How to Deploy a Cisco CSR 1000v on Google Cloud Platform

Deploying a Cisco CSR 1000v on Google Cloud Platfrom involves these tasks:

- Create an SSH Key, on page 1
- Create a VPC Network, on page 2
- Create an External IP Address, on page 2
- Create Firewall Rules, on page 3
- Create a VM Instance, on page 4
- Create Routes, on page 6
- Access the Cisco CSR 1000v CLI, on page 6
- Configuring IPsec VPN for a Cisco CSR 1000v on Google Cloud Platform, on page 7

Create an SSH Key

To create an SSH key, which is required to access a Cisco CSR 1000v VM instance, perform the following steps. Enter the commands at a terminal server.

Step 1 Execute **ssh-keygen -t rsa -f** ~/.ssh/*keyfile* [-C *username*]

~/.ssh/*keyfile* - Directory path and filename of the key. Example: `/users/joe/.ssh/mykey`.

-C *username* - Username, which is added as a comment. This variable is optional.

Two key files are created; a private key and a public key in the .ssh directory. For example, `mykey` and `mykey.pub`.

For more information on creating an SSH key, see *Creating a new SSH key* in the Google Cloud Platform documentation. See also Managing SSH keys in Metadata.

Example:

```
ssh-keygen -t rsa -f /users/joe/.ssh/mykey -C joe
```

Step 2 **cat** ~/.ssh/[*keyfile_pub*]

keyfile_pub specifies the public key; for example, `mykey.pub`.

Example:

Example: `cat /users/joe/.ssh/mykey.pub`

The system displays the contents of the public key. You will need this public key to Create a VM Instance, on page 4.

Create a VPC Network

Before you begin

To learn about VPC networks, see: Virtual Private Cloud (VPC) Network Overview and Using VPC Networks.

Step 1 From the navigation pane in the Google Cloud Platform console, scroll down to **VPC network** and select **VPC networks**.

Step 2 Click **Create VPC Network**.

Step 3 Enter a **Name** for the network. **CREATE VPC NETWORK**.

Step 4 Enter a **Description** for the network.

Step 5 Select **Subnets** > **Add Subnet**.

Step 6 In the New Subnet dialog box, Enter a **Name** for the subnet. For example, `csrnet1`.

Step 7 Select the appropriate option in the **Region** field.

Step 8 Enter an **IP address range**. For example, enter 10.10.1.0/24 for the subnet address.

Step 9 Click **Done** to create the subnet.

To create multiple subnets for the VPC network, repeat steps 5 to 9.

Step 10 Click **Create** to create the VPN Network.

Create an External IP Address

To create an external IP address, you reserve an IP address by performing the following steps. You can later use the IP address to connect to a VM instance using an SSH session.

Step 1 From the navigation menu in the Google Cloud Platform Console, scroll down to "VPC network" and select "External IP Addresses".

For more information about IP addresses, see: IP Addresses.

Step 2 Click **Reserve static address**.

These are the field names and permissible values:

Table 1: External IP Addresses Fields

Field	Value
Name	Enter a name (in lowercase) for this address.
Description	Enter a description for this address.

Field	Value
Network Service Tier	premium The premium tier gives a higher performance than the standard tier.
IP Version	IPv4
Type	Regional
Region	Select a location. Example: "us-east2".

Step 3 Click **Reserve**.

Reserves this IP address.

Create Firewall Rules

To enable traffic to pass to a VM instance, you must create a firewall rule by performing the following steps. For more information on firewall rules, refer to "Firewalls" in VPC Networking and Firewalls.

Note After creating a firewall rule, you can change only some of its values. The following properties cannot be changed: "Network" (that is, the network to which the rule originally applied), "Priority", "Direction of traffic," and "Action on match". Therefore, in future you may need to delete the original rule and replace it with a new rule.

Step 1 From the navigation menu in the Google Cloud Platform Console, scroll down to "VPC network" and select "Firewall Rules".

Step 2 Click "CREATE FIREWALL RULE".

Enter the specified values for the following fields:

Table 2: Firewall Rules Fields

Field	Value
Network	Default.
Priority	1000 Values: 0–65535. Default: 1000. A lower value results in a higher priority being assigned to this rule.
Traffic Direction	Ingress. Values: Ingress, Egress.

Field	Value
Action on Match	Allow. Values: Allow, Deny.
Targets	All instances in the network. Values: "All instances in the network", "Specified target tags", "Specified service account".
Region	Select a location. Example: "us-east2".
Source Filters (optional)	Choose to filter the traffic using up to four different source filter types. For example, if you choose to specify a source IP range, you can enter 0.0.0.0/0 to select any IP address.
Source IP Ranges	0.0.0.0/0 (selects all IP ranges in the network).
Protocols and Ports	A protocol and port range String multiple protocol and port ranges together. For example: "icmp", "udp:4789-4790", "tcp:0-6553".

Step 3 Click **Create**.

Creates a firewall rule. To add another firewall rules, repeat the previous steps.

Create a VM Instance

Perform the following steps to deploy a Cisco CSR 1000v VM instance on Google Cloud Platform.

For more information, see: Creating and Starting a VM Instance.

Step 1 Click **Compute Engine** and **VM Instances**.

Step 2 Click **CREATE INSTANCE**.

Select a boot disk to create a new CSR 1000v VM instance (from "OS Images" or custom images) and enter values for the following fields.

Step 3 Specify the name for your VM ins the **Name** field. You can

Name for your VM, using only lowercase letters. Example: "newtestvm".

Step 4 Specify the **Region**.

Step 5 Specify the **Zone**. The zone is often a data center with a region.

Step 6 Select the **Machine type**. Select one of the following options from the drop-down list: **`n1-standard-2`**, **`n1-standard-4`**, **`n1-standard-8`**. The machine type is associated with an image filename. For example, the 2vCPUs machine type for the Cisco CSR 1000v has an image filename of "n1-standard-2".

Step 7 (Optional) Click **Customize** to select the number of cores(vCPUs), memory size, and GPUs.

Step 8 In the **Boot disk** section, click **Change**.

Step 9 Select a Cisco CSR 1000v image. See the Marketplace to select the CSR 1000v image.

Step 10 In the Boot Disk window, for the **Boot disk** type, select **SSD persistent disk**.

Step 11 Click **Select**.

In the **Create an Instance** window, the name of the previously selected image appears in the **Boot disk** section.

Note In the **Identity and API Access** section, do not change the value of the **Service account**.

Step 12 Select **Allow default access**.

Step 13 In the **Firewall** section, select either: **Allow HTTP traffic** or **Allow HTTPS traffic**.

Step 14 Click **Management, disks, networking, SSH keys**.

Step 15 Click **Networking**.

Step 16 Click **Add interface**.

Step 17 In the Networking Interfaces dialog box, select the default interface. For example, the default security group is 10.142.0.0/20.

Step 18 In the Networking Interface window, select the first default interface.

Step 19 Set **IP Forwarding** to **On**. This setting prevents the traffic from being blocked.

Step 20 Set **Primary internal IP** to Ephemeral (automatic). This private IP address is obtained automatically from the selected subnet.

Step 21 Set **External IP** to Ephemeral (automatic).

Specify Ephemeral (automatic). Later, you can use this public IP address when you start an SSH session from a terminal server. You may also choose to specify this External IP address as static. The external IP address of each interface is either ephemeral or static.

Step 22 Click **Done**.

Step 23 (Optional) Click **Add network interface** to add a second interface.

This step is optional. If you do not want to add a second interface, go to step 31 "SSH Keys".

Step 24 Enter **Name** to specify the name of the second interface.

Step 25 Select a **Network**.

Step 26 Select a **Subnetwork**.

Step 27 For the primary internal IP, select **Ephemeral (automatic)**. The private IP address is obtained automatically from the selected subnet.

Step 28 For the external IP, select **None**.

For the second interface, you can select **None**. You do not need a public IP address on this interface as you previously set an external IP address on the first interface.

Step 29 Click **Done**.

Step 30 In the **SSH Keys** section, paste the SSH key from the public key that you created earlier in the Create an SSH Key, on page 1 section.

The SSH key is an instance-wide SSH key. The settings are applicable only to this VM instance, and not to the whole project.

Step 31 Click **Create**.

The newly created Cisco CSR 1000v VM instance boots up, and may take 5 to 10 minutes. To check whether the VM instance is up, click the Cisco CSR 1000v name and under **Logs**, click **Serial Port**. If you see, for example, "Adding eth0 entry", it indicates that the instance is still booting up.

Create Routes

Perform the following steps to create each route for traffic in the VPC network.

Step 1 Under "VPC Network", select **Routes**.

The "Route details" window opens.

Step 2 Click **CREATE ROUTE**.

Enter the specified values for the fields:

Table 3: Route Fields

Field	Value
Name	Enter a name (in lowercase) for this address. Example: "northboundtosouthbound".
Description	Enter a description for this address. Example: "Route to Linux".
Network	Name of the VPC network. Example: "csrnet220".
Destination IP range	Example: 10.12.1.0/24.
Next hop	Enter a value for the "Next hop" destination, using one of the following fields: Instance, Gateway, or IP address. Example (IP address): 10.11.1.2.

Step 3 Click **Create**.

Creates a route.

Access the Cisco CSR 1000v CLI

This task describes how to access the CLI of the Cisco CSR 1000v VM using SSH and how to increase the speed of the interfaces.

Before you begin

Before accessing the Cisco CSR 1000v VM instance using an SSH session, the Cisco CSR 1000v VM instance must be up.

Note In the "VM instances" window, the SSH tab is not enabled for a Cisco CSR 1000v VM. You must, therefore, set up an SSH using CLI commands, which are described in the table at the Procedure section.

Procedure

	Command or Action	Purpose
Step 1	In a terminal server, enter the following command: **ssh -i** ~/.ssh/[*keyfile*] *username@ instance-external-IP* . **Example:** `ssh -i /users/joe/.ssh/mykey.pub joe@10.0.0.2`	Logs into the Cisco CSR 1000v using an SSH session. ~/.ssh/keyfile represents the path and filename of the public key. After logging in, you can enter Cisco IOS XE commands using the CLI.
Step 2	**interface** *interface-name* **Example:** `Router(config)# interface GigabitEthernet1`	Enters interface configuration mode. (The following steps are recommended in order to increase the speed to 10 Gbps for each interface.).
Step 3	**ip address dhcp** **Example:** `Router(config-if)# ip address dhcp`	Acquires an IP address on an interface from DHCP.
Step 4	**speed 10000** **Example:** `Router(config-if)# speed 10000`	Set speed to 10 Gbps.
Step 5	**no negotiation auto** **Example:** `Router(config-if)# no negotiation auto`	Disables autonegotiation.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 7	Repeat steps 2 to 6 to increase the speed for the second interface of the Cisco CSR 1000v.	

Configuring IPsec VPN for a Cisco CSR 1000v on Google Cloud Platform

This example shows the configuration of an IPsec VPN on a Cisco CSR 1000v on GCP.

```
crypto isakmp policy 1
 encr aes
 hash sha256
 authentication pre-share
 group 14
crypto isakmp key cisco123 address 0.0.0.0
crypto ipsec transform-set T1 esp-3des esp-md5-hmac
 mode transport
crypto ipsec profile P1
 set transform-set T1
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 198.51.100.253
 tunnel protection ipsec profile P1
end

ip route 6.6.6.6 255.255.255.255 Tunnel0
```