Deploy the Firewall Management Center Virtual on GCP

Google Cloud Platform (GCP) is a public cloud service provided by Google that that allows you to build and host applications Google's scalable infrastructure. Google's virtual private cloud (VPC) gives you the flexibility to scale and control how workloads connect regionally and globally. GCP allows you to build your own VPCs on top of Google's public infrastructure.

You can deploy the Firewall Management Center Virtual on the GCP.

Overview

The Firewall Management Center Virtual runs the same software as physical the Firewall Management Center to deliver proven security functionality in a virtual form factor. The Firewall Management Center Virtual can be deployed in the public GCP. It can then be configured to manage virtual and physical devices.

GCP Machine Type Support

The Firewall Management Center Virtual supports both compute-optimized and general purpose machine high-memory machine types, and high-CPU machine types. The Firewall Management Center Virtual supports the following GCP machine types.

Note Supported machine types may change without notice.

Note Machine type selection is restricted. The user can choose only machine types that are supported for the specific Firewall Management Center Virtual version selected.

Table 1: Supported Compute-Optimized Machine Types

Compute-Optimized Machine Types	Attributes	
	vCPUs	RAM (GB)
c2d-standard-8	8	32 GB
c2d-standard-16	16	64 GB

Table 2: Supported General Purpose Machine Types

General Purpose Machine Types	Attributes	
	vCPUs	RAM (GB)
e2-standard-8	8	32
e2-standard-16	16	64
e2-highmem-8	8	64
e2-highmem-16	16	128
n1-highmem-8	8	52
n1-highmem-16	16	104
n2d-standard-8	8	32
n2d-standard-16	16	64

Prerequisites

- Create an GCP account at https://cloud.google.com.
- A Cisco Smart Account. You can create one at Cisco Software Central (https://software.cisco.com/).
  - Configure all license entitlements for the security services from the Firewall Management Center.
  - See “Licensing the System” in the Firewall Management Center Configuration Guide for more information about how to manage licenses.
- Interface requirements:
  - Management interface — One used to connect the Firewall Threat Defense device to the Firewall Management Center.
- Communications paths:
  - Public IP for administrative access to the Firewall Management Center.
- For the Firewall Management Center Virtual and System compatibility, see Cisco Secure Firewall Threat Defense Compatibility Guide.

Guidelines and Limitations

Supported Features

- Deployment in the GCP Compute Engine
- Maximum of 32 vCPUs per instance (based on the GCP machine type)
- Licensing – Only BYOL is supported

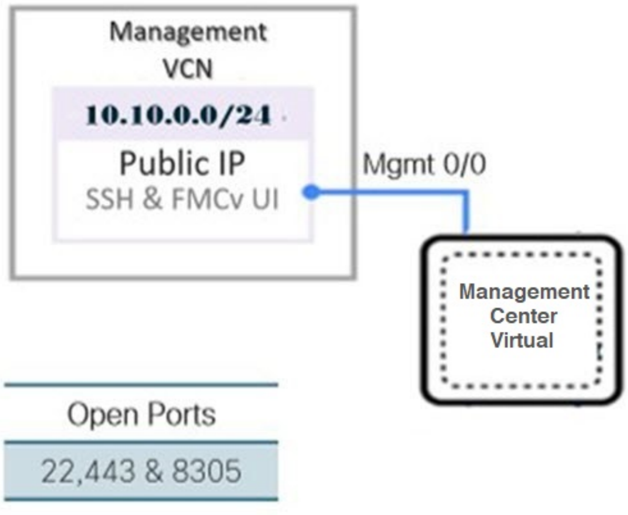
Unsupported Features

- IPv6
- Firewall Management Center Virtual native HA
- Autoscale
- Transparent/inline/passive modes
- Multi-context mode

Sample Network Topology

The following figure illustrates the typical topology for the Firewall Management Center Virtual with 1 subnet configured in GCP.

Figure 1: Topology Example for theFirewall Management Center Virtual Deployment on GCP



Deploy the Firewall Management Center Virtual

The following procedures describe how to prepare your GCP environment and launch the Firewall Management Center Virtual instance.

Create VPC Networks

The Firewall Management Center Virtual deployment requires the Management VPC for the management Firewall Management Center Virtual. See Figure 1 on page 3 as a guide.

Procedure

Step 1 In the GCP console, choose **VPC networks**, then click **Create VPC Network**.

Step 2 In the **Name** field, enter a descriptive name for your VPC network.

Step 3 From **Subnet creation mode**, click **Custom**.

Step 4 In the **Name** field under **New subnet**, enter the desired name.

Step 5 From the **Region** drop-down list, select the region appropriate for your deployment.

Step 6 From the **IP address range field**, enter the first network's subnet in CIDR format, such as 10.10.0.0/24.

Step 7 Accept the defaults for all other settings, then click **Create**.

Create the Firewall Rules

Each of the VPC networks requires firewall rules to allow SSH and traffic. Create the firewall rules for each VPC network.

Procedure

Step 1 In the GCP console, choose **Networking** > **VPC network** > **Firewall**, then click **Create Firewall Rule**.

Step 2 In the **Name** field, enter a descriptive name for your firewall rule, for example, *vpc-asiasouth-mgmt-ssh*.

Step 3 From the **Network** drop-down list, select the name of the VPC network for which you are creating the firewall rule, for example, *fmcv-south-mgmt*.

Step 4 From the **Targets** drop-down list, select the option applicable for your firewall rule, for example, **All instances in the network**.

Step 5 In the **Source IP ranges** field, enter the source IP address ranges in CIDR format, for example, 0.0.0.0/0.

Traffic is only allowed from sources within these IP address ranges.

Step 6 Under **Protocols and ports**, select **Specified protocols and ports**.

Step 7 Add your security rules:

a) Add a rule to allow SSH (TCP/22).

b) Add a rule to allow TCP port 443.

You access the Firewall Management Center Virtual UI which requires port 443 to be opened for HTTPS connections.

Step 8 Click **Create**.

Create the Firewall Management Center Virtual Instance on GCP

You can follow the steps below to deploy the Firewall Management Center Virtual instance from the GCP console.

Procedure

Step 1 Log into to the GCP Console.

Step 2 Click **Navigation menu** > **Marketplace**.

Step 3 Search the Marketplace for “Firewall Management Center BYOL” and choose the offering.

Step 4 Click **Launch**.

a) **Deployment name** — Specify a unique name for the instance.

b) **Image version** — Select the version from the drop-down list.

c) **Zone** — Select the zone where you want to deploy the Firewall Management Center Virtual.

d) **Machine type** — Choose the correct machine type based on the GCP Machine Type Support, on page 1.

e) **SSH key (optional)** — Paste the public key from the SSH key pair.

The key pair consists of a public key that GCP stores and a private key file that the user stores. Together they allow you to connect to your instance securely. Be sure to save the key pair to a known location, as it will be required to connect to the instance.

f) Choose whether to allow or **Block project-wide SSH keys** to access this instance. See the Google documentation Allowing or blocking project-wide public SSH keys from a Linux instance.

g) **Startup script** — Provide the day0 configuration for the Firewall Management Center Virtual.

The following example shows a sample day0 configuration you can copy and paste in the **Startup script** field:

```
{
"AdminPassword": "myPassword@123456",
"Hostname": "cisco-fmcv"
}
```

Tip
To prevent execution errors, you should validate your day0 configuration using a JSON validator.

h) Select the **Boot disk type** from the drop-down list.

By default, the **Standard Persistent Disk** is selected. Cisco recommends that you use the default Boot disk type.

i) The **Boot disk size in GB** default value is 250 GB. Cisco recommends that you keep the default boot disk size. It cannot be less than 250 GB.

j) Click **Add network interface** to configure the Management interface.

Note
You cannot add interfaces to an instance after you create it. If you create the instance with an improper interface configuration, you must delete the instance and recreate it with the proper interface configuration.

- From the **Network** drop-down list, select a VPC network, for example, *vpc-branch-mgmt*.
- From the **External IP** drop-down list, select the appropriate option.

  For the management interface, select the **External IP** to **Ephemeral**.
- Click **Done**.

k) **Firewall**— Apply the firewall rules.

- Check the **Allow TCP port 22 traffic from the Internet (SSH access)** check box to allow SSH.
- Check the **Allow HTTPS traffic from the Internet (FMC GUI)** check box to allow HTTPS connections.
- Check the **Allow TCP port 8305 traffic from the Internet (SFTunnel comm.)** check box to allow the Firewall Management Center Virtual and managed devices to communicate using a two-way, SSL-encrypted communication channel.

l) Click **More** to expand the view and make sure that **IP Forwarding** is set to **On**.

Step 5 Click **Deploy**.

Note
Startup time depends on a number of factors, including resource availability. It can take up to 35 minutes for the initialization to complete. Do not interrupt the initialization or you may have to delete the appliance and start over.

What to do next

View the instance details from the VM instance page of the GCP console. You'll find the internal IP address, external IP address, and controls to stop and start the instance. You need to stop the instance if you need to edit it.

Access the Firewall Management Center Virtual Instance on GCP

Make sure that you have already created a firewall rule to allow SSH (TCP connections through port 22); see Create the Firewall Rules, on page 4 for more information.

This firewall rule enables access to the Firewall Management Center Virtual instance and allows you to connect to the instance using the following methods.

- External IP
  - Browser window
  - Any other SSH client or third-party tools
- Serial console
  - Gcloud command line

See the Google documentation, Connecting to instances for more information.

Note If you choose not to add a Day0 configuration, you can log in to the Firewall Management Center Virtual instance using the default credentials. You are prompted to set the password on the first login attempt.

Connect to the Firewall Management Center Virtual Instance Using the Serial Console

Procedure

Step 1 In the GCP console, choose **Compute Engine** > **VM instances**.

Step 2 Click the Firewall Management Center Virtual instance name to open the **VM instance details** page.

Step 3 Under the **Details** tab, click **Connect to serial console**.

See the Google documentation, Interacting with the serial console for more information.

Connect to the Firewall Management Center Virtual Instance Using an External IP

The Firewall Management Center Virtual instance is assigned with an internal IP and an external IP. You can use the external IP to access the Firewall Management Center Virtual instance.

Procedure

Step 1 In the GCP console, choose **Compute Engine** > **VM instances**.

Step 2 Click the Firewall Management Center Virtual instance name to open the **VM instance details** page.

Step 3 Under the **Details** tab, click the drop-down menu for the **SSH** field.

Step 4 Select the desired option from the **SSH** drop-down menu.

You can connect to the Firewall Management Center Virtual instance using the following method.

- Any other SSH client or third-party tools—See the Google documentation, Connecting using third-party tools for more information.

Connect to the Firewall Management Center Virtual Instance Using Gcloud

Procedure

Step 1 In the GCP console, choose **Compute Engine** > **VM instances**.

Step 2 Click the Firewall Management Center Virtual instance name to open the **VM instance details** page.

Step 3 Under the **Details** tab, click the drop-down menu for the **SSH** field.

Step 4 Click **View gcloud command** > **Run in Cloud Shell**.

The Cloud Shell terminal window opens. See the Google documentation, gcloud command-line tool overview, and gcloud compute ssh for more information.