

Implemente un CSR1000v/C8000v en la plataforma de nube de Google

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configuración del proyecto](#)

[Paso 1. Asegúrese de que hay un proyecto válido y activo para la cuenta.](#)

[Paso 2. Cree un nuevo VPC y una nueva subred.](#)

[Paso 3. Implementación de instancias virtuales.](#)

[Verificar implementación](#)

[Conexión remota a la nueva instancia](#)

[Inicie sesión en CSR1000v/C8000v con Bash Terminal](#)

[Inicie sesión en CSR1000v/C8000v con PuTTY](#)

[Inicie sesión en CSR1000v/C8000V con SecureCRT](#)

[Métodos de inicio de sesión de VM adicionales](#)

[Autorizar a usuarios adicionales a iniciar sesión en CSR1000v/C8000v en GCP](#)

[Configurar un nuevo nombre de usuario/contraseña](#)

[Configuración de un nuevo usuario con clave SSH](#)

[Verificar usuarios configurados al iniciar sesión en CSR1000v/C8000v](#)

[Troubleshoot](#)

[Si se muestra el mensaje de error "Operation Timed Out".](#)

[Si se requiere una contraseña](#)

[Información Relacionada](#)

Introducción

Este documento describe el procedimiento para implementar y configurar un Cisco CSR1000v y un Catalyst 8000v (C800v) en la Plataforma de nube de Google (GCP).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Tecnologías de virtualización/máquinas virtuales (VM)

- Plataformas de nube

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Una suscripción activa a la plataforma de nube de Google con un proyecto creado
- consola GCP
- GCP Marketplace
- Terminal Bash, Masilla o SecureCRT
- Claves de Secure Shell (SSH) públicas y privadas

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

A partir de la versión 17.4.1, el CSR1000v se convierte en C8000v con la misma funcionalidad, pero se han añadido nuevas funciones, como las licencias SD-WAN y Cisco DNA. Para más información, consulte la ficha técnica oficial de los productos:

[Hoja de datos del router de servicios en la nube 1000v de Cisco](#)

[Hoja de datos del software Cisco Catalyst 8000V Edge](#)

Por lo tanto, esta guía es aplicable para la instalación de los routers CSR1000v y C8000v.

Configuración del proyecto

 Nota: En el momento en que se escribe este documento, los nuevos usuarios tienen 300USD de créditos gratuitos para explorar completamente el GCP como Free Tier durante un año. Esto lo define Google y no está bajo el control de Cisco.

 Nota: Este documento requiere la creación de claves SSH públicas y privadas. Para obtener información adicional, consulte [Generar una clave SSH de instancia para implementar un CSR1000v en la plataforma de nube de Google](#)

Paso 1. Asegúrese de que hay un proyecto válido y activo para la cuenta.

Asegúrese de que su cuenta tiene un proyecto válido y activo, que debe estar asociado a un

grupo con permisos para Motor de cálculo.

Para esta implementación de ejemplo, se utiliza un proyecto creado en el GCP.

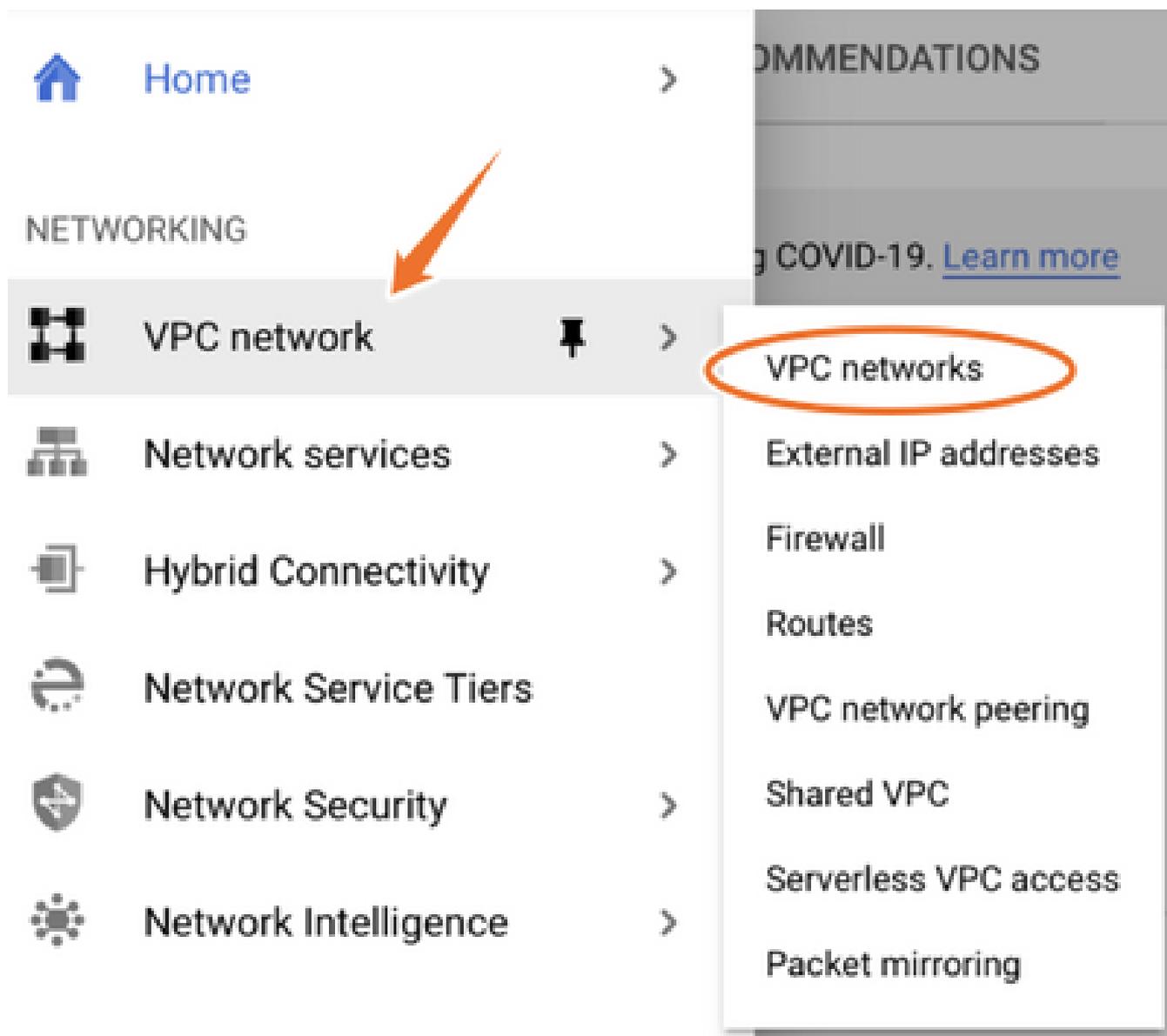
 Nota: Para crear un nuevo proyecto, consulte [Creación y gestión de proyectos](#).

Paso 2. Cree un nuevo VPC y una nueva subred.

Cree una nueva nube privada virtual (VPC) y una subred que se debe asociar a la instancia de CSR1000v.

Es posible utilizar el VPC predeterminado o un VPC y una subred creados anteriormente.

En el panel de la consola, seleccione VPC network > VPC networks como se muestra en la imagen.



Seleccione Create VPC Network como se muestra en la imagen.

Name ↑	Region	Subnets	MTU ⓘ	Mode	IP address ranges	Gateways	Firewall Rules
▼ default		24	1460	Auto ▼			22
	us-central1	default			10.128.0.0/20	10.128.0.1	
	europa-west1	default			10.132.0.0/20	10.132.0.1	
	us-west1	default			10.138.0.0/20	10.138.0.1	
	asia-east1	default			10.140.0.0/20	10.140.0.1	
	us-east1	default			10.142.0.0/20	10.142.0.1	
	asia-northeast1	default			10.146.0.0/20	10.146.0.1	
	asia-southeast1	default			10.148.0.0/20	10.148.0.1	
	us-east4	default			10.150.0.0/20	10.150.0.1	
	australia-southeast1	default			10.152.0.0/20	10.152.0.1	

 Nota: actualmente, CSR1000v solo se implementa en la región central de Estados Unidos en GCP.

Configure el nombre de VPC como se muestra en la imagen.

← Create a VPC network

Name * 
csr-vpc

Lowercase letters, numbers, hyphens allowed

Description

Configure el nombre de subred asociado con el VPC y seleccione la región us-central1.

Asigne un rango de direcciones IP válidas dentro del us-central1 CIDR de 10.128.0.0/20., como se muestra en la imagen.

Deje otros parámetros predeterminados y seleccione el botón Create:

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

- Custom
 Automatic

New subnet

Name *
csr-subnet

Lowercase letters, numbers, hyphens allowed

[Add a description](#)

Region *
us-central1

IP address range *
10.10.1.0/24

 Nota: Si se selecciona "automático", GCP asigna un rango válido automático dentro de la región CIDR.

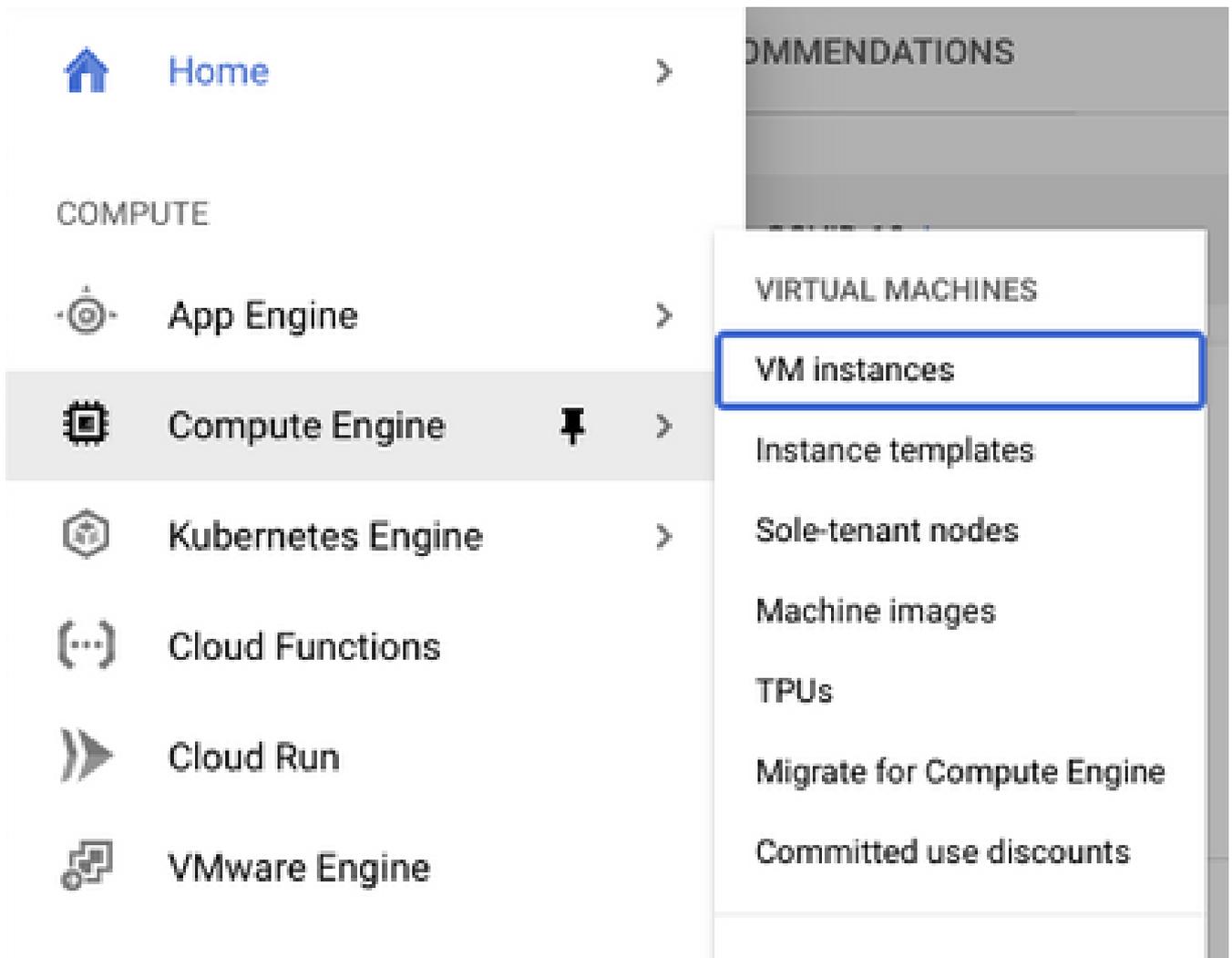
Una vez finalizado el proceso de creación, el nuevo VPC aparece en la sección Redes VPC como se muestra en la imagen.

VPC networks [+ CREATE VPC NETWORK](#) [REFRESH](#)

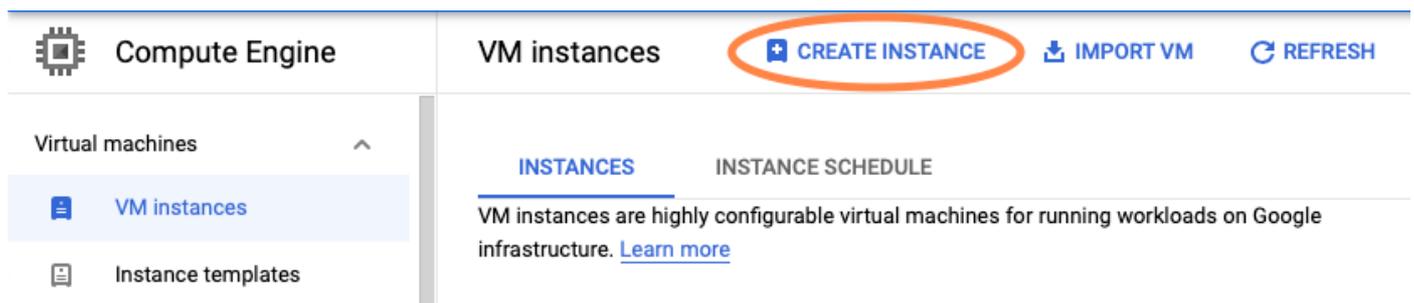
Name ↑	Region	Subnets	MTU ?	Mode	IP address ranges	Gateways
▼ csr-vpc		1	1460	Custom		
	us-central1	csr-subnet			10.10.1.0/24	10.10.1.1

Paso 3. Implementación de instancias virtuales.

En la sección Compute Engine, seleccione Compute Engine > Instancias de VM como se muestra en la imagen.



Una vez en el panel de VM, seleccione la pestaña Create Instance como se muestra en la imagen.



Utilice GCP Marketplace como se muestra en la imagen para mostrar los productos de Cisco.



Create an instance

To create a VM instance, select one of the options:



New VM instance

Create a single VM instance from scratch



New VM instance from template

Create a single VM instance from an existing template



New VM instance from machine image

Create a single VM instance from an existing machine image



Marketplace

Deploy a ready-to-go solution onto a VM instance

En la barra de búsqueda, escriba Cisco CSR o Catalyst C8000v, elija el modelo y la versión que se adapte a sus requisitos y seleccione Iniciar.

Para este ejemplo de implementación, se seleccionó la primera opción, como se muestra en la imagen.

Filter Type to filter

Category

Compute

(4)

Networking

(7)

Type

Virtual machines

3

Virtual machines

7 results

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

Cisco Systems

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

**Cisco Cloud Services Router 1000V - 16.12 - BYOL**

Cisco Systems

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

**Cisco Cloud Services Router 1000V - 17.2.1r - BYOL**

Cisco Systems

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

**Cisco Cloud Services Router 1000V - 17.3 - BYOL**

Cisco Systems

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

Marketplace > "catalyst 8000v edge software - byol" > Virtual machines

Filter Type to filter

Virtual machines

Category



1 result

Compute

(1)

Networking

(1)

Type

Virtual machines



Catalyst 8000V Edge Software - BYOL

Cisco Systems

As part of Cisco's Cloud connect portfolio, the Bring Your Own License (BYOL) version of C 8000V) delivers the maximum performance for virtual enterprise-class networking service the Catalyst 8000V (C8000V) DNA packages and supports the high-performance versions

 Nota: BYOL significa "Traiga su propia licencia".

 Nota: Actualmente, GCP no admite el modelo de pago sobre la marcha (PAYG).

GCP requiere ingresar los valores de configuración que deben asociarse con la VM, como se muestra en la imagen:

Se requiere un nombre de usuario y una clave pública SSH para implementar un CSR1000v/C8000v en GCP, como se muestra en la imagen. Consulte [Generar una Clave SSH de Instancia para Implementar un CSR1000v en la Plataforma de Google Cloud](#) si las claves SSH no se han creado.

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

Deployment name

Instance name

Username

Instance SSH Key

Zone ?

Machine type ?

15 GB memory

[Customize](#)

Boot Disk

Boot disk type ?

Boot disk size in GB ?

Seleccione el VPC y la subred creados anteriormente y elija Ephemeral en la IP externa, para tener una IP pública asociada con la instancia como se muestra en la imagen.

Después de que se configure. Seleccione el botón Iniciar.

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

 Nota: El puerto 22 es necesario para conectarse a la instancia CSR a través de SSH. El puerto HTTP es opcional.

Una vez completada la implementación, seleccione Compute Engine > VM instance para verificar que el nuevo CSR1000v se implementó correctamente, como se muestra en la imagen.

VM instances [CREATE INSTANCE](#) [IMPORT VM](#) [REFRESH](#) [START / RESUME](#) [STOP](#)

Filter VM instances [Columns](#)

<input type="checkbox"/> Name ^	Zone	Recommendation	In use by	Internal IP	External IP	Connect
<input checked="" type="checkbox"/> csr-cisco	us-central1-f			10.10.1.2 (nic0)		SSH  

Verificar implementación

Conexión remota a la nueva instancia

Los métodos más comunes para iniciar sesión en un CSR1000v/C8000V en GCP son la línea de comandos en un terminal Bash, Putty y SecureCRT. En esta sección, la configuración necesaria para conectar con los métodos anteriores.

Inicie sesión en CSR1000v/C8000v con Bash Terminal

La sintaxis necesaria para conectarse de forma remota a la nueva CSR es la siguiente:

```
<#root>
```

```
ssh -i private-key-path username@publicIPAddress
```

Ejemplo:

```
<#root>
```

```
$
```

```
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:c3JsVDEt68CeUFGhp91rYz7tU07htbsPhAwanh3feC4.  
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.
```

Si la conexión se realiza correctamente, se muestra el mensaje CSR1000v

```
<#root>
```

```
$
```

```
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, RELEASED FOR FIELD  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2018 by Cisco Systems, Inc.  
Compiled Tue 17-Jul-18 16:57 by mcpre
```

Inicie sesión en CSR1000v/C8000v con PuTTY

Para conectarse con Putty, utilice la aplicación PuTTYgen para convertir la clave privada del formato PEM al formato PPK.

Consulte [Convertir Pem en archivo Ppk con PuTTYgen](#) para obtener información adicional.

Una vez generada la clave privada en el formato adecuado, debe especificar la ruta en masilla.

Seleccione la sección Archivo de clave privada para la autenticación en la opción de autenticación del menú de conexión SSH.

Vaya a la carpeta en la que está almacenada la clave y seleccione la clave creada. En este ejemplo, las imágenes muestran la vista gráfica del menú Masilla y el estado deseado:



Category:

- ... Keyboard
- ... Bell
- ... Features
- [-] Window
 - ... Appearance
 - ... Behaviour
 - ... Translation
 - [+] Selection
 - ... Colours
- [-] **Connection**
 - ... Data
 - ... Proxy
 - ... Telnet
 - ... Rlogin
 - [-] **SSH**
 - ... Kex
 - ... Host keys
 - ... Cipher
 - [+] **Auth**
 - ... TTY
 - ... X11
 - ... Tunnels

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 username in SSH-2

Private key file for authentication:

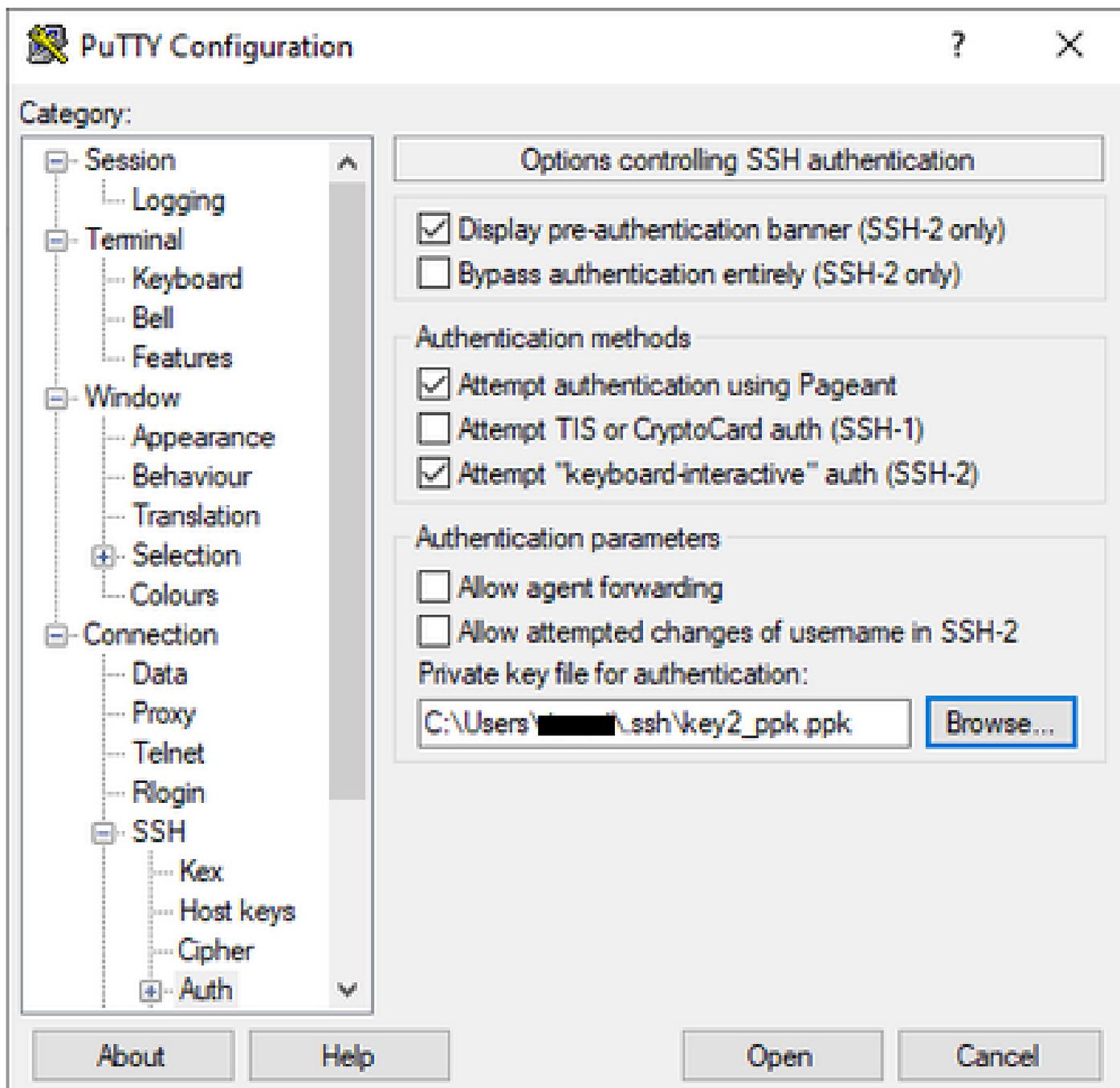
Browse...

About

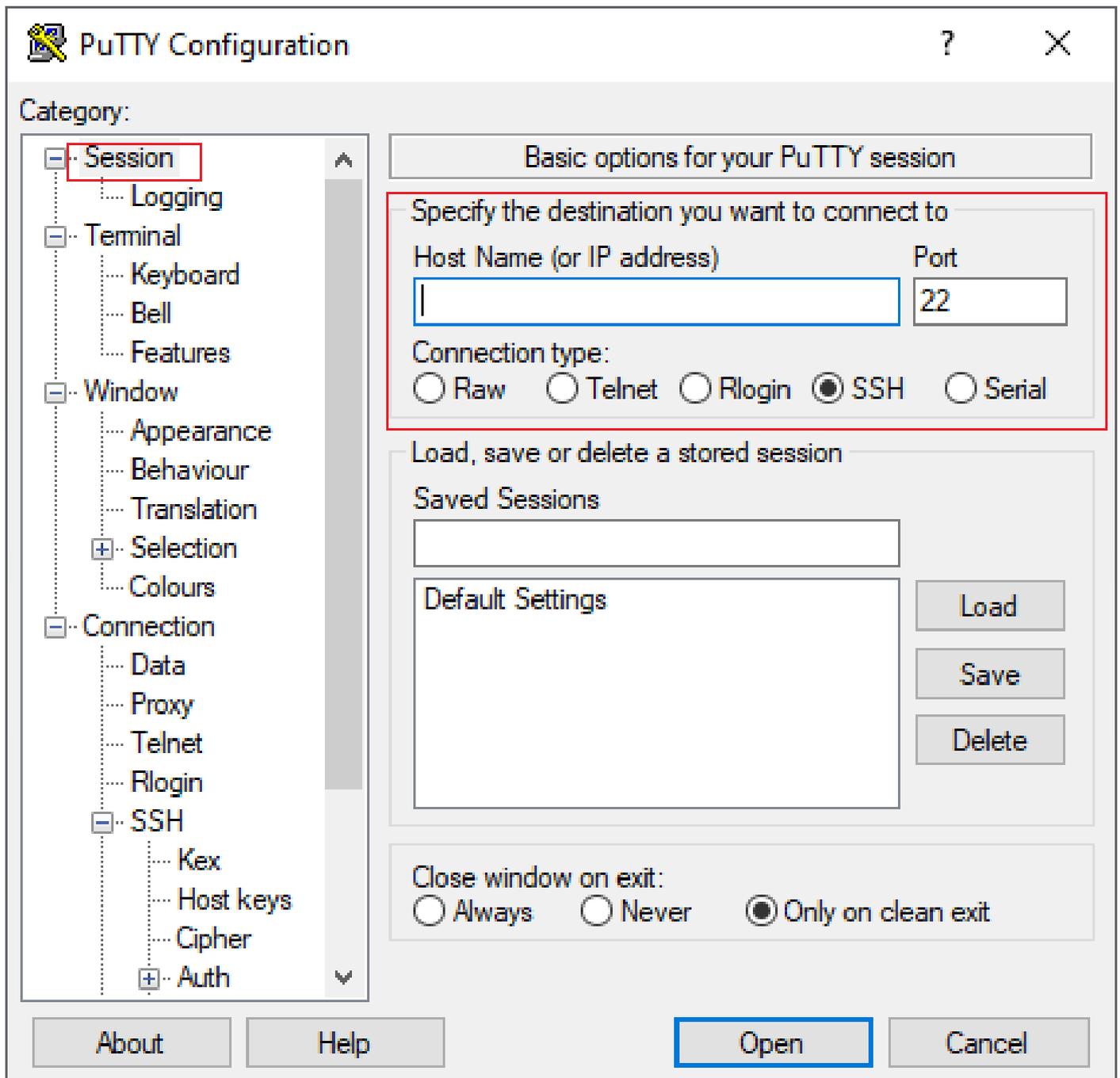
Help

Open

Cancel



Una vez seleccionada la clave adecuada, vuelva al menú principal y utilice la dirección IP externa de la instancia de CSR1000v para conectarse a través de SSH, como se muestra en la imagen.



 Nota: Se solicita el nombre de usuario/contraseña definidos en las claves SSH generadas para iniciar sesión.

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

```
csr-cisco#
```

Inicie sesión en CSR1000v/C8000V con SecureCRT

SecureCRT requiere la clave privada en formato PEM, que es el formato predeterminado para las claves privadas.

En SecureCRT, especifique la ruta de acceso a la clave privada en el menú:

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

La imagen muestra la ventana esperada:

Quick Connect

Protocol: SSH2

Hostname:

Port: 22 Firewall: None

Username:

Authentication

- Password
- PublicKey
- Keyboard Interactive
- GSSAPI

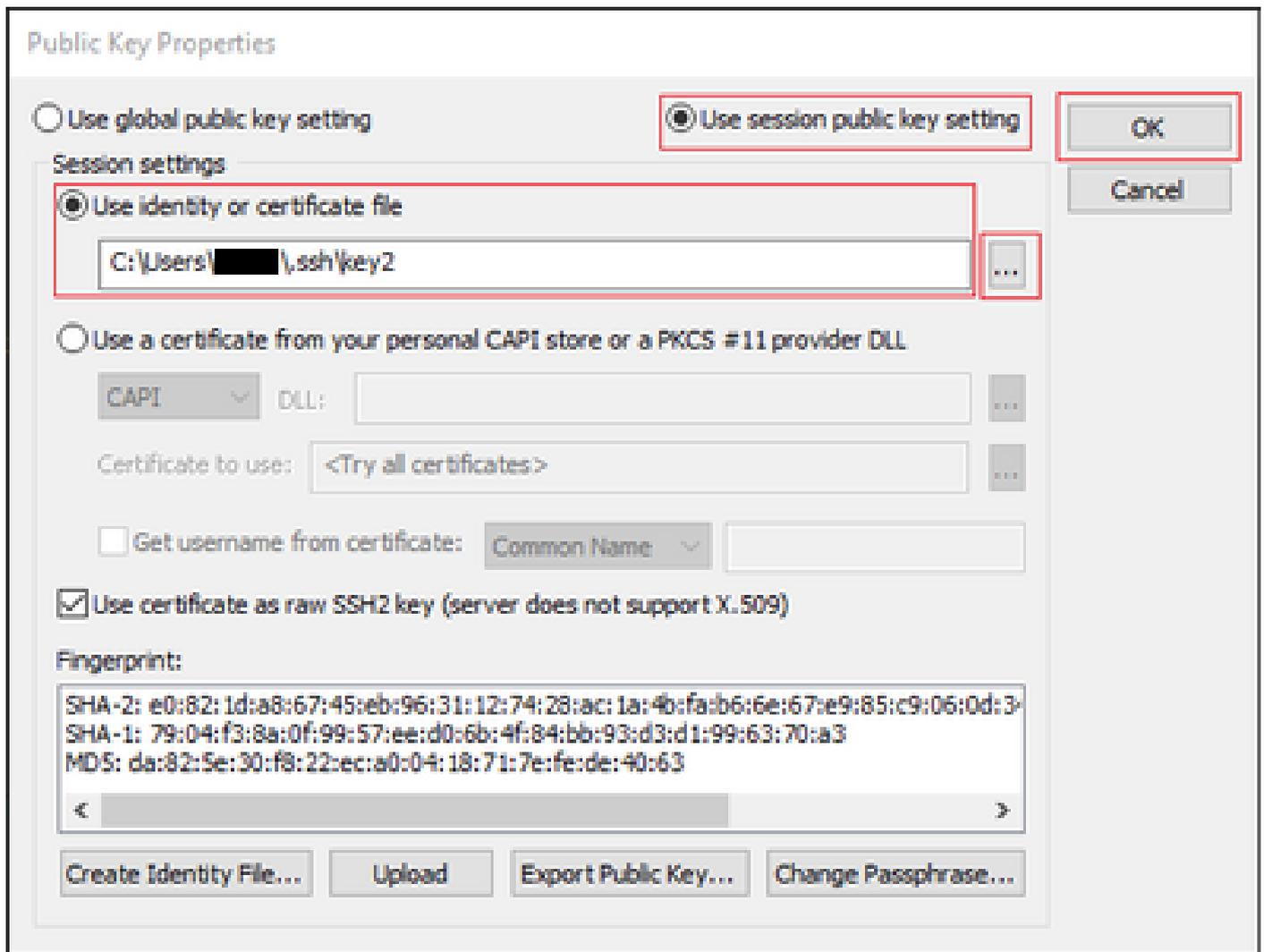
Properties...

Show quick connect on startup Save session

Open in a tab

Connect Cancel

Seleccione Use session public key string > Select Use identity or certificate file > Select ... button > Navegue hasta el directorio y seleccione la clave deseada > Select OK como se muestra en la imagen.



Finalmente, conéctese a la IP externa de la dirección de instancia a través de SSH como se muestra en la imagen.

Quick Connect

Protocol: SSH2

Hostname: |

Port: 22 Firewall: None

Username:

Authentication

- PublicKey
- Keyboard Interactive
- GSSAPI
- Password

Show quick connect on startup Save session Open in a tab

Connect Cancel

 Nota: Se solicita el nombre de usuario/contraseña definidos en las claves SSH generadas para iniciar sesión.

```
<#root>
```

```
csr-cisco#
```

```
show logging
```

```
Syslog logging: enabled (0 messages dropped, 3 messages rate-limited, 0 flushes, 0 overruns, xml 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] [local]
```

csr-cisco#

Métodos de inicio de sesión de VM adicionales



Nota: Consulte la documentación de [Conexión a las VM de Linux mediante métodos avanzados](#).

Autorizar a usuarios adicionales a iniciar sesión en CSR1000v/C8000v en GCP

Una vez que haya iniciado sesión en la instancia de CSR1000v correctamente, es posible configurar usuarios adicionales con estos métodos:

Configurar un nuevo nombre de usuario/contraseña

Utilice estos comandos para configurar un nuevo usuario y contraseña:

```
<#root>
```

```
enable
```

```
configure terminal
```

```
username <username> privilege <privilege level> secret <password>
```

```
end
```

Ejemplo:

```
<#root>
```

```
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#
```

Ahora, un nuevo usuario puede iniciar sesión en la instancia de CSR1000v/C8000v.

Configuración de un nuevo usuario con clave SSH

Para obtener acceso a la instancia de CSR1000v, configure la clave pública. Las claves SSH de los metadatos de instancia no proporcionan acceso a CSR1000v.

Utilice estos comandos para configurar un nuevo usuario con una clave SSH:

```
<#root>
configure terminal

ip ssh pubkey-chain

username <username>

key-string

<public ssh key>

exit

end
```

 Nota: La longitud máxima de la línea en la CLI de Cisco es de 254 caracteres, por lo que la cadena de clave no puede ajustarse a esta limitación; es conveniente ajustar la cadena de clave para que se ajuste a una línea de terminal. Los detalles sobre cómo superar esta limitación se explican en [Generar una Clave SSH de Instancia para Implementar un CSR1000v en la Plataforma de Google Cloud](#)

```
<#root>
$
fold -b -w 72 /mnt/c/Users/ricneri/.ssh/key2.pub
```

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQD1dzZ/iJi3VeHs4qDoxOP67jebaGwC6vkC
n29bwSQ4CPJGVRLcVSNPcPPqVydiXVEOG8e9gFszkpk6c2meO+TRsSLiwHigv281yw5xhn1U
ck/AYpy9E6TyEEu9w6Fz0xTG2Qhe1n9b5Les6K9PFP/mR6WUMbfmaFredV/sADnODPO+OfTK
/OZPg34DNfcFhg1ja5GzudRb3S4nBBhDzuVrVC9RbA4PHVMXrLbIfq1ks3PCVG0tW1HxxTU4
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 AAAAB3NzaC1yc2EAAAADAQABAAQD1dzZ/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)#
```

```
ADnODPO+OfTK/OZPg34DNfcFhg1ja5GzudRb3S4nBBhDzuVrVC9RbA4PHVMXrLbIfqlk
```

```
csr-cisco(conf-ssh-pubkey-data)#
```

```
s3PCVG0tW1HxxTU4FCkmEAg4NEqMVLsm26nLvrNK6z71RMcIKZZcST+SL61Qv33gkUKI
```

```
csr-cisco(conf-ssh-pubkey-data)#
```

```
oGB9qx/+D1RvurVXFcdq3Cmxm2swHmb6MlrEtqIv cisco
```

```
csr-cisco(conf-ssh-pubkey-data)#
```

```
exit
```

```
csr-cisco(conf-ssh-pubkey-user)#
```

end

csr-cisco#

Verificar usuarios configurados al iniciar sesión en CSR1000v/C8000v

Para confirmar que la configuración se estableció correctamente, inicie sesión con las credenciales creadas o con el par de claves privadas para la clave pública con las credenciales adicionales.

Desde el lado del router, vea el registro de inicio de sesión correcto con la dirección IP del terminal.

<#root>

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)

<snip>

*Jan 8 00:22:24.907: %SEC_log in-5-log in_SUCCESS: log in Success [user: <snip>] [Source: <snip>] [local]

csr-cisco#

Troubleshoot

Si se muestra el mensaje de error "Operation Timed Out".

<#root>

\$

ssh -i CSR-sshkey <snip>@X.X.X.X

ssh: connect to host <snip> port 22: Operation timed out

Posibles Causas:

- La instancia no ha finalizado su implementación.
- La dirección pública no es la asignada a nic0 en la máquina virtual.

Solución:

Espere a que se complete la implementación de VM. Normalmente, una implementación de CSR1000v tarda hasta 5 minutos en completarse.

Si se requiere una contraseña

Si se requiere una contraseña:

```
<#root>
```

```
$
```

```
ssh -i CSR-sshkey <snip>@X.X.X.X
```

```
Password:
```

```
Password:
```

Posible causa:

- El nombre de usuario o la clave privada no son correctos.
- En las versiones más recientes de los sistemas operativos como MacOS o Linux, la utilidad OpenSSH no tiene RSA habilitado de forma predeterminada.

Solución:

- Asegúrese de que el nombre de usuario es el mismo que se especificó al implementar CSR1000v/C8000v.
- Asegúrese de que la clave privada es la misma que la incluida en el momento de la implementación.
- Especifique el tipo de clave aceptada en el comando ssh:

```
<#root>
```

```
ssh -o PubkeyAcceptedKeyTypes=ssh-rsa -i <private_key> <user>@<host_ip>
```

Información Relacionada

- [Hoja de datos del router de servicios en la nube 1000v de Cisco](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).