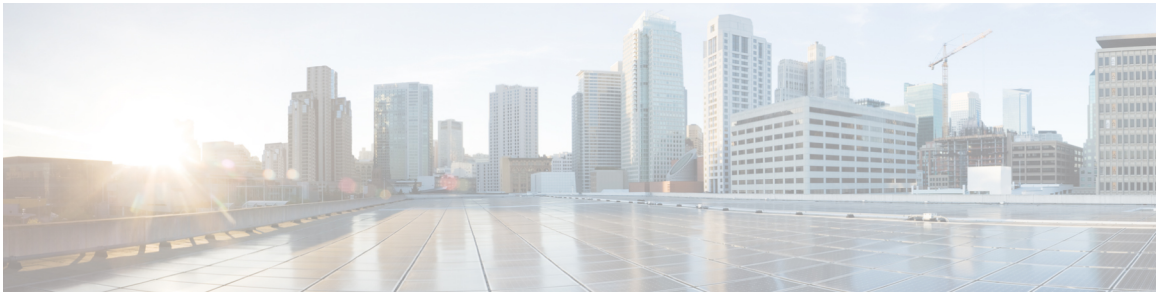


Cisco Catalyst 8000V Edge Software Deployment Guide for Google Cloud Platform

First Published: 2020-11-30

Last Modified: 2025-08-15

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

Full Cisco Trademarks with Software License ?

CHAPTER 1 **Preface** 1

- Audience and Scope 1
- Feature Compatibility 1
- Document Conventions 2
- Communications, Services, and Additional Information 3
- Documentation Feedback 4
- Troubleshooting 4

CHAPTER 2 **Overview of Cisco Catalyst 8000V** 5

- Prerequisites for Deploying Cisco Catalyst 8000V 5
- Deployment Requirements 6
- Cisco Catalyst 8000V with Two Network Interfaces 7
- Licensing 7

CHAPTER 3 **Deploying Cisco Catalyst 8000V by Using the GCP Console** 9

- Guidelines for Deploying Cisco Catalyst 8000V 9
- Create an SSH Key 10
- Create a VPC Network 11
- Create an External IP Address 11
- Deploy the Cisco Catalyst 8000V Instance 12
  - Choose the Machine Configuration 12
  - Configure the OS and Storage Properties 13
  - Configure the Firewall and Networking Options 14

Add an Additional Interface 14
Configure the Security Options 15
Access the Cisco Catalyst 8000V CLI 15
Configure a Sample Feature 17

CHAPTER 4 **Deploying Cisco Catalyst 8000V by Using Terraform** 19
Guidelines for Deploying Cisco Catalyst 8000V 19
Create an SSH Key 20
Create a VPC Network 21
Deploy the Cisco Catalyst 8000V Instance 21
Configure the Template Settings 21
Configure the Machine and Disk Properties 22
Configure the Network Settings and Interfaces 23
Configure the Firewall Settings 23
Add the Startup Script 24
Access the Cisco Catalyst 8000V CLI 25
Verify Interface Mapping 26

CHAPTER 5 **Using Custom Routes** 27
Create Routes 27
Custom Routes in the Same VPC Network 28
Routing Between VPC Networks or On-Premises Networks 28

CHAPTER 6 **Configure a Sample Feature** 29

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

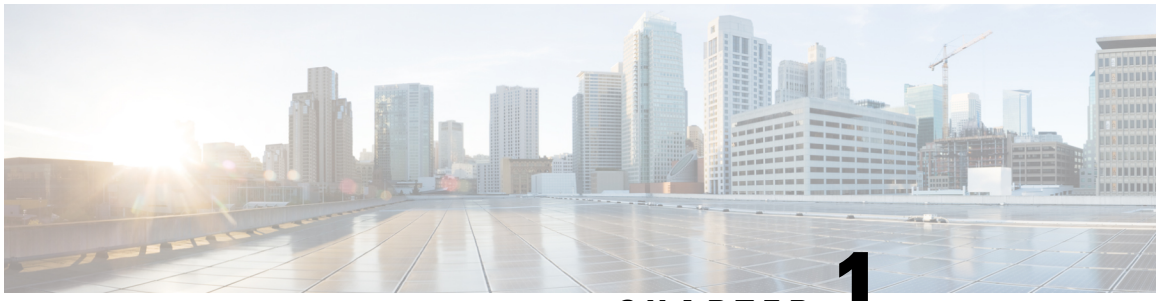
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020–2025 Cisco Systems, Inc. All rights reserved.



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, on page 1
- Feature Compatibility, on page 1
- Document Conventions, on page 2
- Communications, Services, and Additional Information, on page 3
- Documentation Feedback, on page 4
- Troubleshooting, on page 4

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 results 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 Marketplace.
- 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.

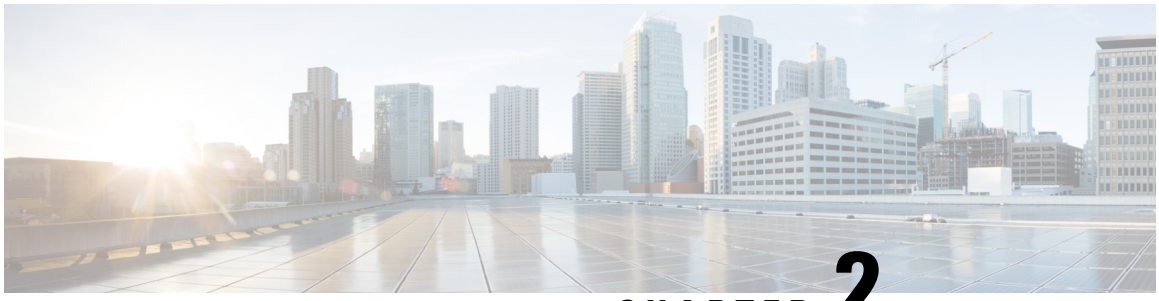
Documentation Feedback

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, on page 5
- Deployment Requirements, on page 6
- Cisco Catalyst 8000V with Two Network Interfaces, on page 7
- Licensing, on page 7

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.

Deployment Requirements

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.

List of resources

This 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.

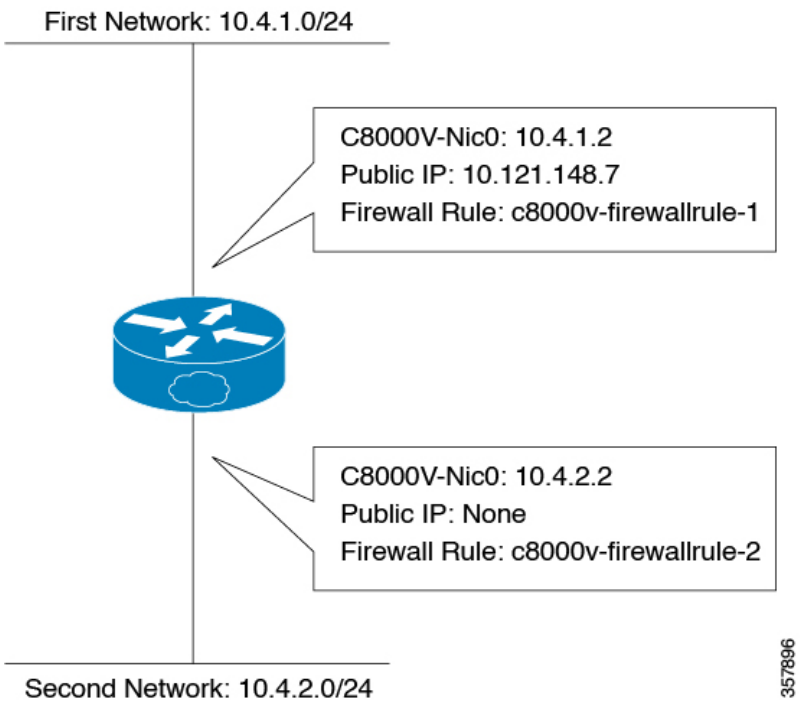
Supported instance types

To see the list of instances that are supported for deploying Cisco Catalyst 8000V in GCP, see the Compatibility Matrix.

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

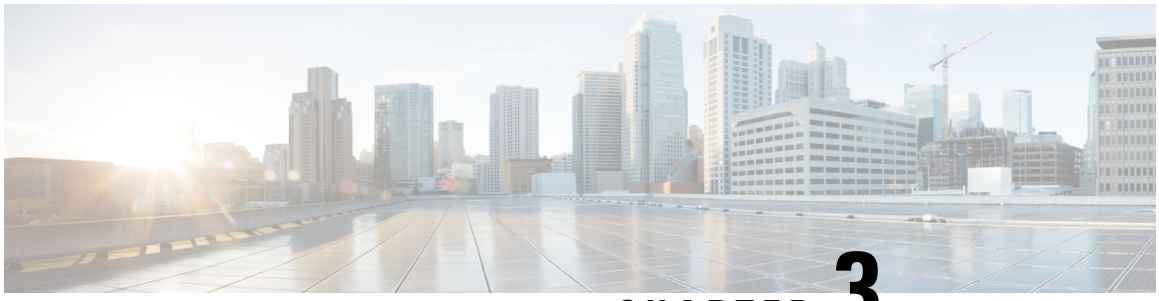
Cisco Catalyst 8000V supports the Bring Your Own License (BYOL) licensing model on GCP under the following licensing types:

- 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 by Using the GCP Console

This chapter specifies the procedure for deploying Cisco Catalyst 8000V on Google Cloud Platform (GCP) by using the GCP Console. The GCP Console is a web-based graphical user interface (GUI) that enables the deployment of Cisco Catalyst 8000V instances manually.

- Guidelines for Deploying Cisco Catalyst 8000V, on page 9
- Create an SSH Key, on page 10
- Create a VPC Network, on page 11
- Create an External IP Address, on page 11
- Deploy the Cisco Catalyst 8000V Instance, on page 12
- Access the Cisco Catalyst 8000V CLI, on page 15
- Configure a Sample Feature, on page 17

Guidelines for Deploying Cisco Catalyst 8000V

Before you deploy a Cisco Catalyst 8000V instance, see these guidelines and recommendations.

Restrictions

- You can choose the gVNIC option only if you're using an N4 instance. If you've deployed Cisco Catalyst 8000V in GCP by using N1 or N2 instance series, you cannot resize your existing VMs to N4 instance series due to the variation in disks.
- If you use the Infrastructure Manager through public worker pools to run the Terraform that is used for the VM deployment, your permissions might restrict the usage of public pools, especially if you use VPC Service Controls. To overcome this issue, use Google Cloud Build, which allows the creation of private worker pools with your own security and configuration. Use this method to deploy VMs if the standard GUI launch option is restricted.

  Download the Cisco Catalyst 8000V Terraform through the Command-Line Deployment option and add the private worker pool option in the Terraform deployment script. First, manually deploy the Cisco Catalyst 8000V instance via CLI and then add the worker pool parameters.

Guidelines

- A maximum transmission unit (MTU) is the size, in bytes, of the largest possible IP packet, including IP headers, layer 4 protocol headers, and layer 4 data, that can fit inside an Ethernet frame.

  When using gvNIC-based instances, the MTU of the GCP VPC will be inherited by the guest VM, that is, Cisco Catalyst 8000V. If the GCP VPC MTU is set below 1500 bytes, Cisco Catalyst 8000V uses this MTU value. If the GCP VPC MTU is set above 1500 bytes, Cisco Catalyst 8000V uses an MTU ranging from 1500 bytes up to the configured MTU of the VPC.

  For Cisco Catalyst 8000V deployments in SD-WAN mode that utilize bootstrap configuration from vManage, it is important that the configured MTU matches the GCP VPC MTU, especially when the VPC MTU is less than 1500 bytes. Any mismatch in MTU values could lead to deployment failures.

  To configure the MTU settings, see Maximum transmission unit.

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.

Procedure

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

A Virtual Private Cloud (VPC) network is a virtual version of a physical network that is implemented in the cloud service provider. Create a VPC network to provide connectivity to your VM instance.

Before you begin

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

Procedure

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 In the **Name** field, specify a name for the network.

Step 4 In the **Description** field, provide 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.

Procedure

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.
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.

Deploy the Cisco Catalyst 8000V Instance

This section specifies the overall deployment process for creating a Cisco Catalyst 8000V instance by using the GCP Console. See each of these sections to view the deployment workflow in detail.

Choose the Machine Configuration

Perform these steps to set the machine configuration for a VM instance.

Before you begin

- Billing must be enabled for your GCP account.
- Familiarize yourself with the basic concepts of creating a VM instance. For more information, see Creating and Starting a VM Instance.

Procedure

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

Step 2 In the **VM Instances** page, click the **Create Instance** button.

Step 3 Set these machine configurations:

Field	Description
Name	Specify the name for your VM in this field. Use only lowercase letters, for example, **`newtestvm`**.
Region	Choose the appropriate region from the drop-down list.

Field	Description
Zone	Specify the zone for your instance in this field. The zone is often a data center within a region.

Step 4 In the Machine Type area, choose one of these two settings:

- **Preset**: The preset amounts of vCPUs and memory will be selected.
- **Custom**: Choose this option to customize the number of cores (vCPUs), memory size, and GPUs for the VM instance.

Step 5 Choose the required machine type from the **Machine Type** drop-down list.

The machine type from a machine family determines the resources available to that instance. Each machine family is further organized into machine series and predefined machine types within each series. For example, within the N2 machine series in the general-purpose machine family, you can select the n2-standard-4 machine type.

To view the list of supported machine types and instances, see Supported Instance Types for Google Cloud Platform.

Step 6 Configure the **CPU Platform** and **Visible Core Count** settings, if applicable.

Configure the OS and Storage Properties

Perform these steps to configure the OS and storage properties for the VM instance.

Procedure

Step 1 In the Web UI, from the left navigation pane, choose **OS and storage**.

The system displays the OS details such as the image name, size, license type, and so on.

Step 2 To modify any of these options, choose **Change**.

Step 3 In the **Boot disk** pop-up window, configure the boot disk options.

Step 4 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 the **Public Images** tab. Select the image from the list of images displayed.
- To create the VM instance using a defined list of trusted images, choose the **Custom Images** tab and select the Cisco Catalyst 8000V image.

Note
If you chose the N4 instance family under Machine Type, you must choose a Cisco Catalyst 8000V 17.18.1 or later image only.

Step 5 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 6 In the **Disk Size** field, enter the boot disk size in GB.

Configure the Firewall and Networking Options

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

Procedure

Step 1 In the left navigation page, choose **Networking**.

Step 2 In the **Firewall** field, select either **Allow HTTP traffic**, **Allow HTTPS traffic**, or **Allow Load Balancer Health Checks** radio button.

Step 3 Optionally, choose a **Network Tag** for your instance. To learn more about tags, see Manage Tags for Resources.

Step 4 From the **Hostname** field, set a hostname for your VM instance, if required.

Step 5 From the **IP Forwarding** drop-down list, choose **On** to prevent the traffic from being blocked.

Step 6 Under **Network Interfaces**, configure these settings:

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

b) **Subnetwork**: Choose 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.

c) **Network Interface Card**: Choose the network interface card for the instance from this drop-down list. You can choose the gVNIC option only if you're using an N4 instance. If you've deployed Cisco Catalyst 8000V in GCP by using N1 or N2 instance series, you cannot resize your existing VMs to N4 instance series due to the variation in disks.

d) **IP Stack Type**: Choose **IPv4 and IPv6 (dual-stack)** or **IPv6 (single-stack)**.

e) **Alias IP Range**: Configure this field if you want to assign multiple internal IP addresses to the VM instance.

Step 7 (Optional) To add an interface, click the **Add a Network Interface** option.

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.

Procedure

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

Perform these steps to configure the SSH option for the VM instance. If required, add a startup script to customize the boot options for the instance.

Procedure

Step 1 In the left navigation pane, choose **Security**.

Step 2 In the **VM Access** area, in the **SSH Keys** field, paste the SSH key from the public key that you created as described in Create an SSH Key.

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

Step 3 In the **Advanced** area, add your startup configuration by copying and pasting the startup configuration information in the **Startup script** field.

If the startup script is not specified, the default configuration is applied.

Step 4 Click **Create**.

The newly created Cisco Catalyst 8000V VM instance starts. This process could take several minutes. To verify that the VM instance is running, click your VM on the **Instances** page. Choose **Logs** > **Serial Port**. The status appears in this page.

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 these 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.

Procedure

Step 1 **ssh -i** ~/.ssh/[*keyfile*] *username@ instance-external-IP* .

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.

Example:

```
ssh -i /users/joe/.ssh/mykey.pub joe@10.0.0.2
```

Step 2 **interface** *interface-name*

Enters interface configuration mode.

Example:

```
Router(config)# interface GigabitEthernet1
```

It is recommended that you perform the following steps to increase the interface's speed for each interface.

Step 3 **ip address dhcp**

Acquires an IP address on an interface from DHCP.

Example:

```
Router(config-if)# ip address dhcp
```

Step 4 **speed <interface speed>**

Sets the speed of the interface.

Example:

```
Router(config-if)# speed 10000
```

Step 5 **no negotiation auto**

Disables auto negotiation.

Example:

```
Router(config-if)# no negotiation auto
```

Step 6 **exit**

Exits the interface configuration mode.

Example:

```
Router(config-if)# exit
```

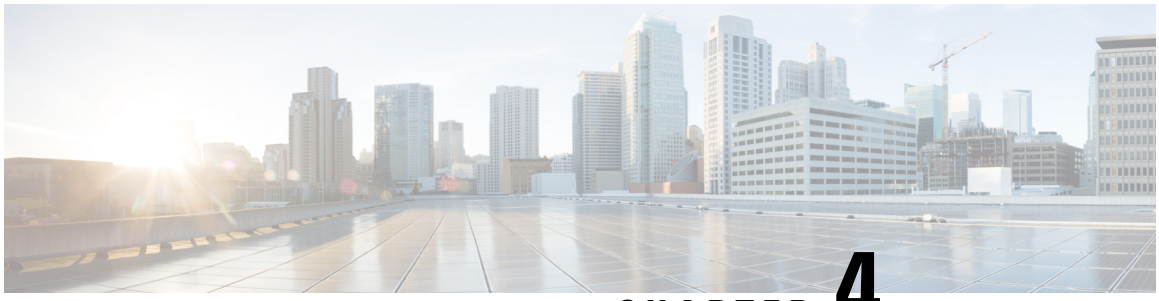
(Optional) Repeat steps 2 to 6 to increase the speed of the second interface of the Cisco Catalyst 8000V instance.

Configure 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 by Using Terraform

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

Terraform is an Infrastructure as code (IaC) tool that lets you provision and manage cloud infrastructure in GCP. To learn how to deploy Cisco Catalyst 8000V by using Terraform, perform the tasks in this chapter.

- Guidelines for Deploying Cisco Catalyst 8000V, on page 19
- Create an SSH Key, on page 20
- Create a VPC Network, on page 21
- Deploy the Cisco Catalyst 8000V Instance, on page 21
- Access the Cisco Catalyst 8000V CLI, on page 25
- Verify Interface Mapping, on page 26

Guidelines for Deploying Cisco Catalyst 8000V

Before you deploy a Cisco Catalyst 8000V instance, see these guidelines and recommendations.

Restrictions

- You can choose the gVNIC option only if you're using an N4 instance. If you've deployed Cisco Catalyst 8000V in GCP by using N1 or N2 instance series, you cannot resize your existing VMs to N4 instance series due to the variation in disks.
- If you use the Infrastructure Manager through public worker pools to run the Terraform that is used for the VM deployment, your permissions might restrict the usage of public pools, especially if you use VPC Service Controls. To overcome this issue, use Google Cloud Build, which allows the creation of private worker pools with your own security and configuration. Use this method to deploy VMs if the standard GUI launch option is restricted.

  Download the Cisco Catalyst 8000V Terraform through the Command-Line Deployment option and add the private worker pool option in the Terraform deployment script. First, manually deploy the Cisco Catalyst 8000V instance via CLI and then add the worker pool parameters.

Guidelines

- A maximum transmission unit (MTU) is the size, in bytes, of the largest possible IP packet, including IP headers, layer 4 protocol headers, and layer 4 data, that can fit inside an Ethernet frame.

  When using gvNIC-based instances, the MTU of the GCP VPC will be inherited by the guest VM, that is, Cisco Catalyst 8000V. If the GCP VPC MTU is set below 1500 bytes, Cisco Catalyst 8000V uses this MTU value. If the GCP VPC MTU is set above 1500 bytes, Cisco Catalyst 8000V uses an MTU ranging from 1500 bytes up to the configured MTU of the VPC.

  For Cisco Catalyst 8000V deployments in SD-WAN mode that utilize bootstrap configuration from vManage, it is important that the configured MTU matches the GCP VPC MTU, especially when the VPC MTU is less than 1500 bytes. Any mismatch in MTU values could lead to deployment failures.

  To configure the MTU settings, see Maximum transmission unit.

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.

Procedure

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

A Virtual Private Cloud (VPC) network is a virtual version of a physical network that is implemented in the cloud service provider. Create a VPC network to provide connectivity to your VM instance.

Before you begin

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

Procedure

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 In the **Name** field, specify a name for the network.

Step 4 In the **Description** field, provide 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 Instance

This section specifies the overall deployment process for creating a Cisco Catalyst 8000V instance by using Terraform in GCP. See each of these sections to learn about each process in detail.

Configure the Template Settings

Procedure

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 window, in the **Deployment name** field, provide the depolyment name. By default, this field displays the name in the *cisco-<deployment number>* format.

Step 4 From the **Deployment Service Account** field, click one of the following radio buttons:

- **Existing Account**: Choose this option if you already have a service account. If you choose this option, the system displays the **Select A Service Account** drop-down field. Choose your service account from this drop-down list.
- **New Account**: Choose this option if you want to create a service account. For more information on creating service accounts, see Service Accounts.

Step 5 In the **Instance Name** field, specify 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])?)'">).

Step 6 In the **Username** field, specify the username to be used to access the Cisco Catalyst 8000V instance.

Step 7 In the **Instance SSH Key** field, specify the public key to be used for SSHing into the instance. To know how to create an ssh-key, see SSH-Key.

Step 8 In the **Image Version** field, choose the version of the Cisco Catalyst 8000V, for example, **`17.16`**.

What to do next

Configure the machine size and bootdisk settings.

Configure the Machine and Disk Properties

This section tells you how to configure the machine and disk properties while deploying a Cisco Catalyst 8000V instance in GCP by using Terraform.

Before you begin

Ensure you've configured the VM template settings.

Procedure

Step 1 In the New Cisco Catalyst 8000V Deployment window, from the **Zone** drop-down list, choose the Zone where your Cisco Catalyst 8000V is deployed.

Step 2 From the **Machine Type** field, choose the size of the Cisco Catalyst 8000V that you want to deploy. For more information on Cisco Catalyst 8000V sizes, see MachineTypes.

Step 3 From the **Bootdisk** area, configure the following settings:

a) **Bootdisk type**: Choose the bootdisk type for your deployment. By default, the SSD Persistent disk is selected. Cisco recommends that you use the default Boot disk type.

b) **Boot disk size in GB**: Choose the bootdisk size for your depolyment. The default value is 10 GB. Cisco recommends that you use the default Boot disk size.

Step 4 To enhance the performance, disable Hyper-Threading on your GCP instance. To disable Hyper-Threading, configure the vCPU to core ratio when you create your instance. For an existing instance, edit the Machine Configuration to disable Hyper-Threading. Choose **Machine configuration** > **Advanced Configurations** and configure the **vCPUs to core ratio** field to **1 vCPU per core**.

What to do next

Configure the network settings and the interfaces for your deployment.

Configure the Network Settings and Interfaces

This task instructs you on how to configure the network settings and add interfaces when you deploy a Cisco Catalyst 8000V instance in GCP by using Terraform.

Procedure

Step 1 In the New Cisco Catalyst 8000V Deployment window, navigate to the **Networking** area.

Step 2 Under **Network Interfaces**, choose the network in the region where you want to deploy the Cisco Catalyst 8000V instance from the Network field.

You must create the network before you create the Cisco Catalyst 8000V instance. Ensure that at least one subnet is associated to that network. For more information about networks, see Virtual Private Cloud Network Overview.

Step 3 From the **Subnetwork** field, choose 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.

Step 4 To set gVNIC as the network interface, expand the **Advanced Options** > **Networking** section. From the **Network Interface Card** drop-down list, choose **gVNIC**.

Note
You can choose the gVNIC option only if you're using an N4 instance. If you've deployed Cisco Catalyst 8000V in GCP by using N1 or N2 instance series, you cannot resize your existing VMs to N4 instance series due to the variation in disks.

Step 5 From the **External IP** field, choose one of these options to configure the public IP address that you must use to SSH into the Cisco Catalyst 8000V instance.

- **Static**: Choose this option if you want to set a static address as this external IP address.
- **Ephemeral**: Choose this option if you want to use this public IP address when you start an SSH session from a terminal server.
- **None**: Choose this option to not configure any external IP address.

For more information about IP addresses, see IP Addresses.

Step 6 To add an additional interface, click the **Add Additional Interface** option. Configure the **Network**, **Subnetwork**, and **External IP** fields to add the additional interface.

Note
You can configure a maximum of 8 interfaces only, for this deployment.

What to do next

Configure the firewall settings.

Configure the Firewall Settings

Refer to this section if you want to configure the firewall settings for your network when you deploy Cisco Catalyst 8000V in GCP.

Procedure

Step 1 In the New Cisco Catalyst 8000V Deployment window, navigate to the **Firewall** area.

Step 2 Configure the firewall rule associated to the network by configuring these settings:

a) **Allow TCP port 22 traffic from the internet**: Choose this option to create a firewall rule that allows incoming SSH connections on TCP port 22. After you choose this option, you can set the **Source IP ranges for TCP port 22 traffic**.

b) **Allow HTTP traffic from the internet**: Choose this option to create a firewall rule that allows incoming traffic on TCP port 80.

c) **Allow TCP port 21 traffic from the internet**: Choose this option to create a firewall rule that alows incoming traffic on TCP port 21.

d) **IP Forwarding**: Choose this option to enable IP forwarding for your VM instance.

You can also create additional Firewall rules for your deployment. For more information on firewall rules, see Firewalls in VPC Networking and Firewalls.

What to do next

Add the startup script by copying and pasting the script or by adding the URL to your configuration file.

Add the Startup Script

Refer to this section to learn how to add startup script or a startup configuraiton for Cisco Catalyst 8000V deployed in GCP.

Procedure

Step 1 On the New Cisco Catalyst 8000V Deployment window, navigate to the **Advanced** area.

Step 2 Add your startup configuration by configuring one of these two fields:

- **Startup-script**: Copy and paste the startup configuration information in this field. Note that the configuration information should not exceed 10000 characters when you choose this option.
- **Custom Data File URL**: Paste the URL to the custom data file in this field. This URL must be publicly accessible. For longer configuration files, use this option to add your startup script.

Step 3 Click **Deploy** to deploy the Cisco Catalyst 8000V instance by using GCP Terraform.

After the deployment is complete, a publicly accessible storage bucket, containing all the information about the Terraform, is created. It is recommded that you make the storage bucket private.

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 these 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.

Procedure

Step 1 **ssh -i** ~/.ssh/[*keyfile*] *username@ instance-external-IP* .

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.

Example:

```
ssh -i /users/joe/.ssh/mykey.pub joe@10.0.0.2
```

Step 2 **interface** *interface-name*

Enters interface configuration mode.

Example:

```
Router(config)# interface GigabitEthernet1
```

It is recommended that you perform the following steps to increase the interface's speed for each interface.

Step 3 **ip address dhcp**

Acquires an IP address on an interface from DHCP.

Example:

```
Router(config-if)# ip address dhcp
```

Step 4 **speed <interface speed>**

Sets the speed of the interface.

Example:

```
Router(config-if)# speed 10000
```

Step 5 **no negotiation auto**

Disables auto negotiation.

Example:

```
Router(config-if)# no negotiation auto
```

Step 6 **exit**

Exits the interface configuration mode.

Example:

```
Router(config-if)# exit
```

(Optional) Repeat steps 2 to 6 to increase the speed of the second interface of the Cisco Catalyst 8000V instance.

Verify Interface Mapping

When you boot the Cisco Catalyst 8000V instance for the first time, the router interfaces are mapped to the logical vNIC interfaces that were added when the VM was created.

After you boot the Cisco Catalyst 8000V instance, you can verify the mapping between the logical interface on the router with the vNIC and the vNIC MAC address by performing this task.

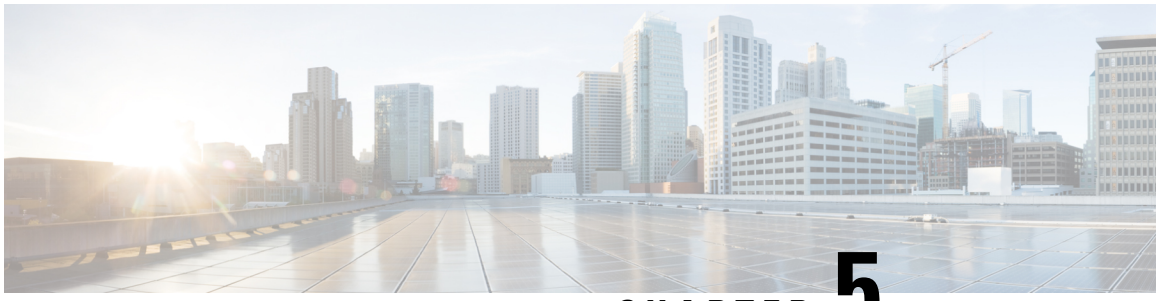
Procedure

Run the **show platform software vnic-if interface-mapping** command.

Displays the logical interface that the Cisco Catalyst 8000V instance uses to map to the interface on the hypervisor.

```
C8000v-router# show platform software vnic-if interface-mapping
------------------------------------------------------------
Interface Name        Driver Name         Mac Addr
------------------------------------------------------------
GigabitEthernet4       net_gve            4201.0a5a.aa02
GigabitEthernet3       net_gve            4201.0a5a.820c
GigabitEthernet2       net_gve            4201.0a5a.170c
GigabitEthernet1       net_gve            4201.0a5a.f307
------------------------------------------------------------
```

Note the **net_gve** value under **Driver Name**. This indicates that gVNIC interface is being used by the 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, on page 27
- Custom Routes in the Same VPC Network, on page 28
- Routing Between VPC Networks or On-Premises Networks, on page 28

Create Routes

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

Procedure

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.

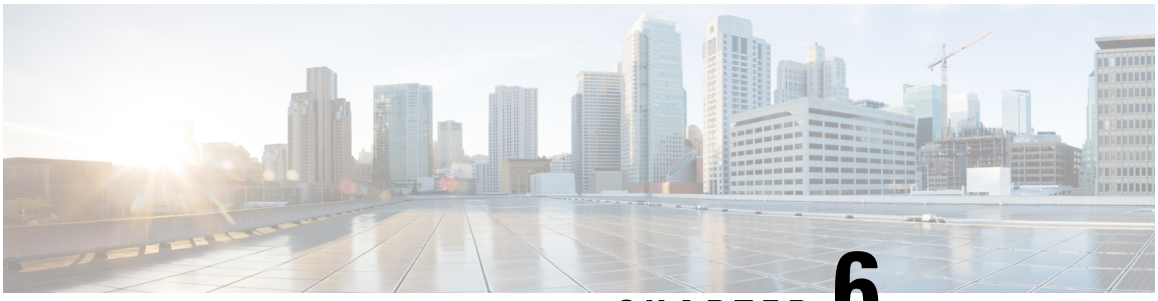
Custom Routes in the Same VPC Network

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

Configure 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
```