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

Contenido

Introducción

Este documento describe el procedimiento para implementar y configurar un router Cisco Cloud Services Router 1000v (CSR1000v) y un router de borde Catalyst 8000v (C800v) en la plataforma de nube de Google (GCP).

Colaborado por Eric Garcia, Ricardo Neri, Ingenieros del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Tecnologías de virtualización/máquinas virtuales (VM)
- Plataformas de nube

Componentes Utilizados

- Una suscripción activa a Google Cloud Platform con un proyecto creado
- consola GCP
- Mercado GCP
- Terminal Bash, Putty o SecureCRT
- Claves de Secure Shell públicas y privadas (SSH)

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. 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 añaden nuevas funciones, como SDWAN y licencias de ADN. Para obtener más información, verifique la ficha técnica oficial de 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:** Al momento de escribir este documento, los nuevos usuarios tienen 300 USD de créditos gratuitos para explorar por completo GCP como nivel libre 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 más información, 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 se debe asociar a un grupo con permisos para el motor de cálculo.

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

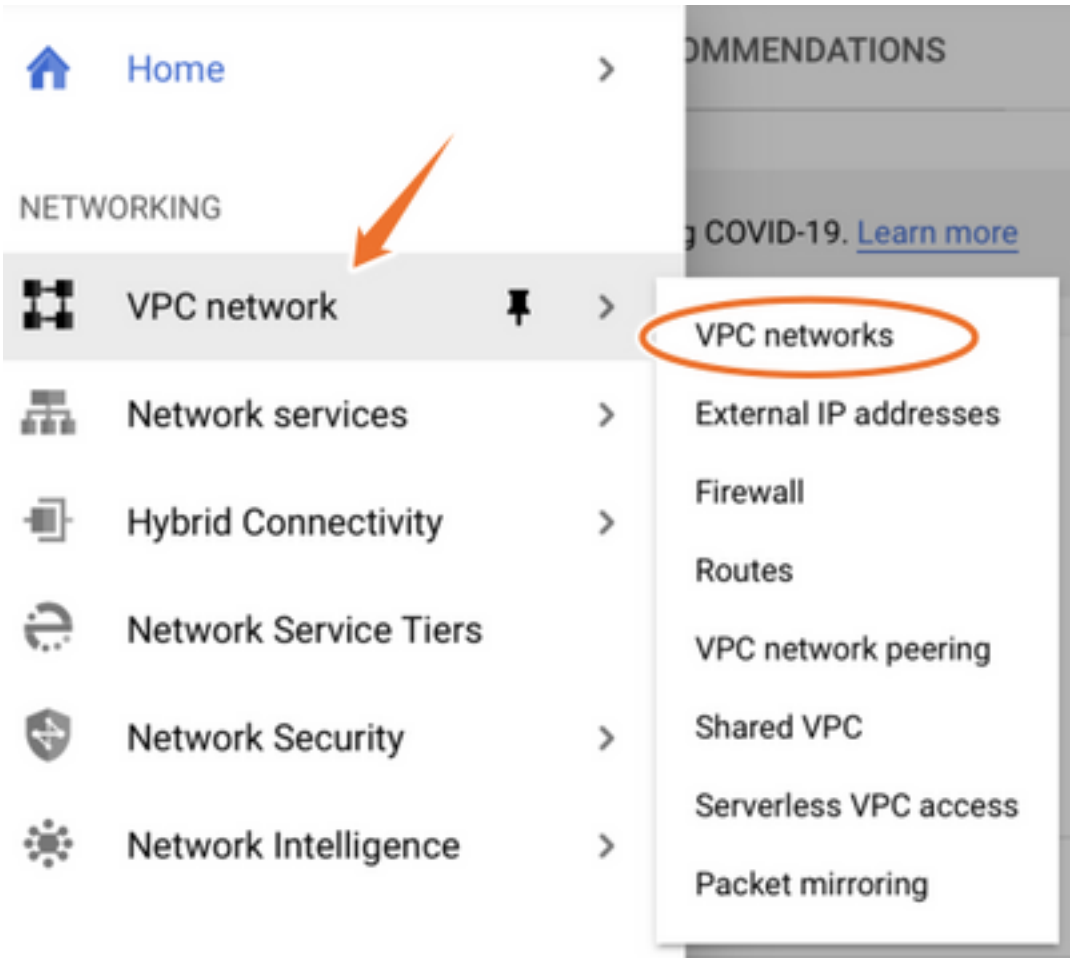
> **Nota:** Para crear un nuevo proyecto, consulte Crear y administrar proyectos.

Paso 2. Cree un nuevo VPC y una subred.

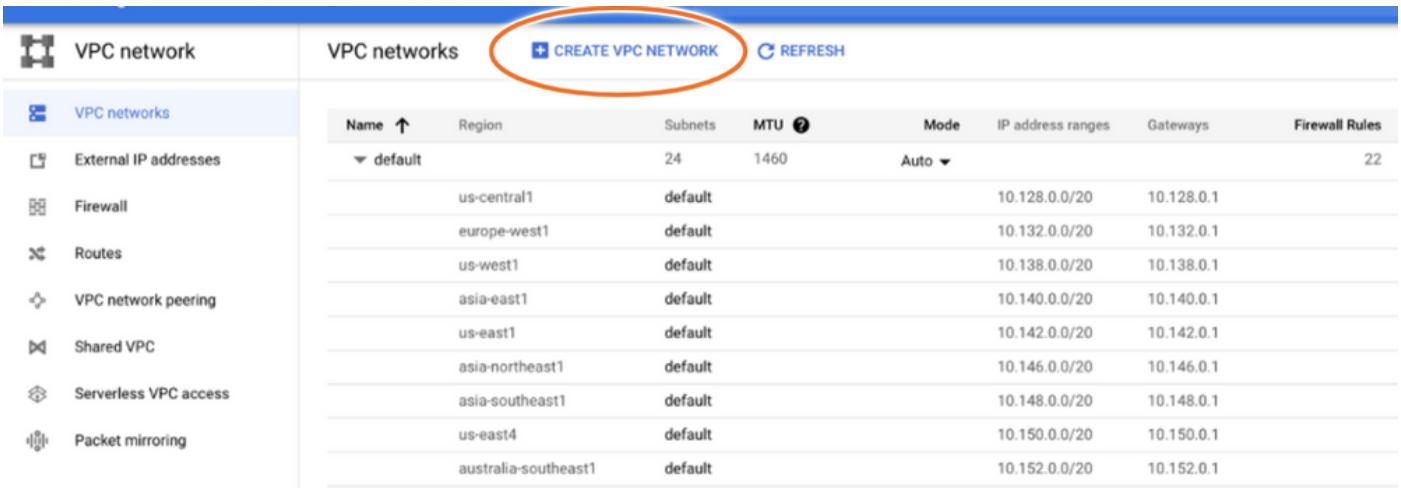
Cree una nueva nube privada virtual (VPC) y una subred que se debe asociar a la instancia de CSR1000v.

Es posible utilizar la VPC predeterminada o una VPC y subred creadas previamente.

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

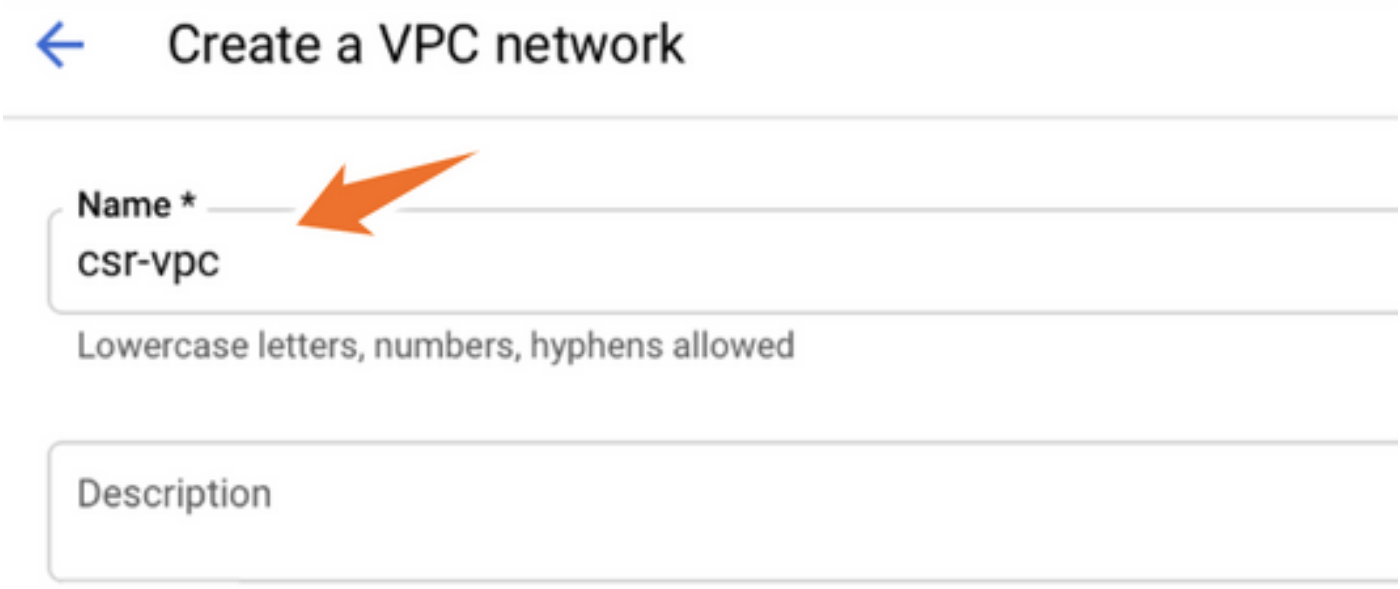


Seleccione **Crear red VPC** como se muestra en la imagen.



Nota: Actualmente, CSR1000v solo se implementa en la región centro-estadounidense en GCP.

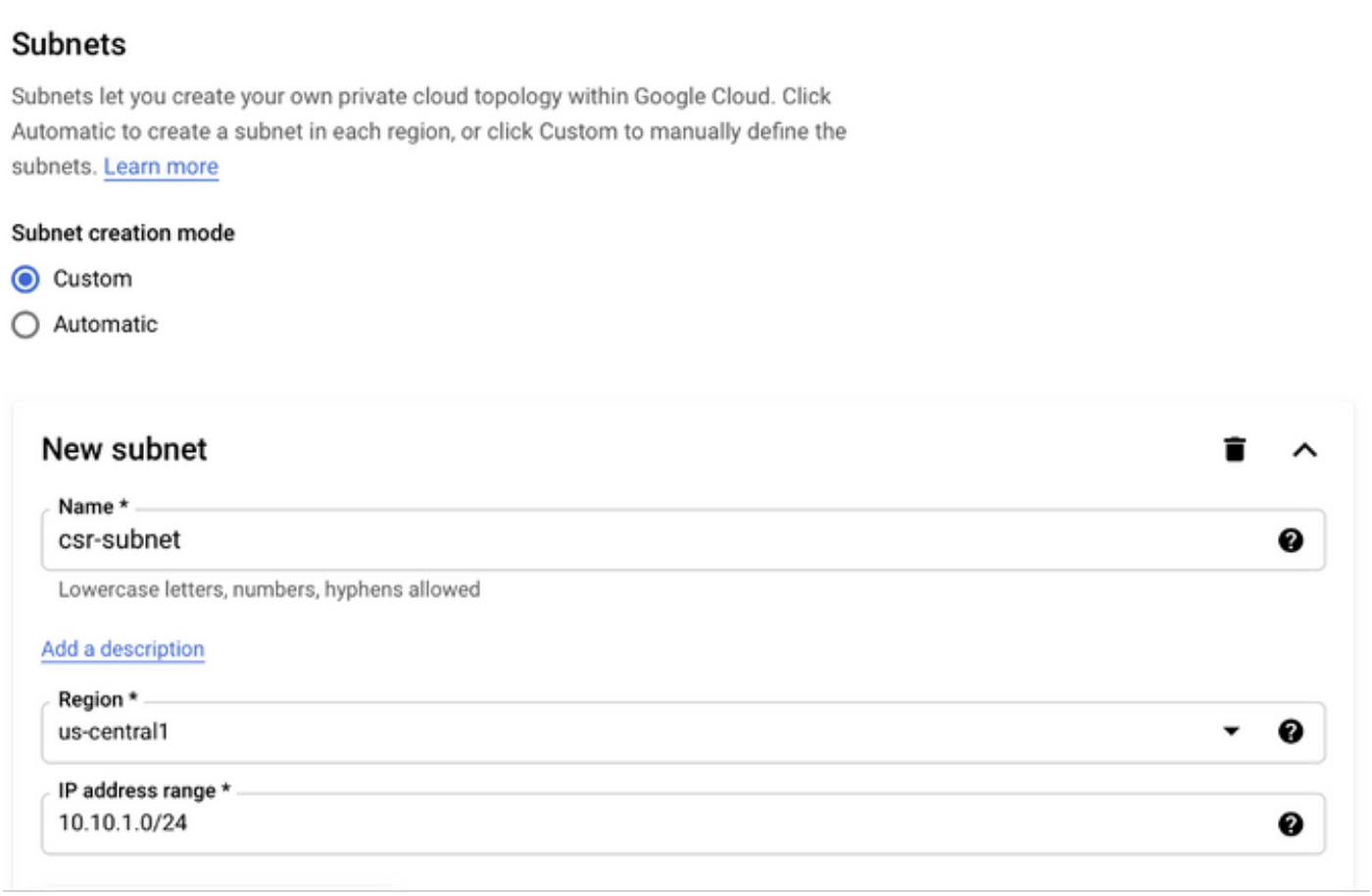
Configure el nombre VPC como se muestra en la imagen.



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

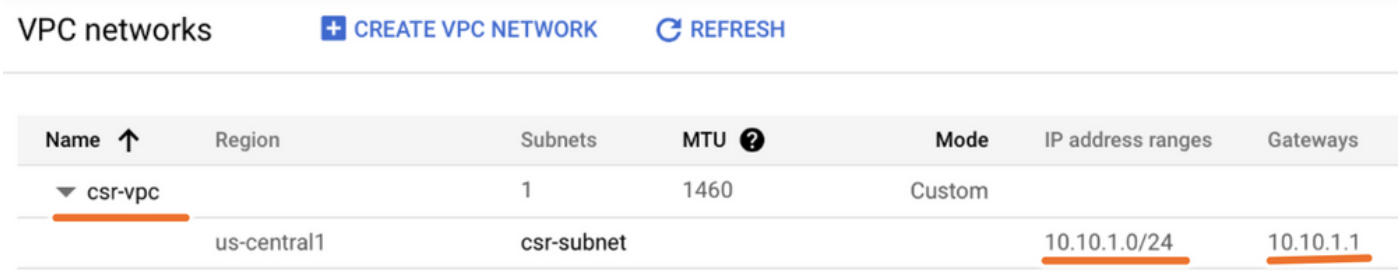
Asigne un rango de direcciones IP válido dentro del CIDR us-central1 de 10.128.0.0/20. como se muestra en la imagen.

Deje otras configuraciones como predeterminadas y seleccione el botón **crear**:



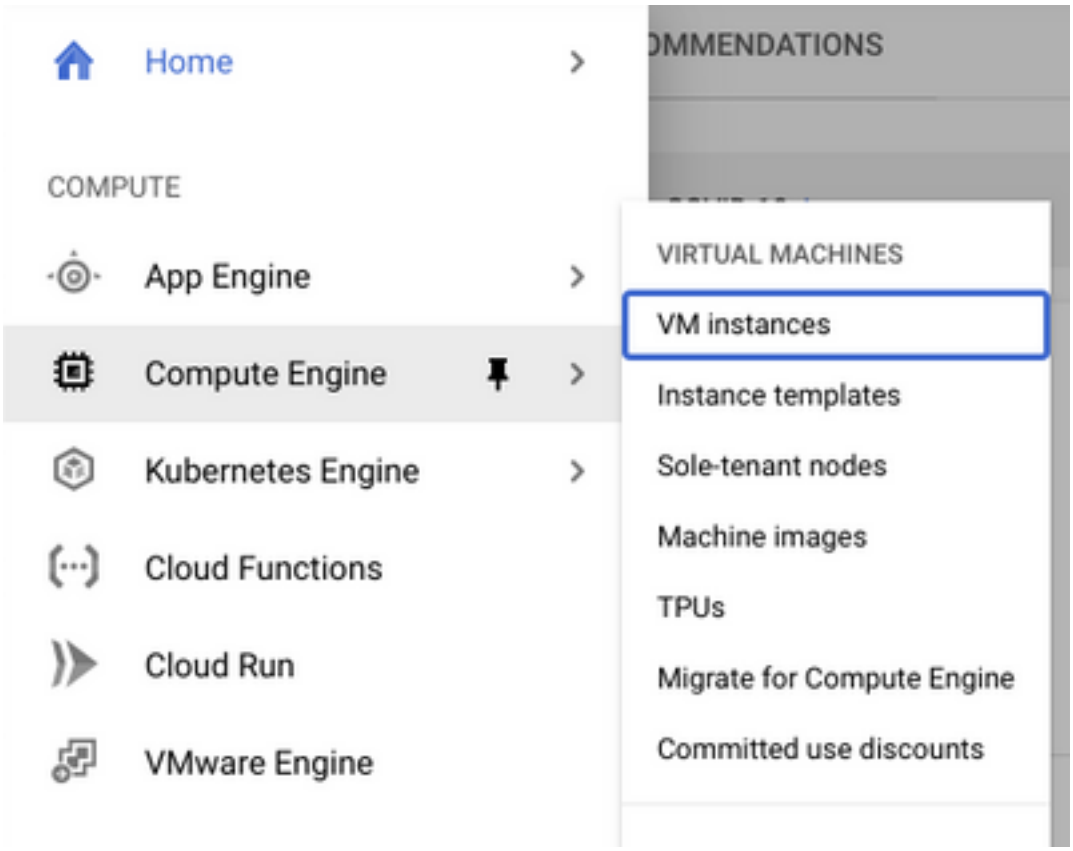
Nota: Si se selecciona "automático", GCP asigna un rango válido automático dentro de la región CIDR.

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

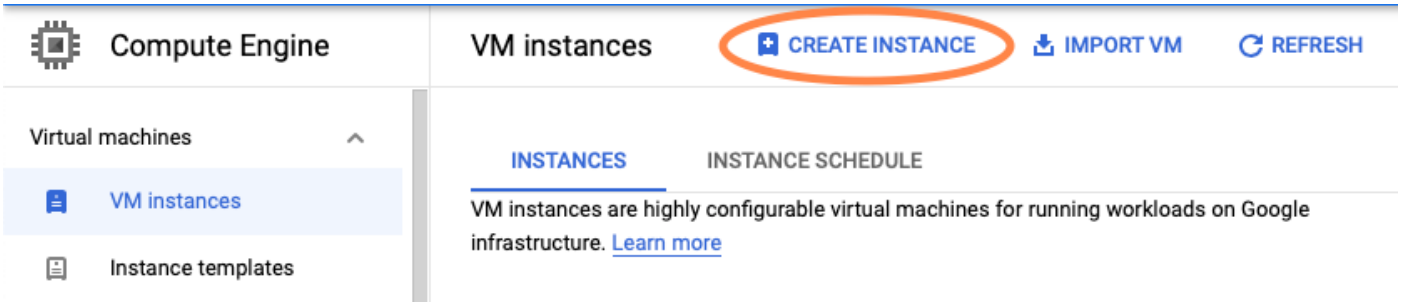


Paso 3. Implementación de instancias virtuales.

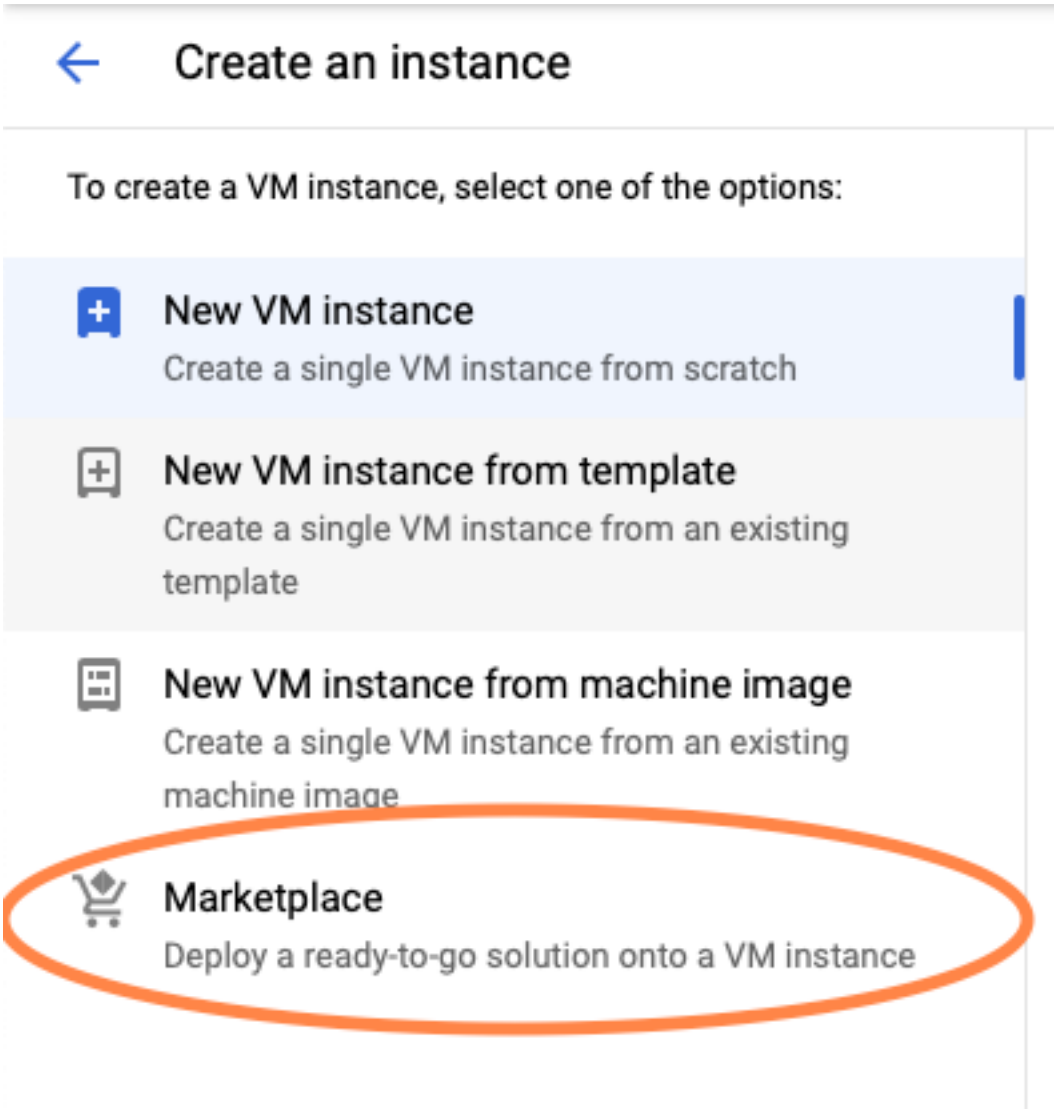
En la sección **Motor de cómputo**, seleccione **Motor de cómputo > Instancias VM** como se muestra en la imagen.



Una vez en el **panel de VM**, seleccione la pestaña **Crear instancia** como se muestra en la imagen.



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



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

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

Marketplace

csr 1000v

Marketplace > "csr 1000v" > Virtual machines

Filter Type to filter

Category

Compute (4)

Networking (7)

Type

Virtual machines

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 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 - 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

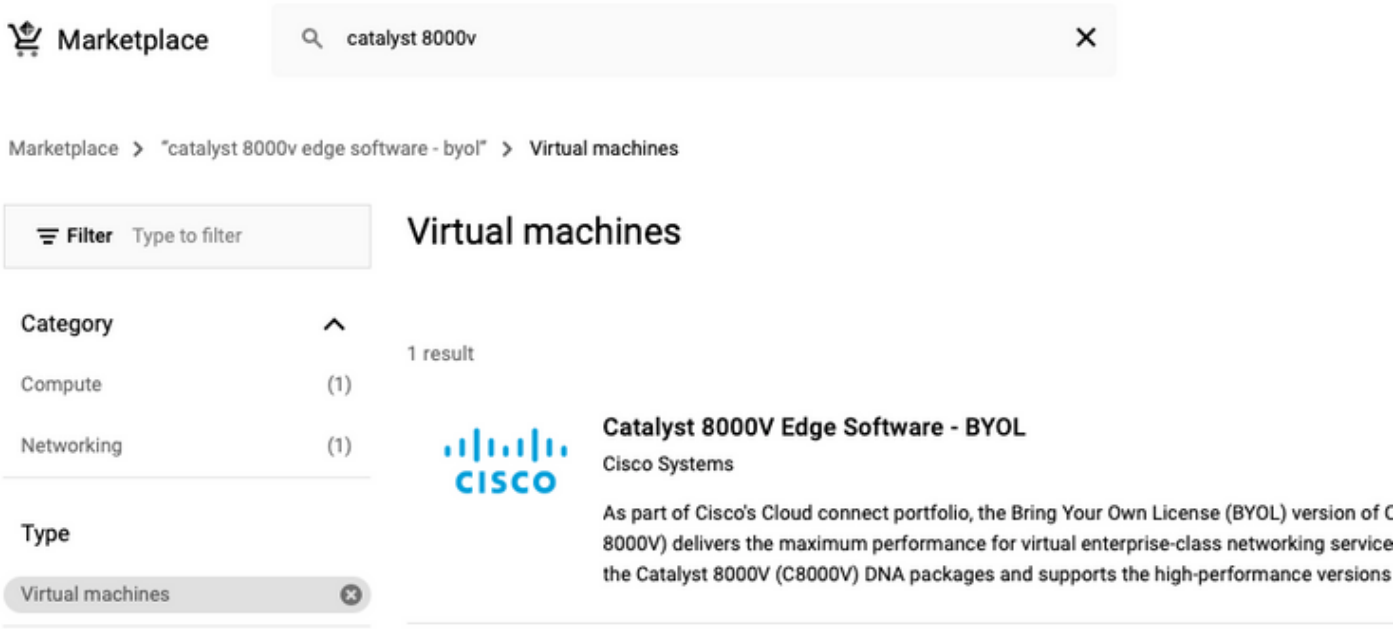
Cisco Systems

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. Th
enables enterprise IT to deploy the same enterprise-class networking services in the cloud th

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. Th
enables enterprise IT to deploy the same enterprise-class networking services in the cloud th

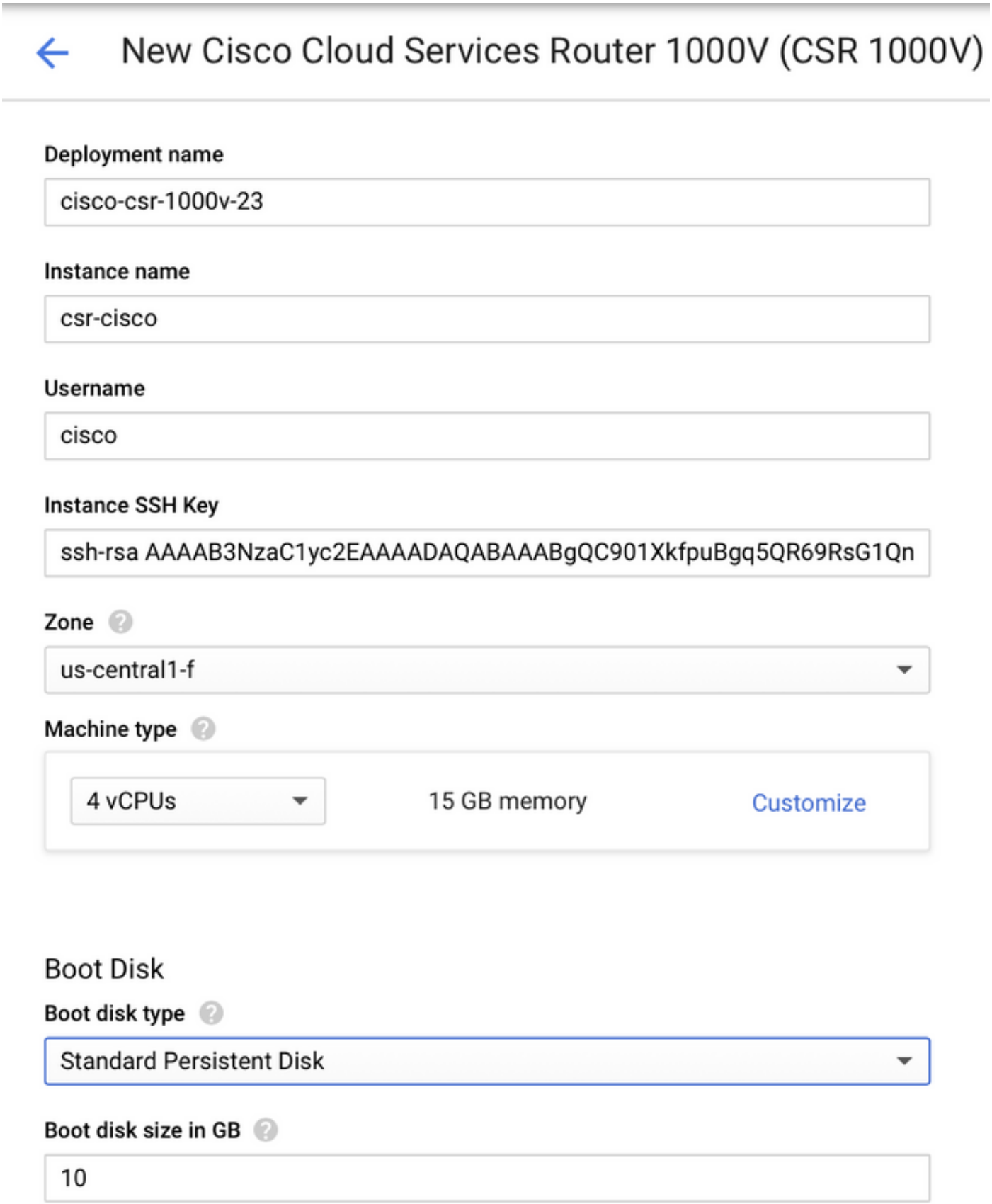


Nota: BYOL significa "Bring Your Own License".

Nota: Actualmente, GCP no admite el modelo de pago por uso (PAYG).

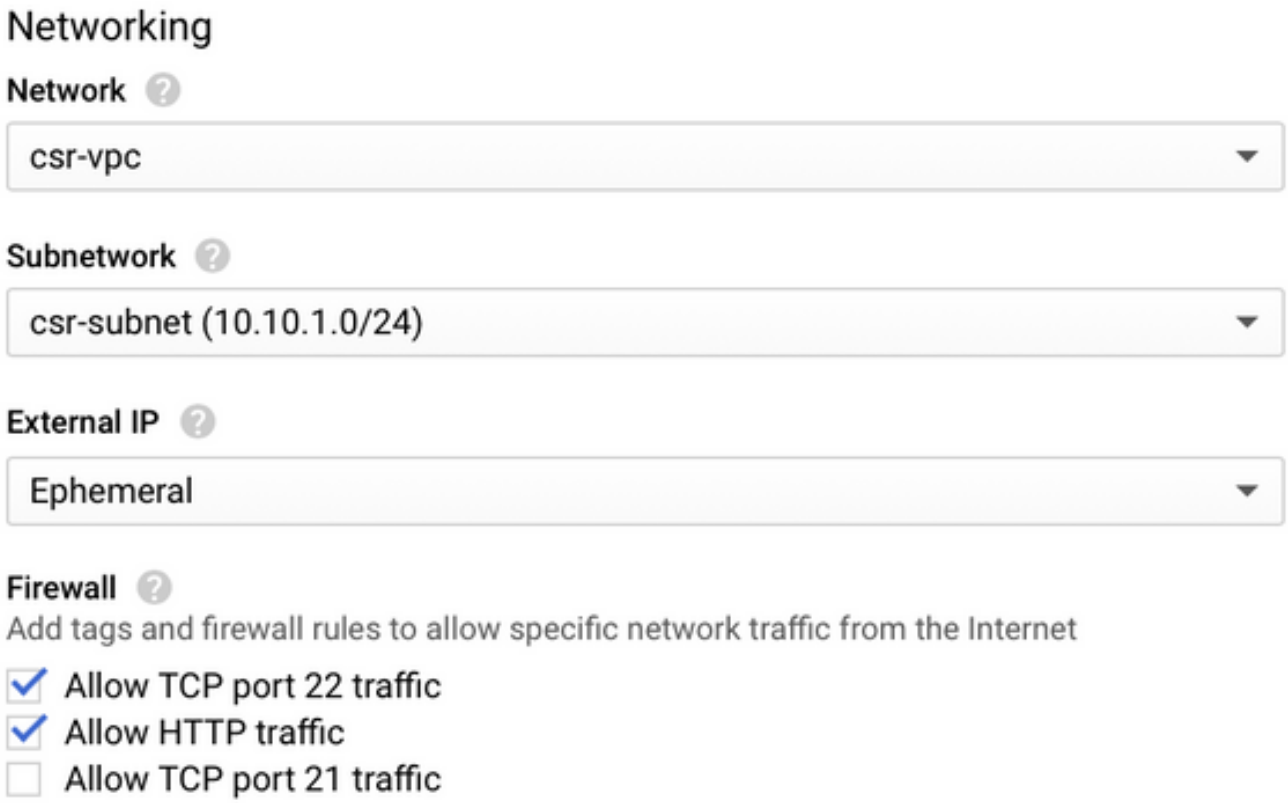
GCP necesita ingresar los valores de configuración que deben asociarse con la VM, como se muestra en la imagen:

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 una CSR1000v en la plataforma de nube de Google si no se han creado las claves SSH.



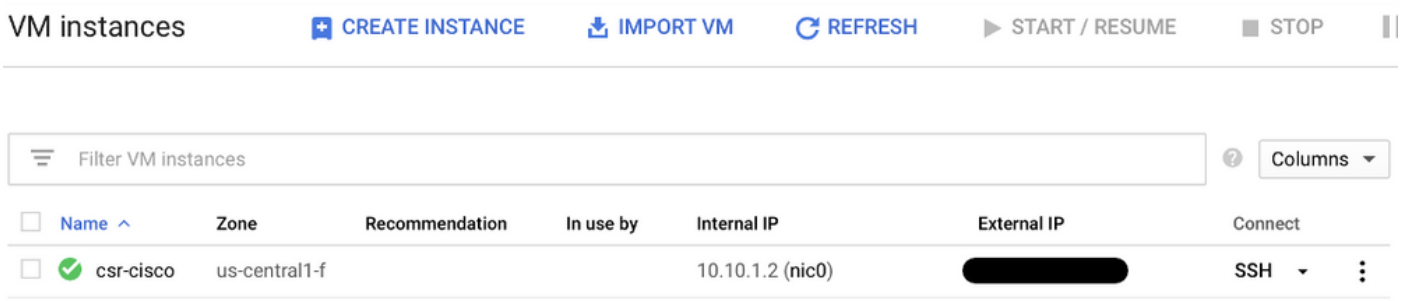
Seleccione el VPC y la subred creados anteriormente y elija Ephemeral en IP externa para tener una IP pública asociada a la instancia como se muestra en la imagen.

Después de que se configure. Seleccione el botón **de inicio**.



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.



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 conectarse con los métodos anteriores.

Inicie sesión en CSR1000v/C8000v con el terminal Bash

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

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

Ejemplo:

```
$ 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.
```

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

```
$ 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
```

Inicie sesión en CSR1000v/C8000v con PuTTY

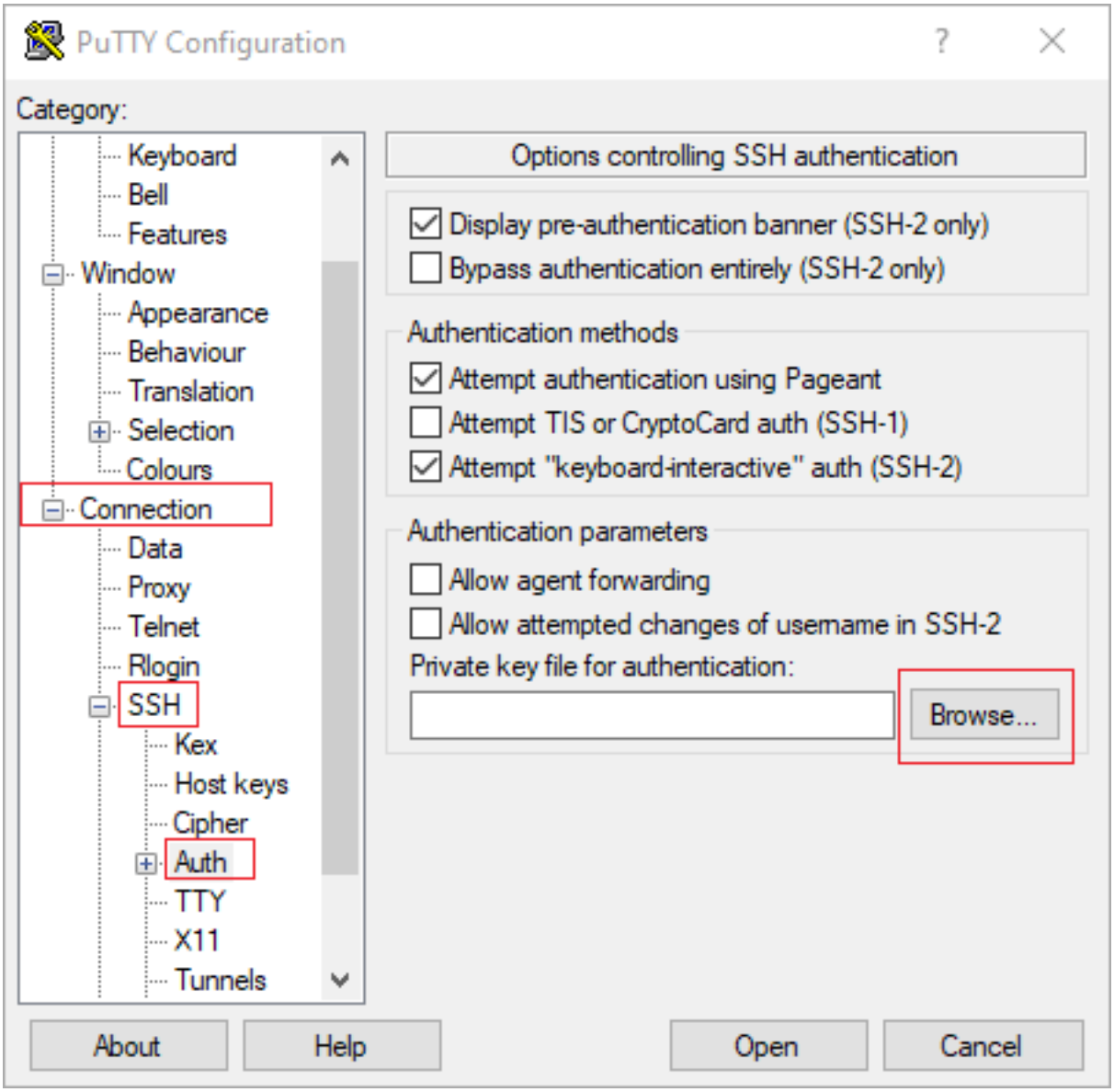
Para conectarse con Putty, utilice la aplicación PuTTYgen para convertir la clave privada del formato PEM al formato PPK.

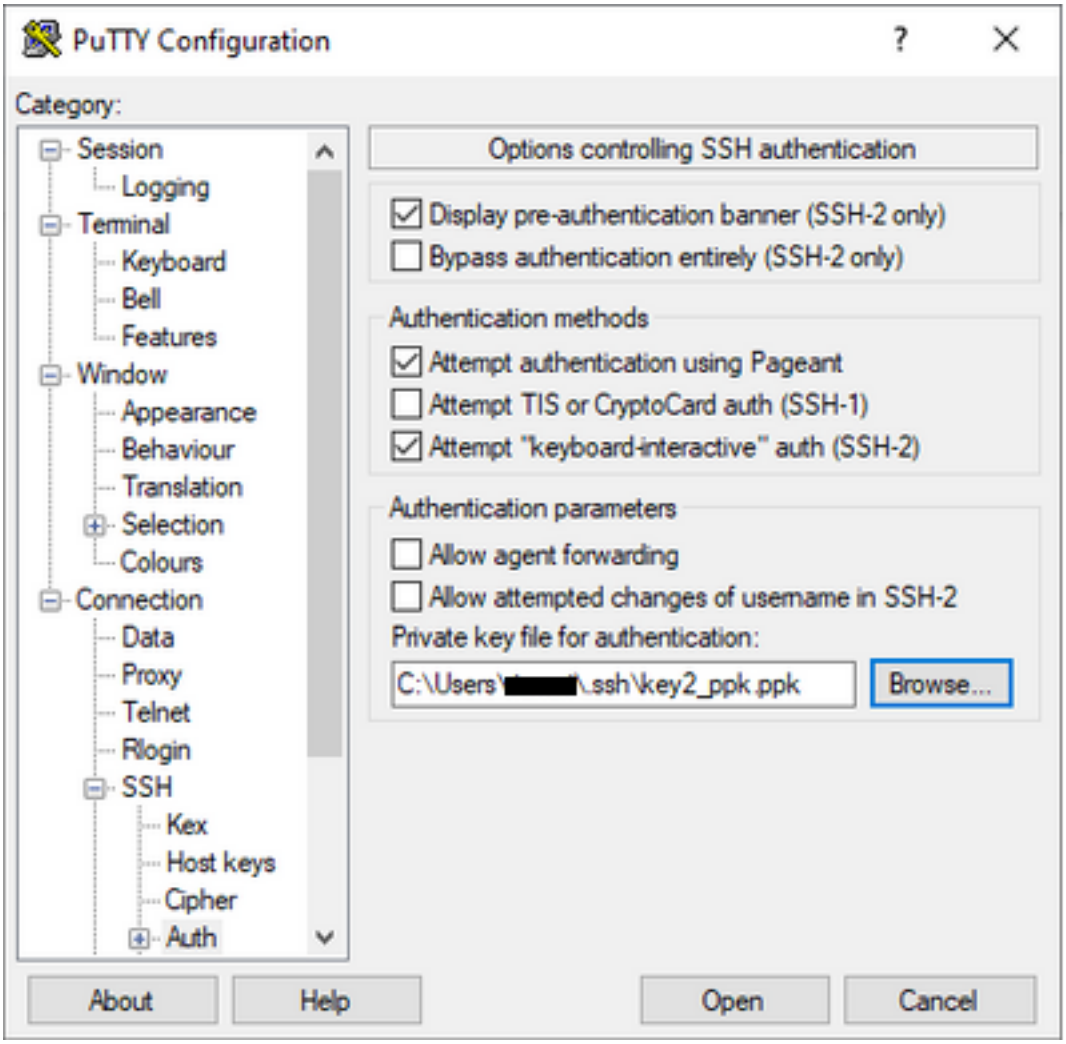
Consulte Convertir Pem en archivo Ppk mediante PuTTYgen para obtener información adicional.

Una vez que la clave privada se genera en el formato adecuado, debe especificar la ruta en Putty.

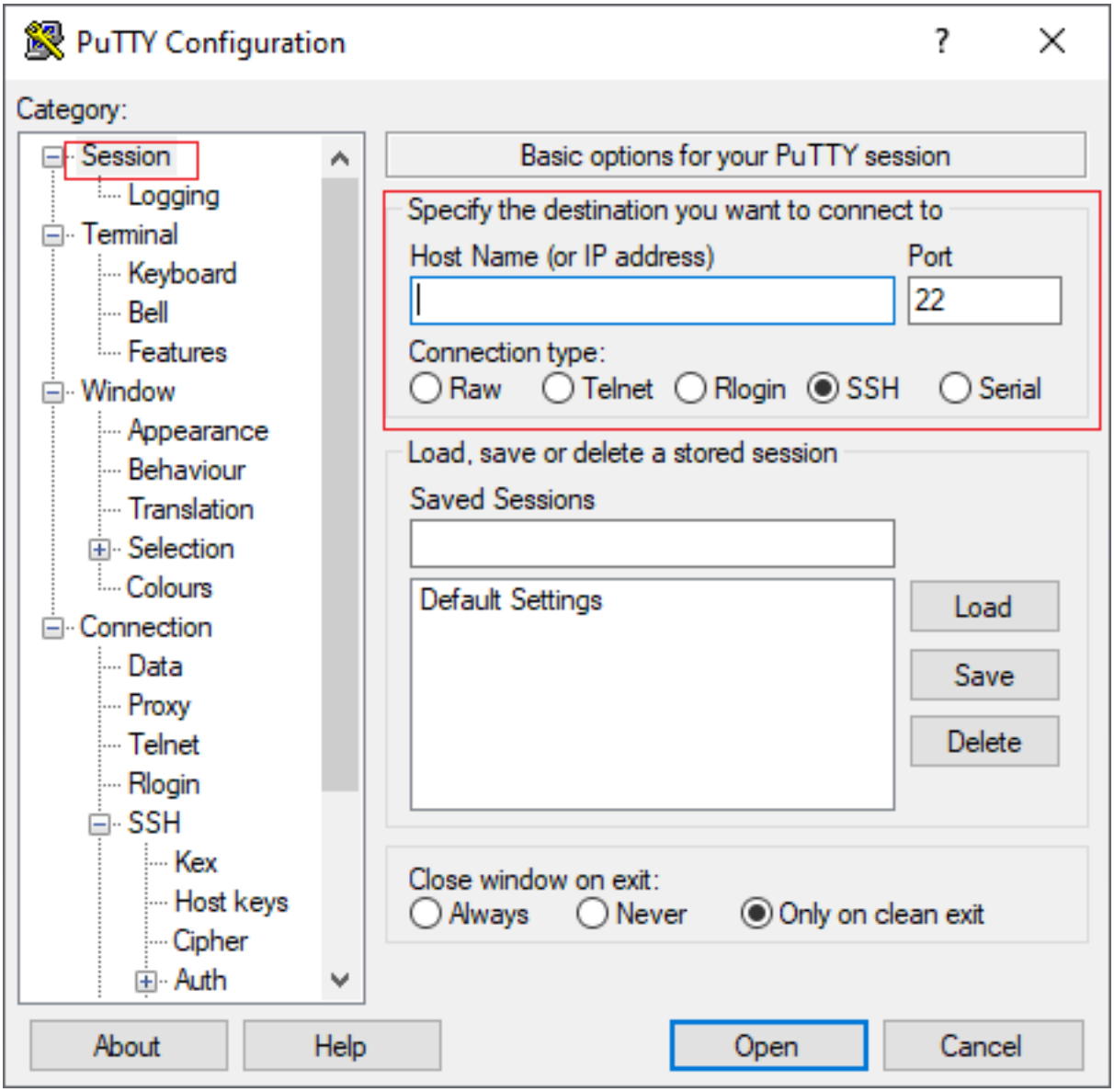
Seleccione la sección **Archivo de clave privada para la autenticación** en la opción de autenticación del **menú** de **conexión** SSH.

Vaya a la carpeta donde se almacena la clave y seleccione la clave creada. En este ejemplo, las imágenes muestran la vista gráfica del menú Putty y el estado deseado:


PuTTY Configuration
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 CSR1000v para conectarse a través de SSH, como se muestra en la imagen.



Nota: Se solicita el nombre de usuario/contraseña definido 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#
```

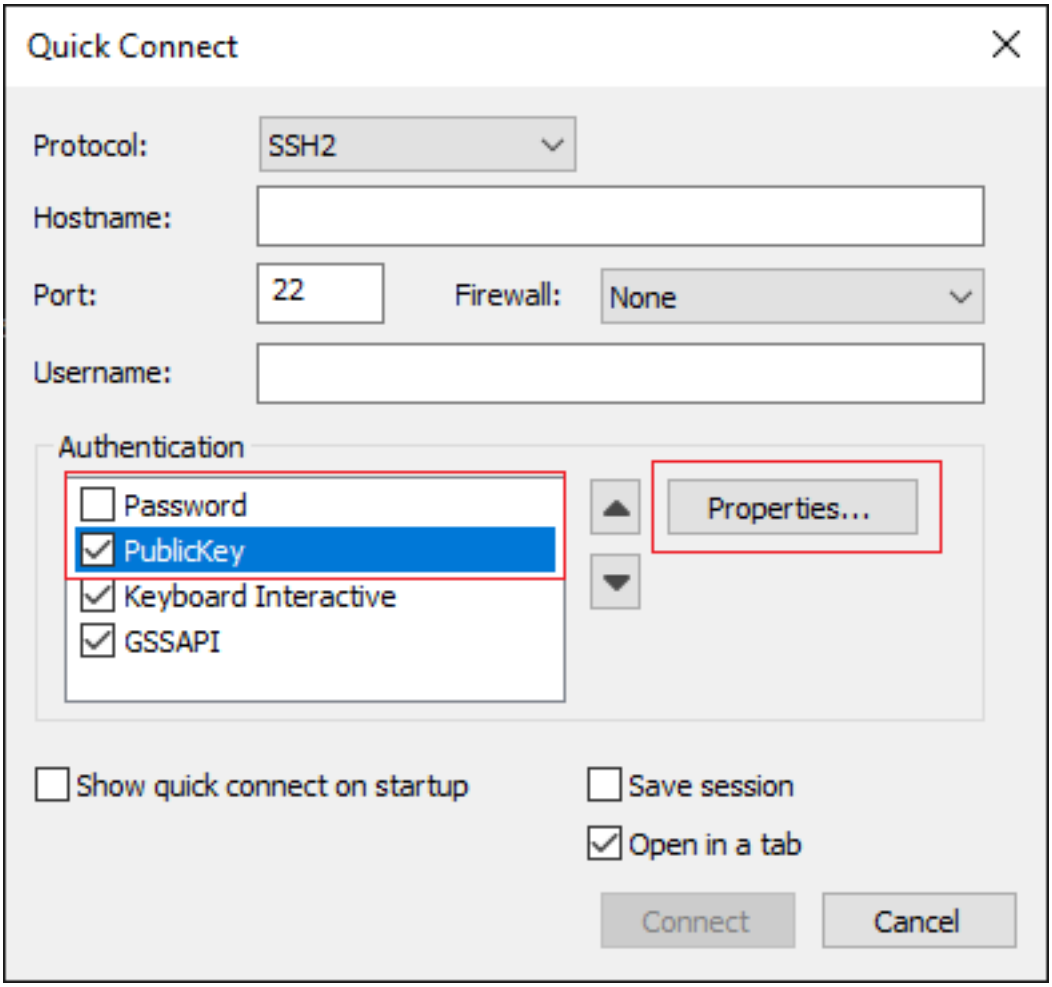
Inicie sesión en CSR1000v/C8000V con SecureCRT

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

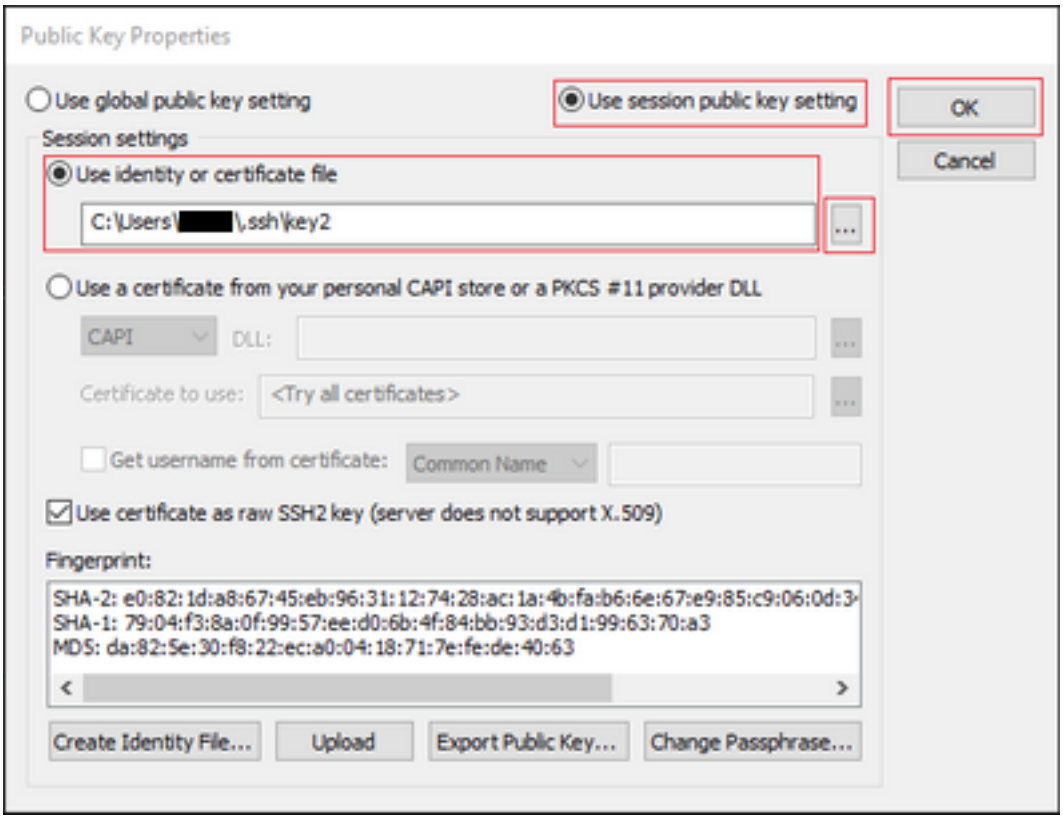
En SecureCRT, especifique la ruta de acceso a la clave privada en el menú:

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

La imagen muestra la ventana esperada:

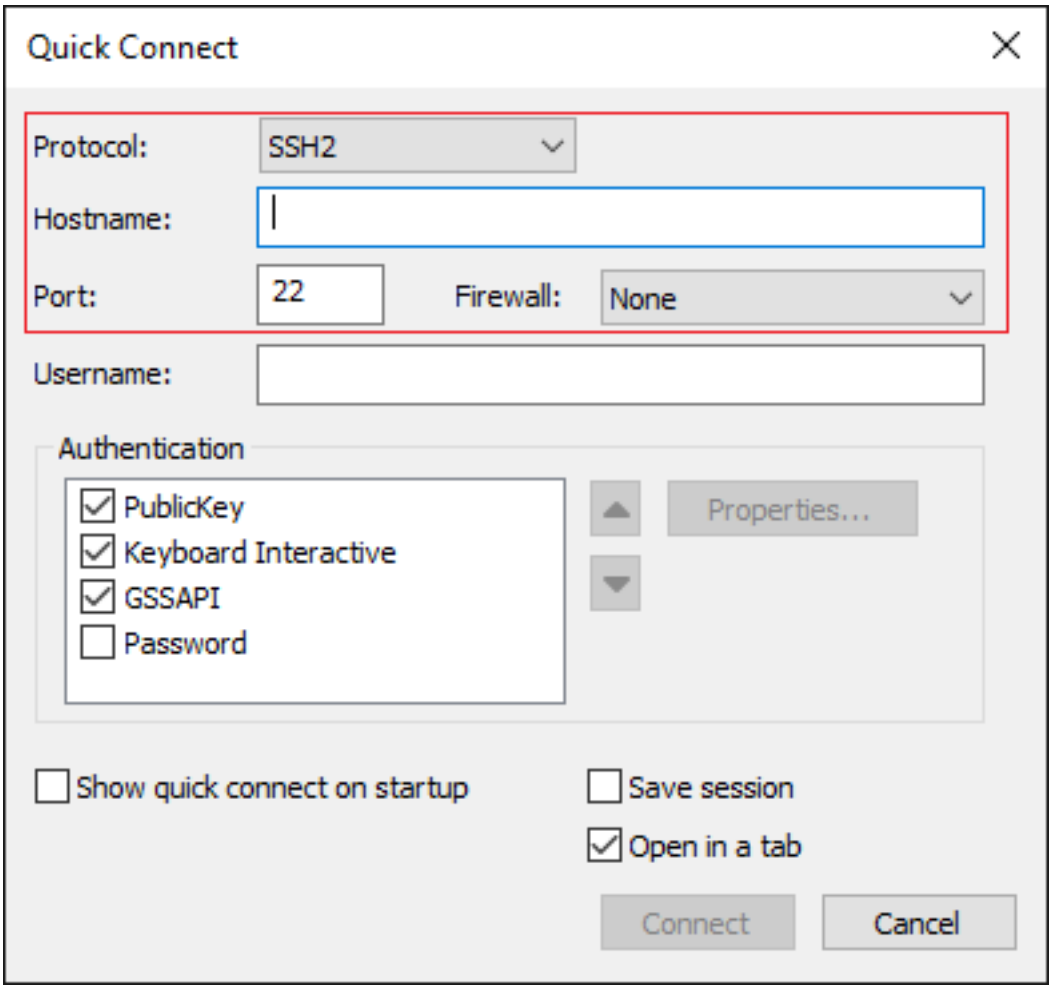


Seleccione **Usar cadena de clave pública de sesión** > Seleccionar **Usar archivo de identidad o certificado** > Seleccionar **...** Botón > Vaya al directorio y seleccione la tecla deseada > Seleccione **Aceptar** como se muestra en la imagen.



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

en la imagen.



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

```
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#
```

Métodos de inicio de sesión de VM adicionales

Nota: Por favor consulte la documentación Connect to Linux VMs usando métodos avanzados.

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

Una vez que se ha 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:

```
enable
configure terminal
username <username> privilege <privilege level> secret <password>
end
```

Ejemplo:

```
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 CSR1000v/C8000v.

Configurar un usuario nuevo con clave SSH

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

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

```
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 es posible que la cadena de clave no encaje en 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 nube de Google

```
$ fold -b -w 72 /mnt/c/Users/ricneri/.ssh/key2.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDldzZ/iJi3VeHs4qDoxOP67jebaGwC6vkC
n29bwSQ4CPJGVRLcVSNPcPPqVydiXVEOG8e9gFszkpk6c2meO+TRsSLiwHigv28lyw5xhn1U
ck/AYpy9E6TyEEu9w6Fz0xTG2Qhe1n9b5Les6K9PFP/mR6WUMbfmaFredV/sADnODPO+OfTK
/OZPg34DNfcFhglja5GzudRb3S4nBBhDzuVrVC9RbA4PHVMXrLbIfqlks3PCVGOtW1HxxTU4
FCkmEAg4NEqMVLSm26nLvrNK6z7lRMcIKZZcST+SL6lQv33gkUKIoGB9qx/+DlRvurVXfCdq
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
AAAAB3NzaC1yc2EAAAADAQABAAABAQDldzZ/iJi3VeHs4qDoxOP67jebaGwC
csr-cisco(conf-ssh-pubkey-
data)#6vkCn29bwSQ4CPJGVRLcVSNPcPPqVydiXVEOG8e9gFszkpk6c2meO+TRsSLiwHigv28l
csr-cisco(conf-ssh-pubkey-
data)#yw5xhn1Uck/AYpy9E6TyEEu9w6Fz0xTG2Qhe1n9b5Les6K9PFP/mR6WUMbfmaFredV/s
csr-cisco(conf-ssh-pubkey-
data)#ADnODPO+OfTK/OZPg34DNfcFhglja5GzudRb3S4nBBhDzuVrVC9RbA4PHVMXrLbIfqlk
csr-cisco(conf-ssh-pubkey-
data)#s3PCVGOtW1HxxTU4FCkmEAg4NEqMVLSm26nLvrNK6z7lRMcIKZZcST+SL6lQv33gkUKI
csr-cisco(conf-ssh-pubkey-data)#oGB9qx/+DlRvurVXfCdq3Cmxm2swHmb6MlrEtqIv 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 ha configurado correctamente, inicie sesión con las credenciales creadas o con el par de claves privadas para la clave pública con la credencial adicional.

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

```
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

Si se muestra el mensaje de error "Operation timed out" (Operación con tiempo de espera agotado).

```
$ 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 terminado 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:

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

Posible causa:

- El nombre de usuario o la clave privada son incorrectos.

Solución:

- Asegúrese de que el nombre de usuario es el mismo que se especificó cuando se implementó CSR1000v/C8000v.
- Asegúrese de que la clave privada es la misma que la que ha incluido en el momento de la implementación.

Información Relacionada

- Hoja de datos del router de servicios en la nube 1000v de Cisco
- Soporte Técnico y Documentación - Cisco Systems