Deploy a CSR1000v/C8000v on Google Cloud Platform

Contents

Introduction Prerequisites Requirements **Components Used Background Information Project Setup** Step 1. Ensure a Valid and Active Project for the Account. Step 2. Create a New VPC and Subnet. Step 3. Virtual Instance Deployment. Verify Deployment Connect Remotely to the New Instance Log in to CSR1000v/C8000v with Bash Terminal Log in to CSR1000v/C8000v with PuTTY Log in to CSR1000v/C8000V with SecureCRT Additional VM Log in Methods Authorize Additional Users to Log in to CSR1000v/C8000v in GCP Configure a New Username/Password Configure a New User with SSH Key Verify Configured Users on Log in to CSR1000v/C8000v **Troubleshoot** If the "Operation timed out" Error Message is Displayed. If a Password is Required **Related Information**

Introduction

This document describes the procedure to deploy and configure a Cisco Cloud Services Router 1000v (CSR1000v) and Catalyst 8000v (C800v) Edge Router on Google Cloud Platform (GCP).

Contributed by Eric Garcia, Ricardo Neri, Cisco TAC Engineers.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

• Virtualization technologies / Virtual Machines (VMs)

Cloud Platforms

Components Used

- An active subscription to Google Cloud Platform with a project created
- GCP console
- GCP marketplace
- Bash terminal, Putty, or SecureCRT
- Public and private Secure Shell (SSH) Keys

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

From 17.4.1 onwards, the CSR1000v becomes C8000v with the same functionality but new features added such as SDWAN and DNA licensing. For further reference, please verify the official products datasheet:

Cisco Cloud Services Router 1000v Data Sheet

Cisco Catalyst 8000V Edge Software Data Sheet

Therefore, this guide is applicable for the installation of both CSR1000v and C8000v routers.

Project Setup

Note: At the moment this document is written, new users have 300USD of free credits to fully explore GCP as Free Tier for one year. This is defined by Google and it is not under Cisco control.

Note: This document requires the creation of public and private SSH keys. For additional information, please refer to <u>Generate an Instance SSH Key to Deploy a CSR1000v in</u> <u>Google Cloud Platform</u>

Step 1. Ensure a Valid and Active Project for the Account.

Ensure your account has a valid and active project, these must be associated with a group with permissions for Compute Engine.

For this example deployment, a created project in the GCP is used.

Note: To create a new project, please refer to Create and manage projects.

Step 2. Create a New VPC and Subnet.

Create a new Virtual Private Cloud (VPC) and a subnet that must be associated with the CSR1000v instance.

It is possible to use the default VPC or a previously created VPC and subnet.

In the console dashboard, select **VPC network > VPC networks** as shown in the image.



Select Create VPC Network as shown in the image.

H	VPC network	VPC networks	REATE VPC NETWORK	C REFRESH				
-								
8	VPC networks	Name 🛧 Region	Subnets	мти 😧	Mode	IP address ranges	Gateways	Firewall Rules
땁	External IP addresses	✓ default	24	1460	Auto 👻			22
88	Firewall	us-central1	default			10.128.0.0/20	10.128.0.1	
		europe-west1	default			10.132.0.0/20	10.132.0.1	
24	Routes	us-west1	default			10.138.0.0/20	10.138.0.1	
\diamond	VPC network peering	asia-east1	default			10.140.0.0/20	10.140.0.1	
bd	Shared VPC	us-east1	default			10.142.0.0/20	10.142.0.1	
~		asia-northeast	default			10.146.0.0/20	10.146.0.1	
\Leftrightarrow	Serverless VPC access	asia-southeast	1 default			10.148.0.0/20	10.148.0.1	
រង្វ៉ែរ	Packet mirroring	us-east4	default			10.150.0.0/20	10.150.0.1	
		australia-south	east1 default			10.152.0.0/20	10.152.0.1	

Note: Currently, CSR1000v is only deployed in the us-central region on GCP.

Configure the VPC name as shown in the image.







Configure the subnet name associated with the VPC and select region us-central1.

Assign a valid IP address range within the us-central1 CIDR of 10.128.0.0/20. as shown in the image.

Leave other settings as default and select create button:

Subnets

Subnets let you create your own private cloud topology within Google Cloud. Click Automatic to create a subnet in each region, or click Custom to manually define the subnets. Learn more

Subnet creation mode

- O Custom
- Automatic

New subnet	i ^
Name * csr-subnet	0
Lowercase letters, numbers, hyphens allowed	
dd a description	
add a description Region *	
dd a description Region * us-central1	- 0
dd a description Region * us-central1 IP address range *	- 0

Note: If "automatic" is selected, GCP assigns an automatic valid range within the region CIDR.

Once the creation process finishes, the new VPC appears in the **VPC networks** section as shown in the image.

VPC networks		CREATE VPC NETWORK	C REFRESH			
Name 个	Region	Subnets	ΜΤυ 😧	Mode	IP address ranges	Gateways
▼ csr-vpc		1	1460	Custom		
	us-central1	csr-subnet	t		10.10.1.0/24	10.10.1.1

Step 3. Virtual Instance Deployment.

In **Compute Engine** section, select **Compute Engine > VM instances** as shown in the image.

A	Home	>	OMMENDATIONS
COMP	PUTE		
۰Ô۰	App Engine	>	VIRTUAL MACHINES
			VM instances
۲	Compute Engine	∓ > `	Instance templates
\$	Kubernetes Engine	>	Sole-tenant nodes
(…)	Cloud Functions		Machine images
)≽	Cloud Run		Migrate for Compute Engine
\$	VMware Engine		Committed use discounts

Once in the VM dashboard, select the Create Instance tab as shown in the image.

Compute Engine	VM instances	CREATE INSTANCE 📩 IMPORT VM	C REFRESH			
Virtual machines	INSTANCES	INSTANCE SCHEDULE				
VM instances	VM instances are highly configurable virtual machines for running workloads on Google					
instance templates	infrastructure. Learn mo	infrastructure. Learn more				

Use GCP marketplace as shown in the image, in order to display Cisco products.



In the search bar, type **Cisco CSR** or **Catalyst C8000v**, choose model and version that fits your requirements and select **Launch**.

For this example deployment, the first option was selected as shown in the image.

🖄 Marketplace

Q csr 1000v

Marketplace > "csr 1000v" > Virtual machines

= Filter Type to filter		Virtual mad	chines
Category	^	7 results	
Compute	(4)	7100010	
Networking	(7)	alialia cisco	Cisco Cloud Services Router 1000V (CSR 1000V) Cisco Systems
Туре			The Bring Your Own License (BYOL) of Cisco Cloud Services Router (CSR1000V) delivers ent Google Compute Platform. This software supports all the four CSR Technology packages. The spables enterprise IT to deploy the same enterprise class patworking equipacity in the cloud the
Virtual machines	0		enables enterprise in to deploy the same enterprise-class networking services in the cloud th

cisco

Cisco Cloud Services Router 1000V - 16.12 - BYOL

Cisco Systems

The Bring Your Own License (BYOL) of Cisco Cloud Services Router (CSR1000V) delivers ent Google Compute Platform. This software supports all the four CSR Technology packages. Th enables enterprise IT to deploy the same enterprise-class networking services in the cloud th



Cisco Cloud Services Router 1000V - 17.2.1r - BYOL

Cisco Systems

The Bring Your Own License (BYOL) of Cisco Cloud Services Router (CSR1000V) delivers ent Google Compute Platform. This software supports all the four CSR Technology packages. The enables enterprise IT to deploy the same enterprise-class networking services in the cloud the

uluiu cisco

Cisco Cloud Services Router 1000V - 17.3 - BYOL

Cisco Systems

The Bring Your Own License (BYOL) of Cisco Cloud Services Router (CSR1000V) delivers ent Google Compute Platform. This software supports all the four CSR Technology packages. The enables enterprise IT to deploy the same enterprise-class networking services in the cloud the

×

🖄 Marketplace	Q cata	alyst 8000v	×
Marketplace > "catalyst 80	000v edge sof	tware - byol" 🗲 Virtua	Imachines
= Filter Type to filter		Virtual mad	chines
Category	^	1 result	
Compute	(1)	ahaha	Catalyst 8000V Edge Software - BYOL Cisco Systems
Туре		cisco	As part of Cisco's Cloud connect portfolio, the Bring Your Own License (BYOL) version of 0 8000V) delivers the maximum performance for virtual enterprise-class networking service
Virtual machines	0		the Catalyst 8000V (C8000V) DNA packages and supports the high-performance versions

Note: BYOL stands for "Bring Your Own License".

Note: Currently, GCP does not support Pay As You Go (PAYG) model.

GCP requires to enter the configuration values that must be associated with the VM, as shown in the image:

A username and SSH public key is required to deploy a CSR1000v/C8000v in GCP as shown in the image. Please refer to <u>Generate an Instance SSH Key to Deploy a CSR1000v in Google Cloud</u> <u>Platform</u> if the SSH keys have not been created.

New Cisco Cloud Services Router 1000V (CSR 1000V)

Deployment name

cisco-csr-1000v-23

Instance name

csr-cisco

Username

cisco

Instance SSH Key

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC901XkfpuBgq5QR69RsG1Qn

us-central1-f								
Machine type 📀								
4 vCPUs 💌	15 GB memory	Customize						
Poot Dick								
DOUL DISK								
Boot disk type 📀								

10

Select the VPC and subnet created before and choose Ephemeral in external IP, in order to have a Public IP associated with the instance as shown in the image.

After this is configured. Select the **launch** button.

Networking

Network csr-vpc Subnetwork csr-subnet (10.10.1.0/24) External IP Ephemeral Firewall Add tags and firewall rules to allow specific network traffic from the Internet

- Allow TCP port 22 traffic
- Allow HTTP traffic
- Allow TCP port 21 traffic

Note: Port 22 is needed to connect to the CSR instance via SSH. The HTTP port is optional.

Once the deployment is completed, select **Compute Engine > VM instances** in order to verify that the new CSR1000v was deployed successfully as shown in the image.

VM instances		CREATE INSTANCE	🛃 IMPOI	RT VM C	REFRESH	▶ START / RESUME		STOP	
Filter VM insta	ances						0	Column	ns 🔻
Name ^	Zone	Recommendation	In use by	Internal IP		External IP	Co	nnect	
🗌 🥑 csr-cisco	us-central1	-f		10.10.1.2 (nic	:0)		SS	SH 🗸	:

Verify Deployment

Connect Remotely to the New Instance

The most common methods to log in to a CSR1000v/C8000V in GCP are the command line in a Bash terminal, Putty and SecureCRT. In this section, the configuration needed to connect with the previous methods.

Log in to CSR1000v/C8000v with Bash Terminal

The syntax needed to connect remotely to the new CSR is:

Example:

\$ ssh -i CSR-sshkey <snip>@X.X.X.X
The authenticity of host 'X.X.X.X (X.X.X.X)' can't be established.
RSA key fingerprint is SHA256:c3JsVDEt68CeUFGhp9lrYz7tU07htbsPhAwanh3feC4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'X.X.X.X' (RSA) to the list of known hosts.
If the connection is successful, CSR1000v prompt is displayed

```
$ ssh -i CSR-sshkey <snip>@X.X.X.X
csr-cisco# show version
Cisco IOS XE Software, Version 16.09.01
Cisco IOS Software [Fuji], Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version
16.9.1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Tue 17-Jul-18 16:57 by mcpre
```

Log in to CSR1000v/C8000v with PuTTY

To connect with Putty, use the PuTTYgen application in order to convert the private key from PEM to PPK format.

Please refer to Convert Pem to Ppk File Using PuTTYgen for additional information.

Once the private key is generated in the proper format, you have to specify the path in Putty.

Select the **Private key file for authentication** section in the auth option of the SSH **connection** menu.

Browse to the folder where the key is stored and select the created key. In this example, the images show the graphical view of the Putty menu and the desired state:



🕵 PuTTY Configurati	on	? ×	(
Category:			
Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Colours Colours Connection Data Proxy Telnet	^	Options controlling SSH authentication Display pre-authentication banner (SSH-2 only) Bypass authentication entirely (SSH-2 only) Authentication methods Attempt authentication using Pageant Attempt TIS or CryptoCard auth (SSH-1) Attempt "keyboard-interactive" auth (SSH-2) Authentication parameters Allow agent forwarding Allow attempted changes of usemame in SSH-2 Private key file for authentication: C:\Users\textstyle Ssh\key2_ppk.ppk	
Rlogin SSH Kex Host keys Cipher Auth	✓	Open Cancel	

Once the proper key is selected, return to the main menu and use the external IP address of the CSR1000v instance to connect via SSH as shown in the image.

🕵 PuTTY Configuratio	on		?	×
Category:				
 Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour 	^	Basic options for your PuTTY ses Specify the destination you want to connect Host Name (or IP address) Connection type: Raw Telnet Rlogin SSH Load, save or delete a stored session	ision t to Port 22 O Se	erial
		Saved Sessions Default Settings	Load Save Delet	d e
Kex Host keys Cipher Auth About	✓ Help	Close window on exit: Always Never Only on cle	ean exit Canc	el

Note: Username/password defined in the SSH keys generated are requested to log in.

```
log in as: cisco
Authenticating with public key "imported-openssh-key"
Passphrase for key "imported-openssh-key":
```

csr-cisco#

Log in to CSR1000v/C8000V with SecureCRT

SecureCRT requires the private key in PEM format, which is the default format for the private keys.

In SecureCRT specify the path to the private key in the menu:

File > Quick Connect > Authentication > Uncheck Password > PublicKey > Properties.

The image shows the expected window:

Quick Connect	×
Protocol: SSH2	~
Hostname:	
Port: 22 Fire	wall: None \checkmark
Username:	
Authentication Password PublicKey Keyboard Interactive GSSAPI	Properties
Show quick connect on startup	 Save session ✓ Open in a tab Connect Cancel

Select Use session public key string > Select Use identity or certificate file > Select ... button > Navigate to the directory and select the desired key > Select OK as shown in the image.

se global public key setting	Use s	ession public key set	ting OK
ssion settings) Use identity or certificate file			Canc
C:\Users\\.ssh\key2			
) Use a certificate from your personal CAPI	store or a PKCS #1	1 provider DLL	_
CAPI V DLL:			
Certificate to use: <pre><try all="" certificates=""></try></pre>			
Get username from certificate: Com	mon Name 🗠		
Use certificate as raw SSH2 key (server d	oes not support X.5	09)	
ngerprint:			_
HA-2: e0:82:1d:a8:67:45:eb:96:31:12:74: HA-1: 79:04:f3:8a:0f:99:57:ee:d0:6b:4f:8 D5: da:82:5e:30:f8:22:ec:a0:04:18:71:7e	28:ac:1a:4b:fa:b6: 4:bb:93:d3:d1:99:6 ::fe:de:40:63	5e:67:e9:85:c9:06:0 3:70:a3	d:3-
c			>

Finally, connect to the instance's external IP address via SSH as shown in the image.

Quick Connect		×
Protocol: Hostname: Port: Username:	SSH2 ~	None ~
Authentication Authentication PublicKey Keyboard GSSAPI Password	Interactive	 Properties
Show quick co	onnect on startup	 Save session ✓ Open in a tab Connect Cancel

Note: Username/password defined in the SSH keys generated are requested to log in.

```
csr-cisco# show logging
Syslog logging: enabled (0 messages dropped, 3 messages rate-limited, 0 flushes, 0 overruns, xml
disabled, filtering disabled)
No Active Message Discriminator.
<snip>
*Jan 7 23:16:13.315: %SEC_log in-5-log in_SUCCESS: log in Success [user: cisco] [Source:
X.X.X.X] [localport: 22] at 23:16:13 UTC Thu Jan 7 2021
csr-cisco#
```

Additional VM Log in Methods

Note: Please refer to Connect to Linux VMs using advanced methods documentation.

Authorize Additional Users to Log in to CSR1000v/C8000v in GCP

Once logged in to the CSR1000v instance is successful, it is possible to configure additional users with these methods:

Configure a New Username/Password

Use these commands to configure a new user and password:

enable
configure terminal
username <username> privilege <privilege level> secret <password>
end
Example:

csr-cisco# configure terminal Enter configuration commands, one per line. End with CNTL/Z. csr-cisco(config)# csr-cisco(config)# username cisco privilege 15 secret cisco csr-cisco(config)# end csr-cisco# A new user is now able to log in to the CSR1000v/C8000v instance.

Configure a New User with SSH Key

In order to get access to the CSR1000v instance, configure the public key. SSH keys in the instance metadata do not provide access to CSR1000v.

Use these commands to configure a new user with an SSH key:

```
configure terminal
ip ssh pubkey-chain
username <username>
key-string
<public ssh key>
exit
end
```

Note: The maximum line length at the Cisco CLI is 254 characters thus the key string might not fit this limitation, it is convenient to wrap the key string to fit a terminal line. The details about how to overcome this limitation are explained in <u>Generate an Instance SSH Key to</u> <u>Deploy a CSR1000v in Google Cloud Platform</u>

```
$ fold -b -w 72 /mnt/c/Users/ricneri/.ssh/key2.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQD1dzZ/iJi3VeHs4qDoxOP67jebaGwC6vkC
n29bwSQ4CPJGVRLcVSNPcPPqVydiXVEOG8e9gFszkpk6c2meO+TRsSLiwHigv281yw5xhn1U
ck/AYpy9E6TyEEu9w6Fz0xTG2Qhe1n9b5Les6K9PFP/mR6WUMbfmaFredV/sADnODPO+OfTK
/OZPg34DNfcFhg1ja5GzudRb3S4nBBhDzuVrVC9RbA4PHVMXrLbIfq1ks3PCVGOtW1HxxTU4
FCkmEAg4NEqMVLSm26nLvrNK6z71RMcIKZZcST+SL61Qv33gkUKIoGB9qx/+D1RvurVXfCdq
3Cmxm2swHmb6MlrEtqIv cisco
$
```

```
csr-cisco# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
csr-cisco(config)#
```

```
csr-cisco(config)# ip ssh pubkey-chain
csr-cisco(conf-ssh-pubkey)# username cisco
csr-cisco(conf-ssh-pubkey-user)# key-string
csr-cisco(conf-ssh-pubkey-data)#ssh-rsa
```

```
AAAAB3NzaClyc2EAAAADAQABAAABAQDldzZ/iJi3VeHs4qDoxOP67jebaGwC
csr-cisco(conf-ssh-pubkey-
data)#6vkCn29bwSQ4CPJGVRLcVSNPcPPqVydiXVEOG8e9gFszkpk6c2meO+TRsSLiwHigv281
csr-cisco(conf-ssh-pubkey-
data)#yw5xhn1Uck/AYpy9E6TyEEu9w6Fz0xTG2Qhe1n9b5Les6K9PFP/mR6WUMbfmaFredV/s
csr-cisco(conf-ssh-pubkey-
data)#ADnODP0+OfTK/OZPg34DNfcFhglja5GzudRb3S4nBBhDzuVrVC9RbA4PHVMXrLbIfqlk
csr-cisco(conf-ssh-pubkey-
data)#s3PCVGOtW1HxxTU4FCkmEAg4NEqMVLSm26nLvrNK6z71RMcIKZZcST+SL6lQv33gkUKI
csr-cisco(conf-ssh-pubkey-data)#oGB9qx/+DlRvurVXfCdq3Cmxm2swHmb6MlrEtqIv cisco
csr-cisco(conf-ssh-pubkey-user)# end
csr-cisco(
```

Verify Configured Users on Log in to CSR1000v/C8000v

In order to confirm the configuration was properly set, please log in with the credentials created or with the private key pair for the public key with the additional credential.

From the router side, see the success log-in log with the terminal IP address.

```
csr-cisco# show clock
*00:21:56.975 UTC Fri Jan 8 2021
csr-cisco#
csr-cisco# show logging
Syslog logging: enabled (0 messages dropped, 3 messages rate-limited, 0 flushes, 0 overruns, xml
disabled, filtering disabled)
<snip>
*Jan 8 00:22:24.907: %SEC_log in-5-log in_SUCCESS: log in Success [user: <snip>] [Source:
<snip>] [localport: 22] at 00:22:24 UTC Fri Jan 8 2021
csr-cisco#
```

Troubleshoot

If the "Operation timed out" Error Message is Displayed.

```
$ ssh -i CSR-sshkey <snip>@X.X.X.X
ssh: connect to host <snip> port 22: Operation timed out
Possible causes:
```

- The instance hasn't finished its deployment.
- The Public address is not the one assigned to nic0 in the VM.

Solution:

Wait for the VM deployment to complete. Usually, a CSR1000v deployment takes up to 5 minutes to complete.

If a Password is Required

If a password is required:

```
$ ssh -i CSR-sshkey <snip>@X.X.X.X
Password:
Password:
Possible cause:
```

• The username or private key is incorrect. Solution:

- Ensure the username is the same that was specified when CSR1000v/C8000v was deployed.
- Ensure the private key is the same you included at the deployment time.

Related Information

- <u>Cisco Cloud Services Router 1000v Data Sheet</u>
- <u>Technical Support & Documentation Cisco Systems</u>