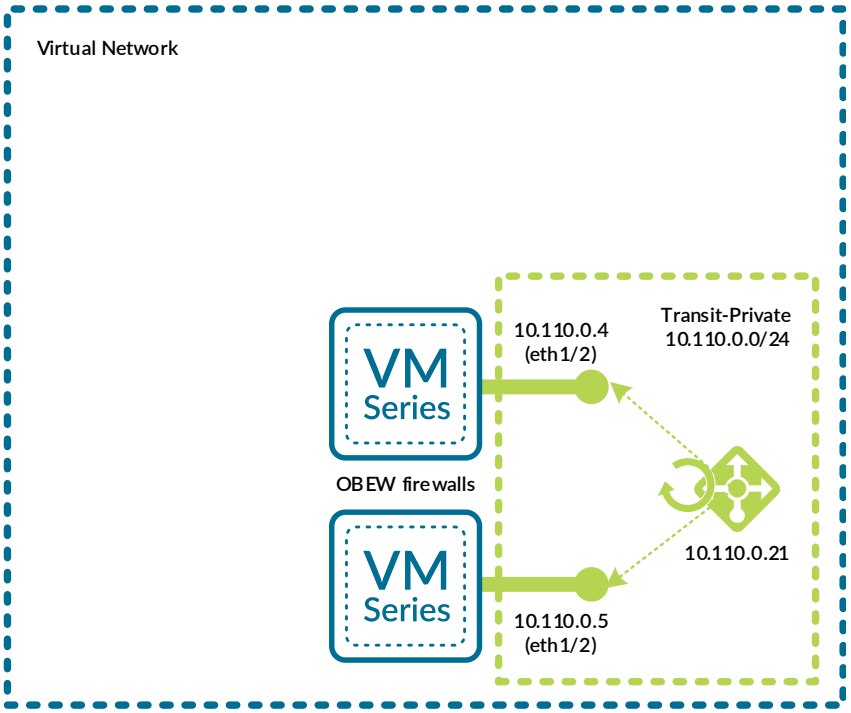
Configuring Outbound and East-West Traffic Profiles

5.1 Create the Azure Internal Load Balancer

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

You create the Azure internal load balancer with a single private front-end IP address and associate it with the private interfaces of a pair of VM-Series firewalls.

Figure 9 Azure internal load balancer for outbound access



You use the front-end 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 **Resource Group** list, choose **AzureRA-Transit**.

Step 3: In the **Name** box, enter **AzureRA-Transit-Internal**

Step 4: In the Type section, select **Internal**.

Step 5: In the SKU section, select **Standard**.

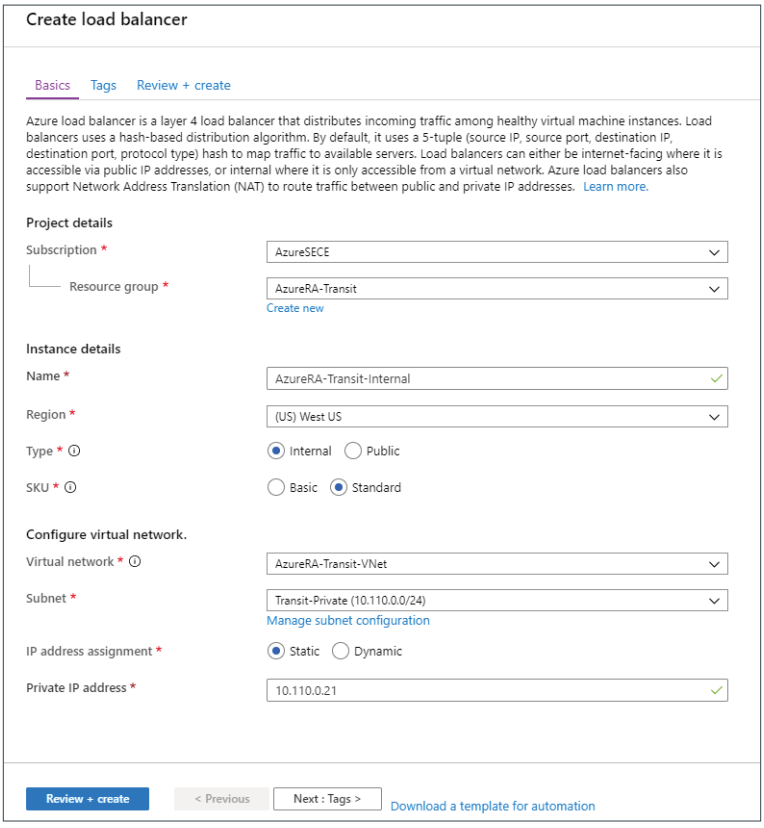
Step 6: In the **Virtual network** list, choose **AzureRA-Transit-VNet**.

Step 7: In the **Subnet** list, choose **Transit-Private**.

Step 8: In the IP address assignment section, select **Static**.

Step 9: In the **Private IP address** box, enter **10.110.0.21**. This address is associated with the default front-end IP configuration (**LoadBalancerFrontEnd**), which is used for outbound, east-west, and backhaul access. If necessary, you can add additional front-end IP addresses to the load balancer after it has been created.

Step 10: Click **Review + create**.



Step 11: On the next screen, click **Create**.

5.2 Configure the Azure Internal Load Balancer

Step 1: In **Home** > **Load Balancers** > **AzureRA-Transit-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**.

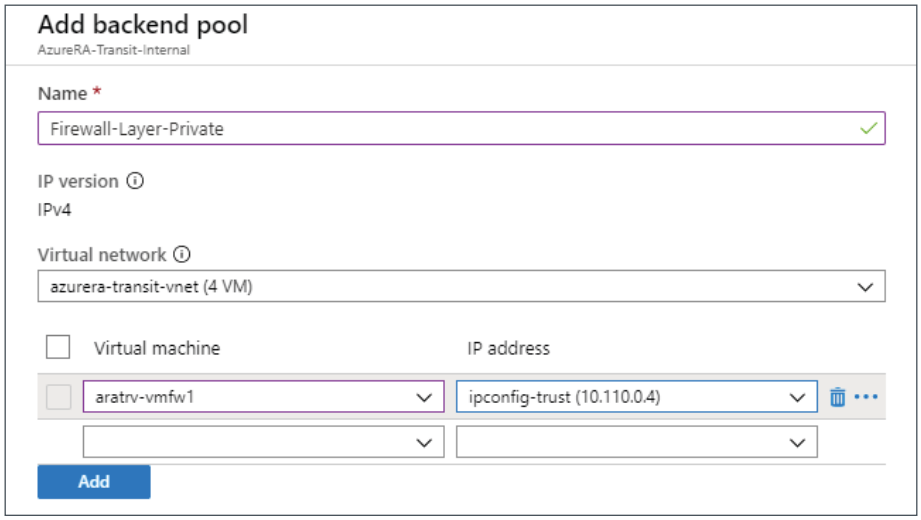
Step 4: In **Home** > **Load Balancers** > **AzureRA-Transit-Internal**, click **Backend pools**, and then click **Add**.

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

Step 6: In the **Virtual network** list, choose **AzureRA-Transit-VNet**.

Step 7: In the Virtual machines section, in the **Virtual machine** column, select a VM-Series device to add to this back-end pool (example: **ARATRV-VMFW1**).

Step 8: In the Virtual machines section, in the **IP address** column, select the **IP configuration** that is associated to the **Transit-Public** subnet. (example: **ipconfig-trust**).



Step 9: Repeat Step 7 and Step 8 for all VM-Series firewalls that you are assigning to this back-end pool.

Step 10: Click **Add**.

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

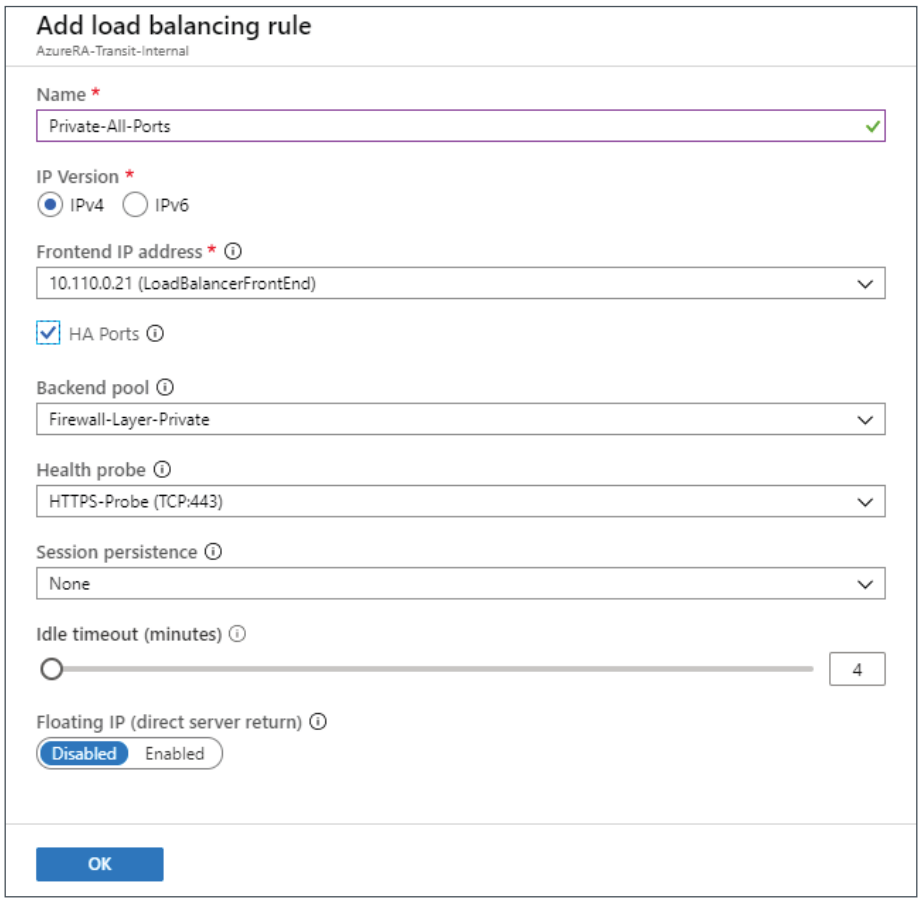
Step 12: In the **Name** box, enter **Private-All-Ports**.

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

Step 14: Select **HA ports**.

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

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



5.3 Configure Azure User-Defined Routes

Azure networking automatically creates system routes for the address space defined in the VNet. You also add additional system routes 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

Azure does not forward data traffic to the firewalls within the VNet until you create UDRs that direct traffic to the firewalls. In a resilient environment, you must create a UDR for Azure to forward data traffic to load balancers that act as front ends for the firewalls contained in their back-end pools.

Table 10 Azure system routes

Address space	Address prefix	Next-hop type
VNet defined	10.110.0.0/16	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 can 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, the UDR controls traffic within the subnet (*host-to-host traffic*).

As an example, if you applied a UDR for 10.110.0.0/16 with a next-hop of 10.110.0.21 (firewall load balancer) to the 10.110.1.0/24 subnet, then traffic between host 10.110.1.4 and host 10.110.1.5 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 can perform load balancing is by using UDRs to forward traffic to an Azure load-balancing resource.

After adding UDRs, Azure evaluates the effective route table using traditional routing rules based on longest match of the destination address.

Figure 10 User-defined routes within Transit VNet model

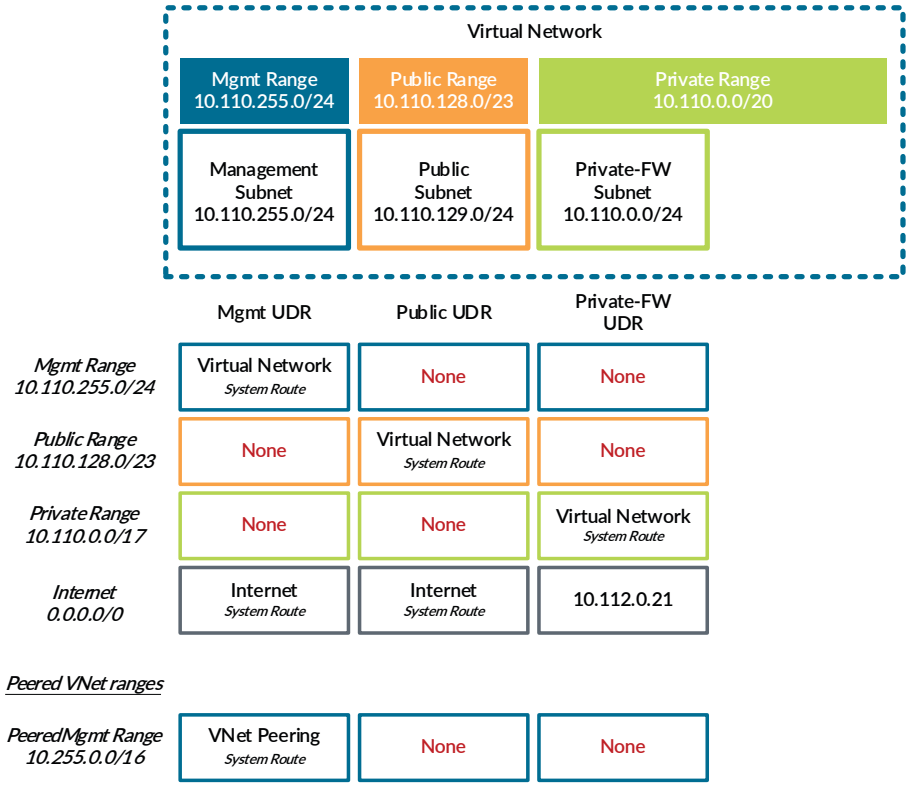


Table 11 Azure route tables

Subnet	Route table name	Resource group	Table of UDRs
Transit-Management	ARATRV-Management	AzureRA-Transit	Table 12
Transit-Public	ARATRV-Public	AzureRA-Transit	Table 13
Transit-Private	ARATRV-Private	AzureRA-Transit	Table 14

Table 12 Management subnet UDRs (10.110.255/24)

Route name	Address prefix	Next-hop type	Next-hop address	Comments
Blackhole-Public	10.110.128.0/23	None	—	Block traffic to Public IP address space
Blackhole-Private	10.110.0.0/17	None	—	Block traffic to Private IP address space

Table 13 Public subnet UDRs (10.110.129.0/24)

Route name	Address prefix	Next-hop type	Next-hop address	Comments
Blackhole-Management	10.110.255.0/24	None	—	Block traffic to management IP address space
Blackhole-PeeredManagement	10.255.0.0/16	None	—	Block traffic to management IP address space in peered VNet
Blackhole-Private	10.110.0.0/17	None	—	Block traffic to private IP address space

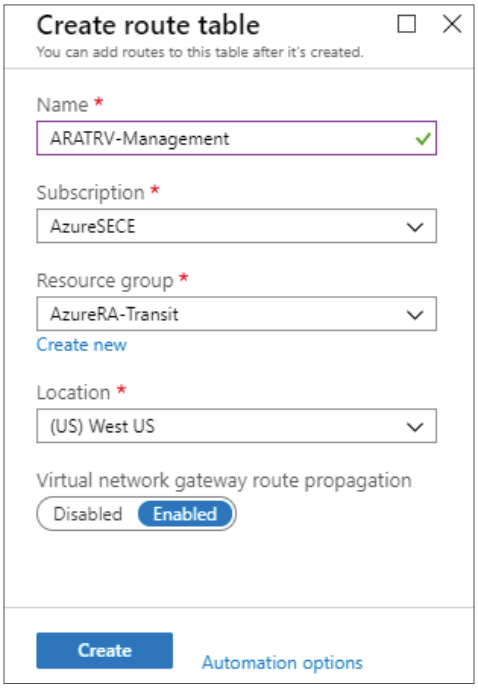
Table 14 Private Subnet UDRs (10.110.0.0/24)

Route name	Address prefix	Next-hop type	Next-hop address	Comments
Blackhole-Management	10.110.255.0/24	None	—	Block traffic to management IP address space
Blackhole-PeeredManagement	10.255.0.0/16	None	—	Block traffic to management IP address space in peered VNet
Blackhole-Public	10.110.128.0/23	None	—	Block traffic to public IP address space
UDR-default	0.0.0.0/0	Virtual appliance	10.110.0.21	Front-end IP of load balancer. Overrides system route

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

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

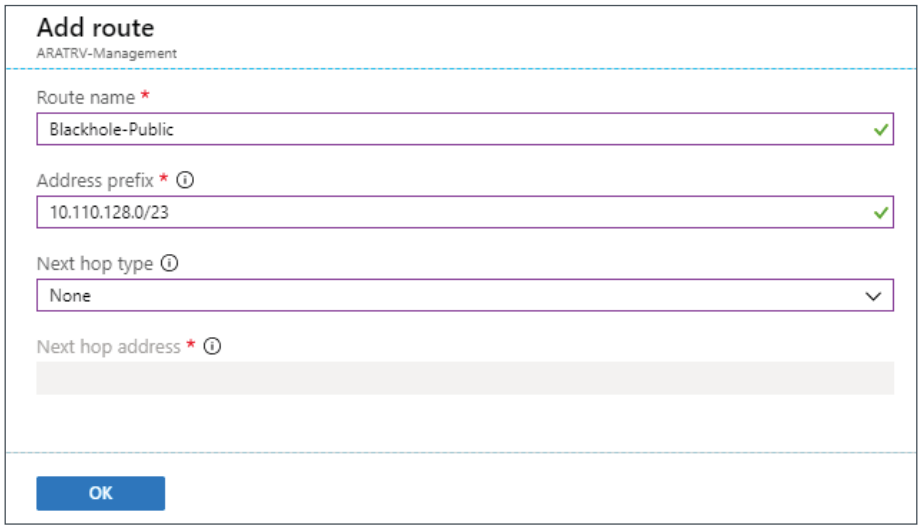
Step 3: In the **Resource Group** list, choose **AzureRA-Transit**, and then click **Create**.



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

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

- In Home > Routes tables > **ARATRV-Management—Routes**, click Add.
- In the Route name box, enter **Blackhole-Public**.
- In the Address prefix box, enter **10.110.128.0/23**.
- In the Next hop type list, choose **None**.
- If the Next-hop type is Virtual appliance, then enter the Next hop address value.
- Click OK.



Step 6: Repeat this procedure for each remaining entry in Table 11.

5.4 Apply Route Tables to the Subnets

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

Step 1: In Home > Virtual networks > **AzureRA-Transit-VNet**, click Subnets.

Step 2: Click **Transit-Management**.

Step 3: In the Route table list, choose **ARATRV-Management**, and then click Save.

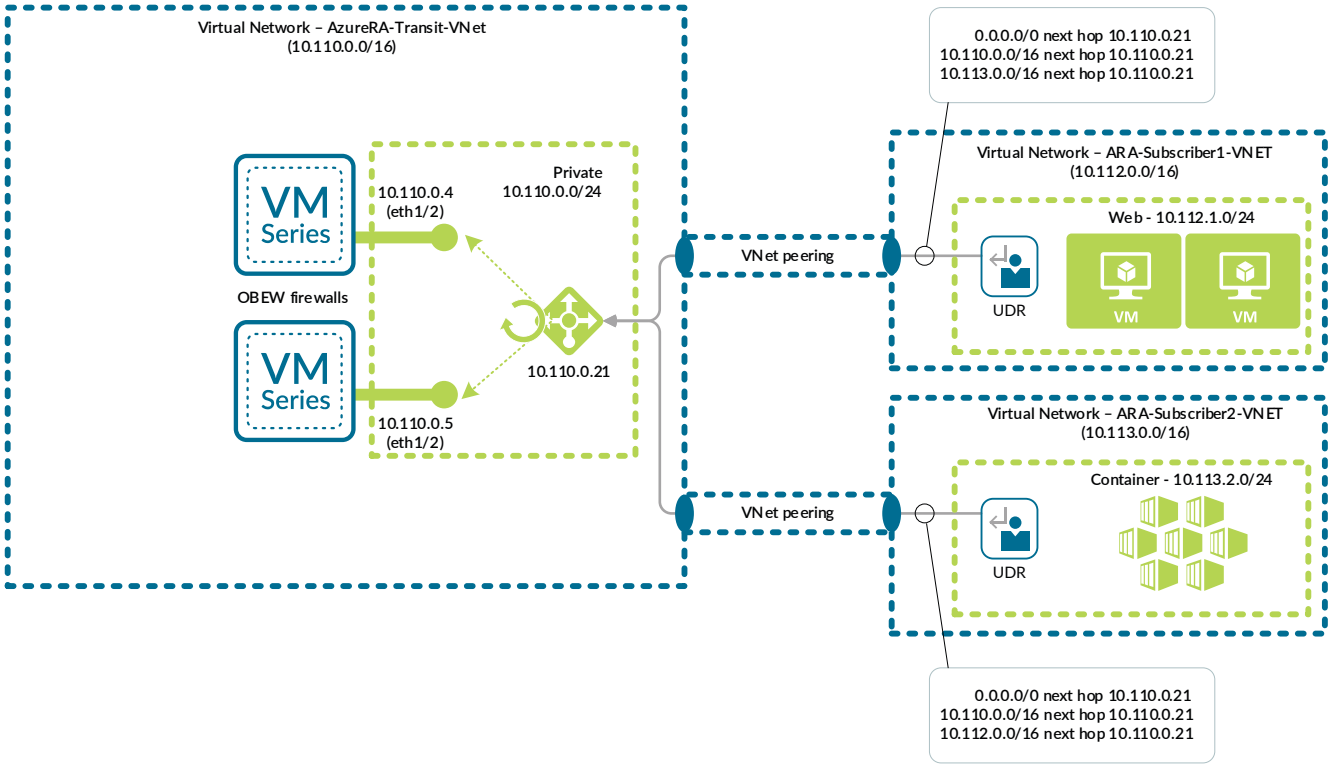
Step 4: Repeat Step 2 and Step 3 for each entry in Table 11.

5.5 Create Peering between the Transit VNet and Subscriber VNets

This guide assumes that you have already created subscriber VNets. In order to access service and resources through the transit VNet, you must create a VNet peer connection between the transit VNet and each subscriber VNet.

This procedure is required for the outbound and east-west traffic profiles.

Figure 11 Peer connections to subscriber VNets



After you configure the peering relationship from a single VNet, Azure then makes the necessary configuration updates on both VNet peers.

Table 15 Transit VNet peer connections

Transit-VNet (source)	Name of the peering (to remote virtual network)	Virtual network (destination/ subscriber)	Address space (subscriber)	Name of the peering (to Transit VNet)
AzureRA-Transit-VNet	VNet-Peer_ARA-Subscriber1-VNet	ARA-Subscriber1-VNET	10.112.0.0/16	VNet-Peer_AzureRA-Transit-VNet
AzureRA-Transit-VNet	VNet-Peer_ARA-Subscriber2-VNet	ARA-Subscriber2-VNET	10.113.0.0/16	VNet-Peer_AzureRA-Transit-VNet

Step 1: In **Home > Virtual networks > AzureRA-Transit-VNet**, click **Peerings**.

Step 2: Click **Add**.

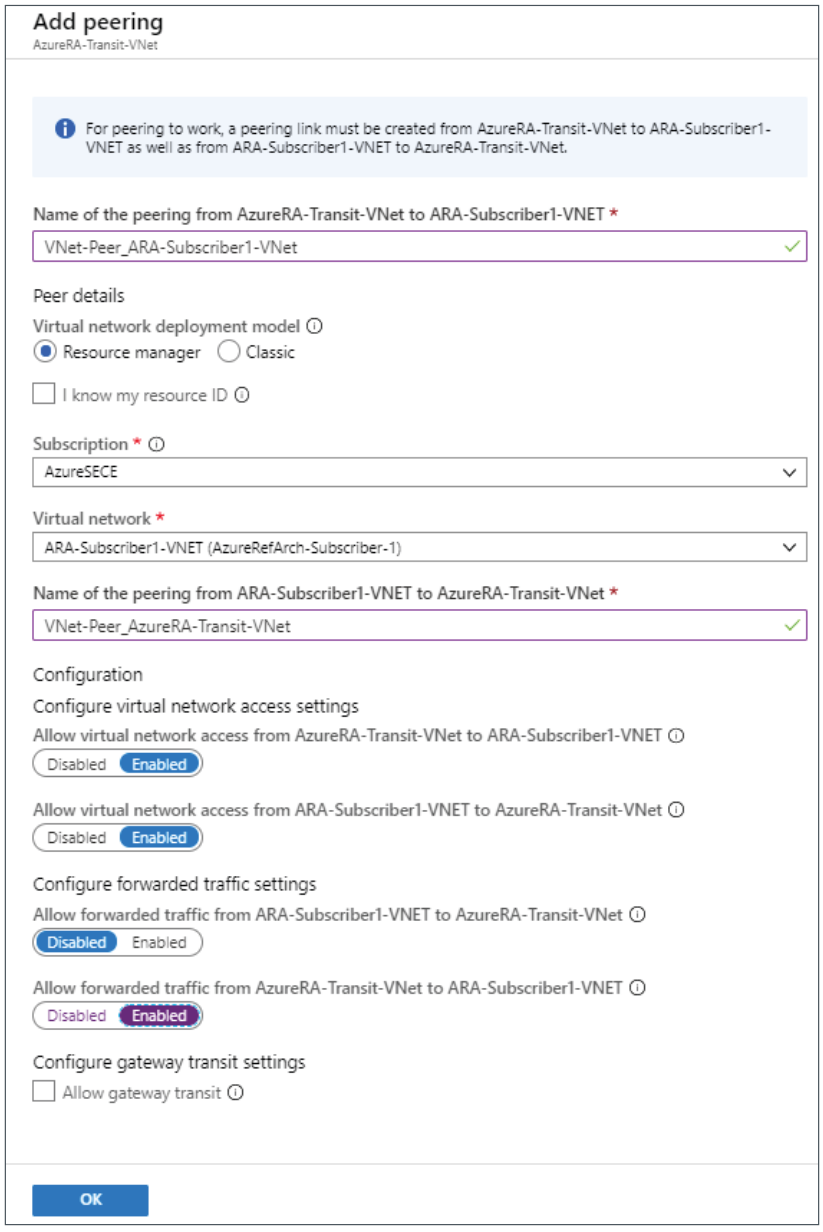
Step 3: In the **Name of the peering from AzureRA-Transit-VNet to remote virtual network** box, enter **VNet-Peer_ARA-Subscriber1-VNet**.

Step 4: In the **Virtual network** list, choose **ARA-Subscriber1-VNET**.

Step 5: In the **Name of the peering from ARA-Subscriber-1-VNET to AzureRA-Transit-VNet** box, enter **VNet-Peer_AzureRA-Transit-VNet**.

Step 6: In the Allow forwarded traffic from **AzureRA-Transit-VNet** to **ARA-Subscriber-1-VNET** section, select **Enabled**. This setting allows the peer VNet's forwarded traffic (traffic not originating from inside the peer virtual network) into your virtual network.

Step 7: Click **OK**.



Step 8: Repeat Step 2 through Step 7 for each entry in Table 15.

Next, you verify that the effective routes for your transit VNet private subnet properly include the routes from peered VNets.

Step 9: In **Home** > **Route tables** > **ARATRV-Private**, click **Effective Routes**.

Step 10: In the **Network interface** list, choose any interface from a running virtual machine with an interface associated to the **Transit-Private** subnet (example: **ARATRV-VMFW1-eth2**).

Step 11: In the **Effective routes** table for your transit VNet private subnet, verify that the address space from peered VNets is **Active**.

Default	Active	10.112.0.0/16	VNet peering
Default	Active	10.113.0.0/16	VNet peering

Note

Establishing the peer connection automatically creates system routes. These routes include any IP address space that is configured for the peered VNet. This does not include routes from VNets that are peers of peers.

5.6 Configure Azure User-Defined Routes for the Subscriber VNets

The Transit VNet model requires that subscriber VNets both have an existing peer connection and an applied UDR that redirects traffic to the front-end IP of the internal load balancer in the transit VNet.

Figure 12 Additional user-defined routes for subscriber VNets

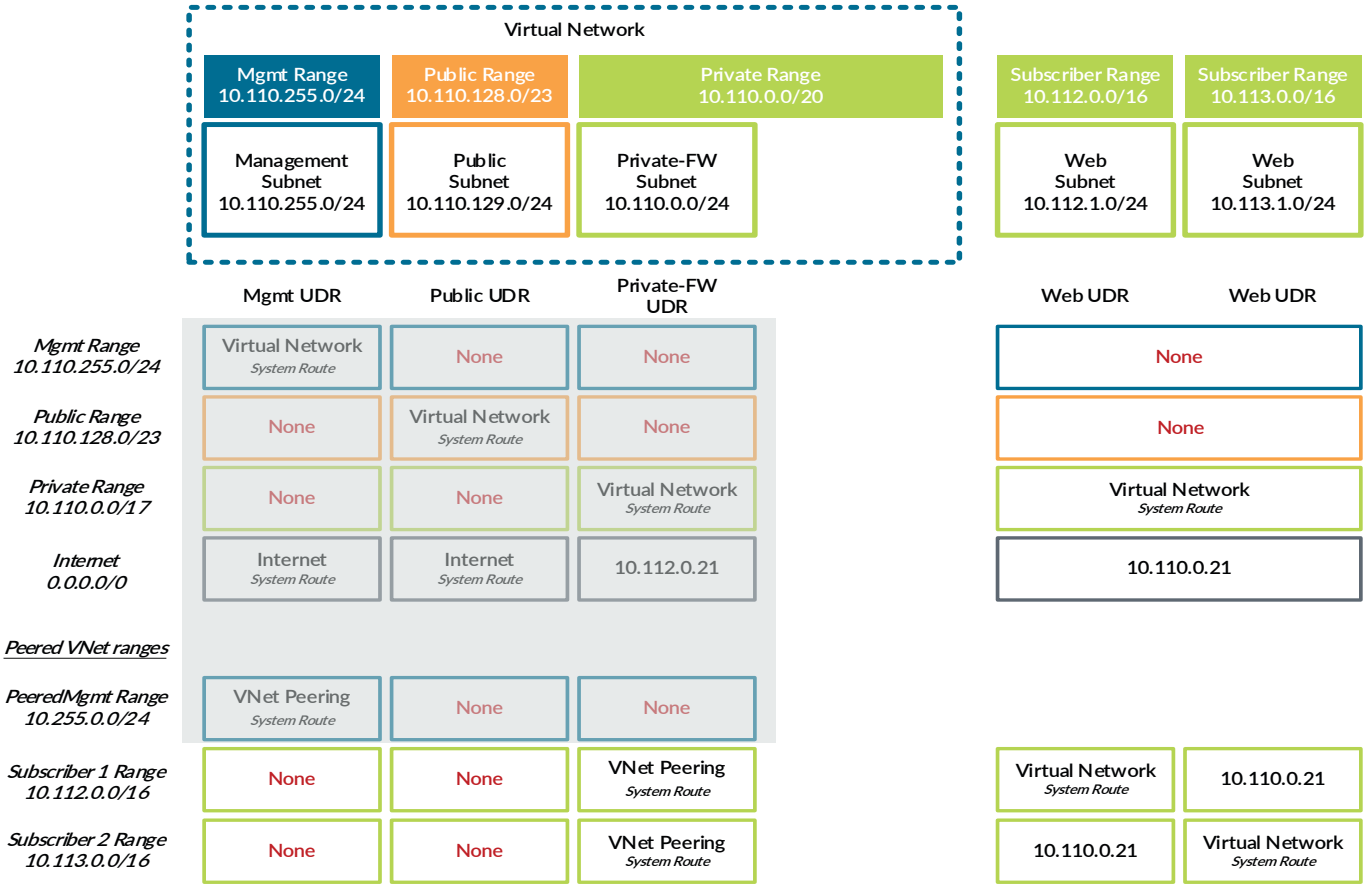


Table 16 Azure subscriber VNet route tables

Route table name	Resource group	Virtual network	Subnet	Table of UDRs
ARATRV-Sub1-Server	ARA-Subscriber-1	ARA-Subscriber1-VNET	Server (10.112.1.0/24)	Table 17
ARATRV-Sub2-Server	ARA-Subscriber-2	ARA-Subscriber2-VNET	Server (10.113.1.0/24)	Table 18

Table 17 Subscriber-1 server subnet UDRs (10.112.1.0/24)

Route name	Address prefix	Next-hop type	Next-hop address	Comments
Blackhole-Management	10.110.255.0/24	None	—	Block traffic to management IP address space
Blackhole-Public	10.110.128.0/23	None	—	Block traffic to public IP address space
UDR-default	0.0.0.0/0	Virtual appliance	10.110.0.21	Front-end IP of load balancer. Overrides system route. Used for outbound traffic profile.
Net-10.113.0.0_16	10.113.0.0/16	Virtual appliance	10.110.0.21	Front-end IP of load balancer Used for east-west traffic profile

Table 18 Subscriber-2 server subnet UDRs (10.113.1.0/24)

Route name	Address prefix	Next-hop type	Next-hop address	Comments
Blackhole-Management	10.110.255.0/24	None	—	Block traffic to management IP address space
Blackhole-Public	10.110.128.0/23	None	—	Block traffic to public IP address space
UDR-default	0.0.0.0/0	Virtual appliance	10.110.0.21	Front-end IP of load balancer. Overrides system route Used for outbound traffic profile.
Net-10.112.0.0_16	10.112.0.0/16	Virtual appliance	10.110.0.21	Front-end IP of load balancer Used for east-west traffic profile

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

Step 2: In the **Name** box, enter **ARATRV-Sub1-Server**.

Step 3: In the **Resource Group** list, choose **ARA-Subscriber-1**, and then click **Create**.

Step 4: In **Home** > **Route tables** > **ARATRV-Sub1-Server**, click **Routes**.

Step 5: Repeat these sub-steps for all entries in the table of UDRs for the corresponding subscriber:

- In **Home > Routes tables > ARATRV-Sub1-Server—Routes**, click **Add**.
- In the **Route name** box, enter **Blackhole-Management**.
- In the **Address prefix** box, enter **10.110.255.0/24**.
- In the **Next hop type** list, choose **None**.
- If the Next-hop type is **Virtual appliance**, enter the **Next-hop address** value.
- Click **OK**.

Step 6: Repeat Step 1 through Step 5 for each entry in Table 16.

Next, you modify the existing route tables for the management and public ranges in order to block access to the subscriber ranges.

Table 19 Existing Azure route tables requiring modification

Route table name	Resource group	Virtual network	Subnet	Table of UDRs
ARATRV-Management	AzureRA-Transit	AzureRA-Transit-VNET	Transit-Management	Table 20
ARATRV-Public	AzureRA-Transit	AzureRA-Transit-VNET	Transit-Public	Table 20

Table 20 Additional discard UDRs

Route name	Address prefix	Next-hop type	Comments
Blackhole-Sub1	10.112.0.0/16	None	Block traffic to Subscriber-1 IP address space
Blackhole-Sub2	10.113.0.0/16	None	Block traffic to Subscriber-2 IP address space

Step 7: In **Home > Route tables > ARATRV-Management**, click **Routes**.

Step 8: Repeat these sub-steps for all entries in Table 20:

- In **Home > Routes tables > ARATRV-Management—Routes**, click **Add**.
- In the **Route name** box, enter **Blackhole-Sub1**.
- In the **Address prefix** box, enter **10.112.0.0/16**.
- In the **Next hop type** list, choose **None**.

Step 9: Repeat Step 7 and Step 8 for each entry in Table 19.

5.7 Apply Route Tables to the Subnets

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

Step 1: In **Home > Virtual networks > ARA-Subscriber1-VNET**, click **Subnets**.

Step 2: Click **Server**.

Step 3: In the **Route table** list, choose **ARATRV-Sub1-Server**, and then click **Save**.

Step 4: Repeat Step 1 through Step 3 for each entry in Table 16.

Next, you verify that the effective routes for your subscriber subnets properly include the routes from the peered VNet.

Step 5: In **Home > Route tables > ARATRV-Sub1-Server**, click **Effective Routes**.

Step 6: In the **Network interface** list, choose any interface from a running virtual machine with an interface associated to the **Server** subnet (example: **ara-sub1-server1185**).

Step 7: In the **Effective Routes** table, verify that the address space from the transit VNet is **Active**. Prefixes that exactly match discard routes should now appear as **Invalid**.

Step 8: If necessary, repeat Step 5 through Step 7 for additional subscriber subnets.

Effective routes

Source	State	Address Prefixes	Next Hop Type	Next Hop Type IP Address	User Defined Route Name
Default	Invalid	0.0.0.0/0	Internet	-	-
User	Active	0.0.0.0/0	None	10.1.0.21	UDR-default
Default	Active	10.110.0.0/16	VNet peering	-	-
User	Active	10.110.128.0/23	None	-	Blackhole-Public
User	Active	10.110.255.0/24	None	-	Blackhole-Management
User	Active	10.112.0.0/16	Virtual appliance	10.110.0.21	Net-10.112.0.0_16
Default	Active	10.113.0.0/16	Virtual network	-	-
User	Active	10.6.0.0/16	None	10.1.0.21	Net-10.6.0.0_16

Note

You should not see system routes for any other subscriber VNets or the Panorama management VNet, because these are peered only to the transit VNet (peers of peers).

Procedures

Configuring Inbound Access Traffic Profile (Public Load Balancer Option)

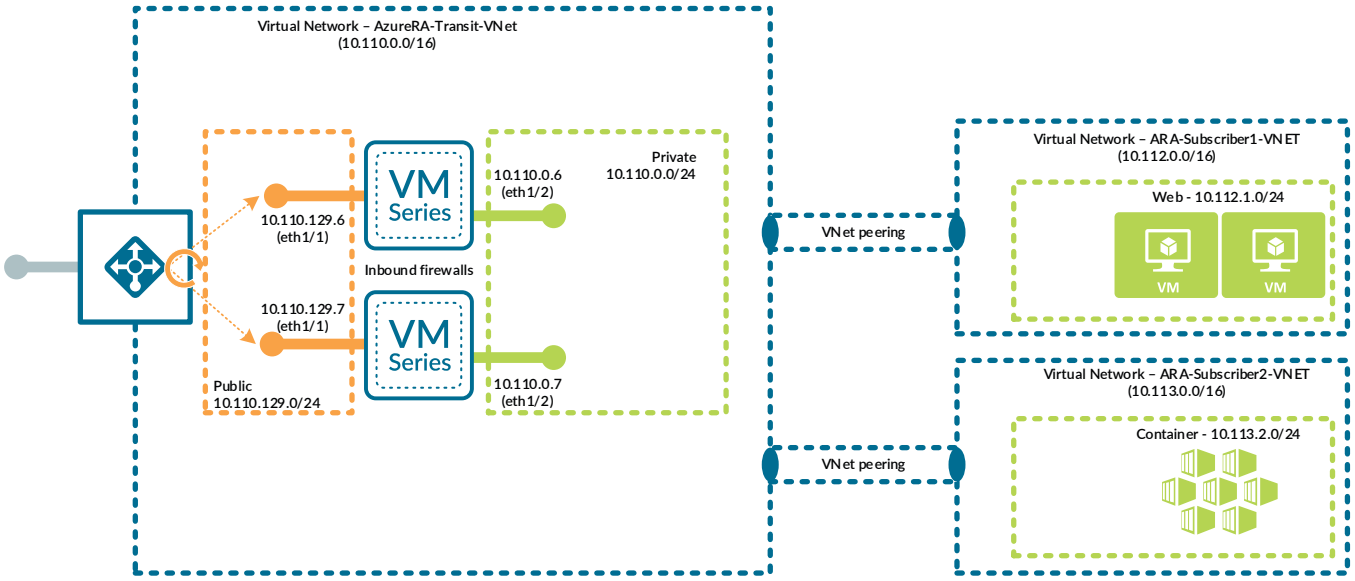
If you have selected the Azure public load balancer for inbound traffic, complete this section.

6.1 Create Peering between the Transit VNet and Subscriber VNets

This guide assumes that you have already created subscriber VNets. In order to access service and resources through the transit VNet, you must create a VNet peer connection between the transit VNet and each subscriber VNet.

This procedure is required for the inbound access traffic profiles. If you have not already completed Procedure 5.5, complete this procedure now. If you already completed Procedure 5.5, skip this procedure.

Figure 13 Peer connections to subscriber VNets



After you configure the peering relationship from a single VNet, Azure then makes the necessary configuration updates on both VNet peers.

Table 21 Transit VNet peer connections

Transit-VNet (source)	Name of the peering (to remote virtual network)	Virtual network (destination/ subscriber)	Address space (subscriber)	Name of the peering (to Transit VNet)
AzureRA-Transit-VNet	VNet-Peer_ARA-Subscriber1-VNet	ARA-Subscriber1-VNET	10.112.0.0/16	VNet-Peer_AzureRA-Transit-VNet
AzureRA-Transit-VNet	VNet-Peer_ARA-Subscriber2-VNet	ARA-Subscriber2-VNET	10.113.0.0/16	VNet-Peer_AzureRA-Transit-VNet

Step 1: In **Home > Virtual networks > AzureRA-Transit-VNet**, click **Peerings**.

Step 2: Click **Add**.

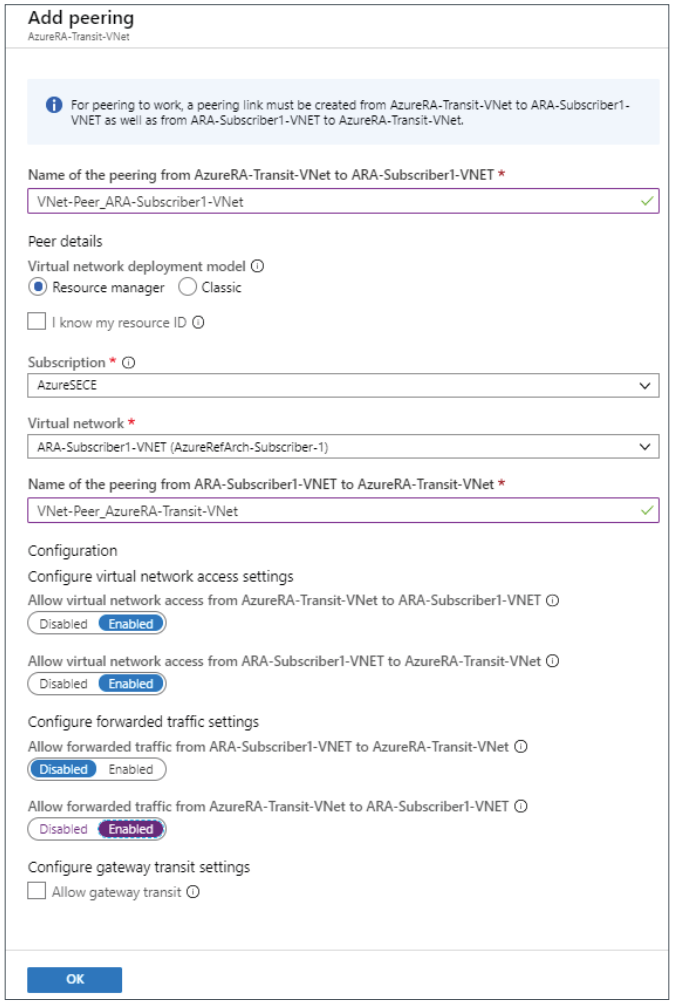
Step 3: In the **Name of the peering from AzureRA-Transit-VNet to remote virtual network** box, enter **VNet-Peer_ARA-Subscriber1-VNet**.

Step 4: In the **Virtual network** list, choose **ARA-Subscriber1-VNET**.

Step 5: In the **Name of the peering from ARA-Subscriber-1-VNET to AzureRA-Transit-VNet** box, enter **VNet-Peer_AzureRA-Transit-VNet**.

Step 6: In the Allow forwarded traffic from **AzureRA-Transit-VNet** to **ARA-Subscriber-1-VNET** section, select **Enabled**. This setting allows the peer VNet's forwarded traffic (traffic not originating from inside the peer virtual network) into your virtual network.

Step 7: Click **OK**.



Step 8: Repeat Step 2 through Step 7 for each entry in Table 21.

Next, you verify that the effective routes for your transit VNet private subnet properly include the routes from peered VNets.

Step 9: In **Home > Route tables > ARATRV-Private**, click **Effective Routes**.

Step 10: In the **Network interface** list, choose any interface from a running virtual machine with an interface associated to the **Transit-Private** subnet (example: **ARATRV-VMFW1-eth2**).

Step 11: In the **Effective routes** table for your transit VNet private subnet, verify that the address space from peered VNets is **Active**.

Default	Active	10.112.0.0/16	VNet peering
Default	Active	10.113.0.0/16	VNet peering

Note

Establishing the peer connection automatically creates system routes. These routes include any IP address space that is configured for the peered VNet. This does not include routes from VNets that are peers of peers.

6.2 Create the Public IP Address for the Azure Public Load Balancer

This procedure creates and assigns a public IP address as the front-end IP address for the Azure public load balancer for inbound traffic to the web server resources.

Note that you define a FQDN 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 SKU section, select **Standard**.

Step 3: In the **Name** box, enter **ARATRV-Public-Web**.

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

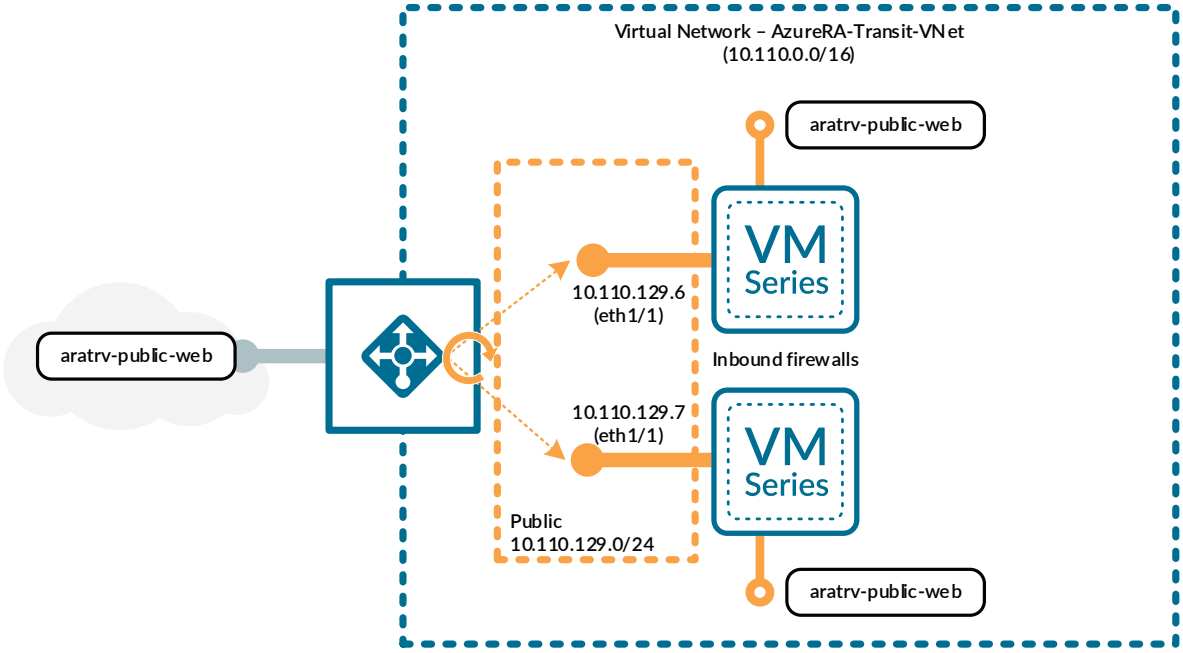
Step 5: In the **Resource Group** list, choose **AzureRA-Transit**, and then click **Create**.

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

6.3 Create the Azure Public Load Balancer

You create the Azure public load balancer with a single public front-end IP address and associate it with the public interfaces of a pair of VM-Series firewalls, and you configure the load balancer rules to use floating IP.

Figure 14 Azure public load balancer



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

Step 2: In the **Resource Group** list, choose **AzureRA-Transit**.

Step 3: In the **Name** box, enter **AzureRA-Transit-Public**.

Step 4: In the **Region** list, choose **(US) West US**.

Step 5: In the Type section, select **Public**.

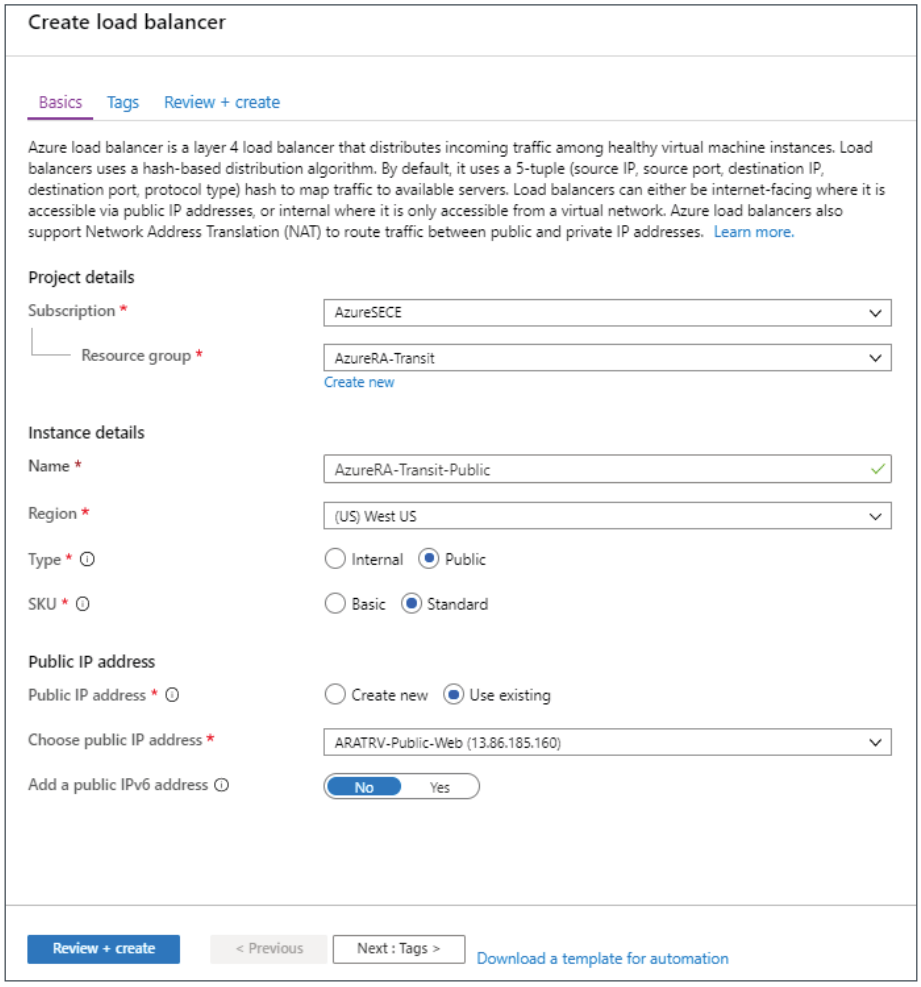
Step 6: In the SKU section, select **Standard**.

Step 7: In the Public IP address section, select **Use Existing**.

Step 8: In the **Choose public IP address** list, choose **ARATRV-Public-Web**.

This address is associated with the default front-end IP configuration (**LoadBalancerFrontEnd**). If necessary, you can add additional front-end IP addresses to the load balancer after it has been created.

Step 9: Click **Review + create**, and then on the next screen, click **Create**.



6.4 Configure the Azure Public Load Balancer

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

Step 1: In **Home > Load Balancers > AzureRA-Transit-Public**, click **Health probes**.

Step 2: Click **Add**.

Step 3: In the **Name** box, enter **SSH-Probe**.

Step 4: In the **Port** box, enter **22**, and then click **OK**.

Step 5: In **Home > Load Balancers > AzureRA-Transit-Public**, click **Backend pools**.

Step 6: Click **Add**.

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

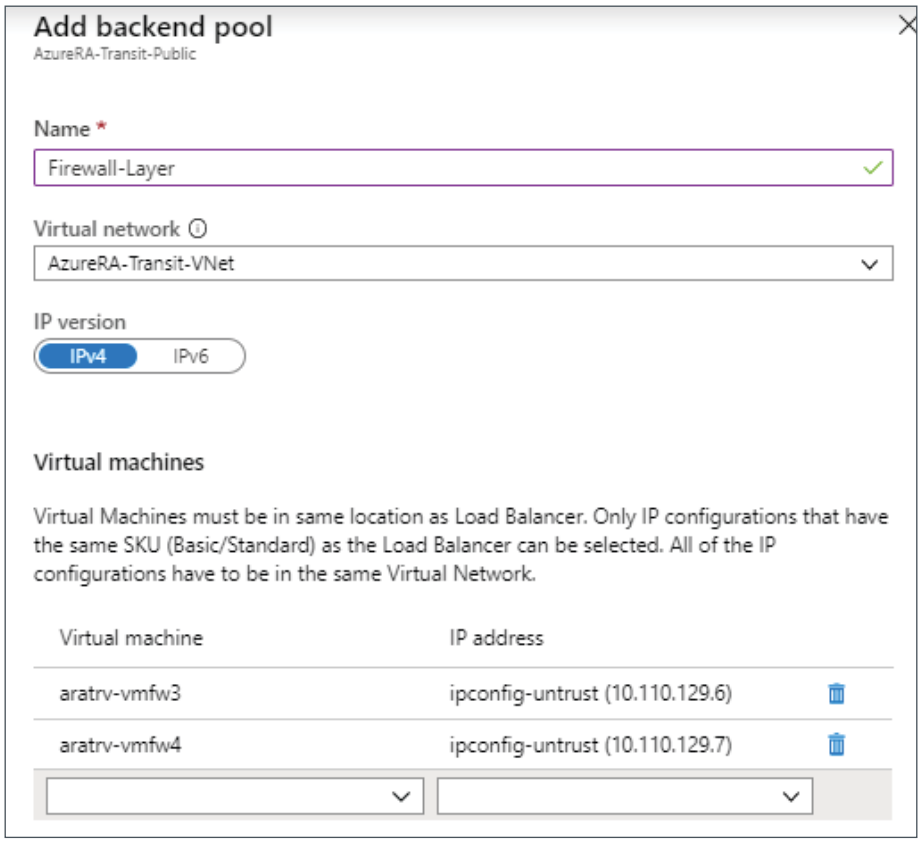
Step 8: In the **Virtual network** list, choose **AzureRA-Transit-VNet**.

Step 9: In the Virtual machines section, in the **Virtual machine** column, select a VM-Series firewall you are adding to this back-end pool (example: **ARATRV-VMFW3**).

Step 10: In the Virtual machines section, in the **IP address** column, select the IP configuration that is associated to the **Transit-Public** subnet (example: **ipconfig-untrust**).

Step 11: Repeat Step 9 and Step 10 for all VM-Series firewalls that you are assigning to this back-end pool.

Step 12: Click **Add**.



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

Step 13: In **Home** > **Load Balancers** > **AzureRA-Transit-Public**, click **Load balancing rules**.

Step 14: Click **Add**.

Step 15: In the **Name** box, enter **AzureRA-Transit-Public-Web-80**.

Step 16: In the **Frontend IP address** list, choose **LoadBalancerFrontEnd**.

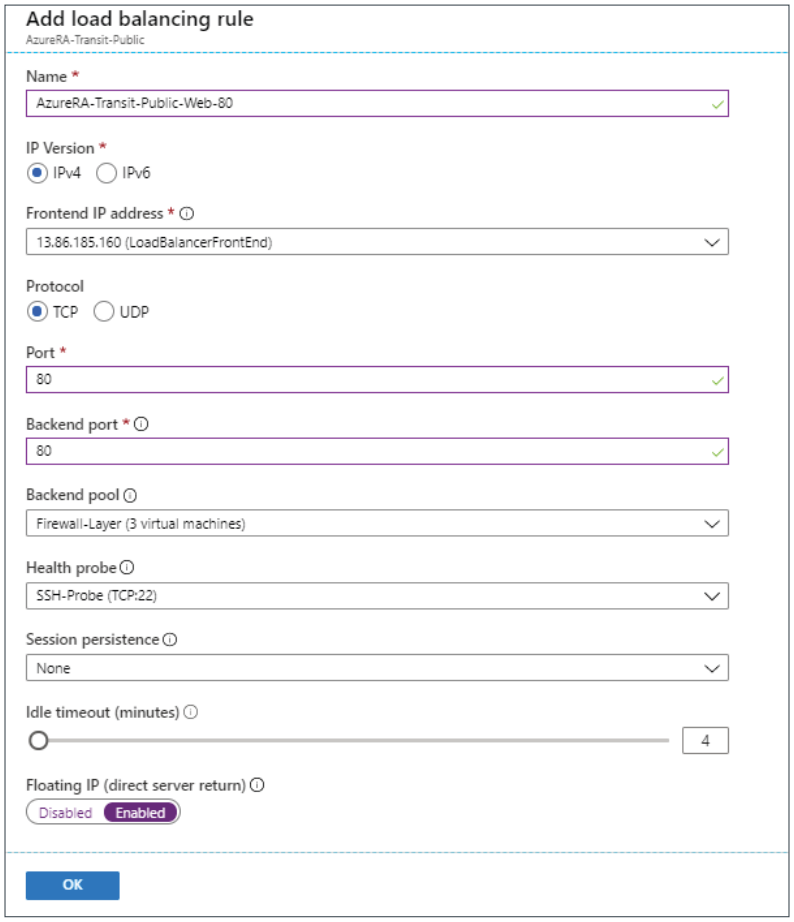
Step 17: In the **Port** box, enter **80**.

Step 18: In the **Backend port** box, enter **80**.

Step 19: In the **Backend pool** list, choose **Firewall-Layer**.

Step 20: In the **Health probe** list, choose **SSH-Probe**.

Step 21: In the Floating IP (direct server return) section, select **Enabled**, and then click **OK**.



Step 22: If necessary, repeat Step 14 through Step 21 for additional ports.

Procedures

Configuring Inbound Access Traffic Profiles (Application Gateway Option)

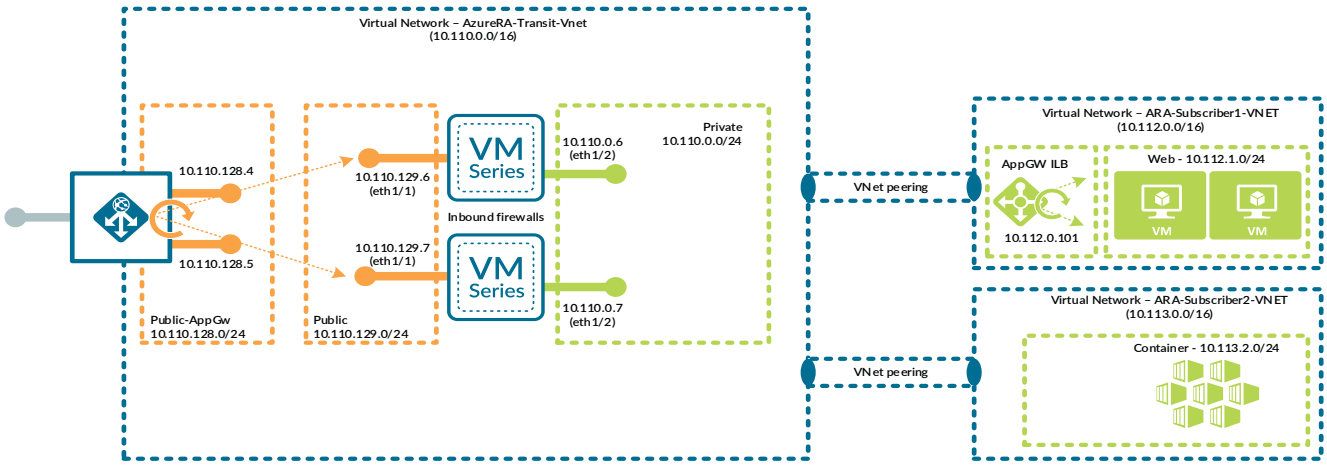
If you have selected the Azure application gateway option for inbound traffic, complete this section.

7.1 Create Peering between the Transit VNet and Subscriber VNets

This guide assumes that you have already created subscriber VNets. In order to access service and resources through the transit VNet, you must create a VNet peer connection between the transit VNet and each subscriber VNet.

This procedure is required for the inbound access traffic profiles. If you have not already completed Procedure 5.5 or Procedure 6.1, complete this procedure now. If you already completed Procedure 5.5 or Procedure 6.1, skip this procedure.

Figure 15 Peer connections to subscriber VNets



After you configure the peering relationship from a single VNet, Azure then makes the necessary configuration updates on both VNet peers.

Table 22 Transit VNet peer connections

Transit-VNet (source)	Name of the peering (to remote virtual network)	Virtual network (destination/ subscriber)	Address space (subscriber)	Name of the peering (to Transit VNet)
AzureRA-Transit-VNet	VNet-Peer_ARA-Subscriber1-VNet	ARA-Subscriber1-VNET	10.112.0.0/16	VNet-Peer_AzureRA-Transit-VNet
AzureRA-Transit-VNet	VNet-Peer_ARA-Subscriber2-VNet	ARA-Subscriber2-VNET	10.113.0.0/16	VNet-Peer_AzureRA-Transit-VNet

Step 1: In **Home > Virtual networks > AzureRA-Transit-VNet**, click **Peerings**.

Step 2: Click **Add**.

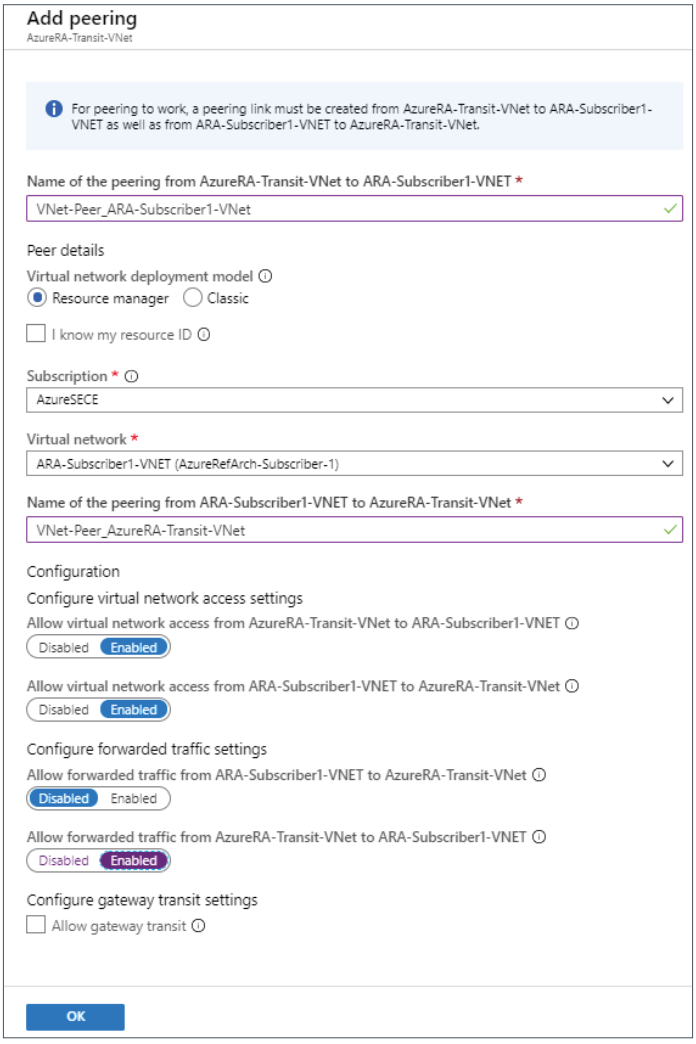
Step 3: In the **Name of the peering from AzureRA-Transit-VNet to remote virtual network** box, enter **VNet-Peer_ARA-Subscriber1-VNet**.

Step 4: In the **Virtual network** list, choose **ARA-Subscriber1-VNET**.

Step 5: In the **Name of the peering from ARA-Subscriber-1-VNET to AzureRA-Transit-VNet** box, enter **VNet-Peer_AzureRA-Transit-VNet**.

Step 6: In the Allow forwarded traffic from **AzureRA-Transit-VNet** to **ARA-Subscriber-1-VNET** section, select **Enabled**. This setting allows the peer VNet's forwarded traffic (traffic not originating from inside the peer virtual network) into your virtual network.

Step 7: Click **OK**.



Step 8: Repeat Step 2 through Step 7 for each entry in Table 22.

Next, you verify that the effective routes for your transit VNet private subnet properly include the routes from peered VNets.

Step 9: In **Home > Route tables > ARATRV-Private**, click **Effective Routes**.

Step 10: In the **Network interface** list, choose any interface from a running virtual machine with an interface associated to the **Transit-Private** subnet (example: **ARATRV-VMFW1-eth2**).

Step 11: In the **Effective routes** table for your transit VNet private subnet, verify that the address space from peered VNets is **Active**.

Default	Active	10.112.0.0/16	VNet peering
Default	Active	10.113.0.0/16	VNet peering

Note

Establishing the peer connection automatically creates system routes. These routes include any IP address space that is configured for the peered VNet. This does not include routes from VNets that are peers of peers.

7.2 Create the Public IP Address for the Azure Application Gateway

This procedure creates and assigns a public IP address as the front-end IP address for the Azure application gateway for inbound traffic to the web server resources.

Note that you define a FQDN 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 SKU section, select **Standard**.

Step 3: In the **Name** box, enter **ARATRV-Public-AppGW**.

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

Step 5: In the **Resource Group** list, choose **AzureRA-Transit**, and then click **Create**.

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

7.3 Add the Application Gateway Subnet to the Virtual Network

Azure does not permit you to configure route tables on the application gateway subnet, so you modify the existing VNet in order to add an additional subnet for the application gateway.

Step 1: In **Home > Virtual networks > AzureRA-Transit-VNet**, click **Subnets**.

Step 2: Click **Subnet**.

Step 3: In the **Name** box, enter **Transit-Public-AppGW**.

Step 4: In the **Address Range (CIDR block)** box, enter **10.110.128.0/24**, and then click **OK**.

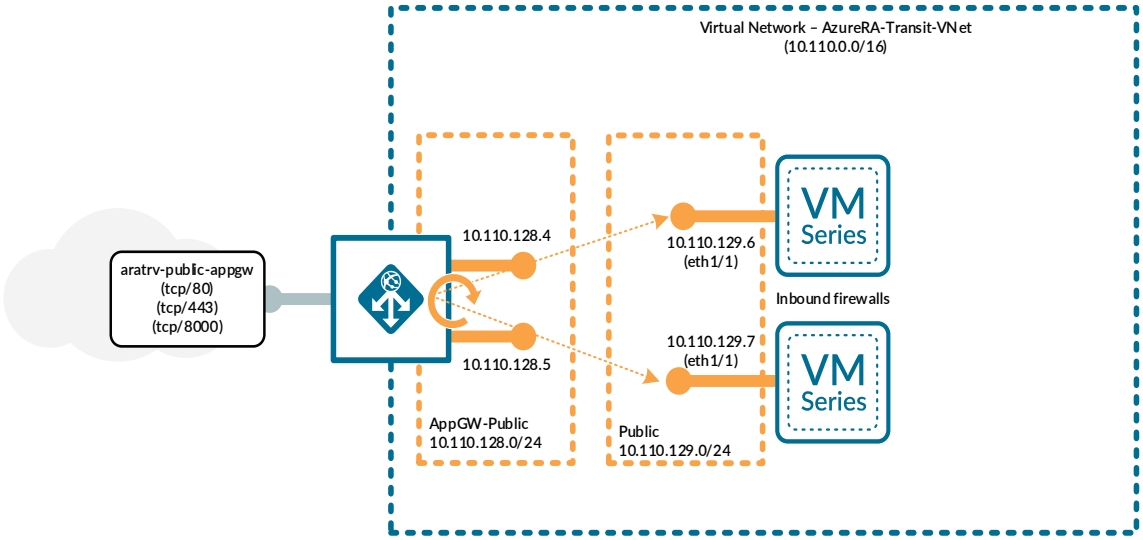
7.4 Create the Azure Application Gateway

This procedure creates an application gateway with a public front-end IP address and creates an HTTP listener on TCP/80. You can create additional listeners after creating the application gateway.

> **Note**
>
> This example does not use autoscaling and is explicitly configured for two instances only.

In this guide, Palo Alto Networks recommends that you use path-based rules in your application gateway configuration. You use application gateway rules to associate the front-end listeners with the HTTP/HTTPS back ends. Basic rules allow only a single HTTP/HTTPS back end for each listener. Use path-based rules to associate multiple HTTP/HTTPS back ends for a listener. A path-based rule includes both basic default settings and additional path-based exceptions within a single rule.

Figure 16 Azure application gateway



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

Step 2: In the **Resource group** list, choose **AzureRA-Transit**, and then click **OK**.

Step 3: In the **Application gateway name** box, enter **AzureRA-Transit-AppGW**.

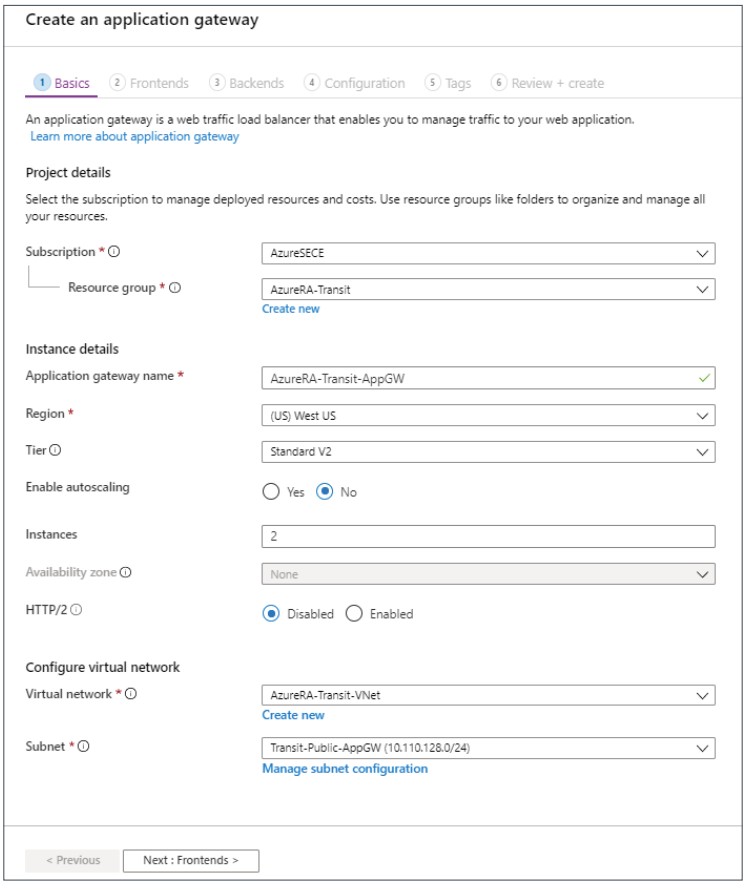
Step 4: In the **Region** list, choose **(US) West US**.

Step 5: In the **Tier** list, choose **Standard V2**.

Step 6: In the Enable autoscaling section, select **No**.

Step 7: In the Configure virtual network section, in the **Virtual network** list, choose **AzureRA-Transit-VNet**.

Step 8: In the Configure virtual network section, in the **Subnet** list, choose **Transit-Public-AppGW**, then click **Next: Frontends**.



Step 9: In the **Public IP address** list, choose **ARATRV- Public-AppGW**, and then click **Next: Backends**.

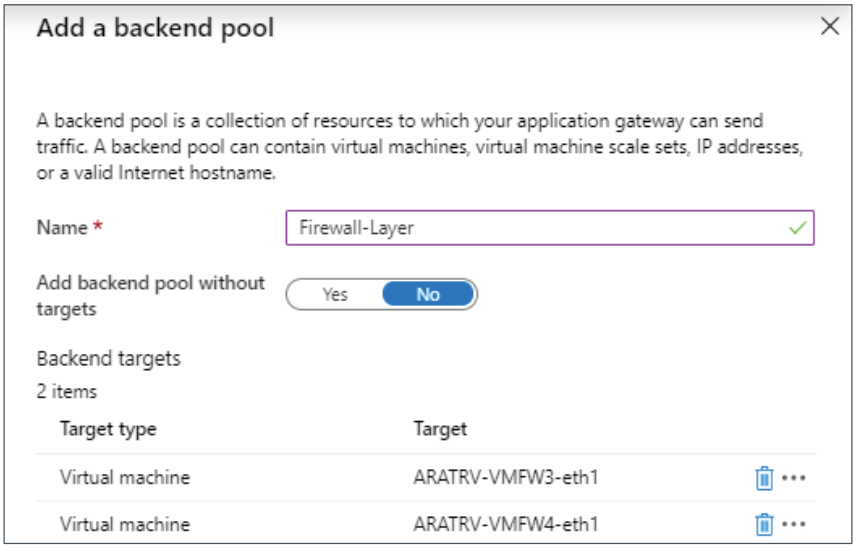
Step 10: Click **Add a backend pool**.

Step 11: In the **Name** box, enter **Firewall-Layer**.

Step 12: In the Backend targets section, in the **Target type** list, choose **Virtual machine**.

Step 13: In the Backend targets section, in the **Target** list, choose the VM-Series interface associated to the Transit-Public subnet for the inbound access traffic profile (example: **ARATRV-VMFW3-eth1**).

Step 14: Repeat Step 12 and Step 13 for all VM-Series firewalls that you are assigning to this back-end pool, and then click **Add**.



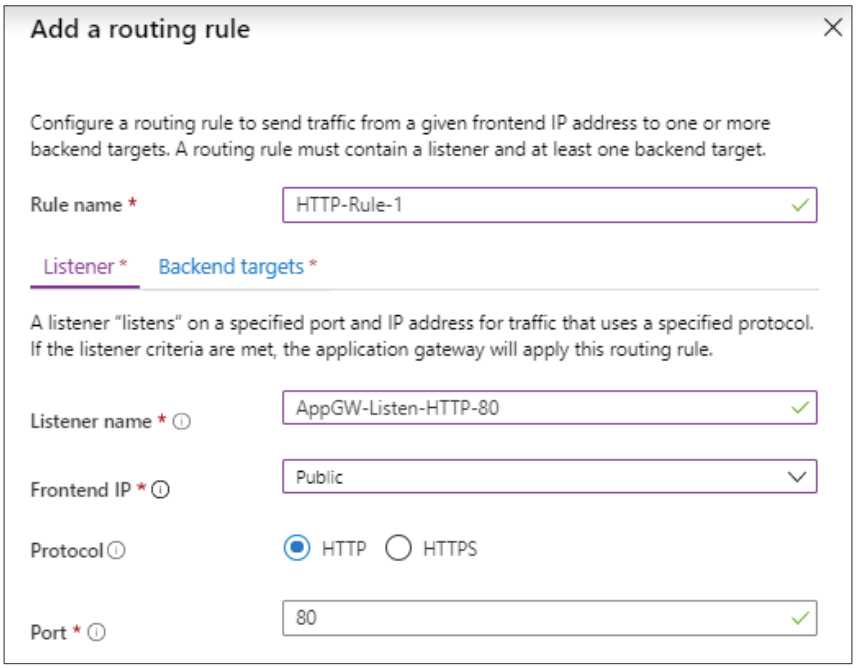
Step 15: Click **Next: Configuration**.

Step 16: In the Routing rules section, click **Add a rule**.

Step 17: In the **Rule name** box, enter **HTTP-Rule-1**.

Step 18: In the **Listener name** box, enter **AppGW-Listen-HTTP-80**.

Step 19: In the **Frontend IP** list, choose **Public**.



Step 20: Click **Backend targets**.

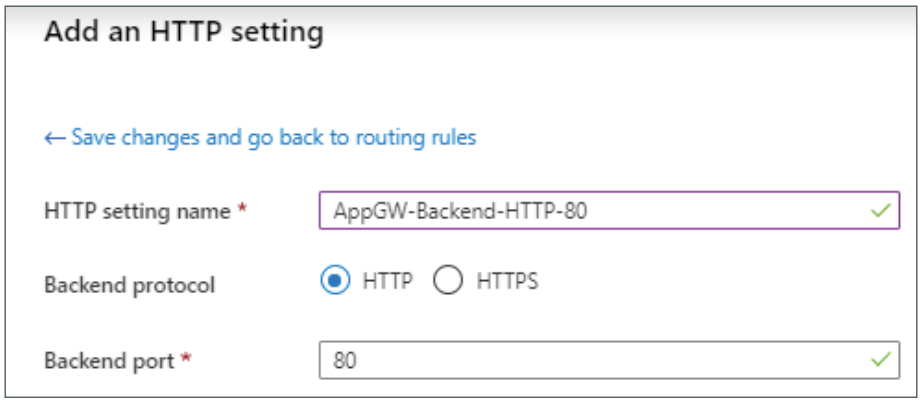
Step 21: In the **Backend target** list, choose **Firewall-Layer**.

Step 22: In the HTTP setting section, click **Create new**. The Add an HTTP setting pane appears.

Step 23: In the **HTTP setting name** box, enter **AppGW-Backend-HTTP-80**.

Step 24: In the **Backend port** box, enter **80**.

Step 25: Click **Save changes and go back to routing rules**. This closes the Add an HTTP setting pane.



Note

If you do not add additional targets at this time, the application gateway rule is created as a basic rule. You cannot convert a basic rule to a path-based rule.

Step 26: Click **Add multiple targets to create a path-based rule**.

Step 27: In the **Path** box, enter **/images/***.

Step 28: In the **Path rule name** box, enter **Images**.

Step 29: In the HTTP setting section, click **Create new**. The Add an HTTP setting pane appears.

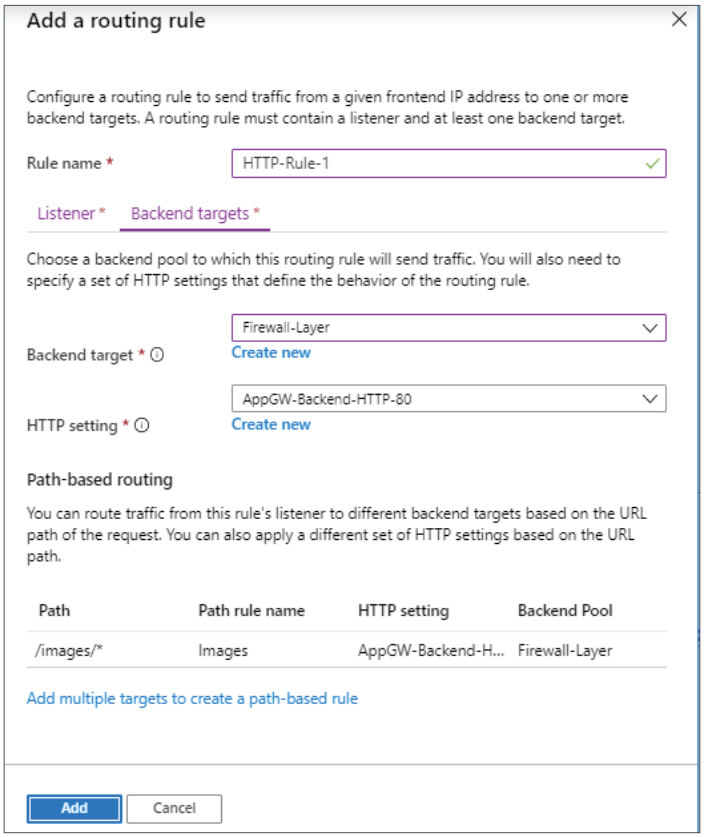
Step 30: In the **HTTP setting name** box, enter **AppGW-Backend-HTTP-8081**.

Step 31: In the **Backend port** box, enter **8081**.

Step 32: Click **Save changes and go back to routing rules**. This closes the Add an HTTP setting pane.

Step 33: In the Backend target list, choose **Firewall-Layer**, and then click **Add**.

Step 34: On the Add a routing rule pane, click **Add**.



Step 35: Click **Next: Tags**.

Step 36: On the next screen, click **Next: Review + create**.

Step 37: On the next screen, click **Create**.

7.5 Configure the Azure Application Gateway

Two configuration options are available for the application gateway:

- **Internal load balancer (Figure 17)**—You use a load-balancer front-end IP address for the application gateway back ends. Port-based NAT policy rules on the firewall translate any traffic from the application gateways to the firewall public interface IP address to the front-end IP of the internal load balancer. You also configure port mapping on the load balancer in order to direct traffic to the actual web server resources.
- **Without internal load balancer (Figure 18)**—You use web server resources for the application gateway back ends. 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.

In this procedure, you initially configure the application gateway with an internal load balancer. If you would like to use a direct-to-web-server configuration, you complete additional steps at the end of this procedure in order to modify the configuration.

Figure 17 Application gateway with internal load balancer

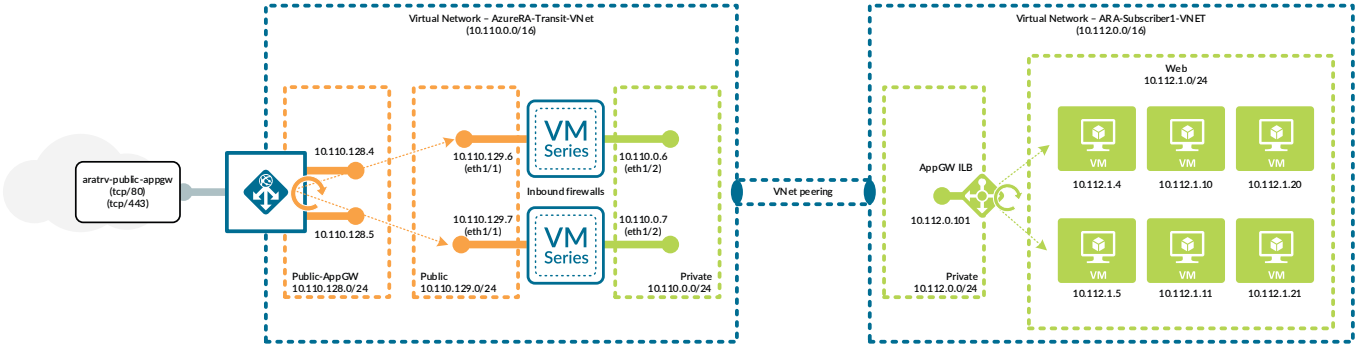


Figure 18 Application gateway without internal load balancer (direct to web server)

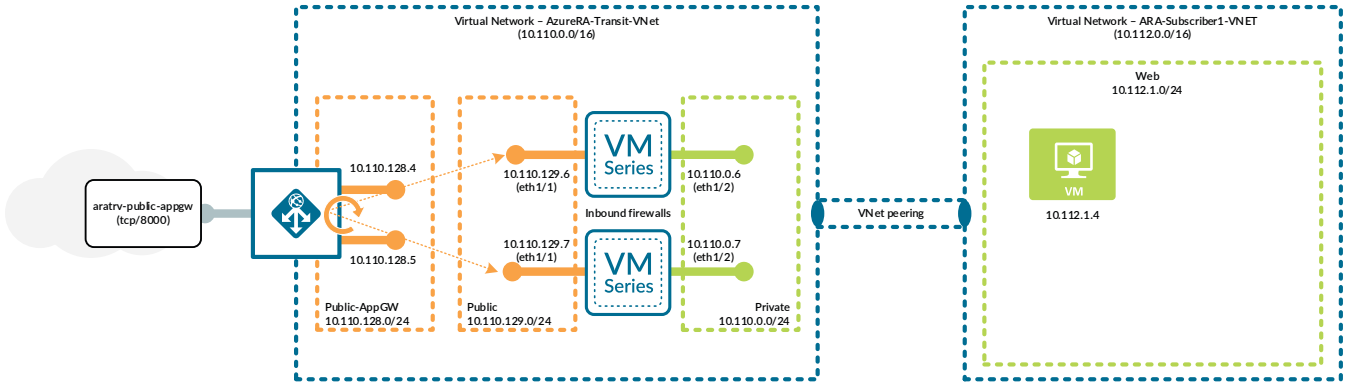


Table 23 Application gateway listeners

Listener name	Listener port	Protocol	Usage
AppGW-Listen-HTTP-80	80	HTTP	HTTP listener (already created during initial deployment).
AppGW-Listen-HTTP-8000	8000	HTTP	Direct to server, uses destination NAT on firewall. No load balancer required.
AppGW-Listen-HTTPS-443	443	HTTPS	SSL re-encryption and SSL offload

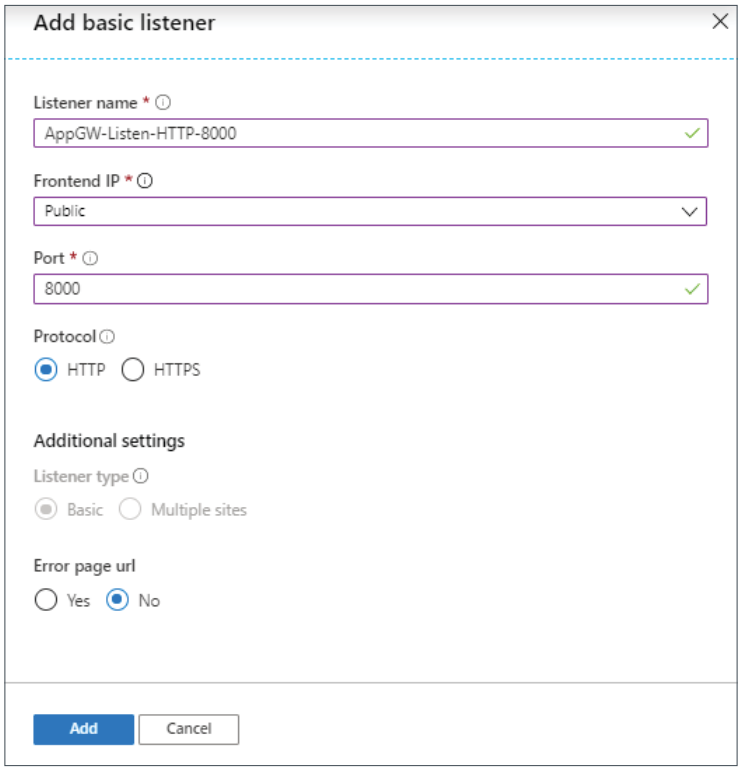
An additional HTTP listener for TCP/8000 is created to show the details for destination NAT configuration on the firewall that does not require the use of an internal load balancer.

Step 1: In **Home** > **Application Gateways** > **AzureRA-Transit-AppGW**, click **Listeners**, and then click **Basic**.

Step 2: In the **Name** box, enter **AppGW-Listen-HTTP-8000**.

Step 3: In the **Frontend IP** list, choose **Public**.

Step 4: In the **Port** box, enter **8000**, and then click **Add**.



Next, you add an additional HTTPS listener for TCP/443. SSL requires this listener. 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://aratrv-public-appgw.westus.cloudapp.azure.com, then you need a certificate with a subject alternate name for the FQDN *aratrv-public-appgw.westus.cloudapp.azure.com* or you need a wildcard certificate for **.westus.cloudapp.azure.com*.

Alternatively, if you have a DNS CNAME entry for your domain that maps *web.yourdomain.com* to *aratrv-public-appgw.westus.cloudapp.azure.com*, then you could use a certificate with a subject alternate name for the FQDN *web.yourdomain.com* or you could use a wildcard certificate for **.yourdomain.com*.

Step 5: In **Home** > **Application Gateways** > **AzureRA-Transit-AppGW**, click **Listeners**, and then click **Basic**.

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

Step 7: In the **Frontend IP** list, choose **Public**.

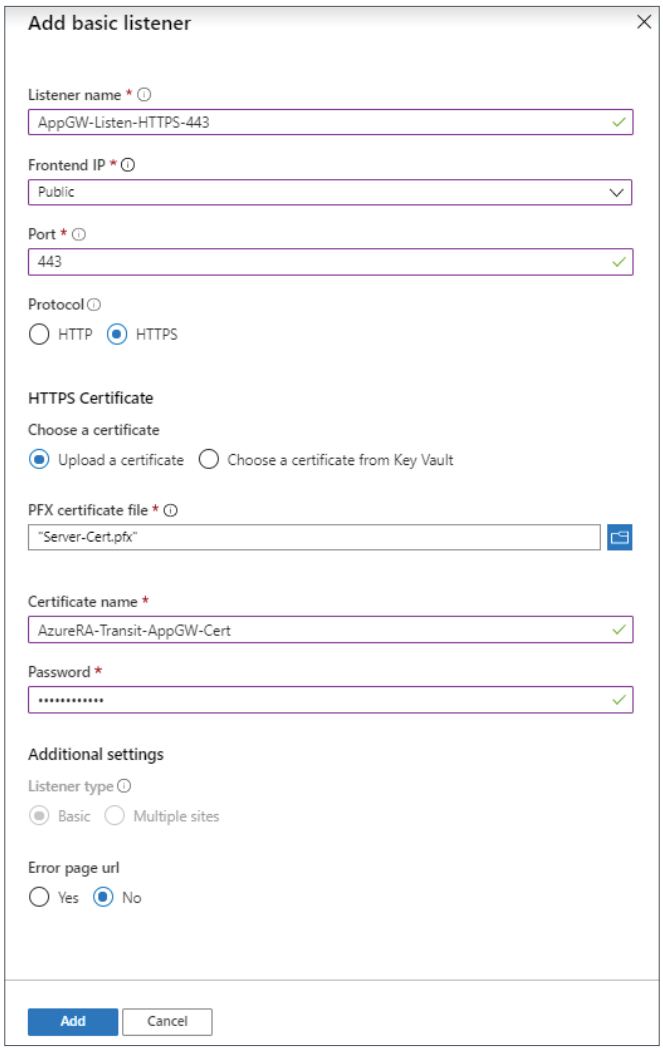
Step 8: In the Protocol section, select **HTTPS**. Verify that the value in the **Port** box updates to **443**.

Step 9: In the Choose a certificate section, select **Upload a certificate**.

Step 10: Next to the **PFX certificate file** box, click the browse icon, and then select the public web server certificate.

Step 11: In the **Certificate name** box, enter **AzureRA-Transit-AppGW-Cert**.

Step 12: In the certificate **Password** box, enter the certificate password, and then click **Add**.



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

By default, you create an HTTP back end on TCP/80 when you first deploy the application gateway, and you also create an additional HTTP back end when you add a path-based rule. Additional HTTP/HTTPS back ends are required for any other usages. Table 24 lists example usages and back ends. You have already created the first two entries in the table.

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

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

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

Table 24 HTTP/HTTPS back ends

Front-end listener (protocol/port)	Path	Usage	HTTP/HTTPS back end	HTTP/HTTPS back end (protocol/port)
HTTP/80	All	Default	AppGW-Backend-HTTP-80 (already created)	HTTP/80
HTTP/80	/images/*	URL path-based routing	AppGW-Backend-HTTP-8081 (already created)	HTTP/8081
HTTP/8000	All	Direct to web server (no internal load balancer 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 13: In **Home > Application gateways > AzureRA-Transit-AppGW**, click **HTTP settings**, and then click **Add**.

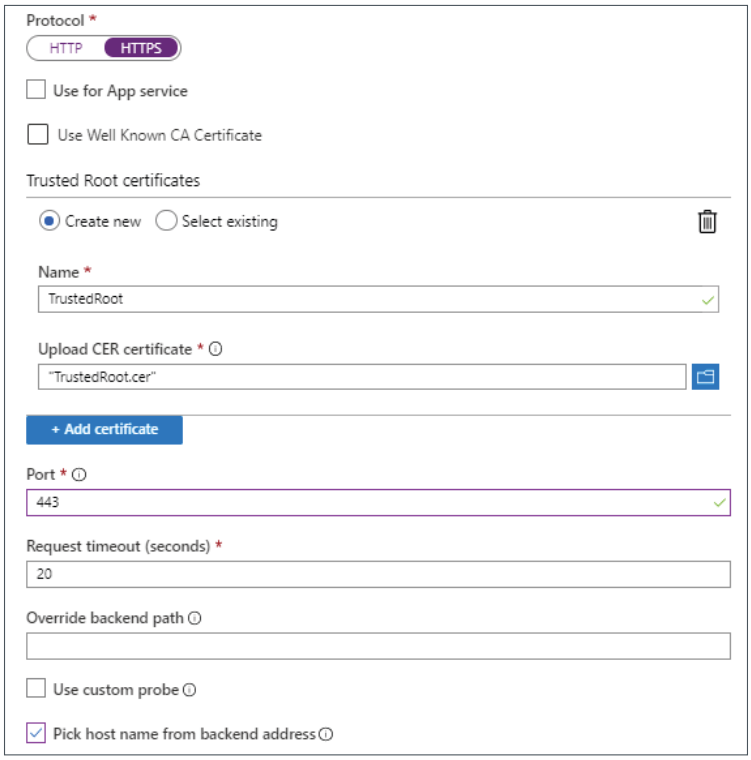
Step 14: In the **Name** box, enter **AppGW-Backend-HTTP-8000**.

Step 15: In the Protocol section, select **HTTP**.

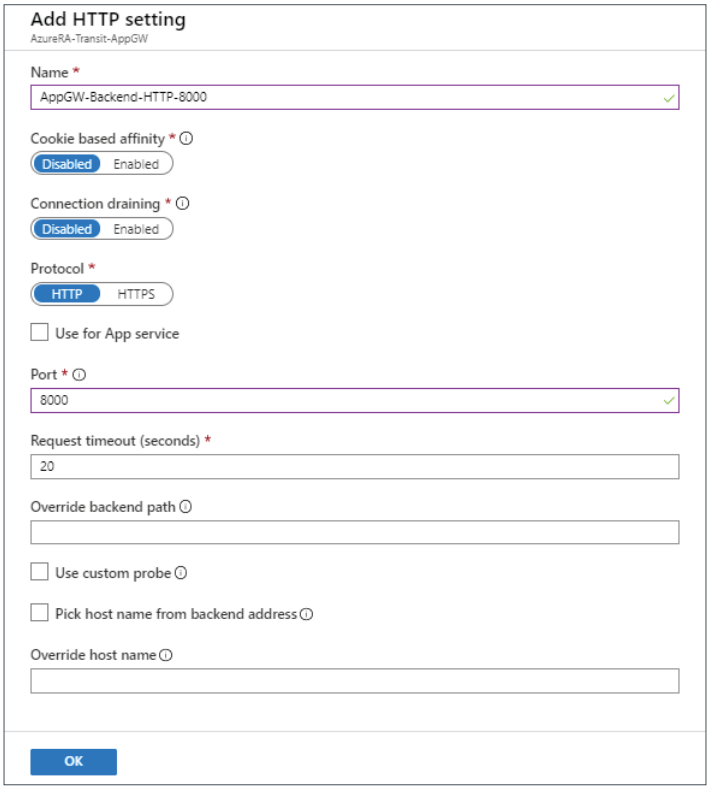
Step 16: If the back-end protocol is not HTTPS, skip to Step 17.

If back-end protocol is **HTTPS**, perform the following sub-steps:

- In the Trusted Root certificates section, select **Create new**.
- In the **Name** box, enter **TrustedRoot**.
- Next to the **Upload CER certificate** box, click the browse icon, and then select the trusted root certificate (example: **TrustedRoot.cer**).
- Select **Pick host name from backend address**.



Step 17: In the **Port** box, enter **8000**, and then click **OK**.



Step 18: Repeat Step 13 through Step 17 for all rows in Table 24.

Step 19: In **Home > Application gateways > AzureRA-Transit-AppGW**, click **Rules**.

Step 20: Click **Path-based**.

Step 21: In the **Name** box, enter **HTTPS-Rule-1**.

Step 22: In the **Listener** list, choose **AppGW-LISTEN-HTTPS-443**.

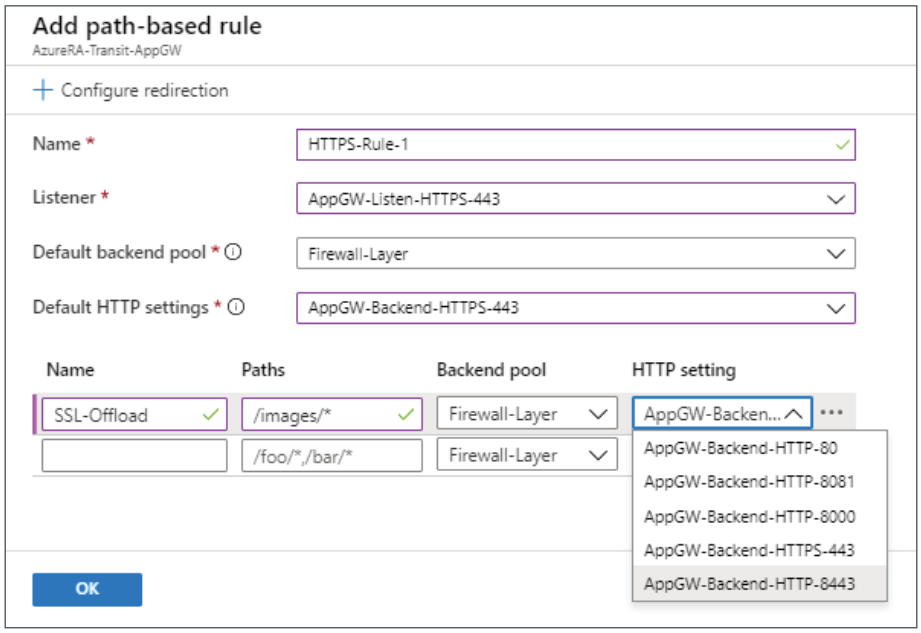
Step 23: In the **Default backend pool** list, choose **Firewall-Layer**.

Step 24: In the **Default HTTP settings** list, choose **AppGW-Backend-HTTPS-443**.

Step 25: In the path-based rule configuration section, perform the following sub-steps:

- In the **Name** box, enter **SSL-Offload**.
- In the **Paths** box, enter **/images/***.
- In the **Backend pool** list, choose **Firewall-Layer**.
- In the **HTTP setting** list, choose **AppGWBackend-HTTP-8443**.

Step 26: Click **OK**.



If you would like to use a direct-to-web-server configuration, complete Step 27 through Step 31. These steps provide an example of an application gateway basic rule for the direct web to server option.

Step 27: In **Home > Application gateways > AzureRA-Transit-AppGW**, click **Rules**, and then click **Basic**.

Step 28: In the **Name** box, enter **HTTP-Rule-2**.

Step 29: In the **Listener** list, choose **AppGW-Listen-HTTP-8000**.

Step 30: In the **Backend pool** list, choose **Firewall-Layer**.

Step 31: In the **HTTP setting** list, choose **AppGW-Backend-HTTP-8000**, and then click **OK**.

7.6 Create the Azure Inbound Internal Load Balancer for the Application Gateway

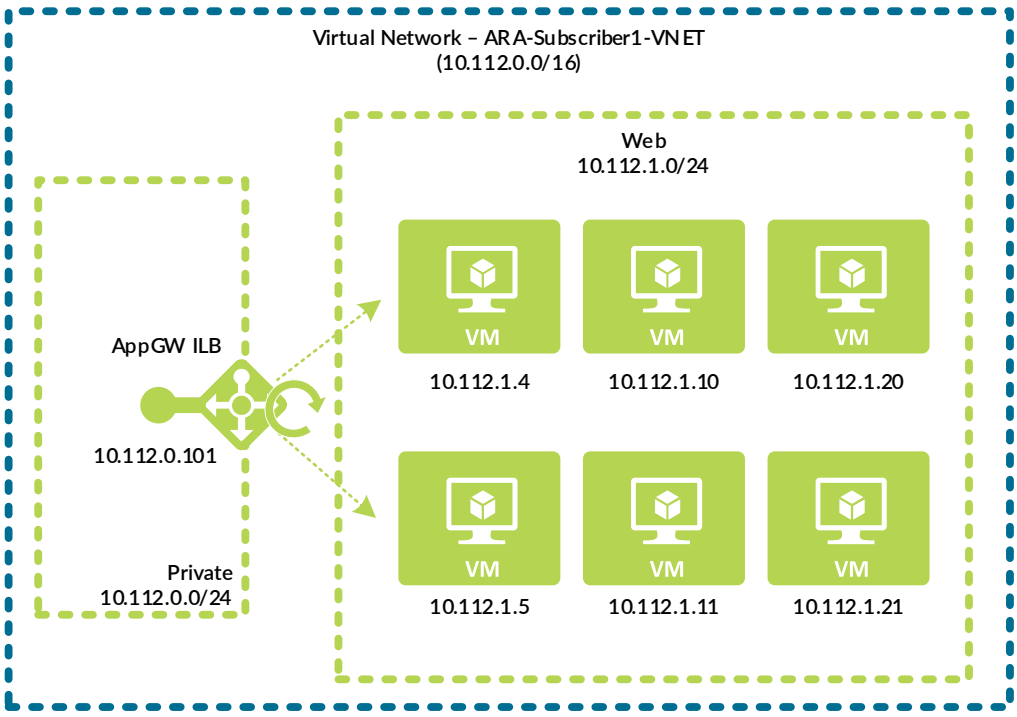
(Optional)

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 back end corresponds only to a single web server.

You create the Azure internal load balancer with a single private front-end IP address and associate it with the web server resources for the application gateway.

Figure 19 Internal load balancer for the application gateway



You use the front-end IP address as the NAT destination for the application gateway firewall rules.

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

Step 2: In the **Resource Group** list, choose **AzureRefArch-Subscriber-1**.

Step 3: In the **Name** box, enter **Subscriber1-AppGW-ILB**.

Step 4: In the **Region** list, choose **(US) West US**.

Step 5: In the Type section, select **Internal**.

Step 6: In the SKU section, select **Standard**.

Step 7: In the **Virtual network** list, choose **ARA-Subscriber1-VNET**.

Step 8: In the **Subnet** list, choose **Subscriber1-Private**.

Step 9: In the IP address assignment section, select **Static**.

Step 10: In the **Private IP address** box, enter **10.112.0.101**.

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

Step 11: Click **Review + create**, and then on the next screen, click **Create**.

7.7 Configure the Azure Inbound Internal Load Balancer for the Application Gateway

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

Table 25 Example internal load-balancer rules

Rule	Front-end IP	Back-end pool	Front-end port	Back-end pool	Pool members	Back-end port
AppGW-1	10.112.0.101	Web-Pool-1	TCP/80	Web-Pool-1	10.112.1.4 10.112.1.5	TCP/80
AppGW-2	10.112.0.101	Image-Pool-2	TCP/8081	Image-Pool-2	10.112.1.10 10.112.1.11	TCP/80
AppGW-3	10.112.0.101	Image-Pool-2	TCP/8443	Image-Pool-2	10.112.1.10 10.112.1.11	TCP/8443
AppGW-4	10.112.0.101	SSL-Pool-3	TCP/443	SSL-Pool-3	10.112.1.20 10.112.1.21	TCP/443

This example uses separate web server back-end pools for each usage: HTTP default, images, and SSL. You use the back-end pool for the image servers for cleartext HTTP access and for SSL offload. In this case, because there are two rules associated with the same back-end pool, the pool members must listen on multiple ports (TCP/80 and TCP/8443). You configure load-balancer health probes for all back-end web server ports.

Step 1: In **Home > Load Balancers > Subscriber1-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 > Subscriber1-AppGW-ILB**, click **Backend pools**.

Step 9: Click **Add**.

Step 10: In the **Name** box, enter **Web-Pool-1**.

Step 11: For each pool member listed for this back-end pool in Table 25, perform the following sub-steps:

- In the Virtual machines section, in the **Virtual machine** column, select a virtual machine that you are assigning to this back-end pool (example: **ARATRV-Sub1-Web1**).
- In the Virtual machines section, in the **IP address** column, select the **IP configuration** that is associated to the **Subscriber-1-Web** subnet (example: **ipconfig1**).
- Click **Add**.

Step 12: Repeat Step 9 through Step 11 for each back-end pool listed in Table 25.

Step 13: In **Home > Load Balancers > Subscriber1-AppGW-ILB**, click **Load balancing rules**.

Step 14: For each rule listed in Table 25, perform the following sub-steps:

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

USING PANORAMA TO CONFIGURE THE CENTRALIZED SECURITY POLICY AND NAT POLICY

This section includes the objects, NAT policy rules, and security policy rules for each of the following traffic profiles in the Transit VNet model:

- Outbound access traffic profile
- East-west traffic profile
- Inbound access traffic profile

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

You perform all procedures and steps in this section on Panorama.

Note

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

Procedures

8.1 Permit Azure Probes

You must permit health probes from the Azure load balancer on the firewall interfaces. The Azure load balancer sends probes at 3-second intervals, which would generate a significant amount of firewall log activity. This procedure creates a security policy rule that explicitly permits the probes and suppresses any logging from matches to the rule.

Palo Alto Networks recommends the use of an explicit rule to permit the probes instead of relying on the default intrazone rule. The rule permitting the probes 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://azurera-panorama-1.westus.cloudapp.azure.com).

Step 2: Navigate to **Objects**.

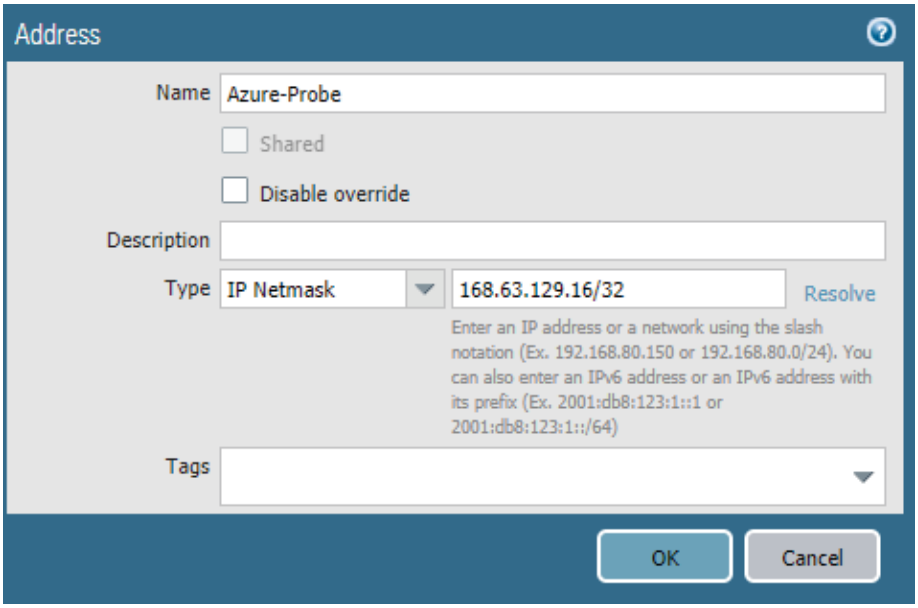
Step 3: In the **Device Group** list, choose **Transit-VNet**.

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

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

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

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



Step 8: Navigate to **Policies**.

Step 9: In the **Device Group** list, choose **Transit-VNet**.

Step 10: In **Policies > Security > Pre Rules**, click **Add**.

Step 11: In the **Name** box, enter **Permit Azure Probes and Suppress Logs**.

Step 12: In the **Rule Type** list, choose **intrazone**.

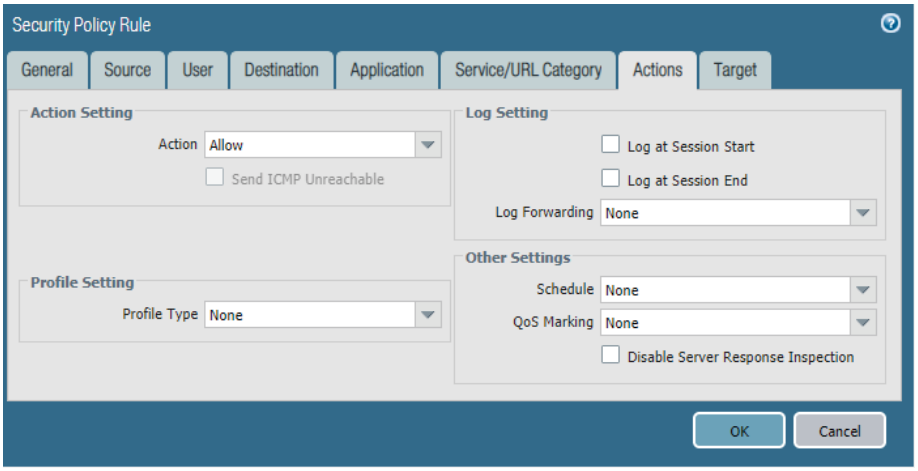
Step 13: On the Source tab, in the Source Zone pane, select **Any**.

Step 14: In the Source Address pane, click **Add**, and then select **Azure-Probe**.

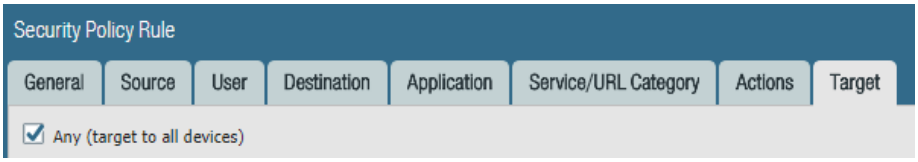
Step 15: In the Service/URL Category tab, in the Service pane, select **any**.

Step 16: On the Actions tab, in the Action Setting section, in the **Action** list, choose **Allow**.

Step 17: In the Log Setting section, clear **Log at Session End**.

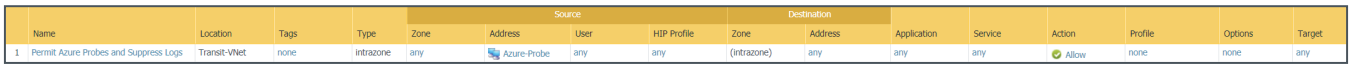


Step 18: On the Target tab, verify that **Any (target to all devices)** is selected, and then click **OK**.



Caution

Make sure to target all devices (any) in the device group. Otherwise, the policy rule is not automatically applied to new group members.



Step 19: On the **Commit** menu, click **Commit and Push**.

Procedures

Configuring the Outbound Access Traffic Profile

9.1 Create and Associate a Public IP Address with the Firewall

9.2 Create Address Objects

9.3 Configure the NAT Policy

9.4 Configure the Security Policy

9.1 Create and Associate a Public IP Address with the 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. You create a new public IP address for the public interface of each firewall used for outbound access. Azure network uses this IP address for traffic leaving the VNet.

Use Azure Resource Manager to complete this procedure.

Step 1: Sign in to Azure at https://portal.azure.com.

Step 2: In **Home > Public IP addresses**, click **Add**.

Step 3: In the SKU section, select **Standard**.

Step 4: In the **Name** box, enter **aratrv-vmfw1-outbound**.

Step 5: In the **DNS name label** box, enter **aratrv-vmfw1-outbound**.

Step 6: In the **Resource Group** list, choose **AzureRA-Transit**, and then click **Create**. You have successfully created the public IP address.

Step 7: In **Home > Public IP address > aratrv-vmfw1-outbound**, click **Associate**.

Step 8: In the Associate Public IP address pane, in the **Resource type** list, choose **Network interface**.

Step 9: In the Choose Network Interface pane, select the public interface of **ARATVR-VMFW1** (example: **ARATRV-VMFW1-eth1**), and then click **OK**.

Step 10: Repeat this procedure for any additional firewalls used for outbound access.

9.2 Create Address Objects

You create network objects in order to simplify the creation of NAT and security policy rules.

Table 26 Outbound traffic address objects

Object name	Description	Type	Type value
Net-10.112.0.0_16	Subscriber-1	IP Netmask	10.112.0.0/16
Net-10.113.0.0_16	Subscriber-2	IP Netmask	10.113.0.0/16

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

Step 2: Navigate to **Objects**.

Step 3: In the **Device Group** list, choose **Transit-VNet-OBEW**.

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

Step 5: In the **Name** box, enter **Net-10.112.0.0_16**.

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

Step 7: In the **Type value** box, enter **10.112.0.0/16**, and then click **OK**.

Step 8: Repeat Step 4 through Step 7 for all rows in Table 26.

9.3 Configure the 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://azurera-panorama-1.westus.cloudapp.azure.com).

Step 2: Navigate to **Policies**.

Step 3: In the **Device Group** list, choose **Transit-VNet-OBEW**.

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

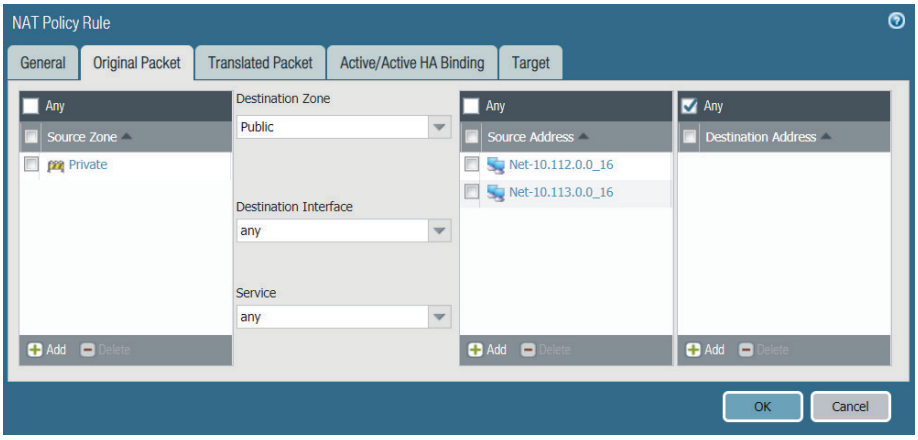
Step 5: In the **Name** box, enter **Outbound-Internet**.

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

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

Step 8: In the Source Address pane, click **Add**, and then select **Net-10.112.0.0_16**.

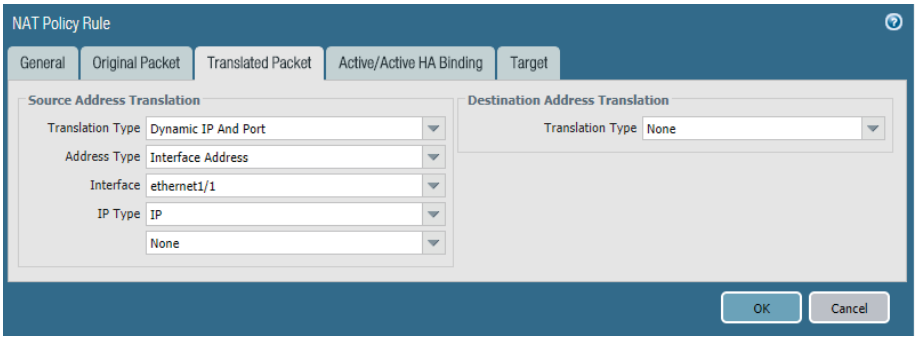
Step 9: Repeat Step 8 for all objects in Table 26.



Step 10: On the Translated Packet tab, in the Source Address Translation section, in the **Translation Type** list, choose **Dynamic IP And Port**.

Step 11: In the Source Address Translation section, in the **Address Type** list, choose **Interface Address**.

Step 12: In the Source Address Translation section, in the **Interface** list, choose **ethernet1/1**.



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 in the device group. Otherwise, the policy rule is not automatically applied to new group members.

9.4 Configure the 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://azurera-panorama-1.westus.cloudapp.azure.com).

Step 2: Navigate to **Policies**.

Step 3: In the **Device Group** list, choose **Transit-VNet-OBEW**.

Step 4: In **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 then select **Private**.

Step 7: In the Source Address pane, click **Add**, and then select **Net-10.112.0.0_16**.

Step 8: Repeat Step 7 for all objects in Table 26.

Step 9: On the Destination tab, in the Destination Zone pane, click **Add**, and then select **Public**.

Step 10: On the Application tab, in the Applications pane, click **Add**.

Step 11: In the search box, enter **web-browsing**, and then in the results list, choose **web-browsing**.

Step 12: In the Applications pane, click **Add**.

Step 13: In the search box, enter **ssl**, and then in the results list, choose **ssl**.

Step 14: In the Applications pane, click **Add**.

Step 15: In the search box, enter **google-base**, and then in the results list, choose **google-base**.

Step 16: On the Service/URL Category tab, in the **Service** pane, select **application-default**.

Step 17: On the Actions tab, in the Action Setting section, in the **Action** list, choose **Allow**.

Step 18: In the Log Setting section, in the **Log Forwarding** list, choose **CortexDL**.

Step 19: On the Target tab, verify that **Any (target to all devices)** is selected, and then click **OK**.

	Name	Location	Tags	Type	Source				Destination		Application	Service	Action	Profile	Options	Target
					Zone	Address	User	HIP Profile	Zone	Address						
2	Outbound-Internet	Transit-VNet-OBEW	none	universal	Private	Net-10.112.0.0_16 Net-10.113.0.0_16	any	any	Public	any	google-base ssl web-browsing	application-default	Allow	none		any

Caution

Make sure to target all devices (any) in the device group. Otherwise, the policy rule is not automatically applied to new group members.

Step 20: On the **Commit** menu, click **Commit and Push**.

Procedures

Configuring the East-West Traffic Profile

10.1 Configure Traffic between the Subscribers

10.1 Configure Traffic between the Subscribers

This procedure applies to traffic that originates from a virtual machine within a private subnet in a subscriber VNet and is destined to a virtual machine in a private subnet in a different subscriber VNet. You configure this traffic to route to the firewall through a user-defined route table applied to the source virtual machine's subnet.

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 peered VNets, 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 front-end IP and back-end pool. 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 9.2. 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 two subscriber subnets with each as a source to the other destination.

Table 27 East-west security policy rules (example)

Rule	Source	Destination
Sub1-to-Sub2	Net-10.112.0.0_16	Net-10.113.0.0_16
Sub2-to-Sub1	Net-10.113.0.0_16	Net-10.112.0.0_16

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://azurera-panorama-1.westus.cloudapp.azure.com).

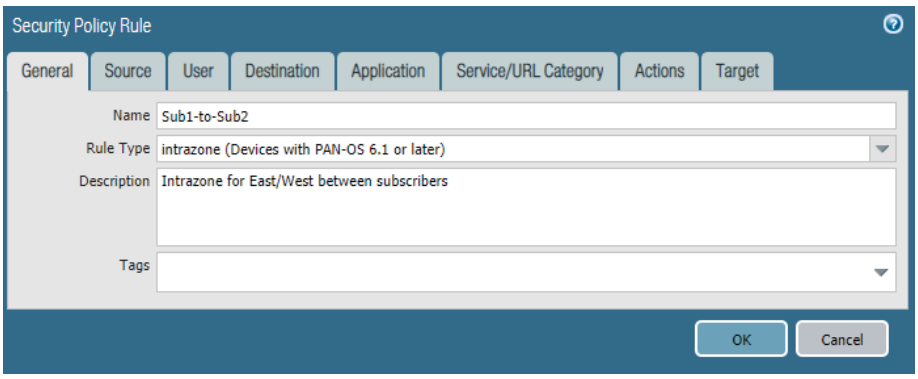
Step 2: Navigate to **Policies**.

Step 3: In the **Device Group** list, choose **Transit-VNet-OBEW**.

Step 4: In **Policies > Security > Pre Rules**, click **Add**.

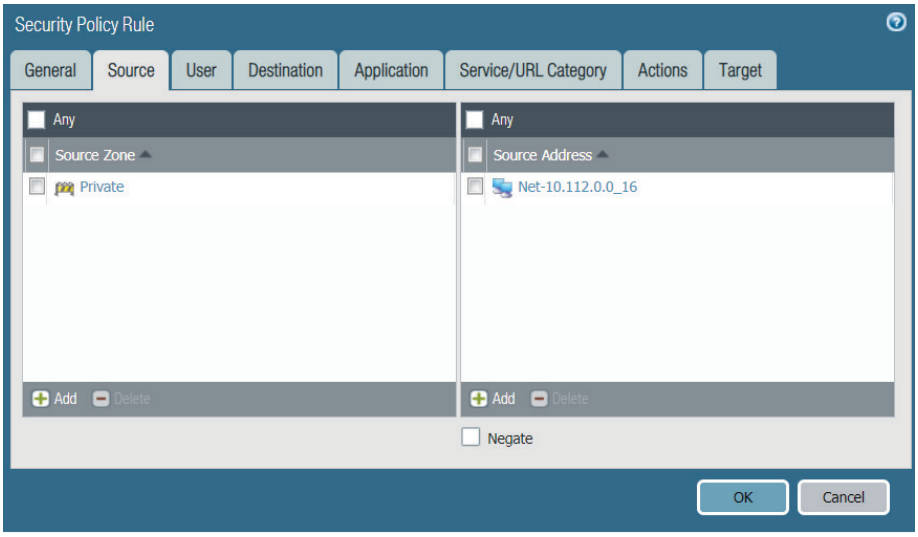
Step 5: In the **Name** box, enter **Sub1-to-Sub2**.

Step 6: In the **Rule Type** list, choose **intrazone**.

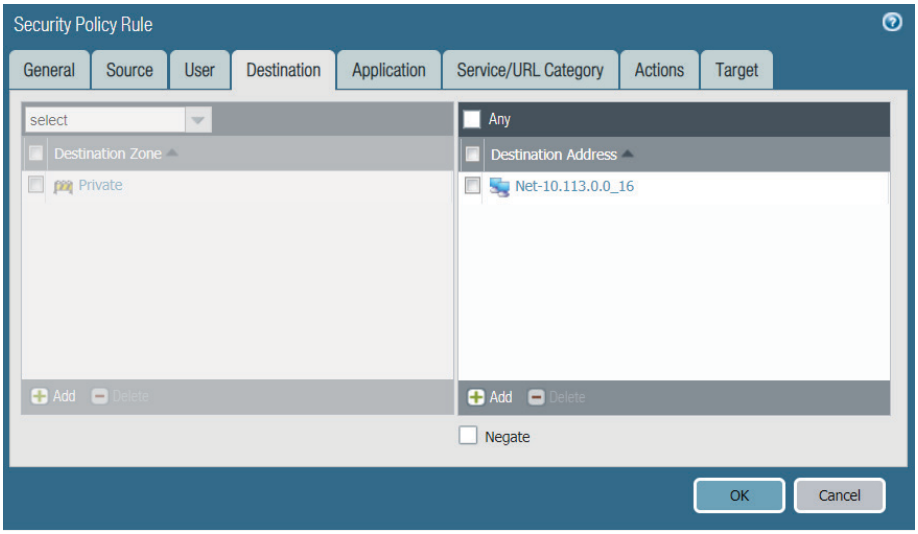


Step 7: On the Source tab, in the Source Zone pane, click **Add**, and then select **Private**.

Step 8: In the Source Address pane, click **Add**, and then select **Net-10.112.0.0_16**.



Step 9: On the Destination tab, in the Destination Address pane, click **Add**, and then select **Net-10.113.0.0_16**.



Step 10: On the Application tab, in the Applications pane, click **Add**.

Step 11: In the search box, enter **ssh**, and then in the results list, choose **ssh**.

Step 12: In the Applications pane, click **Add**.

Step 13: In the search box, enter **ms-rdp**, and then in the results list, choose **ms-rdp**.

Step 14: In the Applications pane, click **Add**.

Step 15: In the search box, enter **web-browsing**, and then in the results list, choose **web-browsing**.

Step 16: In the Applications pane, click **Add**.

Step 17: In the search box, enter **ssl**, and then in the results list, choose **ssl**.

Step 18: On the Service/URL Category tab, in the Service pane, select **application-default**.

Step 19: On the Actions tab, in the Action Setting section, in the **Action** list, choose **Allow**.

Step 20: In the Log Setting section, in the **Log Forwarding** list, choose **CortexDL**.

Step 21: 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 is not automatically applied to new group members.

Step 22: Repeat Step 4 through Step 21 for all rows in Table 27.

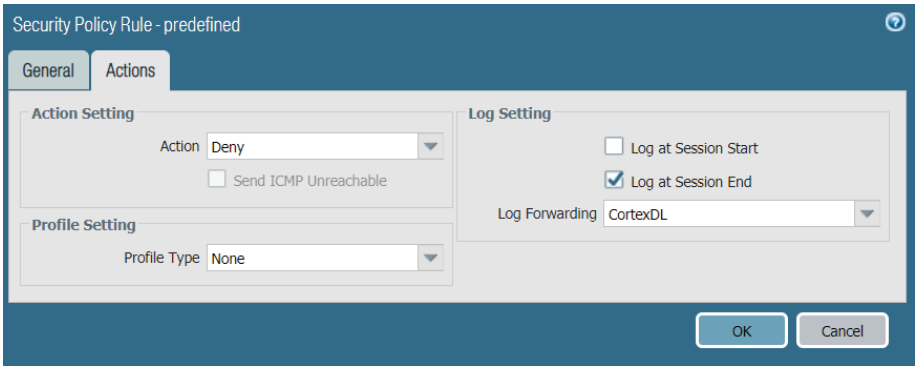
				Source		Destination							
	Name	Location	Type	Zone	Address	Zone	Address	Application	Service	Action	Profile	Options	Target
5	Sub1-to-Sub2	Transit-VNet-OBEW	intrazone	Private	Net-10.112.0.0_16	(intrazone)	Net-10.113.0.0_16	ms-rdp ssh ssl web-browsing	application-default	Allow	none		any
6	Sub2-to-Sub1	Transit-VNet-OBEW	intrazone	Private	Net-10.113.0.0_16	(intrazone)	Net-10.112.0.0_16	ms-rdp ssh ssl web-browsing	application-default	Allow	none		any

Step 23: In **Policies > Security > Default Rules**, select the row **intrazone-default**, and then click **Override**.

Step 24: On the **Actions** tab in the Action Setting section, in the **Action** list, choose **Deny**.

Step 25: In the Log Setting section, check **Log at Session End**.

Step 26: In the Log Setting section, in the **Log Forwarding** list, choose **CortexDL**, and then click **OK**.



Step 27: On the **Commit** menu, click **Commit and Push**.

Procedures

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

11.1 Create Address Objects

This procedure assumes that you have already deployed a set of web server resources in the Subscriber1-Server subnet. In a resilient web server model, the web servers are in a back-end pool of an Azure internal load balancer. Security and NAT policy rules reference the load-balancer front-end IP, which should be defined as an address object (example: **10.112.0.20**). This guide does not include the procedure to create this load balancer or to create the web server resources.

Table 28 Inbound traffic address objects

Object name	Description	Type	Type value
Web-Public-LB-FQDN	FQDN of public web server	FQDN	aratrv-public-web.westus.cloudapp.azure.com
Web-Private-LB	IP address of private internal load balancer in Subscriber-1 VNet	IP Netmask	10.112.0.20/32

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

Step 2: Navigate to **Objects**.

Step 3: In the **Device Group** list, choose **Transit-VNet-Inbound**.

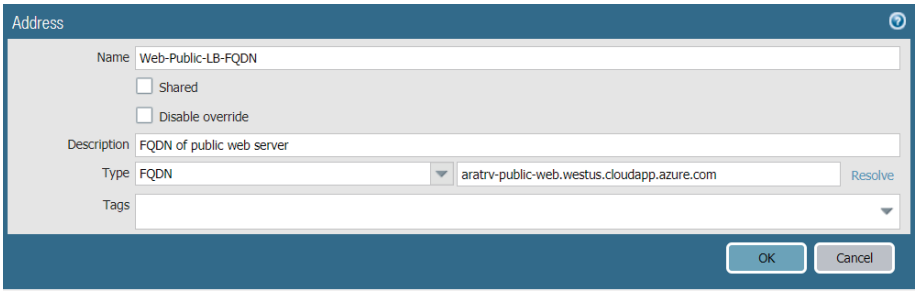
Step 4: In **Objects > Addresses**, click **Add**.

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

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

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

Step 8: Repeat Step 4 through Step 7 for all rows in Table 28.



11.2 Configure the 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://azurera-panorama-1.westus.cloudapp.azure.com).

Step 2: Navigate to **Policies**.

Step 3: In the **Device Group** list, choose **Transit-VNet-Inbound**.

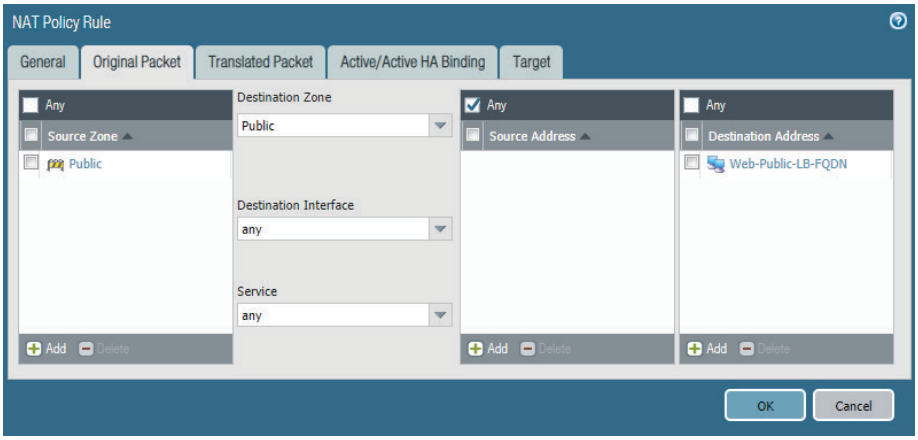
Step 4: In **Policies > NAT > Pre Rules**, click **Add**.

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

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

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

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



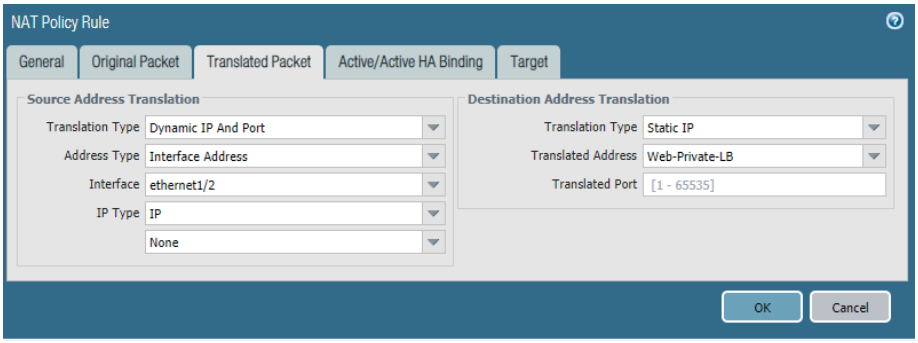
Step 9: On the Translated Packet tab, in the Source Address Translation section, in the **Translation Type** list, choose **Dynamic IP And Port**.

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

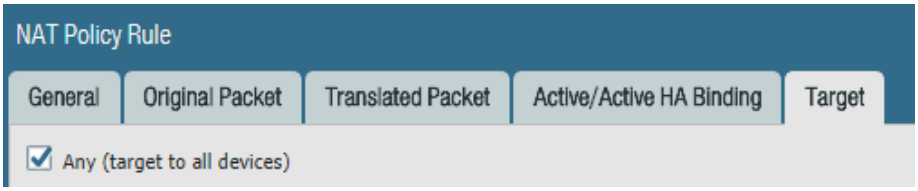
Step 11: In the Source Address Translation section, in the **Interface** list, choose **ethernet1/2**.

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

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



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



Caution

Make sure to target all devices in the device group. Otherwise, the policy rule is not automatically applied to new group members.

11.3 Configure the 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 traffic profile permits these applications:

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

Add additional applications to your policy as required.

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

Step 2: Navigate to **Policies**.

Step 3: In the **Device Group** list, choose **Transit-VNet-Inbound**.

Step 4: In **Policies > Security > Pre Rules**, click **Add**.

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

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

Step 7: On the Destination tab, in the Destination Zone pane, click **Add**, and then select **Private**.

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

Step 9: On the Application tab, in the Applications pane, click **Add**.

Step 10: In the search box, enter **web-browsing**, and then in the results list, choose **web-browsing**.

Step 11: In the Applications pane, click **Add**.

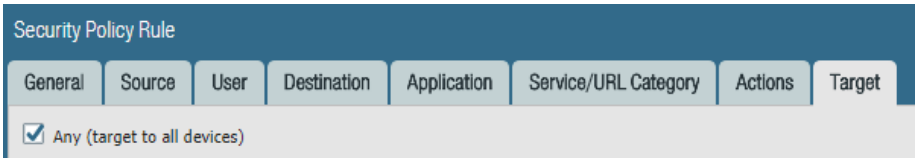
Step 12: In the search box, enter **ssl**, and then in the results list, choose **ssl**.

Step 13: On the Service/URL Category tab, in the Service pane, select **application-default**.

Step 14: On the Actions tab, in the Action Setting section, in the **Action** list, choose **Allow**.

Step 15: In the Log Setting section, in the **Log Forwarding** list, choose **CortexDL**.

Step 16: 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 is not automatically applied to new group members.

Step 17: On the **Commit** menu, click **Commit and Push**.

Procedures

Configuring the Inbound Access Traffic Profile (Application Gateway Option)

12.1 Enable XFF

12.2 Create Address Objects

12.3 Configure the NAT Policy

12.4 Configure the Security Policy

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

12.1 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.

Note

Palo Alto Networks recommends that you review and install the most recent application and content updates. If your Panorama system is running with a more recent content release than your VM-Series devices, the URL filtering profile created in this procedure may contain new URL filtering categories. When you commit and push the configuration, these categories may not be recognized on the VM-Series devices running older content releases and the commit fails.

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

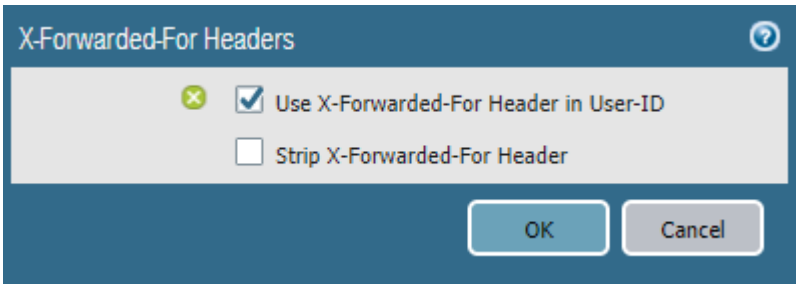
Step 2: Navigate to **Device**.

Step 3: In the **Template** list, choose **Transit-2-Zone-Inbound**.

Step 4: Navigate to **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 **Objects**.

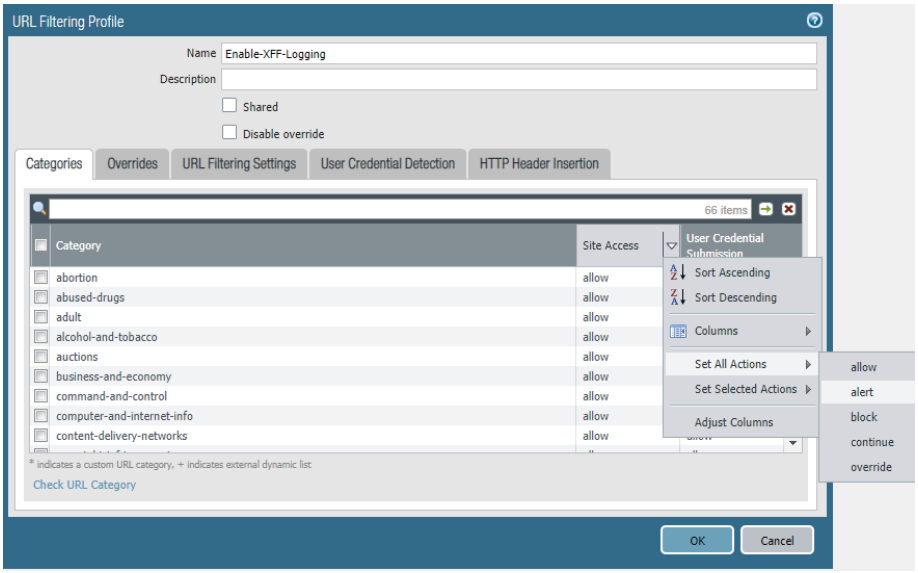
Step 8: In the **Device Group** list, choose **Transit-VNet-Inbound**.

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

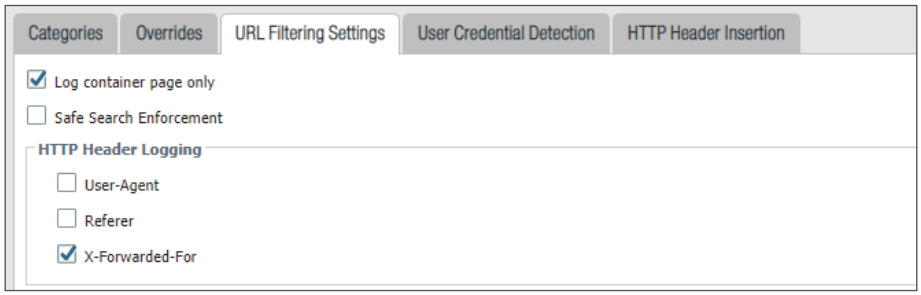
Step 10: In the URL Filtering Profile pane, in the **Name** box, enter **Enable-XFF-Logging**.

Step 11: In the **Site Access** column, click the down arrow, and then select **Set All Actions > alert**. This sets all categories to alert.

> **Note**
>
> URL filtering logs are not generated if the Site Access category action is *allow*. Palo Alto Networks suggests that you initially configure all categories to *alert*.
>
> The application gateway health probes generate a significant amount of log messages with the category of private-ip-address. You can set the Site Access category action for this category to *allow* in order to suppress these messages.



Step 12: On the URL Filtering Settings tab, in the HTTP Header Logging section, select **X-Forwarded-For**, and then click **OK**.



12.2 Create Address Objects

You create address objects for the NAT policy rules and Security policy rules to simplify the creation of the rules in following procedures.

Palo Alto Networks recommends that you use a subnet range to match the application gateway instances because Azure dynamically assigns an IP address for each application gateway instance but does not provide details of which addresses are assigned. If you use a subnet range, you can easily add additional application gateway instances (manually or autoscaled) without having to modify your firewall policies.

This procedure assumes that you have already deployed a set of web server resources in the Subscriber1-Server subnet. In a resilient web server model, the web servers are in a back-end pool of an Azure internal load balancer. The load-balancer front-end IP is referenced by security and NAT policy rules and should be defined as an address object (example: **10.112.0.101**).

Table 29 Inbound traffic address objects

Object name	Description	Type	Type value
ARATRV-VMFW3-Public	Public subnet interface of first inbound firewall (ARATRV-VMFW3 ethernet1/1)	IP Netmask	10.110.129.6/32
ARATRV-VMFW4-Public	Public subnet interface of first inbound firewall (ARATRV-VMFW4 ethernet1/1)	IP Netmask	10.110.129.7/32
AppGW-Subnet	Application gateway subnet (matches all instances)	IP Netmask	10.110.128.0/24
AppGW-Internal-LB	IP address of AppGW internal load balancer	IP Netmask	10.112.0.101/32
Direct-Web	IP address of web server resource (does not require internal load balancer)	IP Netmask	10.112.1.4/32

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

Step 2: Navigate to **Objects**.

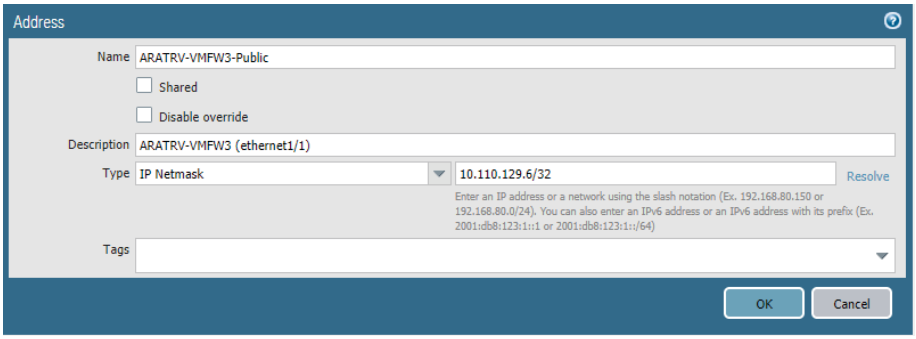
Step 3: In the **Device Group** list, choose **Transit-VNet-Inbound**.

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

Step 5: In the **Name** box, enter **ARATRV-VMFW3-Public**.

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

Step 7: In the **Type value** box, enter **10.110.129.6/32**, and then click **OK**.



Step 8: Repeat Step 4 through Step 7 for all rows in Table 29.

12.3 Configure the 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.

You configure the application gateway 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, you create a custom service for each non-standard port that is not predefined. The configuration example in this guide uses the destination ports as listed in Table 30.

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 30 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://azurera-panorama-1.westus.cloudapp.azure.com).

Step 2: Navigate to **Objects**.

Step 3: In the **Device Group** list, choose **Transit-VNet-Inbound**.

Step 4: In **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 30.

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 31 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 back end as specified in Table 24 must have a corresponding NAT translation rule on each firewall. The firewall that corresponds to a back-end resource in the private networks maps the original packet service (or destination TCP port) to a translated address and translated port. These resources can be either load-balancer front-ends or actual servers. You already created address objects for the back-end resources in Procedure 12.2.

Table 31 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-Subnet	ARATRV-VMFW3-Public	AppGW-Internal-LB/80	ARATRV-VMFW3
Inbound-AppGW-FW-2_HTTP-80	service-http	AppGW-Subnet	ARATRV-VMFW4-Public	AppGW-Internal-LB/80	ARATRV-VMFW4
Inbound-AppGW-FW-1_HTTP-8000	service-http-8000	AppGW-Subnet	ARATRV-VMFW3-Public	Direct-Web/80	ARATRV-VMFW3
Inbound-AppGW-FW-2_HTTP-8000	service-http-8000	AppGW-Subnet	ARATRV-VMFW4-Public	Direct-Web/80	ARATRV-VMFW4
Inbound-AppGW-FW-1_HTTP-8081	service-http-8081	AppGW-Subnet	ARATRV-VMFW3-Public	AppGW-Internal-LB/8081	ARATRV-VMFW3
Inbound-AppGW-FW-2_HTTP-8081	service-http-8081	AppGW-Subnet	ARATRV-VMFW4-Public	AppGW-Internal-LB/8081	ARATRV-VMFW4
Inbound-AppGW-FW-1_HTTPS-443	service-https	AppGW-Subnet	ARATRV-VMFW3-Public	AppGW-Internal-LB/443	ARATRV-VMFW3
Inbound-AppGW-FW-2_HTTPS-443	service-https	AppGW-Subnet	ARATRV-VMFW4-Public	AppGW-Internal-LB/443	ARATRV-VMFW4
Inbound-AppGW-FW-1_HTTP-8443	service-http-8443	AppGW-Subnet	ARATRV-VMFW3-Public	AppGW-Internal-LB/8443	ARATRV-VMFW3
Inbound-AppGW-FW-2_HTTP-8443	service-http-8443	AppGW-Subnet	ARATRV-VMFW4-Public	AppGW-Internal-LB/8443	ARATRV-VMFW4

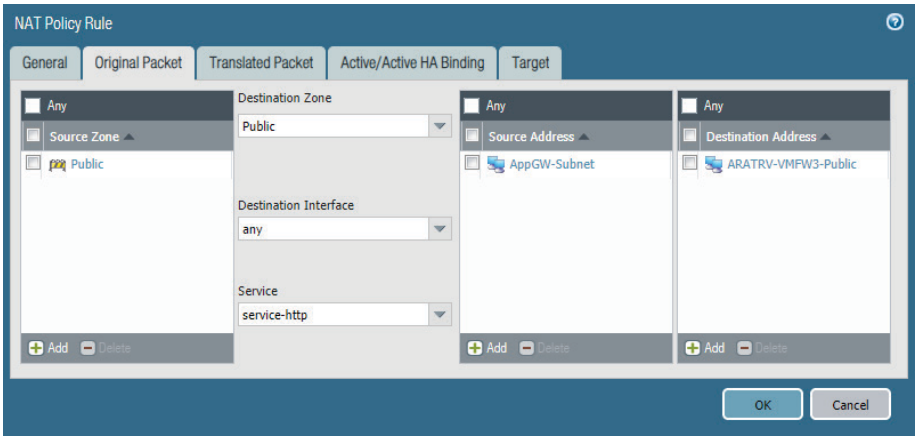
Step 8: Log in to Panorama (example: https://azurera-panorama-1.westus.cloudapp.azure.com).

Step 9: Navigate to **Policies**.

Step 10: In the **Device Group** list, choose **Transit-VNet-Inbound**.

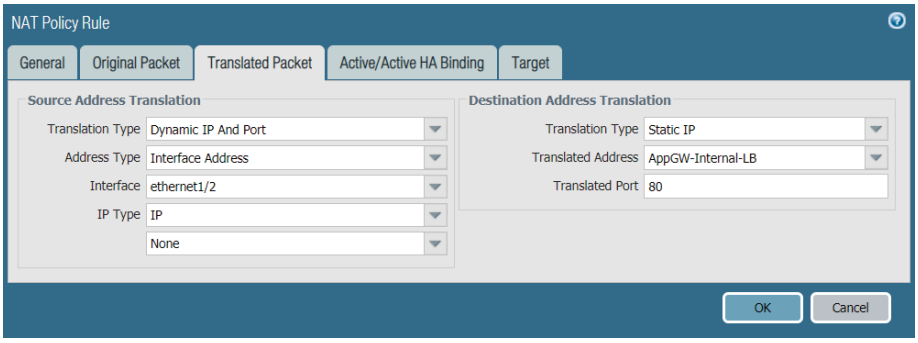
Step 11: For each entry in Table 31, perform the following sub-steps:

- In **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 then select **Public**.
- In the **Destination Zone** list, choose **Public**.
- In the **Service** list, choose **service-http**.
- In the Source Address pane, click **Add**, and then select **AppGW-Subnet**.
- In the Destination Address pane, click **Add**, and then enter **ARATRV-VMFW3-Public**.

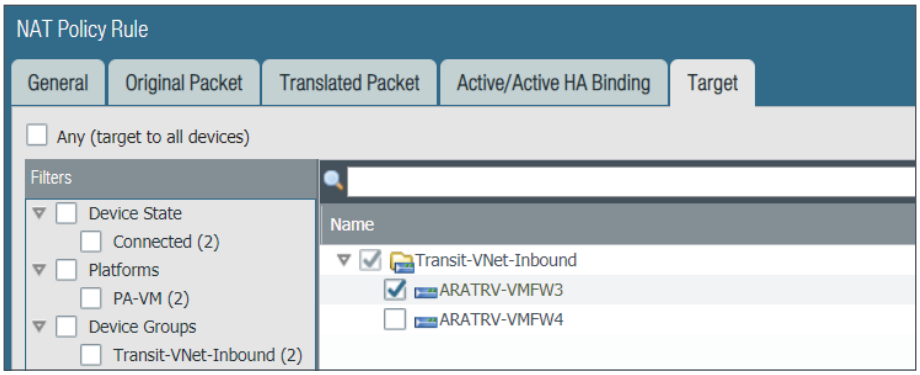


- On the Translated Packet tab, in the Source Address Translation section, in the **Translation Type** list, choose **Dynamic IP And Port**.
- In the Source Address Translation section, in the **Address Type** list, choose **Interface Address**.
- In the Source Address Translation section, in the **Interface list**, choose **ethernet1/2**.
- In the Destination Address Translation section, in the **Translation Type** list, choose **Static IP**.
- In the Destination Address Translation section, in the **Translated Address** list, choose **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: **ARATRV-VMFW3**), 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 policies. The target for each set of rules lists only one firewall.

Figure 20 NAT policy rules for the first firewall

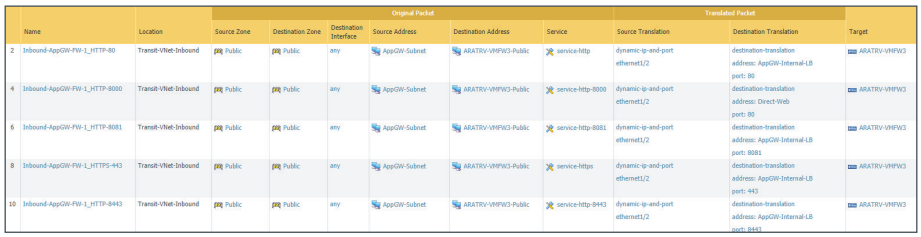
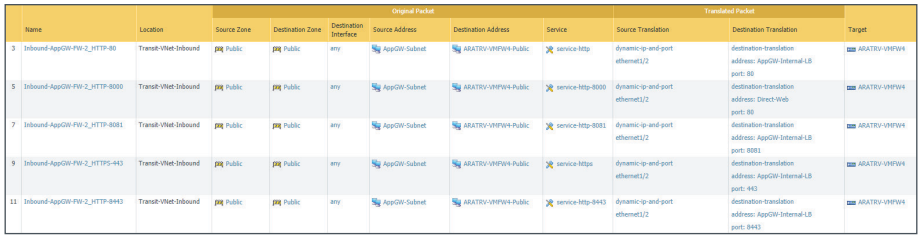


Figure 21 NAT policy rules for the second firewall



12.4 Configure the 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. In Step 6, the destination address must match the IP address of the public interface of each firewall. Table 32 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 32 Security policy rules for the application gateway

Name	Source object	Destination address	Target firewall
Inbound-AppGW-FW-1	AppGW-Subnet	ARATRV-VMFW3-Public	ARATRV-VMFW3
Inbound-AppGW-FW-2	AppGW-Subnet	ARATRV-VMFW4-Public	ARATRV-VMFW4

Step 1: In **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 then select **Public**.

Step 4: In the Source Address pane, click **Add**, and then select **AppGW-Subnet**.

Step 5: On the Destination tab, in the Destination Zone pane, click **Add**, and then select **Private**.

Step 6: In the Destination Address pane, click **Add**, and then enter **ARATRV-VMFW3-Public**.

Step 7: On the Application tab, in the Applications pane, click **Add**.

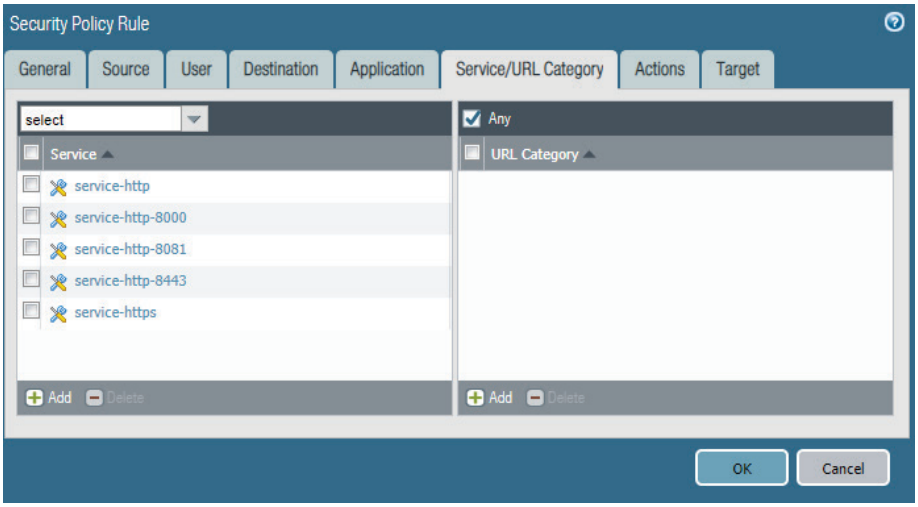
Step 8: In the search box, enter **web-browsing**, and then in the results list, choose **web-browsing**.

Step 9: In the Applications pane, click **Add**.

Step 10: In the search box, enter **ssl**, and then in the results list, choose **ssl**.

Next, you configure the application gateway 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, you must explicitly list each service in use.

Step 11: On the Service/URL Category tab, in the Service pane, click **Add**, and then select each service listed in Table 30.



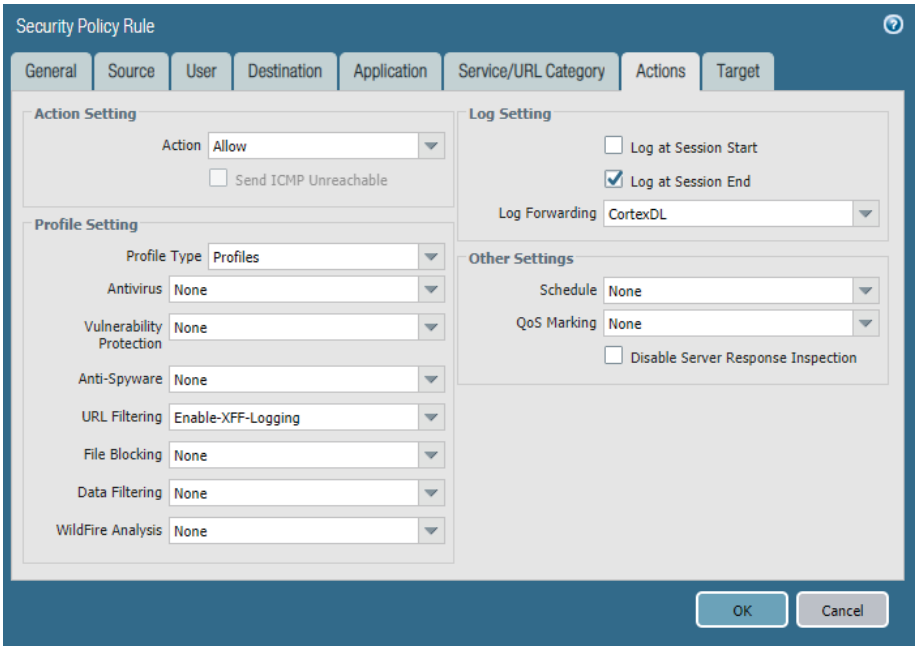
Step 12: On the Actions tab, in the Action Setting section, in the **Action** list, choose **Allow**.

> **Note**
>
> You must modify the default settings for the firewall's URL filtering log in order to view the XFF header information for sessions. Navigate to **Monitor > Logs > URL Filtering**, add the X-Forwarded-For column to the default view, and then rearrange the column order.

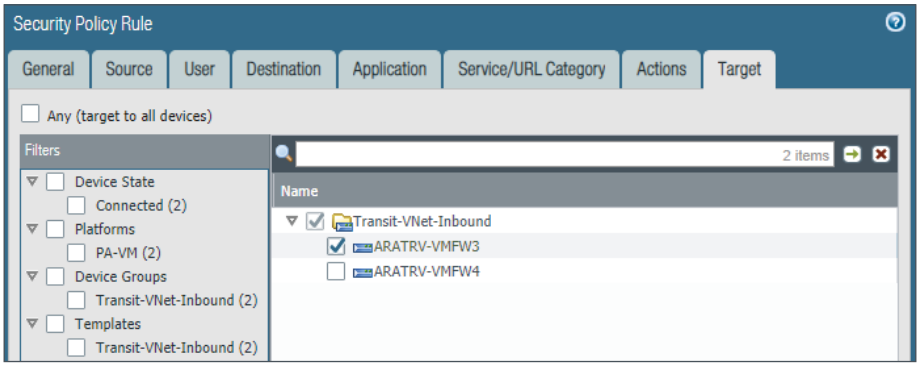
Step 13: In the Profile Setting section, in the **Profile Type** list, choose **Profiles**.

Step 14: In the Profile Setting section, in the **URL Filtering** list, choose **Enable-XFF-Logging**.

Step 15: In the Log Setting section, in the **Log Forwarding** list, choose **CortexDL**.



Step 16: On the Target tab, select only the firewall target from the current entry in the table (example: **ARATRV-VMFW3**), 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 policies. The target for each rule lists only one firewall.

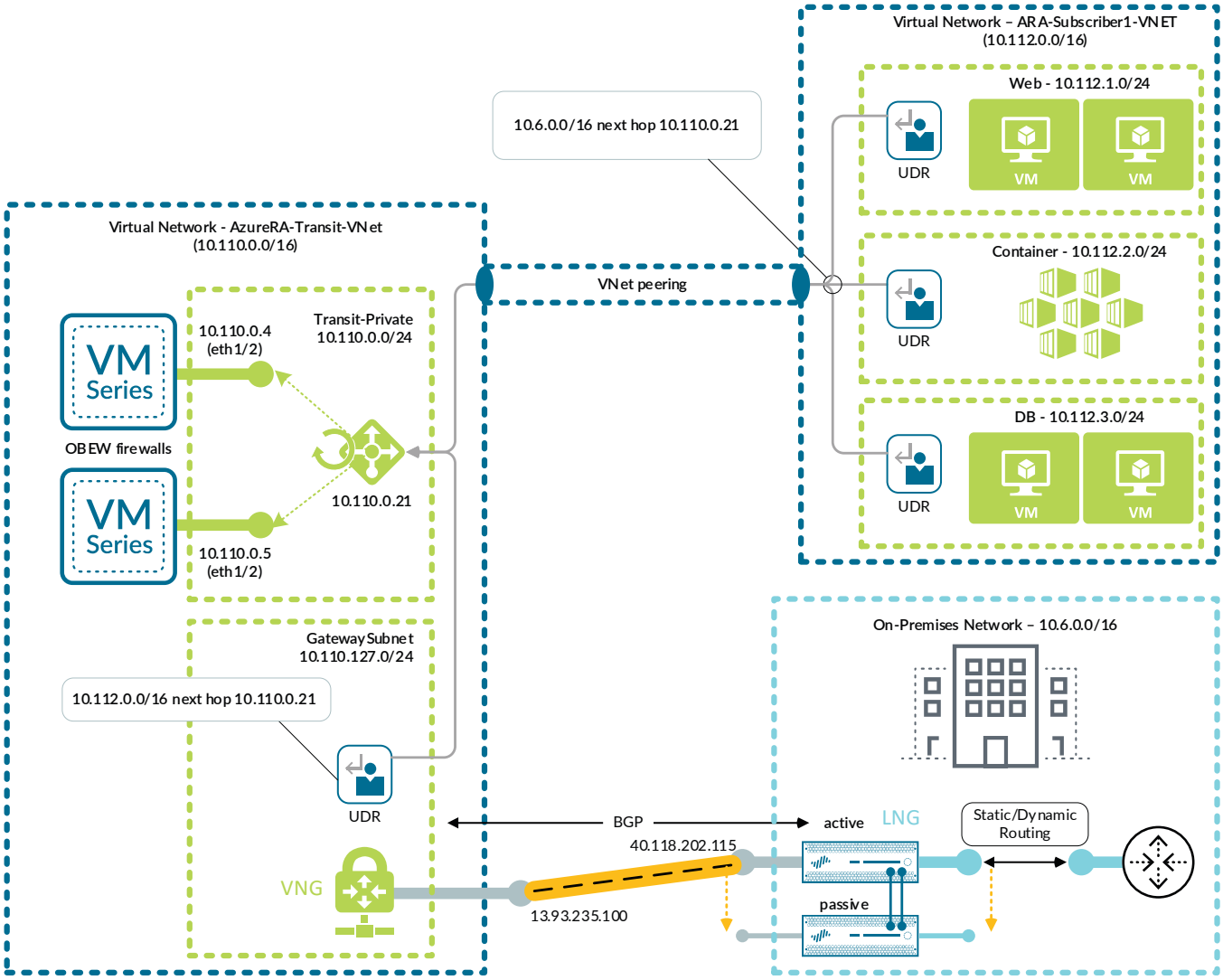
	Name	Location	Type	Source Zone	Source Address	Destination Zone	Destination Address	Application	Service	Action	Profile	Options	Target
3	Inbound-AppGW-FW-1	Transit-VNet-Inbound	universal	Public	AppGW-Subnet	Private	ARATRV-VMFW3-Public	ssl web-browsing	service-http service-http-8000 service-http-8081 service-http-8443 service-https	Allow			ARATRV-VMFW3
4	Inbound-AppGW-FW-2	Transit-VNet-Inbound	universal	Public	AppGW-Subnet	Private	ARATRV-VMFW4-Public	ssl web-browsing	service-http service-http-8000 service-http-8081 service-http-8443 service-https	Allow			ARATRV-VMFW4

Step 17: On the **Commit** menu, click **Commit and Push**.

Deployment Details for a Backhaul Connection

Use the procedures in this chapter to build an IPSec VPN connection for backhaul traffic between the Azure transit VNet and your on-premises network over the internet. The VPN endpoints used are the Azure Virtual Network Gateway (VNG) and an on-premises Local Network Gateway (LNG). The LNG used in this guide is a Palo Alto Networks next-generation firewall.

Figure 22 Backhaul connection to on-premises network



Note

The connection from Azure to the on-premises network was tested and validated only with a specific design that uses BGP routing. Other variants to the backhaul design might work with similar configurations but have not been explicitly tested.

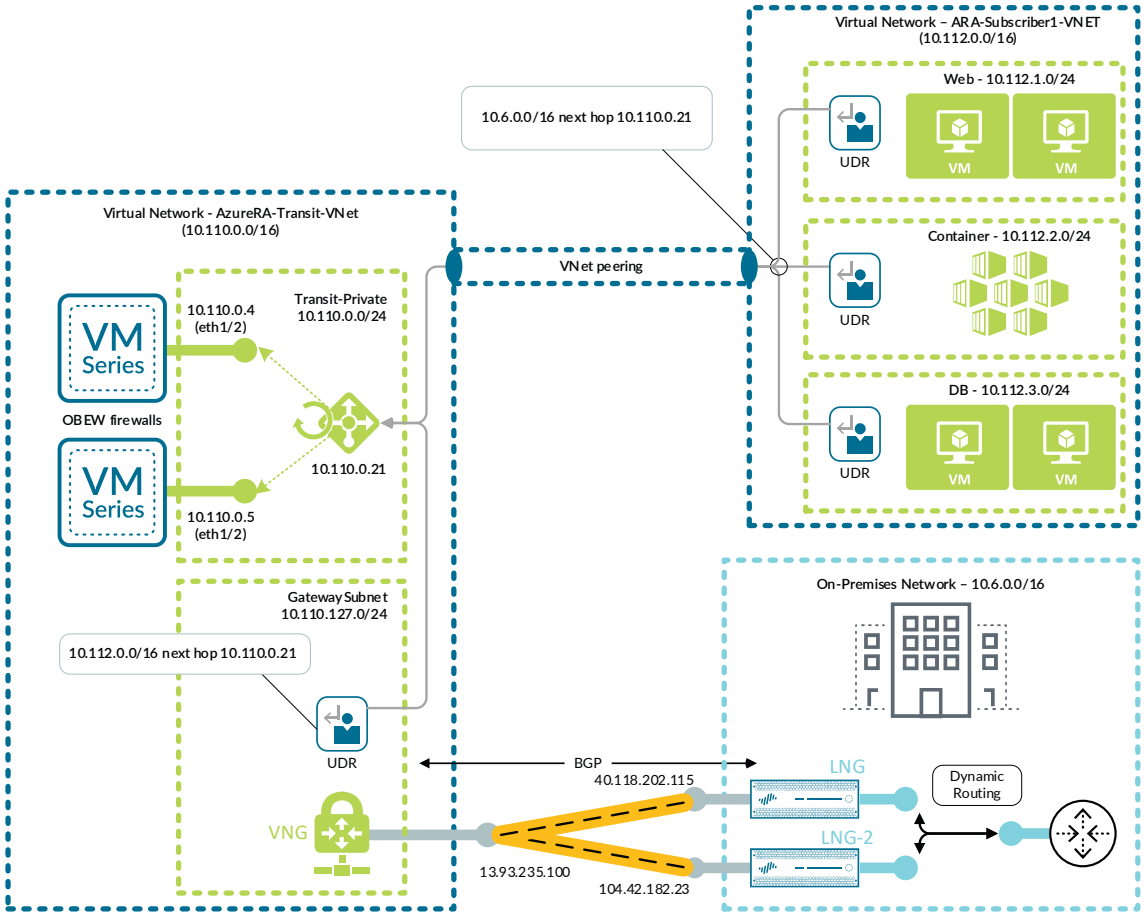
Two resilient design options are included:

- **Active/passive**—Deploy an active/passive firewall pair at your on-premises network and configure a single VPN tunnel from the VNG to the firewall pair. The high-availability features of the firewall provide resiliency for this topology. If the active firewall fails, the passive firewall becomes active. In this configuration, only a single firewall is forwarding traffic. You use BGP for dynamic route learning.
- **Active/active**—Deploy an active/active firewall pair at your on-premises network and configure a VPN tunnel from the VNG to each firewall. You configure BGP to prefer one tunnel as the active path and the other tunnel as a backup path. If the firewall with the active path fails, BGP reroutes traffic to the backup path through the other active firewall. Traffic flows only over a single tunnel in both directions to ensure route symmetry. If you have multiple prefixes on your on-premises network, you can configure BGP for both links to be active, with each link active for a group of prefixes. This configuration is beyond the scope of this guide.

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 23 Backhaul connection to the on-premises network with active/active firewall pair



Procedures

Configuring Azure Networking for a Backhaul Connection

The procedures in this section rely on the following assumptions:

- The on-premises network IP address block is **10.6.0.0/16**.
- The existing on-premises firewall(s) must have a statically assigned public IP address.
- The Azure subnets reachable for Panorama and VM-Series management are **10.255.0.0/24** and **10.110.255.0/24**.
- The Azure subscriber subnets reachable for in-band access (Subscriber-1 and Subscriber-2) use the IP address ranges **10.112.0.0/16** and **10.113.0.0/16**.

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

13.1 Configure Azure User-Defined Routes

The Azure VNG requires its own subnet. You create the route table of UDRs for the VNG subnet first so that you can associate the route table when you create the subnet.

Figure 24 User-defined route additions for a backhaul connection

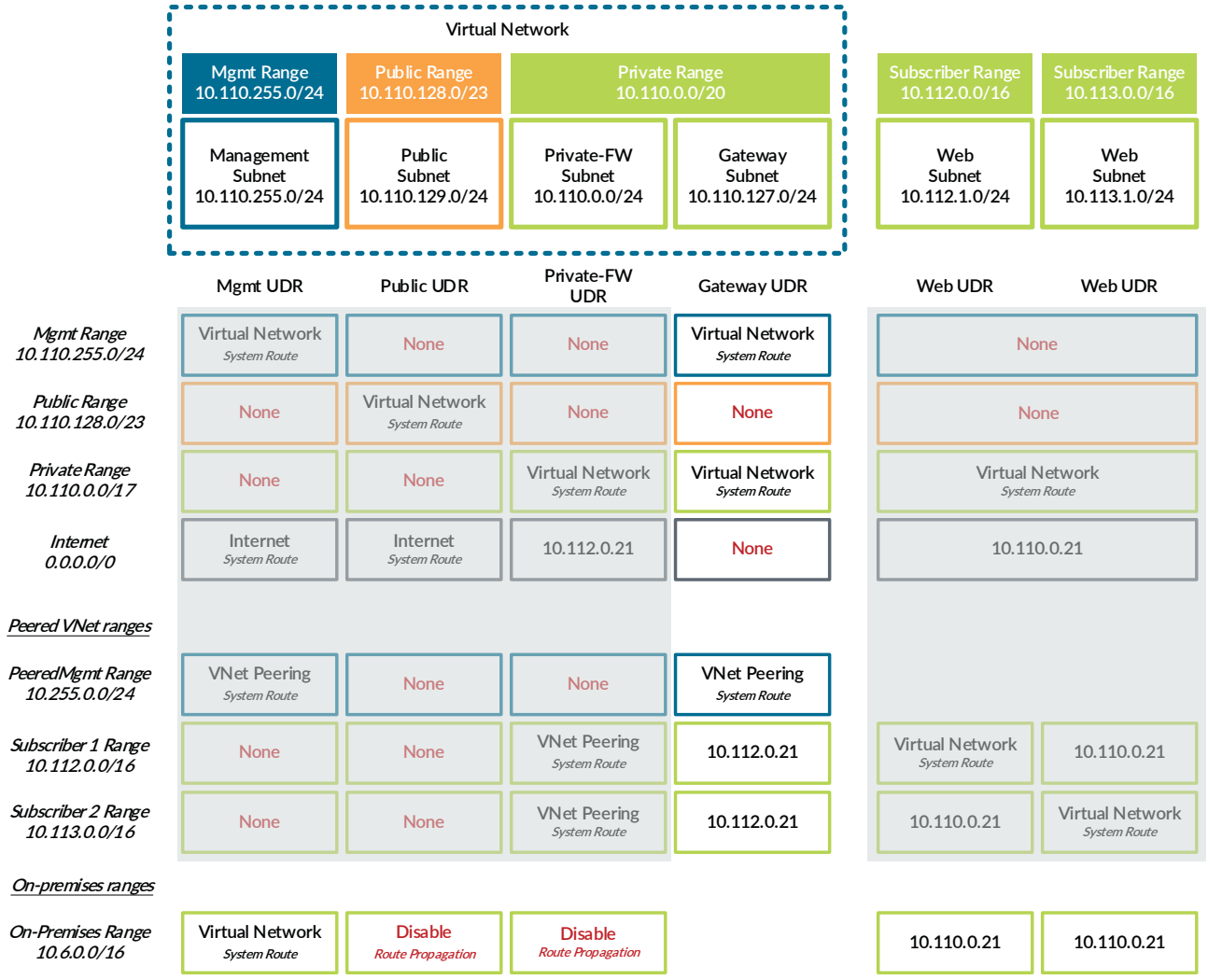


Table 33 VPN gateway subnet UDRs (10.110.127.0/24)

Route name	Address prefix	Next-hop type	Next-hop address	Comments
Blackhole-Public	10.110.128.0/23	None	—	Block traffic to Public IP address space
Blackhole-Internet	0.0.0.0/0	None	—	Block traffic to internet
Net-10.112.0.0_16	10.112.0.0/16	Virtual appliance	10.110.0.21	Front-end IP of load balancer Forwards to Subscriber-1 VNet
Net-10.113.0.0_16	10.113.0.0/16	Virtual appliance	10.110.0.21	Front-end IP of load balancer Forwards to Subscriber-2 VNet

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

Step 2: In the **Name** box, enter **ARATRV-VPNGW**.

Step 3: In the **Resource Group** list, choose **AzureRA-Transit**, and then click **Create**.

Step 4: In **Home** > **Route tables** > **ARATRV-VPNGW**, click **Routes**.

Step 5: Repeat these sub-steps for all entries in Table 33:

- In **Home** > **Route tables** > **ARATRV-VPNGW—Routes**, click **Add**.
- In the **Route name** box, enter **Blackhole-Public**.
- In the **Address prefix** box, enter **10.110.128.0/23**.
- In the **Next hop type** list, choose **None**.
- If the Next-hop type is **Virtual appliance**, enter the Next-hop address value.
- Click **OK**.

13.2 Modify the Existing Route Tables

By default, Azure networking routes traffic originating from all subnets and destined to the on-premises network range directly to the VNG. This design allows implicit access for the management subnet to support in-band management of Panorama and the VM-Series firewalls.

Blocking the traffic or enforcing a firewall policy requires that you create UDRs. Configure the public network UDR to disable VNG route propagation. This configuration blocks traffic destined to the on-premises network from the public subnet. For policy enforcement, configure the subscriber UDRs to redirect traffic from all other subnets to the firewall layer.

You originally created the route tables in Table 34 in Procedure 5.3 and Procedure 5.6. Modify the route tables listed in Table 34 by adding the additional specified routes. If you have additional on-premises prefixes, then each prefix requires a UDR in each route table.

Caution

When adding additional on-premises networks, you must manually update the route tables to redirect to the new prefixes as they are added. This procedure is required even when running dynamic BGP routing. Prefixes must match exactly for the UDR overrides to replace the active routes.

Palo Alto Networks suggests that you disable VNG route propagation for all subnets, except for the Management subnet, as a best practice. This ensures that system routes cannot be used to access the on-premises networks. UDR redirection to the load-balancer front-end IP is still required.

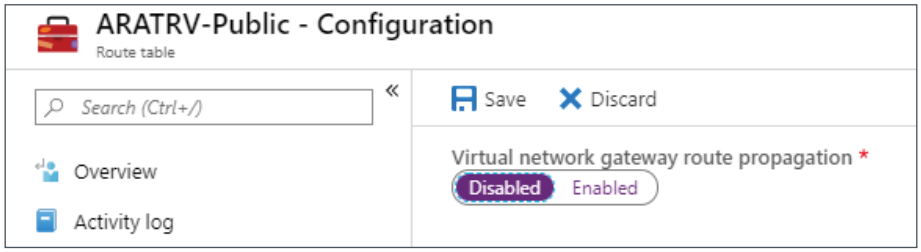
Table 34 Route table modifications for a backhaul connection

Route table name	Route name	Address prefix	Next-hop type	Next-hop address	Comments
ARATRV-Public	—	—	—	—	Disable VNG route propagation
ARATRV-Private	—	—	—	—	Disable VNG route propagation
ARATRV-Sub1-Server	Net-10.112.0.0_16	10.112.0.0/16	Virtual appliance	10.110.0.21	Front-end IP of load balancer Access to on-premises network through the firewall layer
ARATRV-Sub2-Server	Net-10.113.0.0_16	10.113.0.0/16	Virtual appliance	10.110.0.21	Front-end IP of load balancer Access to on-premises network through the firewall layer

If you are running BGP, disable VNG route propagation for the public subnet, private subnet, and all subscriber subnets listed in Table 34. This configuration prevents any BGP learned routes from being installed in the active route table for these subnets.

Step 1: In **Home** > **Route tables** > **ARATRV-Public**, click **Configuration**.

Step 2: In the Virtual network gateway route propagation section, click **Disabled**, then click **Save**.



Step 3: If there is a value in the **Route name** column in Table 34, continue with this procedure.

If there is no specified value in the **Route name** column in Table 34, skip the remaining steps and proceed to the next table entry.

Step 4: In **Home** > **Route tables** > **ARATRV-Sub1-Server**, click **Routes**.

Step 5: In **Home** > **Route tables** > **ARATRV-Sub1-Server—Routes**, click **Add**.

Step 6: In the **Route name** box, enter **Net-10.6.0.0_16**.

Step 7: In the **Address prefix** box, enter **10.6.0.0/16**.

Step 8: In the **Next hop type** list, choose **Virtual appliance**.

Step 9: Repeat this procedure for all entries in Table 34.

13.3 Create the VNG Subnet

This procedure adds a new gateway subnet for the Azure VNG to the existing transit VNet.

Step 1: In **Home > Virtual networks > AzureRA-Transit-VNet**, click **Subnets**.

Step 2: Click **Gateway subnet** to add a new gateway subnet.

Step 3: In the **Address Range (CIDR block)** box, enter **10.110.127.0/24**.

Step 4: Click the Route table section, select **ARATRV-VPNGW**, and then click **OK**.

13.4 Create the Public IP Address for the Azure VNG

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

Step 2: In the SKU section, select **Basic**.

> **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 3: In the **Name** box, enter **ARATRV-VNG-Public**.

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.

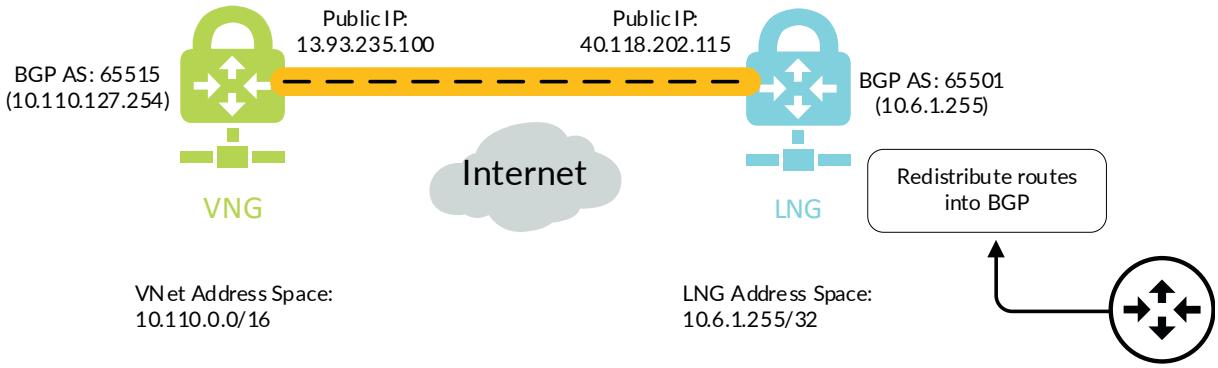
Step 5: In the **Resource Group** list, choose **AzureRA-Transit**, and then click **Create**.

The on-premises firewall requires a peer IP address for the Azure VNG. Azure does not assign the actual IP address until you create the VNG and associate the public IP address.

13.5 Deploy the Virtual Network Gateway on Azure

This procedure uses dynamic routing with BGP. When you use BGP, discard routing with user-defined routes is no longer necessary. Instead, you previously disabled VNG route propagation for selected subnets (already completed in a previous procedure).

Figure 25 BGP configuration



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

Step 2: In the **Name** box, enter **ARATRV-VNG.**

Step 3: In the Region list, choose **(US) West US**. The region is used to filter the virtual network list.

Step 4: In the Gateway type section, select **VPN**.

Step 5: In the VPN type section, select **Route-based**.

Step 6: In the **SKU** list, choose **VpnGw1**. The basic SKU does not support BGP or IKEv2.

Step 7: Click the Virtual Network section, and then select **AzureRA-Transit-VNet**.

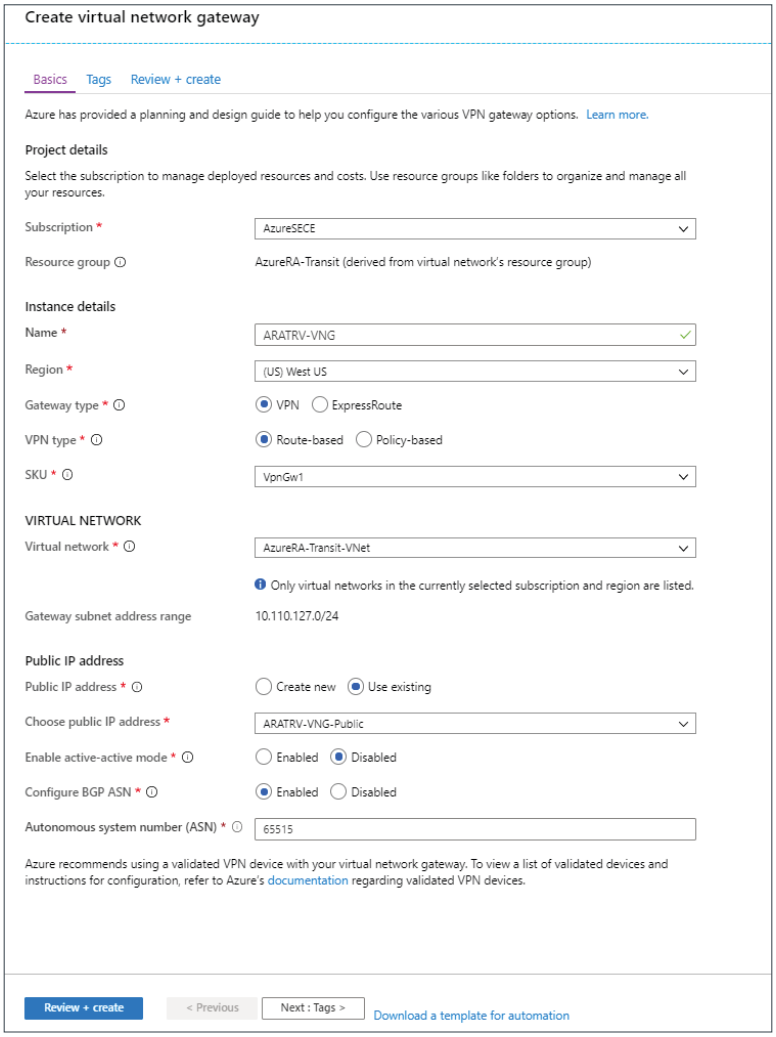
Step 8: In the Public IP address section, select **Use existing**.

Step 9: In the Choose public IP address list, select **ARATRV-VNG-Public**.

Step 10: In the Configure BGP ASN section, select **Enabled**.

Step 11: In the **Autonomous system number (ASN)** box, accept the proposed default value of **65515**.

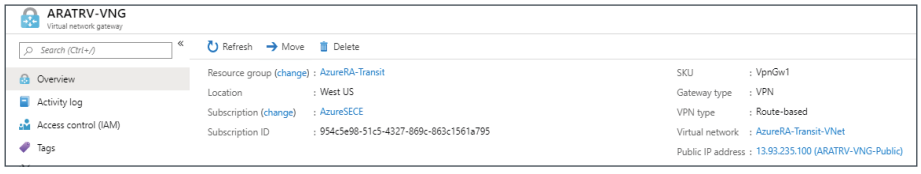
Step 12: Click **Review + create**.



Step 13: On the next screen, click **Create**.

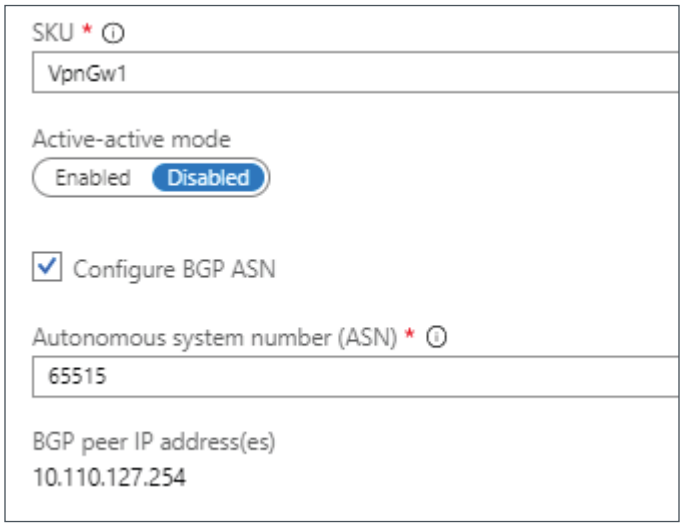
> **Note**
>
> The Azure VNG deployment typically takes 15 minutes or more to complete.

Step 14: In **Home > Virtual network gateways > ARATRV-VNG**, record the public IP address (example: **13.93.235.100**).



Step 15: In **Home > Virtual network gateways > ARATRV-VNG**, click **Configuration**.

Step 16: Record the **BGP peer IP address** assigned to the virtual network gateway (example: **10.110.127.254**).



13.6 Create the Local Network Gateway

The local network gateway corresponds to the on-premises 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 **ARATRV-LNG-OnPrem**.

Step 3: In the **IP address** box, enter the public IP address of the on-premises IPSec VPN peer (example: **40.118.202.115**).

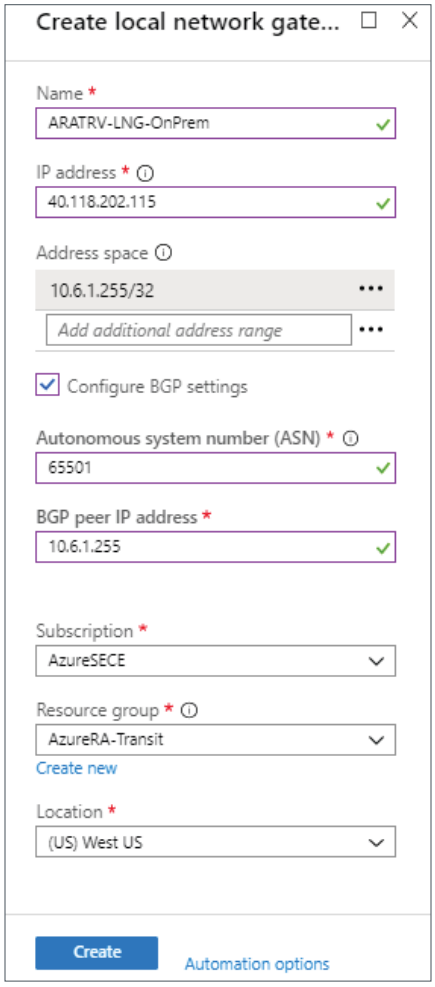
Step 4: In the **Address space** box, enter the IP prefix for the BGP peer address from the on-premises firewall to which this LNG corresponds (example: **10.6.1.255/32**).

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 **10.6.1.255**.

Step 8: In the **Resource Group** list, choose **AzureRA-Transit**, and then click **Create**.



13.7 Create the VPN Connection from the VNG to the LNG

Step 1: In **Home > Connections**, click **Add**.

Step 2: In **Home > Connections > Create connection > Basics**, in the **Connection type** list, choose **Site-to-site (IPsec)**.

Step 3: In the **Resource Group** list, choose **AzureRA-Transit**, and then click **OK**.

Step 4: In **Home > Connections > Create connection > Settings**, click the **Virtual network gateway** section, and then select **ARATRV-VNG**.

Step 5: Click the **Local network gateway** section, and then select **ARATRV-LNG-OnPrem**.

Step 6: In the **Connection name** box, enter **ARA-Transit-to-OnPrem**.

Step 7: In the **Shared key (PSK)** box, enter the value for the pre-shared key (complex password).

Step 8: Select **Enable BGP**, and then click **OK**.

Step 9: In **Home > Connections > Create connection > Summary**, review the summary, and if it's acceptable, click **OK**.

13.8 Enable the Virtual Network Gateway for VNet Peers

Azure networking allows you to share a VNG across multiple VNets. After you create your VNG, enable the **Allow gateway transit** feature on the peer connections that are sourced from your transit VNet. You must enable each peer connection separately.

On each peer VNet, you must enable the **Use remote gateways** feature on the peer connections towards the transit VNet.

Table 35 Transit VNet Peer Connections

Transit-VNet (source)	Peering name	Virtual network (destination/ subscriber)	VNet peer setting
AzureRA-Transit-VNet	VNet-Peer_AzureRA-VNet	AzureRA-VNet	Allow gateway transit
AzureRA-Transit-VNet	VNet-Peer_ARA-Subscriber1-VNet	ARA-Subscriber1-VNET	Allow gateway transit
AzureRA-Transit-VNet	VNet-Peer_ARA-Subscriber2-VNet	ARA-Subscriber2-VNET	Allow gateway transit

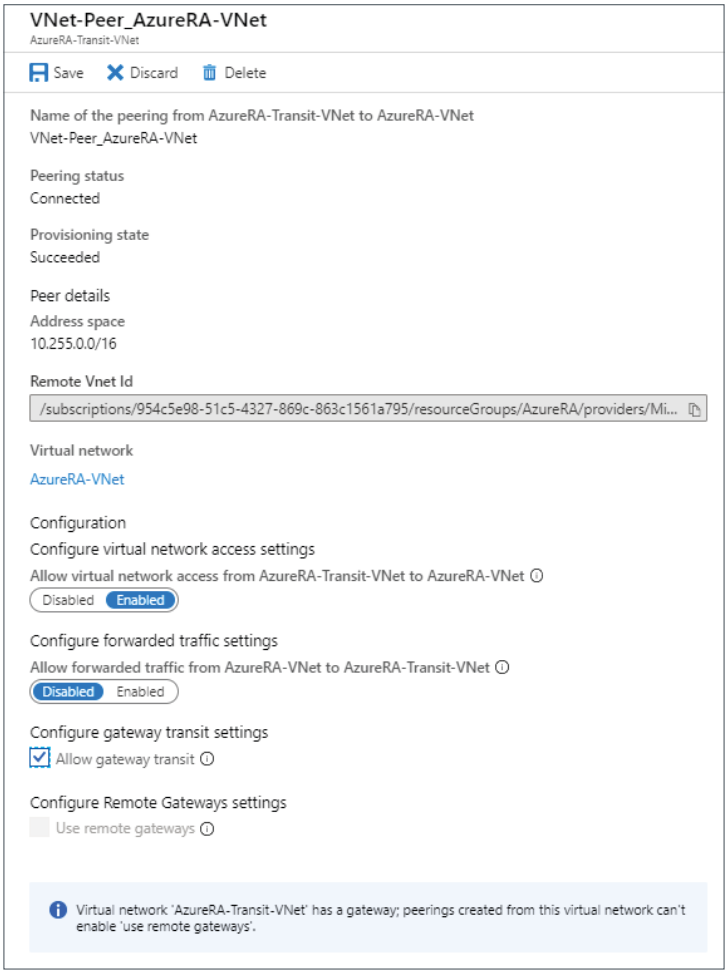
Table 36 Subscriber VNet Peer Connections

Subscriber VNET (source)	Peering name	Virtual network (destination)	VNet peer setting
AzureRA-VNet	VNet_Peer_AzureRA-Transit-VNet	AzureRA-Transit-VNet	Use remote gateways
ARA-Subscriber1-VNET	VNet_Peer_AzureRA-Transit-VNet	AzureRA-Transit-VNet	Use remote gateways
ARA-Subscriber2-VNET	VNet_Peer_AzureRA-Transit-VNet	AzureRA-Transit-VNet	Use remote gateways

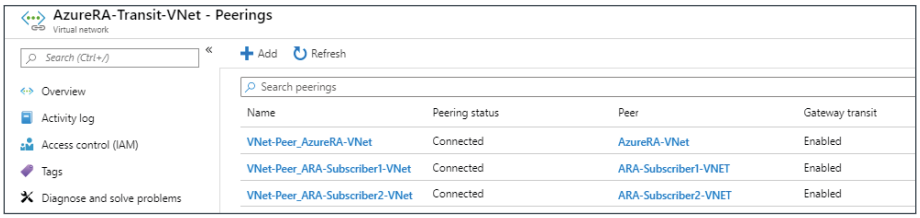
Step 1: In **Home > Virtual networks > AzureRA-Transit-VNet**, click **Peerings**.

Step 2: Repeat the following for each entry in Table 35:

- Select **VNet-Peer_AzureRA-VNet**.
- In the Configure gateway transit settings section, select **Allow gateway transit**.
- Click **Save**, and then click **X** to close.



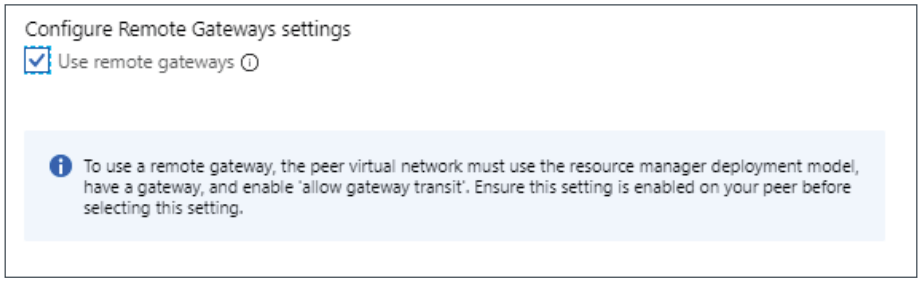
Step 3: In **Home > Virtual networks > AzureRA-Transit-VNet - Peerings**, in the Gateway transit column, verify that gateway transit has been enabled for all peered VNets.



Step 4: In **Home > Virtual networks > AzureRA-VNet**, click **Peerings**.

Step 5: Repeat the following for each entry in Table 36:

- Select **VNet-Peer_AzureRA-Transit-VNet**.
- In the Configure Remote Gateways settings section, select **Use remote gateways**.
- Click **Save**, and then click **X** to close.



Procedures

These procedures assume the on-premises firewall is configured and running with a public interface reachable from the internet and a private interface with access to internal subnets. You have already configured the firewall with a default virtual router, and you have configured DNS and NTP.

You perform the following procedures on the on-premises next-generation firewall or VM-Series device. If you are using a second resilient on-premises firewall, you repeat this group of procedures.

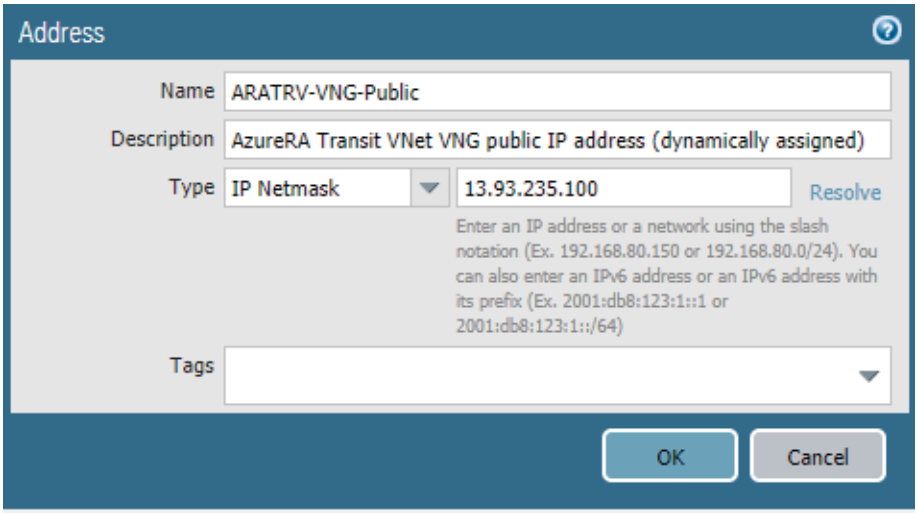
14.1 Configure Objects and Interfaces

Step 1: In **Objects > Addresses**, click **Add**.

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

Step 3: In the **Type** list, choose **IP Netmask**.

Step 4: In the **Type value** box, enter the public IP address that Azure assigned (example: **13.93.235.100**), and then click **OK**.



Step 5: In **Network** > **Zones**, click **Add**. The Zone window appears.

Step 6: In the **Name** box, enter **VPN**.

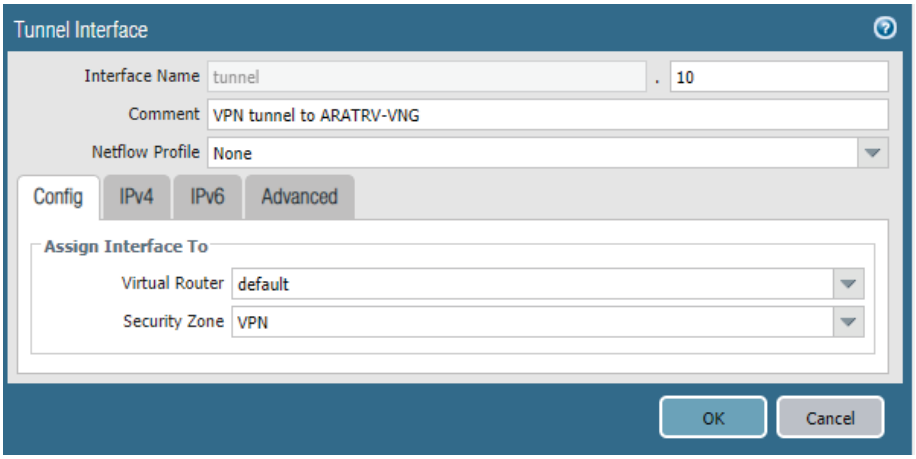
Step 7: In the **Type** list, choose **Layer3**, and then click **OK**.

Step 8: In **Network** > **Interfaces**, on the Tunnel tab, click **Add**. The Tunnel Interface window appears.

Step 9: In the **Interface Name.subinterface** box, enter **10**.

Step 10: In the **Virtual Router** list, choose **default**.

Step 11: In the **Security Zone** list, choose **VPN**.



Step 12: On the IPv4 tab, in the IP pane, click **Add**.

Step 13: If you are configuring the primary device, enter **10.6.1.255/32**, and then click **OK**.

If you are configuring the second device for a resilient backhaul connection, enter **10.6.1.254/32**, and then click **OK**.

Step 14: On the Advanced tab, in the **MTU** box, enter **1424**, and then click **OK**.

You use this value to minimize IP packet fragmentation due to the tunnel and IPSec encapsulation overhead.

Step 15: In **Network Interfaces**, click the public-facing Ethernet interface (example: **ethernet1/1**).

Step 16: On the Advanced tab, in the Other Info section, select **Adjust TCP MSS**, and then click **OK**.

You enable this feature to minimize IP packet fragmentation due to the tunnel and IPSec encapsulation overhead.

14.2 Configure IKEv2 and IPSec

Use the values specified in Table 37 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. This table lists the strongest authentication and encryption values that are compatible with Azure.

Table 37 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 window appears.

Step 2: In the **Name** box, enter **Azure-IKEv2**.

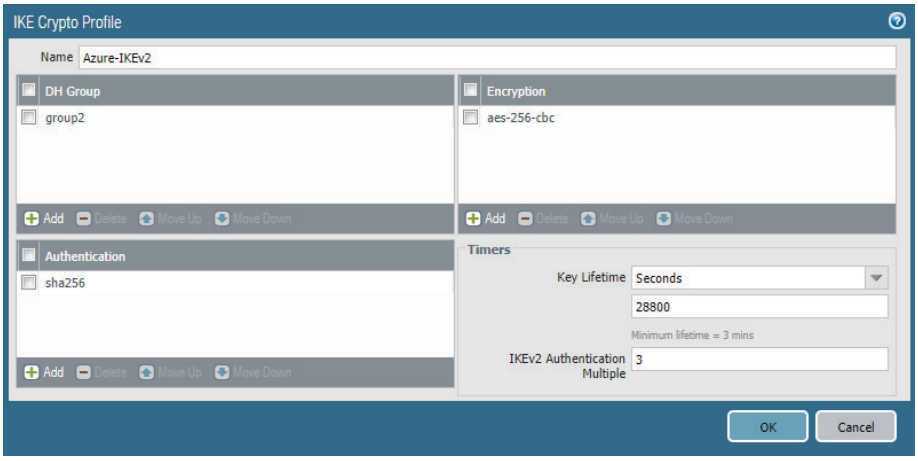
Step 3: In the DH Group pane, click **Add**, and then select **group2**.

Step 4: In the Authentication pane, click **Add**, and then select **sha256**.

Step 5: In the Encryption pane, click **Add**, and then select **aes-256-cbc**.

Step 6: In the Timers section, in the **Key Lifetime** list, choose **Seconds**, and then 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 window appears.

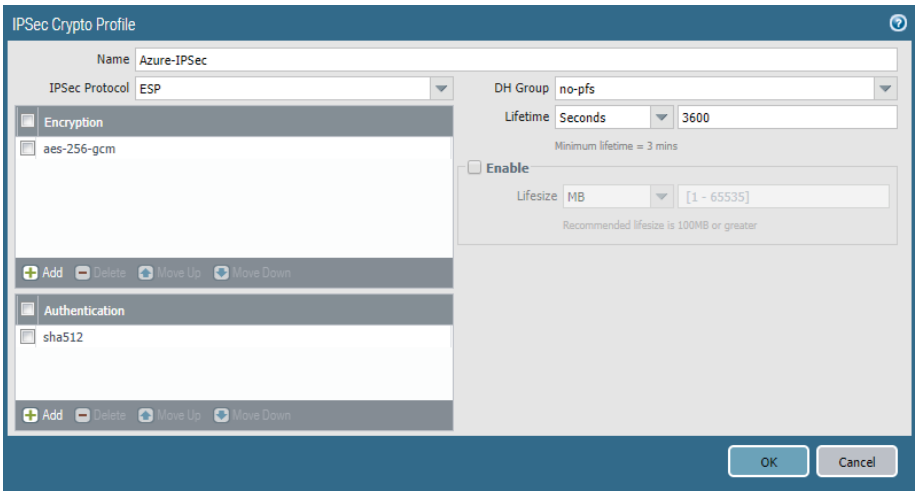
Step 9: In the **Name** box, enter **Azure-IPSec**.

Step 10: In the Encryption pane, click **Add**, and then select **aes-256-gcm**.

Step 11: In the Authentication pane, click **Add**, and then select **sha512**.

Step 12: In the **DH Group** list, choose **no-pfs**.

Step 13: In the **Lifetime** list, choose **Seconds**, enter **3600**, and then click **OK**.



Step 14: In **Network** > **Network Profiles** > **IKE Gateways**, click **Add**. The IKE Gateway window appears.

Step 15: In the **Name** box, enter **OnPrem-to-AzureRA-Transit-IKEv2**.

Step 16: In the **Version** list, choose **IKEv2 only mode**.

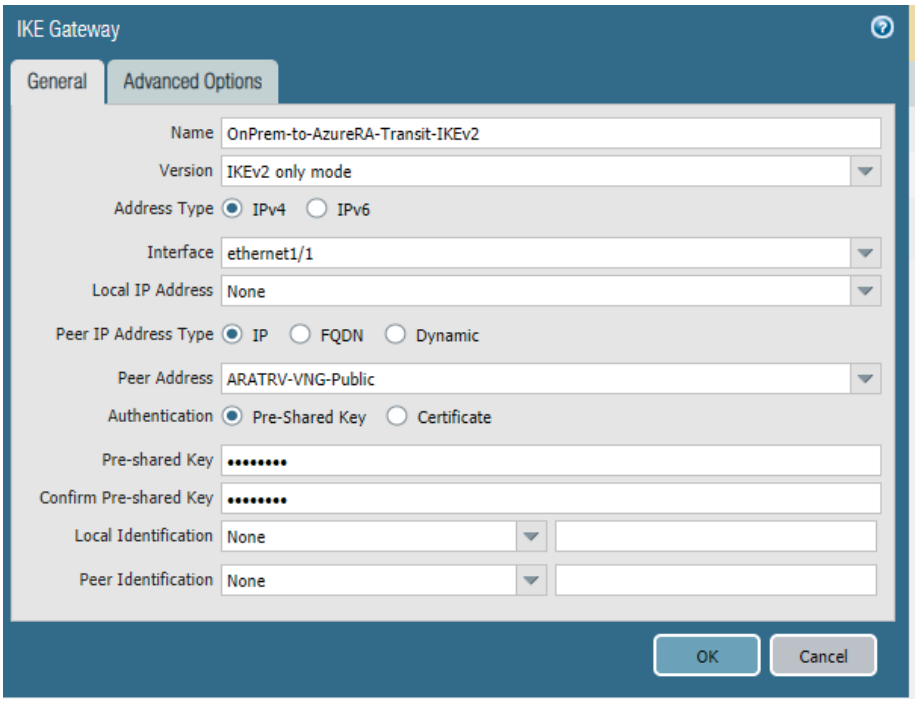
Step 17: In the **Interface** list, choose the public interface of the firewall (example: **ethernet1/1**).

Step 18: In the Peer IP Address Type section, select **IP**.

Step 19: In the **Peer Address** list, choose **ARATRV-VNG-Public**.

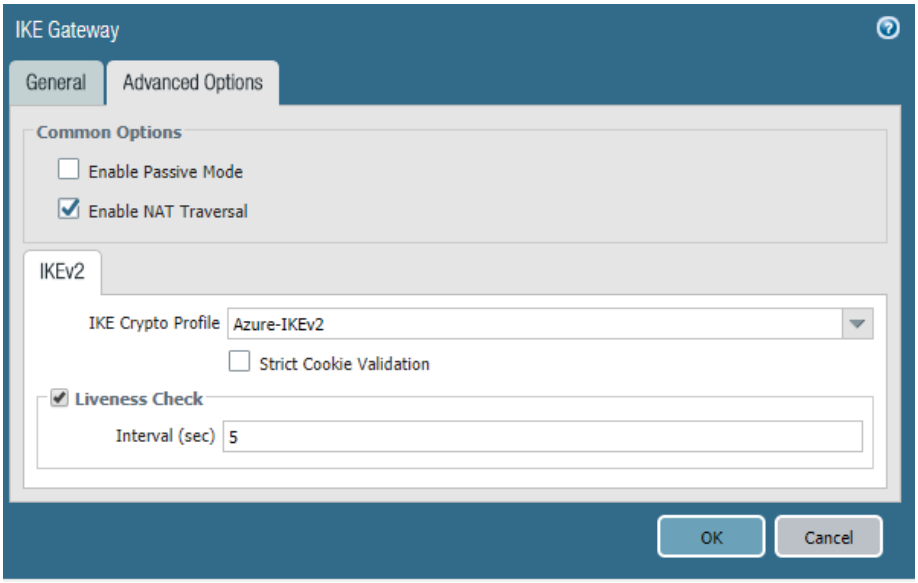
Step 20: In the **Pre-shared Key** box, enter the Shared key (PSK) that matches the VPN connection configured on Azure.

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, choose **Azure-IKEv2**, and then click **OK**.



Step 24: In **Network** > **IPSec Tunnels**, click **Add**.

Step 25: In the **Name** box, enter **OnPrem-to-AzureRA-Transit**.

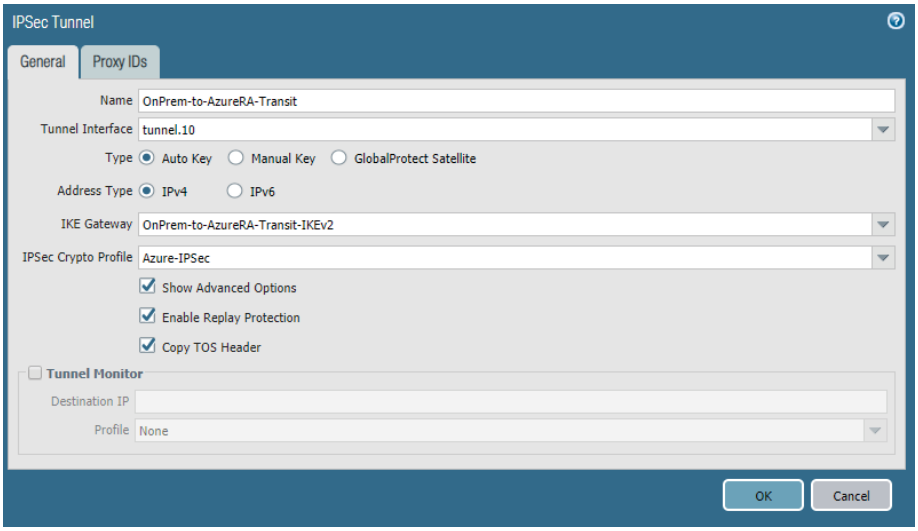
Step 26: In the **Tunnel Interface** list, choose **tunnel.10**.

Step 27: In the **IKE Gateway** list, choose **OnPrem-to-AzureRA-IKEv2**.

Step 28: In the **IPSec Crypto Profile** list, choose **Azure-IPSec**.

Step 29: Select **Show Advanced Options**.

Step 30: Select **Copy TOS Header**, and then click **OK**.



14.3 Configure a Static Route for BGP

BGP dynamic routing requires the creation of a single static route that corresponds to the Azure routing peer prefix. The firewall dynamically learns all other destinations using the routing protocol.

This procedure assumes you are using the default virtual router.

Step 1: In **Network > Virtual Routers**, click **default**. The Virtual Router—default window appears.

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

Step 3: In the **Name** box, enter **Azure-BGP-Router-ID**.

Step 4: In the **Destination** box, enter **10.110.127.254/32**.

Step 5: In the **Interface** list, choose **tunnel.10**.

Step 6: In the **Next Hop** list, choose **None**, and then click **OK**.

Step 7: Click **OK**. This closes the Virtual Router window.

14.4 Configure BGP

This procedure requires that you have a BGP autonomous system number. The example uses 65501 for the on-premises firewall. The BGP peering configuration uses the tunnel interface IP address of the firewall as the BGP router ID.

> **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-premises network and firewall, then redistribute the routes from the routing protocol instead of the connected route.
>
> When configuring a resilient backhaul connection, a dynamic routing protocol is required. This ensures symmetric routing.

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.

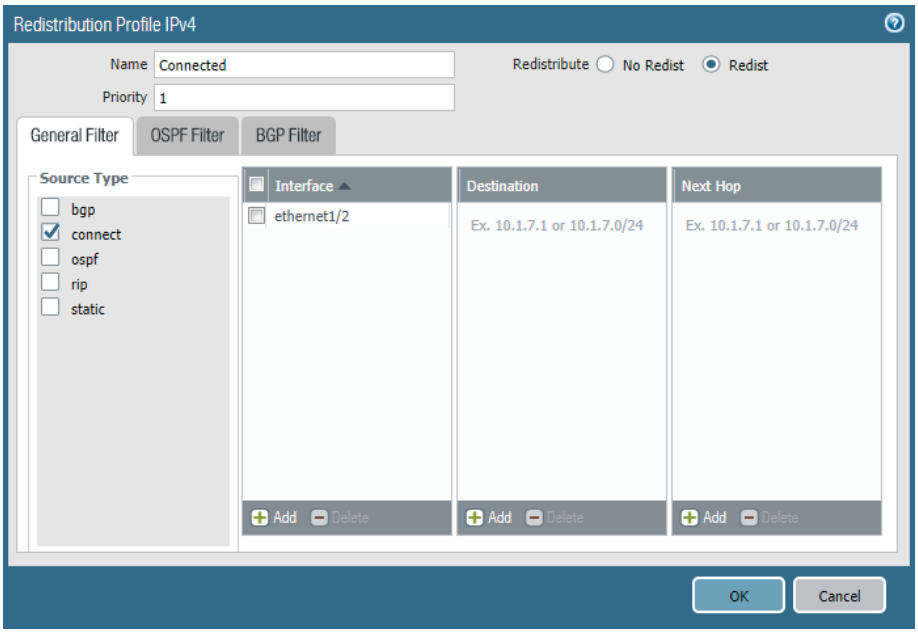
Step 3: In the **Name** box, enter **Connected**.

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 then click **OK**.



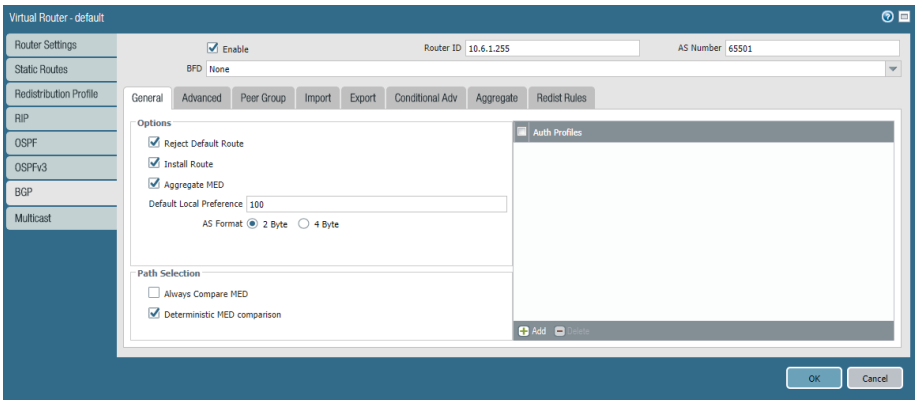
Step 8: On the BGP tab, select **Enable**.

Step 9: If you are configuring the primary device, in the **Router ID** box, enter **10.6.1.255**.

If you are configuring the second device for a resilient backhaul connection, in the **Router ID** box, enter **10.6.1.254**.

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 **AzureRA-Transit**.

Step 16: In the **Peer AS** box, enter the autonomous system number assigned to the Azure virtual network gateway. The default is **65515**.

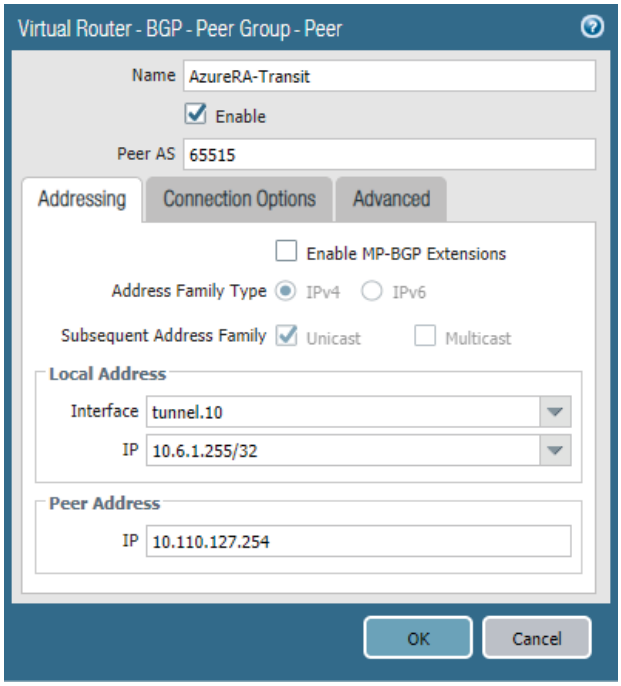
Step 17: In the Local Address pane, in the **Interface** list, choose **tunnel.10**.

Step 18: If you are configuring a primary device, in the Local Address pane, in the **IP** list, choose **10.6.1.255/32**.

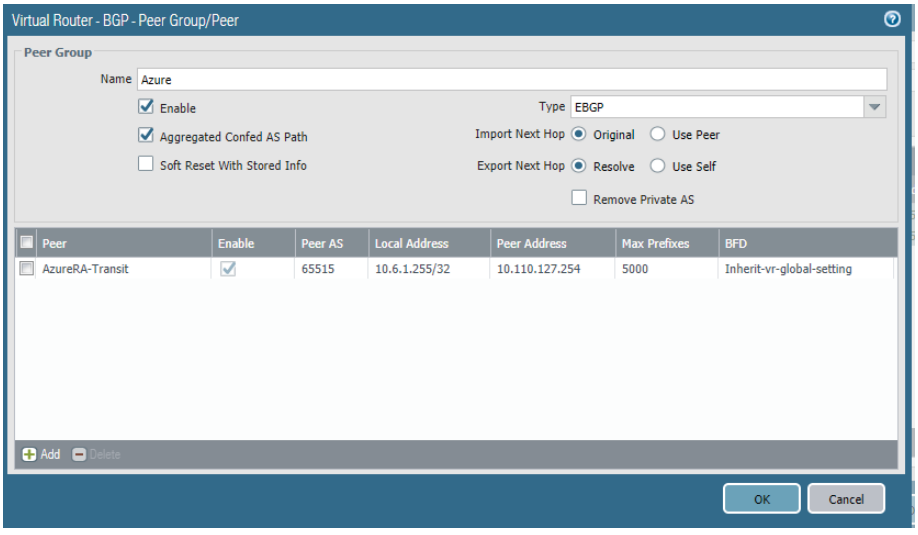
If you are configuring the second device for a resilient backhaul connection, in the Local Address pane, in the **IP** list, choose **10.6.1.254/32**.

Step 19: In the Peer Address pane, in the **IP** box, enter the BGP peer IP address that Azure assigned to the virtual network gateway (example: **10.110.127.254**).

Step 20: On the Connection Options tab, in the **Multi Hop** box, enter **2**, and then click **OK**.

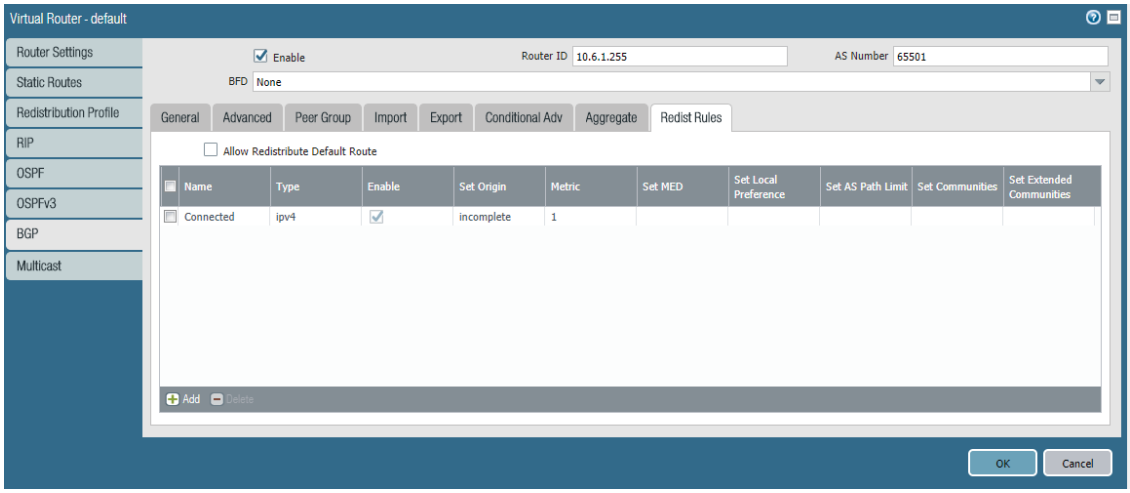


Step 21: Click **OK**. This closes the Virtual Router—BGP—Peer Group/Peer window.



Step 22: On the Redist Rules tab, click **Add**. The Virtual Router—BGP—Redistribute Rules—Rule window appears.

Step 23: In the **Name** list, choose **Connected**, and then click **OK**.



Step 24: Click **OK**. This closes the Virtual Router—default window, and then click **Commit**.

Your on-premises devices should be able to reach the management subnets in Azure.

Procedures

Configuring a Resilient Backhaul Connection

15.1 Create the Second Local Network Gateway

15.2 Create the VPN Connection from the VNG to the Second LNG

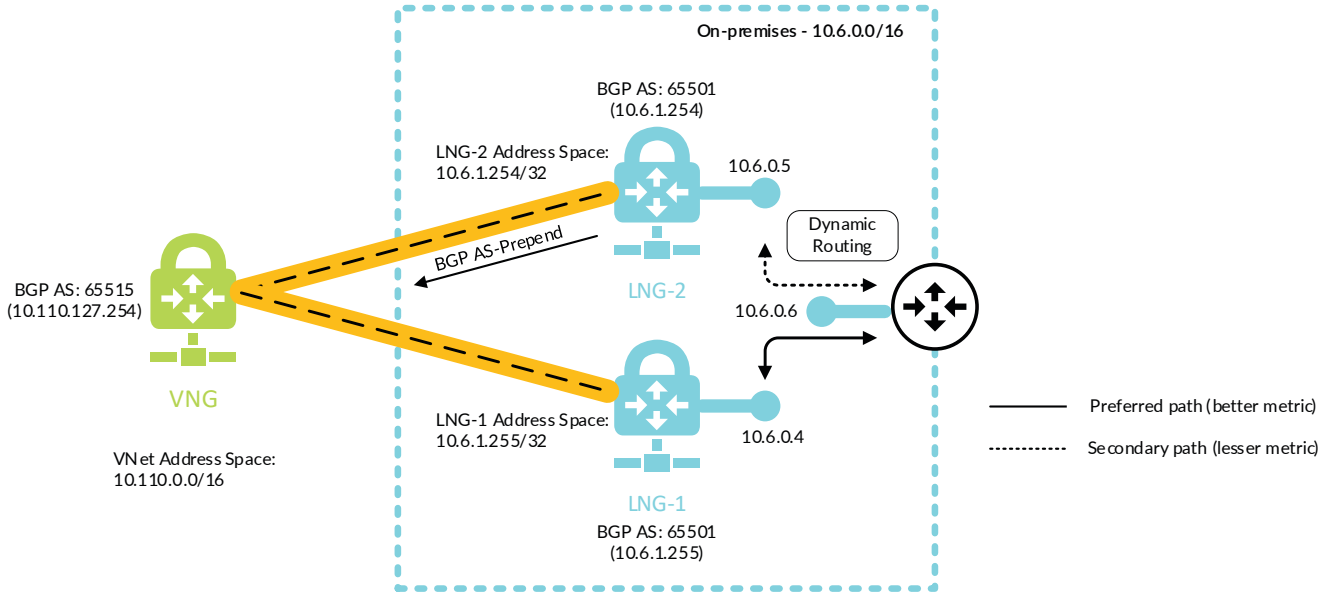
15.3 Configure an Additional On-Premises Firewall

This group of procedures 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. You already configured the first connection with BGP routing.

This procedures in this section rely on the following assumptions:

- The existing on-premises firewall BGP peer address (assigned to the tunnel interface) is **10.6.1.254**.
- The second existing on-premises firewall must have a statically assigned public IP address.
- The on-premises network uses dynamic routing between the on-premises firewalls and the internal private network. The downstream router learns the Azure routes from both on-premises firewalls and uses routing metrics to select the preferred path through the first connection.
- BGP AS-Prepend is used to make the second connection less preferred.

Figure 26 Resilient routing for a backhaul connection



15.1 Create the Second Local Network Gateway

Using this procedure, you create the local network gateway that corresponds to the second on-premises 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 **ARATRV-LNG-OnPrem-2**.

Step 3: In the **IP address** box, enter the public IP address of the on-premises IPSec VPN peer (example: **104.42.182.23**).

Step 4: In the **Address space** box, enter the IP prefix for the BGP peer address from the on-premises firewall to which this LNG corresponds (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, choose **AzureRA-Transit**, and then click **Create**.

15.2 Create the VPN Connection from the VNG to the Second LNG

Step 1: In **Home > Connections**, click **Add**.

Step 2: In **Home > Connections > Create connection > Basics**, in the **Connection type** list, choose **Site-to-site (IPsec)**.

Step 3: In the Resource Group list, choose **AzureRA-Transit**, and then click **OK**.

Step 4: In **Home > Connections > Create connection > Settings**, click the **Virtual network gateway** section, and then select **ARATRV-VNG**.

Step 5: Click the **Local network gateway** section, and then select **ARATRV-LNG-OnPrem-2**.

Step 6: In the **Connection name** box, enter **ARA-Transit-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**, and then click **OK**.

Step 9: In **Home > Connections > Create connection > Summary**, review the summary, and if it's acceptable, click **OK**.

15.3 Configure an Additional On-Premises Firewall

Using this procedure, you configure a second on-premises firewall to be used for the resilient backhaul connection. You configure this firewall by repeating earlier procedures, and then you configure BGP to make the second connection less preferred.

The BGP configuration prepends a second AS number to the routes advertised from the second firewall. Azure receives all prefixes from both LNGs and uses the AS-path length to make its routing decision. This routing configuration ensures that when both LNGs are available, Azure chooses the first connection in order to send traffic from Azure to the on-premises networks. This does not influence the path selection in the opposite direction.

Caution

If you do not configure on-premises routing to prefer the first connection, then asymmetric routing occurs. The firewall drops network traffic because it doesn't see both directions of the flow. This guide does not include these configuration details.

Step 1: Repeat Procedure 14.1 through Procedure 14.4 to configure the second firewall, using the values specified for a second device for a resilient backhaul connection.

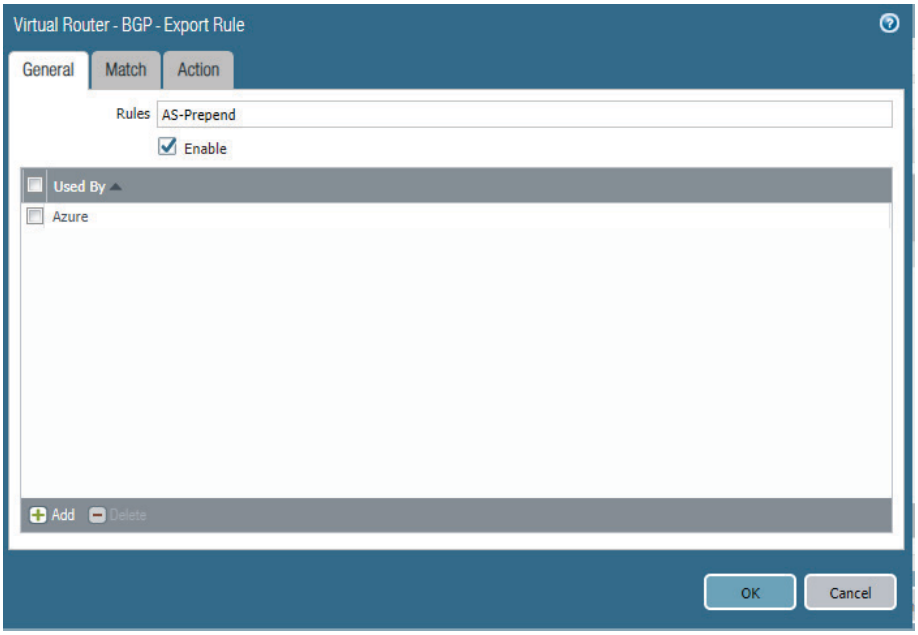
Step 2: In **Network > Virtual Routers**, click **default**. The Virtual Router—default window appears.

Step 3: On the BGP tab, change to the Export tab.

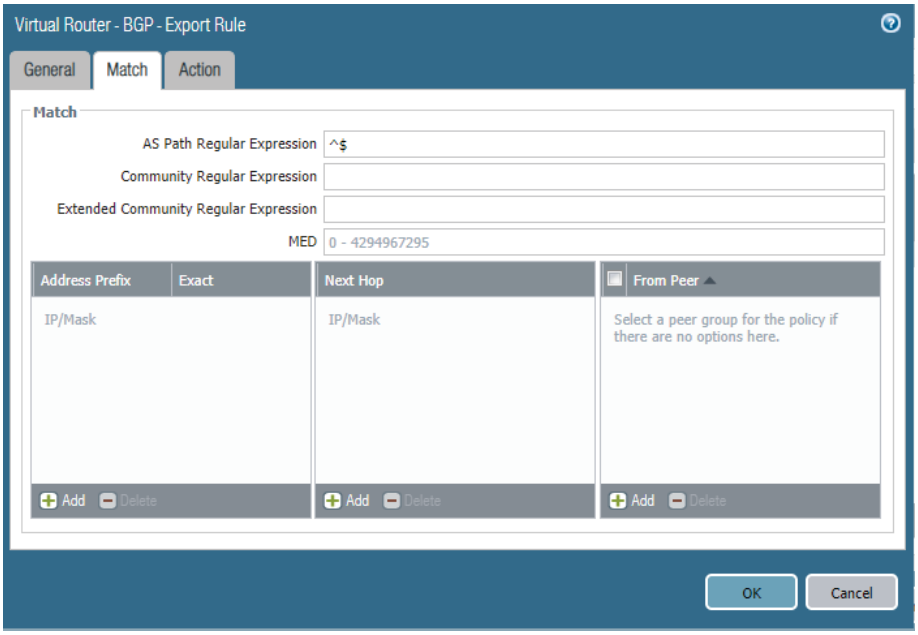
Step 4: Click **Add**, The Virtual Router—BGP—Export Rule window appears.

Step 5: In the **Rules** box, enter **AS-Prepend**.

Step 6: In the Used By pane, click **Add**, and then select **Azure**.

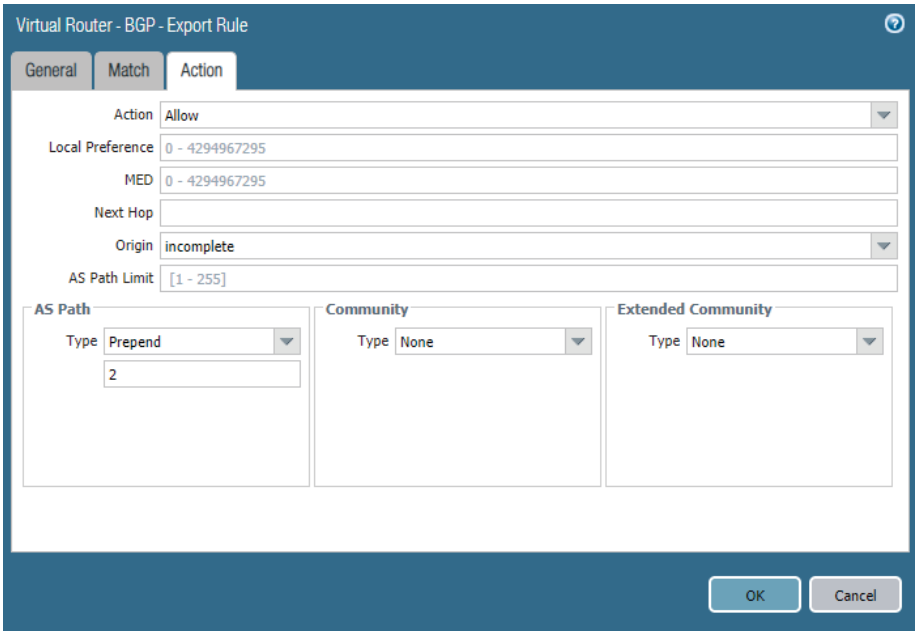


Step 7: On the Match tab, in the **AS Path Regular Expression** box, enter **^$**. This regular expression matches all prefixes that are local to this autonomous system.



Step 8: On the Action tab, in the AS Path section, do the following:

- In the **Type** list, choose **Prepend**.
- In the **Type value** box, enter **2**.
- Click **OK**. This closes the Virtual Router—BGP—Export Rule window.



Step 9: Click **OK**. This closes the Virtual Router—default window, and then click **Commit**.

Procedures

The security policy for the backhaul connection is enforced at multiple locations. The on-premises firewall that terminates the VPN tunnel to Azure can use interzone security policy rules between the private zone and the VPN zone. The VM-Series firewalls on Azure can use intrazone security policy rules for the private zone.

Completing this group of procedures enables traffic from the on-premises location to the private network. You must repeat Procedure 16.2 with the source and destination addresses reversed in order to enable traffic in the opposite direction from the private network to the on-premises network.

This guide includes only the VM-Series policy.

16.1 Create Address Objects for the Backhaul Connection

This procedure reuses objects already created in Procedure 9.2. If necessary, create additional objects by using the same procedure. The original table of objects (Table 26) is repeated here.

Table 38 Outbound traffic address objects (also used for backhaul traffic)

Object name	Description	Type	Type value
Net-10.112.0.0_16	Subscriber-1	IP Netmask	10.112.0.0/16
Net-10.113.0.0_16	Subscriber-2	IP Netmask	10.113.0.0/16

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

Step 2: Navigate to **Objects**.

Step 3: In the **Device Group** list, choose **Transit-VNet-OBEW**.

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

Step 5: In the **Name** box, enter **Net-10.6.0.0_16**.

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

Step 7: In the **Type value** box, enter **10.6.0.0/16**, and then click **OK**.

16.2 Configure the Security Policy for the Backhaul Connection

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 traffic profile permits these applications:

- SSH (ssh)
- RDP (ms-rdp)
- Web browsing (web-browsing)
- SSL (ssl)

This policy permits access to Azure private resources from connections initiated from devices from on-premises networks. Add additional required applications to your policy as needed.

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

Step 2: Navigate to **Policies**.

Step 3: In the **Device Group** list, choose **Transit-VNet-OBEW**.

Step 4: In **Policies > Security > Pre Rules**, click **Add**.

Step 5: In the **Name** box, enter **Backhaul-to-Subscriber**.

Step 6: In the **Rule Type** list, choose **intrazone**.

Step 7: On the Source tab, in the Source Zone pane, click **Add**, and then select **Private**.

Step 8: In the Source Address pane, click **Add**, and then select **Net-10.6.0.0_16**.

Step 9: On the Destination tab, in the Destination Address pane, click **Add**, and then select **Net-10.112.0.0_16**.

Step 10: Repeat Step 9 for all objects in Table 38.

Step 11: On the Application tab, in the Applications pane, click **Add**.

Step 12: In the search box, enter **ssh**, and then in the results list, choose **ssh**.

Step 13: In the Applications pane, click **Add**.

Step 14: In the search box, enter **ms-rdp**, and then in the results list, choose **ms-rdp**.

Step 15: In the Applications pane, click **Add**.

Step 16: In the search box, enter **web-browsing**, and then in the results list, choose **web-browsing**.

Step 17: In the Applications pane, click **Add**.

Step 18: In the search box, enter **ssl**, and then in the results list, choose **ssl**.

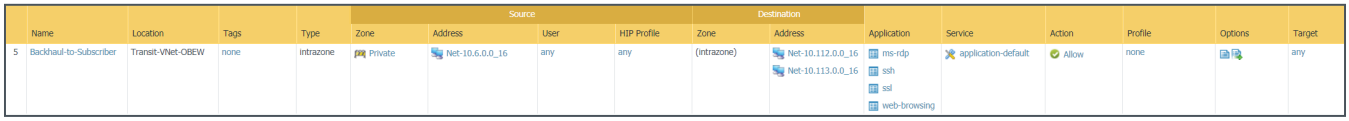
Step 19: On the Service/URL Category tab, in the Service pane, select **application-default**.

Step 20: On the Actions tab, in the Action Setting section, in the **Action** list, choose **Allow**.

Step 21: In the Log Setting section, in the **Log Forwarding** list, choose **CortexDL**.

Step 22: 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 is not automatically applied to new group members.



					Source				Destination							
	Name	Location	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options	Target
5	Backhaul-to-Subscriber	Transit-VNet-OBEW	none	intrazone	Private	Net-10.6.0.0_16	any	any	(intrazone)	Net-10.112.0.0_16 Net-10.113.0.0_16	ms-rdp ssh ssl web-browsing	application-default	Allow	none		any

Step 23: On the **Commit** menu, click **Commit and Push**.

Deployment Details for Automated Bootstrapping

Procedures

This group of procedures provides an alternate deployment method to Procedure 2.1. In addition to deploying the VM-Series firewalls by using the ARM template, the automated bootstrap process licenses the VM-Series device 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.

This guide also includes the option to upgrade to a specific software version and install application and content updates as part of the bootstrap process.

Note

If you choose to upgrade the software image and install updates, you should expect an additional 5-10 minutes to complete the bootstrap process.

After deployment using the bootstrap, you add a new VM-Series device to the back-end pools for the Azure public load balancer and/or internal load balancer. This completes the integration and makes the VM-Series device active.

The Transit VNet design model uses two sets of templates and device groups that correspond to the traffic profiles discussed earlier in the guide. Each traffic profile requires its own bootstrap package, which you create using the parameters in Table 39 and deploy in the corresponding file share directory.

Table 39 Transit VNet template stacks and device groups

Traffic profile	Template stack	Device group	File share and directory
OBEW	Transit-VNet-OBEW	Transit-VNet-OBEW	vmseries-bootstrap/OBEW
Inbound	Transit-VNet Inbound	Transit-VNet Inbound	vmseries-bootstrap/Inbound

17.1 Create the Bootstrap Package

In this procedure, you generate VM auth key on Panorama. This procedure requires the use of the command line. This guide does not include instructions for generating the VM auth key by using API.

Step 1: Using SSH, log in to the Panorama command line.

Step 2: 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.

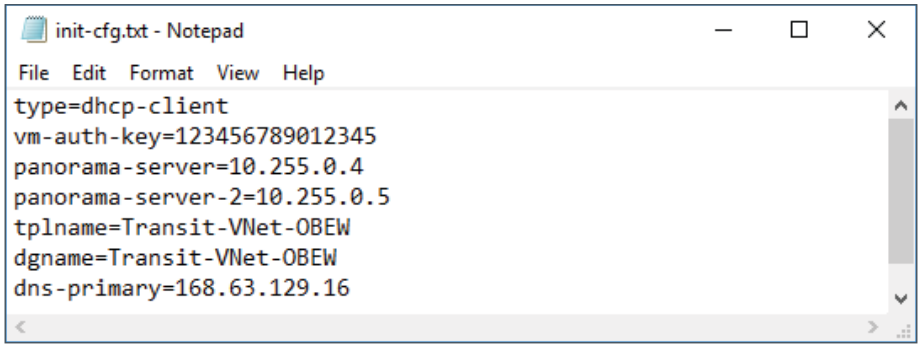
```
request bootstrap vm-auth-key generate lifetime 8760


VM auth key 123456789012345 generated. Expires at: 2020/10/24 07:33:28
```

Step 3: Using the parameters and values in the following table, create a separate init-cfg.txt file for each traffic profile.

The following table includes the parameters required for a successful bootstrap on Azure. The VM-Series device registers with Panorama, and Panorama assigns it to the listed template stack and device group. Create the file by using a text editor and save as init-cfg.txt

Table 40 Required parameters for Azure bootstrapping

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	10.255.0.4
Panorama IP address (secondary)	panorama-server-2 (optional for H/A only)	10.255.0.5 (optional for high-availability only)
Template stack name	tplname	Transit-VNet-OBEW Transit-VNet Inbound
Device group name	dgname	Transit-VNet-OBEW Transit-VNet Inbound

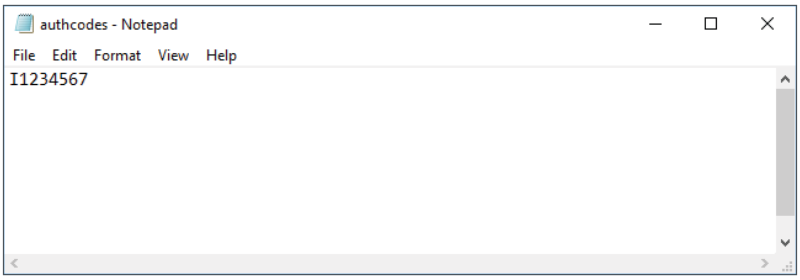


Because you are using BYOL, you must license the firewall during the bootstrap process by using an authcodes file that contains a valid auth code bundle for your organization.

Step 4: Create the authcodes file by using a text editor and saving the file as **authcodes** without a file type extension. An auth code bundle includes all of the VM-Series feature licenses within a single auth code (example: **I1234567**).

Caution

The filename for the authcodes file must not include any file type extension, such as .txt. If you save the file with an extension, the bootstrap process fails.



Step 5: If you do not want to upgrade the software version and install application and content updates, continue to the next procedure.

If you want to upgrade the software version and install application and content updates as part of the bootstrap process, download the VM-Series software and dynamic updates file listed in Table 41 from the Palo Alto Networks customer support portal (https://support.paloaltonetworks.com). Palo Alto Networks provides frequent updates to the content and applications packages and recommends using the latest versions available.

Table 41 Examples of available files for updates

File	Description	Download location
PanOS_vm-8.1.11	PAN-OS version 8.11 for VM-Series firewalls	Updates > Software Updates
panupv2-all-contents-8205-5740	Content package (8205-5740)	Updates > Dynamic Updates
panupv2-all-apps-8205-5740	Applications package (8205-5740)	Updates > Dynamic Updates

17.2 Deploy the Bootstrap Package to Azure Storage

This procedure creates a new file share for bootstrap packages in an existing storage account. Each bootstrap package is located within a unique directory within the file share.

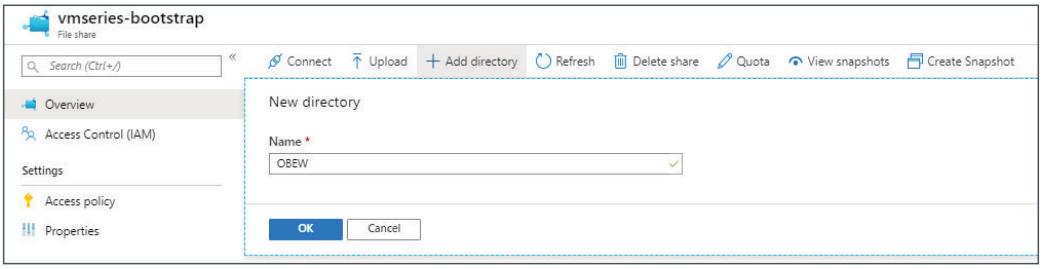
Step 1: In **Home > Storage accounts > azurerav2transit > File service > File shares**, click **File share**.

Step 2: In the **Name** box, enter **vmseries-bootstrap**, and then click **Create**.

Step 3: In Home > Storage accounts > **azurerav2transit** > File service > File shares, click **vmseries-bootstrap**.

Step 4: Click **Add directory**.

Step 5: In the **Name** box, enter **OBEW**, and then click **OK**.



Step 6: Click **Add directory**.

Step 7: In the **Name** box, enter **Inbound**, and then click **OK**.

Next, you create the bootstrap package using the structure provided in Table 42.

Table 42 Bootstrap package structure

Bootstrap directory	Directory name	File	Notes
OBEW	config	init-cfg.txt (for OBEW)	—
OBEW	content	panupv2-all-contents-8205-5740 panupv2-all-apps-8205-5740	Optional
OBEW	license	authcodes	—
OBEW	software	PanOS_vm-8.1.11	Optional
Inbound	config	init-cfg.txt (for inbound)	—
Inbound	content	panupv2-all-contents-8205-5740 panupv2-all-apps-8205-5740	Optional
Inbound	license	authcodes	—
Inbound	software	PanOS_vm-8.1.11	Optional

Step 8: In Home > Storage accounts > **azurerav2transit** — File shares > vmseries-bootstrap, click **OBEW**.

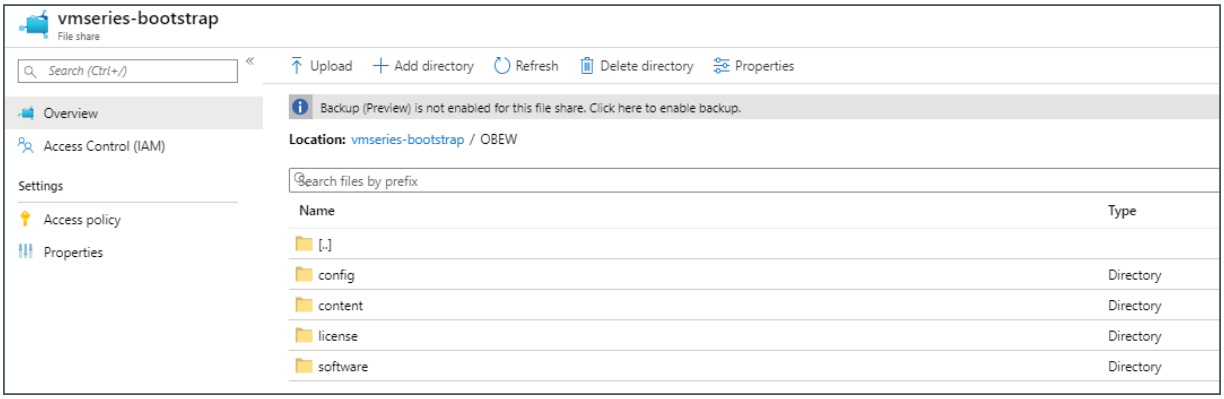
Step 9: Click **Add directory**.

Step 10: In the **Name** box, enter **config**, and then click **OK**.

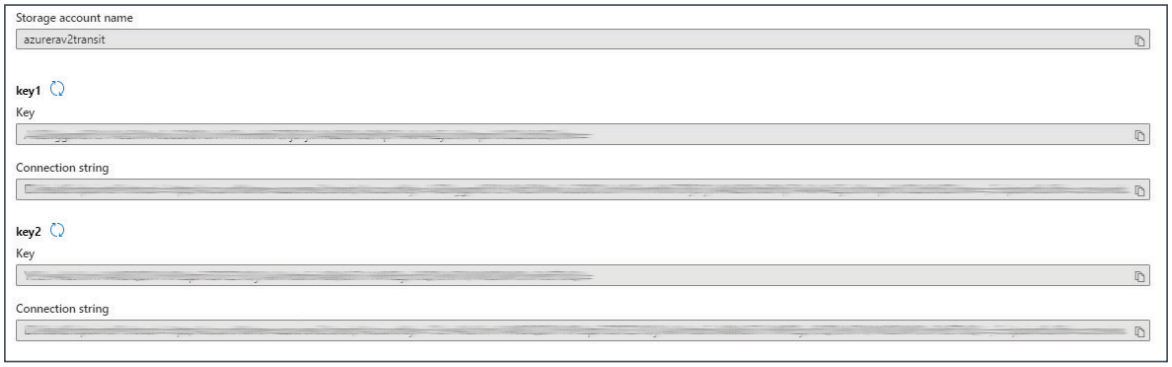
Step 11: For the bootstrap directory you are configuring, do the following for each file listed in the **File** column of Table 42:

- Click the directory name (example: **config**).
- Click **Upload**.
- In the Upload files pane, browse to your local file system, and then select the corresponding file (example: **init-cfg.txt**).
- Click **Upload**.

Step 12: Repeat Step 8 through Step 11 for each entry in Table 42.



Step 13: In **Home > Storage accounts > azurerav2transit > Settings > Access keys**, record the access key for the storage account (either key1 or key2) by using **Click to copy**.



Note

You need to provide the storage account, a valid access key for the storage account, the file share, and the file share directory at deployment time.

The following is an example of these values for an OBEW firewall:
Storage Account Name: azurerav2transit
Access Key: <key>
File Share Name: vmseries-bootstrap
File Share Directory: OBEW

The following is an example of these values for an inbound firewall:
Storage Account Name: azurerav2transit
Access Key: <key>
File Share Name: vmseries-bootstrap
File Share Directory: Inbound

17.3 Create the Public IP Address for the VM-Series Firewalls

This procedure is identical to Procedure 1.7. It is repeated here for completeness.

Unless on-premises network connectivity has been established, you manage the VM-Series devices deployed on Azure by using public IP addresses.

Table 43 Additional Azure resources required for bootstrap deployment

Parameter	Value	Comments
Resource Group	AzureRA-Transit	Existing resource group for transit VNet
Public IP for VM-Series 5 (OBEW)	aratrv-vmfw5	Public IP for management interface
Public IP for VM-Series 6 (Inbound)	aratrv-vmfw6	Public IP for management interface

In this procedure, you create a public IP address that is associated to the management interface of the VM-Series firewalls at deployment time. If necessary, you repeat this procedure to create additional public IP addresses for additional VM-Series devices. Use the parameters listed in Table 43 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. Palo Alto Networks recommends managing your devices by using the DNS name rather than the public IP address, which might change.

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

Step 2: In the SKU section, select **Standard**.

Step 3: In the **Name** box, enter **aratrv-vmfw5**.

Step 4: In the **DNS name label** box, enter **aratrv-vmfw5**.

Step 5: In the **Resource Group** list, choose **AzureRA-Transit**, and then click **Create**.

Procedures

To complete these procedures, you use the Azure Resource Manager deployed from a 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.

18.1 Deploy the VM-Series Firewall with Bootstrap Configuration

This procedure is essentially identical to Procedure 2.1, with additional steps to provide the bootstrap information.

Table 44 VM-Series bootstrap deployment parameters

Parameter	Value	Comments
Resource group	AzureRA-Transit	Existing
Location		Tested in West US
VM name	ARATRV-VMFW5 ARATRV-VMFW6	First bootstrap device (OBEW). Assumes two firewalls already deployed First bootstrap device (Inbound). Assumes two firewalls already deployed
Storage account name	azurerav2transit	—
Storage account existing RG	AzureRA-Transit	—
Fw Av set	ARA-Transit-OBEW-AS	Use for all OBEW firewalls
Fw Av set	ARA-Transit-Inbound-AS	Use for all Inbound firewalls
VM size	Standard_D3_v2	For more information, see Minimum System Requirements for the VM-Series on Azure
Public IP type	standard	Standard-SKU IP addressing required for use with Azure Standard load balancer
Image version	8.1.0	—
Image Sku	byol	—
Bootstrap firewall	yes	—
Bootstrap storage account	azurerav2transit	The bootstrap storage account can be in any resource group within the same Azure subscription and location.
Storage account access key	<key>	Use value recorded from Procedure 17.2, Step 13
Storage account file share	vmseries-bootstrap	Created in Procedure 17.2
Storage account file share directory	OBEW	Use for all OBEW firewalls Created in Procedure 17.2
Storage account file share directory	Inbound	Use for all inbound firewalls Created in Procedure 17.2
Virtual network name	AzureRA-Transit-VNet	—
Virtual network address prefix	10.110.0.0/16	Match the IP address space from AzureRA-Transit-VNet
Virtual network existing RG name	AzureRA-Transit	—
Subnet0Name	Transit-Management	—
Subnet1Name	Transit-Public	—
Subnet2Name	Transit-Private	—
Subnet0Prefix	10.110.255.0/24	—
Subnet1Prefix	10.110.129.0/24	—

Table continued on next page

Continued from previous page

Parameter	Value	Comments
Subnet2Prefix	10.110.0.0/24	—
Subnet0Start Address	10.110.255.8 10.110.255.9	First bootstrap device (OBEW) Second bootstrap device (inbound)
Subnet1Start Address	10.110.129.8 10.110.129.9	First bootstrap device (OBEW) Second bootstrap device (inbound)
Subnet2Start Address	10.110.0.8 10.110.0.9	First bootstrap device (OBEW) Second bootstrap device (inbound)
Admin username	refarchadmin	—
Admin password	<password>	—
Public IP address name	aratrv-vmfw5 aratrv-vmfw6	First bootstrap device (OBEW) Second bootstrap device (inbound)
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-3-interfaces-existing-environment-BS

Use the parameters in Table 44 to deploy each VM-Series firewall with bootstrap configuration.

Step 1: On the template, click **Deploy to Azure**. This deploys the VM-Series firewall.

Step 2: In the **Resource Group** list, choose **AzureRA-Transit**.

Step 3: In the **Vm Name** box, enter **ARATRV-VMFW5**.

Step 4: In the **Storage Account Name** box, enter **azurerav2transit**.

Step 5: In the **Storage Account Existing RG** box, enter **AzureRA-Transit**.

Step 6: In the **Fw Av Set** box, enter **ARA-Transit-OBEW-AS**.

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

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

Step 9: In the **Image Version** list, choose **8.1.0**.

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

Step 11: In the **Bootstrap Firewall** list, choose **yes**.

Step 12: In the **Bootstrap Storage Account** box, enter **azurerav2transit**.

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 **OBEW**.

Step 16: In the **Virtual Network Name** box, enter **AzureRA-Transit-VNet**.

Step 17: In the **Virtual Network Address Prefix** box, enter **10.110.0.0/16**.

Step 18: In the **Virtual Network Existing RG Name** box, enter **AzureRA-Transit**.

Step 19: In the **Subnet0Name** box, enter **Transit-Management**.

Step 20: In the **Subnet1Name** box, enter **Transit-Public**.

Step 21: In the **Subnet2Name** box, enter **Transit-Private**.

Step 22: In the **Subnet0Prefix** box, enter **10.110.255.0/24**.

Step 23: In the **Subnet1Prefix** box, enter **10.110.129.0/24**.

Step 24: In the **Subnet2Prefix** box, enter **10.110.0.0/24**.

Step 25: In the **Subnet0Start Address** box, enter **10.110.255.8**.

Step 26: In the **Subnet1Start Address** box, enter **10.110.129.8**.

Step 27: In the **Subnet2Start Address** box, enter **10.110.0.8**.

Step 28: In the **Admin Username** box, enter **refarchadmin**.

Step 29: In the **Admin Password** box, enter the password.

Step 30: In the **Public IP Address Name** box, enter **aratrv-vmfw5**.

Step 31: In the **Nsg Name** box, enter **None**.

Step 32: Review the terms and conditions. If they are acceptable, select **I agree to the terms and conditions**, and then 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. The device software is upgraded, and application and content updates are applied. After the services are restarted, the device receives template and device group configuration from Panorama and is ready to be managed.

18.2 Outbound Access—Create and Associate a Public IP Address with the Firewall

Perform this procedure for all OBEW firewalls. This procedure is identical to Procedure 9.1. 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. You create a new public IP address for the public interface of each firewall used for outbound access. This method supports all TCP and UDP ports.

Use Azure Resource Manager to complete this procedure.

Step 1: Sign in to Azure at https://portal.azure.com.

Step 2: In **Home > Public IP addresses**, click **Add**.

Step 3: In the SKU section, select **Standard**.

Step 4: In the **Name** box, enter **aratrv-vmfw5-outbound**.

Step 5: In the **DNS name label** box, enter **aratrv-vmfw5-outbound**.

Step 6: In the **Resource Group** list, choose **AzureRA-Transit**, and then click **Create**. You have successfully created the public IP address.

Step 7: In **Home > Public IP address > aratrv-vmfw5-outbound**, click **Associate**.

Step 8: In the Associate Public IP address pane, in the **Resource type** list, choose **Network interface**.

Step 9: In the Choose Network Interface pane, select the public interface of **ARATVR-VMFW5** (example: **ARATRV-VMFW5-eth1**), and then click **OK**.

Step 10: Repeat this procedure for any additional OBEW firewalls.

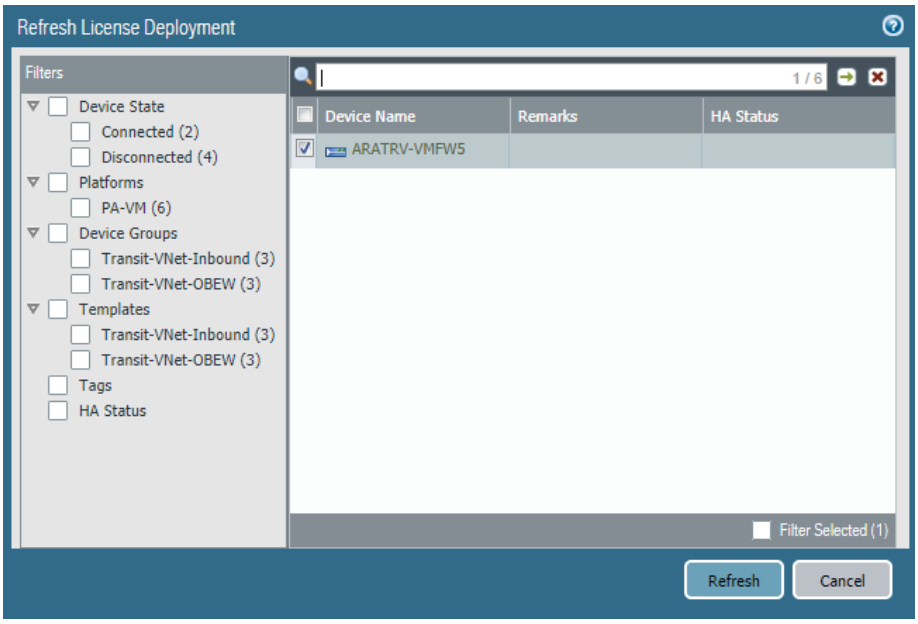
18.3 Refresh License to Enable Log Forwarding to Cortex Data Lake

This procedure is identical to Procedure 4.4 and is included here for completeness.

Step 1: Log in to Panorama (example: https://azurera-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 each VM-Series device, and then click **Refresh**.



Step 4: Verify the details for each VM-Series device include **Successfully installed license 'Logging Service,'** and then click **Close**.

18.4 Add VM-Series Devices to Back-End Pools for Load-Balancer and Application Gateway

You already created the private and public load balancers in Procedure 5.1 and Procedure 6.3, 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 back-end pools.

This procedure only includes the steps to add an additional VM-Series device to existing back-end pools. Repeat this procedure for each VM-Series device as required.

Step 1: Repeat the following for all OBEW firewalls:

- In **Home** > **Load Balancers** > **AzureRA-Transit-Internal**, click **Backend pools**.
- Click **Firewall-Layer-Private**.
- In the Virtual machines section, in the **Virtual machine** column, select a VM-Series firewall that you are adding to this back-end pool (example: **ARATRV-VMFW5-bs**).
- In the Virtual machines section, in the **IP address** column, select the **IP configuration** that is associated to the **Transit-Private** subnet (example: **ipconfig-trust**).
- Click **Save**, and then click **X** to exit.

Step 2: Repeat the following for all inbound firewalls:

- In **Home** > **Load Balancers** > **AzureRA-Transit-Public**, click **Backend pools**.
- Click **Firewall-Layer**.
- In the Virtual machines section, in the **Virtual machine** column, select a VM-Series firewall that you are adding to this back-end pool (example: **ARATRV-VMFW6-bs**).
- In the Virtual machines section, in the **IP address** column, select the **IP configuration** that is associated to the **Transit-Public** subnet (example: **ipconfig-untrust**).
- Click **Save**, and then click **X** to exit.

18.5 Inbound Access (Application Gateway)—Create an Address Object

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

Step 2: Navigate to **Objects**.

Step 3: In the **Device Group** list, choose **Transit-VNet-Inbound**.

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

Step 5: In the **Name** box, enter **ARATRV-VMFW6-Public**.

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

Step 7: In the **Type value** box, enter **10.110.129.9/32**, and then click **OK**.

18.6 Inbound Access (Application Gateway)—Configure the NAT Policy

The application gateway NAT policy rules you created in Procedure 12.3 had specific firewall targets only, and they did not include the devices you created using the bootstrap process. You create the additional NAT policy rules now.

Table 45 NAT translation rules for application gateway

Name	Service	Source objects	Destination address	Translated address/ translated port	Target firewall
Inbound-AppGW-FW-3_HTTP-80	service-http	AppGW-Subnet	ARATRV-VMFW6-Public	AppGW-Internal-LB/80	ARATRV-VMFW6
Inbound-AppGW-FW-3_HTTP-8000	service-http-8000	AppGW-Subnet	ARATRV-VMFW6-Public	Direct-Web/80	ARATRV-VMFW6
Inbound-AppGW-FW-3_HTTP-8081	service-http-8081	AppGW-Subnet	ARATRV-VMFW6-Public	AppGW-Internal-LB/8081	ARATRV-VMFW6
Inbound-AppGW-FW-3_HTTPS-443	service-https	AppGW-Subnet	ARATRV-VMFW6-Public	AppGW-Internal-LB/443	ARATRV-VMFW6
Inbound-AppGW-FW-3_HTTP-8443	service-http-8443	AppGW-Subnet	ARATRV-VMFW6-Public	AppGW-Internal-LB/8443	ARATRV-VMFW6

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

Step 2: Navigate to **Policies**.

Step 3: In the **Device Group** list, choose **Transit-VNet-Inbound**.

Step 4: For each entry in Table 45, perform the following sub-steps:

- In **Policies > NAT > Pre Rules**, click **Add**.
- In the **Name** box, enter **Inbound-AppGW-FW-3_HTTP-80**.
- On the Original Packet tab, in the Source Zone pane, click **Add**, and then select **Public**.
- In the **Destination Zone** list, choose **Public**.
- In the **Service** list, choose **service-http**.
- In the Source Address pane, click **Add**, and then select **AppGW-Subnet**.
- In the Destination Address pane, click **Add**, and then enter **ARATRV-VMFW6-Public**.
- On the Translated Packet tab, in the Source Address Translation section, in the **Translation Type** list, choose **Dynamic IP And Port**.
- In the Source Address Translation section, in the **Address Type** list, choose **Interface Address**.
- In the Source Address Translation section, in the **Interface list**, choose **ethernet1/2**.

- In the Destination Address Translation section, in the **Translation Type** list, choose **Static IP**.
- In the Destination Address Translation section, in the **Translated Address** list, choose **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: **ARATRV-VMFW6**), 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 policies. The target for each set of rules lists only one firewall.

Figure 27 NAT policy rules for the bootstrap inbound firewall

	Name	Location	Original Packet						Translated Packet		Target
			Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation	
4	Inbound-AppGW-FW-3_HTTP-80	Transit-VNet-Inbound	Public	Public	any	AppGW-Subnet	ARATRV-VMFW6-Public	service-http	dynamic-ip-and-port ethernet1/2	destination-translation address: AppGW-Internal-LB port: 80	ARATRV-VMFW6
7	Inbound-AppGW-FW-3_HTTP-8000	Transit-VNet-Inbound	Public	Public	any	AppGW-Subnet	ARATRV-VMFW6-Public	service-http-8000	dynamic-ip-and-port ethernet1/2	destination-translation address: Direct-Web port: 80	ARATRV-VMFW6
10	Inbound-AppGW-FW-3_HTTP-8081	Transit-VNet-Inbound	Public	Public	any	AppGW-Subnet	ARATRV-VMFW6-Public	service-http-8081	dynamic-ip-and-port ethernet1/2	destination-translation address: AppGW-Internal-LB port: 8081	ARATRV-VMFW6
13	Inbound-AppGW-FW-3_HTTPS-443	Transit-VNet-Inbound	Public	Public	any	AppGW-Subnet	ARATRV-VMFW6-Public	service-https	dynamic-ip-and-port ethernet1/2	destination-translation address: AppGW-Internal-LB port: 443	ARATRV-VMFW6
16	Inbound-AppGW-FW-3_HTTP-8443	Transit-VNet-Inbound	Public	Public	any	AppGW-Subnet	ARATRV-VMFW6-Public	service-http-8443	dynamic-ip-and-port ethernet1/2	destination-translation address: AppGW-Internal-LB port: 8443	ARATRV-VMFW6

18.7 Inbound Access (Application Gateway)—Configure the Security Policy

The application gateway security policy rules you created in Procedure 12.4 had specific firewall targets only, and they did not include the devices you created using the bootstrap process. You create the additional security policy rules now.

Table 46 Services for the 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

Each firewall needs a unique security policy rule. In Step 6, the destination address must match the IP address of the public interface of each firewall. If your firewall layer includes additional firewalls, then you must add a new rule for each additional firewall.

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

Step 2: In the **Name** box, enter **Inbound-AppGW-FW-3**.

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

Step 4: In the Source Address pane, click **Add**, and then select **AppGW-Subnet**.

Step 5: On the Destination tab, in the Destination Zone pane, click **Add**, and then select **Private**.

Step 6: In the Destination Address pane, click **Add**, and then enter **ARATRV-VMFW6-Public**.

Step 7: On the Application tab, in the Applications pane, click **Add**.

Step 8: In the search box, enter **web-browsing**, and then in the results list, choose **web-browsing**.

Step 9: In the Applications pane, click **Add**.

Step 10: In the search box, enter **ssl**, and then in the results list, choose **ssl**.

Next, you configure the application gateway 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, you must explicitly list each service in use.

Step 11: On the Service/URL Category tab, in the Service pane, click **Add** and select each service listed in Table 46.

Step 12: On the Actions tab, in the Action Setting section, in the **Action** list, choose **Allow**.

Step 13: In the Profile Setting section, in the **Profile Type** list, choose **Profiles**.

Step 14: In the Profile Setting section, in the **URL Filtering** list, choose **Enable-XFF-Logging**.

Step 15: In the Log Setting section, in the **Log Forwarding** list, choose **CortexDL**.

Step 16: On the Target tab, select only the firewall target from the current entry in the table (example: **ARATRV-VMFW6**), 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 policies. The target for each rule lists only one firewall.

				Source		Destination							
	Name	Location	Type	Zone	Address	Zone	Address	Application	Service	Action	Profile	Options	Target
5	Inbound-AppGW-FW-3	Transit-VNet-Inbound	universal	Public	AppGW-Subnet	Private	ARATRV-VMFW6-Public	ssl web-browsing	service-http service-http-8000 service-http-8081 service-http-8443 service-https	Allow			ARATRV-VMFW6

Step 17: On the **Commit** menu, click **Commit and Push**.

18.8 Inbound Access (Application Gateway)—Add VM-Series Devices to the Application Gateway Back-End Pool

You already created the application gateway in 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 application gateway back-end pool.

This procedure includes the steps to add an additional VM-Series device to an existing back-end pool. Repeat this procedure for each VM-Series device as required.

Perform this procedure for inbound firewalls only.

Step 1: In **Home > Application Gateways > AzureRA-Transit-AppGW**, click **Backend pools**.

Step 2: Click **Firewall-Layer**.

Step 3: In the Backend targets section, in the **Target type** list, choose **Virtual machine**.

Step 4: In the Backend targets section, in the **Target** list, choose the VM-Series interface associated to the Transit-Public subnet for the inbound access traffic profile (example: **ARTRV-VMFW6-eth1**).

Step 5: Click **Save**, and then click **X** to exit.

Step 6: Repeat this procedure for each VM-Series device as required.

You can use the feedback form to send comments about this guide.

HEADQUARTERS

Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054, USA
http://www.paloaltonetworks.com

Phone: +1 (408) 753-4000
Sales: +1 (866) 320-4788
Fax: +1 (408) 753-4001
info@paloaltonetworks.com

B-000118P-1 01/20