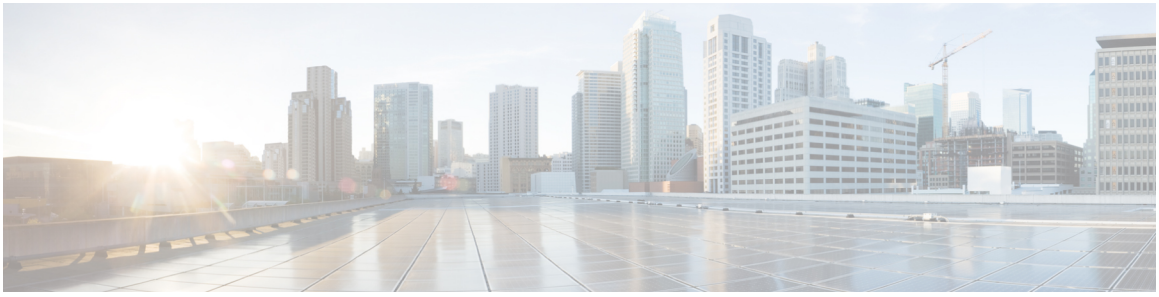
Cisco Catalyst 8000V Edge Software Deployment Guide for Google Cloud Platform

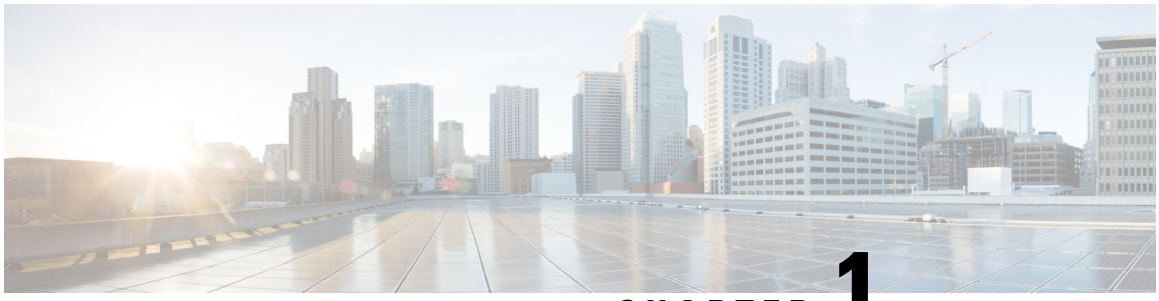
First Published: 2020-11-30

Last Modified: 2023-08-22

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS



CHAPTER 1

Preface

This preface describes the audience, organization, and conventions of this document. It also provides information on how to obtain other documentation.

This preface includes the following sections:

Audience and Scope

This document is designed for the person who is responsible for configuring your Cisco Enterprise router. This document is intended primarily for the following audiences:

- Customers with technical networking background and experience.
- System administrators familiar with the fundamentals of router-based internetworking but who might not be familiar with Cisco IOS software.
- System administrators who are responsible for installing and configuring internetworking equipment, and who are familiar with Cisco IOS software.

Feature Compatibility

For more information about the Cisco IOS XE software, including features available on your device as described in the configuration guides, see the respective router documentation set.

To verify support for specific features, use the Cisco Feature Navigator tool. This tool enables you to determine the Cisco IOS XE software images that support a specific software release, feature set, or a platform.

Document Conventions

This documentation uses the following conventions:

Convention	Description
^ or **Ctrl**	The ^ and **Ctrl** symbols represent the Control key. For example, the key combination **^D** or **Ctrl-D** means hold down the **Control** key while you press the **D** key. Keys are indicated in capital letters but are not case sensitive.
string	A string is a nonquoted set of characters shown in italics. For example, when setting an SNMP community string to public, do not use quotation marks around the string or the string will include the quotation marks.

The command syntax descriptions use the following conventions:

Convention	Description
bold	Bold text indicates commands and keywords that you enter exactly as shown.
italics	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional element (keyword or argument).
|	A vertical line indicates a choice within an optional or required set of keywords or arguments.
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.

Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. For example, see the following table.

Convention	Description
[x {y | z}]	Braces and a vertical line within square brackets indicate a required choice within an optional element.

Examples use the following conventions:

Convention	Description
`screen`	Examples of information displayed on the screen are set in Courier font.
`bold screen`	Examples of text that you must enter are set in Courier bold font.
< >	Angle brackets enclose text that is not printed to the screen, such as passwords.
!	An exclamation point at the beginning of a line indicates a comment line. Exclamation points are also displayed by the Cisco IOS XE software for certain processes.
[ ]	Square brackets enclose default responses to system prompts.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Note Means *reader take note*. Notes contain helpful suggestions or references to materials that may not be contained in this manual.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

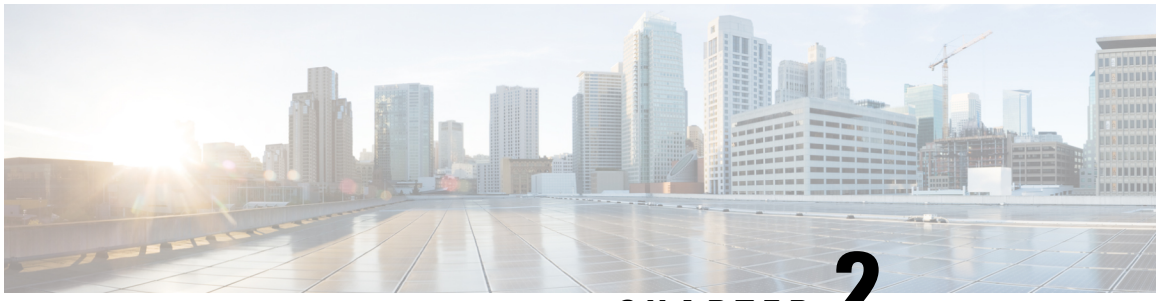
Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at https://www.cisco.com/en/US/support/index.html.

Go to **Products by Category** and choose your product from the list, or enter the name of your product. Look under **Troubleshoot and Alerts** to find information for the issue that you are experiencing.



CHAPTER 2

Overview of Cisco Catalyst 8000V

The Cisco Catalyst 8000V Edge Software is a virtual router that runs on Cisco IOS XE. Apart from deploying in hypervisors, Cisco Catalyst 8000V can be deployed as a virtual machine in a public cloud such as Google Cloud Platform (GCP).

This guide specifies the deployment procedures and the post deployment configurations for Cisco Catalyst 8000V on GCP. You can choose to deploy Cisco Catalyst 8000V software on new or existing infrastructure, such as a VPC network.

Features Supported

Cisco Catalyst 8000V provides enterprise-class networking services and VPN technologies. The following VPN features are supported on Cisco Catalyst 8000V: IPsec, DMVPN, FlexVPN, and SSLVPN. Further, you can use dynamic routing protocols, such as EIGRP, OSPF, and BGP.

You can secure, inspect, and audit network traffic with the application-aware Zone-Based Firewall. You can also use IP SLA and Application Visibility and Control (AVC) to detect performance issues, fingerprint application flows, and export detailed flow data.

Prerequisites for Deploying Cisco Catalyst 8000V

The following are the prerequisites when deploying a Cisco Catalyst 8000V device on Google Cloud Platform (GCP):

- You must have a user account or subscription with Google Cloud Platform.
- Several resources must be deployed before or during the deployment of Cisco Catalyst 8000V.
- To obtain full traffic throughput, you must obtain a software license for Cisco Catalyst 8000V. Otherwise, the throughput is limited to 10 Mbps in the autonomous mode and 250Mbps in the controller mode.

Note By default, Cisco Catalyst 8000V boots with Ipbase which includes a minimal set of features only. To use all the features, configure the essentials, advantage, or the premier boot level.

Google Cloud Platform Resources

To deploy a Cisco Catalyst 8000V on Google Cloud Platform (GCP), you must create a project with the following resources: virtual machines, interfaces, VPC networks, routes, public IP addresses, firewall rules, and storage. Resources that exist in different projects can only connect through an external network. For more information on projects, see The Project resource, and Creating and Managing Projects in the Google Cloud Platform (GCP) resource hierarchy.

The following list is a summary of some of the resources that are used by a project for Cisco Catalyst 8000V on Google Cloud Platform:

- Virtual Private Cloud (VPC) network - connects VM instances and has subnets with defined IP addresses.
- VM instance - created from a boot disk image. For example, n1-standard-2 (2 vCPUs, 7.5 GB RAM, 2 virtual Network Interface Cards (vNICs)).
- Subnet - includes a subnet route which is the next hop IP address. The next hop IP address defines a communication path to and from the resources for the subnet.
- Firewall rules - security rules for the VPC network.
- Routes - a route maps an IP address range to a destination. This route allows the VPC network to send packets to the correct destination for an IP address. For more information, see Routes Overview.
- Storage - persistence disk storage that is used to hold disk or container images for VM instances. For more information, see Storage Options.
- Interfaces - You can assign a public IP address to each network interfaces of a Cisco Catalyst 8000V VM. Usually, a public IP address is assigned to the first interface. All the Cisco Catalyst 8000V VM interfaces are in a private subnet. You can assign the IP address of each private interface using the **ip dhcp address** command in the interface configuration. Alternatively, you can assign a static IP address using the **ip address** command. For example, `ip address 1.1.1.1 255.255.255.0`. If you use a static IP address, ensure that the IP address is the same as the IP address assigned by GCP. Later, to view some details about the interface, use the **show ip interface brief** command.

Supported Instance Types for Google Cloud Platform

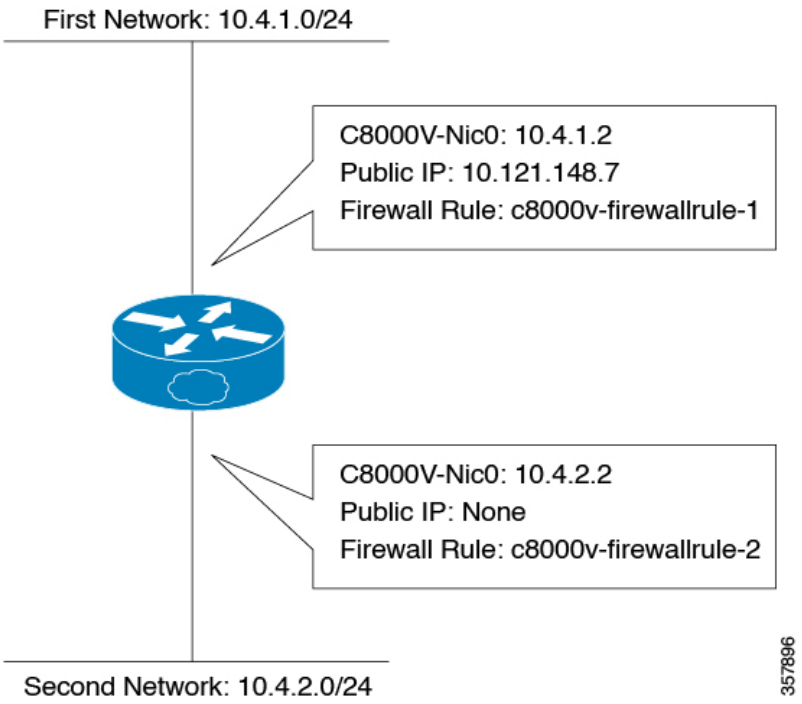
Cisco IOS XE Release	Supported Instance Types	Notes
Cisco IOS XE 17.13.1a	N1: n1-standard-4, n1-standard-8	BYOL only
Cisco IOS XE 17.12.2 Cisco IOS XE 17.12.1a	N1: n1-standard-4, n1-standard-8	BYOL only

Cisco IOS XE Release	Supported Instance Types	Notes
Cisco IOS XE 17.11.1a	N1: n1-standard-2, n1-standard-4, n1-standard-8	BYOL only
Cisco IOS XE 17.10.1a	N1: n1-standard-2, n1-standard-4, n1-standard-8	BYOL only
Cisco IOS XE 17.9.4a Cisco IOS XE 17.9.3a Cisco IOS XE 17.9.2a Cisco IOS XE 17.9.1a	N1: n1-standard-2, n1-standard-4, n1-standard-8	BYOL only
Cisco IOS XE 17.8.1a	N1: n1-standard-2, n1-standard-4, n1-standard-8	BYOL only
Cisco IOS XE 17.7.2 Cisco IOS XE 17.7.1a	N1: n1-standard-2, n1-standard-4, n1-standard-8	BYOL only
Cisco IOS XE 17.6.6a Cisco IOS XE 17.6.5a Cisco IOS XE 17.6.5 Cisco IOS XE 17.6.4 Cisco IOS XE 17.6.3a Cisco IOS XE 17.6.2 Cisco IOS XE 17.6.1a	N1: n1-standard-2, n1-standard-4, n1-standard-8	BYOL only
Cisco IOS XE 17.5.1a	N1: n1-standard-2, n1-standard-4, n1-standard-8	BYOL only
Cisco IOS XE 17.4.2 Cisco IOS XE 17.4.1b Cisco IOS XE 17.4.1a	N1: n1-standard-1, n1-standard-2, n1-standard-4, n1-standard-8	BYOL only Support for both autonomous and controller modes

Cisco Catalyst 8000V with Two Network Interfaces

This example shows a topology diagram that results after deploying a Cisco Catalyst 8000V device on GCP.

Figure 1: Sample Topology of a Cisco Catalyst 8000V device on GCP



The Cisco Catalyst 8000V VM was created from image "n1-Standard-2" and has two interfaces and two vCPUs. This Cisco Catalyst 8000V instance has a public IP address of 40.121.148.7 for the interface of the first subnet (NIC0). The firewall rule "c8000v-firewallrule-1" is assigned to this interface.

Note Create a firewall rule to allow traffic to pass in a custom VPC network. Without a firewall rule, by default, all the traffic is blocked.

Licensing

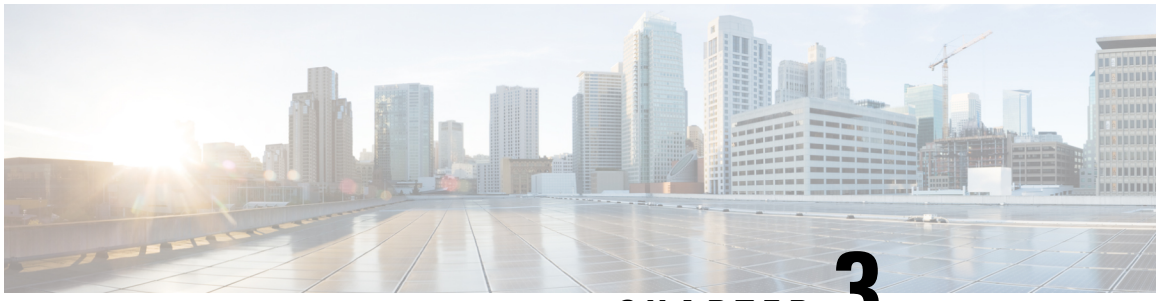
Cisco Catalyst 8000V supports the Bring Your Own License (BYOL) licensing model on GCP under the following licensing types:

- Cisco Smart Licensing Usage Policy - Cisco Smart Licensing Usage Policy is an evolved version of the existing Smart Licensing model with the overarching objective of providing a licensing solution that does not interrupt the operations of your network. Rather, this model enables a compliance relationship to account for the hardware and software licenses that you purchase and use. To know how to configure and use this licensing type, see Smart Licensing Using Policy for Cisco Enterprise Routing Platforms.
- Cisco Smart Licensing - If you are a user who has upgraded to Cisco Catalyst 8000V from Cisco CSR1000V or Cisco ISRV, you can continue using Smart Licensing.

  Cisco Smart Licensing assigns a license to the Cisco Catalyst 8000V instances dynamically. This allows you to manage licenses across different Cisco Catalyst 8000V instances without having to lock each

license to a specific Cisco Catalyst 8000V UDI serial number. For more information on Cisco Smart Licensing, see Smart Licensing.

The cost of licensing using BYOL in GCP includes the cost of a GCP instance and the cost of a Cisco Catalyst 8000V license.



CHAPTER 3

Deploying Cisco Catalyst 8000V Using VM Templates

This chapter specifies the procedure for deploying Cisco Catalyst 8000V on Google Cloud Platform (GCP) by using VM templates, and contains the following sections detailing the various tasks in the procedure.

Create an SSH Key

The first task in the deployment procedure is to create an SSH key. SSH keys act as a method of authentication to access your Cisco Catalyst 8000V instance. When you create an SSH key, a public key and a private key are created in the .ssh directory.

RSA is the default key type until Cisco IOS XE 17.9.x. From Cisco IOS XE 17.10.1a, support for ED25519 key type is added.

To create an SSH key, perform the following steps. Enter the commands in a terminal server.

Step 1 Run the **ssh-keygen -t rsa -f** ~/.ssh/*keyfile* [-C *username*] command. Here,

~/.ssh/*keyfile* is the directory path and filename of the key, for example, `/users/joe/.ssh/mykey`.

-C *username* is the username that is added as a comment. This variable is optional.

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

For more information on creating an SSH key, see Creating a new SSH key. See also Managing SSH keys in Metadata.

Example:

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

Step 2 Run the **cat** ~/.ssh/[*keyfile_pub*] command. Here, *keyfile_pub* specifies the public key, for example, `mykey.pub`.

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.

Create a VPC Network

Before you begin

Learn about VPC networks. For information about VPC networks, see Virtual Private Cloud (VPC) Network Overview and Using VPC Networks.

Step 1 In the navigation pane of the Google Cloud Platform console, choose **VPC network** > **VPC Networks**.

Step 2 Choose **Create VPC Network**.

Step 3 Enter a **Name** for the network.

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

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

Step 6 In the **New Subnet** dialog box, enter a **Name** for the subnet, for example, **`c8kvnet1`**.

Step 7 Choose the appropriate option from the **Region** drop-down list.

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 step 5 to step 9.

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

Create an External IP Address

To create an external IP address, you must reserve an IP address by performing the following steps. Only devices with external IP addresses can send and receive traffic directly to and from the network. Create the IP address to connect to a VM instance using an SSH session. For more information about IP addresses, see: IP Addresses.

Step 1 In the navigation pane of the Google Cloud Platform console, scroll down to **VPC Network**, and click **External IP Addresses**.

Step 2 Click **Reserve static address**. The following fields are displayed. The permissible values for these fields are listed in the following table:

Table 1: External IP Addresses Fields

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

Field	Value
Description	Enter a description for this address.
Network Service Tier	Premium: The premium tier gives a higher performance than the standard tier. To know more about network tiers in GCP, see Network Service Tiers Overview.
IP Version	The IP version of the instance. Choose **IPv4**.
Type	Choose **Regional**.
Region	Choose a location from the drop-down list, for example, **us-east2**.

Step 3 Click **Reserve** to reserve this IP address.

Create a VM Instance

Upload the VM Image

Perform the following steps to upload a custom Cisco Catalyst 8000V image that you'll use to deploy the VM.

Before you begin

To learn about VM instances in GCP, see Creating and Starting a VM Instance.

Step 1 In the navigation pane of the Google Cloud Platform console, choose **Compute Engine** and **VM Instances**.

Step 2 Click **Create Instance**.

Step 3 To create a new Cisco Catalyst 8000V VM instance by using a boot disk image, do one of the following:

- To create the VM instance using a public OS image, choose **OS Images**. Select the image from the list of images displayed.
- To create the VM instance using a defined list of trusted images, choose **Custom Images** and upload your image.

Configure the Properties for the VM

To configure the properties for your VM instance, perform the following steps in the Create Instance window.

Before you begin

Perform the Create a VM instance task.

Step 1 Specify the name for your VM in the **Name** field. Use only lowercase letters, for example, **`newtestvm`**.

Step 2 Choose the appropriate **Region** from the drop-down list.

Step 3 Specify the zone for your instance in the **Zone** field. The zone is often a data center with a region.

Step 4 Choose one of these machine types from the **Machine Type** drop-down list—n1-standard-2, n1-standard-4, or n1-standard-8. The machine type is associated with an image filename. For example, the 2vCPUs machine type for the Cisco Catalyst 8000V has the image filename n1-standard-2.

Step 5 (Optional) Click **Customize** to customize the number of cores (vCPUs), memory size, and GPUs for your VM instance.

Configure the DIsk Options for the VM

To configure the boot disk options for your VM instance, perform the following steps in the **Boot Disk** section in the **Create Instance** window.

Step 1 Click **Change**.

A pop-up window with the **Boot Disk** options is displayed.

Step 2 Click the **Custom Image** tab, and select the Cisco Catalyst 8000V image that you uploaded.

Step 3 From the **Boot disk** drop-down list, choose the persistent disk storage option for your VM. It is recommended that you choose the **SSD persistent disk** option.

Step 4 In the **Disk Size** field, enter the boot disk size in GB.

Step 5 Click **Select** to save all the disk options.

The name of the Cisco Catalyst 8000V image you selected is displayed in the **Boot disk** section.

Configure the Firewall and Networking Options

Perform the following steps to configure the firewall options and the networking options for your VM.

Step 1 In the **Identity and API Access** field, the default value is **Service account**. Do not change this value. This field specifies how your VM instance interacts with the other resources within your project.

Step 2 In the **Firewall** field, choose either **Allow HTTP traffic** or **Allow HTTPS traffic** to allow HTTP or HTTPS traffic to the VM.

Step 3 Click the **Networking** tab, and configure the following networking properties.

a) Click **Add interface**.

b) In the **Networking Interface** window, choose the default interface for your VM. For example, the default security group is 10.12.0.2.

c) Choose the first default interface for your VM.

d) From the **IP Forwarding** drop-down list, choose **On** to prevent the traffic from being blocked.

e) From the **Primary internal IP** drop-down list, choose **Ephemeral (automatic)**. This private IP address is obtained automatically from the selected subnet.

f) From the **External IP** drop-down list, choose **Ephemeral (automatic)**. The external IP address of each interface is either ephemeral or static. When you select the **Ephemeral (automatic)** option, you can use this public IP address when you start an SSH session from a terminal server. You can also choose to set a static address as this external IP address.

Step 4 Click **Done** to save the properties and go to the previous window.

Add an Additional Interface

Perform these steps to configure an additional interface when you deploy a Cisco Catalyst 8000V VM instance in GCP. This is an optional task. If you don't want to add another interface, proceed to Configuring the Security Properties section.

Step 1 Click **Add network interface** to add a second interface.

Note For every new interface that you add, you must create a new VPC.

Step 2 In the **Name** field, specify the name of the second interface.

Step 3 From the **Network** drop-down list, choose the network for your second interface..

Step 4 From the **Subnetwork** drop-down list, select the subnetwork.

Step 5 In the primary internal IP field, choose **Ephemeral (automatic)**. The private IP address is obtained automatically from the subnet you selected.

Step 6 In the external IP field, choose **None**.

Note If you have created the second or additional interface, you do not need a public IP address for this interface because you have already set an external IP address for your first interface.

Step 7 Click **Done**.

Configure the Security Options

Step 1 In the **Security** section, in the **Block Project-Wide SSH Keys** field, paste the SSH key from the public key that you created as described in Create an SSH Key.

Note 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 2 (Optional) To provide custom data, click **Management**.

Step 3 (Optional) Copy and paste the custom data in the **Startup Script** field. For more information on custom data, see the Day Zero Configuration chapter.

Step 4 Click **Create**.

The newly created Cisco Catalyst 8000V VM instance starts, and this process could take several minutes. To check whether the VM instance is up, click on your VM on the **Instances** page. Choose **Logs** > **Serial Port**. The status is indicated here.

Access the Cisco Catalyst 8000V CLI

SSH keys act as the authentication method to access your Cisco Catalyst 8000V instance. Apart from the RSA key type, Cisco Catalyst 8000V also supports the ED25519 key type from Cisco IOS XE 17.10.1a. To set up an SSH using the CLI, perform the following steps.

Before you begin

- Perfrom the Day 0 configuration as mentioned in the Day Zero Configuration chapter.
- Ensure that the Cisco Catalyst 8000V VM instance is up. This is required for you to access the Cisco Catalyst 8000V VM instance using an SSH session.

Note In the VM Instances window, the **SSH** tab is not enabled for a Cisco Catalyst 8000V VM. You must set up an SSH using the following commands.

SUMMARY STEPS

1. **ssh -i** ~/.ssh/[*keyfile*] *username@ instance-external-IP* .
2. **interface** *interface-name*
3. **ip address dhcp**
4. **speed <interface speed>**
5. **no negotiation auto**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**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 Catalyst 8000V instance using an SSH session. Here, `~/.ssh/keyfile` represents the path and filename of the public key. After logging in, you can enter the Cisco IOS XE commands using the CLI.
Step 2	**interface** *interface-name* **Example:** `Router(config)# interface GigabitEthernet1`	Enters interface configuration mode. It is recommended that you perform the following steps to increase the interface's speed 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 <interface speed>** **Example:** `Router(config-if)# speed 10000`	Sets the speed of the interface.

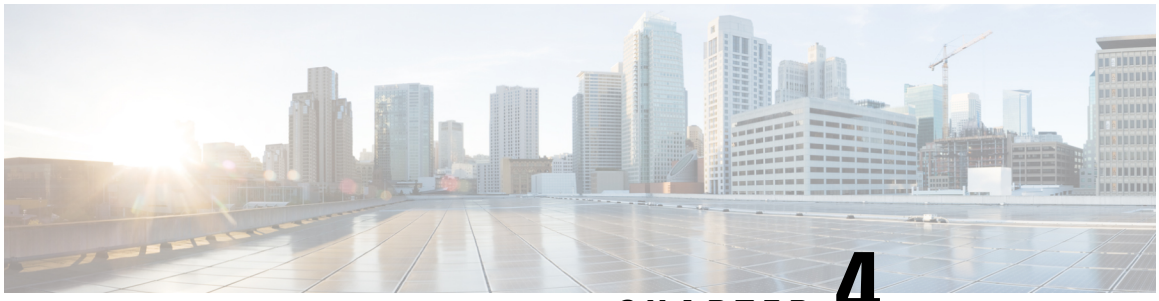
	Command or Action	Purpose
Step 5	**no negotiation auto** **Example:** `Router(config-if)# no negotiation auto`	Disables auto negotiation.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode. (Optional) Repeat steps 2 to 6 to increase the speed of the second interface of the Cisco Catalyst 8000V instance.

Configuring a Sample Feature

After you deploy Cisco Catalyst 8000V in GCP and access the CLI, you can configure the supported features. In this section, the following code sample shows how to configure an IPsec VPN on a Cisco Catalyst 8000V instance running 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
```



CHAPTER 4

Deploying Cisco Catalyst 8000V Using Solution Templates

You can deploy a Cisco Catalyst 8000V router in Google Cloud Platform (GCP) in two ways: by using a VM instance, or by using a solution template. This chapter specifies the procedures to deploy an instance by using a solution template.

Create an SSH Key

The first task in the deployment procedure is to create an SSH key. SSH keys act as a method of authentication to access your Cisco Catalyst 8000V instance. When you create an SSH key, a public key and a private key are created in the .ssh directory.

RSA is the default key type until Cisco IOS XE 17.9.x. From Cisco IOS XE 17.10.1a, support for ED25519 key type is added.

To create an SSH key, perform the following steps. Enter the commands in a terminal server.

Step 1 Run the **ssh-keygen -t rsa -f** ~/.ssh/*keyfile* [-C *username*] command. Here,

~/.ssh/*keyfile* is the directory path and filename of the key, for example, `/users/joe/.ssh/mykey`.

-C *username* is the username that is added as a comment. This variable is optional.

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

For more information on creating an SSH key, see Creating a new SSH key. See also Managing SSH keys in Metadata.

Example:

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

Step 2 Run the **cat** ~/.ssh/[*keyfile_pub*] command. Here, *keyfile_pub* specifies the public key, for example, `mykey.pub`.

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.

Create a VPC Network

Before you begin

Learn about VPC networks. For information about VPC networks, see Virtual Private Cloud (VPC) Network Overview and Using VPC Networks.

Step 1 In the navigation pane of the Google Cloud Platform console, choose **VPC network** > **VPC Networks**.

Step 2 Choose **Create VPC Network**.

Step 3 Enter a **Name** for the network.

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

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

Step 6 In the **New Subnet** dialog box, enter a **Name** for the subnet, for example, `c8kvnet1`.

Step 7 Choose the appropriate option from the **Region** drop-down list.

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 step 5 to step 9.

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

Deploy the Cisco Catalyst 8000V Template

Step 1 Go to the Google Marketplace and search for Cisco Catalyst 8000V. Select the Cisco Catalyst 8000V template.

Step 2 Click **Launch On Compute Engine**.

Step 3 In the New Cisco Catalyst 8000V Deployment screen, provide the following details:

a) **Deployment name**: This field is filled by default, and displays the cisco-c8000v-<deployment number>.

b) **Instance Name**: The name of the Cisco Catalyst 8000V instance in text format. You must follow the GCP naming pattern for successful deployment. The name of the instance must be a combination of regex '(?:[a-z](?:[-a-z0-9]{0,61}[a-z0-9])?)'">)

c) **Username**: Specify the username that is used to access the Cisco Catalyst 8000V instance.

d) **Instance SSH Key**: Specify the public key to be used for SSHing into the instance. To know how to create an ssh-key, see SSH-Key.

e) **Zone**: Select the zone where the Cisco Catalyst 8000V is deployed from the drop-down list.

f) **Machine Type**: Select the size of the Cisco Catalyst 8000V that you want to deploy. For more information on Cisco Catalyst 8000V sizes, see MachineTypes.

g) **Custom Data File URL**: Provide a link to the publicly-readable custom date file. For example, `http://storage.googleapis.com/customdatatest/customdata.txt`. For more information, see the Custom Data section in the *Cisco Catalyst 8000V Installation and Upgrade Guide*.

Bootdisk

h) **Bootdisk type**: By default, the SSD Persistent disk is selected. Cisco recommends that you use the default Boot disk type.

i) **Boot disk size in GB**: The default value is 10 GB. Cisco recommends that you use the default Boot disk size.

Networking

j) **Network (VPC)**: Select the network in the region where you want to deploy the Cisco Catalyst 8000V instance. You must create the Network (VPC) before you create the Cisco Catalyst 8000V instance. Ensure that at least one subnet is associated to that Network (VPC). For more information about VPC networks, see Virtual Private Cloud Network Overview and Using VPC Networks.

k) **Subnetwork**: Select the subnet that is associated with the selected Network (VPC). This subnet acts as the first Network Interface (nic0) of the Cisco Catalyst 8000V instance.

l) **ExternalIP**: The public IP address that you must use to SSH into the Cisco Catalyst 8000V instance. This can be static, Ephemeral (Dynamic) and None. For more information about IP addresses, see IP Addresses.

m) **Firewall**: The firewall wall rule associated to the VPC Network.With the current Solution Template, you can use TCP ports 21, 22, 80. You can also create additional Firewall rules. For more information on firewall rules, see Firewalls in VPC Networking and Firewalls.

Note You can also specify source ranges for firewalls rules.

n) **IP Forwarding**: The default value to allow traffic between interfaces on the Cisco Catalyst 8000V instance. By default, the value for IP Forwarding is ON.

o) **Additional Network Interfaces**: Configure this field if you want to configure additional interfaces. By default, the value of this field is 0. To add additional interfaces, specify additional interfaces that are needed for the Cisco Catalyst 8000V instance. Select the additional network interfaces based on the machine type. For more information on deployment of instance with multiple interfaces in GCP, see Creating Instances With Multiple Network Interfaces.

Note For the deployment to be successful, even if you do not require all the additional interfaces, you must select the **Additional Network Interfaces** option. This is a known issue where Google brings up to 8 interfaces, and you must fill in all the eight interfaces.

For example, in the following image, even though two additional NICs were selected, note that the 7 additional interfaces are configured with the networks and subnets present in region where the Cisco Catalyst 8000V instance is deployed.

After successful deployment, the system displays a message that the Cisco Catalyst 8000V instance has been deployed.

Access the Cisco Catalyst 8000V CLI

SSH keys act as the authentication method to access your Cisco Catalyst 8000V instance. Apart from the RSA key type, Cisco Catalyst 8000V also supports the ED25519 key type from Cisco IOS XE 17.10.1a. To set up an SSH using the CLI, perform the following steps.

Before you begin

- Perfrom the Day 0 configuration as mentioned in the Day Zero Configuration chapter.

- Ensure that the Cisco Catalyst 8000V VM instance is up. This is required for you to access the Cisco Catalyst 8000V VM instance using an SSH session.

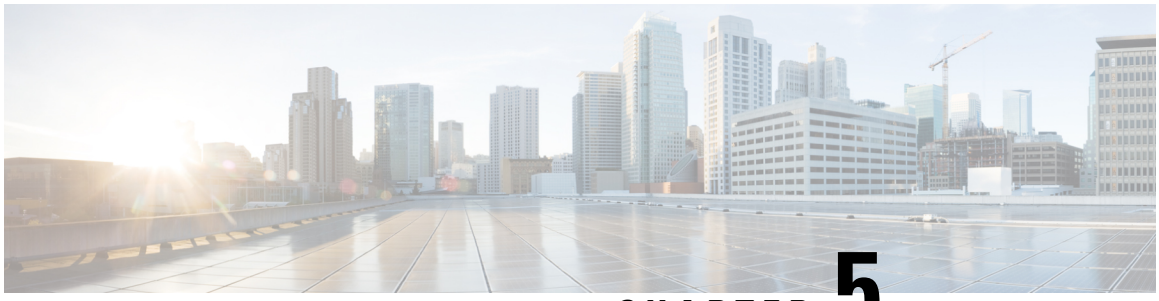
Note In the VM Instances window, the **SSH** tab is not enabled for a Cisco Catalyst 8000V VM. You must set up an SSH using the following commands.

SUMMARY STEPS

1. **ssh -i** ~/.ssh/[*keyfile*] *username@ instance-external-IP* .
2. **interface** *interface-name*
3. **ip address dhcp**
4. **speed <interface speed>**
5. **no negotiation auto**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**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 Catalyst 8000V instance using an SSH session. Here, `~/.ssh/keyfile` represents the path and filename of the public key. After logging in, you can enter the Cisco IOS XE commands using the CLI.
Step 2	**interface** *interface-name* **Example:** `Router(config)# interface GigabitEthernet1`	Enters interface configuration mode. It is recommended that you perform the following steps to increase the interface's speed 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 <interface speed>** **Example:** `Router(config-if)# speed 10000`	Sets the speed of the interface.
Step 5	**no negotiation auto** **Example:** `Router(config-if)# no negotiation auto`	Disables auto negotiation.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode. (Optional) Repeat steps 2 to 6 to increase the speed of the second interface of the Cisco Catalyst 8000V instance.



CHAPTER 5

Using Custom Routes

When you deploy a Cisco Catalyst 8000V instance in a VPC network, a route is created for each subnet to which the Cisco Catalyst 8000V device is connected. For example, if you deploy a Cisco Catalyst 8000V instance in GCP with two subnets, each subnet has an associated route.

See the following sections to know how to use custom routes in Cisco Catalyst 8000V running on GCP:

Create Routes

Perform the following steps to create a route that defines the path for the traffic in the VPC network.

Step 1 In the console, under **VPC Network**, select **Routes**.

Step 2 From the Route Details page, click **CREATE ROUTE**. Enter the specified values for the following fields:

Table 2: Route Fields

Field	Value
Name	Enter a name, in lowercase, for this address. For example, **`northboundtosouthbound`**.
Description	Enter a description for this address.
Network	The name of the VPC network. For example, **`c8000vnet220`**.
Destination IP range	Enter the destination IP address. For example, **`10.12.1.0/24`**.
Next hop	Enter a value for the Next hop destination by using one of the following fields: **Instance**, **Gateway**, or **IP Address**.

Step 3 Click **Create** to create the route.

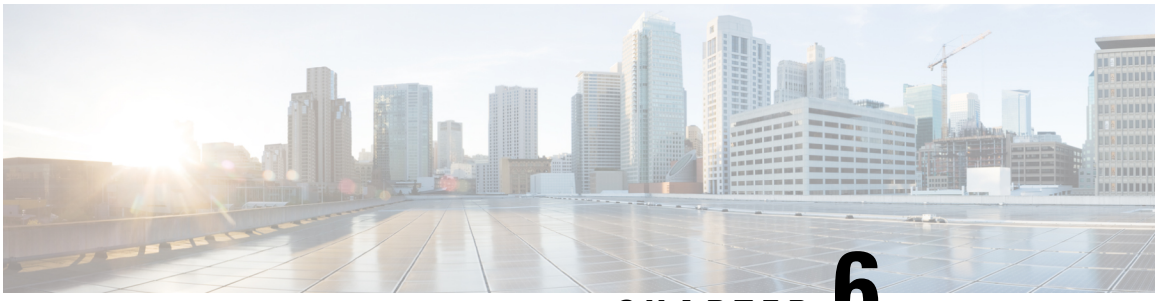
Custom Routes in the Same VPC Network

By default, the GCP network infrastructure provides a basic routing service which interconnects all the subnets within a VPC network. By default, packets are blocked between subnets unless firewall rules are changed to allow them to pass.

Routing Between VPC Networks or On-Premises Networks

To connect two VPC networks or to connect a VPC network to an on-premises network, create a route to specify Cisco Catalyst 8000V as the next hop router to each remote network. To force traffic through the Cisco Catalyst 8000V instance, add a route (default route or specific destination route) that points to the Cisco Catalyst 8000V instance.

For example, the following route was added with a destination IP address pointing to the Cisco Catalyst 8000V device. The "Next hop" refers to the Cisco Catalyst 8000V VM instance.



CHAPTER 6

Configuring a Sample Feature

After you deploy Cisco Catalyst 8000V in GCP and access the CLI, you can configure the supported features. In this section, the following code sample shows how to configure an IPsec VPN on a Cisco Catalyst 8000V instance running 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
```