

Implante um CSR1000v/C8000v na plataforma de nuvem do Google

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configuração do projeto](#)

[Etapa 1. Garanta um projeto válido e ativo para a conta.](#)

[Etapa 2. Crie um novo VPC e sub-rede.](#)

[Etapa 3. Implantação de Instância Virtual.](#)

[Verificar Implantação](#)

[Conectar-se remotamente à nova instância](#)

[Faça login no CSR1000v/C8000v com Bash Terminal](#)

[Faça login no CSR1000v/C8000v com PuTTY](#)

[Faça login no CSR1000v/C8000V com SecureCRT](#)

[Métodos adicionais de login de VM](#)

[Autorizar usuários adicionais a fazer login no CSR1000v/C8000v no GCP](#)

[Configurar um novo nome de usuário/senha](#)

[Configurar um novo usuário com chave SSH](#)

[Verifique os usuários configurados ao fazer login no CSR1000v/C8000v](#)

[Troubleshooting](#)

[Se a mensagem de erro "Operation Timed Out" for exibida.](#)

[Se for necessária uma senha](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve o procedimento para implantar e configurar um Cisco CSR1000v e um Catalyst 8000v (C800v) no Google Cloud Platform (GCP).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Tecnologias de virtualização / Máquinas Virtuais (VMs)

- Plataformas em nuvem

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Uma assinatura ativa do Google Cloud Platform com um projeto criado
- console GCP
- mercado de GCP
- Terminal Bash, Putty ou SecureCRT
- Chaves Secure Shell (SSH) públicas e privadas

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio


A partir da versão 17.4.1, o CSR1000v se torna o C8000v com a mesma funcionalidade, mas com novos recursos adicionados, como o SD-WAN e o licenciamento do Cisco DNA. Para obter mais informações, verifique a ficha técnica oficial dos produtos:


[Data Sheet do Cisco Cloud Services Router 1000v](#)

[Dados técnicos do software Cisco Catalyst 8000V Edge](#)

Portanto, este guia é aplicável para a instalação de roteadores CSR1000v e C8000v.

Configuração do projeto

 Observação: no momento em que este documento é escrito, os novos usuários têm 300 USD de créditos gratuitos para explorar totalmente o GCP como camada gratuita por um ano. Isso é definido pelo Google e não está sob o controle da Cisco.

 Observação: este documento requer a criação de chaves SSH públicas e privadas. Para obter informações adicionais, consulte [Gerar uma Chave SSH de Instância para Implantar um CSR1000v no Google Cloud Platform](#)

Etapa 1. Garanta um projeto válido e ativo para a conta.

Verifique se sua conta tem um projeto válido e ativo, que deve estar associado a um grupo com permissões para o Mecanismo de Computação.

Para esta implantação de exemplo, um projeto criado no GCP é usado.

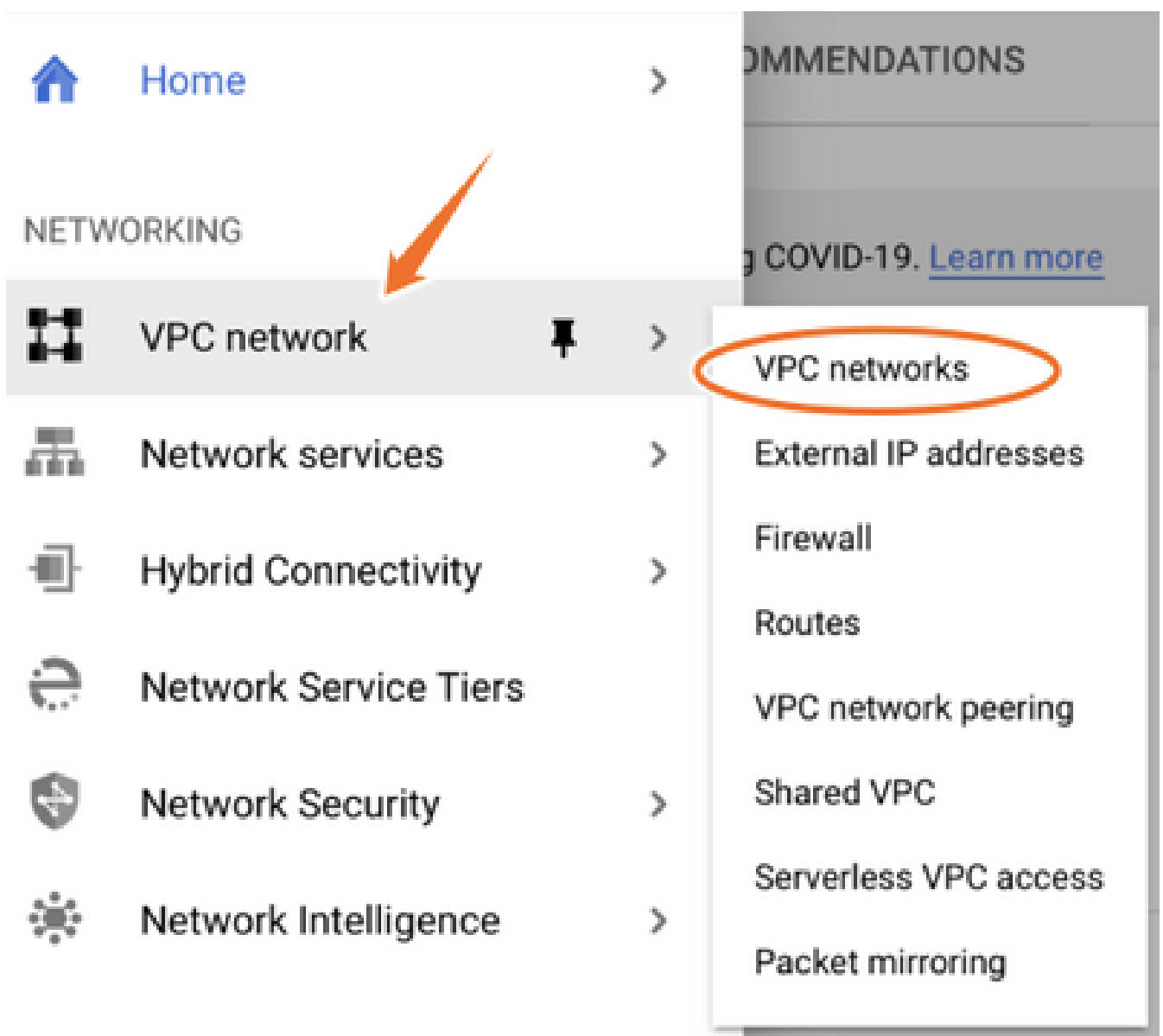
 Observação: para criar um novo projeto, consulte [Criar e gerenciar projetos](#).

Etapa 2. Crie um novo VPC e sub-rede.

Crie uma nova Virtual Private Cloud (VPC) e uma sub-rede que deve ser associada à instância CSR1000v.

É possível usar o VPC padrão ou um VPC e uma sub-rede criados anteriormente.

No painel de controle do console, selecione VPC network > VPC networks conforme mostrado na imagem.




Selecione Create VPC Network como mostrado na imagem.

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	

✎ Observação: atualmente, o CSR1000v é implantado somente na região central dos EUA no GCP.

Configure o nome do VPC conforme mostrado na imagem.

← Create a VPC network

Name * 
csr-vpc

Lowercase letters, numbers, hyphens allowed

Description

Configure o nome da sub-rede associado ao VPC e selecione a região us-central1.

Atribua um intervalo de endereços IP válido dentro do CIDR us-central1 de 10.128.0.0/20. como mostrado na imagem.

Deixe outras configurações como padrão e selecione o botão criar:

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

 Observação: se "automático" for selecionado, o GCP atribuirá um intervalo válido automático dentro da região CIDR.

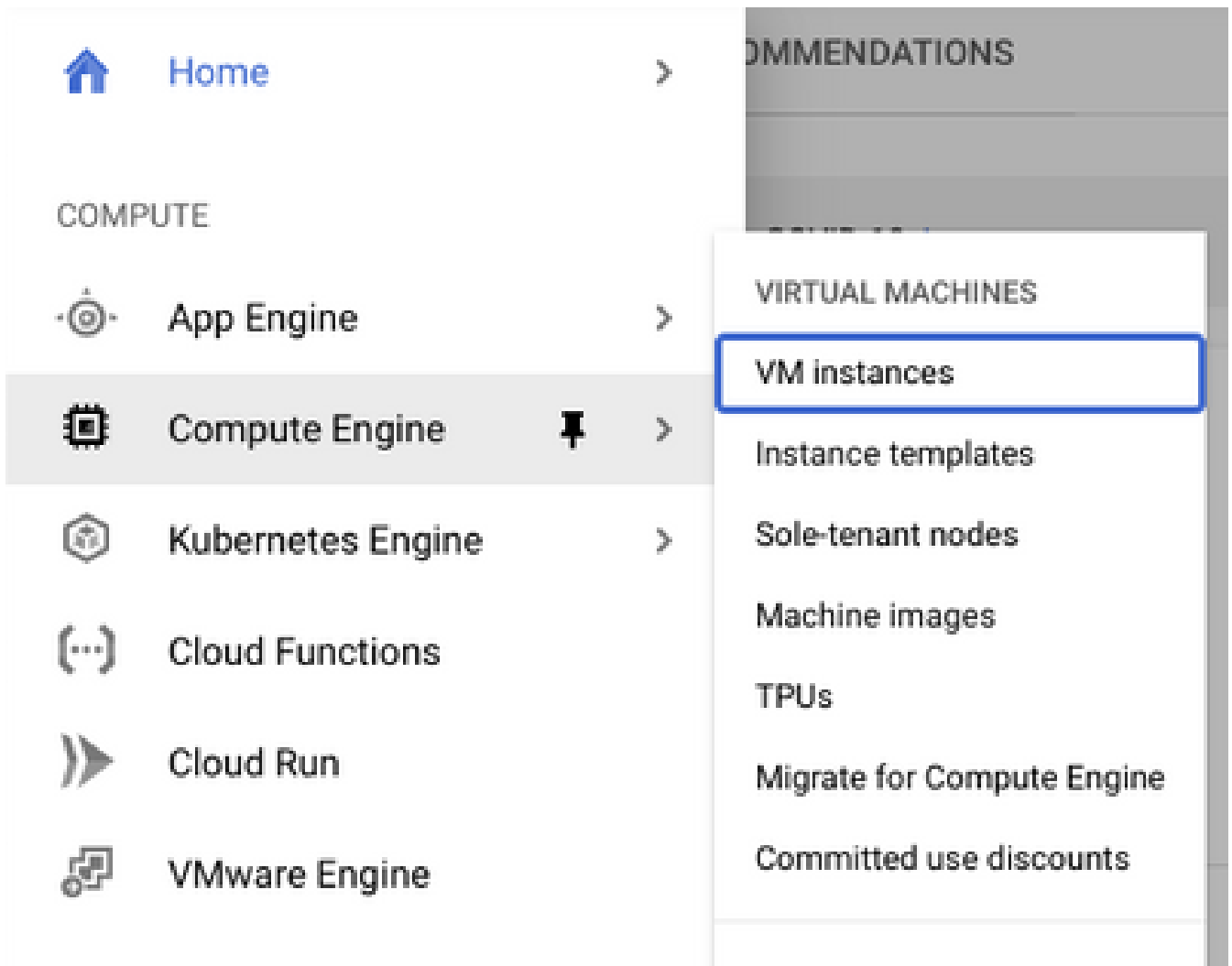
Quando o processo de criação terminar, o novo VPC aparecerá na seção Redes VPC, como mostrado na imagem.

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

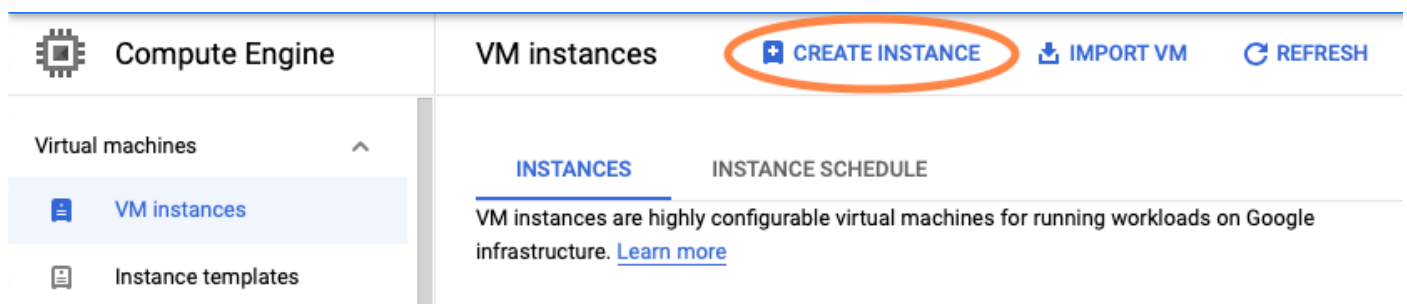
Name ↑	Region	Subnets	MTU ?	Mode	IP address ranges	Gateways
▼ csr-vpc		1	1460	Custom		
	us-central1	csr-subnet			10.10.1.0/24	10.10.1.1

Etapa 3. Implantação de Instância Virtual.

Na seção Mecanismo de computação, selecione Mecanismo de computação > instâncias de VM como mostrado na imagem.



No painel da VM, selecione a guia Criar instância como mostrado na imagem.



Use o mercado GCP como mostrado na imagem para exibir produtos da 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

Na barra de pesquisa, digite Cisco CSR ou Catalyst C800v, escolha o modelo e a versão que atenda às suas necessidades e selecione Iniciar.

Para este exemplo de implantação, a primeira opção foi selecionada conforme mostrado na imagem.

Filter Type to filter

Category

Compute

(4)

Networking

(7)

Type

Virtual machines

X

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

Observação: BYOL significa "Bring Your Own License" (traga sua própria licença).

Observação: atualmente, o GCP não suporta o modelo de pagamento progressivo (PAYG).

O GCP requer a inserção dos valores de configuração que devem ser associados à VM, como mostrado na imagem:

Um nome de usuário e uma chave pública SSH são necessários para implantar um CSR1000v/C8000v no GCP, como mostrado na imagem. Consulte [Generate an Instance SSH Key to Deploy a CSR1000v in Google Cloud Platform](#) se as chaves SSH não tiverem sido criadas.

← 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 ?

Selecione o VPC e a sub-rede criados antes e escolha Efêmero no IP externo, para ter um IP Público associado à instância, como mostrado na imagem.

Depois disso ser configurado. Selecione o botão de ativação.

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

 Observação: a porta 22 é necessária para se conectar à instância do CSR via SSH. A porta HTTP é opcional.

Quando a implantação estiver concluída, selecione Compute Engine > VM instances para verificar se o novo CSR1000v foi implantado com êxito, como mostrado na imagem.

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 Implantação

Conectar-se remotamente à nova instância

Os métodos mais comuns para fazer login em um CSR1000v/C8000V no GCP são a linha de comando em um terminal Bash, Putty e SecureCRT. Nesta seção, a configuração necessária para se conectar aos métodos anteriores.

Faça login no CSR1000v/C8000v com Bash Terminal

A sintaxe necessária para se conectar remotamente ao novo CSR é:

```
<#root>
```

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

Exemplo:

```
<#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.
```

Se a conexão for bem-sucedida, o prompt CSR1000v será exibido

```
<#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
```

Faça login no CSR1000v/C8000v com PuTTY

Para conectar com Putty, use o aplicativo PuTTYgen para converter a chave privada do formato PEM para PPK.

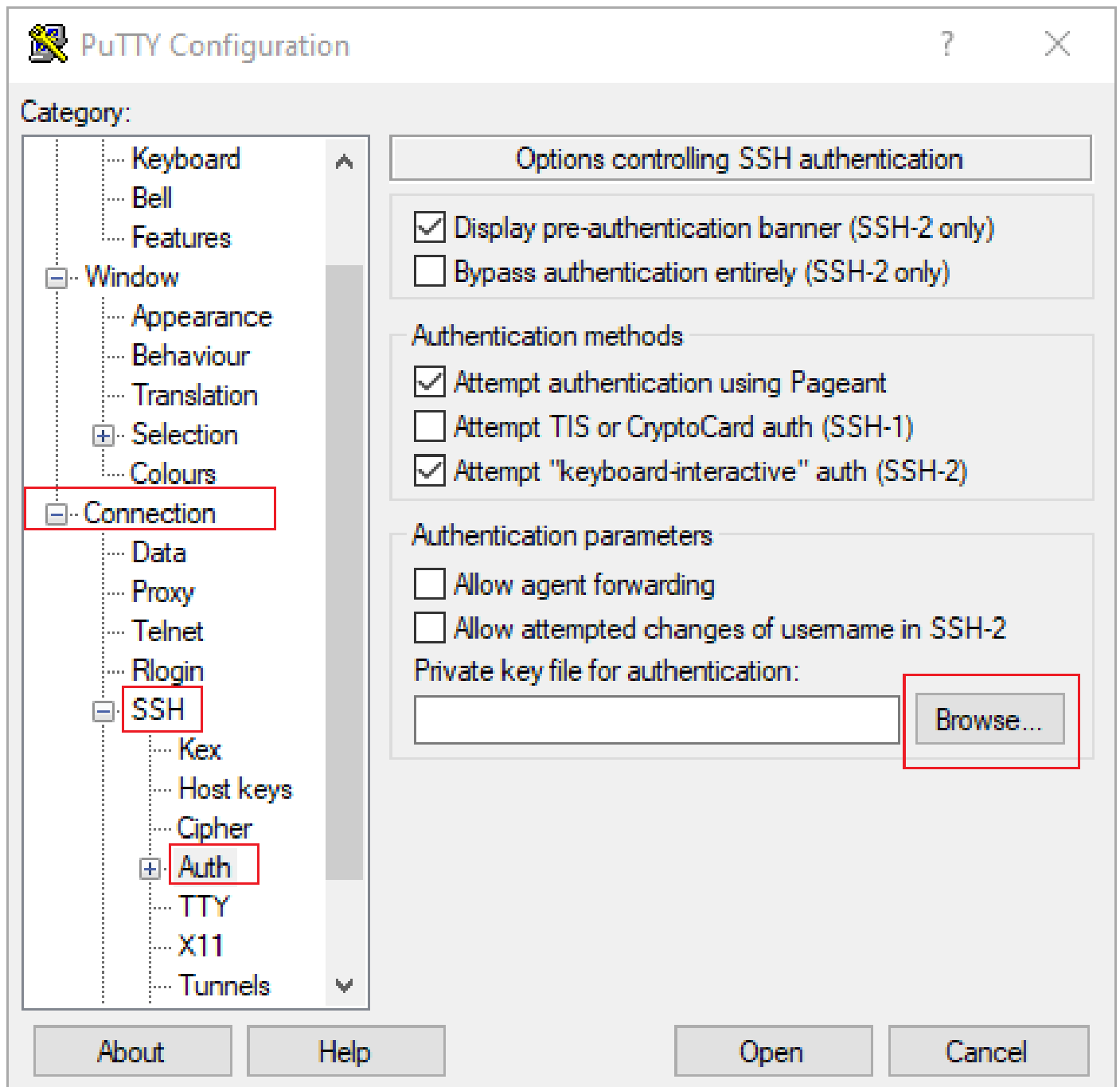
Consulte [Convert Pem to Ppk File Using PuTTYgen](#) para obter informações adicionais.

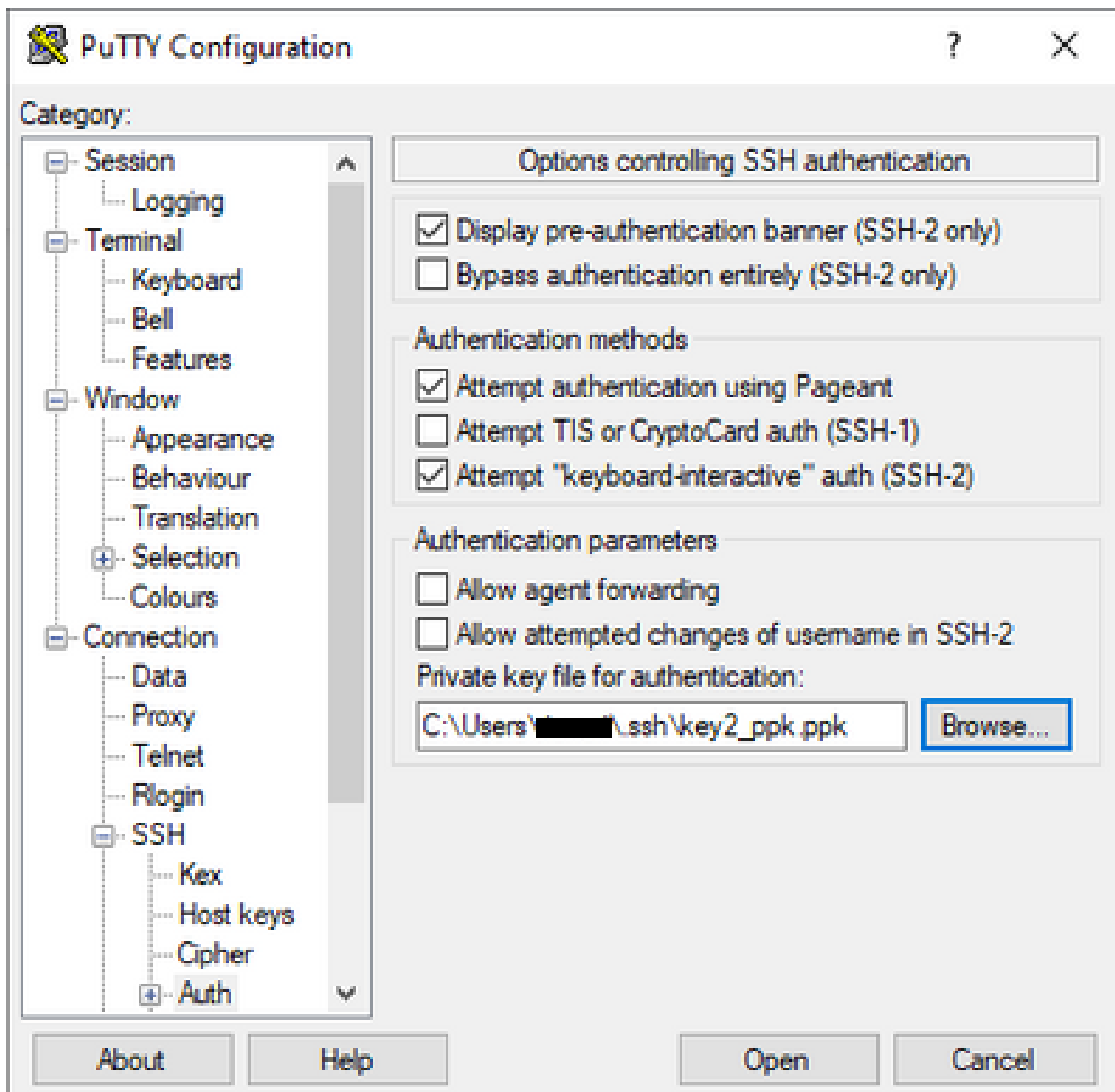
Depois que a chave privada for gerada no formato apropriado, você terá que especificar o caminho em Putty.

Selecione o arquivo de chave privada para a seção de autenticação na opção auth do menu SSH connection.

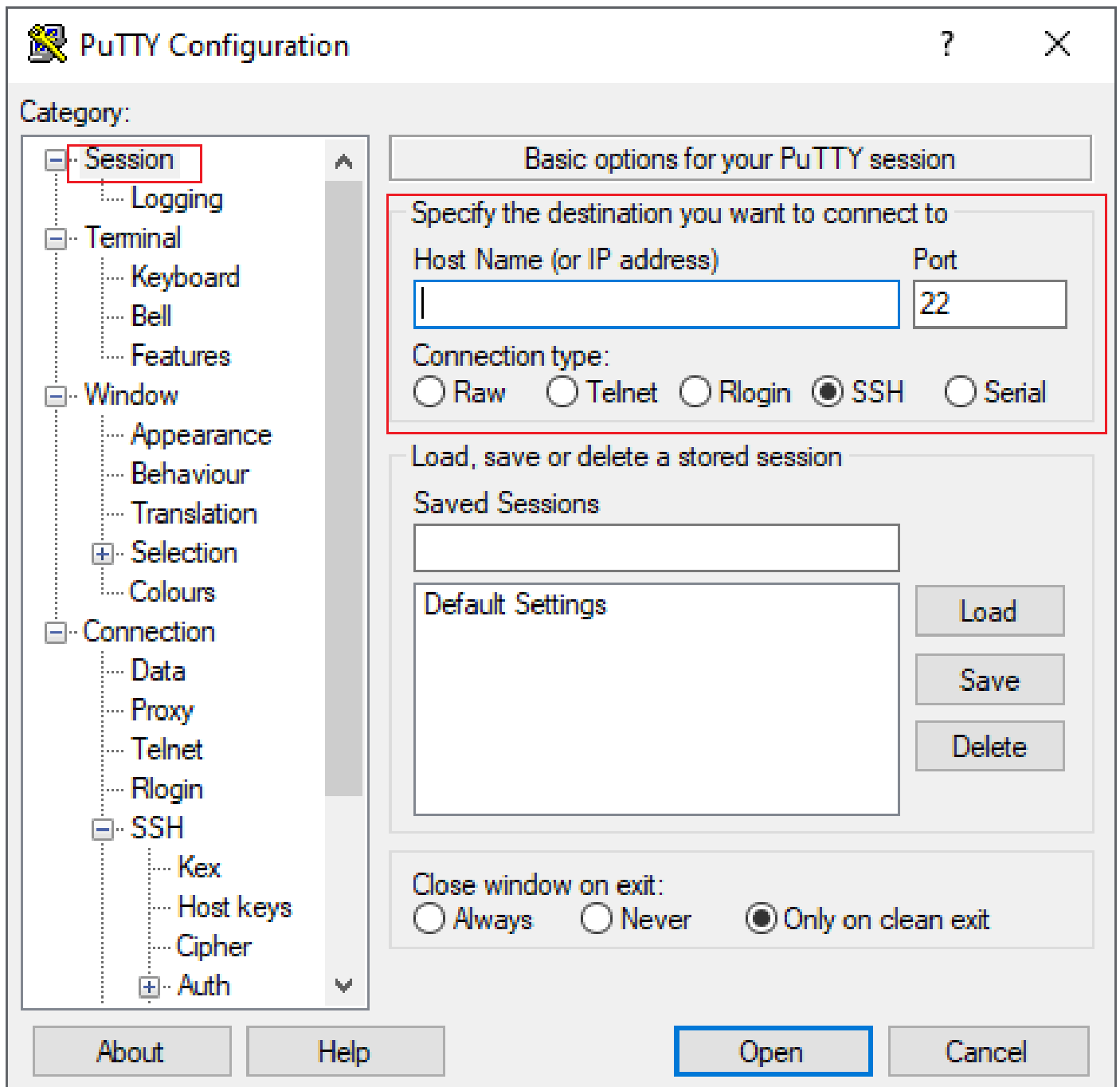
Navegue até a pasta onde a chave está armazenada e selecione a chave criada. Neste exemplo,


as imagens mostram a visualização gráfica do menu Putty e o estado desejado:





Depois que a chave apropriada for selecionada, retorne ao menu principal e use o endereço IP externo da instância CSR1000v para se conectar via SSH, como mostrado na imagem.



 Observação: o nome de usuário/senha definidos nas chaves SSH geradas são solicitados para fazer login.

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

```
csr-cisco#
```

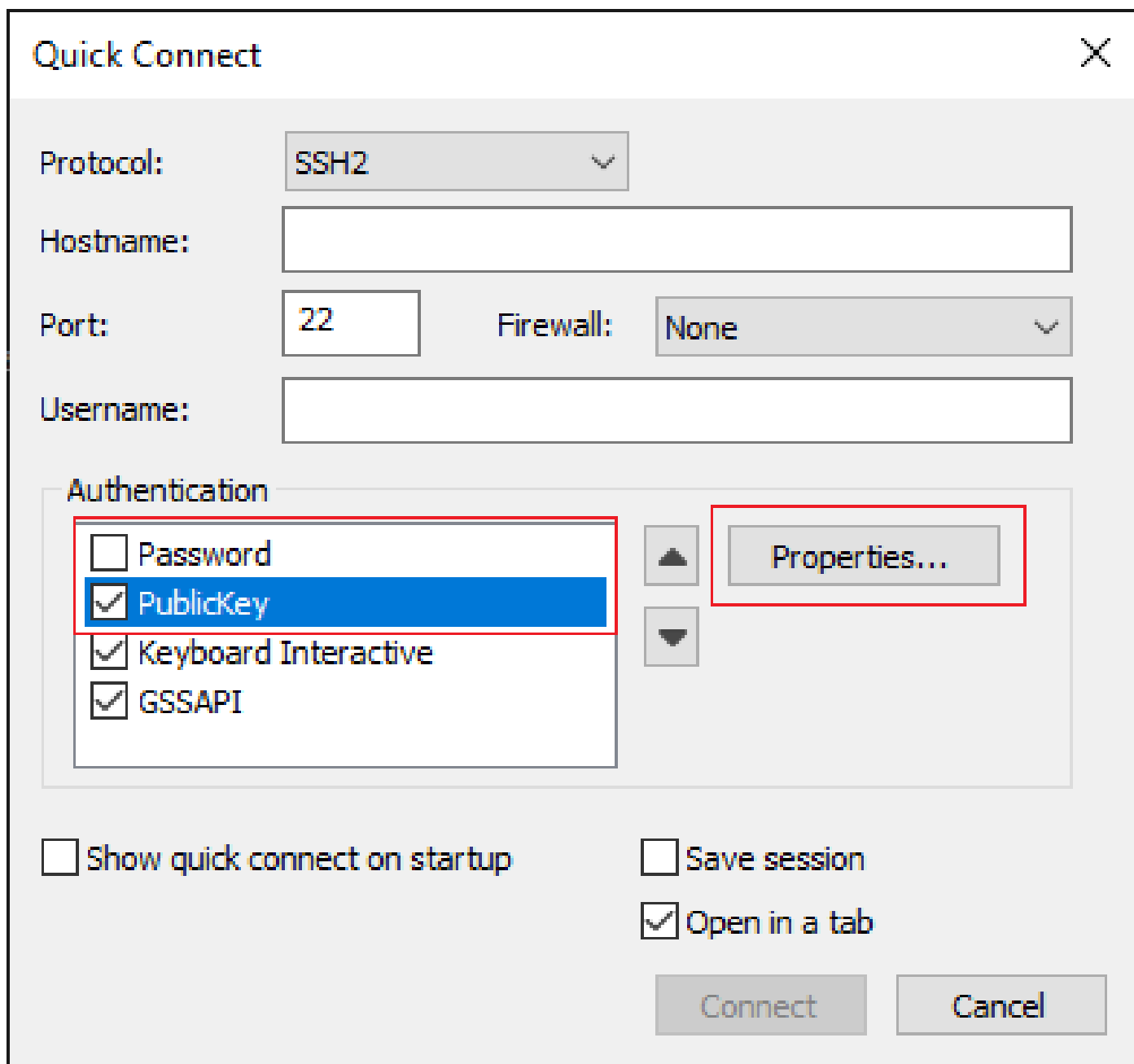
Faça login no CSR1000v/C8000V com SecureCRT

O SecureCRT requer a chave privada no formato PEM, que é o formato padrão para as chaves privadas.

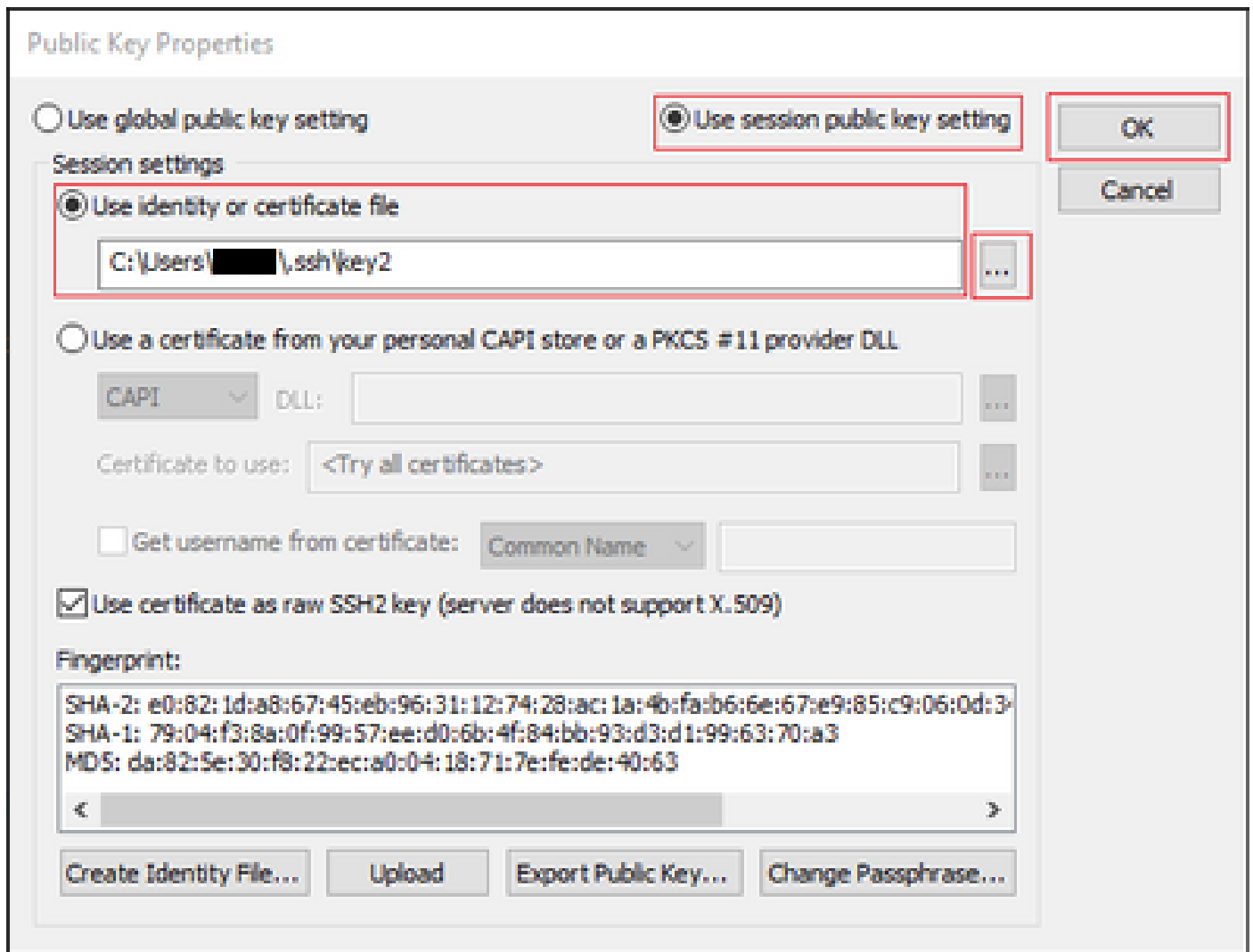
No SecureCRT, especifique o caminho para a chave privada no menu:

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

A imagem mostra a janela esperada:



Selecione Use session public key string > Select Use identity or certificate file > Select ... > Navegue até o diretório e selecione a chave desejada > Select OK como mostrado na imagem.



Finalmente, conecte-se ao IP externo do endereço da instância via SSH, como mostrado na imagem.

Quick Connect X

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

 Observação: o nome de usuário/senha definidos nas chaves SSH geradas são solicitados para fazer login.

```
<#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 adicionais de login de VM

 Observação: consulte [Conectar-se a VMs Linux usando a documentação de métodos avançados](#).

Autorizar usuários adicionais a fazer login no CSR1000v/C8000v no GCP

Depois que o login na instância do CSR1000v for bem-sucedido, é possível configurar usuários adicionais com estes métodos:

Configurar um novo nome de usuário/senha

Use estes comandos para configurar um novo usuário e uma nova senha:

```
<#root>
```

```
enable
```

```
configure terminal
```

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

```
end
```

Exemplo:

```
<#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#
```

Um novo usuário agora pode fazer login na instância do CSR1000v/C8000v.

Configurar um novo usuário com chave SSH

Para obter acesso à instância CSR1000v, configure a chave pública. As chaves SSH nos metadados da instância não fornecem acesso a CSR1000v.

Use estes comandos para configurar um novo usuário com uma chave SSH:

```
<#root>
```

```
configure terminal
```

```
ip ssh pubkey-chain
```


```
username <username>
```

```
key-string
```

```
<public ssh key>
```

```
exit
```

```
end
```

 Observação: o comprimento máximo da linha na CLI da Cisco é de 254 caracteres, portanto, a sequência de chaves não pode se ajustar a essa limitação. É conveniente envolver a sequência de chaves para se ajustar a uma linha de terminal. Os detalhes sobre como superar essa limitação são explicados em [Gerar uma Chave SSH de Instância para Implantar um CSR1000v na Plataforma de Nuvem do Google](#).

```
<#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#
```

Verifique os usuários configurados ao fazer login no CSR1000v/C8000v

Para confirmar se a configuração foi definida corretamente, faça login com as credenciais criadas ou com o par de chaves privadas para a chave pública com a credencial adicional.

No lado do roteador, consulte o log de login bem-sucedido com o endereço IP do 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#
```

Troubleshooting

Se a mensagem de erro "Operation Timed Out" for exibida.

```
<#root>
```

```
$
```

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

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

Possíveis causas:

- A instância não concluiu sua implantação.
- O endereço público não é aquele atribuído à nic0 na VM.

Solução:

Aguarde a conclusão da implantação da VM. Geralmente, uma implantação do CSR1000v leva até 5 minutos para ser concluída.

Se for necessária uma senha

Se for necessária uma senha:

```
<#root>
```

```
$
```

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

```
Password:
```

```
Password:
```

Possível causa:

- O nome de usuário ou a chave privada está incorreto.
- Em versões mais recentes de sistemas operacionais como MacOS ou Linux, o utilitário OpenSSH não tem RSA habilitado por padrão.

Solução:

- Certifique-se de que o nome de usuário seja o mesmo que foi especificado quando CSR1000v/C8000v foi implantado.
- Certifique-se de que a chave privada seja a mesma que você incluiu no momento da implantação.
- Especifique o tipo de chave aceita no comando ssh:

```
<#root>
```

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

Informações Relacionadas

- [Data Sheet do Cisco Cloud Services Router 1000v](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.