# *Auto Scaling the VM-Series Firewall on Google Cloud Platform*

techDOCS

paloalto NETWORKS

## Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

## About the Documentation

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

## Copyright

## Last Revised

November 7, 2019

# Table of Contents

# Auto Scaling the VM-Series Firewall on Google Cloud Platform

The Panorama plugin for Google Cloud Platform (GCP) version 2.0 Beta enables Panorama to manage VM-Series firewalls securing VM monitoring and auto scaling deployments in GCP.

This topic focuses on an auto scaling use case that requires Google shared VPC technology to create a common VPC network composed of a host project containing shared VPC networks and the VM-Series firewalls, and a service project containing a sample application deployment. Palo Alto networks supplies templates to help you deploy the VM-Series firewalls in the host project and deploy the sample application in the service project.

Using Panorama to maintain your GCP managed instance groups has the following benefits:

- BYOL and PAYG licenses can be used for the VM-Series firewalls. If you choose BYOL your deployment can support de-licensing of instances in response to a scale-down event.
- Panorama automatically monitors the VM-Series firewall status and automatically deregisters a VM-Series firewall when it is automatically removed.
- With Panorama, you can create application enablement policies that protect and control the network. Using Panorama for centralized policy and firewall management increases operational efficiency in managing and maintaining a distributed network of firewalls.

- Auto Scaling Components for Google Cloud Platform
- Deploy GCP Auto Scaling Templates
- Known Issues
- Get Help

# Auto Scaling Components for Google Cloud Platform

- Software Version Requirements
- GCP Auto Scaling Prerequisites

## Software Version Requirements

- Panorama—Panorama physical or virtual appliance running version 9.0.4 or later in Panorama mode, and the following plugins.

  - VM-Series plugin version 1.0.4 or later.
  - Panorama plugin for GCP version 2.0.

    ✏️ *You cannot upgrade the GCP plugin from version 1.0 to version 2.0.*

    The GCP plugin takes care of the interactions required to license, bootstrap and configure the VM-Series firewalls using device groups and template stacks on Panorama, and programs the NAT rules to direct traffic to the firewalls.

    Obtain the Panorama plugin for GCP from the auto scaling beta site (registration required) and install it as described in Prepare the Panorama Plugin.

  The Panorama appliance must be able to communicate with the VM-Series firewalls deployed on your GCP shared VPC infrastructure to enable centralized management of the auto scaling VM-Series firewalls.

- VM-Series Firewalls—The PAN-OS version for the auto scaling set of VM-Series firewalls is PAN-OS 8.1.4 or later. The Panorama must be running a PAN-OS version that is the same or later than the managed firewalls.

  The managed firewalls require a valid license.

- Templates—Download the templates for deploying the auto scaling VM-Series firewall and the sample application template from GitHub. The zip file contains separate zip files for the firewall and application templates.

  Palo Alto Networks provides the templates to deploy VM-Series firewall instances in the host project so you can secure inbound traffic for a GCP application deployment in the service project. The firewall templates create a Cloud Pub/Sub service that relays information from GCP to the Panorama plugin for GCP. With this infrastructure in place, the plugin can leverage dynamic address groups to apply security policy on inbound traffic routed to services running on GCP, and use auto scale metrics to deploy VM-Series firewalls to meet increased demand for application workload resources or to eliminate firewalls that are no longer needed.

## GCP Auto Scaling Prerequisites

The auto scaling deployment on GCP requires a shared VPC with host and service projects that use a common VPC network. In this topology, the host project contains the networks and VM-Series firewalls that secure traffic to your applications, which are deployed in the service project.

Complete the following tasks before you deploy the auto scaling templates.

- Prepare a Host Project
- Prepare a Service Project

- Prepare the Panorama Plugin
- Prepare a VM-Series Firewall Bootstrap Package

> 💡 *If you have not done so,* install *the Google Cloud SDK. You will use the command line interface to deploy the firewall template and the application template, and to attach the service project to the host project.*

## Prepare a Host Project

You need a host project and a service project to form the shared VPC topology that supports the firewall and application templates. You can create a new host project or prepare an existing project to act as your host.

To set up the Shared VPC an organization admin must grant the host project administrator the Shared VPC Admin role. The Shared VPC Admin can enable a project to act as a host, and grant the Service Project Admin role to the service project administrator. Review the GCP documentation on Administrators and IAM roles.

STEP 1 | In the GCP console, create a GCP project. If you want to use an existing one, go to the next step.

To create a new project, select your organization or **No organization**, click **New Project** and fill in your project information. Note, this is your only chance to **EDIT** the project ID.

STEP 2 | Enable GCP service APIs.
1. Select the host project and from the Navigation menu, select **APIs & Services**.
2. Search for and view each API below. **ENABLE** any APIs that do not display the "API enabled" status.

   - ❑ Cloud Pub/Sub API
   - ❑ Cloud Deployment Manager API
   - ❑ Cloud Storage API
   - ❑ Compute Engine API
   - ❑ Google Compute Engine Instance Group Manager API
   - ❑ Google Compute Engine Instance Group Updater API
   - ❑ Google Compute Engine Instance Groups API
   - ❑ Kubernetes Engine API
   - ❑ Stackdriver API
   - ❑ Stackdriver Logging API
   - ❑ Stackdriver Monitoring API

STEP 3 | Create a service account for deploying the VM-Series firewall, and assign the IAM roles required for auto scaling. This service account email must be added to the VM-Series firewall .yaml file.
1. In the GCP console select **IAM & Admin** > **Service accounts** and select **+CREATE SERVICE ACCOUNT**.

   Fill in the service account details and **CREATE**.
2. Give the service account permissions to auto scale resources in this project.

   Add the following roles:

   - ❑ Compute Engine > Compute Admin
   - ❑ Kubernetes Engine > Kubernetes Engine Cluster Admin
   - ❑ Kubernetes Engine > Kubernetes Engine Cluster Viewer

- ❑ Deployment Manager > Deployment Manager Editor
- ❑ Monitoring > Monitoring Metric Writer
- ❑ Pub/Sub > Admin
- ❑ Stackdriver > Stackdriver Accounts Editor
- ❑ Storage > Storage Admin

**Continue** when you are finished.

3. (Optional) Add email addresses to grant users or administrators access to this service account.
4. Click **DONE**.

STEP 4 | Create a service account that a Panorama administrator can use to interact with the host project.

1. Give the service account the following roles:

- ❑ Compute Engine > Compute Viewer
- ❑ Pub/Sub > Admin

2. Download the private key in JSON form, and store it in a safe location.You will need this key when you Configure the Panorama Plugin for GCP.

💡 *In the CLI, set your project to the host project you just created.*

```
gcloud set project <your-autoscale-host-project-name>
```

*Create a configuration for auto scaling. Your new config is automatically activated unless you disable activation.*

```
gcloud config configurations create CONFIGURATION_NAME
gcloud config list
```

## *Prepare a Service Project*

Create a separate service project, or choose an existing project, for your application.

To learn more about host and service projects in a shared VPC, see the Shared VPC Overview, and review the Administrators and IAM roles. A host project administrator must have the proper role to set up the Shared VPC, make the application project a service project for the host project. See the instructions in Provisioning Shared VPC.

Create a service account for deploying an application and assign the IAM roles required for auto scaling.

1. In the GCP console select **IAM & Admin** > **Service accounts** and select **+CREATE SERVICE ACCOUNT**.

Fill in the service account details and **CREATE**.

2. Give the service account permissions to auto scale resources in this project.

Add the following roles:

- ❑ Compute Engine > Compute Admin
- ❑ Compute Engine > Compute Network User
- ❑ Project > Editor
- ❑ Pub/Sub > Admin

**Continue** when you are finished.

3. (Optional) Add email addresses to grant users or administrators access to this application.
4. Download a JSON file with a private key.

   Click **+CREATE KEY**, select JSON, click **CREATE**, and store the key in a secure location.
5. Click **DONE**.

## Prepare the Panorama Plugin

Install the Panorama plugin and create assets to support the auto scaling firewall deployment.

STEP 1 | Obtain the Panorama plugin for GCP from the auto scaling beta site (registration required).

STEP 2 | In Panorama, select **Panorama** > **Device Deployment** > **Plugins**, **upload** the plugin, and **Install** it. After the installation you can see the plugin in the Panorama dashboard **General Information** list, and in the Panorama context, view the Google Cloud Platform in the list of plugins, with the Setup, VM Monitoring, and AutoScaling topics.

STEP 3 | On Panorama create the following resources:
1. Add a template, and a template stack and commit the changes.
2. Create Untrust and Trust zones.
3. Create a virtual router.
4. In a template, create two Layer 3 interfaces—ethernet1/1 (Untrust) and ethernet1/2 (Trust) interfaces.

   - ethernet1/1 (Untrust)—Enable DHCP Client and Automatically create default route pointing to default gateway provided by server (enabled by default)
   - ethernet1/2 (Trust)—Enable DHCP Client and disable Automatically create default route pointing to default gateway provided by server
5. Assign both interfaces to the same virtual router.
6. Create an Administrator to log in to the VM-Series firewall.
7. Configure the template stack you created earlier. Select **Device** > **VM-Series** > **Google** and **Enable Publish PAN-OS metrics to Stackdriver**.
8. Add Device Groups and reference the template created above (a VM can be a member of only one Device Group across all plugins).
9. Commit your changes.

## Prepare a VM-Series Firewall Bootstrap Package

The firewall templates include a sample `init-cfg.txt` file. You must customize this file for your deployment and

STEP 1 | Set up a Google storage bucket with the folders required to Bootstrap the VM-Series Firewall on Google Cloud Platform. You can use an existing bootstrap package or create a new bootstrap package, for these folders.

STEP 2 | Edit the values in the `init-cfg.txt` file to customize the file for your environment.

The firewall templates include a sample `init-cfg.txt` file.

| Parameter | Value | Comment |
|---|---|---|
| type | dhcp-client | |
| op-command-modes | mgmt-interface-swap | Required in this Beta release. |

| Parameter | Value | Comment |
|---|---|---|
| hostname | <pa-vm> | Optional name you assigned when you prepared the host project. Only required if a specific host is necessary, and dhcp-send-hostname is no. |
| vm-auth-key | <vmauthkey> | A key that Panorama must validate before adding a firewall as a managed device. See Generate the VM Auth Key On Panorama. |
| panorama-server | <panorama-ip> | The IP address of the Panorama management device you configured in Prepare the Panorama Plugin. |
| tplname | <tmplstk-name> | The template stack you created in Prepare the Panorama Plugin. |
| dgname | <dg-name> | The name of the Device Group you created in the Panorama Plugin for GCP. |
| dns-primary | 8.8.8.8 | Your primary DNS. |
| dns-secondary | 208.67.222.222 | Your secondary DNS. |
| dhcp-send-hostname | yes | Leave as is. |
| dhcp-send-client-id | yes | Leave as is. |
| dhcp-accept-server-hostname | yes | Leave as is. |
| dhcp-accept-server-domain | yes | Leave as is. |

STEP 3 | Upload your edited `init-cfg.txt` file to the `/config` folder in your bootstrap package.

STEP 4 | If you are using BYOL, create a text file named `authcodes` (no extension), add your auth code, and upload the file to the `/license` folder.

# Deploy GCP Auto Scaling Templates

You can download the Palo Alto Networks auto scaling templates from https://github.com/PaloAltoNetworks/GCP-AutoScaling. The zip file contains separate zips for firewall and application templates. Each template directory contains many files but you only need to edit the YAML files.

*This beta supports greenfield deployments only.*

**Firewall Templates**

The firewall templates create VM-Series firewalls and other resources for a greenfield deployment. It creates new networks and the familiar subnetworks for the VM-Series firewall: management, untrust, and trust. The firewall templates also deploy a Cloud Pub/Sub messaging service to handle communications with your firewall instance group.

- Application Load Balancer (HTTP External Load Balancer)

  HTTP external load balancer is a proxy-based load balancer that performs SNAT and DNAT on the inbound traffic from Internet. The HTTP load balancer is designed to support only the 80, 8080 and 443 TCP ports.

  To support multiple applications using HTTP load balancer in load balancer sandwich architecture, we can use the GCP HTTP load balancer urlMap and namedPort to map different URLs to different ports in the load balancer. In turn, the Firewall can translate the ports to different applications which is represented by one internal load balancer per application.

  To customize the firewall template, edit `vm-series-fw-nlb.yaml` or `vm-series-fw-alb.yaml`.
- Network Load Balancer (TCP Load Balancer)

  TCP load balancer is a non-proxy based load balancer, which means it doesn't perform NATing on inbound traffic from the Internet.

  TCP load balancer in GCP allows adding multiple frontend IP addresses with an arbitrary port, making it possible to support multiple applications.

  Another advantage of TCP load balancer is that the original client IP address is preserved, which is desirable for some applications.

  To customize application load balancer template, edit `vm-series-fw-nlb.yaml` or `vm-series-fw-alb.yaml`.

**Application Templates**

The application templates provide a sample application. Customize these templates so that your application servers can subscribe to the Pub/Sub service and communicate with your VM-Series firewalls and the GCP plugin on Panorama.

To customize the application template, edit `apps.yaml`

- Deploy the Firewall Template
- Configure the Shared VPC
- Configure the Panorama Plugin for GCP
- Deploy the Application Template
- Onboard a New Application

# Deploy the Firewall Template

Edit the Firewall template from the host project.

Edit the `vm-series-fw-*.yaml` environment variables to reflect your cloud environment.

```
properties:
    region: us-east1
zones:
  -us-east1-b
  # Do not modify the lb-type field.
  lb-type: nlb
  cloud-nat: yes
  forwarding-rule-port: 80
```

```
#urlPath-namedPort-maps:
    - appName: app1
```

```
    bootstrap-bucket: bootstrap-1
    image: vmseries-byol-814
    machine-type: n1-standard-4
```

For the service-account, supply the email address for the host project service account you created earlier (step 3).

```
    service-account: username-autoscale@gcp-autoscale-
host.iam.gserviceaccount.com
```

The fw-instance-tag value will be the managed instance group name in the deployment.

```
    fw-instance-tag: vm-series-fw
```

Choose one metric. Possible values are: panSessionActive, panSessionUtilization, DataPlaneCPUUtilizationPct, DataPlanePacketBufferUtilization, or panSessionUtilization

```
metric: custom.googleapis.com/VMSeries/panSessionActive
max-size: 2
min-size: 1
target-type: GAUGE
util-target: 100
```

min-size and max-size represent the minimum and maximum number of firewalls in an instance group.

```
# Greenfield deployment
mgmt-network-cidr: 172.22.2.0/24
untrust-network-cidr: 172.22.1.0/24
trust-network-cidr: 172.22.3.0/24
mgmt-network-access-source-range:
- 199.167.54.229/32
- 199.167.52.5/32
mgmt-network-access-ports:
- 22
- 443
```

**STEP 2 |** Deploy the firewall template.

```
gcloud deployment-manager deployments create <firewall-deployment-name>
--config vm-series-fw-nlb.yaml --automatic-rollback-on-error
```

Take note of the outputs the CLI prints after the deployment: The subnet names, the deployment name, and the Panorama Pub/Sub topic name. You need these values to configure the Shared VPC and for the application template deployment.

The firewall deployment name must be configured in the Panorama plugin for GCP auto scaling definition.

## Configure the Shared VPC

After the firewall template is deployed in the host project, configure the service project that supports your applications. An administrator with Shared VPC credentials performs these tasks from the host project. To understand more about the host project and service projects in the context of shared VPC, see the Shared VPC Overview.

**STEP 1 |** Create a shared VPC using the Trust VPC created when you deployed the firewall template.

Set up Shared VPC for the host (firewall) project:

```
gcloud compute shared-vpc enable HOST_PROJECT_ID
```

**STEP 2 |** Make the application project a service project for the host project.

Add the service account email (<project number>@cloudservices.gserviceaccount.com) from Service/ application project administrator as a member in host project with below role:

- Compute Admin
- Compute Network User
- Pub/Sub Admin

**STEP 3 |** Attach the service/application project to the host project.

```
gcloud compute shared-vpc associated-projects add SERVICE_PROJECT_ID --host-
project HOST_PROJECT_ID
```

Additional options are available to share only specific subnets, rather than all subnets in the host project.

## Configure the Panorama Plugin for GCP

**STEP 1 |** Log in to the Panorama web interface and select **Panorama** > **Google Cloud Platform** > **Setup**.

**STEP 2 |** **Add** a GCP Service Account Credential.

- Name the service account credential.
- (Optional) Enter a description of the service account.
- **Browse** to upload the JSON file generated you created when you created the GCP service account for Panorama autoscaling.

  *You can only use a service account once. Do not create multiple credentials from a single JSON file.*

**STEP 3 |** **Commit** the changes on Panorama.

**STEP 4 |** Select **Panorama** > **Google Cloud Platform** > **AutoScaling**.

**STEP 5 | Add** a GCP AutoScaling configuration.

1. For the **Firewall Deployment Name** supply the name from 2
2. Add a **Description** for this firewall.
3. Select the GCP service account credential for your host project (from step 2).
4. Select a template stack for the VM-Series firewalls deployed with the firewall template.

## Deploy the Application Template

The Service project adminstrator deploys the Application template from the service project.

**STEP 1 |** Create a separate application project (service project) to deploy the application.

**STEP 2 |** Prepare the application template.

```
properties:
   host-project: gcp-autoscale-host
   fw-deployment-name: fw-template-9
   region: us-east1
   zones:
     - us-east1-b
     - us-east1-c
```

**STEP 3 |** Deploy a new application with the application template and define a label for the named port.

```
gcloud deployment-manager deployments create <your-template>--config
apps.yaml --labels named-port=82--automatic-rollback-on-error
```

## Onboard a New Application

To secure an application you have deployed using an external load balancer and an autoscaled VM-Series firewall deployment, follow these steps. For every application you must supply the application name, the named ports, and the path.

**STEP 1 |** Prepare new named port and URL path to be added to the HTTP external load balancer created when you deployed the firewall template.

**STEP 2 |** Update all instance groups named-ports with an additional service name and port values for app2 and app3.

```
gcloud compute instance-groups set-named-ports
 fw-template2-fw-igm-us-east1-b
--zone us-east1-b --named-ports=app1:80,app2:81,app3:82

gcloud compute instance-groups set-named-ports
 fw-template2-fw-igm-us-east1-c
--zone us-east1-c --named-ports=app1:80,app2:81,app3:82
```

**STEP 3 |** Create a new http-health-check.

```
gcloud compute backend-services create fw-template2-backend-app3
```

```
--protocol="HTTP"
--port-name=app3
--http-health-checks=fw-template2-healthcheck-app3
--load-balancing-scheme="EXTERNAL"
--global
```

**STEP 4 |** Create a new backend service with the port-name created earlier on the HTTP external load balancer.

```
gcloud compute backend-services create fw-template2-backend-app3
--protocol="HTTP" --port-name=app3
--http-health-checks=fw-template2-healthcheck-app3 --load-balancing-
scheme="EXTERNAL" --global
```

Check to see if it is visible.

```
gcloud compute backend-services list
```

**STEP 5 |** Edit url-maps and add new path rule. For example:

```
- paths:
    - /app3
    - /app3/*service:
    https://www.googleapis.com/compute/v1/projects/stellar-cumulus-95806/
global/backendServices/fw-template2-backend-app3
```

```
gcloud compute url-maps edit fw-template2-ext-loadbalancer
```

**STEP 6 |** To secure this application with the VM-Series firewall, manually trigger the pub/sub message through the gcloud CLI. This sends a message to the topic created in the firewall template.

```
gcloud pubsub topics publish ptemplate-path>/fw-template-4-gcp-autoscale-
host-panorama-apps-deployment
--attribute ilb-ip=172.22.3.6,app-deployment-name=fw-template-4-app1,
ilb-port=80,named-port=80,fw-deployment-name=fw-template-4,
host-project=gcp-autoscale-host,type=ADD-APP --message "ADD-APP"
```

> *After you onboard an application you can view it in the Panorama plugin for GCP. Select Panorama > Google Cloud Platform > Autoscaling > Show Status. The Details column displays if you have deployed an application. Click the Status link. NAT Rule Programmed is True if a NAT rule exists, and Protected is True when an application has successfully onboarded.*

**STEP 7 |** To update application attributes, such as ilb-ip, ilb-port, or named-port, issue the pubsub command:

```
gcloud pubsub topics publish <template-path>/fw-template-4-gcp-autoscale-
host-panorama-apps-deployment
--attribute ilb-ip=172.22.3.7,app-deployment-name=<your-app>,
ilb-port=81,named-port=80,
fw-deployment-name=fw-template-4,host-project=gcp-autoscale-host,
```

```
type=UPDATE-APP --message "UPDATE-APP"
```

STEP 8 | To stop securing the application, issue the following command:

```
gcloud pubsub topics publish <template-path>/fw-template-3-vmseries-
dev-242318-panorama-apps-deployment --attribute ilb-ip=172.22.3.20,app-
deployment-name=fw-templ-3-app-1,ilb-port=80,
named-port=80,fw-deployment-name=<your-deployment>,type=DEL-APP
--message "DEL-APP"
```

# Known Issues

This plugin supports VM Monitoring and Auto Scaling tasks. Please review the known issues for the Panorama plugin for GCP version 2.0 Beta.

- Auto Scaling
- VM Monitoring
- General

**Auto Scaling**

| Issue ID | Description |
|---|---|
| PAN-129356 | Panorama management server sometimes crashes and restarts when you add a device. |
| PLUG-2940 | When the **Push NAT Rules automatically** is disabled, then the onboarded application is not added to the database and is not displayed in **Panorama** > **Google Cloud Platform** > **Auto Scaling**. |
| PLUG-2731 | When you add a new auto scaling configuration, the plugin creates a new NAT rule and address objects but does not commit the change to the associated Device Group as expected. Although partial commit does not occur, the following message is displayed:<br><br>`Partial changes to commit:`<br>`changes to configuration by all administrators`<br>`Changes to device-group configuration: (your-`<br>`configuration)` |
| PLUG-2692 | On Panorama, the GCP plugin gets a message from Pub/Sub, generates the configuration, initializes a commit, then pushes the configuration to the device. Although this process is shown to be successful on Panorama, the shared policy remains out-of-sync for all managed firewalls so the NAT rules aren't pushed. After the initial commit, you must manually push the configuration to your managed firewalls. |

**VM Monitoring**

| Issue ID | Description |
|---|---|
| PLUG-2716 | If a monitoring definition cannot retrieve tags, the **Status** column displays **Fail** but there is no related error message. Use the following CLI command to get status information:<br><br>`show plugins gcp vm-mon-status` |

| Issue ID | Description |
|---|---|
| PLUG-2650 | A GCP service account and its related project can be associated with only one monitoring definition. At this time the Panorama web interface does not prevent you from making multiple monitoring definitions for the same project. |
| PLUG-2499 | You must ensure that a Device Group is a member of only one notify group. Your Panorama can have many plugins installed—for example plugins for AWS, Azure, GCP, and more. If you add a Device Group to multiple notify groups, tags learned by one plugin are overwritten by another. |

**General**

| Issue ID | Description |
|---|---|
| | At this time the GCP plugin for Panorama version 2.0.0 Beta version supports VM Monitoring and Auto Scaling, but does not support Google Kubernetes Engine (GKE). Do not use the GCP Plugin web interface for **Setup** > **GKE Service Account**. |
| PLUG-2380 | The Google Cloud Platform plugin cannot be upgraded from 1.0.0 to 2.0.0. |
| PLUG-2618 | You cannot use the Panorama CLI to configure a GCP service account object. You must use the web interface. |
| PLUG-2657 | A GCP service account credential file can be used only once. At this time the Panorama web interface does not prevent making multiple Panorama service account objects with the same credential. |
| PLUG-1694 | (PAN-OS VMs with PAYG licenses) Your pay-as-you-go (PAYG) license is not retained when you upgrade a PAN-OS 8.1 release to PAN-OS 9.0. To recover your license after an upgrade to 9.0, upgrade the VM-Series plugin to 1.0.2 or later, and reboot the firewall. If you have manually installed the VM-Series plugin on Panorama, ensure that the version is the same or later than the version on your managed devices. |

# Get Help

The following topics provide information on where to find more about this release and how to request support:

- Related Documentation
- Requesting Support

## Related Documentation

Refer to the following documentation on https://docs.paloaltonetworks.com/ or search the documentation for more information on our products:

- **Palo Alto Networks Compatibility Matrix**—Provides compatibility and interoperability information for Palo Alto Networks hardware and software products.
- **Panorama Administrator's Guide**—Provides the basic framework to quickly set up the Panorama™ virtual appliance or an M-Series appliance running version 8.1 or 9.0 for centralized administration of the Palo Alto Networks firewalls.
- **PAN-OS Administrator's Guide**—Provides the concepts and solutions to get the most out of your Palo Alto Networks next-generation firewalls. This includes taking you through the initial configuration and basic set up on your Palo Alto Networks firewalls for PAN-OS 8.1 or 9.0.
- **VM-Series Deployment Guide**—Provides deployment concepts and workflows for setting up, licensing, and managing the VM-Series firewall on public and private cloud platforms.

## Requesting Support

To learn about Support programs, to manage your account or devices, or to open a support case, go to https://support.paloaltonetworks.com.

To provide feedback on the documentation, please write to us at: documentation@paloaltonetworks.com.

**Contact Information**

**Corporate Headquarters:**

**Palo Alto Networks**

3000 Tannery Way

Santa Clara, CA 95054

https://www.paloaltonetworks.com/company/contact-support

Palo Alto Networks, Inc.

www.paloaltonetworks.com