Securing Applications in AWS: Centralized Design

DEPLOYMENT GUIDE

APRIL 2021

Table of Contents

Preface 1

Purpose of This Guide 3

- Objectives 3
- Audience 3
- Related Documentation 4

Deployment Overview 5

Design Models 6

- Choosing a Design Model 6
- Centralized Design Model 7
- Isolated Design Model 30

Assumptions and Prerequisites 43

Deploying AWS VPC Infrastructure 44

- Configuring the VPC, Subnets, and Services 44

Deploying Outbound and East-West Security 55

- Configuring the VPC, Subnets, and Services 55
- Configuring Panorama Device Groups, Templates, and Template Stacks 69
- Deploying the VM-Series Instances 85

Deploying Inbound Security 94

- Deploying the Combined Inbound Security Option with a GWLB 94
- Deploying the Centralized Inbound Security Option 104

Deploying Backhaul VPN to On-Premises Services 112

- Configuring VPN Attachments 112
- Configuring an On-Premises Firewall for VPN Connectivity to the Transit Gateway 115

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 10.0.5
- Changed the version of the Cloud Services plugin to version 1.7.0-h3
- Updated the Transit Gateway design to use the Gateway Load Balancer
- Updated the deployment methodology to simplified bootstrapping using user-data
- Updated BYOL to use software firewall credits
- Changed phrasing, terminology, and diagrams for clarity

Purpose of This Guide

This guide provides reference architectures for Palo Alto Networks VM-Series 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 high-availability design.
- Provides deployment details for the Centralized design model, which scales enterprise cloud deployments. This guide describes deploying VM-Series firewalls to provide resilient visibility and protection for the subscriber virtual private cloud's (VPC's) inbound, east-west, and outbound traffic using the AWS transit gateway and Gateway Load Balancer.
- Provides decision criteria for deployment scenarios, as well as procedures for enabling features of 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 for technical readers, including system architects and design engineers, who want to deploy the 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 secure application environments in AWS. The design models in this section offer example architectures that secure inbound and outbound traffic flows, traffic between VPCs, and the connection to your on-premises networks.

All of the design models use a separate management VPC to centralize management 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:

- **Centralized**—Supports connecting large quantities of VPCs, with a scalable solution to secure outbound, inbound, and east-west inter-VPC traffic flows using a transit gateway to connect the VPCs.
- **Isolated**—Supports outbound and inbound traffic flows. This design model does not support east-west traffic flows between VPCs. This design is useful for regional security where one or more isolated VPCs need protection.

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 outbound, inbound, and east-west flows? The Isolated design model provides outbound and inbound security to one or more VPCs but does not provide VPC-to-VPC connectivity or security. The Centralized 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.
- **Segmentation**—Understanding application flows and how to scale and troubleshoot is important to the design. Pieces of the application might need to be segmented from each other for the best security control. Consider the *Centralized design model* for a scalable design when you need to segment pieces of the application into separate VPCs. When an application VPC is self-contained and does not need to communicate with another VPC or on-premises networks, you can apply network security in several ways. In the *Isolated design model*, you centralize the security instances in a dedicated security VPC while providing one or more isolated VPCs security services.

CENTRALIZED DESIGN MODEL

In the Centralized design model, you segment application resources across multiple VPCs that connect in a hub-and-spoke topology. The hub of the topology, or transit gateway, is the central point of connectivity between VPCs and on-premises resources attached through a VPN or AWS Direct Connect.

This model has a dedicated VPC for security services where VM-Series firewalls are deployed for traffic inspection and control. The security VPC does not contain any application resources. The security VPC centralizes resources that multiple workloads can share.

The TGW ensures that all spoke-to-spoke and spoke-to-on-premises traffic transits the VM-series firewalls.

Figure 1 Centralized Design

Transit Gateway Design

In this design, there are two or more spoke VPCs for application resources. For resiliency, you should deploy the resources in the spoke VPCs across availability zones. You can dedicate each VPC to an application, or if you need inspection and control between pieces of an application, each VPC can contain the application resources that share a common level of security control. You use separate VPCs for segmentation because traffic between resources in a VPC always goes directly between resources and cannot be redirected to a firewall.

Because this design uses Panorama to manage the VM-Series firewalls, and because you might have multiple sets of firewalls to manage, deploy Panorama in a VPC dedicated to management. Use another VPC to deploy the VM-Series firewalls. Like with the spoke VPCs, deploy Panorama and the VM-Series firewalls across availability zones for resiliency.

The TGW has VPC attachments in the availability zones of each spoke VPC, the management VPC, and the security VPC.

TGW route tables behave like route domains. You can create isolated networks, allowing you to steer and control traffic flow between VPCs and on-premises connections by deploying multiple route tables on the TGW and associating the attachments to them. This design uses two TGW route tables: security and spokes.

You set which TGW route table an attachment uses by associating the attachment to a route table. An attachment can only be associated with one TGW route table. Each TGW route table can associate with multiple attachments. Associate the VPN attachment for the on-premises networks, as well as the VPC attachments for the spokes and management VPCs, to the spokes route table. Associate the VPC attachment for the security VPC to the security route table.

Figure 2 Attachments and associations

The spokes route table on the TGW has the security VPC routes propagated to it and a static default route pointing to the security VPC. The spokes route table does not have more specific routes to other VPCs or on-premises networks to ensure that spoke-to-spoke communication can occur only through the VM-Series firewalls in the security VPC.

The security route table on the TGW allows the VM-Series firewalls to reach all VPCs and on-premises networks. Propagate routes from every attachment to the security route table. You can use static routes in the TGW route table for on-premises connections, or you can propagate routes over BGP from a VPN attachment into a TGW route table. Routes propagated with BGP support ECMP.

Figure 3 TGW Route Tables

Security VPC

This design deploys a VPC dedicated to security. In the security VPC, you deploy the VM-Series firewalls in separate availability zones and deploy a GWLB to distribute traffic to the firewalls.

When deploying the security VPC, configure it with a non-overlapping IP address block that is appropriately sized for your organization's needs. For resiliency, use multiple availability zones and consider breaking your subnet ranges into availability zone-based blocks that you can summarize in security groups and routing tables.

Figure 4 VPC availability zone-based IP blocks

To supply inbound and outbound internet access, you must deploy an IGW into the VPC. The IGW performs network address translation of the management interface's private IP address to its associated public IP address and allows outbound traffic from the firewall to reach the internet.

VM-Series Firewalls

Deploy two or more VM-Series firewalls in separate availability zones.

Although the VM-Series firewall supports multiple interface deployment configurations such as virtual wire, Layer 2, and tap mode, VM-Series firewall interfaces on AWS are always Layer 3 interfaces because of AWS networking requirements. In AWS, you should always configure VM-Series firewall interfaces to obtain their IP address through DHCP.

Because this design model uses overlay routing, the VM-Series firewall requires three Ethernet interfaces: a management interface, a private dataplane interface for traffic from the GWLB, and a public dataplane interface for outbound traffic.

When you deploy a VM-Series instance from the AWS Marketplace, it has a single interface by default. You have to create the additional interfaces and associate them with the VM-Series instance. You also need to create two Elastic IP addresses. Assign one to the management interface so you can manage the firewall and the other to the public interface so the VM-Series firewall can support outbound traffic flows.

Although the dataplane interfaces both get their IP addresses from DHCP, only the public interface should accept the default route.

Attach each firewall interface to separate subnets. The management and public subnets have separate route tables as follows:

- The management route table has all 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 all the public subnets assigned to it and a default route to the IGW for internet access.

You do not need to modify the default routing of the subnets dedicated to the private dataplane interface. However, you should configure a security group on the firewall's private dataplane interface that allows health checks and UDP traffic destined to port 6081 from all the GWLB subnets. The security group should deny all other traffic.

The private dataplane interface should have at least one subinterface. The GWLB endpoints should map to subinterfaces instead of the dataplane interface. Mapping all endpoints to a subinterface allows you to have a restrictive security policy on the dataplane interface that allows health checks only from the GWLB subnets. This security policy provides a layer of protection if an endpoint is misconfigured or newly added to the GWLB.

Note

Although the firewall does not use the subinterfaces for traffic forwarding, you must configure them to receive a DHCP address and to have a unique VLAN number. AWS does not assign the subinterface an IP address, which is expected and does not affect traffic forwarding with a GWLB.

Figure 5 VM-Series firewall interfaces and AWS route tables

You must also enable Geneve parsing and overlay routing on the firewall.

> **Note**
>
> If you don't enable Geneve parsing, the firewall sees traffic destined to the dataplane interface IP address with a destination port of 6081. With parsing enabled, the firewall is able to look inside the encapsulation to the actual traffic.

You can automate the VM-Series configuration management by using Panorama in the management VPC to provide a secure, scalable, and automated architecture. Bootstrapping speeds up the process of configuring and licensing the firewall and making it operational on the network. This process allows the deployment of the firewall with only a basic configuration so that it can connect to Panorama and obtain the complete working configuration.

Although you can enable Geneve parsing and map the GWLB endpoints to subinterfaces after deployment, it must be done directly on the firewall and cannot be configured in Panorama. Because a manual per-device configuration can be challenging as you scale out devices, you should configure Geneve parsing and overlay routing during bootstrap instead.

GWLB

A GWLB in the security VPC transparently distributes traffic across the VM-Series firewalls. You should deploy the GWLB in all of the security VPC's availability zones, with a single endpoint service.

The GWLB targets the VM-Series firewalls instances and uses HTTPS health checks to monitor their availability.

TGW Attachment

The security VPC attaches to the TGW through a VPC attachment. The VPC attachments terminate into the security VPC in dedicated subnets, one per availability zone.

Enable appliance mode on the attachments in the security VPC in order to ensure that traffic routes through the same attachment zone even when the source and destination of the traffic are in different zones. If appliance mode is not enabled, it is possible to have asymmetric traffic flowing through different firewalls, which the firewalls drop.

Outbound Traffic

This design uses overlay routing for outbound security on the VM-Series firewalls. Outbound traffic from instances in the spoke VPCs traverses the TGW and egresses the AWS environment through the VM-Series firewalls.

Default routes in the spoke VPCs direct outbound traffic to the TGW. To direct traffic to the security VPC, the TGW uses the spokes route table and the static default route pointing to the security VPC.

To support outbound traffic flows, the security VPC has GWLB endpoints in each of the availability zones in which the firewalls are deployed. The GWLB endpoints are associated with dedicated subnets, which allows them to have a unique routing table. The route tables in the security VPC for outbound traffic are as follows:

- A routing table for each of the TGW attachment subnets directs all traffic from the TGW to the GWLB endpoint in the attachment's availability zone.
- A routing table the GWLB endpoint subnets directs return traffic to the spoke VPCs address space to the TGW. In most cases, routes to the RFC 1918 address space is the simplest method for a configuration that does not need to be modified as you add spoke VPCs to the TGW.

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

Figure 6 GWLB and route table details

On the VM-Series firewalls, map the GWLB endpoints to a subinterface on the private dataplane interface. The subinterface must have a unique zone and VLAN number. The zone is used in policy, and the VLAN number is not used in traffic forwarding.

The firewall also has routes to the spoke VPC address space—or for simplicity, routes to all the RFC 1918 address space—that point to the private dataplane interface's default gateway.

Figure 7 Firewall endpoint mapping and routing

Outbound Traffic Flow

1. In the application VPC, the instance in the application VPC sends traffic to a service on the internet. The route table applied to the instance's subnet directs traffic to the TGW attachment in its availability zone.
2. On the TGW, the application VPC is associated with the spokes route table. The TGW uses the static route in the that route table to forward the traffic to the security VPC.
3. In the security VPC, the route table applied to the subnet that contains the TGW attachment has a default route that forwards traffic to the GWLB endpoint in the attachment's availability zone.
4. In the security VPC, the GWLB endpoint forwards the traffic to the GWLB which chooses a VM-Series firewall from its target group. Because cross-zone load balancing is enabled, it could be any available firewall.
5. The firewall receives the traffic from the GWLB and associates it with the private zone, which is configured on the subinterface that is mapped to the GWLB endpoints in the security VPC.
6. The firewall applies the decryption, NAT, and security policies before forwarding it out its public dataplane interface based on the default route learned from DHCP on that interface. The outbound traffic's source IP address is translated to the IP address of the firewall's public interface.
7. In the security VPC, the route table applied to the subnet that contains the firewall's public interface has a default route that forwards traffic to the IGW. The IGW translates the source IP address of the outbound traffic to the EIP associated with the firewall's public interface and forwards the traffic to the internet.

Figure 8 Outbound traffic flow

Return Traffic Flow

1. In the security VPC, the IGW translates the destination IP address of the return traffic to the firewall's public interface's IP address.
2. The firewall receives the traffic and associates the return traffic with an active session on the firewall. The firewall's route table directs the traffic destined to the application VPC out the private interface. Because this is the same interface that received the traffic from the GWLB, the firewall uses the session information, including the TLVs associated with the Geneve encapsulation, to return the traffic to the GWLB.
3. In the security VPC, the GWLB uses the session information to forward the traffic to the GWLB endpoint that received the original traffic.
4. In the security VPC. The route table associated with the subnet that contains the GWLB endpoint has a route that forwards traffic destined to the application VPCs address space to the TGW attachment in its availability zone.
5. On the TGW, the security VPC is associated with the security route table. The TGW uses that route table to forward traffic to the application VPC.
6. In the application VPC, the TGW attachment forwards the traffic to the instance.

Figure 9 Outbound return traffic flow

Security Policy

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 security policy allows appropriate application traffic from private instances to the internet. Using the zones of the private subinterface and the public dataplane interface to define the policy. You should implement the outbound security policy by using positive security policies (*allow-listing*). Security profiles prevent known malware and vulnerabilities from entering the network in return traffic allowed by the security policy. URL filtering, data loss prevention, file blocking, and data filtering protect against data exfiltration.

Inbound Traffic

Inbound traffic originates outside the VPC and is destined to applications or services hosted within your VPCs, such as web servers. You have two options for implementing inbound security resiliency:

- **Combined**—You can use the VM-Series and GWLB in the security VPC, with distributed GWLB endpoints in the application VPCs. Unlike with outbound traffic, this design option does not use the transit gateway for traffic forwarding between the security VPC and the application VPCs.
- **Centralized**—You can use an AWS load-balancer sandwich design. This design uses a resilient, public-facing load balancer in the security VPC and a second resilient load balancer on the private side of the firewalls in the application VPCs. This design option uses the transit gateway for traffic forwarding between the security VPC and application VPCs.

> **Note**
>
> The combined option uses the GWLB to apply security for inbound traffic transparently and does not require address translation. The centralized option does not use the GWLB and requires that the firewall translate the traffic source IP address to ensure traffic returns to the correct firewall in the security VPC.

Combined Option

This design option adds distributed inbound security to the existing VM-Series firewalls in the security VPC and builds upon the previously discussed configuration in order to support outbound traffic flows. If you have regulatory or other compliance concerns, a separate set of firewalls dedicated to inbound traffic flows might be more appropriate.

This design uses the GWLB and VM-Series firewalls in the security VPC, with GWLB endpoints in the application VPCs for the transparent inspection of inbound traffic.

To support inbound security with this design option, modify each application VPC that requires inbound security as follows:

- To supply inbound access, deploy an IGW to the application VPC.
- Add GWLB endpoints in each of the availability zones and associate them with the GWLB in the security VPC.
- Add a gateway route table that directs traffic to the subnets in an availability zone to the GWLB endpoint in that availability zone.
- Add an internet-facing load balancer with the application instances in the VPC as the targets.
- Add a route table for the GWLB endpoint subnets. The route table must direct traffic that is destined to the internet to the IGW.
- Add a route table for each of the subnets that contain the load balancer. The route tables must direct traffic that is destined to the internet to the GWLB endpoint in its availability zone.

Figure 10 Combined inbound security—application VPC

To support inbound security with this design option, modify the security VPC as follows:

- Add a subinterface on the private dataplane interface for each application VPC.
- Map all GWLB endpoints in the application's VPC to the subinterface.

> **Note**
>
> Because inbound traffic flows with the combined design option are intra-zone, you should modify the default intra-zone policy to block traffic.

In this design, the VM-Series firewalls inspect and transparently secure traffic before the internet-facing load balancer receives it. Because this design option uses GWLB for resiliency, the firewalls do not modify the traffic source or destination IP address.

Because the firewall is in the first device in the traffic path, if you want to filter traffic before the firewall receives it, you must use a network ACL on the GWLB endpoint subnets. If you are using an ALB, the firewall decrypts and re-encrypts the traffic before the ALB sees it.

The design option supports one or more application VPCs. Each application VPC that requires inbound security requires an IGW and GWLB endpoints. The VM-Series firewalls in the security VPC inspect and secure the traffic, relying on the AWS PrivateLink connection between the GWLB endpoint and the GWLB to transmit traffic between the application VPC and the security VPC.

The VM-Series firewall security policy allows application traffic to the internet-facing load balancer. VM-Series firewall security profiles prevent known malware and vulnerabilities from entering the network in traffic allowed by the security policy.

Inbound Traffic Flow

1. The URL request from the end-user is directed toward **example.lb.aws.com**. This request is sent to a DNS. DNS returns an IP address for each of the load balancer's enabled availability zones. The client OS picks an IP address and sends the traffic. In the application VPC, the IGW translates the destination public IP address to the IP address of the load balancer.

2. In the application VPC, the gateway route table associated with the IGW directs the traffic to the GWLB endpoint in the destination's availability zone. The GWLB endpoint forwards the traffic to the GWLB in the security VPC.

3. In the security VPC, the GWLB chooses a VM-Series firewall from its target group. Because cross-zone load balancing is enabled, it could be any available firewall.

4. The firewall receives the traffic from the GWLB on its private dataplane interface and associates it with the application's zone, which is configured on the subinterface that is mapped to the GWLB endpoints in the application's VPC.

5. The firewall's route table directs the traffic destined to the application VPC out the private interface. The firewall applies security policies before forwarding. The security policy is an intra-zone policy. Because this is the same interface that received the traffic from the GWLB, the firewall uses the session information, including the TLVs associated with the Geneve encapsulation, to return the traffic to the GWLB.

6. In the security VPC, the GWLB uses the session information to forward the traffic to the GWLB endpoint that received the original traffic.

7. In the application VPC, the GWLB endpoint forwards the traffic to the internet-facing load balancer.

8. In the application VPC, the internet-facing load balancer receives the traffic and picks a target from the target group. The targets are the application instances. The load balancer translates the packet's destination address to the selected instance interface IP address and translates the source IP address to the private IP address of the load balancer so that traffic returns to it on the return flow.

Figure 11 Combined inbound security—inbound traffic flow

Return Traffic Flow

1. In the application VPC, the instance sends return traffic to the load-balancer.
2. In the application VPC, the load balancer modifies the source and destination IP addresses. The route table applied to the subnet that contains the load balancer has a default route that forwards traffic to the GWLB endpoint in its availability zone.
3. The GWLB endpoint forwards the traffic to the GWLB in the security VPC.
4. In the security VPC, the GWLB chooses the same VM-Series firewall from its target group that was used for the inbound traffic flow.
5. The firewall receives the traffic from the GWLB on its private dataplane interface. The firewall receives the traffic and associates the return traffic to an active session on the firewall. The firewall uses the session information, including the TLVs associated with the Geneve encapsulation to return the traffic to the GWLB.
6. In the security VPC, the GWLB uses the session information to forward the traffic to the GWLB endpoint that received the original traffic.
7. In the application VPC, the GWLB endpoint forwards the traffic to the IGW.
8. The IGW translates the source IP address of the outbound traffic to the EIP associated with the load balancer and forwards the traffic to the internet.

Figure 12 Combined inbound security—return traffic

Centralized Option

This design option adds centralized inbound security to the existing VM-Series firewalls in the security VPC and builds upon the previously discussed configuration to support outbound traffic flows. A separate set of firewalls dedicated to inbound traffic flows might be more appropriate if you have regulatory or other compliance concerns. This design option does not use the GWLB for inbound traffic. Instead, it relies on a public ALB/NLB for resiliency and NAT to ensure traffic returns to the correct firewall.

To support centralized inbound security, modify the security VPC as follows:

- Add an internet-facing application or network load balancer.
- Add a route table for the subnets that contain firewall private interfaces. The route table must direct traffic that is destined to the spoke VPCs address space to the TGW. In most cases, routes to the RFC 1918 address space are the most straightforward method for a configuration, because you should not need to modify it as you add spoke VPCs to the TGW.
- Modify the security group on the firewall's private dataplane interface. Adjust the security group to allow return traffic from the application VPCs and health checks from the GWLB subnets. Use an ACL to deny UDP traffic on port 6081 from any network other than the GWLB subnets in the VPC.

Figure 13 Centralized inbound security—ALB and route tables

For inbound traffic, the Application Load Balancer terminates incoming connections to its listener and initiates corresponding new connections to the VM-Series firewalls in the target group. The ALB is associated with the availability zones that contain VM-Series firewalls. If you configure the ALB for multiple web applications behind the same VM-Series firewalls, you must define unique target groups for each application. Each target group contains the same VM-Series firewalls 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 back-end availability on all specified HTTP and HTTPS ports.

Destination IP address translation rules on the VM-Series firewalls map incoming traffic from the ALB listener 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. 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 back ends on ports other than 80 or 443, you should configure the security policy rules' services to include the specific service ports in use instead of *application-default*.

Traffic routing services such as domain name servers and firewall next-hop configurations use FQDN to resolve load-balancer IP addresses versus hard-coded IP addresses. Using FQDN allows the load balancers to be dynamic and scale up or down in size and remain resilient; one availability zone might go down, and the other can continue feeding sessions to the application instances.

Inbound Traffic Flow

1. The URL request from the end-user is directed toward example.lb.aws.com. This request is sent to a DNS. DNS returns an IP address for each of the load balancer's enabled availability zones. The client OS picks an IP address and sends the traffic. The IGW translates the destination public IP address to the IP address of the load balancer.

2. In the security VPC, the internet-facing load balancer receives the traffic and picks a target from the target group. The targets are the private IP addresses for the public-facing interface on each of the VM-Series firewalls. The load balancer translates the packet's destination address to the selected VM-Series firewall's public interface IP address and translates the source IP address to the private IP address of the load balancer so that traffic returns to it on the return flow.

3. The firewall translates the IP addresses on the incoming traffic. The firewall changes the source IP address to the IP address of the firewall's private interface so that the return traffic from the instance travels back through the same firewall in order to maintain state and translation tables. The firewall changes the destination IP address to the IP address of the internal load balancer. The firewall learns the IP addresses for the internal load balancer by sending a DNS request for the FQDN assigned to the load balancers. This returns multiple IP addresses, one for each of the subnets or availability zones into which you deployed the load balancer.

4. The firewall's route table directs the traffic destined to the application VPC out the private interface.
5. In the security VPC, the route table applied to the subnet that contains the firewall's private interface has a route that forwards traffic destined to the application VPCs address space to the TGW attachment in its availability zone.
6. On the TGW, the security VPC is associated with the security route table. The TGW uses that route table to forward traffic to the application VPC.
7. In the application VPC, the TGW attachment forwards the traffic to the internal load balancer.
8. The internal load balancers have instances in both availability zones and do a round-robin load balancing to the active instances in the target list, translating the source IP address to its IP address.

Figure 14 Centralized inbound security—inbound traffic flow

Return Traffic Flow

1. In the application VPC, the instance in the application VPC sends return traffic to the load balancer.
2. In the application VPC, the load balancer sends the return traffic to the firewall. The route table applied to the load balancer's subnet directs the traffic to the TGW attachment in its availability zone.
3. On the TGW, the application VPC is associated with the spokes route table. The TGW uses the static route in the route table to forward the traffic to the security VPC.
4. In the security VPC, the route table applied to the subnet that contains the TGW attachment uses local routing to direct traffic to the VM-Series firewall interface.
5. The firewall receives the traffic and associates the return traffic to an active session on the firewall. The firewall translates the source IP address to the firewall's public interface and destination IP address to the IP address of the internet-facing load balancer.
6. In the security VPC, the route table applied to the subnet that contains the load balancer has a default route that forwards traffic to the IGW.
7. The IGW translates the source IP address of the outbound traffic to the EIP associated with the load balancer and forwards the traffic to the internet.

Figure 15 Centralized inbound security—return traffic flow

Health checks ensure that each path is operational and that instances are operational. The checks also monitor the return path is operational as the public load balancer probes through the firewall to the internal load balancer. The internal load balancers probe the instances in their target group to make sure they are operational.

East-West Traffic

East-west traffic, or traffic between VPCs, flows through the VM-Series firewalls in the security VPC. This traffic follows the same path as outbound traffic and does not require additional configuration in the AWS VPCs beyond what is required for outbound traffic flows.

As with the outbound traffic, you use VM-Series firewall security policies to limit what applications and resources the instances in each VPC can reach. To differentiate east-west traffic flows from outbound traffic flows on the VM-Series firewall, use zone information. Outbound traffic flows are inter-zone flows using the zones applied to the private subinterface and the public dataplane interface. East-west traffic flows are intra-zone flows and use only the zone applied to the private subinterface.

Note

Because the east-west traffic flows are intra-zone, you should modify the default intra-zone policy to block traffic.

East-West Traffic Flow

1. In the first application VPC, an instance sends traffic to an instance in the second application VPC. The route table applied to the instance's subnet directs the traffic to the TGW attachment in its availability zone.
2. On the TGW, the application VPCs are associated with the spokes route table. The TGW uses the static route in the route table to forward the traffic to the security VPC.
3. In the security VPC, the route table applied to the subnet that contains the TGW attachment has a default route that forwards traffic to the GWLB endpoint in the attachment's availability zone.
4. In the security VPC, the GWLB endpoint forwards the traffic to the GWLB, which chooses a VM-Series firewall from its target group. Because cross-zone load balancing is enabled, it could be any available firewall.
5. The firewall receives the traffic from the GWLB and associates it with the private zone, which is configured on the subinterface that is mapped to the GWLB endpoints in the security VPC.
6. The firewall applies security policies before forwarding it out its private dataplane interface. The firewall's route table directs the traffic destined to the application VPCs out of the private interface. Because this is the same interface that received the traffic from the GWLB, the firewall uses the session information, including the TLVs associated with the Geneve encapsulation to return the traffic to the GWLB.

7. In the security VPC, the GWLB uses the session information to forward the traffic to the GWLB endpoint that received the original traffic.
8. In the security VPC, the route table associated with the subnet that contains the GWLB endpoint has a route that forwards traffic destined for the second application VPC's address space to the TGW attachment in its availability zone.
9. On the TGW, the security VPC is associated with the security route table. The TGW uses that route table to forward traffic to the second application VPC.
10. In the second application VPC, the TGW attachment forwards the traffic to the instance.

Figure 16 East-west traffic flow

Return Traffic Flow

1. In the second application VPC, an instance sends return traffic to an instance in the first application VPC. The route table applied to the instance's subnet directs the traffic to the TGW attachment in its availability zone.
2. On the TGW, the application VPCs are associated with the spokes route table. The TGW uses the static route in the route table to forward the traffic to the security VPC.
3. In the security VPC, the route table applied to the subnet that contains the TGW attachment has a default route that forwards traffic to the GWLB endpoint in the attachment's availability zone.
4. In the security VPC, the GWLB endpoint forwards the traffic to the GWLB, which chooses the same VM-Series firewall from its target group..

5. The firewall receives the traffic from the GWLB and associates it with the private zone, which is configured on the subinterface that is mapped to the GWLB endpoints in the security VPC.
6. The firewall receives the traffic and associates the return traffic to an active session on the firewall. The firewall's route table directs the traffic destined to the application VPCs out of the private interface. Because this is the same interface that received the traffic from the GWLB, the firewall uses the session information, including the TLVs associated with the Geneve encapsulation, to return the traffic to the GWLB.
7. In the security VPC, the GWLB uses the session information to forward the traffic to the GWLB endpoint that received the original traffic.
8. In the security VPC. The route table associated with the subnet that contains the GWLB endpoint has a route that forwards traffic destined to the first application VPCs address space to the TGW attachment in its availability zone.
9. On the TGW, the security VPC is associated with the security route table. The TGW uses that route table to forward traffic to the second application VPC.
10. In the first application VPC, the TGW attachment forwards the traffic to the instance.

Figure 17 East-west return traffic flow

Backhaul to On-Premises Networks

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 18 Backhaul with Direct Connect gateway

Figure 42 shows VPN connectivity from on-premises gateways to the TGW via a VPN attachment. There is a VPN attachment for each CGW, and each attachment is made of two tunnels.

Figure 19 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 management VPC to the firewalls via the Transit gateway.

ISOLATED DESIGN MODEL

The Isolated Design model centralizes the security instances in a dedicated security VPC, while providing one or more isolated VPCs inbound and outbound security services.

Figure 20 Isolated Design

Security VPC

This design deploys a VPC dedicated to security. In the security VPC, you deploy the VM-Series firewalls in separate availability zones and deploy a GWLB to distribute traffic to the firewalls.

When deploying the security VPC, configure it with a non-overlapping IP address block that is appropriately sized for your organization's needs. For resiliency, use multiple availability zones and consider breaking your subnet ranges into availability zone-based blocks that you can summarize in security groups and routing tables.

Figure 21 VPC availability zone-based IP blocks

To supply outbound internet access, you must deploy an IGW into the VPC. The IGW performs network address translation of the management interface's private IP address to its associated public IP address and allows outbound traffic from the firewall to reach the internet.

VM-Series Firewalls

Deploy two or more VM-Series firewalls in separate availability zones.

Although the VM-Series firewall supports multiple interface deployment configurations such as virtual wire, Layer 2, and tap mode, VM-Series firewall interfaces on AWS are always Layer 3 interfaces because of AWS networking requirements. In AWS, you should always configure VM-Series firewall interfaces to obtain their IP address through DHCP.

Because this design model uses overlay routing, the VM-Series firewall requires three Ethernet interfaces: a management interface, a private dataplane interface for traffic from the GWLB, and a public dataplane interface for outbound traffic.

When you deploy a VM-Series instance from the AWS Marketplace, it has a single interface by default. You have to create the additional interfaces and associate them with the VM-Series instance. You also need to create two Elastic IP addresses. Assign one to the management interface so you can manage the firewall and the other to the public interface so the VM-Series firewall can support outbound traffic flows.

Although the dataplane interfaces both get their IP addresses from DHCP, only the public interface should accept the default route.

Attach each firewall interface to separate subnets. The management and public subnets have separate route tables, as follows:

- The management route table has all management subnets assigned to it, a default route to the IGW for internet access, and a route to the VPC peering connection for access to Panorama.
- The public route table has all public subnets assigned to it and a default route to the IGW for internet access.

You do not need to modify the default routing of the subnets dedicated to the private dataplane interface. However, you should configure a security group on the firewall's private dataplane interface that allows health checks and UDP traffic destined to port 6081 from all the GWLB subnets. The security group should deny all other traffic.

The private dataplane interface should have at least one subinterface. The GWLB endpoints should map to subinterfaces instead of the dataplane interface. Mapping all endpoints to a subinterface allows you to have a restrictive security policy on the dataplane interface that allows health checks only from the GWLB subnets. This security policy provides a layer of protection if an endpoint is misconfigured or newly added to the GWLB.

Note

Although the firewall does not use the subinterfaces for traffic forwarding, you must configure them to receive a DHCP address and to have a unique VLAN number. AWS does not assign the subinterface an IP address, which is expected and does not affect traffic forwarding with a GWLB.

Figure 22 VM-Series firewall interfaces and AWS route tables

You must also enable Geneve parsing and overlay routing on the firewall.

> **Note**
>
> If you don't enable Geneve parsing, the firewall sees traffic destined to the dataplane interface IP address with a destination port of 6081. With parsing enabled, the firewall is able to look inside the encapsulation to the actual traffic.

You can automate the VM-Series configuration management by using Panorama in the management VPC to provide a secure, scalable, and automated architecture. Bootstrapping speeds up the process of configuring and licensing the firewall and making it operational on the network. This process allows deployment of the firewall with only a basic configuration so that it can connect to Panorama and obtain the complete operational configuration.

While you can enable Geneve parsing and map the GWLB endpoints to subinterfaces after deployment it must be done directly on the firewall and cannot be configured in Panorama. Because a manual per-device configuration can be challenging as you scale out devices, you should configure Geneve parsing and overlay routing during bootstrap instead.

GWLB

A GWLB in the security VPC transparently distributes traffic across the VM-Series firewalls. The GWLB should be deployed in all the security VPC's availability zones, with a single endpoint service.

The GWLB targets the VM-Series firewalls instances and uses HTTPS heath checks to monitor their availability.

Outbound Traffic

This design uses overlay routing for outbound security on the VM-Series firewalls. Outbound traffic from instances in the isolated VPCs uses the PrivateLink connections from GWLB endpoints in the applications VPCs to the GWLB in the security VPC to egress the AWS environment through the VM-Series firewalls.

To support outbound traffic flows, in each of the isolated application VPCs, deploy GWLB endpoints in each of the availability zones that the instances are deployed into. The GWLB endpoints are associated with dedicated subnets, which allows them to have a unique routing table.

A routing table for each of the instance subnets direct all outbound traffic to the GWLB endpoint in the instance's availability zone. You do not need to modify the default routing of the subnets dedicated to the GWLB. By default, they can reach all the IP addresses within the isolated application VPC.

Figure 23 Outbound network and route table details

On the VM-Series firewalls in the security VPC, create a subinterface on the private dataplane interface for each isolated application VPC. Map the GWLB endpoints in the VPC to its subinterface. The subinterface must have a unique zone and VLAN number. The zone is used in policy, and VLAN number is not used in traffic forwarding.

The firewall also has routes to the isolated application VPC address space—or for simplicity, routes to all the RFC 1918 address space—that point to the private dataplane interface's default gateway.

Figure 24 Firewall endpoint mapping and routing

Outbound Traffic Flow

1. In the application VPC, the instance in the application VPC sends traffic to a service on the internet. The route table applied to the instance's subnet forwards traffic to the GWLB endpoint in its availability zone.
2. In the application VPC, the GWLB endpoint forwards the traffic over PrivateLink to the GWLB in the security VPC.
3. In the security VPC, the GWLB chooses a VM-Series firewall from its target group. Because cross-zone load balancing is enabled, it could be any available firewall.
4. The firewall receives the traffic from the GWLB and associates it with the application VPC's zone, which is configured on the subinterface that is mapped to the GWLB endpoints in the application's VPC.
5. The firewall applies the Decryption, NAT, and Security policies before forwarding it out its public dataplane interface based on the default route learned from DHCP on that interface. The outbound traffic's source IP address is translated to the firewall's public interface's IP address.
6. In the security VPC, the route table applied to the subnet that contains the firewall's public interface has a default route that forwards traffic to the IGW. The IGW translates the source IP address of the outbound traffic to the EIP associated with the firewall's public interface and forwards the traffic to the internet.

Figure 25 Outbound traffic flow

Return Traffic Flow

1. In the security VPC, the IGW translates the destination IP address of the return traffic to the firewall's public interface's IP address.
2. The firewall receives the traffic and associates the return traffic with an active session on the firewall. The firewall's route table directs the traffic destined to the application VPC out the private interface. Because this is the same interface that received the traffic from the GWLB, the firewall uses the session information, including the TLVs associated with the Geneve encapsulation, to return the traffic to the GWLB.
3. In the security VPC, the GWLB uses the session information to forward the traffic to the GWLB endpoint that received the original traffic in the application VPC.
4. In the application VPC, the GWLB endpoint forwards the traffic to the instance.

Figure 26 Return traffic flow

Security Policy

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 security policy allows appropriate application traffic from private instances to the internet. Using the zones of the private subinterface and the public dataplane interface to define the policy. You should implement the outbound security policy by using positive security policies (*allow listing*). Security profiles prevent known malware and vulnerabilities from entering the network in return traffic allowed by the security policy. URL filtering, Data Loss Prevention, file blocking, and data filtering protect against data exfiltration.

Inbound Traffic

Inbound traffic originates outside the VPC and is destined to applications or services hosted within your VPCs, such as web servers. This design uses the GWLB and VM-Series firewalls in the security VPC, with GWLB endpoints in the application VPCs for the transparent inspection of inbound traffic.

This design uses the existing VM-Series firewalls in the security VPC and builds upon the previously discussed configuration to support outbound traffic flows. A separate set of firewalls dedicated to inbound traffic flows might be more appropriate if you have regulatory or other compliance concerns.

To support inbound security with this design option, modify each application VPC that requires inbound security as follows:

- To supply inbound access, deploy an IGW to the application VPC.
- Add a gateway route table that directs traffic to the subnets in an availability zone to the GWLB endpoint in that availability zone.
- Add an internet-facing load balancer with the application instances in the VPC as the targets. Individual instances with associated EIPs are also supported.
- Add a route table for the GWLB endpoint subnets. The route table must direct traffic that is destined to the internet to the IGW.
- Add a route table for each of the subnets that contain the load balancer. The route tables must direct traffic that is destined to the internet to the GWLB endpoint in its availability zone.

Note

Because the east-west traffic flows are intra-zone, you should modify the default intra-zone policy to block traffic.

Figure 27 Isolated inbound security—application VPC

In this design, the VM-Series firewalls inspect and transparently secure traffic before the internet-facing load balancer receives it. Because this design option uses GWLB for resiliency, the firewalls do not modify the traffic source or destination IP address.

Because the firewall is in the first device in the traffic path, if you want to filter traffic before the firewall receives it, you must use a network ACL on the GWLB endpoint subnets. If you are using an ALB, the firewall decrypts and re-encrypts the traffic before the ALB sees it.

The design option supports one or more application VPCs. Each application VPC that requires inbound security requires and IGW, and GWLB endpoints. The VM-Series firewalls in the security VPC inspect and secure the traffic, relying on the AWS PrivateLink connection between the GWLB endpoint and the GWLB to transmit traffic between the application VPC and the security VPC.

The VM-Series firewall security policy allows application traffic to the internet-facing load balancer, and VM-Series firewall security profiles prevent known malware and vulnerabilities from entering the network in traffic allowed by the security policy.

Inbound Traffic Flow

1. The URL request from the end-user is directed toward example.lb.aws.com. This request is sent to a DNS. DNS returns an IP address for each of the load balancer's enabled availability zones. The client OS picks an IP address and sends the traffic. In the application VPC, the IGW translates the destination public IP address to the IP address of the load balancer.

2. In the application VPC, the gateway route table associated with the IGW, directs the traffic to the GWLB endpoint in the destination's availability zone. The GWLB endpoint forwards the traffic to the GWLB in the security VPC.

3. In the security VPC, the GWLB chooses a VM-Series firewall from its target group. Because cross-zone load balancing is enabled it could be any available firewall.

4. The firewall receives the traffic from the GWLB on its private dataplane interface and associates it with the application's zone, which is configured on the subinterface that is mapped to the GWLB endpoints in the application's VPC.

5. The firewall's route table directs the traffic destined to the application VPC out the private interface. The firewall applies security policies before forwarding. The security policy is an intra-zone policy. Because this is the same interface that received the traffic from the GWLB, the firewall uses the session information, including the TLVs associated with the Geneve encapsulation, to return the traffic to the GWLB.

6. In the security VPC, the GWLB uses the session information to forward the traffic to the GWLB endpoint that received the original traffic.

7. In the application VPC, the GWLB endpoint forwards the traffic to the internet-facing load balancer.

8. In the application VPC, the internet-facing load balancer receives the traffic and picks a target from the target group. The targets are the application instances. The load balancer translates the packet's destination address to the selected instance interface IP address and translates the source IP address to the private IP address of the load balancer so that traffic returns to it on the return flow.

Figure 28 Inbound traffic flow

Return Traffic Flow

1. In the application VPC, the instance sends return traffic to the load-balancer.
2. In the application VPC, the load balancer modifies the source and destination IP addresses. The route table applied to the subnet that contains the load balancer has a default route that forwards traffic to the GWLB endpoint in its availability zone.
3. The GWLB endpoint forwards the traffic to the GWLB in the security VPC.
4. In the security VPC, the GWLB chooses the same VM-Series firewall from its target group that was used for the inbound traffic flow.
5. The firewall receives the traffic from the GWLB on its private dataplane interface. The firewall receives the traffic and associates the return traffic to an active session on the firewall.
   The firewall uses the session information, including the TLVs associated with the Geneve encapsulation to return the traffic to the GWLB.
6. In the security VPC, the GWLB uses the session information to forward the traffic to the GWLB endpoint that received the original traffic.
7. In the application VPC, the GWLB endpoint forwards the traffic to the IGW.
8. The IGW translates the source IP address of the outbound traffic to the EIP associated with the load balancer and forwards the traffic to the internet.

Figure 29 Return traffic

East-West Traffic

VPC networking provides direct reachability between all instances within a VPC, regardless of IP address and subnet allocation. All instances within a VPC can reach any other instance within the same VPC, regardless of AWS route tables. You can use AWS security groups and ACLs to permit or deny traffic into or out of an instance or group of instances.

East-west traffic between subnets within a VPC always goes directly between instances. AWS route tables cannot override this behavior, and a limitation of this 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.

The Centralized design model provides a scalable design for inspection and control of east-west, inbound, and outbound traffic.

Backhaul to On-Premises Networks

Because you cannot use a gateway route table to direct traffic from a VGW to a GWLB endpoint, the isolated design model does not support securing backhaul traffic to on-premises networks.

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 management VPC to the security VPC via VPC peering.

Assumptions and Prerequisites

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 that supports the Gateway Load Balancer.

Palo Alto Networks VM-Series firewalls and Panorama:

- The tested PAN-OS version in this guide is 10.0.5.
- The tested Cloud Services plugin for Panorama is 1.7.0-h3.
- 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 10.0.5. 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 new VPCs 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

1.1 Create the Spoke VPCs

1.2 Create IP Subnets for the Spoke VPCs

1.3 Create Security Groups for the Spoke VPCs

1.4 Create a Transit Gateway

1.5 Create Transit Gateway Route Tables

1.6 Create Transit Gateway Attachments

1.7 Associate Attachments to the Route Tables

1.8 Create Spoke VPC Route Tables

1.9 Modify Management VPC Routes and Security Group

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 Spoke VPCs

First, you create two VPCs that connect to the transit gateway. Inbound, outbound, and east-west traffic flows from the instances in these VPCs will cross the VM-Series firewalls also connected to the transit gateway.

Table 1 Spoke VPCs

VPC name	IPv4 CIDR block	VPC function
web	10.104.0.0/16	Example VPC for web servers
db	10.105.0.0/16	Example VPC for database (DB) servers

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 **web**.

Step 5: In the **IPv4 CIDR block** box, enter the IP address and mask **10.104.0.0/16**, and then click **Create VPC**.

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 6: In the **Actions** list, choose **Edit DNS Hostnames**. The Edit DNS Hostnames window opens.

Step 7: On the DNS Hostnames dialog box, select **Enable**, and then click **Save changes**.

Step 8: Repeat this procedure for the second VPC in Table 1.

1.2 Create IP Subnets for the Spoke VPCs

You should break up the initial IPv4 CIDR block into subnets. You can assign only IP address space in the configured CIDR space(s) to a subnet.

Table 2 Spoke VPC IP subnets

Subnet name	VPC	Availability zone	IPv4 CIDR block
web-instances-2a	web	us-west-2a	10.104.0.0/24
web-tgw-2a	web	us-west-2a	10.104.1.0/24
web-instances-2b	web	us-west-2b	10.104.128.0/24
web-tgw-2b	web	us-west-2b	10.104.129.0/24
db-instances-2a	db	us-west-2a	10.105.0.0/24
db-tgw-2a	db	us-west-2a	10.105.1.0/24
db-instances-2b	db	us-west-2b	10.105.128.0/24
db-tgw-2b	db	us-west-2b	10.105.129.0/24

Step 1: Navigate to **Virtual Private Cloud > Subnets**, and then click **Create subnet**.

Step 2: In the **VPC** list, choose **web**.

Step 3: In the **Subnet Name** box, enter **web-instances-2a**.

Step 4: In the **Availability Zone** list, choose **us-west-2a**.

Step 5: In the **IPv4 CIDR block** box, enter **10.104.0.0/24**.

Step 6: Click **Create subnet**.

Step 7: Repeat this procedure for all the subnets in Table 2.

1.3 Create Security Groups for the Spoke VPCs

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.

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

First, for the instances in the Web VPC, you create a public security group that allows all traffic from private networks.

Step 1: Navigate to **Security** > **Security Groups**, and then click **Create Security Group**.

Step 2: In the **Security group name** box, enter **web-instances**.

Step 3: In the **Description** box, enter **Allow inbound traffic from private networks**.

Step 4: In the **VPC** list, choose **web**.

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

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

Step 7: In the **Source Type** list, choose **Custom**.

Step 8: In the **Source** box, enter **10.0.0.0/8**.

Step 9: In the Tags pane, click **Add new tag**.

Step 10: In the **Key** box, enter **Name**.

Step 11: In the **Value** box, enter **web-instances**.

Step 12: Click **Create security group**.

Next, for the instances in the DB VPC, you create a public security group that allows all traffic from private networks.

Step 13: Navigate to **Security** > **Security Groups**, and then click **Create Security Group**.

Step 14: In the **Security group name** box, enter **db-private**.

Step 15: In the **Description** box, enter **Allow inbound traffic from private networks**.

Step 16: In the **VPC** list, choose **db**.

Step 17: In the Inbound rules pane, click **Add Rule**.

Step 18: In the **Type** list, choose **All traffic**.

Step 19: In the **Source Type** list, choose **Custom**.

Step 20: In the **Source** box, enter **10.0.0.0/8**.

Step 21: In the Tags pane, click **Add new tag**.

Step 22: In the **Key** box, enter **Name**.

Step 23: In the **Value** box, enter **db-instances**.

Step 24: Click **Create security group**.

1.4 Create a Transit Gateway

Step 1: Navigate to **Transit Gateways** > **Transit Gateways**.

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

Step 3: In the **Name tag** box, enter **TGW**.

Step 4: In the **Description** box, enter **Transit Gateway**.

Step 5: Clear **Default route table association** and **Default route table propagation**. You create the route tables for the transit gateway in the next procedure.

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

1.5 Create Transit Gateway Route Tables

Next, you create two transit gateway route tables. The route tables can include static routes and dynamically learned routes from VPN attachments.

First, you create the route table for the security VPCs.

Step 1: In **Transit Gateways > Transit Gateway Route Tables**, click **Create Transit Gateway Route Table**.

Step 2: In the **Name tag** box, enter security.

Step 3: In the **Transit Gateway ID** list, choose TGW.

Step 4: Click **Create Transit Gateway Route Table**, and then click **Close**.

Next, you create the transit gateway route table for the spoke VPCs.

Step 5: In **Transit Gateways > Transit Gateway Route Tables**, click **Create Transit Gateway Route Table**.

Step 6: In the **Name tag** box, enter spokes.

Step 7: In the **Transit Gateway ID** list, choose TGW.

Step 8: Click **Create Transit Gateway Route Table**, and then click **Close**.

1.6 Create Transit Gateway Attachments

After the transit gateway becomes available, you create the attachments from your spoke VPCs to the transit gateway. Because you deployed Panorama in a separate VPC in the **Panorama on AWS: Deployment Guide**, you also need to connect the management VPC to the transit gateway.

Table 3 VPC attachments

Attachment name and VPC	Subnet 1	Subnet 2
web	web-tgw-2a	web-tgw-2b
db	db-tgw-2a	db-tgw-2b
management	management-2a	management-2b

Step 1: In **Transit Gateway > Transit Gateway Attachments**, click **Create Transit Gateway Attachment**.

Step 2: In the **Transit Gateway ID** list, choose **TGW**.

Step 3: For **Attachment type**, select **VPC**.

Step 4: In the **Attachment name tag** box, enter **web**.

Step 5: In the **VPC ID** list, choose **web**.

Step 6: For **Subnet IDs**, select **web-tgw-2a** and **web-tgw-2b**.

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

Step 8: Repeat this procedure for the remaining VPCs in Table 3.

1.7 Associate Attachments to the Route Tables

Transit gateway route tables are routing domains, and you control which routes are available to a spoke VPC based on the route table with which it is associated. You control the routes available in a routing domain by selectively propagating the attachments into it.

First, you associate the Web and DB VPC attachments to the spokes route table, which allows you to control traffic flows through the VM-Series firewalls.

Step 1: Navigate to **Transit Gateways > Transit Gateway Route Tables**.

Step 2: In the top pane, select **spokes**.

Step 3: In the bottom pane, on the Associations tab, click **Create Association**. The Create Association windows opens.

Step 4: In the **Choose attachment to associate** list, choose **web**.

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

Step 6: In the bottom pane, on the Associations tab, click **Create Association**.

Step 7: In the **Choose attachment to associate** list, choose **DB**.

Step 8: Click **Create association**, and then click **Close**.

Step 9: In the bottom pane, on the Associations tab, click **Create Association**.

Step 10: In the **Choose attachment to associate** list, choose **Management**.

Step 11: Click **Create association**, and then click **Close**.

Next, you propagate the routes from the Web, DB, and Management VPCs into the security route table.

Step 12: In the top pane, select **security**. Ensure no other route tables are selected.

Step 13: In the bottom pane, on the Propagations tab, click **Create Propagation**.

Step 14: In the **Choose attachment to propagate** list, choose **web**.

Step 15: Click **Create propagation**, and then click **Close**.

Step 16: Click **Create Propagation**.

Step 17: In the **Choose attachment to propagate** list, choose **db**.

Step 18: Click **Create propagation**, and then click **Close**.

Step 19: Click **Create Propagation**.

Step 20: In the **Choose attachment to propagate** list, choose **management**.

Step 21: Click **Create propagation**, and then click **Close**.

1.8 Create Spoke 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 instances in the VPC can natively connect to any other instance 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.

You create the VPC route tables after creating the transit gateway so that the transit gateway exists as a next hop in the routing tables.

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 4 Spoke routes to the TGW

Route table name	VPC	Route destination	Target	Subnets assigned
web-instances	web	0.0.0.0/0	TGW	web-instances-2a, web-instances-2b
db-instances	db	0.0.0.0/0	TGW	db-instances-2a, db-instances-2b

Step 1: 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 **web-instances**.

Step 4: In the **VPC** list, choose **web**.

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

Step 6: In the top pane, select only **web-instances**. Ensure no other route tables are selected.

Step 7: In the bottom pane, on the Routes tab, click **Edit routes**.

Step 8: Click **Add route**, and then in the **Destination** box, enter **0.0.0.0/0**.

Step 9: Click in the **Target** box, and then choose the **TGW**.

Step 10: Click **Save routes**, and then click **Close**.

Destination	Target	Status
10.104.0.0/16	local	active
0.0.0.0/0	tgw-09ea5ed7a07428cd3	active

Step 11: On the Subnet Associations tab, click **Edit subnet associations**.

Step 12: In the list, choose subnets **web-instances-2a** and **web-instances-2b**, and then click **Save**.

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-0c9974bffb8db2b58 | web-instances-2b	10.104.128.0/...	-
subnet-07d707f6aa97f577d | web-tgw-2a	10.104.1.0/24	-
subnet-09e59151e262e535d | web-instances-2a	10.104.0.0/24	-
subnet-05fff981f6a9488d6 | web-tgw-2b	10.104.129.0/...	-

Step 13: Repeat this procedure for the remaining route in Table 4.

1.9 Modify Management VPC Routes and Security Group

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 the Panorama security group that allows the VM-Series firewalls to communicate with Panorama.

First, you create a route that lets Panorama reach the VM-Series firewalls through the TGW.

Step 1: Navigate to **Virtual Private Cloud > Route Tables**.

Step 2: In the top pane, select **management**. Ensure no other route tables are selected.

Step 3: In the bottom pane, on the Routes tab, click **Edit routes**.

Step 4: Click **Add route**, and then in the **Destination** box, enter **10.0.0.0/8**.

Step 5: Click in the **Target** box, and then choose the **TGW**.

Step 6: Click **Save routes**, and then click **Close**.

Next, you add an inbound rule to the security group associated to the Panorama interfaces in order to allow inbound traffic from the VM-Series firewalls.

Step 7: Navigate to **Virtual Private Cloud > Security > Security Groups**.

Step 8: In the top pane, select **panorama**.

Step 9: In the bottom pane, on the Inbound Rules tab, click **Edit Inbound Rules**.

Step 10: Click **Add Rule**.

Step 11: In the **Type** list, choose **All traffic**.

Step 12: In the **Source Type** list, choose **Custom**.

Step 13: In the **Source** box, enter **10.0.0.0/8**, and then click **Save Rules**.

Deploying Outbound and East-West Security

Procedures

Configuring the VPC, Subnets, and Services

2.1 Create the VPC

2.2 Create IP Subnets

2.3 Create a VPC Internet Gateway

2.4 Create Transit Gateway Attachments

2.5 Associate Attachments to the Route Tables

2.6 Create Default Route in Spokes Route Table

2.7 Create Gateway Load Balancer

2.8 Create Endpoint Service

2.9 Create Gateway Load Balancer Endpoints

2.10 Create VPC Route Tables

2.11 Create Security Groups

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, attachments, GWLB, and security groups to support the VM-Series instances.

2.1 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 security.

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

Step 6: Click **Create VPC**.

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: 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**, and then click **Save changes**.

2.2 Create IP Subnets

You should break up the initial IPv4 CIDR block into subnets. You can assign only IP address space in the configured CIDR space(s) to a subnet.

Table 5 IP subnets

Subnet name	Availability zone	IPv4 CIDR block
security-mgmt-2a	us-west-2a	10.100.0.0/24
security-fw-2a	us-west-2a	10.100.1.0/24
security-public-2a	us-west-2a	10.100.2.0/24
security-tgw-2a	us-west-2a	10.100.3.0/24
security-gwlbe-2a	us-west-2a	10.100.4.0/24
security-gwlb-2a	us-west-2a	10.100.5.0/24
security-mgmt-2b	us-west-2b	10.100.64.0/24
security-fw-2b	us-west-2b	10.100.65.0/24
security-public-2b	us-west-2b	10.100.66.0/24
security-tgw-2b	us-west-2b	10.100.67.0/24
security-gwlbe-2b	us-west-2b	10.100.68.0/24
security-gwlb-2b	us-west-2b	10.100.69.0/24
security-gwlb-2c	us-west-2c	10.100.128.0/24
security-gwlb-2d	us-west-2d	10.100.192.0/24

Step 1: Navigate to **Virtual Private Cloud > Subnets**.

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

Step 3: In the **VPC** list, choose security.

Step 4: In the **Subnet name** box, enter security-mgmt-2a.

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 **Add new subnet**.

Step 8: Repeat Step 4 - Step 6 for all the subnets in Table 5, and then click **Create subnet**.

2.3 Create a VPC Internet Gateway

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

Step 1: Navigate to **Virtual Private Cloud > Internet Gateways**.

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

Step 3: Click **Create internet gateway**.

Step 4: In the **Actions** list, choose **Attach to VPC**.

Step 5: In the **Available VPCs** list, choose security, and then click **Attach internet gateway**.

2.4 Create Transit Gateway Attachments

You create a VPC attachment from the security VPC to the transit gateway. The firewalls use this attachment for all traffic to the networks that are reachable through the transit gateway. You must also modify the attachment to enable appliance mode.

Step 1: In **Transit Gateways > Transit Gateway Attachments**, click **Create Transit Gateway Attachment**.

Step 2: In the **Transit Gateway ID** list, choose TGW.

Step 3: For **Attachment type**, select **VPC**.

Step 4: In the **Attachment name tag** box, enter security.

Step 5: In the **VPC ID** list, choose security.

Step 6: Clear the us-west-2c and us-west-2d availability zones.

Step 7: For **Subnet IDs**, select security-tgw-2a and security-tgw-2b.

Step 8: Click **Create Attachment**, and then click **Close**.

Next, enable appliance mode on the attachment.

Step 9: In **Transit Gateways** > **Transit Gateway Attachments**, select the security attachment.

Step 10: In the bottom pane, on the Details tab, copy the **Transit Gateway attachment ID**.

Step 11: Launch AWS CloudShell.

Step 12: Enable appliance mode support on the security VPC TGW attachment. Us the attachment ID you copied in the previous step.

```
aws ec2 modify-transit-gateway-vpc-attachment --transit-gateway-attachment-id
xxxxxxxxxxxx --options ApplianceModeSupport=enable
```

2.5 Associate Attachments to the Route Tables

In this procedure, you configure the TGW so that the firewalls can reach all networks attached to the transit gateway and so that all networks can reach the firewalls.

First, you associate the security VPC attachment to the security route table, which allows the security VPC to reach all the VPCs that are connected to the transit gateway. It can take a few minutes for attachment you created in the previous procedure to become available.

Step 1: Navigate to **Transit Gateways** > **Transit Gateway Route Tables**.

Step 2: In the top pane, select **security**.

Step 3: In the bottom pane, on the Associations tab, click **Create Association**. The Create Association windows opens.

Step 4: In the **Choose attachment to associate** list, choose **security**.

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

Next, you propagate the routes from the security VPC into the security route table.

Step 6: In the top pane, ensure **security** is selected.

Step 7: In the bottom pane, on the Propagations tab, click **Create Propagation**.

Step 8: In the **Choose attachment to propagate** list, choose **security**.

Step 9: Click **Create propagation**, and then click **Close**.

Next, you propagate the routes from the security VPC into the spokes route table.

Step 10: In the top pane, select **spokes**.

Step 11: In the bottom pane, on the Propagations tab, click **Create Propagation**.

Step 12: In the **Choose attachment to propagate** list, choose **security**.

Step 13: Click **Create propagation**, and then click **Close**.

2.6 Create Default Route in Spokes Route Table

You create a default route in the TGW spokes route table that directs all traffic to the security VPC.

Step 1: Navigate to **Transit Gateways > Transit Gateway Route Tables**.

Step 2: In the top pane, select **spokes**.

Step 3: In the bottom pane, on the Routes tab, click **Create static route**.

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

Step 5: In the **Choose attachment** list, choose **security**.

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

2.7 Create Gateway Load Balancer

Step 1: On the EC2 Service, navigate **Load Balancing > Load Balancers**, and then click **Create Load Balancer**.

Step 2: On the Gateway Load Balancer pane, click **Create**.

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

Step 4: In the **VPC** list, choose security.

Step 5: Select all the Availability Zones, and then choose the security-gwlb-2a, security-gwlb-2b, security-gwlb-2c, security-gwlb-2d subnets.

Step 6: Click **Next Configure Routing**.

Step 7: In the **Name** box, enter VM-Series.

Step 8: For **Target type**, choose **IP**.

Step 9: In the **Protocol** list, choose **HTTPS**.

Step 10: In the **Path** box, enter **/php/login.php**.

Step 11: Expand **Advanced health check settings**.

Step 12: In the **Port** box, enter **443**.

Step 13: Click **Next: Register Targets**. Because you haven't deployed the VM-Series firewalls yet, you will register the VM-Series firewalls as targets later in the deployment.

Step 14: Click **Next: Review**, click **Create**, and then click **Close**.

Next, you enable cross zone load balancing.

Step 15: In the top pane, select the **security** load balancer.

Step 16: In the **Actions** list, choose **Edit attributes**.

Step 17: For **Cross-zone load balancing**, select **Enable**, and then click **Save**.

2.8 Create Endpoint Service

Now you create an endpoint service to accept connections from GWLB endpoints. For security, ensure that you have to accept new endpoint connections.

Step 1: On the VPC Service, navigate to **Virtual Private Cloud > Endpoint Services**, and then click **Create Endpoint Service**.

Step 2: In the Associate Load Balancers pane, select the **security** GWLB.

Step 3: Click **Add Tag**

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

Step 5: In the **Value** box, enter **security-GWLB**.

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

Next, you copy the service name from the service for use when creating the endpoints.

Step 7: Navigate to **Virtual Private Cloud > Endpoint Services**, and select the **security-GWLB** service.

Step 8: In the bottom pane, on the Details tab, copy the **Service name**.

2.9 Create Gateway Load Balancer Endpoints

Now you deploy two GWLB endpoints. You must create the GWLB endpoints one at a time.

Step 1: Navigate to **Virtual Private Cloud > Endpoints**, and then click **Create Endpoint**.

Step 2: For **Service Category**, choose **Find service by name**.

Step 3: In the **Service Name** box, paste in the vale from Procedure 2.8, Step 8, and then click **Verify**.

Step 4: In the **VPC** list, choose security.

Step 5: For **Availability Zone**, select the us-west-2a availability zone only. Clear all other availability zones.

Step 6: In the **Subnet ID** list, choose security-gwlbe-2a.

Step 7: Click **Add Tag**.

Step 8: In the **Key** box, enter **Name**.

Step 9: In the **Value** box, enter security-2a.

Step 10: Click **Create endpoint**, and then click **Close**.

Next, you create the second endpoint.

Step 11: Navigate to **Virtual Private Cloud > Endpoints**, and then click **Create Endpoint**.

Step 12: For **Service Category**, choose **Find service by name**.

Step 13: In the **Service Name** box, paste in the vale from Procedure 2.8, Step 8, and then click **Verify**.

Step 14: In the **VPC** list, choose security.

Step 15: For **Availability Zone**, select the us-west-2b availability zone only. Clear all other availability zones.

Step 16: In the **Subnet ID** list, choose security-gwlbe-2b.

Step 17: Click **Add Tag**.

Step 18: In the **Key** box, enter **Name**.

Step 19: In the **Value** box, enter security-2b.

Step 20: Click **Create endpoint**, and then click **Close**.

Next, you accept the connection requests from the two endpoints you just created.

Step 21: Navigate to **Virtual Private Cloud > Endpoint Services**, and then select security-GWLB.

Step 22: In the bottom pane, on the Endpoint Connections tab, select the first endpoint.

Step 23: In the **Actions** list, choose **Accept endpoint connection request**.

Step 24: Click **Yes, accept**.

Step 25: Repeat Step 22 - Step 24 for the second endpoint.

2.10 Create VPC Route Tables

In this procedure, you configure route tables in the security VPC to direct traffic to the TGW, IGW, or GWLB endpoints as appropriate.

Table 6 Routes to the IGW

Route table name	Route destination	Target	Subnets assigned
security-public	0.0.0.0/0	IGW	security-public-2a, security-public-2b
security-mgmt	0.0.0.0/0	IGW	security-mgmt-2a, security-mgmt-2b
	10.255.0.0/16	TGW	
security-tgw-2a	0.0.0.0/0	GWLBe security-2a	security-tgw-2a
security-tgw-2b	0.0.0.0/0	GWLBe security-2b	security-tgw-2b
security-gwlbe	0.0.0.0/0	TGW	security-gwlbe-2a, security-gwlbe-2b

Step 1: 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 security-public.

Step 4: In the **VPC** list, choose security.

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

Step 6: In the top pane, select security-public.

Step 7: In the bottom pane, on the Routes tab, click **Edit routes**.

Step 8: Click **Add route**, and then in the **Destination** box, enter **0.0.0.0/0**.

Step 9: Click in the **Target** box, and then choose the security IGW.

Step 10: 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-029b48cdb1c1a0316	active	No

Step 11: On the Subnet Associations tab, click **Edit subnet associations**.

Step 12: In the list, choose subnets security-public-2a and security-public-2b, and then click **Save**.

☐	subnet-09c31938a4c6ceb59 | security-tgw-2a	10.100.3.0/24	-
☐	subnet-06fe36c188cfa6da7 | security-fw-2b	10.100.65.0/24	-
☑	subnet-0af9fd55ad0a00efe | security-public-2a	10.100.2.0/24	-
☑	subnet-0d223124a73564370 | security-public-2b	10.100.66.0/24	-
☐	subnet-0cae08ba5eb6c7852 | security-fw-2a	10.100.1.0/24	-

Step 13: Repeat this procedure for the remaining route tables in Table 6.

2.11 Create Security Groups

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

- **Public**—Initially all inbound traffic is denied to 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 PAN-OS Administrator's Guide—PAN-OS 10.0 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 denies inbound traffic.

Step 1: Navigate to **Security > Security Groups**, and then click **Create Security Group**.

Step 2: In the **Security group name** box, enter security-firewall-public.

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

Step 4: In the **VPC** list, choose security.

Step 5: Click **Create security group**.

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

Table 7 Security-firewall-mgmt security group—inbound rules

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

Step 6: Navigate to **Security > Security Groups**, and then click **Create Security Group**.

Step 7: In the **Security group** name box, enter security-firewall-mgmt.

Step 8: In the **Description** box, enter Allow inbound management to the firewall.

Step 9: In the **VPC** list, choose security.

Step 10: In the Inbound rules pane, click **Add Rule**.

Step 11: In the **Type** list, choose SSH.

Step 12: In the **Source** list, choose My IP.

Step 13: Repeat Step 10 - Step 12 for the remaining rule in Table 7.

Step 14: Click **Create security group**.

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

Step 15: Navigate to **Security > Security Groups**, and then click **Create Security Group**.

Step 16: In the **Security group** name box, enter security-firewall-private.

Step 17: In the **Description** box, enter Allow inbound traffic to private interface.

Step 18: In the **VPC** list, choose security.

Step 19: In the Inbound rules pane, 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 10.0.0.0/8.

Step 23: In the Inbound rules pane, click **Add Rule**.

Step 24: In the **Type** list, choose All traffic.

Step 25: In the **Source Type** list, choose **Custom**.

Step 26: In the **Source** box, enter 172.16.0.0/12.

Step 27: In the Inbound rules pane, click **Add Rule**.

Step 28: In the **Type** list, choose All traffic.

Step 29: In the **Source Type** list, choose **Custom**.

Step 30: In the **Source** box, enter 192.168.0.0/16.

Step 31: Click **Create security group**.

Procedures

Configuring Panorama Device Groups, Templates, and Template Stacks

3.1 Configure a Parent Device Group

3.2 Configure Log Forwarding Objects

3.3 Create a Baseline Template

3.4 Configure the Firewall Baseline Settings Template

3.5 Create the Network Settings Template

3.6 Create the Management Profile for the Firewalls

3.7 Configure the Network Settings

3.8 Add Private Subinterface

3.9 Add Static Routes

3.10 Create Template Stacks

3.11 Define the Next-Hop Variables for Each Template Stack

3.12 Configure the Device Group

3.13 Configure Health Check Security Policy

3.14 Configure the Outbound NAT Policy

3.15 Configure the Outbound Security Policy

3.16 Configure the East-West Security Policy

3.17 Generate VM Auth Key

Configure device groups and templates to support the VM-Series deployment on AWS. First, you create common settings and then you create and configure settings specific to the outbound and east-west traffic flows. The last step is to create an authorization key that allows the VM-Series to bootstrap their configuration from Panorama.

3.1 Configure a Parent Device Group

Device groups contain VM-Series firewalls that 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. This device group holds a common configuration that could apply to any VM-Series deployment in this environment and is the parent device group for AWS deployments.

Step 1: Log in to the Panorama web interface.

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

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

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

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

Step 1: On the Objects tab, in the **Device Group** list, choose **AWS-Baseline**.

Step 2: In the navigation pane, click **Log Forwarding**, and then click **Add**.

Step 3: In the **Name** box, enter **Forward-to-Cortex-Data-Lake**.

Step 4: Select **Enable enhanced application logging to Cortex Data Lake**, and then click **OK**.

3.3 Create a Baseline Template

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.

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

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

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

Step 9: In **Device > Setup > Content-ID > X-Forwarded-For Headers**, click the **Edit** cog.

Step 10: Select **Enabled for Security Policy**, and then click **OK**.

Step 11: In **Device > Setup > Interfaces**, click **Management**.

Step 12: For **IP Type**, choose **DHCP Client**.

Step 13: In **Administrative Management Services**, select **HTTPS** and **SSH**.

Step 14: In **Network Services**, select **Ping**, and then click **OK**.

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

Next, you enable logging to Cortex Data Lake.

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

Step 16: Verify that the Cortex Data Lake license is active.

Step 17: Navigate to **Device**, and then in the **Template** list, choose **Baseline-VMSeries-Settings**.

Step 18: In **Device > Setup > Management > Cortex Data Lake**, click the **Edit** cog.

Step 19: Select **Enable Cortex Data Lake**, and then select **Enable Enhanced Application Logging**.

Step 20: In the **Region** list, choose **United States - Americas**, and then click **OK**.

Step 21: In **Device** > **Log Settings** > **System**, click **Add**. The Log Settings—System configuration window appears.

Step 22: In the **Name** box, enter System Logs.

Step 23: Select **Panorama/Cortex Data Lake**, and then click **OK**.

Step 24: In **Device** > **Log Settings** > **Configuration**, click **Add**. The Log Settings—Configuration window appears.

Step 25: In the **Name** box, enter Configuration Logs.

Step 26: Select **Panorama/Cortex Data Lake**, and then click **OK**.

Step 27: In the **Commit** menu, click **Commit to Panorama**, and then click **Commit**.

3.5 Create the Network Settings Template

You use templates to configure functions that are common across groups of firewalls. In this procedure, you create a network template that is specific to this design model.

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

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

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

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

3.6 Create the Management Profile for the Firewalls

The GWLB uses HTTPS health checks towards the firewall's private dataplane interface. You use an interface management profile to configure the firewall to respond to the health checks.

Step 1: Navigate to **Network** > **Network Profiles** > **Interface Mgmt**, and then in the **Template** list, choose AWS-Network-Settings.

Step 2: Click **Add**. The Interface Management Profile window appears.

Step 3: In the **Name** box, enter Health Checks.

Step 4: In the Administrative Management Services section, select **HTTPS**, and then click **OK**.

3.7 Configure the Network Settings

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

Interface	Interface type	Zone	Virtual router	Type	Enable default route	Management profile
ethernet1/1	Layer3	internal	vr-default	DHCP client	No	Health checks
ethernet1/2	Layer3	public	vr-default	DHCP client	Yes	None

Step 1: Navigate to **Network > Interfaces**, and then in the **Template** list, choose **AWS-Network-Settings**.

Step 2: Click **Add Interface**.

Step 3: In the **Slot** list, choose **Slot 1**.

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

Step 5: In the **Interface Type** list, choose **Layer3**.

Step 6: On the Config tab, in the **Virtual Router** list, choose **New Virtual Router**. The Virtual Router window appears.

Step 7: In the **Name** box, enter **vr-default**, and then click **OK**.

Step 8: In the **Security Zone** list, choose **New Zone**. The Zone window appears.

Step 9: In the **Name** box, enter **internal**, and then click **OK**.

Step 10: On the IPv4 tab, for **Type**, select **DHCP Client**.

Step 11: Clear **Automatically create default route pointing to default gateway provided by server**, and then click **OK**.

Step 12: On the Advanced tab, if a management profile is listed in Table 8, in the **Management Profile** list, choose that management profile, and then click **OK**.

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

Step 14: Repeat this procedure for the second interface listed in Table 8, making sure to select the default route check box and skipping the management profile.

3.8 Add Private Subinterface

Now you create a subinterface that you use to map the outbound and east-west GWLB endpoints to the private security zone. The subinterface must be configured for DHCP but does not receive an IP address.

Step 1: Navigate **to Network > Interfaces**, and select the **Ethernet 1/1** row.

Step 2: Click **Add Subinterface**.

Step 3: In the subinterface number box, enter 1.

Step 4: In the **Tag** box, enter 1.

Step 5: In the **Virtual Router** list, choose vr-default.

Step 6: In the **Security Zone** list, choose **New Zone**. The Zone window appears.

Step 7: In the **Name** box, enter private, and then click **OK**.

Step 8: On the IPv4 tab, for **Type**, select **DHCP Client**.

Step 9: Clear **Automatically create default route pointing to default gateway provided by server**, and then click **OK**.

3.9 Add Static Routes

In this procedure, you configure the firewalls with routes to the RFC 1918 address space that use the private dataplane interface to route to the spoke VPCs. Because each availability zone has a different subnet, you use a variable to define the next-hop IP address. You set the value of the variable in each template stack to the subnet's gateway.

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

Step 2: On the Static Routes tab, click **Add**.

Step 3: In the **Name** box, enter **10.0.0.0**.

Step 4: In the **Destination** box, enter **10.0.0.0/8**.

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

Step 6: In the **Next Hop** box, select **New Variable**.

Step 7: In the **Name** box, enter **$GW**.

Step 8: In the **Type** box, choose **None**, and then click **OK**.

Step 9: Click **OK**.

Step 10: On the Static Routes tab, click **Add**.

Step 11: In the **Name** box, enter **172.16.0.0**.

Step 12: In the **Destination** box, enter **172.16.0.0/12**.

Step 13: In the **Interface** list, choose **ethernet1/1**.

Step 14: In the **Next Hop** box, select **$GW**, and then click **OK**.

Step 15: On the Static Routes tab, click **Add**.

Step 16: In the **Name** box, enter **192.168.0.0**.

Step 17: In the **Destination** box, enter **192.168.0.0/16**.

Step 18: In the **Interface** list, choose **ethernet1/1**.

Step 19: In the **Next Hop** box, select **$GW**, and then click **OK**.

3.10 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
AWS-a-Stack	Baseline-VMSeries-Settings AWS-Network-Settings
AWS-b-Stack	Baseline-VMSeries-Settings AWS-Network-Settings

Step 1: Navigate to **Panorama > Templates**, and then click **Add Stack**.

Step 2: In the **Name** box, enter AWS-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 AWS-Network-Settings, and then click **OK**.

Step 5: Repeat this procedure for the remaining template stack listed in Table 9.

3.11 Define the Next-Hop Variables for Each Template Stack

You define the next-hop IP address for the static routes in the template stack. Override the $GW variable with the corresponding subnet gateway.

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

Step 2: On the AWS-a Stack row, in the Variables column, click **Manage**.

Step 3: Select the $GW row, and then click **Override**.

Step 4: In the box to the right of IP Netmask, enter 10.100.1.1, and then click **OK**.

Step 5: On the AWS-b Stack row, in the Variables column, click **Manage**.

Step 6: Select the $GW row, and then click **Override**.

Step 7: In the box to the right of IP Netmask, enter 10.100.65.1, and then click **OK**

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

3.12 Configure the Device Group

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

Step 1: Navigate to **Panorama > Device Groups**, and then click **Add**.

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

Step 3: In the **Description** box, enter a valid description.

Step 4: In the Reference Templates pane, click **Add**.

Step 5: In the list, choose AWS Network Settings.

Step 6: In the **Parent Device Group** list, verify that the value is set to AWS-Baseline, and then click **OK**.

3.13 Configure Health Check Security Policy

Now you create a security policy rule that allows HTTPS health checks from the GWLB subnets to the VM-Series.

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

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

Step 3: In the **Name** box, enter Health check.

Step 4: On the Source tab, under Source Zone, click **Add.**

Step 5: In the **Source Zone** list, choose internal.

Step 6: In the **Source Address** list, click **Add**.

Step 7: In the **Source Address** box, enter 10.100.5.0/24

Step 8: In the **Source Address** list, click **Add**.

Step 9: In the **Source Address** box, enter 10.100.69.0/24.

Step 10: In the **Source Address** list, click **Add**.

Step 11: In the **Source Address** box, enter 10.100.128.0/24.

Step 12: In the **Source Address** list, click **Add**.

Step 13: In the **Source Address** box, enter 10.100.192.0/24.

Step 14: On the Destination tab, under Destination Zone, click **Add**.

Step 15: In the **Destination Zone** list, choose internal.

Step 16: On the Application tab, in the Applications pane, click **Add.**

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

Step 18: On the Actions tab, in the **Action** list, choose Allow.

Step 19: In the **Log Forwarding** list, choose None, and then click **OK**.

3.14 Configure the Outbound NAT Policy

For outbound internet traffic, you create a NAT rule that translates the source address of outbound traffic to the IP address of the VM-Series public interface.

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

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

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

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

Step 5: On the Translated Packet tab, in the Source Address Translation section, in the **Translation Type** list, choose **Dynamic IP And Port**.

Step 6: In the Source Address Translation section, in the **Address Type** list, choose **Interface Address**.

Step 7: In the Source Address Translation section, in the **Interface** list, choose **ethernet1/2**, and then click **OK**.

3.15 Configure the Outbound 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). This example uses a common outbound policy for all instances. If you wish to use a differentiated policy, create separate rules for each spoke VPC or subnet.

The common outbound security policy example permits the yum and ntp applications.

Add additional applications to your outbound policy as required.

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

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

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

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

Step 5: On the Destination tab, under Destination Zone, 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 **yum**, and then in the results list, select **yum**.

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, select **ntp**.

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

Step 12: In the Log Forwarding list, choose **Forward-to-Cortex-Data-Lake**, and then click **OK**.

3.16 Configure the East-West Security Policy

Now you configure a security policy rule that allows MySQL traffic from the private zone. This security policy rule uses the web VPC CIDR block as the source and the database VPC CIDR block as the destination. Add additional east-west 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 **web-to-db**.

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

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

Step 5: In the **Source Address** list, click **New Address**.

Step 6: In the **Name** box, enter **web-vpc**.

Step 7: In the **Type** list, choose **IP Netmask**.

Step 8: In the **IP** box, enter the web VPC IP address block **10.104.0.0/16**, and then click **OK**.

Step 9: On the Destination tab, under Destination Zone, click **Add**.

Step 10: In the **Destination Zone** list, choose **private**.

Step 11: In the **Destination Address** list, click **New Address**.

Step 12: In the **Name** box, enter **db-vpc**.

Step 13: In the **Type** list, choose **IP Netmask**.

Step 14: In the **IP** box, enter the database VPC subnet **10.105.0.0/16**, and then click **OK**.

Step 15: On the Application tab, in the Applications pane, click **Add**.

Step 16: In the search box, enter **mysql**, and then in the results list, select **mysql**.

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

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

Next, you override the default intrazone rule and configure it to deny traffic.

Step 19: Navigate to **Policies > Security > Default Rules**.

Step 20: Select the **intrazone-default** row, and then at the bottom of the screen, click **Override**.

Step 21: On the **Actions** tab, in the Action Setting pane, in the **Action** list, choose **Deny**, and then click **OK**.

Step 22: On the **Commit** menu, click **Commit to Panorama**, and then click **Commit**.

3.17 Generate VM Auth Key

Now you generate a VM Auth Key on Panorama to be used during VM-Series bootstrapping.

Step 1: Using SSH, log in to the Panorama command line.

Step 2: Request the VM auth key.

```
request bootstrap vm-auth-key generate lifetime 8760


VM auth key 123456789012345 generated. Expires at: 2022/04/09 14:15:56
```

> **Note**
>
> The lifetime of the key can vary between 1 hour and 8760 hours (1 year). After the specified time, the key expires. Panorama does not register VM-Series firewalls without a valid auth-key in the connection request.

Procedures

Deploying the VM-Series Instances

4.1 Create a VM-Series Deployment Profile

4.2 Create the VM-Series Firewalls

4.3 Create Elastic Network Interfaces for the VM-Series Firewalls

4.4 Attach the Interfaces to the Firewalls

4.5 Create Elastic IP Addresses for the VM-Series Firewall

4.6 Validate Deployment and Refresh Licenses

4.7 Register the VM-Series as GWLB Targets

4.1 Create a VM-Series Deployment Profile

To create a deployment profile, you must have a Customer Support Portal account and you must have activated your credit pool.

Step 1: Log in to the Palo Alto Networks support portal.

Step 2: In **Assets > Software NGFW Credits**, in the Prisma NGFW Credits pane, click **Create Deployment Profile**. The Create Deployment Profile window opens.

Step 3: For **Select firewall type**, choose **VM-Series**.

Step 4: Select **PAN-OS 10.0.4 and above**, and then click **Next**.

Step 5: In the Profile Name box, enter AWS VM-Series.

Step 6: In the **Number of Firewalls** box, enter 2.

Step 7: In the **Planned vCPU/Firewall** box, enter 4.

Step 8: In the **Security Use Case** list, choose **Data Center/ Cloud Inbound Security** and **Data Center/Cloud Outbound Security**.

Step 9: Next to Use Credits to Enable VM Panorama, clear **For Management**, and then click **Create Deployment Profile.**

The deployment profile takes a couple of minutes to deploy.

Step 10: Scroll to the far right of the Current Deployment Profiles list, and capture the AUTH CODE for the deployment profile.

4.2 Create the VM-Series Firewalls

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

Table 10 VM-Series firewall deployment parameters

System name	Subnet	Management IP address
vmseries-a	security-mgmt-2a	10.100.0.10
vmseries-b	security-mgmt-2b	10.100.64.10

Step 1: Sign into 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 Service, 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 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 **security**.

Step 10: In the **Subnet** list, choose **security-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 **10.100.0.10**.

Next, you configure the details for bootstrapping. You configured the:

- Panorama server IP addressing in the Panorama Deployment guide.
- Template stack names in Procedure 3.10.
- Device group name in Procedure 3.12.
- The auth code in Procedure 4.1.
- VM auth key in Procedure 3.17.
- GWLB endpoints in Procedure 2.9.

Step 13: Expand **Advanced Details**, and then in the **User data** box, enter

```
type=dhcp-client
panorama-server=10.255.0.4
panorama-server-2=10.255.1.4
tplname=AWS-a stack
dgname=AWS
dns-primary=169.254.169.253
authcodes=XXXXXXXX
vm-auth-key=123456789012345
plugin-op-commands=aws-gwlb-inspect:enable,aws-gwlb-associate-vpce:vpce-
0903806bc43532694@ethernet1/1.1,aws-gwlb-associate-vpce:vpce-0a81d66a391368361@
ethernet1/1.1,aws-gwlb-overlay-routing:enable
dhcp-accept-server-hostname=yes
dhcp-accept-server-domain=yes
```

Step 14: Click **Next: Add Storage**. The AMI template for VM-Series adds storage for the instance.

Step 15: Click **Next: Add Tags**

Step 16: Click **Add Tag**.

Step 17: In the **Key** box, enter Name.

Step 18: In the **Value** box, enter vmseries-a.

Step 19: Click **Next: Configure Security Group**.

Step 20: For **Assign a security group**, select **Select an existing security group**.

Step 21: Select the security-firewall-mgmt security group, and then click **Review and Launch**. Ensure that only the security-firewall-mgmt security group is selected.

Step 22: Review all selections, and then click **Launch**.

	Security Group ID	Name	Description	Actions
	sg-01c5430d5672d5e1f	default	default VPC security group	Copy to new
	sg-025f2e7fcd31a0166	security-firewall-mgmt	Allow inbound management to the firewall	Copy to new
	sg-0eee85a78bc710b15	security-firewall-private	Allow inbound traffic to private interface	Copy to new
	sg-0cb50403f9102eed2	security-firewall-public	Allowed inbound applications from the internet	Copy to new

Next, you assign key pair for the deployment.

Step 23: 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 26.

Step 24: In the **Key pair name** box, enter the key pair name paloaltonetworks-deployment.

Step 25: 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 26: Click **Launch instances**, and then click **View Instances**.

Step 27: Repeat this procedure to create the second VM-Series firewall, using the parameters from Table 10.

4.3 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 11 ENIs for the VM-Series firewalls

Name and description	Subnet	IP address	Security group
vmseries-a-public	security-public-2a	10.100.2.10	security-firewall-public
vmseries-a-private	security-fw-2a	10.100.1.10	security-firewall-private
vmseries-b-public	security-public-2b	10.100.66.10	security-firewall-public
vmseries-b-private	security-fw-2b	10.100.65.10	security-firewall-private

Step 1: 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 **security-public-2a**.

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

Step 5: In the **IPv4 address** box, enter **10.100.2.10**.

Step 6: In the **Security groups** list, choose **security-firewall-public**, and then click **Create network interface**.

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

Step 7: In the Network Interfaces pane, select **vmseries-a-public**.

Step 8: 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 9: For **Change Source/Dest**, clear **Enable**, and then click **Save**.

Step 10: Repeat this procedure for the remaining interfaces in Table 11.

4.4 Attach the Interfaces to the Firewalls

Now 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 12 Mapping of ENIs to the VM-Series instances

ENI name and description	VM-Series instance	Eth#
vmseries-a-private	vmseries-a	eth1
vmseries-a-public	vmseries-a	eth2
vmseries-b-private	vmseries-b	eth1
vmseries-b-public	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-private**, 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-public** 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: In the top pane, select the vmseries-a instance.

Step 7: In the bottom pane, on the Networking tab, verify that this instance now has three network interfaces.

Step 8: Repeat this procedure for the second VM-Series firewall.

4.5 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 13 EIPs for the VM-Series firewalls

EIP and ENI name	Private IP address
vmseries-a	10.100.0.10
vmseries-a-public	10.100.2.10
vmseries-b	10.100.64.10
vmseries-b-public	10.100.66.10

Step 1: Navigate to **Network & Security > Elastic IPs**.

Step 2: Click **Allocate Elastic IP address**.

Step 3: Click **Add new tag**.

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

Step 5: In the **Value** box, enter vmseries-a, and then click **Allocate**.

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

Step 6: In the **Actions** list, choose **Associate Elastic IP address**.

Step 7: In **Resource type**, select **Network Interface**.

Step 8: In the **Network Interface** list, choose vmseries-a. 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 9: In the **Private IP** list, choose 10.100.0.10, and then click **Associate**.

Step 10: Repeat this procedure for the rest of the interfaces in Table 13.

4.6 Validate Deployment and Refresh Licenses

After the VM-Series firewall deployment, they boot and register with Panorama.

Step 1: Log in to the Panorama web console and navigate to **Panorama > Managed Devices > Summary**.

	DEVICE NAME	MODEL	IP Address IPV4	VARIABLES	TEMPLATE	DEVICE STATE	SHARED POLICY	TEMPLATE
AWS (2/2 Devices Connected): Shared > AWS-Baseline > AWS								
	ip-10-100-0-10	PA-VM	10.100.0.10 (DHCP)	Create	AWS-a stack	Connected	In Sync	In sync
	ip-10-100-64-10	PA-VM	10.100.64.10 (DHCP)	Create	AWS-b stack	Connected	In Sync	In sync

Next, you refresh the VM-Series firewall's license in order to enable Cortex Data Lake.

Step 2: In **Panorama > Device Deployment > Licenses**, click **Refresh**.

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

4.7 Register the VM-Series as GWLB Targets

Now that the VM-Series are deployed and operational, you add the IP address of the VM-Series private dataplane interface to the GWLB's target pool. In Procedure 2.7, you created the target pool but didn't configure it.

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 Service, navigate to **Load Balancing > Target Groups**, and then click VM-Series.

Step 3: Click **Register Targets**.

Step 4: In the **IP** box, enter 10.100.1.10, and then click **Include as pending below**.

Step 5: In the **IP** box, enter 10.100.65.10, and then click **Include as pending below**.

Step 6: Click **Register pending targets**.

Deploying Inbound Security

There are two options for inbound traffic:

- **Combined inbound security with GWLB**—You can implement inbound security resiliency by using the VM-Series and GWLB in the Security VPC, with distributed GWLB endpoints in the application VPCs. Unlike outbound traffic, this design option does not use the Transit Gateway for traffic forwarding between the Security VPC and the application VPCs.
- **Centralized inbound security with ALB/NLB**—You can implement resiliency in AWS for inbound applications by using an AWS load-balancer sandwich design. This design uses a resilient, public-facing load balancer in the Security VPC and a second resilient load balancer on the private side of the firewalls in the application VPCs. This design option uses the Transit Gateway for traffic forwarding between the Security VPC and application VPCs.

Note

The combined option uses the GWLB to apply security for inbound traffic transparently and does not require address translation. The centralized option does not use the GWLB and requires the firewall to translate the traffic source IP address to ensure traffic returns to the correct firewall in the Security VPC.

Procedures

Deploying the Combined Inbound Security Option with a GWLB

5.1 Create a VPC Internet Gateway

5.2 Create IP Subnets for the Spoke VPCs

5.3 Configure the Public Application Load Balancer

5.4 Create Gateway Load Balancer Endpoints

5.5 Create VPC Route Tables

5.6 Add Application Subinterface

5.7 Map the GWLB Endpoints to the Subinterface

5.8 Configure the Security Policy

5.1 Create a VPC Internet Gateway

In this procedure, you create an IGW for internet connectivity and then attach it to the application 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: Navigate to **Virtual Private Cloud > Internet Gateways**.

Step 4: Click **Create internet gateway**, and then in the **Name tag** box, enter **web**.

Step 5: Click **Create internet gateway**.

Step 6: In the **Actions** list, choose **Attach to VPC**.

Step 7: In the **Available VPCs** list, choose **web**, and then click **Attach internet gateway**.

5.2 Create IP Subnets for the Spoke VPCs

Now you add subnets to the application VPC to support the GWLB endpoints and internet-facing load balancer.

Table 14 Spoke VPC IP subnets

Subnet name	VPC	Availability zone	IPv4 CIDR block
web-alb-2a	web	us-west-2a	10.104.2.0/24
web-gwlbe-2a	web	us-west-2a	10.104.3.0/24
web-alb-2b	web	us-west-2b	10.104.130.0/24
web-gwlbe-2b	web	us-west-2b	10.104.131.0/24

Step 1: Navigate to **Virtual Private Cloud > Subnets**.

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

Step 3: In the **VPC** list, choose **web**.

Step 4: In the **Subnet Name** box, enter **web-alb-2a**.

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

Step 6: In the **IPv4 CIDR block** box, enter 10.104.2.0/24.

Step 7: Click **Create subnet**.

Step 8: Repeat this procedure for all the subnets in Table 14.

5.3 Configure the Public Application Load Balancer

Now you create an internet-facing ALB to direct inbound web traffic to the web server instances.

Step 1: On the EC2 Service, navigate to **Load Balancing > Load Balancers**.

Step 2: Click **Create Load Balancer**, and then on **Application Load Balancer**, click **Create**.

Step 3: In the Basic Configuration pane, in the **Name** box, enter ExampleApplication-ALB.

Step 4: For **Scheme**, select **internet-facing**.

Step 5: In the **IP address type** list, choose **ipv4**.

Step 6: 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 7: In the Availability Zones pane, do the following:

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

Step 8: Click **Next: Configure Security Settings**, read the HTTP security warning, and then click **Next: Configure Security Settings**.

Step 9: In **Configure Security Groups > Assign a security group**, select **Create a new security group**, and then click **Next: Configure Routing**.

Step 10: In the **Target Group** list, choose **New target group**.

Step 11: In the **Name** box, enter web-instances.

Step 12: In the **Target type** list, choose **instance**.

Step 13: In the **Protocol** list, choose **HTTP,** and then click **Next: Register Targets**.

Step 14: Under **Instances**, select all the web server instances, and then click **Add to registered**.

Step 15: Click **Next: Review**.

Step 16: Click **Create**, and then click **Close**.

5.4 Create Gateway Load Balancer Endpoints

Now you add GWLB endpoints to the application VPC for inbound traffic. You must create the GWLB endpoints one at a time.

Step 1: On the VPC Service, navigate to **Virtual Private Cloud > Endpoints**, and then click **Create Endpoint**.

Step 2: For **Service Category**, choose **Find service by name**.

Step 3: In the **Service Name** box, paste in the value from Procedure 2.8, Step 8, and then click **Verify**.

Step 4: In the **VPC** list, choose web.

Step 5: For **Availability Zone**, select the us-west-2a availability zone only. Clear all other availability zones.

Step 6: In the **Subnet ID** list, choose web-gwlbe-2a.

Step 7: Click **Add Tag**.

Step 8: In the **Key** box, enter **Name**.

Step 9: In the **Value** box, enter web-2a.

Step 10: Click **Create endpoint**, and then click **Close**.

Next, you create the second endpoint.

Step 11: Navigate to **Virtual Private Cloud > Endpoints**, and then click **Create Endpoint**.

Step 12: For **Service Category**, choose **Find service by name**.

Step 13: In the **Service Name** box, paste the value from Procedure 2.8, Step 8, and then click **Verify**.

Step 14: In the **VPC** list, choose **web**.

Step 15: For **Availability Zone**, select the **us-west-2b** availability zone only. Clear all other availability zones.

Step 16: In the **Subnet ID** list, choose **web-gwlbe-2b**.

Step 17: Click **Add Tag**.

Step 18: In the **Key** box, enter **Name**.

Step 19: In the **Value** box, enter **web-2b**.

Step 20: Click **Create endpoint**, and then click **Close**.

Next, you accept the connection requests from the two endpoints you just created.

Step 21: Navigate to **Virtual Private Cloud > Endpoint Services**, and then select **security-GWLB**.

Step 22: In the bottom pane, on the Endpoint Connections tab, select the first endpoint.

Step 23: In the **Actions** list, choose **Accept endpoint connection request**.

Step 24: Click **Yes, accept**.

Step 25: Repeat Step 22 - Step 24 for the second endpoint.

5.5 Create VPC Route Tables

Now you configure route tables in the application VPC to direct traffic to the IGW or GWLB endpoints, as appropriate. You apply the web-igw route table as an edge association to the IGW instead of to a subnet.

Table 15 Routes in the application VPC

Route table name	Route destination	Target	Subnets assigned
web-alb-2a	0.0.0.0/0	GWLBe web-2a	web-alb-2a
web-alb-2b	0.0.0.0/0	GWLBe web-2b	web-alb-2b
web-gwlbe	0.0.0.0/0	IGW	web-gwlbe-2a, web-gwlbe-2b
web-igw	10.104.0.0/24 10.104.2.0/24	GWLBe web-2a	IGW (edge association)
	10.104.128.0/24 10.104.130.0/24	GWLBe web-2b	

Step 1: 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 web-alb-2a.

Step 4: In the **VPC** list, choose web.

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

Step 6: In the top pane, select web-alb-2a.

Step 7: In the bottom pane, on the Routes tab, click **Edit routes**.

Step 8: Click **Add route**, and then in the **Destination** box, enter **0.0.0.0/0**.

Step 9: Click in the **Target** box, and then choose the GWLB endpoint in the 2a availability zone.

Step 10: Click **Save routes**, and then click **Close**.

Destination	Target	Status	Propagated
10.104.0.0/16	local	active	No
0.0.0.0/0	vpce-0473b59a653d00e00	active	No

Step 11: On the Subnet Associations tab, click **Edit subnet associations**.

Step 12: In the list, choose web-alb-2a, and then click **Save**.

Filter by attributes or search by keyword 1 to 8 of 8

Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
subnet-0c9974bffb8db2b58 | web-instances-2b	10.104.128.0/...	-	rtb-06349fd5cd3c9549e
subnet-091fcf2bd225075bc | web-gwlbe-2a	10.104.3.0/24	-	rtb-05dc23179a049ae27
subnet-07d707f6aa97f577d | web-tgw-2a	10.104.1.0/24	-	Main
subnet-03b7431f42796d9ef | web-alb-2a	10.104.2.0/24	-	rtb-084c30fbe3ceae86e
subnet-09e59151e262e535d | web-instances-2a	10.104.0.0/24	-	rtb-06349fd5cd3c9549e
subnet-0803c4972eb35b153 | web-alb-2b	10.104.130.0/...	-	rtb-0e7c990835895b084
subnet-0000dda15fd1bbc56 | web-gwlbe-2b	10.104.131.0/...	-	rtb-05dc23179a049ae27
subnet-05fff981f6a9488d6 | web-tgw-2b	10.104.129.0/...	-	Main

Step 13: Repeat this procedure for the remaining route tables in Table 15.

5.6 Add Application Subinterface

Now you create a subinterface that you use to map the GWLB endpoints in the application VPC to the application's security zone. You use this subinterface and zone only for inbound traffic.

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

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

Step 3: Select the **Ethernet 1/1** row, and then click **Add Subinterface**.

Step 4: In the subinterface number box, enter 10.

Step 5: In the **Tag** box, enter 10.

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

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

Step 8: In the **Name** box, enter app01, and then click **OK**.

Step 9: On the IPv4 tab, for **Type**, select **DHCP Client**.

Step 10: Clear **Automatically create default route pointing to default gateway provided by server**, and then click **OK**.

Step 11: On the **Commit** menu, click **Commit and Push**, and then click **Commit and Push**.

5.7 Map the GWLB Endpoints to the Subinterface

After the VM-Series firewalls are deployed, you must map the GWLB endpoint to interface via an SSH connection to the VM-Series instance.

To connect to your instances, you need to set up your SSH connection to use the key pair created in Procedure 4.1.

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: Navigate to **Virtual Private Cloud > Endpoints**, and then copy the Endpoint ID for the web-2a and web-2b endpoints.

Step 4: 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 5: On the EC2 Service, navigate to **Instances > Instances**.

Step 6: In the top pane, select the vmseries-a instance.

Step 7: In the bottom pane, on the Details tab, copy the **Public IPv4 DNS** address.

Step 8: Use the admin username to open an SSH session to the FQDN for **vmseries-a**. For example: ssh -i paloaltonetworks-deployment.pem admin@ec2-35-81-15-68.us-west-2.compute.amazonaws.com

Step 9: If your console shows a security alert that the authenticity of the host can't be established, enter **YES** to continue connecting.

Step 10: At the CLI prompt, map both GWLB endpoints to the subinterface.

```
request plugins vm_series aws gwlb associate vpc-endpoint vpce-0473b59a653d00e00
interface ethernet1/1.10
```

```
request plugins vm_series aws gwlb associate vpc-endpoint vpce-0badde8efcfd7ae30
interface ethernet1/1.10
```

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

5.8 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 **app01**.

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

Step 6: In the **Destination Zone** box, enter **app01**.

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

Step 8: In the search box, enter **web-browsing**, and then in the results list, select **web-browsing**.

Step 9: On the Actions tab, in the **Action** list, choose **Allow**.

Step 10: In the **Log Forwarding** list, choose **Forward-to-Cortex-Data-Lake**, and then click **OK**.

Step 11: On the **Commit** menu, click **Commit and Push**, and then click **Commit and Push**.

Procedures

Deploying the Centralized Inbound Security Option

6.1 Configure the Public Application Load Balancer

6.2 Modify Inbound Security Group

6.3 Create VPC Route Table

6.4 Configure the NAT Policy

6.5 Configure the Security Policy

6.6 Locate the Inbound Load-Balancer DNS Name

6.1 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 Service, 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 security.
- Select us-west-2a, and then in the list of subnet IDs, choose security-public-2a.
- Select us-west-2b, and then in the list of subnet IDs, choose security-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 security-firewall-public. Ensure that only the security-firewall-public security group is selected, and then click **Next: Configure Routing**.

Security Group ID	Name	Description
sg-01c5430d5672d5e1f	default	default VPC security group
sg-025f2e7fcd31a0166	security-firewall-mgmt	Allow inbound management to the firewall
sg-0eee85a78bc710b15	security-firewall-private	Allow inbound traffic to private interface
sg-0cb50403f9102eed2	security-firewall-public	Allowed inbound applications from the internet

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

Step 12: In the **Name** box, enter inbound-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 **10.100.2.10**, and then click **Add to list**.

Step 18: In the **IP** box, enter **10.100.66.10**, click **Add to list**, and then click **Next: Review**.

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

6.2 Modify Inbound Security Group

You must modify the security group that you configured at deployment. By default, this security group doesn't allow inbound traffic. Modify it so that web traffic is allowed inbound to the firewall.

Step 1: Navigate to **Security > Security Groups**, and then click security-firewall-public.

Step 2: In the bottom pane, on the Inbound rules tab, click **Edit inbound rules**.

Step 3: In the Inbound rules pane, click **Add Rule**.

Step 4: In the **Type** list, choose HTTP.

Step 5: In the **Source Type** list, choose **Anywhere**, and then click **Save rules**.

6.3 Create VPC Route Table

Now you configure a route table in the security VPC to direct traffic from the firewall's private data plane interface to the TGW.

Table 16 Routes to the TGW

Route table name	Route destination	Target	Subnets assigned
security-fw	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	TGW	security-fw-2a, security-fw-2b

Step 1: 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 security-fw.

Step 4: In the **VPC** list, choose security.

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

Step 6: In the top pane, select security-fw.

Step 7: In the bottom pane, on the Routes tab, click **Edit routes**.

Step 8: Click **Add route**, and then in the **Destination** box, enter **10.0.0.0/8**.

Step 9: Click in the **Target** box, and then choose the TGW.

Step 10: Click **Save routes**, and then click **Close**.

Destination	Target	Status	Propagated
10.100.0.0/16	local	active	No
10.0.0.0/8	tgw-08ce58fb1fc6c9b28	active	No
172.16.0.0/12	tgw-08ce58fb1fc6c9b28	active	No
192.168.0.0/16	tgw-08ce58fb1fc6c9b28	active	No

Step 11: On the Subnet Associations tab, click **Edit subnet associations**.

Step 12: In the list, choose subnets security-fw-2a and security-fw-2b, and then click **Save**.

Step 13: Repeat this procedure for the remaining route tables in Table 16.

6.4 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.

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-example-application.

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

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

Step 6: In the **Destination Interface** list, choose **ethernet1/2**.

Step 7: In the **Service** list, choose **service-http**.

Step 8: On the Translated Packet tab, in the Source Address Translation pane, in the **Translation Type** list, choose **Dynamic IP And Port**.

Step 9: In the **Address Type** list, choose **Interface Address**.

Step 10: In the **Interface** list, choose **ethernet 1/1**.

Step 11: In the **Translation Type** list, choose **Dynamic IP (with session distribution)**.

Step 12: In the **Translated Address** list, choose **New Address**. The New Address object windows appears.

Step 13: In the **Name** box, enter **internal-ALB**.

Step 14: Clear **Shared**.

Step 15: In the **Type** list, choose **FQDN**.

Step 16: In the **FDQN** box, enter internal-ALB-16693.us-west-2.elb.amazonaws.com, and then click **OK**.

> **Note**
>
> You can find the FQDN of the load balancer in the EC2 service. Navigate to **Load Balancing** > **Load Balancers**, and then look in the DNS name column.

6.5 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 internal.

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

Step 8: In the search box, enter web-browsing, and then in the results list, select **web-browsing**.

Step 9: On the Actions tab, in the **Action** list, choose **Allow**.

Step 10: In the **Log Forwarding** list, choose Forward-to-Cortex-Data-Lake, and then click **OK**.

Step 11: On the **Commit** menu, click **Commit and Push**, and then click **Commit and Push**.

6.6 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 Service, 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.

Deploying Backhaul VPN to On-Premises Services

In this section, you configure connectivity to the transit gateway in AWS from an on-premises next-generation firewall or high-availability pair. This design provides configuration for peering the on-premises firewall to the transit gateway with dynamic routing using BGP.

This section assumes:

- The on-premises firewall is an operational Palo Alto Networks next-generation firewall running PAN-OS.
- There is a public IP address assigned to the on-premises firewall to which the VPN tunnels can peer.
- The on-premises firewall advertises reachability to the 10.5.0.0/16 local network.
- There are no additional NAT or security policies needed or configured on the on-premises firewalls.

Procedures

Configuring VPN Attachments

7.1 Create a Customer Gateway

7.2 Create Transit Gateway VPN Attachments

7.3 Associate Attachments to the Route Tables

7.4 Record the Public IP Address of the VPN Tunnels

7.1 Create a Customer Gateway

The on-premises firewall uses two VPN connections to the TGW. The VPN connections use dynamic routing with BGP and equal cost multipath to use multiple tunnels.

In order to complete this procedure, you must have the public IP address of the on-premises firewall's public interface.

Step 1: On the VPC service, navigate to **Virtual Private Network (VPN) > Customer Gateways**, and then click **Create Customer Gateway**.

Step 2: In the **Name** box, enter on-premises-firewall.

Step 3: For **Routing**, select **Dynamic**.

Step 4: In the **BGP ASN** box, enter 65501.

Step 5: In the **IP Address** box, enter the IP address your recorded from your on-premises firewall (example: 199.167.52.150), and then click **Create Customer Gateway**.

7.2 Create Transit Gateway VPN Attachments

Now you create a VPN attachment for the on-premises firewall. Creating the VPN attachments creates the VPN connection in AWS.

Table 17 Tunnel options

CGW	Tunnel 1 inside IP CIDR	Tunnel 2 inside IP CIDR
on-premises-firewall	169.254.1.4/30	169.254.1.8/30

Step 1: On the VPC service, navigate to **Transit Gateways > Transit Gateway Attachments**, and then click **Create Transit Gateway Attachment**.

Step 2: In the **Transit Gateway ID** list, choose TGW.

Step 3: In the VPN Attachment section, for **Attachment type**, select **VPN**.

Step 4: For **Customer Gateway**, select **Existing**.

Step 5: In the **Customer Gateway ID** list, choose on-premises-firewall.

Step 6: For **Routing options**, select **Dynamic**.

Next, you configure the IP addressing and pre-shared key for each of the two IPSec tunnels to each CGW.

Step 7: In the Tunnel Options section, in the **Inside IP CIDR for Tunnel 1** box, enter 169.254.1.4/30.

Step 8: In the **Pre-Shared Key for Tunnel 1** box, enter TGWrefArch.

Step 9: In the **Inside IP CIDR for Tunnel 2** box, enter 169.254.1.8/30.

Step 10: In the **Pre-Shared Key for Tunnel 2** box, enter TGWrefArch.

Step 11: Click **Create attachment**, and then click **Close**.

Step 12: In the Transit Gateway Attachments pane, hover your cursor over the **Name** field next to the new attachment. A pencil image appears. Click the **pencil**.

Step 13: In the **Name** box, enter on-premises-firewall, and then select the checkmark.

7.3 Associate Attachments to the Route Tables

Transit gateway route tables are routing domains, and you can control which routes are available to a spoke VPC based on the route table with which it is associated. You can control the routes available in a routing domain by selectively propagating the attachments into it.

First, you associate the VPN attachment to the spokes route table, which allows on-premises firewall to reach all the VPCs connected to the transit gateway through the east-west firewalls.

Step 1: Navigate to **Transit Gateways > Transit Gateway Route Tables**.

Step 2: In the top pane, select Spokes.

Step 3: In the bottom pane, on the Associations tab, click **Create Association**. The Create Association windows opens.

Step 4: In the **Choose attachment to associate** list, choose **on-premises-firewall**.

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

Next, you propagate the routes from the on-premises firewall into the security route table.

Step 6: In the top pane, select **Security**.

Step 7: In the bottom pane, on the Propagations tab, click **Create Propagation**.

Step 8: In the **Choose attachment to propagate** list, choose **on-premises-firewall**.

Step 9: Click **Create propagation**, and then click **Close**.

7.4 Record the Public IP Address of the VPN Tunnels

In this procedure, you obtain the public IP address for each of the tunnels, which you use to configure the VPN tunnels on the firewalls.

Step 1: Navigate to **Virtual Private Network (VPN) > Site-to-Site VPN Connections**.

Step 2: In the top pane, select **on-premises-firewall**.

Step 3: In the bottom pane, on the Tunnel Details tab, record the **Outside IP Address** for both the tunnels.

Procedures

Configuring an On-Premises Firewall for VPN Connectivity to the Transit Gateway

8.1 Configure IKE and IPSec

8.2 Configure the Zone and Tunnel Interface

8.3 Create an IKE Gateway to the Transit Gateway

8.4 Create an IPSec Tunnel to the Transit Gateway

8.5 Configure a Route Redistribution Profile

8.6 Configure BGP Peering with the Transit Gateway

8.7 Configure the NAT and Security Policies

8.1 Configure IKE and IPSec

Now you configure IKE and IPSec settings based on the default AWS parameters.

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

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

Step 3: In the DH Group pane, click **Add**, and then choose group2.

Step 4: In the Authentication pane, click **Add**, and then choose sha1.

Step 5: In the Encryption pane, click **Add**, and then choose aes-128-cbc.

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

Step 7: In **Network** > **Network Profiles** > **IPSec Crypto**, click **Add**.

Step 8: In the **Name** box, enter AWS-IPSEC.

Step 9: In the Encryption pane, click **Add**, and then choose aes-128-cbc.

Step 10: In the Authentication pane, click **Add**, and then choose sha1.

Step 11: In the **DH Group** list, choose group2.

Step 12: In the **Lifetime** list, choose Second, enter 3600, and then click **OK**.

Step 13: Click **Commit**, and then click **Commit** again.

8.2 Configure the 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 TGW.

Table 18 Object and tunnel details

Name	Public IP address	Tunnel interface	Tunnel IP address
TGW-a	44.231.198.10	tunnel.1	169.254.1.6/30
TGW-b	54.71.121.107	tunnel.2	169.254.1.10/30

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

First, you configure an address object for the TGW with its public IP address.

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

Step 3: In the **Name** box, enter TGW-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 TGW-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 169.254.1.6/30.

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 18.

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

8.3 Create an IKE Gateway to the Transit Gateway

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

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

Step 3: In the **Version** list, choose **IKEv1 only mode**.

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

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

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

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

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 AWS-IKE.

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

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

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

Step 15: Repeat this procedure for the second IKE gateway.

8.4 Create an IPSec Tunnel to the Transit Gateway

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 TGW-a-TUN.

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

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

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

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 Transit Gateway

In this procedure, you deploy peer BGP routing on the on-premises firewalls for connectivity to the AWS TGW. 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 transit gateway. 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 19 BGP peer group parameters

Peer group name	Peer name	Peer AS	Interface	Local IP address	Peer IP address
AWS	TGW-a	64512	tunnel.1	169.254.1.6/30	169.254.1.5
	TGW-b	64512	tunnel.2	169.254.1.10/30	169.254.1.9

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**.

Step 10: On the Peer Group tab, click **Add**.

Step 11: In the Peer Group pane, in the **Name** box, enter AWS.

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 TGW-a.

Step 16: In the **Peer AS** box, enter 64512.

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

Step 18: In the **IP** list, choose 169.254.1.6/30.

Step 19: In the **Peer Address** box, enter 169.254.1.5.

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, click **OK**, and then click **OK** again.

Step 22: Repeat this procedure for the TGW-b peer in Table 19.

Step 23: 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."

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

© 2021 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at http://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies. Palo Alto Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

You can use the feedback form to send comments about this guide.

B-000113P-1-21a