Securing Applications in AWS Single VPC

DEPLOYMENT GUIDE

JUNE 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:

- Changed the version of PAN-OS® to version 9.1.2.
- Changed the version of the Cloud Services plugin to version 1.6.0
- Moved the Panorama™ installation and initial configuration to the *Panorama on AWS: Deployment Guide*.
- Changed phrasing, terminology, and diagrams for clarity

Purpose of This Guide

This guide provides reference architectures for Palo Alto Networks VM-Series virtual firewalls in the Amazon Web Services (AWS) public cloud.

This guide:

- Provides architectural guidance and deployment details for using Palo Alto Networks VM-Series firewalls to provide visibility, control, and protection to your applications built in in an AWS public cloud.
- Requires that you first read the Securing Applications in AWS: Reference Architecture Guide. The reference architecture guide provides design insight and guidance necessary for your organization to plan linkage of pertinent features with the next-generation firewall in a resilient design.
- Provides deployment details for the Single Virtual Private Cloud (VPC) design model, which is well-suited for initial deployments and proof of concepts of Palo Alto Networks VM-Series firewalls in AWS. This guide describes deploying VM-Series firewalls to provide visibility and protection for the VPC's inbound and outbound traffic.
- Provides deployment details for the VM-Series firewall working with AWS load balancers, which provides a resilient design for inbound HTTP traffic and simple connectivity back to on-premises services.
- Provides decision criteria for deployment scenarios, as well as procedures for enabling features of the AWS and the Palo Alto Networks VM-Series firewalls in order to achieve an integrated design.

OBJECTIVES

Completing the procedures in this guide, you are able to successfully deploy a Palo Alto Networks VM-Series firewall in the AWS environment. You also enable the following functionality:

- Application layer visibility and control for traffic inbound from the internet or VPN and traffic outbound from the VPC.
- Firewalls that are prepared to enable full malware and threat prevention services and that connect to WildFire® analytics.
- Centralized logging with Cortex™ Data Lake, which also enables cloud-delivered security analytics.
- Resilient design with the integration of AWS load balancing with VM-Series firewalls.
- Efficient deployment by using Panorama to manage configurations and policy.

AUDIENCE

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

RELATED DOCUMENTATION

The following documents support this guide:

- Securing Data in the Private Data Center and Public Cloud with Zero Trust—Describes how your organization can use the Palo Alto Networks Strata, Prisma™, and Cortex platforms in the design of a Zero Trust security policy in order to protect your sensitive and critical data, applications, endpoints, and systems.
- Securing Applications in AWS: Reference Architecture Guide—Presents a detailed discussion of the available design considerations and options for securing data and applications in the AWS public cloud infrastructure.
- Panorama on AWS: Deployment Guide—Details the deployment of Palo Alto Networks Panorama management nodes in the AWS VPC. The guide includes setup of Panorama in a high-availability configuration and setup of Cortex Data Lake.

Deployment Overview

The Securing Applications in AWS: Reference Architecture Guide describes AWS concepts that provide a cloud-based Infrastructure as a Service and describes how the Palo Alto Networks VM-Series firewalls can complement and enhance the security of applications and workloads in the cloud. The design models presented in the reference architecture guide provide visibility and control over traffic inbound to the applications in AWS, outbound to on-premises or internet services, and flows internal to the VPC.

Design Models

There are many ways to use the concepts discussed in the previous sections to build a secure architecture for application deployment in AWS. The design models in this section offer example architectures for centralized management and securing inbound and outbound application traffic flows, communication between private instances, and the connection to your on-premises networks.

As part of the overall AWS architecture, you use a separate management VPC to create a centralized management location so that a single Panorama deployment can manage VM-Series firewalls deployed across all of your organization's VPCs. Panorama streamlines and consolidates core tasks and capabilities, enabling you to view all your firewall traffic, manage all aspects of device configuration, push global policies, and generate reports on traffic patterns or security incidents. You deploy Panorama in Management-Only mode and securely access it over the public internet. The VM-Series firewalls encrypt and send all firewall logs to Cortex Data Lake over TLS/SSL connections.

The design models presented here differ in how they provide resiliency, scale, and services for the design. The design models in this reference design are:

- **Single VPC**—Proof-of-concept or small-scale, multipurpose design
- **Transit Gateway**—High-performance solution for connecting large quantities of VPCs, with a scalable solution to support inbound, outbound, and east-west traffic flows through separate dedicated security VPCs

CHOOSING A DESIGN MODEL

When choosing a design model, consider the following factors:

- **Scale**—Is this deployment an initial move into the cloud and a proof of concept? Will the application load need to scale quickly and modularly? Are there requirements for inbound, outbound, and east-west flows? The Single VPC design model provides inbound traffic control and scale, outbound control, and outbound scale on a per-availability-zone basis. The Transit Gateway design model offers the benefits of a highly scalable design for multiple VPCs connecting to a central hub for inbound, outbound, and VPC-to-VPC traffic control and visibility.
- **Resilience and availability**—What are the application requirements for availability? The Single VPC model provides a robust inbound design with load balancers to spread the load, detect outages, and route traffic to operational firewalls and instances. The Transit Gateway model provides a highly resilient and available architecture for inbound, outbound, and east-west traffic flows.
- **Complexity**—Understanding application flows and how to scale and troubleshoot is important to the design. Placing all services in a single VPC might seem efficient but could be costly in design complexity. Beyond the initial implementation, consider the Transit Gateway design model for a more intuitive and scalable design.

SINGLE VPC DESIGN MODEL

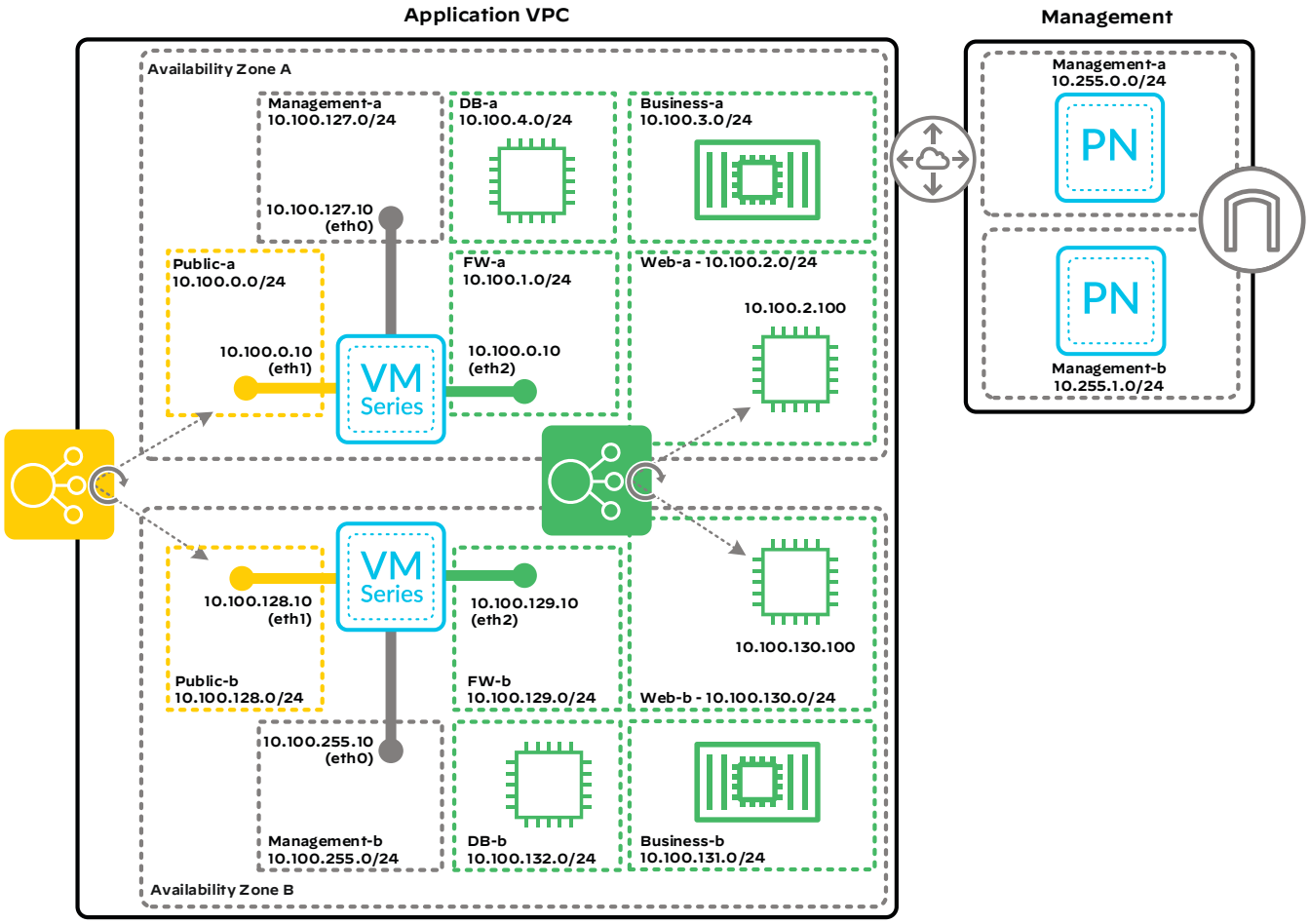
A single standalone VPC might be appropriate for small AWS deployments that:

- Provide the initial move to the cloud for an organization.
- Require a starting deployment that they can build on for a multi-VPC design.

For application resiliency, the architecture consists of a pair of VM-Series firewalls, one in each availability zone within your VPC. You sandwich the firewalls between load balancers for resilient inbound web application traffic and the return traffic. The firewalls are capable of inbound and outbound traffic inspection that is easy to support and transparent to DevOps teams.

You can use security groups and network access control lists to further restrict traffic to individual instances and between subnets. This design model provides the foundation for other architectures in this guide.

Figure 1 Single VPC design model



Inbound Traffic

For resiliency, you deploy two VM-Series firewalls, each in separate availability zones.

There are two options for load balancing inbound traffic:

- **Network Load Balancer**—Choose this option if you require load balancing only at Layer 4 (TCP/UDP). Health checks monitor the application instances through TCP or web server responses.
- **Application Load Balancer**—Choose this option if you require load balancing at Layer 7 (the application layer) for HTTP and HTTPS. The application load-balancer capabilities include host- and path-based routing as well as SSL offloading. Health checks in this design directly monitor the health of the target web server instances.

Inbound Traffic with a Network Load Balancer

For inbound traffic, a Network Load Balancer (NLB) distributes inbound traffic to the VM-Series firewalls. The NLB is associated with the availability zones that contain VM-Series firewalls. Because the NLB proxies the inbound traffic, you can use security group rules on the public interfaces of the firewalls to allow only inbound traffic from other IP addresses on the public subnets.

The NLB forwards traffic destined to the load balancer's FQDN and port pair to the VM-Series firewalls in the target pool. Common ports required for inbound traffic include TCP port 80 (HTTP) and TCP port 443 (HTTPS). The load balancer distributes traffic between the VM-Series firewalls based on the traffic *5-tuple*, which is the source zone, source IP address, destination zone, destination IP address, and destination port defined in the security policy. The public load balancer's health checks monitor target instance availability through the VM-Series firewalls to the private instances.

Access control lists (ACLs) block all inbound traffic to the private instances except for TCP 80 and 443 traffic that traverses through the VM-Series firewall. This approach ensures that internet traffic can communicate with private instances only through the firewall.

The VM-Series firewall applies both a destination and source IP address translation to inbound traffic. The firewall translates the destination IP address from the private IP address of the firewall's public interface to the private instance or load balancer in the private subnets. The firewall translates the source IP address to 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 instances in the private subnets while firewall security profiles prevent known malware and vulnerabilities from entering the network in traffic allowed by the security policy.

Inbound Traffic with Application Load Balancer

For inbound traffic, the Application Load Balancer (ALB) terminates incoming connections to its frontend and initiates corresponding new connections to the VM-Series firewalls in the target pool. The ALB is associated with the availability zones that contain VM-Series firewalls. If you configure the ALB for

multiple web applications that are behind the same set of VM-Series firewalls, you must define unique target pools for each application. Each target pool contains the same VM-Series firewall instance groups but has unique TCP ports assigned.

AWS sources all new connections from the Application Load Balancer interfaces in the public subnets. The destination IP address is the private IP address of the VM-Series firewall's public interface. Health checks monitor backend availability on all specified HTTP and HTTPS ports.

Destination IP address translation rules on the VM-Series firewalls map incoming traffic from the ALB frontend to the private instance or internal load balancer. The VM-Series firewall also applies a source IP address translation to inbound traffic. The firewall translates the source IP address to the IP address of the private interface of the firewall, ensuring return traffic flows symmetrically.

The VM-Series firewall security policy allows HTTP and HTTPS application traffic from the load balancer to the private instances, and VM-Series firewall security profiles prevent known malware and vulnerabilities from entering the network in traffic allowed by the security policy. If you want to support the use of HTTP and HTTPS backends on ports other than 80 or 443, you should configure the services of the security policy rules to include the specific service ports in use instead of *application-default*.

Outbound Traffic

The VM-Series firewalls protect outbound traffic flows and associated return traffic against threats. Configure the route tables for the private subnets so that their default route points to the VM-Series firewall's private interface in their availability zone. You configure the subnets associated with the first availability zone to exit the VPC through the firewall in the first availability zone, and you configure the subnets in the second availability zone to point to the second firewall. This configuration provides resilience for outbound and return traffic on an availability-zone basis.

You use VM-Series firewall security policies to limit what applications and resources the private instances can reach. In most designs, the VM-Series firewall does not need to translate the destination IP address. The VM-Series firewall must translate the source IP address to the IP address of the VM-Series firewall's public interface. Without this source NAT, traffic might not return to the firewall. The default route in the public subnets route table directs traffic from the VM-Series firewall to the internet gateway (IGW). When the outbound traffic leaves the public VPC network, the IGW translates the source address to the public IP address associated to the VM-Series firewall's public interface.

The VM-Series firewall security policy allows appropriate application traffic from private instances to the internet. You should implement the outbound 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

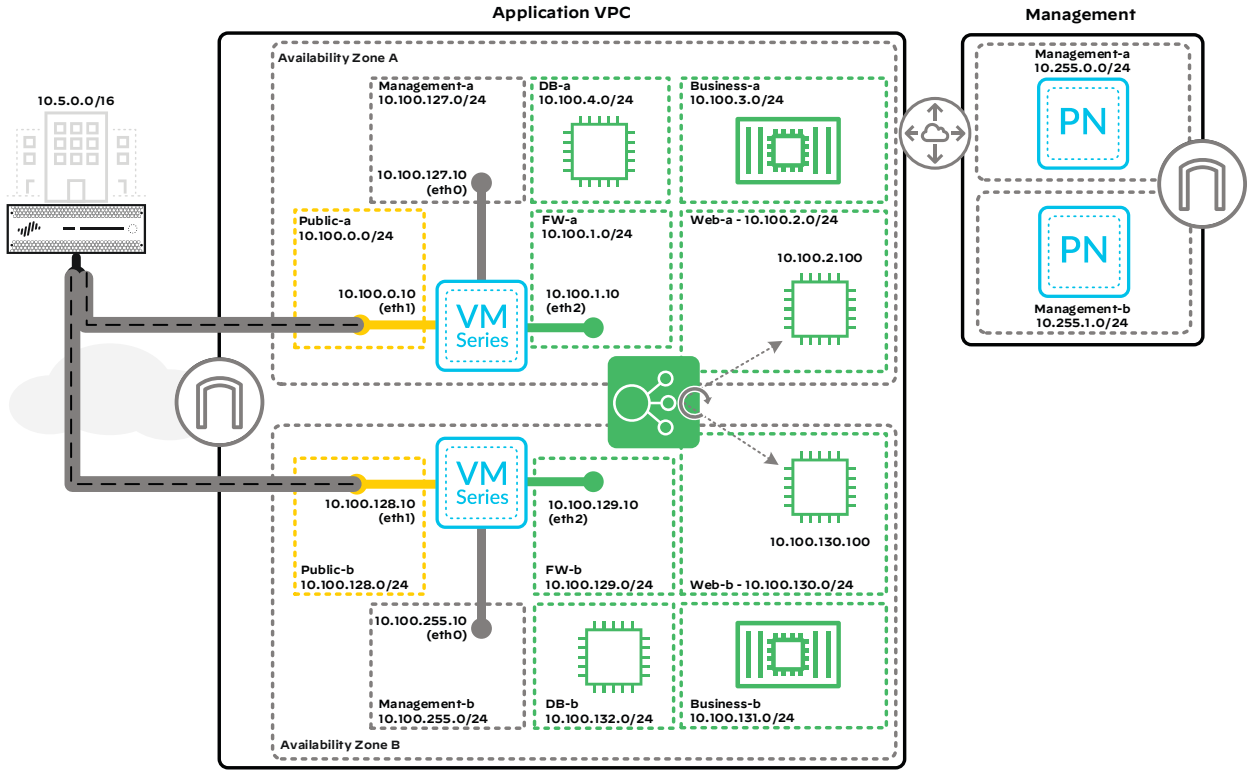
East-west traffic, or traffic between subnets within a VPC, always goes directly between instances. AWS route tables cannot override this behavior, and a limitation of the Single VPC design model is that the VM-Series firewall cannot have control over or visibility to east-west traffic. You can use network ACLs to restrict traffic between subnets. Still, they are not a replacement for the visibility and control provided by the VM-Series firewalls if you need to segment out instances within a VPC. Consider the Transit Gateway design model if you need visibility and control over east-west traffic flows.

Backhaul or Management Traffic

To get traffic from on-premises resources to private instances, VPN connections from on-premises gateways connect to the VM-Series firewalls. Depending on the resiliency required, one or more IPSec tunnels should connect from each of the AWS VM-Series firewalls to the on-premises gateways. The default route configuration for outbound traffic in the private subnets provides the path for traffic from the private instances to reach on-premises resources through the VM-Series firewalls and vice versa. Backhaul traffic has the same resilience characteristics as the outbound traffic flows.

The IPSec tunnels terminate on the public interface of the VM-Series firewall. The VPN tunnel interfaces on the VM-Series firewalls are part of a VPN security zone so that you can configure a policy for VPN connectivity that is separate from the outbound public network traffic. Security policies on the VM-Series firewalls only allow required applications through the dedicated connection from the on-premises resources in the VPN security zone.

Figure 2 Single VPC design model—VPN connection



TRANSIT GATEWAY DESIGN MODEL

This guide describes two designs for providing a scalable, secure architecture for the transit gateway (TGW):

- Multiple security VPCs with VPC-only attachments
- Multiple security VPCs with VPC and VPN attachments

This guide briefly covers the first design and then provides more detail about the second, which is the recommended approach because it routes around failures faster by using dynamic routing and Equal Cost Multipath (ECMP).

In both designs, you connect the spoke VPCs with a VPC attachment. The spoke VPCs can scale up to thousands of VPCs.

What differs between the designs is how you attach the VPCs that contain the VM-Series firewalls to the TGW. You deploy three security VPCs, each with a pair of VM-Series firewalls. Each security VPC controls a specific traffic flow: inbound traffic, outbound traffic, and east-west traffic. Even though you could deploy one security VPC with a pair of firewalls for all traffic, separating the security for each traffic flow allows you to scale up that security function when needed. For example, you might need more firewalls for inbound and its return traffic than for outbound or east-west traffic.

For resiliency, deploy the firewalls in different availability zones.

You can connect your on-premises networks via AWS Direct Connect, VPNs, or both.

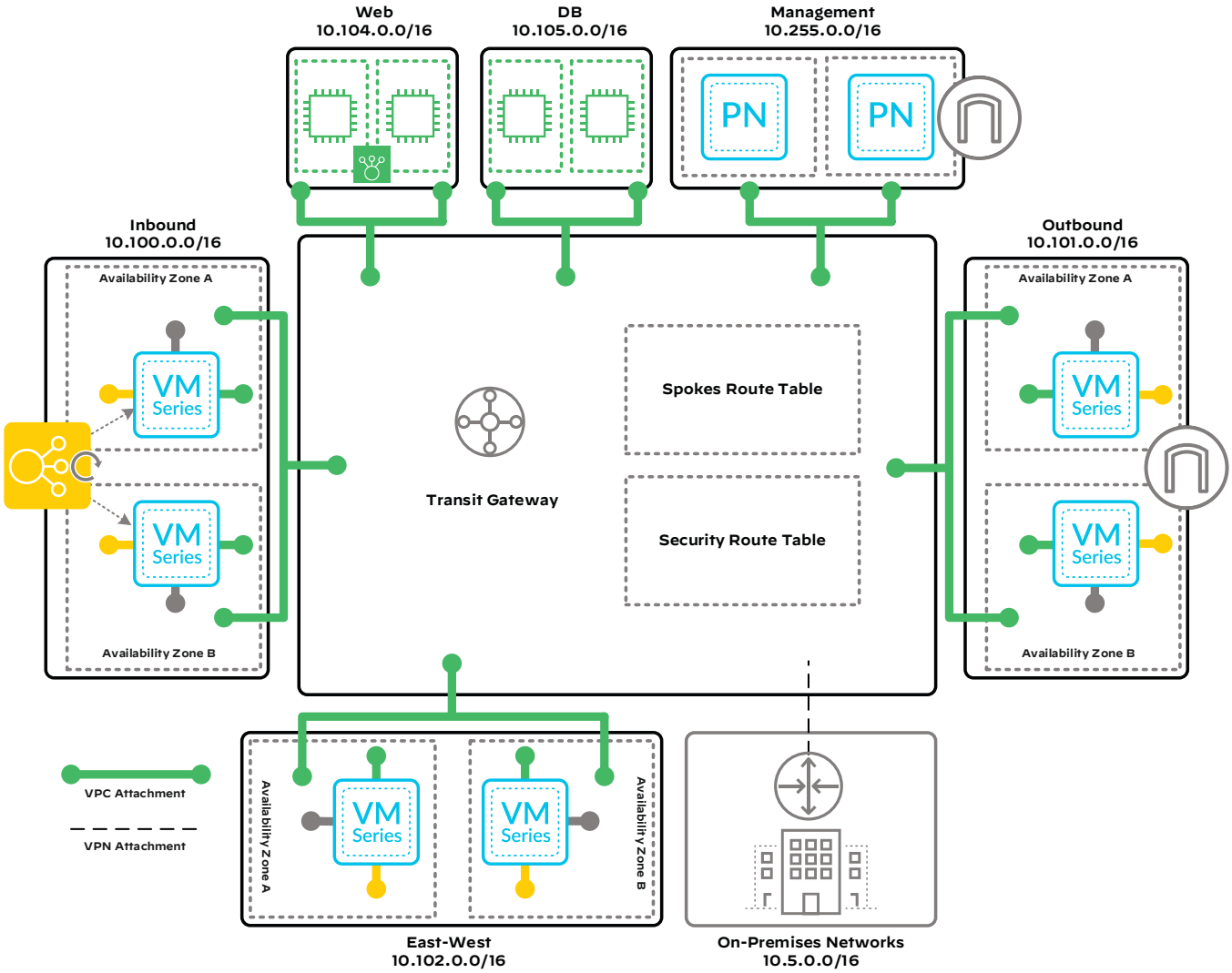
A VPN connection has a limit of 1.25Gbps. To overcome the VPN bandwidth limitation, you can use ECMP routing to aggregate multiple VPN connections. These designs allocate one subnet per availability zone for the network interfaces of the VPC attachment.

Multiple Security VPCs with VPC-Only Attachments

In this design, you attach the three security VPCs (Security-In, Security-Out, and Security-East-West) to the TGW with VPC attachments. With the VPC-only attachment method for the outbound and east-west security VPCs, AWS limits you to static routing; there is no ECMP support. During an outage, you must reconfigure the static routes to an alternative firewall's network interface. You can do this manually or automate it by using AWS CloudWatch, AWS Lambda, and an AWS CloudFormation template script for detection and failover of the firewalls. This automation can take minutes, which is challenging for many customers.

The advantage of VPC attachment is a simple, high-bandwidth design with no VPN tunnels. The disadvantages are the lack of support for ECMP and the inability to provide fast, automatic failover for the firewalls securing outbound and east-west traffic flows.

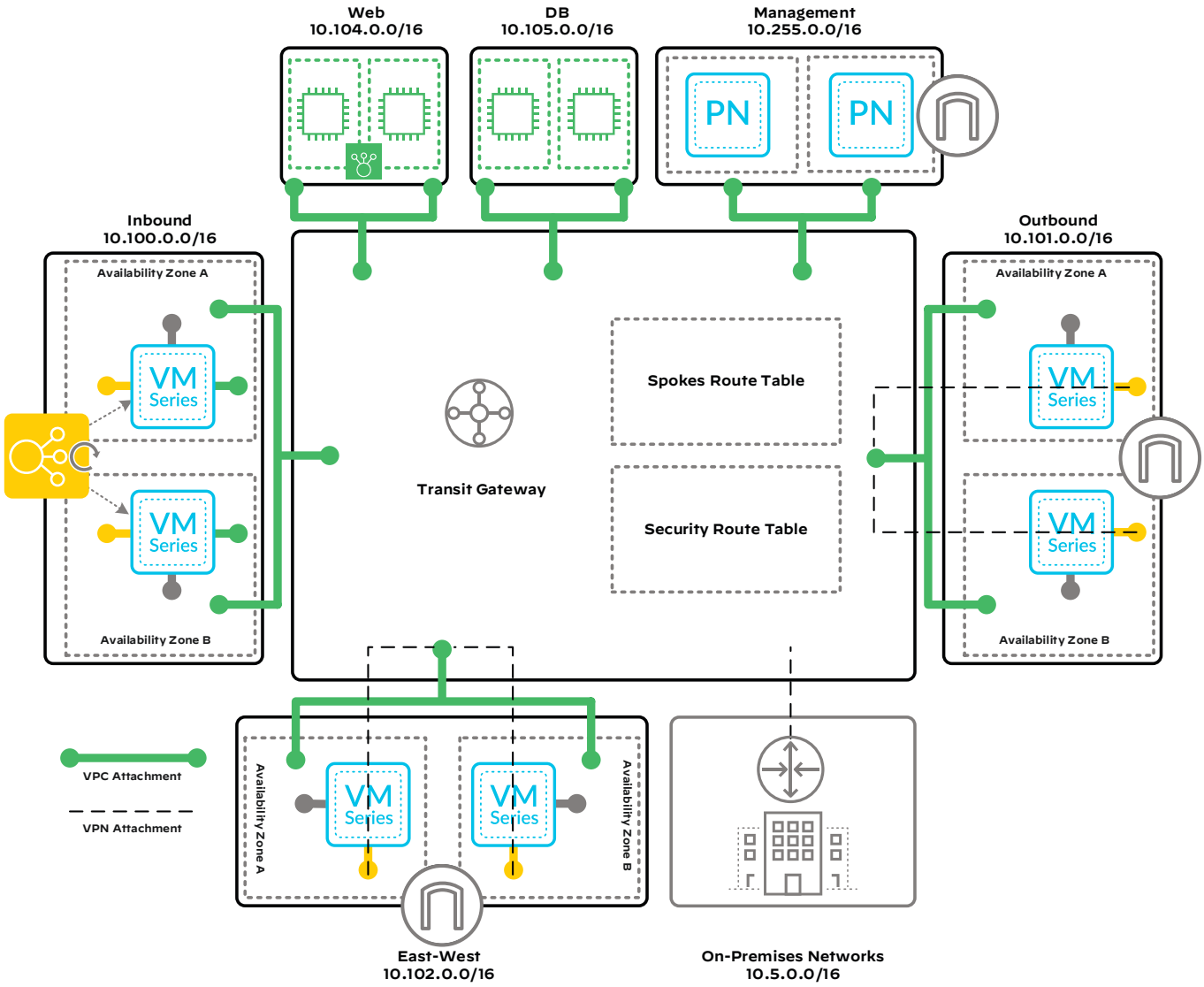
Figure 3 Multiple security VPCs with VPC-only attachments



Multiple Security VPCs with VPC and VPN Attachments

This design is recommended over the VPC-only design because it quickly detects and corrects path failures in the outbound and east-west security VPCs by using ECMP and dynamic routing. In this design, the inbound security VPC uses a VPC attachment type because the load balancers in the inbound security VPC ensure path connectivity and rapid failover. In this design, the outbound and east-west security VPCs connect to the TGW via VPN attachment for data traffic and via a VPC attachment for the firewall management traffic. This ensures a fast recovery time during an outage in the availability zone or VM-Series firewall.

Figure 4 Multiple security VPCs with both VPC and VPN attachments



TGW Design

The TGW design uses two route tables (spokes and security) with all the necessary propagated routes. The TGW in this scenario has:

- VPC attachments for each spoke VPC.
- One VPC attachment for the inbound security VPC.
- Two VPN attachments for the outbound security VPC (two IPSec VPNs from each firewall to the TGW).
- Two VPN attachments for the east-west security VPC (two IPSec VPNs from each firewall to the TGW).
- One VPC attachment for the outbound security VPC, for firewall management in the event that the VPN tunnels are down.
- One VPC attachment for the east-west security VPC, for firewall management in the event that the VPN tunnels are down.

Routing

TGW route tables behave like route domains. You can achieve segmentation of the network by deploying multiple route tables on the TGW and associating VPCs and VPNs to them. You can create isolated networks, allowing you to steer and control traffic flow between VPCs and on-premises connections. This design uses two TGW route tables: security and spokes. The security route table on the TGW has all of the routes propagated to it so that the VM-Series firewall can reach all the VPCs. The spokes route table on the TGW has routes to all the security VPCs but does not have direct routes to other spokes. Only including the routes to the VM-Series firewalls ensure spoke-to-spoke communication can only occur through the VM-Series firewalls in the east-west security VPC.

On the spoke VPCs, VPC route tables route traffic to the TGW. After traffic reaches the TGW, TGW route tables route the traffic to the destination VPC. TGW attachments are associated with a single TGW route table. Each table can have multiple attachments.

You can configure static routes within the TGW route table, or you can use the TGW attachments to propagate routes into the TGW route table. Routes that propagate across a VPN connection with BGP support ECMP.

VPC attachments don’t support ECMP. Static routes allow only a single route of the same destination, pointing to a single next hop. This means you can’t configure two default routes in the same route table in order to separate next hops.

Note

Even though the TGW route tables can support up to 10,000 routes, the BGP prefix limitation is 100 prefixes per virtual gateway.

Spoke VPCs

Private instances are distributed across the spoke VPCs. The spoke VPCs support direct connection to individual instances or to internal load balancers that distribute traffic between instances within the VPC. In the TGW, don't propagate the spoke VPC routes in the spokes routing table, only propagate it to the security routing table. This routing design ensures east-west traffic between spoke VPCs flows to the VM-Series firewalls in the east-west security VPC.

In this design, each spoke VPC has a default route in the VPC routing table pointing to the TGW as the next hop. The TGW route table for the spoke VPCs has the routes mentioned previously in the Routing section, to allow the spoke VPCs to reach the security VPCs and the on-premises network. For routing between the spoke VPCs, they have to route via the firewalls in the east-west security VPC.

Inbound Traffic

This design deploys a VPC dedicated to inbound security with VM-Series firewalls. The inbound security VPC attaches to the TGW through a VPC attachment. The VPC attachment terminates into the inbound security VPC in a dedicated subnet, one per availability zone.

You deploy the two VM-Series firewalls in separate availability zones and deploy an IGW and ALB to distribute incoming traffic to the firewalls. Each firewall's public-facing, private-facing, and management interfaces attach to separate subnets. Each type of subnet has a separate route table as follows:

- The management route table has the management subnets assigned to it, a default route to the IGW for internet access, and a route to the TGW for access to Panorama.
- The public route table has the public subnets assigned to it and a default route to the IGW for internet access.
- The private route table has the private subnets assigned to it and a static route to the TGW for access to the other VPCs attached to the TGW. To make configuration easier, try to use easily summarized IP address blocks for the spoke VPCs.

You do not need to modify the default routing of the subnets dedicated to the TGW attachment. By default, they can reach all the IP addresses within the inbound security VPC.

The VM-Series firewalls have static routes for all internal networks reachable through the TGW, while the VM-Series firewall's public interface obtains a default route through DHCP.

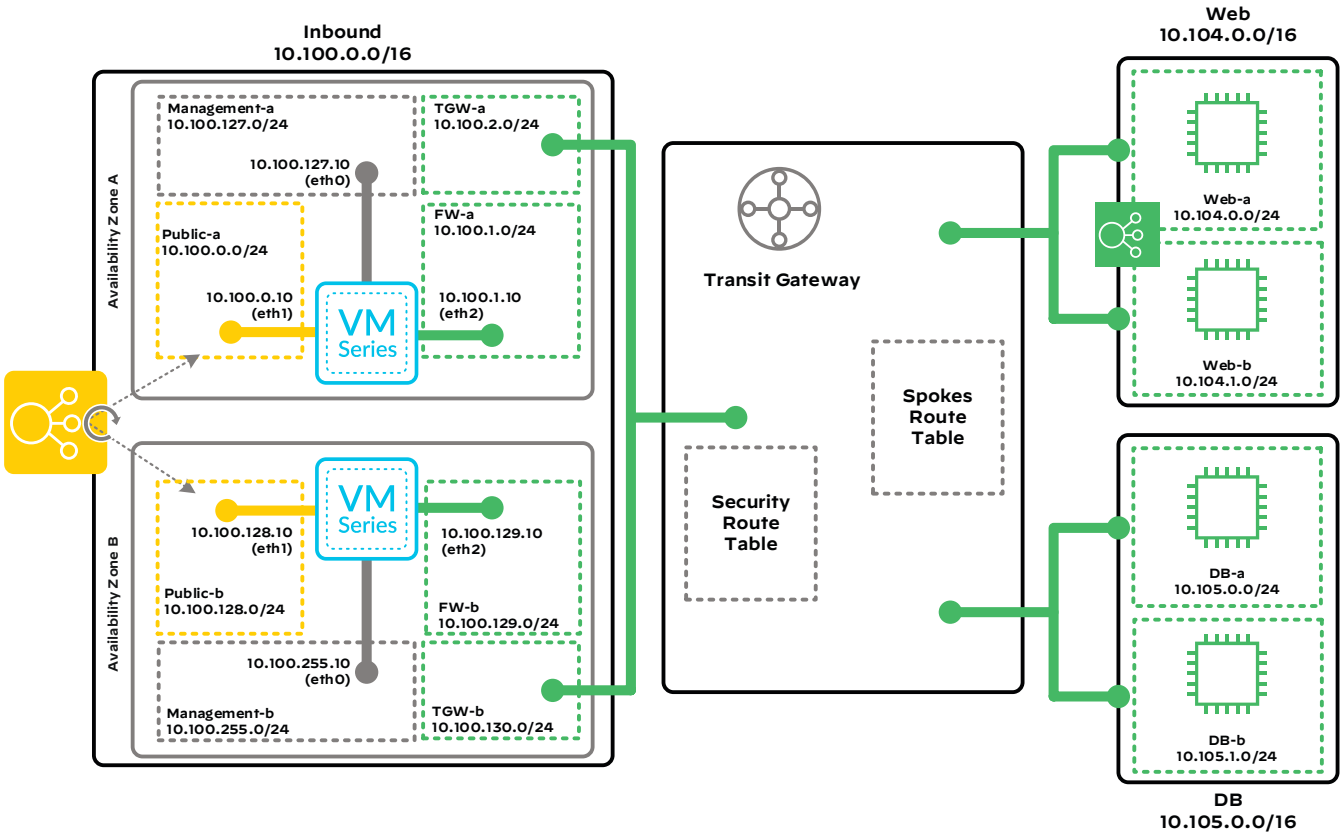
For inbound traffic, the ALB terminates incoming connections to its frontend and initiates corresponding new connections to the VM-Series firewalls in the target pool. The ALB is associated with the availability zones that contain VM-Series firewalls. If you configure the ALB for multiple web applications that are behind the same set of VM-Series firewalls, you must define unique target pools for each application. Each target pool contains the same VM-Series firewall instance groups but has unique TCP ports assigned.

AWS sources all new connections from the Application Load Balancer interfaces in the public subnets. The destination IP address is the private IP address of the VM-Series firewall's public interface. Health checks monitor backend availability on all specified HTTP and HTTPS ports.

Destination IP address translation rules on the VM-Series firewalls map incoming traffic from the ALB frontend to the private instance or internal load balancer. The VM-Series firewall also applies source IP address translation to inbound traffic. The firewall translates the source IP address to the IP address of the private interface of the firewall, ensuring return traffic flows symmetrically.

The VM-Series firewall security policy allows HTTP and HTTPS application traffic from the load balancer to the private instances, and VM-Series firewall security profiles prevent known malware and vulnerabilities from entering the network in traffic allowed by the security policy. If you want to support the use of HTTP and HTTPS backends on ports other than 80 or 443, you should configure the services of the security policy rules to include the specific service ports in use instead of *application-default*.

Figure 5 Inbound security



After inbound traffic egresses the VM-Series firewall, the private route table directs the traffic to the TGW. The TGW uses the security route table to direct traffic to the correct spoke VPC. The TGW attachment in the spoke VPC communicates directly with the instance or load balancer in the VPC.

Return traffic follows a default route to the TGW. The TGW uses the spokes route table to direct traffic to the inbound security VPC. The TGW attachment in the inbound security VPC communicates directly with the VM-Series firewall instance, which returns the traffic towards the internet.

Outbound Traffic

This design deploys a VPC dedicated to outbound security with VM-Series firewalls. You connect the VPC to the TGW through two VPN attachments that connect to the two firewalls deployed in the outbound security VPC. Each firewall has two IPSec tunnels, one to each VPN attachment.

The VPC also attaches to the TGW through a VPC attachment for management. The VPC attachment terminates into the outbound security VPC in a dedicated subnet, one per availability zone.

You deploy the two VM-Series firewalls in separate availability zones and deploy an IGW for connectivity to the internet. Each firewall's public-facing and management interfaces are attached to separate subnets. Each type of subnet has a separate route table as follows:

- The management route table has the management subnets assigned to it, a default route to the IGW for internet access, and a route to the TGW for access to Panorama. Use the VPC attachment for this route.
- The public route table has the public subnets assigned to it and a default route to the IGW for internet access and connectivity to the TGW through VPN.

You do not need to modify the default routing of the subnets dedicated to the TGW attachment. By default, they can reach all the IP addresses within the inbound security VPC.

Because the connectivity to the TGW is across an IPSec tunnel, you do not need to configure a private interface on the firewall. The VM-Series firewalls peer to the TGW using eBGP and advertise a default route across their IPSec tunnels. ECMP and dynamic routing using BGP provide peer detection and failover.

Default routes in the spoke VPCs direct outbound traffic to the TGW. In order to direct traffic to one of the VM-Series firewalls in the outbound security VPC, the TGW uses the spokes route table and the default route learned from the VPN attachments to the VM-Series firewalls.

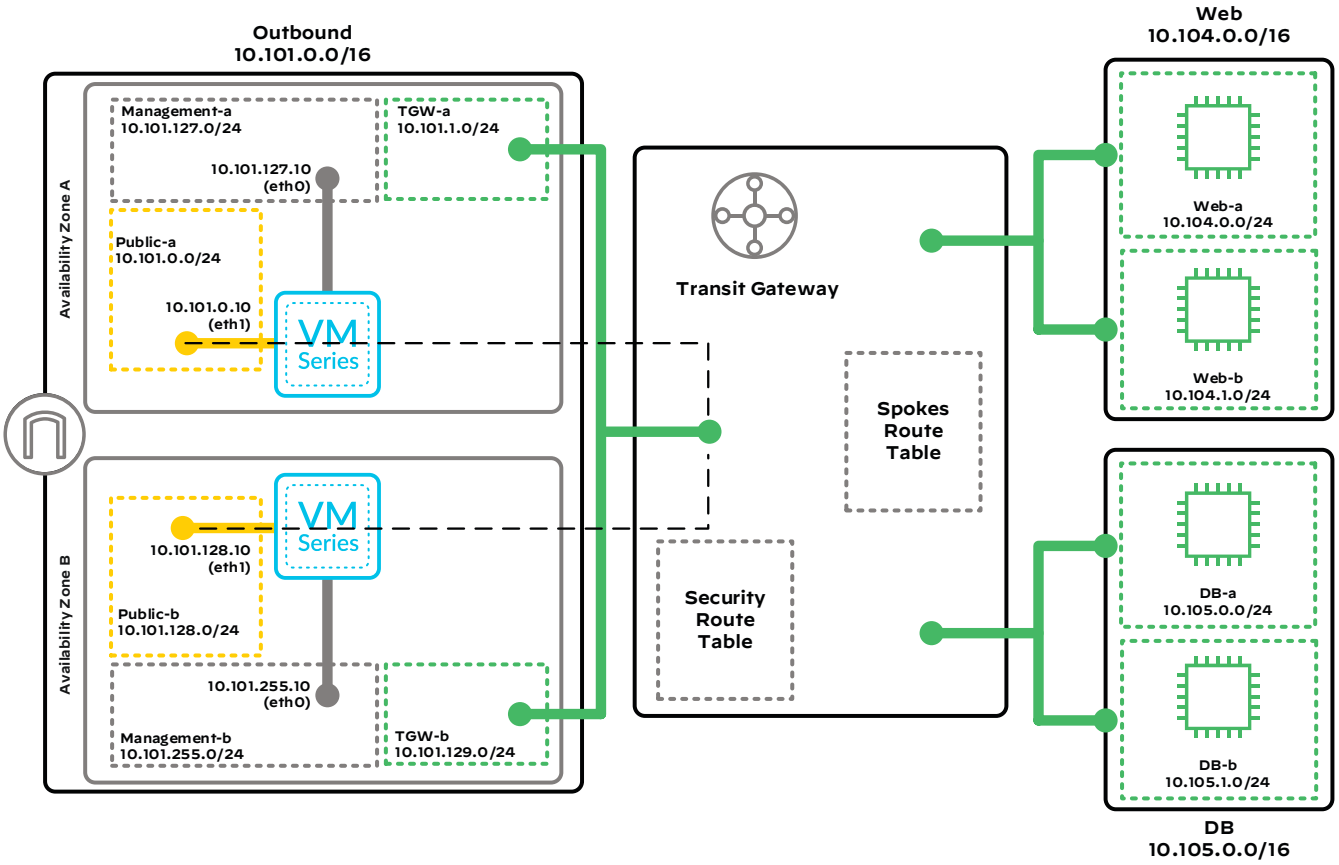
You use VM-Series firewall security policies to limit what applications and resources the private instances can reach. In most designs, the VM-Series firewall does not need to translate the destination IP address. The VM-Series firewall must translate the source IP address to the IP address of the VM-Series firewall's public interface. The default route in the public subnet's route table directs traffic from the VM-Series firewall to the IGW. When the outbound traffic leaves the VPC network, the IGW translates the source address to the public IP address associated with the VM-Series firewall's public interface.

The VM-Series firewall security policy allows appropriate application traffic from private instances

to the internet. You should implement the outbound 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.

Return traffic follows the spoke routes learned from the TGW. The TGW uses the security route table to direct traffic to the correct spoke VPC. The TGW attachment in the spoke VPC communicates directly with the instance in the VPC.

Figure 6 Outbound security



East-West Traffic

This design deploys a VPC dedicated to east-west security with VM-Series firewalls. You connect the VPC to the TGW through two VPN attachments that connect to the two firewalls deployed in the east-west security VPC. Each firewall has two IPSec tunnels, one to each VPN attachment.

The VPC also attaches to the TGW through a VPC attachment for management. The VPC attachment terminates into the east-west security VPC in a dedicated subnet, one per availability zone.

You deploy the two VM-Series firewalls in separate availability zones and deploy an IGW for connectivity to the internet. Each firewall's public-facing and management interfaces are attached to separate subnets.

Each type of subnet has a separate route table as follows:

- The management route table has the management subnets assigned to it, a default route to the IGW for internet access, and a route to the TGW for access to Panorama. Use the VPC attachment for this route.
- The public route table has the public subnets assigned to it and a default route to the IGW for connectivity to the TGW through VPN.

You do not need to modify the default routing of the subnets dedicated to the TGW attachment. By default, they can reach all the IP addresses within the inbound security VPC.

Because the connectivity to the TGW is across an IPSec tunnel, you do not need to configure a private interface on the firewall. The VM-Series firewalls peer to the TGW using eBGP and advertise a route that summarizes all IP address blocks in the spoke VPCs, such as 10.0.0.0/8, across their IPSec tunnels. ECMP and dynamic routing using BGP provide peer detection and failover.

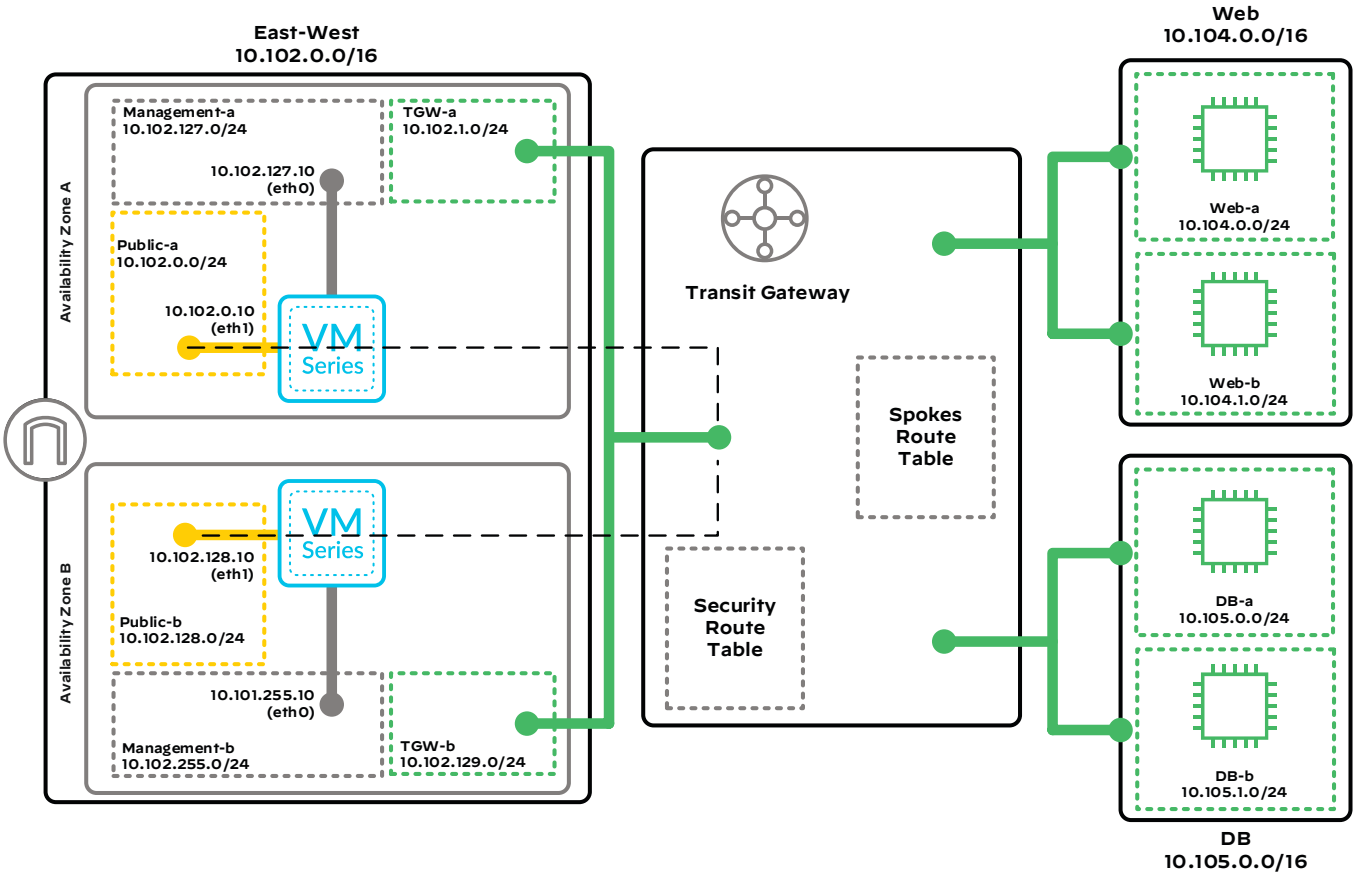
The VPN tunnels advertise 10.0.0.0/8 routes per VPN tunnel into the two TGW routing tables.

This design provides east-west traffic control without address translation. Address translation for east-west traffic flow is challenging to application and database teams. To ensure traffic uses the same firewall in order to avoid asymmetric routing, the east-west firewalls use an active-standby design, which you configure by using the BGP AS-Path attribute. It forces the firewall in the second availability zone to have a longer BGP autonomous system (AS) path than the firewall in the first availability zone. This allows the TGW to prefer the firewall in the first availability zone and failover to the second if there are connectivity issues.

Default routes in the spoke VPCs direct east-west traffic to the TGW. In order to direct traffic to the primary VM-Series firewall in the east-west security VPC, the TGW uses the spokes route table and the summarized internal route learned from the VPN attachments to the east-west VM-Series firewalls.

You use VM-Series firewall security policies to limit what applications and resources the private instances can reach. The VM-Series firewall does not need to perform address translation. The firewall uses the spoke routes learned from the TGW in order to direct traffic to the TGW. The TGW uses the security route table to direct traffic to the correct spoke VPC. The TGW attachment in the spoke VPC communicates directly with the instance in the VPC. Return traffic follows the default route in the spoke VPC to the TGW.

Figure 7 East-west security



Backhaul to On-Premises Traffic

To get traffic from on-premises resources to private instances, you can use VPN connections or AWS Direct Connect. VPN connections from on-premises gateways connect to the TGW as a VPN attachment. Multiple tunnels and ECMP provide resiliency. The default route in the spokes route table provides the path that allows traffic from instances in the spoke VPCs to reach on-premises resources.

You can backhaul to the TGW with Direct Connect either directly in a colocation facility or from on-premises as a service through a WAN provider. Dual connectivity is recommended for resiliency.

Figure 8 Backhaul with Direct Connect gateway

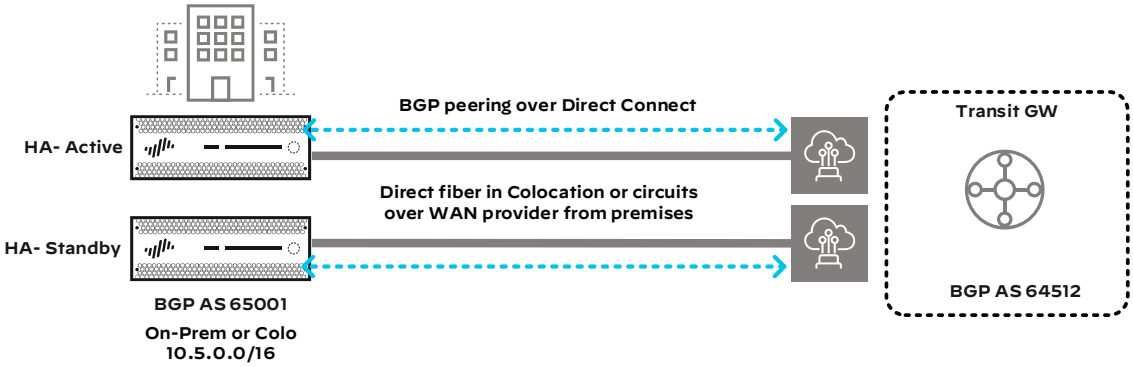


Figure 9 shows VPN connectivity from on-premises gateways to the TGW via a VPN attachment. There is a VPN attachment for each customer gateway, and each attachment is made of two tunnels.

Figure 9 Backhaul with VPN

Management Traffic

This design uses Panorama for the management of the firewalls and uses Cortex Data Lake for logging. You deploy Panorama in an active/standby configuration in a separate, dedicated VPC. You deploy the firewalls with a management interface that routes to Panorama and the internet for software and content updates. The firewalls also need connectivity to subscription services and Cortex Data Lake for logging.

This design connects the dedicated Panorama VPC to the firewalls via a VPC attachment. It is not recommended that you use the VPN attachment because in the event that the VPN tunnels are down, you would lose connectivity to the firewalls.

Scaling

You can scale TGW with thousands of connected VPCs. You can also deploy multiple TGWs per region.

You scale the security solution for each traffic type as follows:

- **Inbound security**—Add additional VM-Series firewalls. The load balancer distributes traffic to the additional firewalls, and source address translation provides for return traffic. You can deploy the firewalls in additional availability zones or within the two existing availability zones.
- **Outbound security**—You can add additional firewalls because you have deployed source address translation and VPN attachments that support ECMP and dynamic routing. You can deploy the firewalls in additional availability zones or within the two existing availability zones.
- **East-west security**—Because address translation is not in use on east-west traffic flows, adding a firewall requires careful planning. You must understand your IP address subnet allocation and understand which spoke IP prefixes you can summarize uniquely in the additional firewalls. The additional firewalls advertise the summarized prefixes for subsets of the spoke VPCs that need east-west inspection.

Assumptions and Prerequisites

Automation

If you do not want to manually complete the steps outlined in this guide, an alternate deployment method that uses automation to provision and configure the cloud infrastructure and Palo Alto Networks components is available at: www.github.com/paloaltonetworks/reference_architecture_automation

AWS:

- Your organization has an active subscription with AWS, and you have the appropriate privileges for configuring compute, network, and storage resources.
- IPv4 IP addressing is used in this deployment guide. IPv6 is available but is not covered.
- Using this guide, you deploy four Elastic IP addresses. Ensure that you have available Elastic IP addresses in the AWS region into which you are deploying.
- You are deploying two VM-Series firewalls.
- You have already deployed the private web-server instances and internal load balancers.
- Palo Alto Networks tested this model in the US West (Oregon) region, although deploying it should be possible in any AWS region.

Palo Alto Networks VM-Series firewalls and Panorama:

- The tested PAN-OS version in this guide is 9.1.2.
- The tested Cloud Services plugin for Panorama is 1.6.0.
- Panorama is implemented in Management-Only mode per the *Panorama on AWS: Deployment Guide*.
- Cortex Data Lake is used for logging.
- The configurations provided for the on-premises firewall in the backhaul VPN connection is for a Palo Alto Networks next-generation firewall running PAN-OS 9.1.2. The firewall is operational with connectivity to the private on-premises network and has a public IP address to which the VPN tunnels can peer.

Palo Alto Networks licensing:

- Your organization has enough licenses for the VM-Series firewalls. This deployment guide uses a bring-your-own-license (BYOL) licensing model. However, you could use pay-as-you-go licenses.

Deploying AWS VPC Infrastructure

Although an account may have existing AWS VPCs, this section describes configuring a new VPC for initial deployment or proof of concept. Larger organizations with an existing footprint in AWS may find value in deployment details regarding features or platforms that they have not yet deployed or experienced.

Procedures

Configuring the VPC, Subnets, and Services

All resources in this guide were created and tested in the AWS US West (Oregon) region. You should change to the AWS region most suitable for your deployment. In this group of procedures, you create the VPC, subnets, and security groups to support the instances.

1.1 Create the VPC

Step 1: Sign in to the AWS console at https://console.aws.amazon.com, and then from the region list at the top of the page, choose the **US West (Oregon)** region.

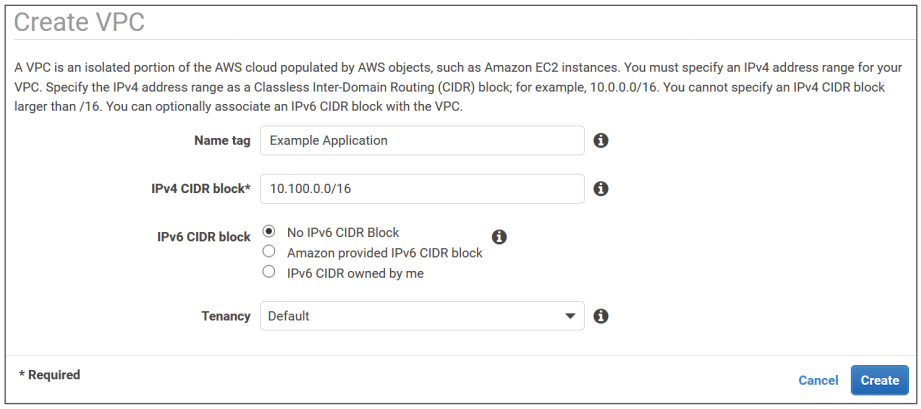
Step 2: Navigate to **Services** > **Networking & Content Delivery** > **VPC**.

Step 3: In the navigation pane on the left, under **Virtual Private Cloud**, choose **Your VPCs**, and then click **Create VPC**.

Step 4: In the **Name tag** box, enter **Example Application**.

Step 5: In the **IPv4 CIDR block** box, enter the IP address and mask **10.100.0.0/16**.

Step 6: Click **Create**, and then click **Close**.



Next, you enable the assignment of public DNS hostnames for the virtual machines (*instances*) that you create in your VPC. If you do not enable DNS hostnames, you may or may not be assigned a public DNS hostname, depending on the DNS attributes of your VPC and if your instance has a public IP address.

Step 7: In the **VPC Dashboard**, select **Example Application**, click the **Actions** list, and then choose **Edit DNS Hostnames**. The Edit DNS Hostnames window opens.

Step 8: On the DNS Hostnames dialog box, select **Enable**.

Step 9: Click **Save**, and then click **Close**.

1.2 Create IP Subnets

The initial IPv4 CIDR block should be broken up into subnets. Only IP address space in the configured CIDR space(s) can be assigned to a subnet.

Table 1 IP subnets

Subnet name	Availability zone	IPv4 CIDR block
Public-2a	us-west-2a	10.100.0.0/24
FW-2a	us-west-2a	10.100.1.0/24
Web-server-2a	us-west-2a	10.100.2.0/24
Business-2a	us-west-2a	10.100.3.0/24
DB-2a	us-west-2a	10.100.4.0/24
Mgmt-2a	us-west-2a	10.100.127.0/24
Public-2b	us-west-2b	10.100.128.0/24
FW-2b	us-west-2b	10.100.129.0/24
Web-server-2b	us-west-2b	10.100.130.0/24
Business-2b	us-west-2b	10.100.131.0/24
DB-2b	us-west-2b	10.100.132.0/24
Mgmt-2b	us-west-2b	10.100.255.0/24

Step 1: On the VPC dashboard, navigate to **Virtual Private Cloud > Subnets**.

Step 2: At the top of the pane, click **Create subnet**.

Step 3: In the **Name tag** box, enter Public-2a.

Step 4: In the **VPC** list, choose Example Application.

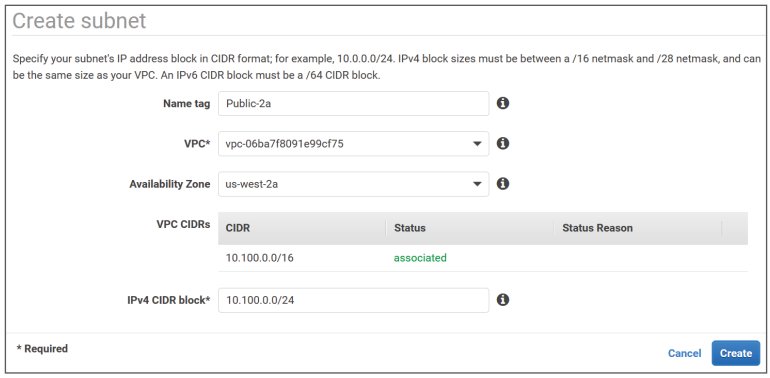
Note

For ease of use, when selecting a VPC the VPC list shows both the VPC name and the VPC ID number. After you select a VPC the VPC list only shows the VPC ID number in the resulting display.

Step 5: In the **Availability Zone** list, choose us-west-2a.

Step 6: In the **IPv4 CIDR block** box, enter 10.100.0.0/24.

Step 7: Click **Create**, and then click **Close**.



Step 8: Repeat this procedure for all the subnets in Table 1.

1.3 Create a VPC Internet Gateway

You create an IGW for internet connectivity and then attach it to the VPC.

Step 1: On the VPC dashboard, navigate to **Virtual Private Cloud > Internet Gateways**.

Step 2: Click **Create internet gateway**, and then in the **Name tag** box, enter **Example Application IGW**.

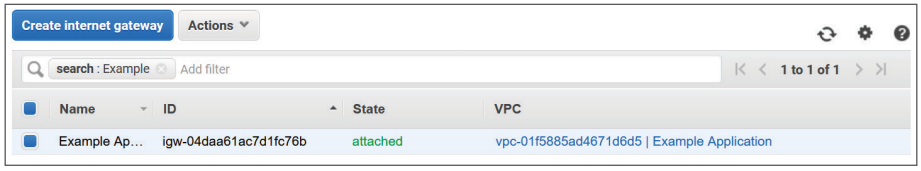
Step 3: Click **Create**, and then click **Close**.

It takes a few minutes for the IGW to initialize.

Step 4: In the **Internet Gateways** list, choose **Example Application IGW**.

Step 5: In the **Actions** list, choose **Attach to VPC**.

Step 6: In the **VPC** list, choose **Example Application**, and then click **Attach**.



1.4 Create VPC Route Tables

Route tables enable you to assign connectivity such as internet gateways and default gateways to specific groups of instances. Recall that all endpoints in the VPC can natively connect to any other endpoint in the assigned VPC CIDR IP address block. A route table cannot change this behavior. There is a main route

table created by default for a VPC, and any subnets that are not assigned to a user-defined route table are assigned to the VPC's main route table. By default, the main route table routes only to the VPC CIDR IP address block. Route tables can control any IP subnet connectivity outside of the VPC CIDR IP address block.

Although you configure the public and management route tables the same, they are broken out separately because you can tailor your management route table to go to only selected management destinations via the IGW or VPC peering connection.

> **Note**
>
> Each route table has a route entry for the VPC CIDR block of IP addresses. This is pre-programmed into every VPC route table.

Table 2 Routes to the IGW

Route table name	Route destination	Target	Subnets assigned
Public-Example Application	0.0.0.0/0	Igw	Public-2a, Public-2b
Mgmt-Example Application	0.0.0.0/0	Igw	Mgmt-2a, Mgmt-2b

Step 1: On the VPC dashboard, navigate to **Virtual Private Cloud > Route Tables**.

Step 2: At the top of the pane, click **Create Route Table**.

Step 3: In the **Name tag** box, enter **Public-Example Application**.

Step 4: In the **VPC** list, choose **Example Application**.

Step 5: Click **Create**, and then click **Close**.

Step 6: With **Public-Example Application** selected in the top pane, click the **Routes** tab on the bottom pane, and then click **Edit routes**.

Step 7: Click **Add route**, and then in the **Destination** box, enter **0.0.0.0/0**.

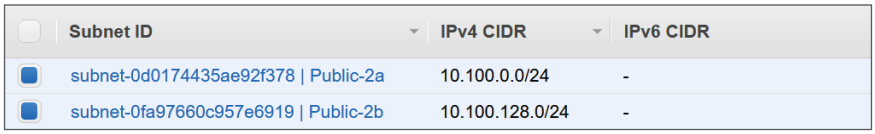
Step 8: Click in the **Target** box, and then choose the **Example Application IGW**.

Step 9: Click **Save routes**, and then click **Close**.

Destination	Target	Status	Propagated
10.100.0.0/16	local	active	No
0.0.0.0/0	igw-04daa61ac7d1fc76b	active	No

Step 10: On the Subnet Associations tab, click **Edit subnet associations**.

Step 11: In the list, choose subnets **Public-2a** and **Public-2b**, and then click **Save**.



Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-0d0174435ae92f378 | Public-2a	10.100.0.0/24	-
subnet-0fa97660c957e6919 | Public-2b	10.100.128.0/24	-

Step 12: Repeat this procedure for the remaining route in Table 2.

1.5 Create Security Groups

When you create an AWS Elastic Compute Cloud (EC2) compute instance to run an application, you must assign the instance to a new or existing security group (SG). Security groups provide a Layer 4 stateful firewall for control of the source/destination IP addresses and ports that are permitted to or from the instances associated. SGs are applied to an instance's network interface. You can associate up to five SGs with a network interface. By default, the security groups do not allow inbound traffic. The default outbound behavior allows all traffic. However, you can customize this for your operations.

You configure three security groups that you assign to the VM-Series firewalls:

- **Public**—Initially all traffic is allowed to the firewall's public interface, and the firewall controls traffic with security policies. After you have your network setup, you narrow the inbound traffic in this security group to only the Layer 4 ports required in order to reduce the load of traffic hitting the firewall's public interface.
- **Management**—Allows ports necessary for Panorama and firewall operation. Depending on your firewall settings, you may need to adjust the rules for full operation. For more information, see Palo Alto Networks PAN-OS 9.1 Reference: Port Number Usage.
- **Private**—Allows all traffic from other instances in the VPC. This is required because the firewalls and load balancers translate the IP address of all traffic coming from the internet to the VPC IPv4 IP address range.

The security groups are configured to allow this design to operate; your settings may vary based on your organization, network, and application requirements.

First, you create a public security group that allows all traffic.

Step 1: On the EC2 Compute dashboard, navigate to **NETWORK & SECURITY > Security Groups**, and then click **Create Security Group**.

Step 2: In the **Security group name** box, enter **Firewall-Public**.

Step 3: In the **Description** box, enter **Allow inbound applications from the internet**.

Step 4: In the **VPC** list, choose **Example Application**.

Step 5: On the Inbound rules pane, click **Add Rule**.

Step 6: In the **Type** list, choose **All traffic**.

Step 7: In the **Source** type list, choose **Anywhere**.

Step 8: Click **Create security group**.

Next, you create a security group that allows you to manage the VM-Series firewall.

Table 3 Firewall-Mgmt security group—inbound rules

Type	Protocol	Port range	Source IP address
SSH	TCP	22	Your IP
HTTPS	TCP	443	Your IP

Step 9: On EC2 Compute dashboard, navigate to **NETWORK & SECURITY > Security Groups**, and then click **Create Security Group**.

Step 10: In the **Security group name** box, enter **Firewall-Mgmt**.

Step 11: In the **Description** box, enter **Allow inbound management to the firewall**.

Step 12: In the **VPC** list, choose **Example Application**.

Step 13: On the Inbound rules pane, click **Add Rule**.

Step 14: In the **Type** list, choose **SSH**.

Step 15: In the **Source** list, choose **My IP**.

Step 16: Repeat Step 13-Step 15 for the remaining rule in Table 3.

Step 17: Click **Create security group**.

Next, you create a security group that controls traffic into the firewall's private interface.

Step 18: On the EC2 Compute dashboard, navigate to **NETWORK & SECURITY > Security Groups**, and then click **Create Security Group**.

Step 19: In the **Security group** name box, enter **Firewall-Private**.

Step 20: In the **Description** box, enter **Allow inbound traffic to private interface**.

Step 21: In the **VPC** list, choose **Example Application**.

Step 22: On the Inbound rules pane, click **Add Rule**.

Step 23: In the **Type** list, choose **All traffic**.

Step 24: In the **Source Type** list, choose **Custom**.

Step 25: In the **Source** box, enter **10.100.0.0/16**.

Step 26: Click **Create security group**.

1.6 Configure VPC Peering

Because you deployed Panorama in a separate VPC in the Panorama on AWS: Deployment Guide you need to connect the two VPCs together. In this procedure you create a peering connection between the VPCs, configure routes that provide communication, and add an inbound rule to Panorama's security group that allows the VM-Series firewalls to communicate to Panorama.

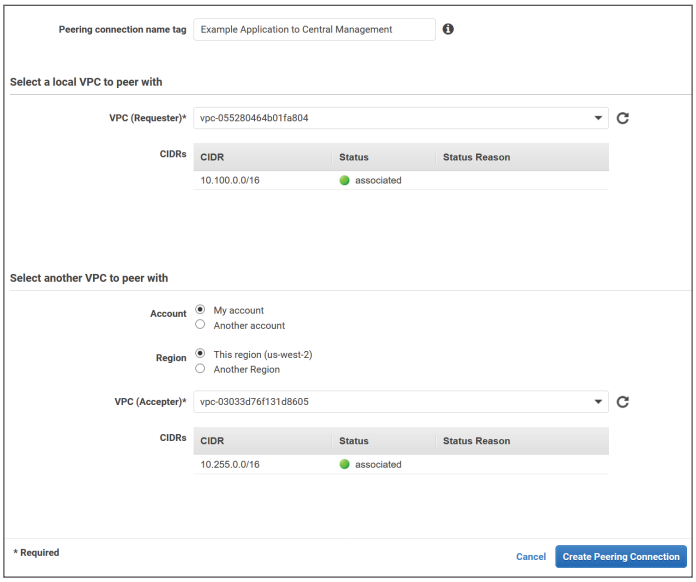
Step 1: On the VPC dashboard, navigate to **Virtual Private Cloud > Peering Connections**.

Step 2: Click **Create Peering Connection**.

Step 3: In the **Peering connection name tag** box, enter **Example Application to Central Management**.

Step 4: In the **VPC (Requester)** list, choose **Example Application**.

Step 5: In the **VPC (Accepter)** list, choose **Management**, and then click **Create Peering Connection**.



Step 6: In the **Actions** list, choose **Accept Request**.

Next, you create a route that lets the VM-Series firewalls reach the Panorama's VPC.

Step 7: On the VPC dashboard, navigate to **Virtual Private Cloud > Route Tables**.

Step 8: With **Mgmt-Example Application** selected in the top pane, click the **Routes** tab on the bottom pane, and then click **Edit routes**.

Step 9: Click **Add route**, and then in the **Destination** box, enter **10.255.0.0/16**.

Step 10: Click in the **Target** box, and then choose the **Example Application to Central Management** peering connection.

Step 11: Click **Save routes**, and then click **Close**.

Next, you create a route that lets Panorama reach the VM-Series firewall's in the Example Application VPC.

Step 12: On the VPC dashboard, navigate to **Virtual Private Cloud > Route Tables**.

Step 13: With **Management** selected in the top pane, click the **Routes** tab on the bottom pane, and then click **Edit routes**.

Step 14: Click **Add route**, and then in the **Destination** box, enter **10.100.0.0/16**.

Step 15: Click in the **Target** box, and then choose the **Example Application to Central Management** peering connection.

Step 16: Click **Save routes**, and then click **Close**.

Next, you modify the security group associated to Panorama's interfaces to allow inbound traffic from the VM-Series firewalls.

Step 17: On the VPC dashboard, navigate to **Virtual Private Cloud > Security > Security Groups**.

Step 18: With **Panorama** select in the top pane, click the **Inbound Rules** tab on the bottom pane, and then click **Edit Inbound Rules**.

Step 19: Click **Add Rule**.

Step 20: In the **Type** list, choose **All traffic**.

Step 21: In the **Source Type** list, choose **Custom**.

Step 22: In the **Source** box, enter **10.100.0.0/16**, and then click **Save Rules**.

Deploying VM-Series Firewalls

In this section, you deploy two VM-Series firewalls in the VPC with a single Ethernet for management. You then add interfaces and IP addressing to the firewalls so that each has three interfaces. Finally, you perform the initial configuration of the firewalls before onboarding them to Panorama in the next section.

Procedures

Deploying a VM-Series Instance on AWS

2.1 Create the VM-Series Firewalls

You deploy two VM-Series firewalls and attach their primary interface to the management subnets.

Table 4 VM-Series firewall deployment parameters

System name	Subnet	Management IP address
vmseries-a	Mgmt-2a	10.100.127.10
vmseries-b	Mgmt-2b	10.100.255.10

Step 1: Sign in to the AWS console, and then in the list at the top of the page, choose the **US West (Oregon)** data center.

Step 2: On the EC2 Compute dashboard, navigate to **INSTANCES > Instances**.

Step 3: In the **Launch Instance** list, choose **Launch Instance**.

Step 4: In the **Choose AMI** workflow, click the **AWS Marketplace** tab. In the search box, enter **Palo Alto Networks**, and then press **ENTER**.

Step 5: For the VM-Series Next-Generation Firewall (BYOL and ELA) instance, click **Select**.

Step 6: Read the Palo Alto Networks Panorama information pane, and then click **Continue**.

Step 7: In the Choose Instance Type pane, scroll down and choose the **m5.xlarge** instance, and then click **NEXT: Configure Instance Details**.

This screen configures the networking details for the instance.

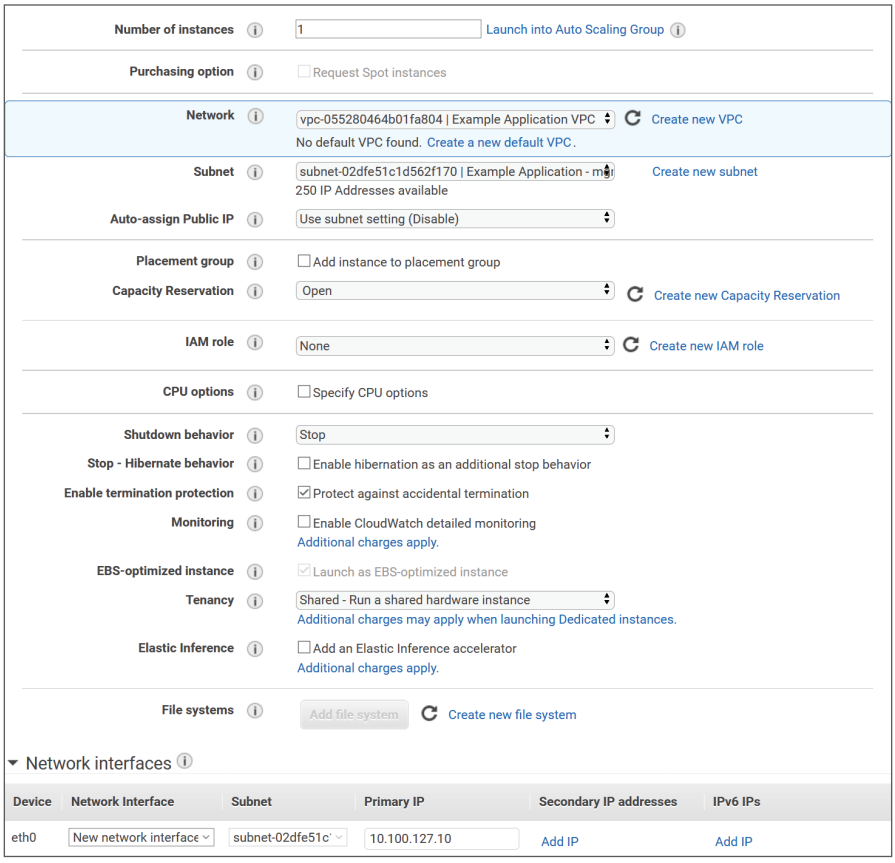
Step 8: In the **Number of instances** box, enter **1**.

Step 9: In the **Network** list, choose **Example Application**.

Step 10: In the **Subnet** list, choose **Mgmt-2a**.

Step 11: For **Enable termination protection**, select **Protect against accidental termination**.

Step 12: Expand **Network Interfaces**, and then in the **Primary IP** box for eth0, enter **10.100.127.10**.



Step 13: Click **Next: Add Storage**. The AMI template for VM-Series adds storage for the instance.

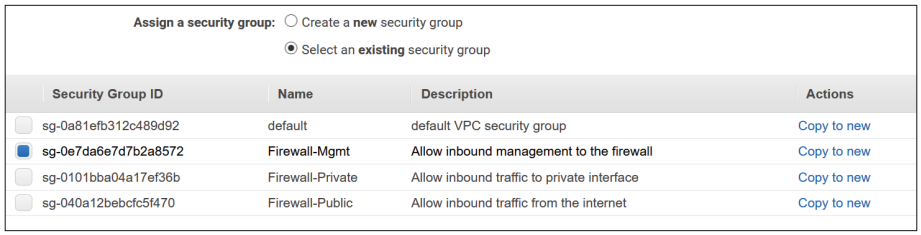
Step 14: Click **Next: Add Tags**. This procedure does not require tags.

Step 15: Click **Next: Configure Security Group**.

Step 16: For **Assign a security group**, select **Select an existing security group**.

Step 17: Select the **Firewall-Mgmt** security group, and then click **Review and Launch**. Ensure that only the **Firewall-Mgmt** security group is selected.

Step 18: Review all selections, and then click **Launch**.



Next, you assign key pair for the deployment.

Step 19: If you do not have an existing key pair, on the Select an existing key pair or create a new pair dialog box, choose **Create a new key pair**, and then continue to the next step.

If you have an existing key pair, do the following:

- On the Select an existing key pair or create a new pair dialog box, choose **Use an existing key pair**.
- In the **Select a key pair** list, choose **paloaltonetworks-deployment**.
- Acknowledge that you have the key pair.
- Skip to Step 22.

Step 20: In the **Key pair name** box, enter the key pair name **paloaltonetworks-deployment**.

Step 21: Click **Download Key Pair**. This downloads a file with a .pem file extension to your machine. Store this file in a convenient and safe place. You need this to create an SSH connection to the instance.

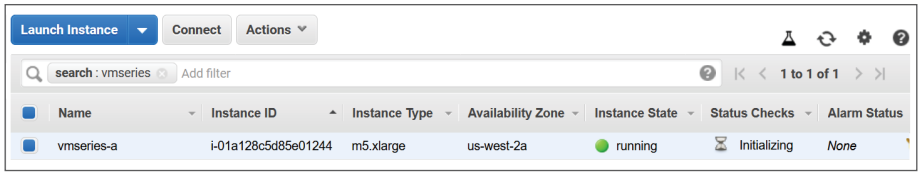
Caution

Be sure to store the private key file in a safe place. Anyone with the private key file can access the instances created with it. If you lose the file, you must create new instances in order to get a new private key file.

Step 22: Click **Launch instances**, and then click **View Instances**.

Step 23: In the Instances pane, hover your cursor over the **Name** field. A pencil image appears. Click the pencil.

Step 24: In the **Name** box, enter vmseries-a, and then select the checkmark.



Step 25: Repeat this procedure to create the second VM-Series firewall, using the parameters from Table 4.

2.2 Create Elastic Network Interfaces for the VM-Series Firewalls

VM-Series instances initialize with a single Ethernet interface, eth0, which is by default the management interface for the firewall. The firewalls each require two additional interfaces, which are elastic network interfaces (ENIs).

Table 5 ENIs for the VM-Series firewalls

Name and description	Subnet	IP address	Security group
vmseries-a-public	Public-2a	10.100.0.10	Firewall-Public
vmseries-a-private	FW-2a	10.100.1.10	Firewall-Private
vmseries-b-public	Public-2b	10.100.128.10	Firewall-Public
vmseries-b-private	FW-2b	10.100.129.10	Firewall-Private

Step 1: On the EC2 Compute dashboard, navigate to **NETWORK & SECURITY > Network Interfaces**, and then click **Create Network Interface**.

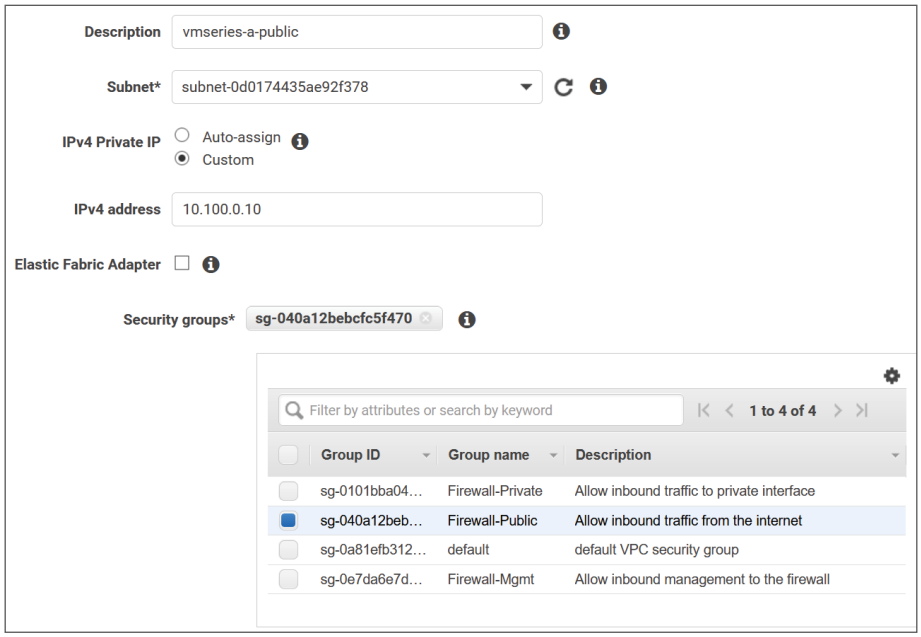
Step 2: In the **Description** box, enter the interface name vmseries-a-public.

Step 3: In the **Subnet** list, choose Public-2a.

Step 4: For **IPv4 Private IP**, choose **Custom**.

Step 5: In the **IPv4 address** box, enter 10.100.0.10.

Step 6: In the **Security groups** list, choose **Firewall-Public**, and then click **Create**.



Next, you enter a name for the interface. The value for the name box matches the description you entered in the workflow. This step makes it easier to identify interfaces in the next procedure.

Step 7: In the Network Interfaces pane, on the new interface, hover your cursor over the **Name** field. A pencil image appears. Click the pencil.

Step 8: In the **Network Interface Name** box, enter **vmseries-a-public**, which should match the description used in Step 2, and then click the checkmark.

Next, you disable source and destination checks on the interface.

Step 9: In the Network Interfaces pane, select **vmseries-a-public**.

Step 10: In the **Actions** list, choose **Change Source/Dest.Check**.

> **Note**
>
> Ensure that you select only one interface. If you select more than one interface, Change Source/Dest. Check is not available in the Actions list.

Step 11: For **Change Source/Dest**, select **Disabled**, and then click **Save**.

Step 12: Repeat this procedure for the remaining interfaces in Table 5.

2.3 Attach the Interfaces to the Firewalls

You attach the ENIs to their instance. When attaching an ENI to an instance, the first ENI attached becomes eth1, and the second becomes eth2.

Table 6 Mapping of ENIs to the VM-Series Instances

ENI name and description	VM-Series instance	Eth#
vmseries-a-public	vmseries-a	eth1
vmseries-a-private	vmseries-a	eth2
vmseries-b-public	vmseries-b	eth1
vmseries-b-private	vmseries-b	eth2

First, you attach the public and private ENI to the first VM-Series firewall.

Step 1: In the Network Interfaces pane, select the first interface, **vmseries-a-public**, and then click **Attach**.

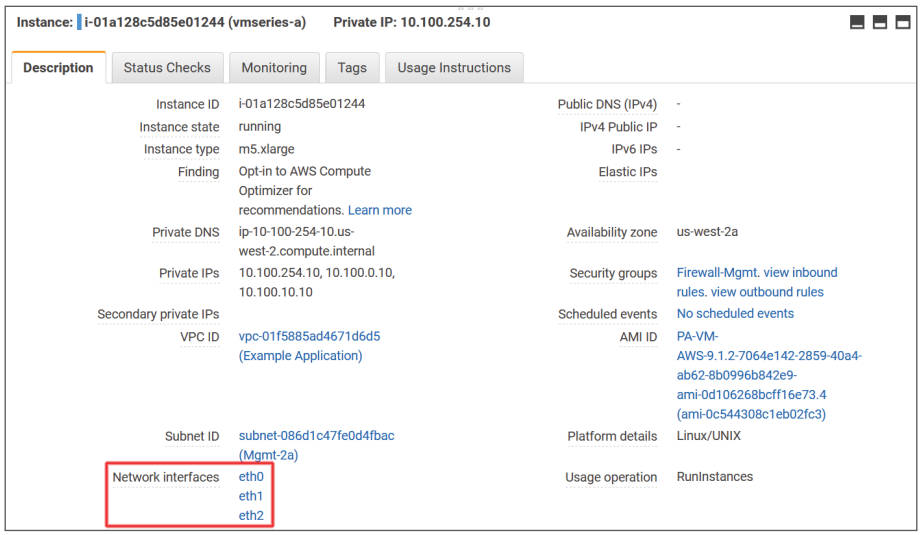
Step 2: On the Attach Network Interface dialog box, select the **vmseries-a** instance, and then click **Attach**.

Step 3: In the Networking Interfaces pane, select the **vmseries-a-private** interface, and then click **Attach**.

Step 4: On the Attach Network Interface dialog box, again select the **vmseries-a** instance, and then click **Attach**.

Step 5: In the navigation pane, click **Instances**.

Step 6: Select the **vmseries-a** instance, and then in the bottom description pane, verify that this instance now has three network interfaces.



Step 7: Repeat this procedure for the second VM-Series firewall.

2.4 Label the Primary Interfaces for the VM-Series Instance

Before assigning Elastic IP addresses to the firewall's management interface, you assign names to the interfaces. This makes it easier to assign EIPs.

Step 1: On the EC2 Compute dashboard, navigate to **NETWORK & SECURITY > Network Interfaces**.

Step 2: Scroll to the right of the window and locate the Primary Private column, and then select the private IP address for **vmseries-a** management interface, **10.100.127.10**.

Step 3: In the Network Interfaces pane, in the **10.100.127.10** row, hover your cursor over the **Name** field. A pencil image appears. Click the pencil.

Step 4: In the network interface **Name** box, enter **vmseries-a-mgmt**, and then click the checkmark.

Next, you assign the name for **vmseries-b** management interface.

Step 5: Scroll to the right of the window and locate the Primary Private column, and then select the private IP address for **vmseries-b** management interface, **10.100.255.10**.

Step 6: In the Network Interfaces pane, in the **10.100.255.10** row, hover your cursor over the **Name** field. A pencil image appears. Click the pencil.

Step 7: In the network interface **Name** box, enter **vmseries-b-mgmt**, and then click the checkmark.

2.5 Create Elastic IP Addresses for the VM-Series Firewall

In this procedure, you create Elastic IP addresses (EIPs) and associate them to the firewall's public and management interfaces.

Table 7 EIPs for the VM-Series firewalls

EIP and ENI name	Private IP address
vmseries-a-mgmt	10.100.127.10
vmseries-a-public	10.100.0.10
vmseries-b-mgmt	10.100.255.10
vmseries-b-public	10.100.128.10

Step 1: On the VPC dashboard, navigate to **Virtual Private Cloud > Elastic IPs**.

Step 2: Click **Allocate Elastic IP address**, and then click **Allocate**.

Step 3: In the **Actions** list, choose **View Details**.

Step 4: Click **Manage Tags**.

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

Step 6: In the **Value** box, enter **vmseries-a-mgmt**, and then click **Save**.

Next, you assign the EIP to the VM-Series firewall.

Step 7: Click **Associate Elastic IP address**.

Step 8: In **Resource type**, select **Network Interface**.

Step 9: In the **Network Interface** list, choose **vmseries-a-mgmt**. These are the ENI names you entered in the previous procedure. You can see the ENI name in the list, but you can't see the ENI number in the field until after you choose the ENI name.

Step 10: In the **Private IP** list, choose **10.100.127.10**, and then click **Associate**.

Step 11: Repeat this procedure for the rest of the interfaces in Table 7.

2.6 Log in to the VM-Series Firewall

Before you login to the VM-Series web interface, you need to set an admin user password. The initial admin password setup must be done via an SSH connection to a CLI shell on the instance.

To connect to your instances, you need to set up your SSH connection to use the key pair created in Procedure 2.1.

Step 1: Use the instructions in the AWS guide Connect to your Linux Instance in order to set up your system to use a SSH connection to access the instance.

Step 2: On the EC2 Compute dashboard, navigate to **INSTANCES > Instances**.

Step 3: Select the **vmseries-a** instance, and then in the lower pane, copy the **Public DNS (IPv4)** address.

The next step uses the SSH tool that you set up in Step 1, the key pair, and the public DNS IP address string.

Note

You may not be able to connect to the firewall through SSH until it is fully operational. If you are prompted for a password, the firewall is most likely not operational yet.

Step 4: Use the admin username to open an SSH session to the FQDN for **vmseries-a**. For example: ssh -i paloaltonetworks-deployment.pem admin@ ec2-54-245-9-203.us-west-2.compute.amazonaws.com

Step 5: If your console shows a security alert that the authenticity of the host can't be established, enter **YES** to continue connecting.

Step 6: At the CLI prompt, set a strong admin password, and then commit.

```
admin@PA-VM> configure
admin@PA-VM# set mgt-config users admin password
Enter password :
Confirm password :
admin@PA-VM# commit
Commit job 2 is in progress. Use Ctrl+C to return to command prompt
......100%
Configuration committed successfully
admin@PA-VM#
```

Step 7: When the commit is complete, use your browser to connect to the firewall's web interface (example: https://ec2-54-245-9-203.us-west-2.compute.amazonaws.com).

Step 8: Accept the browser certificate warning.

Step 9: Log in to the firewall, using **admin** for the username and the password that you just configured.

Step 10: Log out of the SSH session.

Step 11: Repeat this procedure for the second VM-Series firewall.

2.7 License the VM-Series Firewalls

The VM-Series firewalls are now running. However, they are unlicensed and running the default configuration. This procedure assumes that you have a valid license authcode for your VM-Series firewalls and registered that authcode on the Palo Alto Networks customer support portal.

Step 1: Log in to the first VM-Series firewall's web interface.

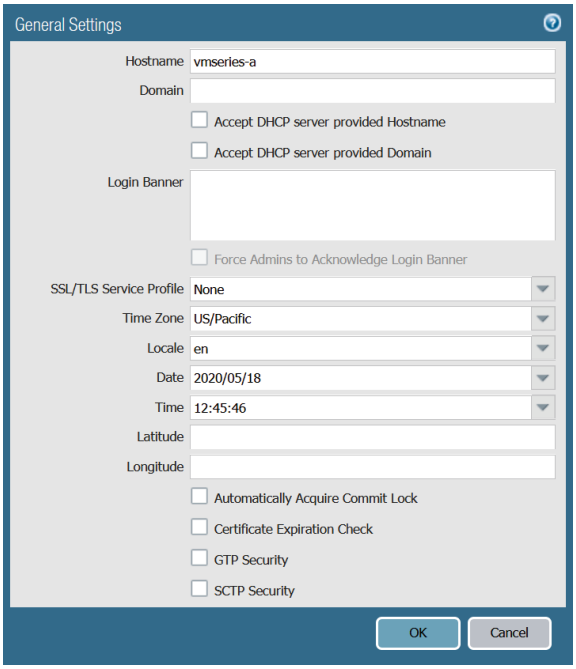
Step 2: Accept the browser certificate warning.

Step 3: On the Welcome dialog box, click **Close**.

Step 4: In **Device > Setup > Management > General Settings**, click the **Edit** cog.

Step 5: In the **Hostname** box, enter **vmseries-a**.

Step 6: In the **Time Zone** list, choose the appropriate time zone (example: US/Pacific), and then click **OK**.



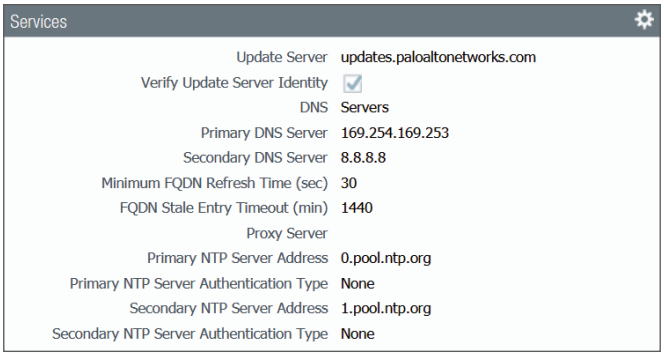
Step 7: In **Device > Setup > Services**, click the **Edit** cog.

Step 8: In the **Primary DNS Server** box, enter 169.254.169.253. This is the DNS address for AWS.

Step 9: In the **Secondary DNS Server** box, enter 8.8.8.8.

Step 10: On the NTP tab, in the Primary NTP Server section, in the **NTP Server Address** box, enter 0.pool.ntp.org.

Step 11: In the Secondary NTP Server section, in the **NTP Server Address** box, enter 1.pool.ntp.org, and then click **OK**.



Step 12: Click **Commit**, and then click **Commit**.

Step 13: In **Device > Licenses**, click **Activate feature using authorization code**.

Step 14: In the **Authorization Code** box, enter your registered authcode, and then click **OK**.

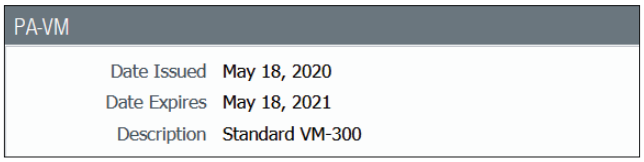
Step 15: Click **OK** in order to restart services.

The firewall displays progress and then restarts. The restart takes approximately 5 minutes.

Step 16: Log in to the VM-Series web interface.

Step 17: In **Dashboard > General Information**, verify that a serial number and VM license model are listed.

Step 18: In **Device > Licenses**, verify that the **PA-VM** has a valid license.



Step 19: Repeat this procedure on the second VM-Series firewall. In Step 5, enter the name of the second VM-Series firewall, **vmseries-b**.

Configuring Panorama for Firewall Management

This section assumes that the AWS management VPC and Panorama deployments are complete and operational as discussed in the Panorama on AWS: Deployment Guide.

This section describes how to configure multiple device groups, templates, and template stacks to support VM-Series next-generation firewall deployment and operation in the Single VPC design model. You use *templates* to configure the settings that enable firewalls to operate on the network. Templates enable you to define a common base configuration. For example, you can use templates to manage interface and zone configurations, profiles for logging, and network profiles for controlling access to zones and IKE gateways. A *template stack* is a combination of templates: the assigned firewalls inherit the settings from every template in the stack. This enables you to avoid the redundancy of adding every setting to every template.

After you complete the initial VM-Series network configuration with template stacks, you use the device groups to deploy security and NAT policies. A *device group* enables grouping based on network segmentation, geographic location, organizational function, or any other common aspect of firewalls that require similar policy configurations. Using device groups, you can configure policy rules and the objects they reference. You can organize device group hierarchically, with shared rules and objects at the top, and device group-specific rules and objects at subsequent levels. The device groups allow you to push new policy to a group of firewalls, reducing configuration deployment time and improving consistency.

Procedures

Configuring Device Groups, Templates, and Template Stacks

First, you configure a common parent device group and two device groups for common policy. Next, you create and configure common and individual group network templates. The last step is to create a set of template stacks that ensure consistent configuration across each functional group of VM-Series firewalls.

3.1 Configure Device Groups

Device groups contain VM-Series firewalls you want to manage as a group. A firewall can belong to only one device group. Panorama treats each group as a single unit when applying policies.

Step 1: Log in to the primary Panorama server.

Step 2: Navigate to **Panorama > Device Groups**, and then click **Add**.

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

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

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

3.2 Configure Log Forwarding Objects

You use this procedure to configure a log forwarding object that security policies use to direct logging information to the Cortex Data Lake instance, which you configured as part of the Panorama deployment.

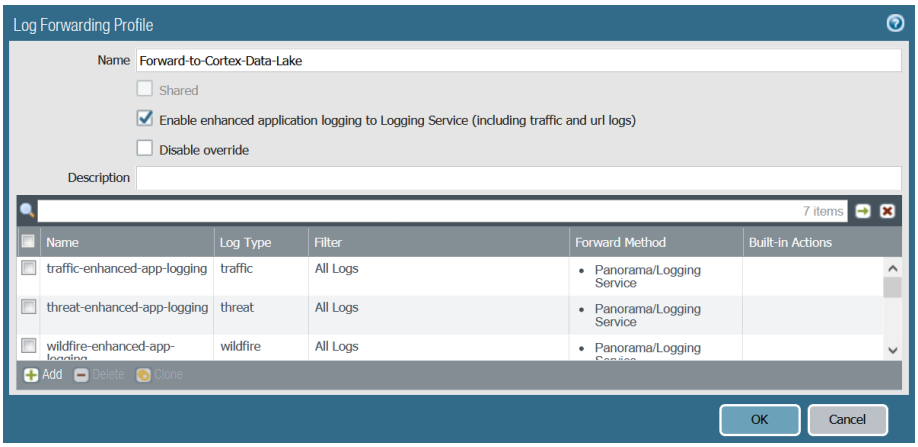
Step 1: Log in to the Panorama web interface.

Step 2: On the Objects tab, in the **Device Group** list, choose **AWS**.

Step 3: In the navigation pane, click **Log Forwarding**, and then click **Add**.

Step 4: In the **Name** box, enter **Forward-to-Cortex-Data-Lake**.

Step 5: Select **Enable enhanced application logging to Logging Service**, and then click **OK**.



Step 6: On the **Commit** menu, select **Commit to Panorama**, and then click **Commit**. It is not mandatory to commit at this time but doing so periodically prevents you from losing work if an outage occurs.

3.3 Create Templates

You use templates to configure functions that are common across groups of firewalls. In this procedure, you create a baseline configuration template that you can use for all VM-Series firewalls in the environment and create a network template that is specific to this design model.

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

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

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

Step 4: Repeat this procedure for **Single-VPC-Network-Settings**.

Step 5: In the **Commit** menu, choose **Commit to Panorama**, and then click **Commit**. It is not mandatory to commit at this time but doing so periodically prevents you from losing work if an outage occurs.

You should now see tabs for device groups and templates.

3.4 Configure the Firewall Baseline Settings Template

Now you perform the baseline configuration template for the VM-Series firewalls. The bootstrap process uses this template to configure common services such as DNS, NTP, and Cortex Data Lake as well as other baseline settings.

Step 1: On the primary Panorama server, navigate to **Device**.

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

Step 3: In **Device** > **Setup** > **Management** > **General Settings**, click the **Edit** cog.

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** > **Global** > **Services**, click the **Edit** cog.

Step 6: In the **Primary DNS Server** box, enter **169.254.169.253**.

Step 7: In the **FQDN Refresh Time** box, enter **60**. The FQDN timer is used for the AWS load balancers later in this design.

Step 8: On the NTP tab, in the **Primary NTP Server** box, enter **0.pool.ntp.org**.

Step 9: In the **Secondary NTP Server** box, enter **1.pool.ntp.org**, and then click **OK**.

Step 10: In **Device > Setup > Content-ID > X-Forwarded-For Headers**, click the **Edit** cog.

Step 11: Select **Use X-Forwarded-For Header in User-ID**, and then click **OK**.

Step 12: In **Device > Setup > Interfaces**, click **Management**.

Step 13: For **IP Type**, choose **DHCP Client**.

Step 14: In **Administrative Management Services**, select **HTTPS** and **SSH**.

Step 15: In **Network Services**, select **Ping**, and then click **OK**.

Note

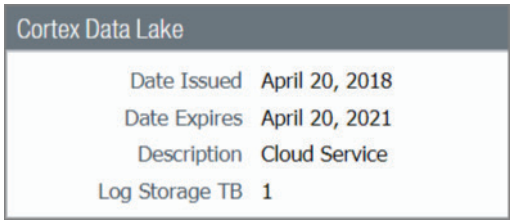
Enabling Ping is optional. However, it is helpful for troubleshooting an installation.

Step 16: On the **Commit** menu, select **Commit to Panorama**, and then click **Commit**. It is not mandatory to commit at this time but doing so periodically prevents you from losing work if an outage occurs.

Next, on the firewalls, you enable logging to Cortex Data Lake.

Step 17: In **Panorama > Licenses**, click **Retrieve license keys from license server**.

Step 18: Verify that the Cortex Data Lake license is active.

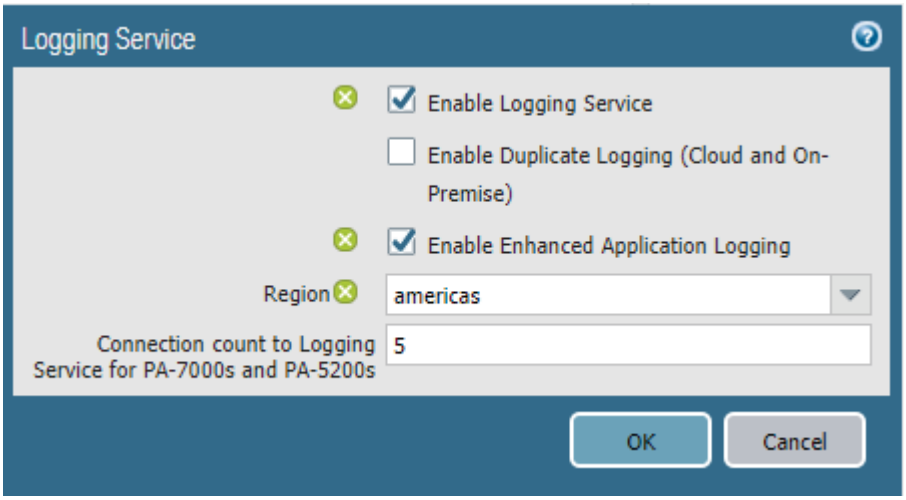


Step 19: Navigate to **Device**, and then in the **Template** list, choose **Baseline-VMSeries-Settings**.

Step 20: In **Device > Setup > Management > Logging Service**, click the **Edit** cog.

Step 21: Select **Enable Logging Service**, and then select **Enable Enhanced Application Logging**.

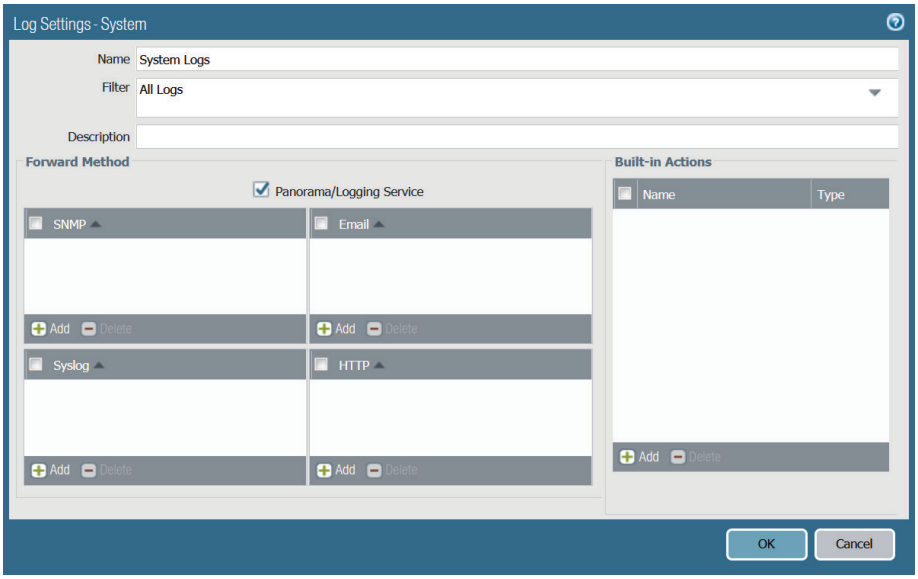
Step 22: In the **Region** list, choose **americas**, and then click **OK**.



Step 23: In **Device > Log Settings > System**, click **Add**. The Log Settings—System configuration window appears.

Step 24: In the **Name** box, enter **System Logs**.

Step 25: Select **Panorama/Logging Service**, and then click **OK**.



Step 26: In **Device > Log Settings > Configuration**, click **Add**. The Log Settings—Configuration window appears.

Step 27: In the **Name** box, enter **Configuration Logs**.

Step 28: Select **Panorama/Logging Service**, and then click **OK**.

Step 29: In the **Commit** menu, click **Commit to Panorama**, and then click **Commit**.

These next steps set the admin user password as part of the template.

Step 30: Navigate to **Device > Administrators**, and at the top of the page, in the **Template** list, choose **Baseline-VMSeries-Settings**.

Step 31: Click **Add**.

Step 32: In the **Name** box, enter **admin**.

Step 33: Enter and confirm a password.

Step 34: For **Administrator Type**, choose **Dynamic**.

Step 35: In the **Dynamic** list, choose **Superuser**, and then click **OK**.

Step 36: In the **Commit** menu, click **Commit to Panorama**, and then click **Commit**.

3.5 Configure the Network Settings Template

Now you create the network settings template that configures interfaces, zones, and routing for the VM-Series firewalls. All interfaces obtain their IP addressing through DHCP, but only the public interface should accept the default route.

Table 8 Interfaces and zones for the Inbound group of VM-Series firewalls

Slot	Interface	Interface type	Zone	Virtual router	Type	Enable default route
slot 1	ethernet1/1	Layer3	public	vr-default	DHCP Client	Yes
slot 1	ethernet1/2	Layer3	private	vr-default	DHCP Client	No

Step 1: Log in to the Panorama web interface.

Step 2: Navigate to **Network > Interfaces**, and then in the **Template** list, choose **Single-VPC-Network-Settings**.

Step 3: Click **Add Interface**.

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

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

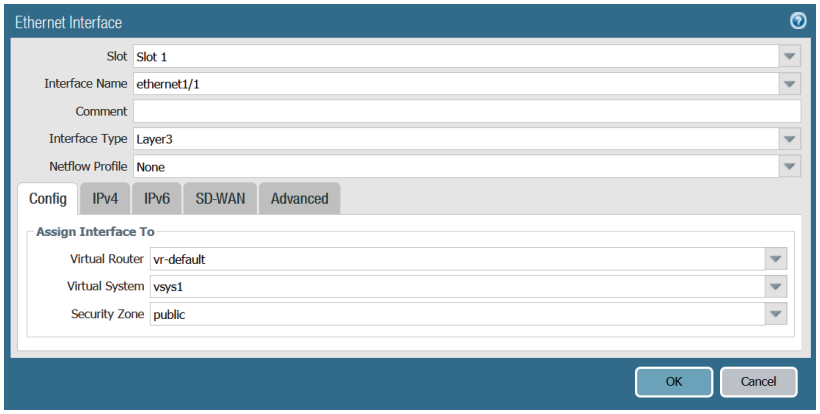
Step 6: In the **Interface Type** list, choose **Layer3**.

Step 7: On the Config tab, in the **Virtual Router** list, choose **New Virtual Router**.

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

Step 9: In the **Security Zone** list, choose **New Zone**.

Step 10: In the **Name** box, enter **public**, and then click **OK**.



Step 11: On the IPv4 tab, for **Type**, select **DHCP Client**.

Step 12: Select **Automatically create default route pointing to default gateway provided by server**, and then click **OK**.

Step 13: Repeat Step 1–Step 12 for the second interface listed in Table 8 while making sure to clear the check box in Step 12.

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

3.6 Create Template Stacks

You use template stacks to combine several templates into a group. You can also assign common settings to the template stack. In this example, you use a template stack to group the baseline and network templates for the firewalls in the different availability zones.

Table 9 Panorama template stacks

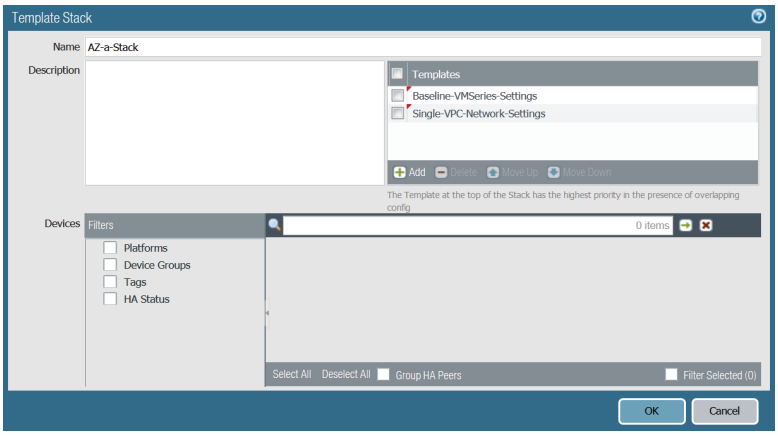
Template stack name	Included templates
AZ-a-Stack	Baseline-VMSeries-Settings Single-VPC-Network-Settings
AZ-b-Stack	Baseline-VMSeries-Settings Single-VPC-Network-Settings

Step 1: On the primary Panorama server, navigate to **Panorama > Templates**, and then click **Add Stack**.

Step 2: In the **Name** box, enter AZ-a-Stack.

Step 3: In the **Description** box, enter an appropriate description.

Step 4: In the Templates pane, click **Add**, select Baseline-VMSeries-Settings and Single-VPC-Network-Settings, and then click **OK**.



Step 5: Repeat Step 1-Step 4 for the remaining template stack listed in Table 9.

Step 6: In the **Commit** menu, click **Commit to Panorama**, and then click **Commit**.

3.7 Create Static Routes

For subnets that are not directly attached to the VM-Series firewall, you define static routes on the firewall. Configure both of the firewalls to have routes to all of the subnets. If the firewalls only have routes to the subnets in their availability zone, there would be reachability issues when using an internal load-balancer.

Table 10 Static routes for the vmseries-a firewall

Name	Subnet	Interface	Next hop
Web Subnet - a	10.100.2.0/24	ethernet1/2	10.100.1.1
Business Subnet -a	10.100.3.0/24	ethernet1/2	10.100.1.1
DB Subnet - a	10.100.4.0/24	ethernet1/2	10.100.1.1
Web Subnet - b	10.100.130.0/24	ethernet1/2	10.100.1.1
Business Subnet - b	10.100.131.0/24	ethernet1/2	10.100.1.1
DB Subnet - b	10.100.132.0/24	ethernet1/2	10.100.1.1

Step 1: Log in to the Panorama web interface.

Step 2: In the **Template** list, choose **AZ-a-Stack**.

Step 3: Navigate to **Network > Virtual Routers**, click **vr-default**, and then click **Override**.

Step 4: On the Static Routes > IPv4 tab, click **Add**.

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

Step 6: In the **Destination** box, enter **10.100.2.0/24**.

Step 7: In the **Interface** list, choose **ethernet1/2**.

Step 8: In the **Next Hop** box, enter **10.100.1.1**, and then click **OK**.

Step 9: Repeat Step 1-Step 8 for all routes listed in Table 10.

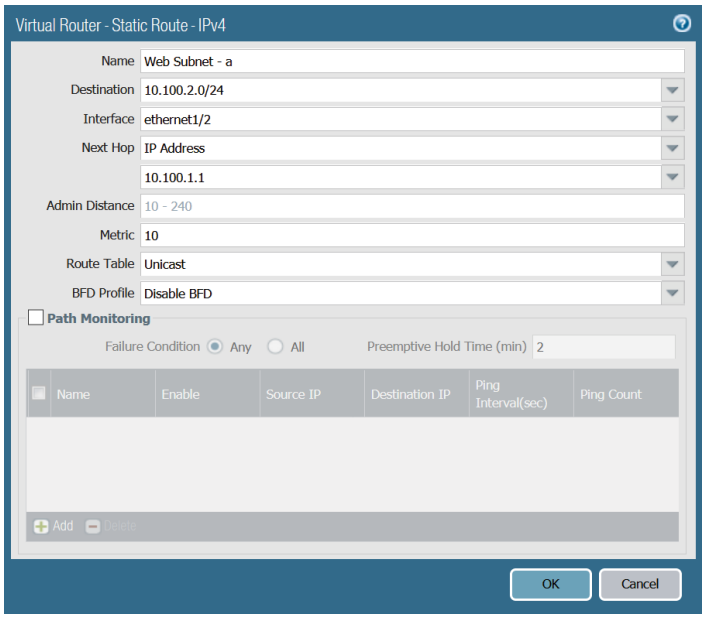


Table 11 Static routes for the vmseries-b firewall

Name	Subnet	Interface	Next hop
Web Subnet - a	10.100.2.0/24	ethernet1/2	10.100.129.1
Business Subnet - a	10.100.3.0/24	ethernet1/2	10.100.129.1
DB Subnet - a	10.100.4.0/24	ethernet1/2	10.100.129.1
Web Subnet - b	10.100.130.0/24	ethernet1/2	10.100.129.1
Business Subnet - b	10.100.131.0/24	ethernet1/2	10.100.129.1
DB Subnet - b	10.100.132.0/24	ethernet1/2	10.100.129.1

Step 10: In the **Template** list, choose **AZ-b-Stack**.

Step 11: Navigate to **Network > Virtual Routers**, click **vr-default**, and then click **Override**.

Step 12: On the Static Routes > IPv4 tab, click **Add**.

Step 13: In the **Name** box, enter **Web Subnet - a**.

Step 14: In the **Destination** box, enter **10.100.2.0/24**.

Step 15: In the **Interface** list, choose **ethernet1/2**.

Step 16: In the **Next Hop** box, enter **10.100.129.1**, and then click **OK**.

Step 17: Repeat Step 10-Step 16 for all routes listed in Table 11.

Step 18: On the **Commit** menu, click **Commit to Panorama**, and then click **Commit**.

Procedures

Next, you onboard the VM-Series firewalls to the Panorama server(s), and then you push configuration templates to the firewalls.

4.1 Add the VM-Series Firewalls to Panorama Server(s)

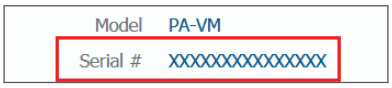
In this procedure, you add the VM-Series firewalls to Panorama and associate them to their respective device group and template stack.

Table 12 Mapping of VM-Series firewalls to template stacks

VM-Series firewall	Device group	Template stack
vmseries-a	AWS	AZ-a-Stack
vmseries-b	AWS	AZ-b-Stack

Step 1: Log in to the first VM-Series firewall's web interface.

Step 2: In **Dashboard > General Information**, record the serial number.

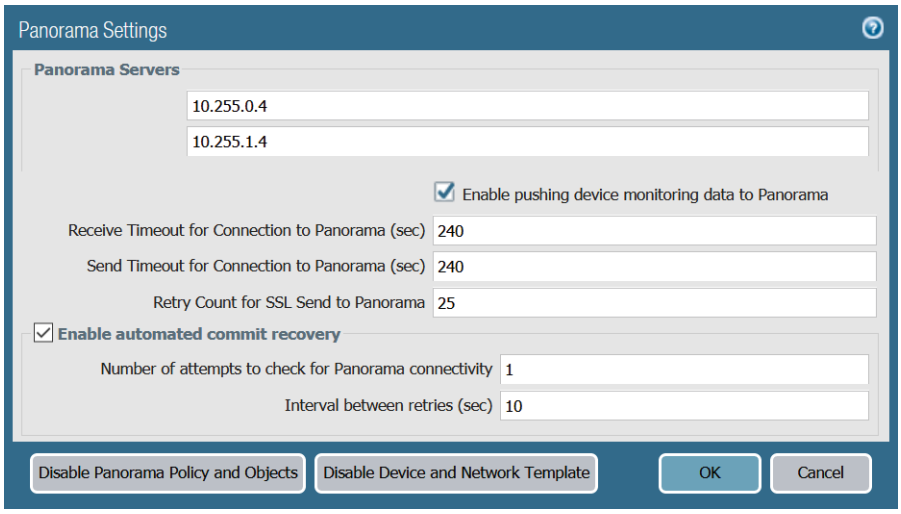


Step 3: In **Device > Setup > Management > Panorama Settings**, click the **Edit** cog.

Step 4: In the Panorama Servers section, in the top box, enter the address for the primary Panorama server (example: 10.255.0.4).

Step 5: If you are using Panorama in a high-availability pair, in the second box, enter the address for the secondary Panorama server (example: 10.255.1.4).

Step 6: Click **OK**.



Step 7: Click **Commit**, and then click **Commit**.

Step 8: Log in to the primary Panorama server.

Step 9: In **Panorama > Managed Devices > Summary**, click **Add**.

Step 10: In the **Devices** box, enter the serial number from Step 2, and then click **OK**. The Device Association window opens.

Step 11: In the **Device Group** list, choose **AWS**.

Step 12: In the **Template Stack** list, choose **AZ-a-Stack**, and then click **OK**.

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

Step 14: In **Panorama > Managed Devices > Summary**, verify that the device state of the VM-Series firewall is Connected. It may take a few minutes for the state to change.

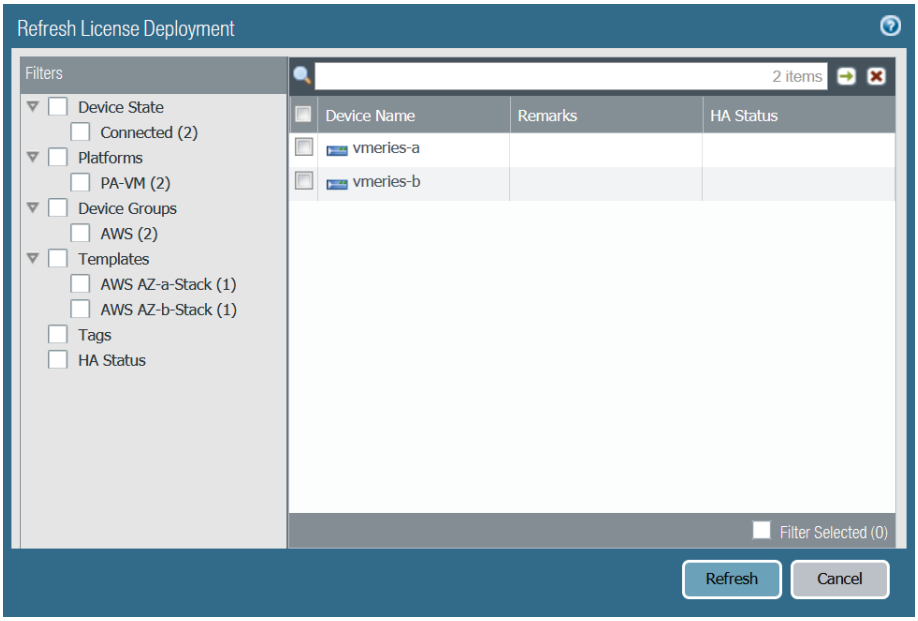
	Device Name	Model	IP Address IPV4	Variables	Template	Device State	Device Certificate	Device Certific Expiry Date
▽	**AWS (1/1 Devices Connected): Shared > AWS**							
	vmseries-a	PA-VM	10.100.127.10 (DHCP)	Create	AZ-a-Stack	Connected	None	N/A

Step 15: Repeat this procedure for the second VM-Series firewall in Table 12.

4.2 Refresh the VM-Series Firewall's License to Enable Cortex Data Lake

Step 1: In **Panorama > Device Deployment > Licenses**, click **Refresh**. The Refresh License Deployment window appears.

Step 2: In the **Device Name** column, select the VM-Series firewalls, and then click **Refresh**.



Deploying Inbound and Outbound Security

This section describes how to deploy the AWS load-balancing infrastructure and then configure firewall policies, objects, and settings to complete networking for web-server access from the internet.

Procedures

5.1 Configure the Public Application Load Balancer

You create an ALB to direct inbound web traffic to the VM-Series firewalls. In this procedure, the load-balancer probes target the private IP addresses of the VM-Series public interfaces.

Step 1: Sign in to the AWS console, and then in the list at the top of the page, choose the **US West (Oregon)** data center.

Step 2: On the EC2 Compute dashboard, navigate to **LOAD BALANCING > Load Balancers**.

Step 3: Click **Create Load Balancer**, and then on **Application Load Balancer**, click **Create**.

Step 4: In the Basic Configuration pane, in the **Name** box, enter **ExampleApplication-ALB**.

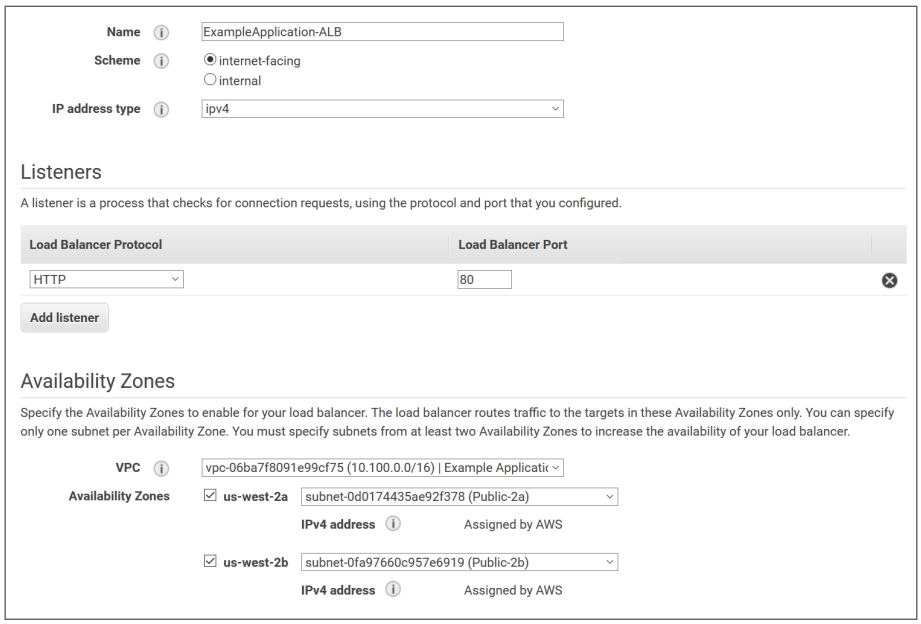
Step 5: For **Scheme**, select **internet-facing**.

Step 6: In the **IP address type** list, choose **ipv4**.

Step 7: In the Listeners pane, in **Load Balancer Protocol** list, choose **HTTP**, and then in the **Load Balancer Port** box, ensure the value is **80**.

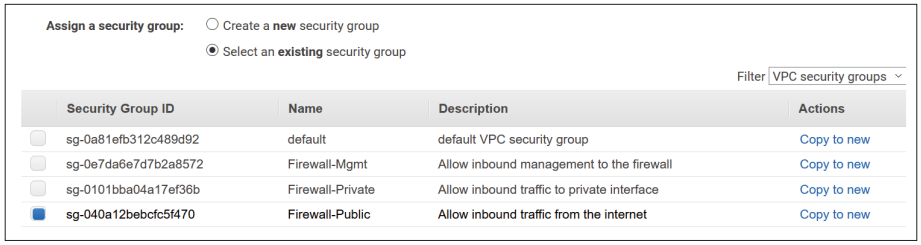
Step 8: In the Availability Zones pane, do the following:

- In the **VPC** list, choose **Example Application**.
- Select **us-west-2a**, and then in the list of subnet IDs, choose **Public-2a**.
- Select **us-west-2b**, and then in the list of subnet IDs, choose **Public-2b**.



Step 9: Click **Next: Configure Security Settings**, read the HTTP security warning, and then click **Next: Configure Security Settings**.

Step 10: In **Configure Security Groups > Assign a security group**, select **Select an existing security group**, and then select **Firewall-Public**. Ensure that only the **Firewall-Public** security group is selected, and then click **Next: Configure Routing**.



Step 11: In the **Target Group** list, choose **New target group**.

Step 12: In the **Name** box, enter **vm-series**.

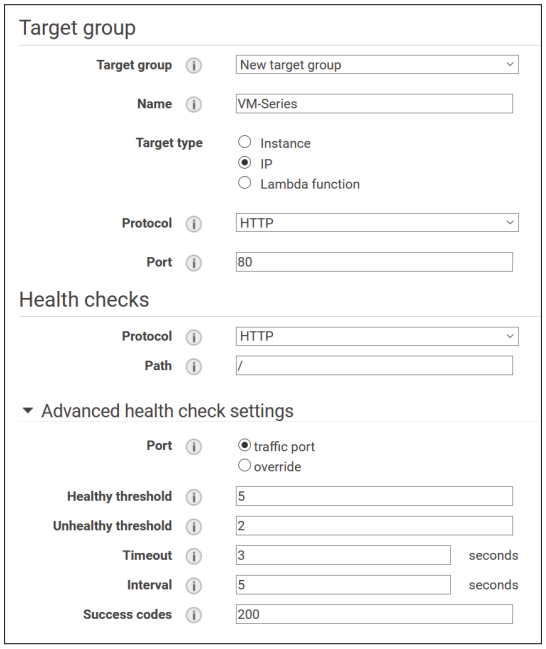
Step 13: In the **Target type** list, choose **IP**.

Step 14: In the **Protocol** list, choose **HTTP**.

The next two steps set the health check probe timers to a more aggressive timeout for faster failover. If you set too aggressive a timeout, you could have false failure detection events. The tuning in your environment may vary, but this setting is moderate.

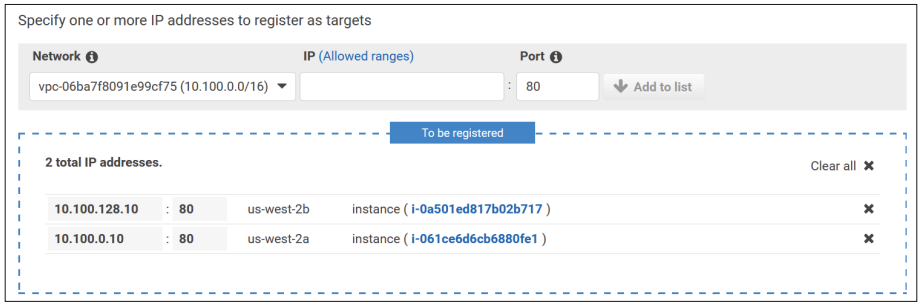
Step 15: Expand **Advanced health check settings**, and then in the **Timeout** box, enter **3**.

Step 16: In the **Interval** box, enter **5**, and then click **Next: Register Targets**.



Step 17: In **Register Targets > Network**, in the **IP** box, enter **10.100.0.10**, and then click **Add to list**.

Step 18: In the **IP** box, enter **10.100.128.10**, click **Add to list**, and then click **Next: Review**.



Step 19: Click **Create**, and then click **Close**.

5.2 Configure the NAT Policy

In Panorama, you create a NAT rule for the firewalls that translates incoming traffic on port 80 to the IP address of the internal load balancer.

The internal Application Load Balancer does not have a static IP address assigned to it; rather, AWS assigns it an FQDN. In this way, the load balancer has an IP address in both availability zone a and b, and if a load balancer fails or scales out with new IP addresses, a periodic check of the FQDN IP address assigns and detects new IP addresses. Use the internal load balancer's FQDN as the new destination of the traffic.

NAT Pre Rules are added to the top of the rule order and are evaluated first. You cannot override Pre Rules on the local device.

Table 13 Example application NAT

Name	Service	Destination FQDN
inbound-example-application	service-http	internal-ALB-1687781693.us-west-2.elb.amazonaws.com

Step 1: Navigate to **Policies > NAT > Pre Rules**, in the **Device Group** list, choose **AWS**, and then click **Add**.

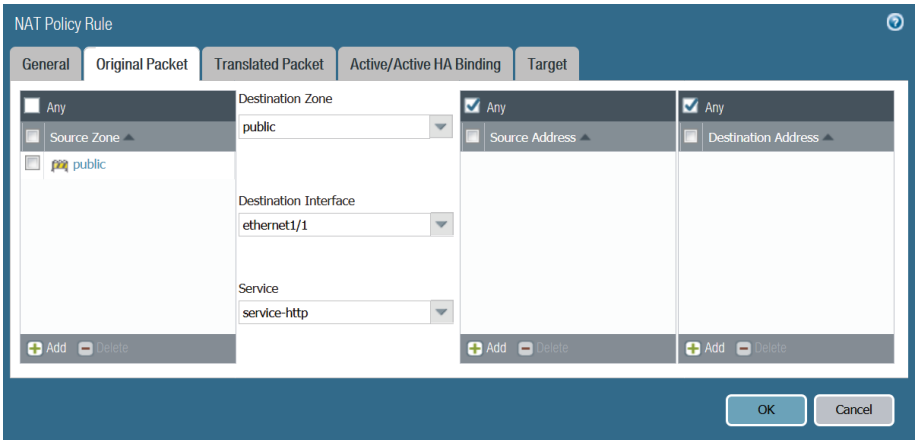
Step 2: In the **Name** box, enter **inbound-example-application**.

Step 3: On the Original Packet tab, in the Source Zone pane, click **Add**, then select **public**.

Step 4: In the **Destination Zone** list, choose **public**.

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

Step 6: In the **Service** list, choose **service-http**.



Step 7: On the Translated Packet tab, in the Source Address Translation pane, , in the **Translation Type** list, choose **Dynamic IP And Port**.

Step 8: In the **Address Type** list, choose **Interface Address**.

Step 9: In the **Interface** list, choose **ethernet 1/2**.

Step 10: In the **Translation Type** list, choose **Dynamic IP (with session distribution)**.

Step 11: In the **Translated Address** list, choose **New Address**. The New Address object windows appears.

Step 12: In the **Name** box, enter **internal-ALB**.

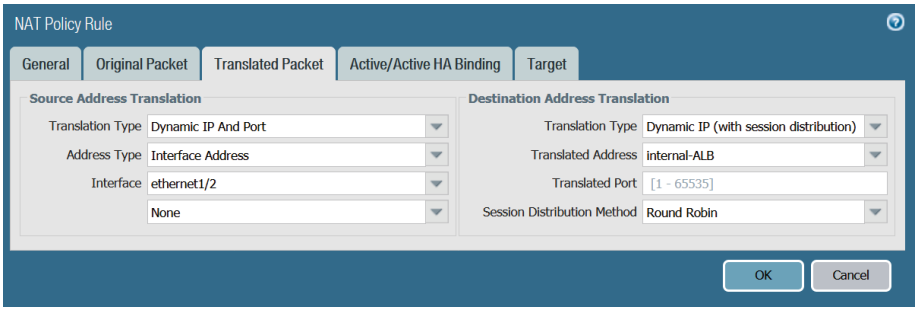
Step 13: Clear **Shared**.

Step 14: In the **Type** list, choose **FQDN**.

Step 15: In the **FDQN** box, enter **internal-ALB-1687781693.us-west-2.elb.amazonaws.com**, and then click **OK**.

> **Note**
>
> You can find the FQDN of the load balancer on the AWS console. In the EC2 dashboard, navigate to **Load Balancing** > **Load Balancers**, and then look in the DNS name column.

Step 16: On the Target tab, select **Any (target to all devices)**, and then click **OK**.



5.3 Enable the XFF and URL Profile

Because AWS translates the source address of traffic traversing the load balancer, it may be useful to enable X-Forwarded-For (XFF) in the firewall so that you can identify the real source address in the VM-Series firewall logs. This procedure assumes that **Use X-Forwarded-For Header in User-ID** has been enabled as part of a baseline settings template in Panorama.

Step 1: Navigate to **Objects > Security Profiles > URL Filtering**, and then click **Add**.

Step 2: In the URL Filtering Profile pane, in the **Name** box, enter **Enable-XFF-Logging**.

Step 3: On the Categories tab, set the action to **Alert** for all categories.

Step 4: On the URL Filtering Settings tab, under **HTTP Header Logging**, select **X-Forwarded-For**, and then click **OK**.

Note

To view the XFF header information for sessions, ensure the Source User column is shown in the firewall's URL filtering log monitor view.

5.4 Configure the Security Policy

This example allows inbound web traffic to the web application. Security Pre Rules are added to the top of the rule order and are evaluated first. You cannot override Pre Rules on the local device.

Step 1: Navigate to **Policies > Security > Pre Rules**, and then click **Add**.

Step 2: In the **Name** box, enter **inbound-example-application**.

Step 3: On the Source tab, under Source Zone, click **Add**.

Step 4: In the **Source Zone** list, choose **public**.

Step 5: On the Destination tab, in the Destination Zone pane, click **Add**.

Step 6: In the **Destination Zone** box, enter **private**.

Step 7: In the Destination Address pane, click **Add**.

Step 8: In the Destination Address pane, click **Add**.

Step 9: In the **Destination Address** box, enter **10.100.0.10/32**.

Step 10: In the Destination Address pane, click **Add**.

Step 11: In the **Destination Address** box, enter **10.100.128.10/32**.

Step 12: On the Application tab, in the Applications pane, click **Add**.

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

Step 14: On the Service/URL Category tab, in the **Service** list, choose **application-default**.

Step 15: On the Actions tab, in the **Action** list, choose **Allow**.

Step 16: In the **Profile Type** list, choose **Profiles**.

Step 17: In the **URL Filtering** list, choose **Enable-XFF-Logging**.

Step 18: In the **Log Forwarding** list, choose **Forward-to-Cortex-Data-Lake**.

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

5.5 Locate the Inbound Load-Balancer DNS Name

At this point, the inbound path for HTTP traffic to web servers should be operational. To reach the web servers, you must know the public load balancer's DNS name.

Step 1: On the EC2 Compute dashboard, navigate to **LOAD BALANCING > Load Balancers**, and then select the public load balancer.

Step 2: On the Description tab, locate the **DNS name**. You use this DNS name *(A record)* to reach the example application.

Procedures

Deploying Outbound Security

6.1 Configure the Firewall NAT Policy

You now configure a policy to allow private IP addressed web servers to access endpoints in the internet. The outbound traffic maps to the Elastic IP address mapped to the firewall's eth1 interface as it crosses the internet gateway function that is mapped to the VPC on the public subnet.

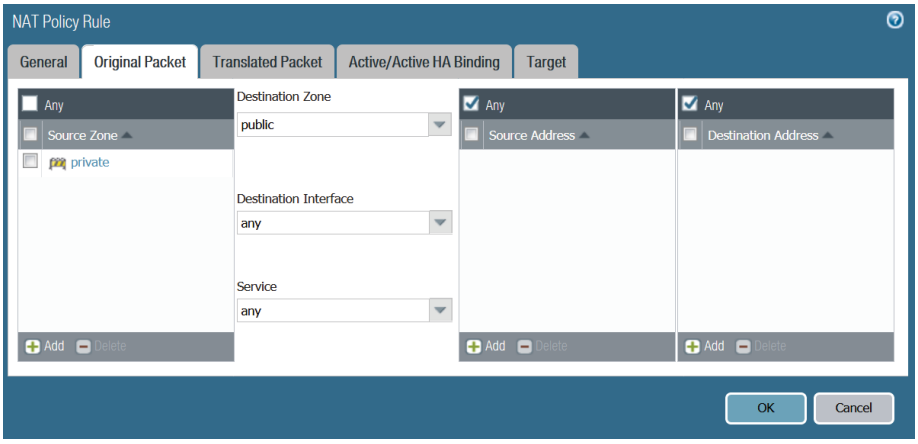
Step 1: Log in to the primary Panorama server.

Step 2: Navigate to **Policies > NAT > Pre Rules**, in the **Device Group** list, choose **AWS**, and then click **Add**.

Step 3: In the **Name** box, enter **outbound-internet**.

Step 4: On the Original Packet tab, in the **Source Zone** pane, click **Add**, and then select **private**.

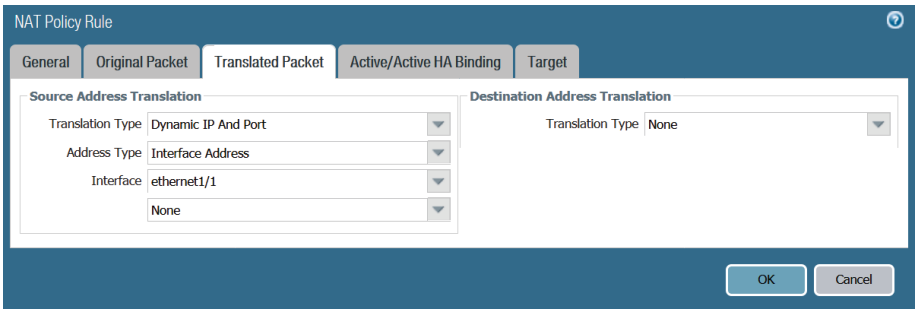
Step 5: In the **Destination Zone** list, choose **public**.



Step 6: On the Translated Packet tab, in the Source Address Translation section, in the **Translation Type** list, choose **Dynamic IP And Port**.

Step 7: In the Source Address Translation section, in the **Address Type** list, choose **Interface Address**.

Step 8: In the **Interface** list, choose **ethernet1/1**, and then click **OK**.



6.2 Configure the Firewall Security Policy

You can use the outbound policy rules to enforce the Acceptable Use Policy for an organization (for example, to block access to specific URL categories or to allow DNS traffic for all users). This example uses a common outbound policy for all private subnets. If you wish to use a differentiated policy, create separate rules for each private subnet.

The common outbound security policy example permits these applications:

- NTP
- DNS
- APT-GET

Add additional applications to your outbound policy as required.

Step 1: Log in to the Panorama web interface.

Step 2: In the **Device Group** list, choose **AWS**.

Step 3: Navigate to **Policies > Security > Pre Rules**, and then click **Add**.

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

Step 5: On the Source tab, under Source Zone, click **Add**.

Step 6: In the **Source Zone** list, choose **private**.

Step 7: On the Destination tab, under Destination Zone, click **Add**.

Step 8: In the **Destination Zone** list, choose **public**.

Step 9: On the Application tab, in the Applications pane, click **Add**.

Step 10: In the search box, enter **ntp**, and then in the results list, choose **ntp**.

Step 11: In the Applications pane, click **Add**.

Step 12: In the search box, enter **dns**, and then in the results list, choose **dns**.

Step 13: In the Applications pane, click **Add**.

Step 14: In the search box, enter **apt-get**, and then in the results list, choose **apt-get**.

Step 15: On the Actions tab, in the **Action** list, choose **Allow**.

Step 16: In the **Log Forwarding** list, choose **Forward-to-Cortex-Data-Lake**.

Step 17: On the Target tab, select **Any (target to all devices)**, and then click **OK**.

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

Step 18: On the **Commit** menu, click **Commit and Push**, and then click **Commit and Push** again.

6.3 Configure AWS Route Tables

Configure a default route for the private networks that points to the VM-Series firewall. Each subnet uses the firewall in its respective availability zone.

Table 14 Route tables

Route table name	Route destination	Target	Subnets assigned
Private-a Example Application	0.0.0.0/0	vmseries-a-private	Web-server-2a, Business-2a, DB-2a
Private-b Example Application	0.0.0.0/0	vmseries-b-private	Web-server-2b, Business-2b, DB-2b

Step 1: On the VPC dashboard, navigate to **Virtual Private Cloud > Route Tables**.

Step 2: At the top of the pane, click **Create Route Table**.

Step 3: In the **Name tag** box, enter **Private-a Example Application**.

Step 4: In the **VPC** list, choose **Example Application**.

Step 5: Click **Create**, and then click **Close**.

Step 6: With **Private-a Example Application** selected in the top pane, click the **Routes** tab on the bottom pane, and then click **Edit routes**.

Step 7: Click **Add route**, and then in the **Destination** box, enter **0.0.0.0/0**.

Step 8: Click in the **Target** box, choose the **vmseries-a-private** network interface.

Step 9: Click **Save routes**, and then click **Close**.

Step 10: On the Subnet Associations tab, click **Edit subnet associations**.

Step 11: In the list, choose subnets **Web-server-2a**, **Business-2a**, and **DB-2a**, and then click **Save**.

Step 12: Repeat this procedure for the remaining route table in Table 14.

At this point, the outbound path for allowed traffic from web servers should be operational.

Deploying Backhaul VPN to On-Premises Services

This procedure configures connectivity to your VPC from an on-premises firewall. This design terminates the VPN connection on the VM-Series firewalls so that traffic to application instances can be controlled by firewall policy.

This design provides configuration for a single on-premises firewall peering to both firewalls in the VPC, with static and dynamic routing options. Optionally, you can set up the on-premise firewall in a high-availability, active/passive configuration.

This procedure provides configuration for an on-premises firewall with the following assumptions:

- The firewall is an operational Palo Alto Networks firewall running PAN-OS.
- The on-premises firewall has a public IP address to which the VPN tunnels can peer.

Procedures

Configuring VM-Series Firewalls for VPN to On-Premises

Using these procedures, you configure the VM-Series firewalls for VPN and BGP connectivity to the on-premises firewalls.

7.1 Create Panorama Template Variables

Next, you create the variables used in the network templates in order to configure the VM-Series firewalls.

Table 15 Panorama template variables

Variable name	Type	Value
$Tunnel-Interface-IP	IP Netmask	None
$BGP-Router-ID	IP Netmask	None
$Tunnel-Interface-Peer	IP Netmask	None
$IKE-Gateway-Peer	IP Netmask	None

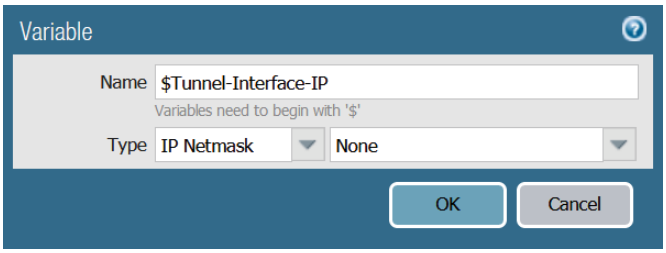
Step 1: Log in to the Panorama web interface.

Step 2: Navigate to **Panorama > Templates**, and in the **Variables** column of **Single-VPC-Network-Settings**, select **Manage**.

Step 3: In the Template Variables pane, click **Add**.

Step 4: In the **Name** box, enter **$Tunnel-Interface-IP**.

Step 5: In the **Type** lists, select **IP Netmask** and **None**, and then click **OK**.



Step 6: Repeat this procedure for all variables listed in Table 15.

Step 7: On the **Commit** menu, click **Commit to Panorama**, and then click **Commit**.

7.2 Configure the VPN Tunnel Interface

First, you add a tunnel interface to the Panorama's **Single-VPC-Network-Settings** template. This template is associated to both template stacks, and Panorama configures both firewalls with these settings.

Step 1: Log in to the primary Panorama web interface.

Step 2: Navigate to **Network > Interfaces**, in the **Template** list, choose **Single-VPC-Network-Settings**.

Step 3: On the Tunnel tab, click **Add**.

Step 4: In the **Interface Name** box, enter **1**.

Step 5: In the **Comment** box, enter **VPN to on-premises NGFWs**.

Step 6: In the **Virtual Router** list, choose **vr-default**.

Step 7: In the **Security Zone** list, choose **New Zone**.

Step 8: In the **Name** box, enter **vpn**, and then click **OK**.

Step 9: On the IPv4 tab, click **Add**, and then select **$Tunnel-Interface-IP**.

Step 10: On the Advanced tab, in the **MTU** box, enter **1427**, and then click **OK**.

Setting the MTU size lower minimizes IP fragmentation due to tunnel and IPSec encapsulation overhead. Next, you set the public-facing interface to detect maximum segment size and prevent fragmentation.

Step 11: In **Network > Interfaces**, on the Ethernet tab, click the public-facing Ethernet interface **ethernet1/1**.

Step 12: On the Advanced tab, in the Other Info section, select **Adjust TCP MSS**, and then click **OK**.

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

7.3 Configure IKEv2 and IPSec

You use the values specified in Table 16 for the steps in this procedure. The Palo Alto Networks firewalls in AWS and the on-premises firewall can successfully negotiate these values. The table lists the strongest authentication and encryption values that are available.

Table 16 IKEv2 and IPSec settings

Parameter	Value	Comments
IKEv2 DH group	group20	Diffie-Helman Group 20
IKEv2 authentication	Sha512	Secure Hash Algorithm-2 with 512-bit digest
IKEv2 encryption	aes-256-cbc	Advanced Encryption Standard 256-bit with Cipher Block Chaining
IKEv2 Key Lifetime	8 hours	Equivalent to 28800 seconds
IKEv2 Authentication Multiple	3	—
IPSec encryption	aes-256-gcm	AES Galois Counter Mode (GCM) with 256-bit key
IPSec authentication	sha512	Secure Hash Algorithm-2 with 512-bit digest
IPSec DH group	20	Diffie-Helman Group 20
IPSec lifetime	1 hour	Equivalent to 3600 seconds

Step 1: Navigate to **Network > Network Profiles > IKE Crypto**, and then in the **Template** list, choose **Single-VPC-Network-Settings**.

Step 2: Click **Add**.

Step 3: In the **Name** box, enter **NGFW-IKE**.

Step 4: In the DH Group pane, click **Add**, and then select **group20**.

Step 5: In the Authentication pane, click **Add**, and then select **sha512**.

Step 6: In the Encryption pane, click **Add**, and then select **aes-256-cbc**.

Step 7: In the Timers pane, in the **Key Lifetime** list, choose **Seconds**, and then enter **28800**.

Step 8: In the **IKEv2 Authentication Multiple** box, enter **3**, and then click **OK**.

Step 9: In **Network > Network Profiles > IPSec Crypto**, click **Add**.

Step 10: In the **Name** box, enter **NGFW-IPSec**.

Step 11: In the Encryption pane, click **Add**, and then select **aes-256-gcm**.

Step 12: In the Authentication pane, click **Add**, and then select **sha512**.

Step 13: In the **DH Group** list, choose **group20**.

Step 14: In the **Lifetime** list, choose **Hours**, enter **1**, and then click **OK**.

7.4 Create an IKE Gateway to the On-Premises Firewall

Step 1: In **Network > Network Profiles > IKE Gateways**, click **Add**.

Step 2: On the General tab, in the **Name** box, enter **NGFW-GW**.

Step 3: In the **Version** list, choose **IKEv2 preferred mode**.

Step 4: In the **Interface** list, choose the firewall's public interface, **ethernet1/1**.

Step 5: For **Peer IP Address Type**, select **IP**.

Step 6: In the **Peer Address** list, choose **$IKE-Gateway-Peer**.

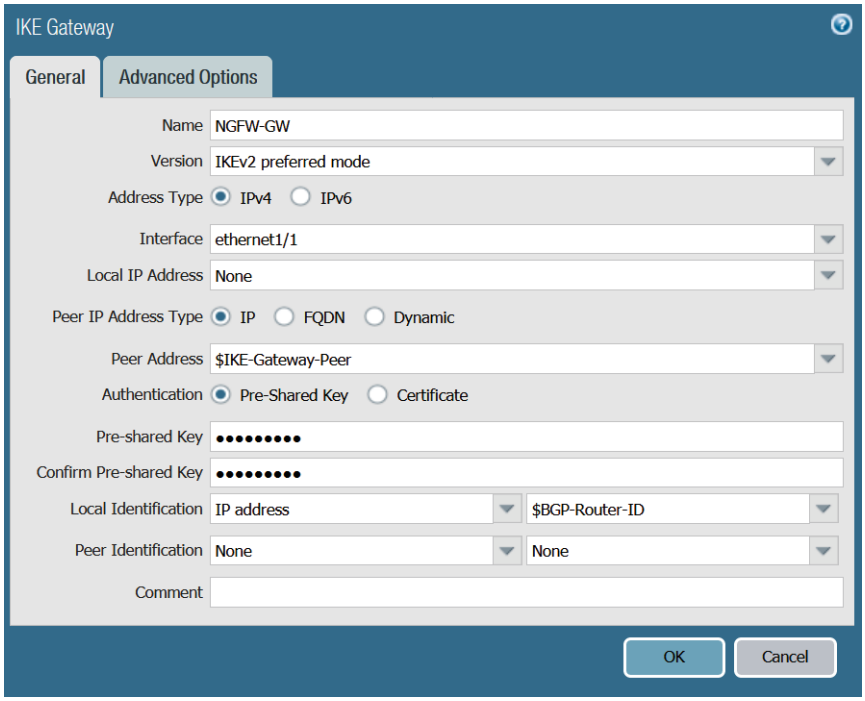
Step 7: For **Authentication**, select **Pre-Shared Key**.

Step 8: In the **Pre-shared Key** box, enter **ref1ARCH2**.

Step 9: In the **Confirm Pre-shared Key** box, enter **ref1ARCH2**.

Step 10: In the **Local Identification** list, choose **IP address**, and then select **$BGP-Router-ID**.

> **Note**
>
> When the far end of the VPN connection is crossing a network address translation, the peer IP address is the public address, and the corresponding private IP address to which it is translated is the peer identification IP address. If there are no NAT traversals, then you can leave the peer identification to the default None setting.



Step 11: On the Advanced Options tab, select **Enable NAT Traversal**.

Step 12: Under IKEv1, in the **Exchange Mode** list, choose **main**.

Step 13: In the **IKE Crypto Profile** list, choose **NGFW-IKE**.

Step 14: In the **Dead Peer Detection** > **Interval** box, enter **10**.

Step 15: In the **Dead Peer Detection** > **Retry** box, enter **3**.

Step 16: Under **IKEv2**, in the **IKE Crypto Profile** list, choose **NGFW-IKE**, and then click **OK**.

Step 17: On the **Commit** menu, click **Commit to Panorama**, and then click **Commit**.

7.5 Create an IPSec Tunnel to the On-Premises Firewall

You now create an IPSec tunnel that uses the tunnel interface. You assign one IPSec tunnel to a tunnel interface.

Step 1: In **Network > IPSec Tunnels**, click **Add**.

Step 2: In the **Name** box, enter **NGFW-TUN**.

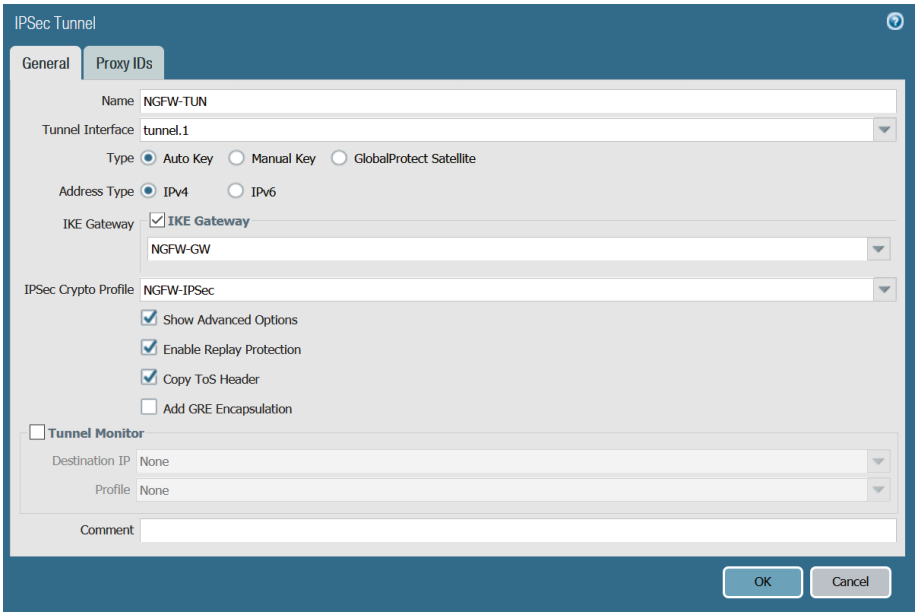
Step 3: In the **Tunnel Interface** list, choose **tunnel.1**.

Step 4: In the **IKE Gateway** list, choose **NGFW-GW**.

Step 5: In the **IPSec Crypto Profile** list, choose **NGFW-IPSec**.

Step 6: Select **Show Advanced Options**.

Step 7: Select **Copy ToS Header**, and then click **OK**.



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

7.6 Configure Route Redistribution Profiles

Next, you create two redistribution profiles in Panorama. You use the redistribution profiles when you configure BGP routing with the on-premises VPN firewalls. The first profile redistributes the connected private interface's subnet, and the second redistributes a filtered set of static routes that includes the web, business, and DB subnets.

Step 1: Navigate to **Network > Virtual Routers**, and then choose **vr-default**.

Step 2: On the Redistribution Profile tab, on the IPv4 pane, click **Add**.

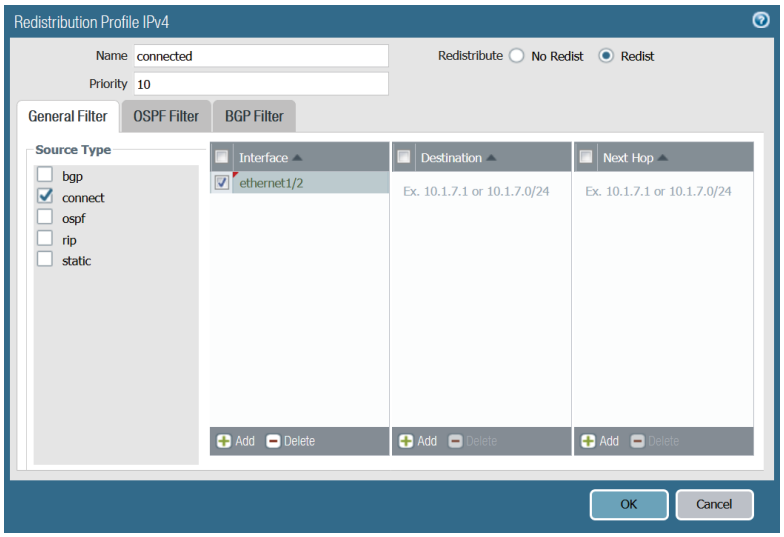
Step 3: In the **Name** box, enter **connected**.

Step 4: In the **Priority** box, enter **10**.

Step 5: For **Redistribute**, select **Redist**.

Step 6: For **Source Type**, select **connect**.

Step 7: In the **Interface** box, click **Add**, select **ethernet1/2**, and then click **OK**.



Step 8: On the Redistribution Profile tab, in the IPv4 pane, click **Add**.

Step 9: In the **Name** box, enter **static**.

Step 10: In the **Priority** box, enter **10**.

Step 11: For **Redistribute**, select **Redist**.

Step 12: For **Source Type**, select **static**.

Step 13: In the **Interface** box, click **Add**, select **ethernet1/2**, and then click **OK**.

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

7.7 Configure BGP Peering with the On-Premises Firewall

Next, you deploy BGP routing on the VM-Series firewalls for on-premises connectivity. Each VM-Series firewall peers with the on-premises next-generation firewall across its IPSec tunnel.

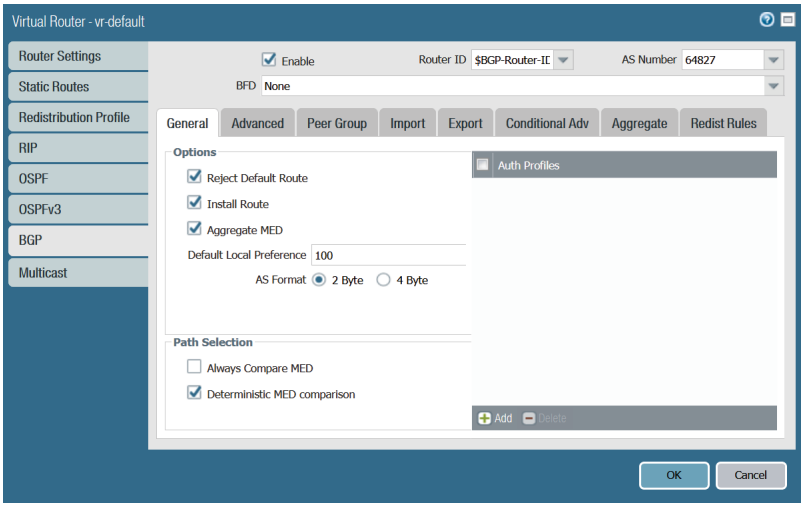
Step 1: Navigate to **Network > Virtual Router**, and then select **vr-default**.

Step 2: On the BGP tab, at the top of the pane, click **Enable**.

Step 3: In the **Router ID** box, enter **$BGP-Router-ID**.

Step 4: In the **AS Number** box, enter **64827**.

Step 5: On the General tab, select **Install Route**.



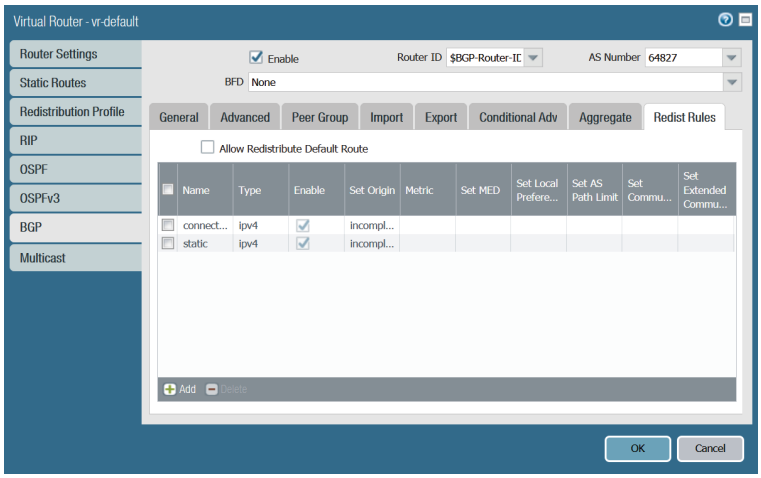
Next, you configure BGP to redistribute the connected and static routes in the redistribution profiles.

Step 6: On the Redist Rules tab, click **Add**.

Step 7: In the **Name** list, choose **connected**, and then click **OK**.

Step 8: On the Redist Rules tab, click **Add**.

Step 9: In the **Name** list, choose **static**, and then click **OK**.



Next, you build BGP peer groups to manage peering with the on-premises next-generation firewall.

Step 10: In **BGP > Peer Group**, click **Add**.

Step 11: In the **Name** box, enter **NGFWs**.

Step 12: For **Import Next Hop**, select **Use Peer**.

Step 13: For **Export Next Hop**, select **Use Self**.

Step 14: Clear **Remove Private AS**, and then click **Add**.

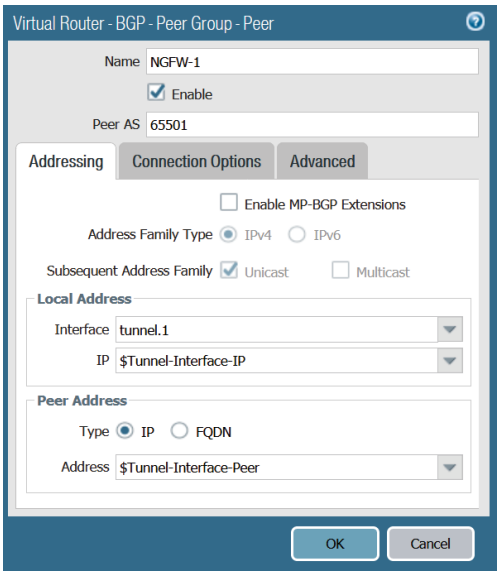
Step 15: In the **Name** box, enter **NGFW-1**.

Step 16: In the **Peer AS** box, enter **65501**.

Step 17: Under Local Address, in the **Interface** list, choose **tunnel.1**.

Step 18: In the **IP** list, choose **$Tunnel-Interface-IP**.

Step 19: In the **Peer Address IP** box, enter $Tunnel-Interface-Peer.



Next, you configure shorter timers to drive a faster convergence in the event of a link or node failure.

Step 20: On the Connections Options tab, in the **Keep Alive Interval** box, enter 10.

Step 21: In the **Hold Time** box, enter 30, and then click **OK**.

Step 22: Click **OK**.

Step 23: On the **Commit** menu, click **Commit to Panorama**, and then click **Commit**.

7.8 Configure the NAT Policy

In this procedure, you use NAT Pre Rules that are added to the top of the NAT rule order and are evaluated first. You cannot override Pre Rules on the local device. The NAT rules for the on-premises-to-private flows ensure that traffic returns to the same VM-Series firewall that processed the inbound flow.

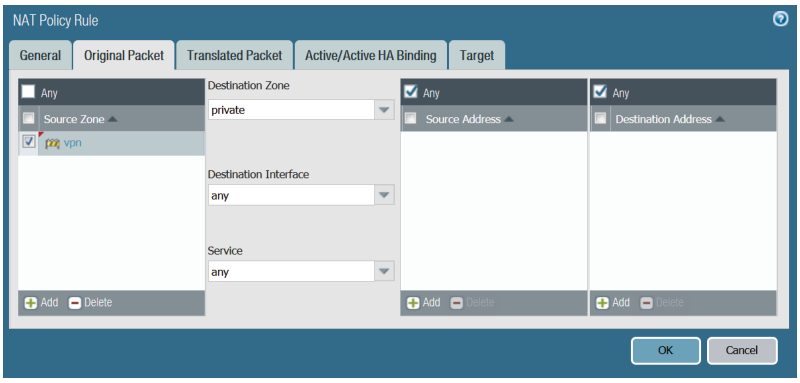
Step 1: Navigate to **Policies > NAT > Pre Rules**.

Step 2: In the **Device Group** list, choose AWS, and then click **Add**.

Step 3: In the **Name** box, enter inbound-vpn.

Step 4: On the Original Packet tab, in the Source Zone pane, click **Add**, and then enter vpn.

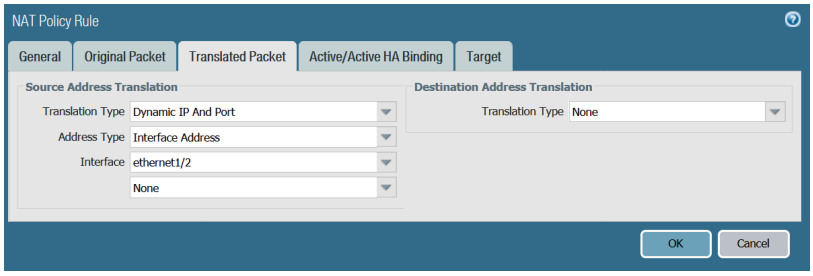
Step 5: In the **Destination Zone** list, choose **private**.



Step 6: On the Translated Packet tab, in the Source Address Translation pane, in the **Translation Type** list, choose **Dynamic IP And Port**.

Step 7: In the Source Address Translation pane, in the **Address Type** list, choose **Interface Address**.

Step 8: In the **Interface** list, choose **ethernet1/2**, and then click **OK**.



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

7.9 Configure the Security Policy

In this procedure, you create three separate security policy rules:

- Inbound traffic from the internet, allowing IKE and IPSEC-ESP-UDP
- Inbound traffic from the tunnel, allowing PING and BGP
- Inbound traffic from on-premises resources, allowing SSH and HTTP

The security policy example for inbound access from the internet permits these applications:

- IKE
- IPSEC-ESP-UDP

Add additional applications to your policy as required.

Step 1: Navigate to **Policies > Security > Pre Rules**, and then click **Add**.

Step 2: In the **Name** box, enter **inbound-internet**.

Step 3: On the Source tab, in the Source Zone pane, click **Add**.

Step 4: In the **Source Zone** list, choose **public**.

Step 5: On the Destination tab, in the Destination Zone pane, click **Add**.

Step 6: In the **Destination Zone** list, choose **public**.

Step 7: On the Application tab, in the Applications pane, click **Add**.

Step 8: In the search box, enter **ike**, and then in the results list, choose **ike**.

Step 9: In the Applications pane, click **Add**.

Step 10: In the search box, enter **ipsec-esp-udp**, and then in the results list, choose **ipsec-esp-udp**.

Step 11: On the Actions tab, in the **Action** list, choose **Allow**.

Step 12: In the **Log Forwarding** list, choose **none**.

Step 13: On the Target tab, select **Any (target to all devices)**, and then click **OK**.

The security policy example for inbound access from the VPN tunnel permits these applications:

- PING
- BGP

Add additional applications to your policy as required.

Step 14: Navigate to **Policies > Security > Pre Rules**, and then click **Add**.

Step 15: In the **Name** box, enter **intrazone-vpn**.

Step 16: On the Source tab, in the Source Zone pane, click **Add**.

Step 17: In the **Source Zone** list, choose **vpn**.

Step 18: On the Destination tab, in the Destination Zone pane, click **Add**.

Step 19: In the **Destination Zone** list, choose **vpn**.

Step 20: On the Application tab, in the Applications pane, click **Add**.

Step 21: In the search box, enter **bgp**, and then in the results list, choose **bgp**.

Step 22: In the Applications pane, click **Add**.

Step 23: In the search box, enter **ping**, and then in the results list, choose **ping**.

Step 24: On the Actions tab, in the **Action** list, choose **Allow**.

Step 25: In the **Log Forwarding** list, choose **none**.

Step 26: On the Target tab, select **Any (target to all devices)**, and then click **OK**.

The security policy example for inbound access from on-premises resources permits these applications:

- SSH
- PING
- WEB-BROWSING

Add additional applications to your policy as required.

Step 27: Navigate to **Policies > Security > Pre Rules**, and then click **Add**.

Step 28: In the **Name** box, enter **inbound-vpn**.

Step 29: On the Source tab, in the Source Zone pane, click **Add**.

Step 30: In the **Source Zone** list, choose **vpn**.

Step 31: On the Destination tab, in the Destination Zone pane, click **Add**.

Step 32: In the **Destination Zone** list, choose **private**.

Step 33: On the Application tab, in the Applications pane, click **Add**.

Step 34: In the search box, enter **ssh**, and then in the results list, choose **ssh**.

Step 35: In the Applications pane, click **Add**.

Step 36: In the search box, enter **web-browsing**, and then in the results list, choose **web-browsing**.

Step 37: In the Applications pane, click **Add**.

Step 38: In the search box, enter **ping**, and then in the results list, choose **ping**.

Step 39: On the Actions tab, in the **Action** list, choose **Allow**.

Step 40: In the **Log Forwarding** list, choose **Forward-to-Cortex-Data-Lake**.

Step 41: On the Target tab, select **Any (target to all devices)**, and then click **OK**.

Step 42: On the **Commit** menu, click **Commit to Panorama**, and then click **Commit**.

7.10 Configure Variable Values and a Push Configuration

In this procedure, you add values to the template variables and push the VPN and BGP configuration to the VM-Series firewalls.

Table 17 Panorama template variable values

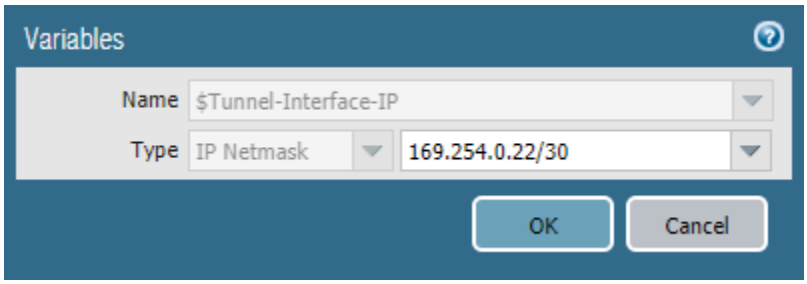
Variable name	vmseries-a value	vmseries-b value
$Tunnel-Interface-IP	169.254.0.22/30	169.254.1.26/30
$BGP-Router-ID	44.231.198.10	54.71.121.107
$Tunnel-Interface-Peer	169.254.0.21	169.254.1.25
$IKE-Gateway-Peer	199.167.52.150	199.167.52.150

Step 1: Navigate to **Panorama > Managed Devices > Summary**, navigate to the **vmseries-a** row, and then click **Create**.

Step 2: In the **Create Device Variable Definition** dialog box, select **No**, and then click **OK**.

Step 3: In the **Template Variables for Device vmseries-a** dialog box, select the row for **$Tunnel-Interface-IP**.

Step 4: Click **Override**, enter **169.254.0.22/30**, and then click **OK**.



Step 5: Repeat this procedure for all **vmseries-a** values in Table 17.

Step 6: Repeat this procedure for **vmseries-b** values in Table 17.

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

Procedures

Configuring an On-Premises Firewall for VPN Connectivity to AWS VM-Series Firewalls

8.1 Configure IKE and IPSec Profiles

For this procedure, you use the values specified in the following table. The VM-Series firewalls can successfully negotiate these values. The table lists the strongest authentication and encryption values that are available.

Table 18 IKE and IPSec profile settings

Parameter	Value	Comments
IKEv2 DH group	group20	Diffie-Hellman Group 20
IKEv2 authentication	sha512	Secure Hash Algorithm-2 with 512-bit digest
IKEv2 encryption	aes-256-cbc	Advanced Encryption Standard 256-bit with Cipher Block Chaining
IKEv2 Key lifetime	28800 sec	—
IKEv2 authentication multiple	3	—
IPSec encryption	aes-256-gcm	AES Galois Counter Mode (GCM) with 256-bit key
IPSec authentication	sha512	Secure Hash Algorithm-2 with 512-bit digest
IPSec DH group	20	Diffie-Hellman Group 20
IPSec lifetime	1 hour	Equivalent to 3600 seconds

Step 1: Navigate to **Network > Network Profiles > IKE Crypto**, and then click **Add**.

Step 2: In the **Name** box, enter NGFW-IKE.

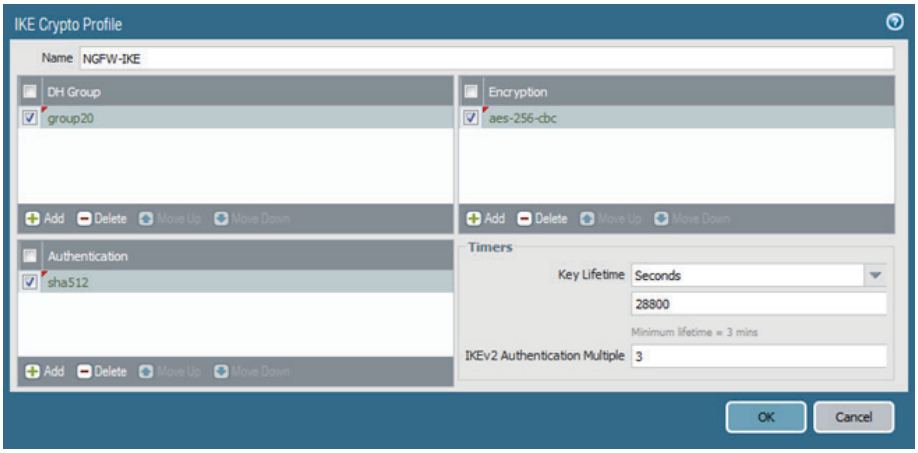
Step 3: In the DH Group pane, click **Add**, and then choose group20.

Step 4: In the Authentication pane, click **Add**, and then choose sha512.

Step 5: In the Encryption pane, click **Add**, and then choose aes-256-cbc.

Step 6: In the Timers pane, in the **Key Lifetime** list, choose Seconds, and then enter 28800.

Step 7: In the **IKEv2 Authentication Multiple** box, enter 3, and then click **OK**.



Step 8: In **Network** > **Network Profiles** > **IPSec Crypto**, click **Add**.

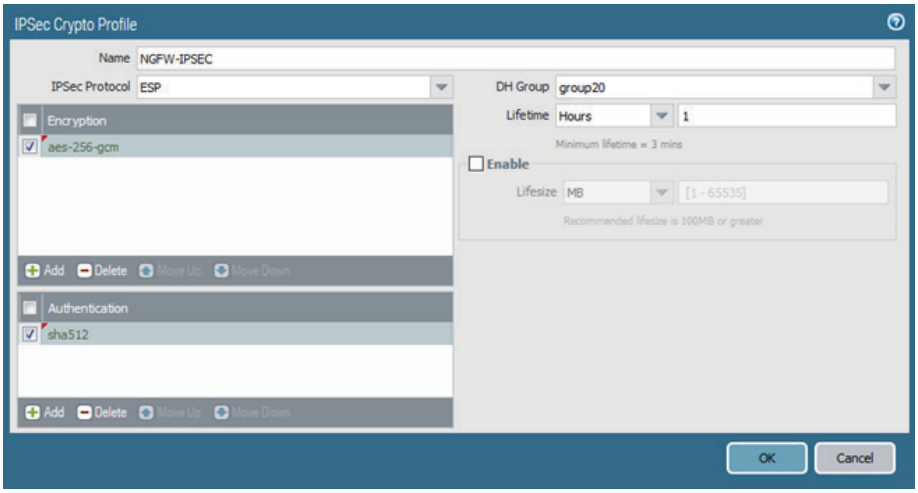
Step 9: In the **Name** box, enter NGFW-IPSEC.

Step 10: In the Encryption pane, click **Add**, and then choose aes-256-gcm.

Step 11: In the Authentication pane, click **Add**, and then choose sha512.

Step 12: In the **DH Group** list, choose group20.

Step 13: In the **Lifetime** list, choose Hours, enter 1, and then click **OK**.



Step 14: Click **Commit**, and then click **Commit** again.

8.2 Configure the Name Objects, Zone, and Tunnel Interface

In this procedure, you configure the on-premises firewall with a VPN zone and tunnel interface for the IPSec tunnel to the VM-Series firewalls.

Table 19 Object and tunnel details

Name	Public IP address	Tunnel interface	Tunnel IP address
vmseries-a	44.231.198.10	tunnel.1	169.254.0.21/30
vmseries-b	54.71.121.107	tunnel.2	169.254.1.25/30

Step 1: Log in to the on-premises firewall's web interface.

First, you configure an address object for the VM-Series firewall with its public interface IP address.

Step 2: In **Objects > Addresses**, click **Add**.

Step 3: In the **Name** box, enter **vmseries-a**.

Step 4: In the **Type** list, choose **IP Netmask**.

Step 5: In the **Address** box, enter **44.231.198.10**, and then click **OK**.

Next, you create a security zone for the IPSec VPN tunnel.

Step 6: In **Network > Zones**, click **Add**.

Step 7: In the **Name** box, enter **vpn**.

Step 8: In the **Type** list, choose **Layer3**, and then click **OK**.

Next, you create the VPN tunnel interfaces.

Step 9: In **Network > Interfaces > Tunnel**, click **Add**.

Step 10: In the **Interface Name** box, enter **1**.

Step 11: In the **Comment** box, enter **link to vmseries-a**.

Step 12: On the Config tab, in the **Virtual Router** list, choose **default**.

Step 13: In the **Security Zone** list, choose **vpn**.

Step 14: On the IPv4 tab, click **Add**, enter **169.254.0.21/30**.

Step 15: On the Advanced tab, in the **MTU** box, enter **1427**, and then click **OK**.

Step 16: Repeat this procedure for the second tunnel interface listed in Table 19.

Step 17: Click **Commit**, and then click **Commit** again.

8.3 Create an IKE Gateway to the AWS VM-Series Firewalls

Step 1: Navigate to **Network > Network Profiles > IKE Gateways**, and then click **Add**.

Step 2: In the **Name** box, enter **VM-Series-a-GW**.

Step 3: In the **Version** list, choose **IKEv2 preferred mode**.

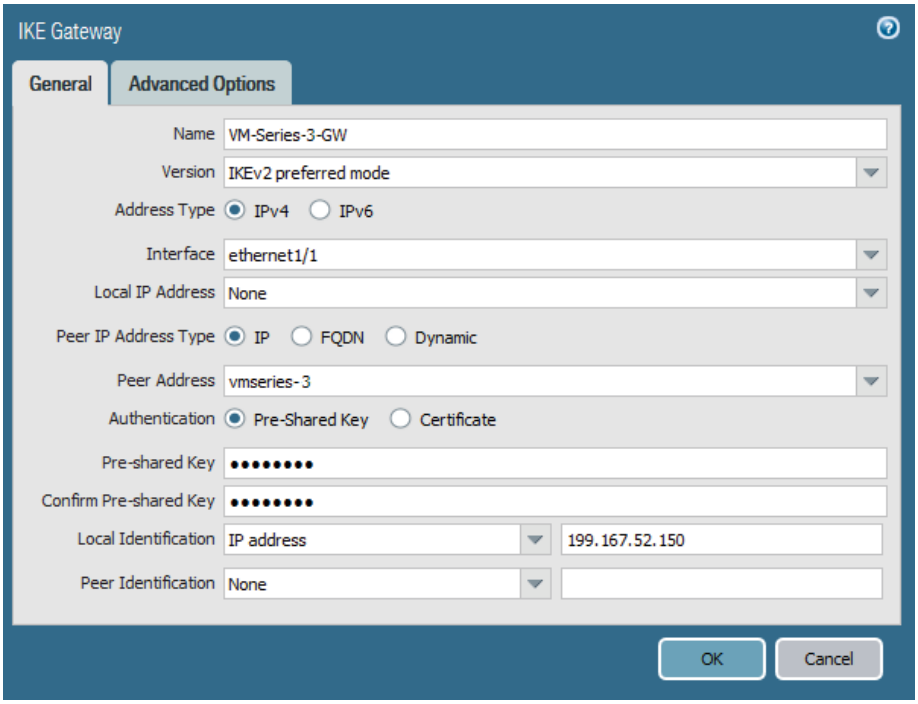
Step 4: In the **Interface** list, choose **ethernet1/1**.

Step 5: In the **Peer Address** list, choose **vmseries-a**.

Step 6: In the **Pre-shared Key** box, enter **ref1ARCH2**.

Step 7: In the **Confirm Pre-shared Key** box, enter **ref1ARCH2**.

Step 8: In the **Local Identification IP address** box, enter **199.167.52.150**. This is the public IP address for ethernet1/1 on this firewall.



Step 9: On the Advanced Options tab, select **Enable NAT traversal**.

Step 10: Under IKEv1, in the **Exchange Mode** list, choose **main**.

Step 11: In the **IKE Crypto Profile** list, choose **NGFW-IKE**.

Step 12: In the **Dead Peer Detection** > **Interval** box, enter **10**.

Step 13: In the **Dead Peer Detection** > **Retry** box, enter **3**.

Step 14: Under IKEv2, in the **IKE Crypto Profile** list, choose **NGFW-IKE**, and then click **OK**.

Step 15: Click **Commit**, and then click **Commit** again.

Step 16: Repeat this procedure for the IKE gateway to the second VM-Series firewall.

8.4 Create an IPSec Tunnel to the AWS VM-Series Firewalls

You now create the IPSec tunnel that runs over the VPN tunnel. You assign one IPSec tunnel to a VPN tunnel.

Step 1: In **Network > IPSec Tunnels**, click **Add**.

Step 2: In the **Name** box, enter VM-Series-a-TUN.

Step 3: In the **Tunnel Interface** list, choose **tunnel.1**.

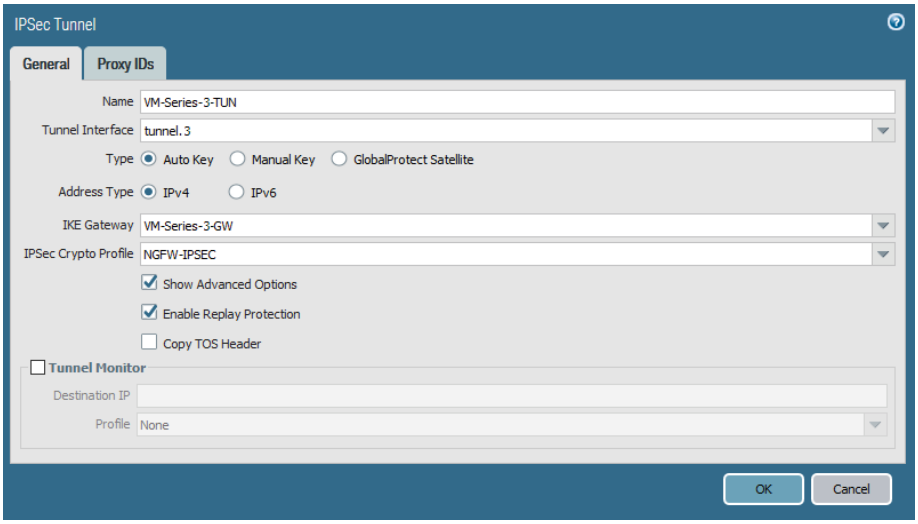
Step 4: In the **IKE Gateway** list, choose VM-Series-a-GW.

Step 5: In the **IPSec Crypto Profile** list, choose NGFW-IPSEC.

Step 6: Select **Show Advanced Options**.

Step 7: Select **Enable Replay Protection**, and then click **OK**.

Step 8: Repeat this procedure for the second IPSec tunnel.



8.5 Configure a Route Redistribution Profile

Next, you create a redistribution profile that redistributes a 10.5.0.0/16 static route in the on-premises VPN firewalls.

Step 1: Log in to the on-premises firewall web interface.

Step 2: Navigate to **Network > Virtual Routers > default**.

Step 3: On the Redistribution Profile tab, in the IPv4 pane, click **Add**.

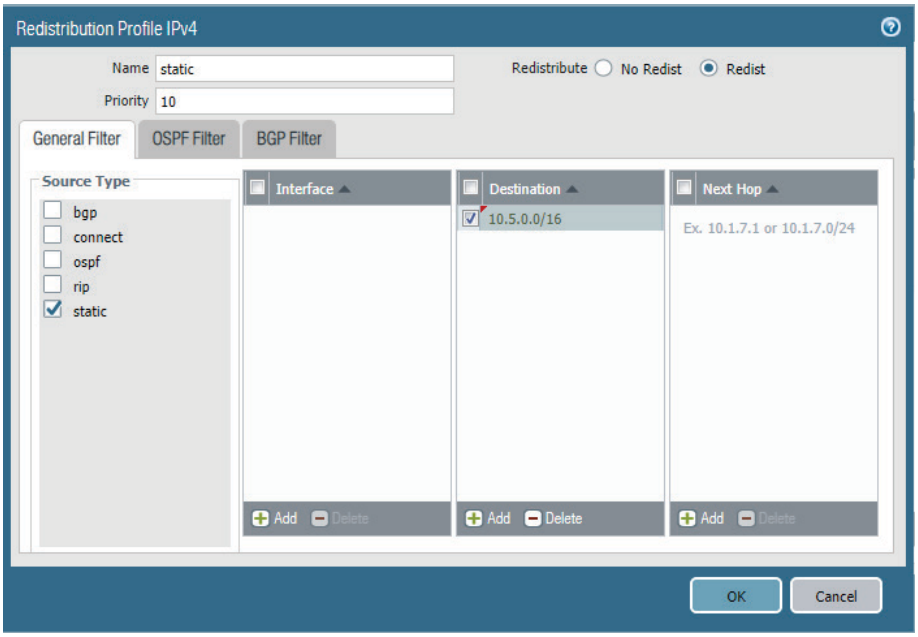
Step 4: In the **Name** box, enter **static**.

Step 5: In the **Priority** box, enter **10**.

Step 6: For **Redistribute**, select **Redist**.

Step 7: For **Source Type**, select **static**.

Step 8: In the **Destination** box, click **Add**, enter **10.5.0.0/16**, and then click **OK**.



8.6 Configure BGP Peering with the AWS VM-Series Firewalls

In this procedure, you deploy peer BGP routing on the on-premises firewalls for connectivity to the AWS VM-Series firewalls. This process assumes you already have configured and enabled the on-premises firewall for BGP.

> **Note**
>
> Ensure that the on-premises firewall does not advertise its public IP address range via BGP to the VM-Series firewalls. If it does advertise the public range, traffic cannot traverse the tunnel, and BGP flaps as the hold timer expires.

First, you build BGP peer groups. The peer IP address is the other available IP address of the local IP address /30 subnet mask range.

Table 20 BGP peer group parameters

Peer group name	Peer name	Peer AS	Interface	Local IP address	Peer IP address
vmseries	vmseries-a	64827	tunnel.1	169.254.0.21/30	169.254.0.22
	vmseries-b	64827	tunnel.2	169.254.1.25/30	169.254.1.26

Step 1: Log in to the on-premises firewall web interface.

Step 2: Navigate to **Network > Virtual Routers > default**.

Step 3: On the BGP tab, at the top of the pane, click **Enable**.

Step 4: In the **Router ID** box, enter 199.167.52.150.

Step 5: In the **AS Number** box, enter 65501.

Step 6: On the General tab, select **Install Route**.

Next, you configure BGP to redistribute connected and static routes.

Step 7: On the Redist Rules tab, click **Add**.

Step 8: In the **Name** list, choose static, and then click **OK**.

Next, you build BGP peer groups to manage peering with the on-premises next-generation firewall.

Step 9: Navigate to **Network > Virtual Routers > default > BGP**, and then on the Peer Group tab, click **Add**.

Step 10: In the **Peer Group Name** box, enter **vmseries**.

Step 11: For **Import Next Hop**, select **Use Peer**.

Step 12: For **Export Next Hop**, select **Use Self**.

Step 13: Clear **Remove Private AS**, and then click **Add**.

Step 14: In the **Name** box, enter **vmseries-a**.

Step 15: In the **Peer AS** box, enter **64827**.

Step 16: Under **Local Address**, in the **Interface** list, choose **tunnel.3**.

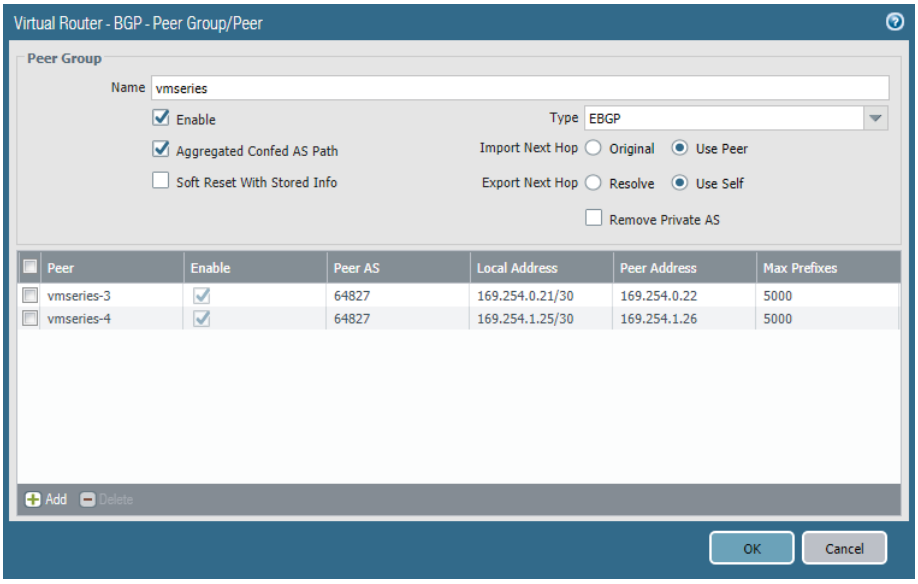
Step 17: In the **IP** list, choose **169.254.0.21/30**.

Step 18: In the **Peer Address** box, enter **169.254.0.22**.

Next, you configure shorter timers to drive a faster convergence in the event of a link or node failure.

Step 19: On the Connections Options tab, in the **Keep Alive Interval** box, enter **10**.

Step 20: In the **Hold Time** box, enter **30**, click **OK**, and then click **OK** again.



Step 21: Repeat this procedure for the **vmseries-b** peer in Table 20.

Step 22: On the **Commit** menu, click **Commit**.

8.7 Configure the NAT and Security Policies

This design assumes that there are no additional NAT or security policies needed on the on-premises firewalls. If they are necessary, follow procedures and policies similar to those in "Configure the Security Policy."

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-000111P-1-20a