

Een CSR1000v/C8000v implementeren op Google Cloud-platform

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Instellen van projecten](#)

[Stap 1. Zorg voor een geldig en actief project voor de rekening.](#)

[Stap 2. Maak een nieuwe VPC en subnet.](#)

[Stap 3. Inzet van virtuele instanties.](#)

[Controleer de implementatie](#)

[Connect op afstand met het nieuwe exemplaar](#)

[Meld u aan bij CSR1000v/C8000v met Bash-terminal](#)

[Inloggen op CSR1000v/C8000v met PuTTY](#)

[Meld u aan bij CSR1000v/C800V met SecureCRT](#)

[Aanvullende VM-inlogmethoden](#)

[Geef extra gebruikers toestemming om in te loggen op CSR1000v/C800v in GCP](#)

[Een nieuwe gebruikersnaam/wachtwoord configureren](#)

[Een nieuwe gebruiker met SSH-toets configureren](#)

[Controleer de ingestelde gebruikers op inloggen bij CSR1000v/C8000v](#)

[Problemen oplossen](#)

[Als de foutmelding "Handeling ingesteld op out" wordt weergegeven.](#)

[Als een wachtwoord vereist is](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft de procedure om een Cisco-cloudservicesrouter 1000v (CSR1000v) en Catalyst 8000v (C800v) Edge-router op Google Cloud Platform (GCP) in te zetten en te configureren.

Bijgedragen door Eric Garcia, Ricardo Neri, Cisco TAC-engineers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Virtualisatietechnologieën/virtuele machines (VM's)

- Cloudplatforms

Gebruikte componenten

- Een actieve abonnement op Google Cloud Platform met een project dat is gemaakt
- GCP-console
- GCP-marktplaats
- Basis-terminal, potentieel of SecureCRT
- Toetsen van openbare en privé Secure Shell (SSH)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Vanaf 17.4.1 wordt de CSR1000v C8000v met dezelfde functionaliteit, maar er worden nieuwe functies toegevoegd, zoals SDWAN- en DNA-licenties. Verifieer voor meer informatie het informatieblad voor officiële producten:

[Cisco Cloud-services router 1000v dataplaat](#)

[Cisco Catalyst 8000V Edge-software release](#)

Daarom is deze handleiding van toepassing voor de installatie van zowel CSR1000v- als C8000v-routers.

Instellen van projecten

Opmerking: Op het moment dat dit document wordt geschreven, hebben nieuwe gebruikers gratis krediet van EUR 300 om GCP voor een jaar als vrij Tier volledig te kunnen verkennen. Dit wordt gedefinieerd door Google en is niet onder Cisco-controle.

Opmerking: voor dit document moeten openbare en particuliere SSH-toetsen worden gemaakt. Raadpleeg voor meer informatie [Generate an Instance SSH Key om CSR1000v te implementeren in Google Cloud Platform](#)

Stap 1. Zorg voor een geldig en actief project voor de rekening.

Zorg ervoor dat uw account een geldig en actief project heeft, dat deze aan een groep met rechten voor Compute Engine zijn gekoppeld.

Voor deze voorbeeldplaatsing, wordt een gecreëerd project in de GCP gebruikt.

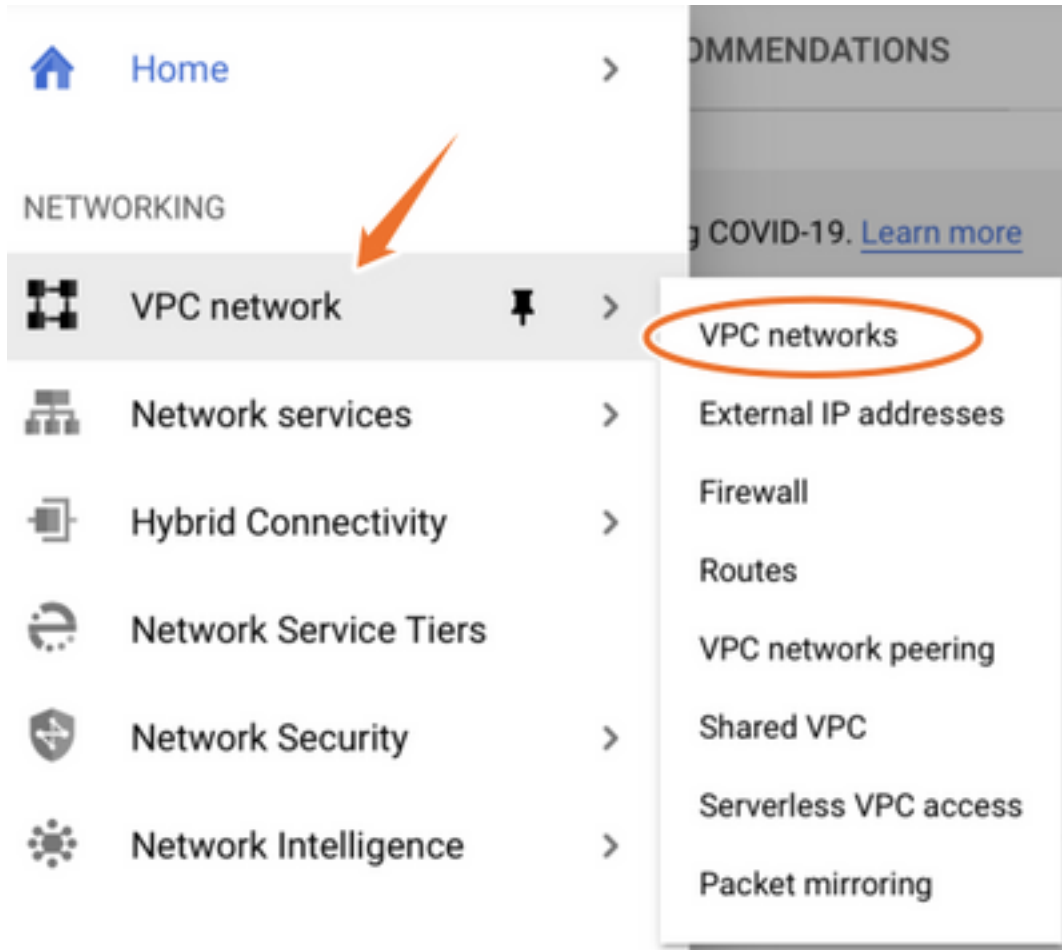
Opmerking: Raadpleeg [Projecten maken en beheren](#) om een nieuw project te maken.

Stap 2. Maak een nieuwe VPC en subnet.

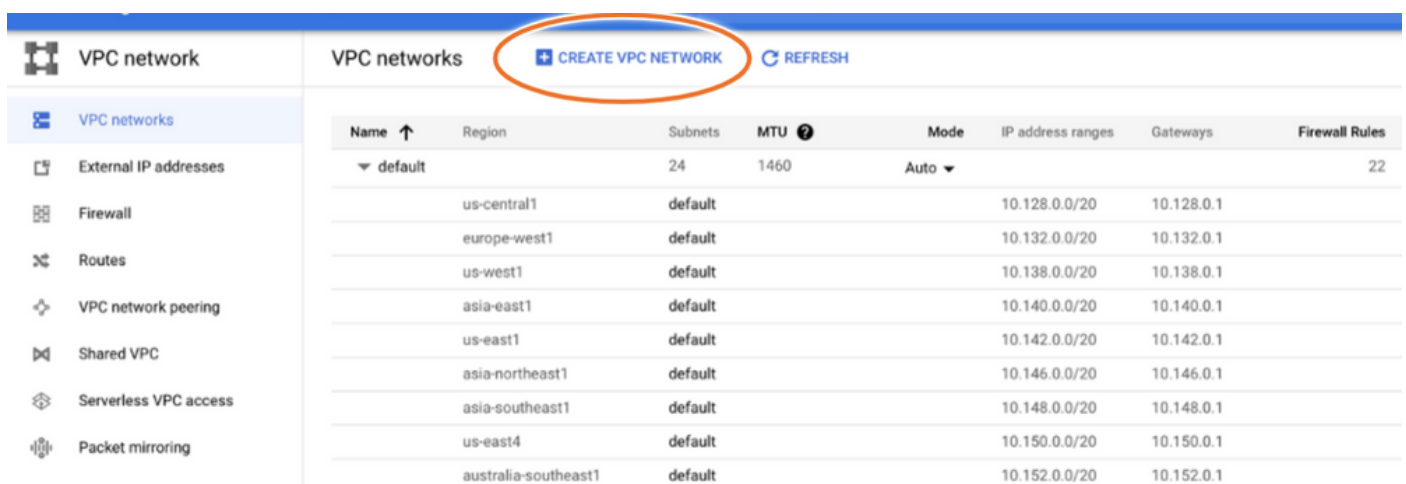
Maak een nieuwe Virtual Private Cloud (VPC) en een netwerk dat met de CSR1000v-instantie moet worden geassocieerd.

Het is mogelijk om de standaard VPC of een eerder gemaakte VPC en SUBNET te gebruiken.

Selecteer in het console-dashboard de optie **VPC-netwerk > VPC-netwerken** zoals in de afbeelding.



Selecteer **VPC Network maken** zoals in de afbeelding.



Opmerking: Op dit moment wordt CSR1000v alleen ingezet in de centraal-amerikaanse

regio op GCP.

Configureer de VPC-naam zoals in de afbeelding.

← Create a VPC network

Name *

csr-vpc

Lowercase letters, numbers, hyphens allowed

Description

Configureer de subnetnaam die aan de VPC is gekoppeld en selecteer de optie regio **us-central1**.

Toewijzen aan een geldig IP-adresbereik binnen de us-central1 CIDR van 10.128.0.0/20 zoals in de afbeelding.

Laat andere instellingen standaard staan en selecteer de optie **Maken** knop:

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

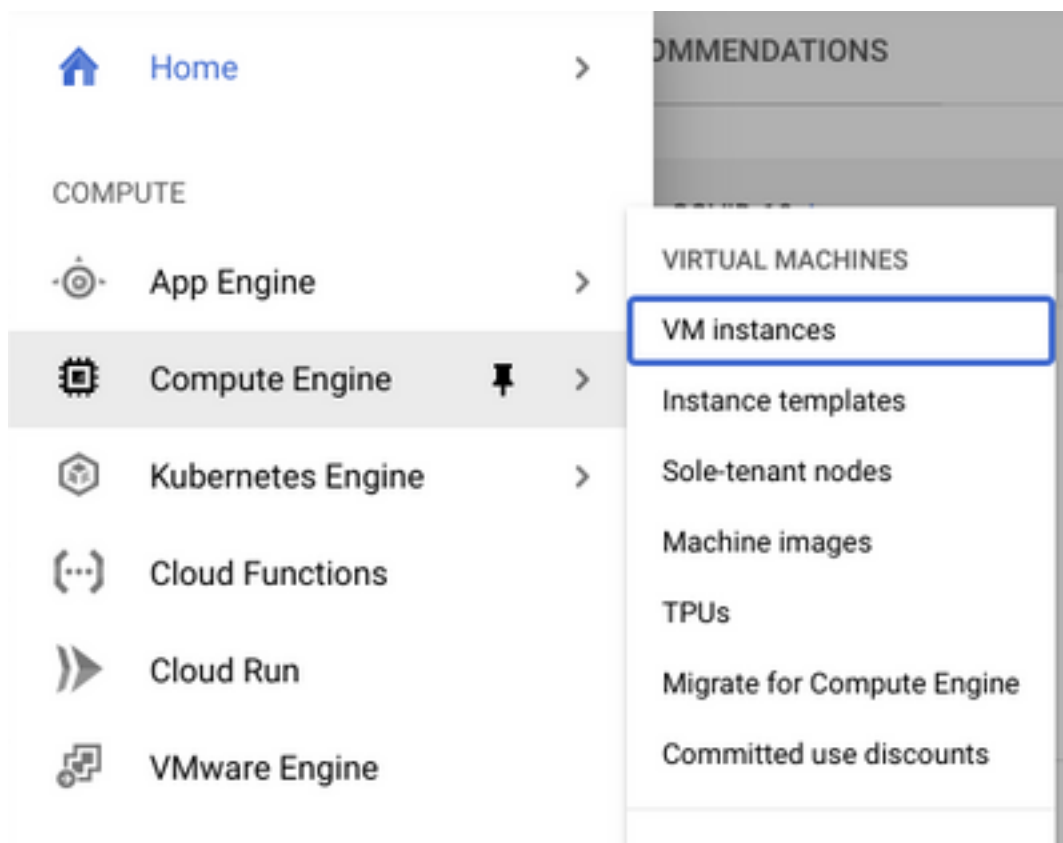
Opmerking: Als "automatisch" is geselecteerd, wijst GCP een automatisch geldig bereik toe binnen het gebied CIDR.

Nadat het aanmaakproces is voltooid, wordt de nieuwe VPC in het gedeelte **VPC-netwerken** weergegeven zoals in de afbeelding.

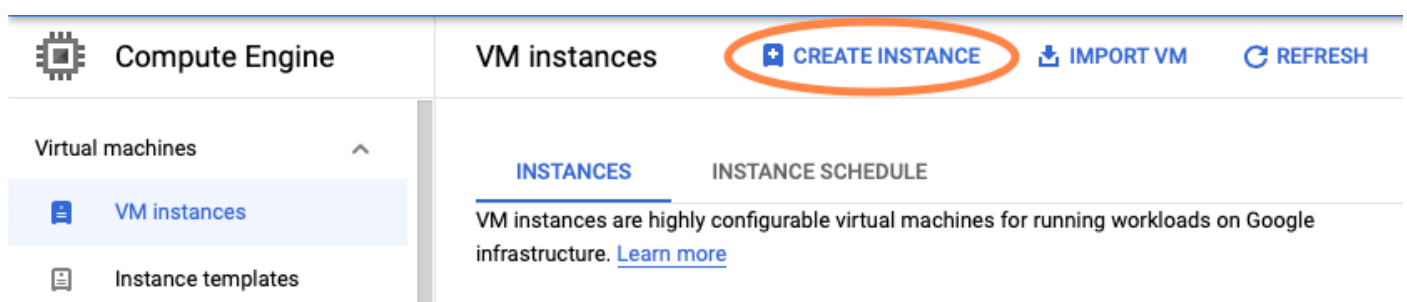
Name ↑	Region	Subnets	MTU ?	Mode	IP address ranges	Gateways
▼ csr-vpc		1	1460	Custom		
	us-central1	csr-subnet			10.10.1.0/24	10.10.1.1

Stap 3. Inzet van virtuele instanties.

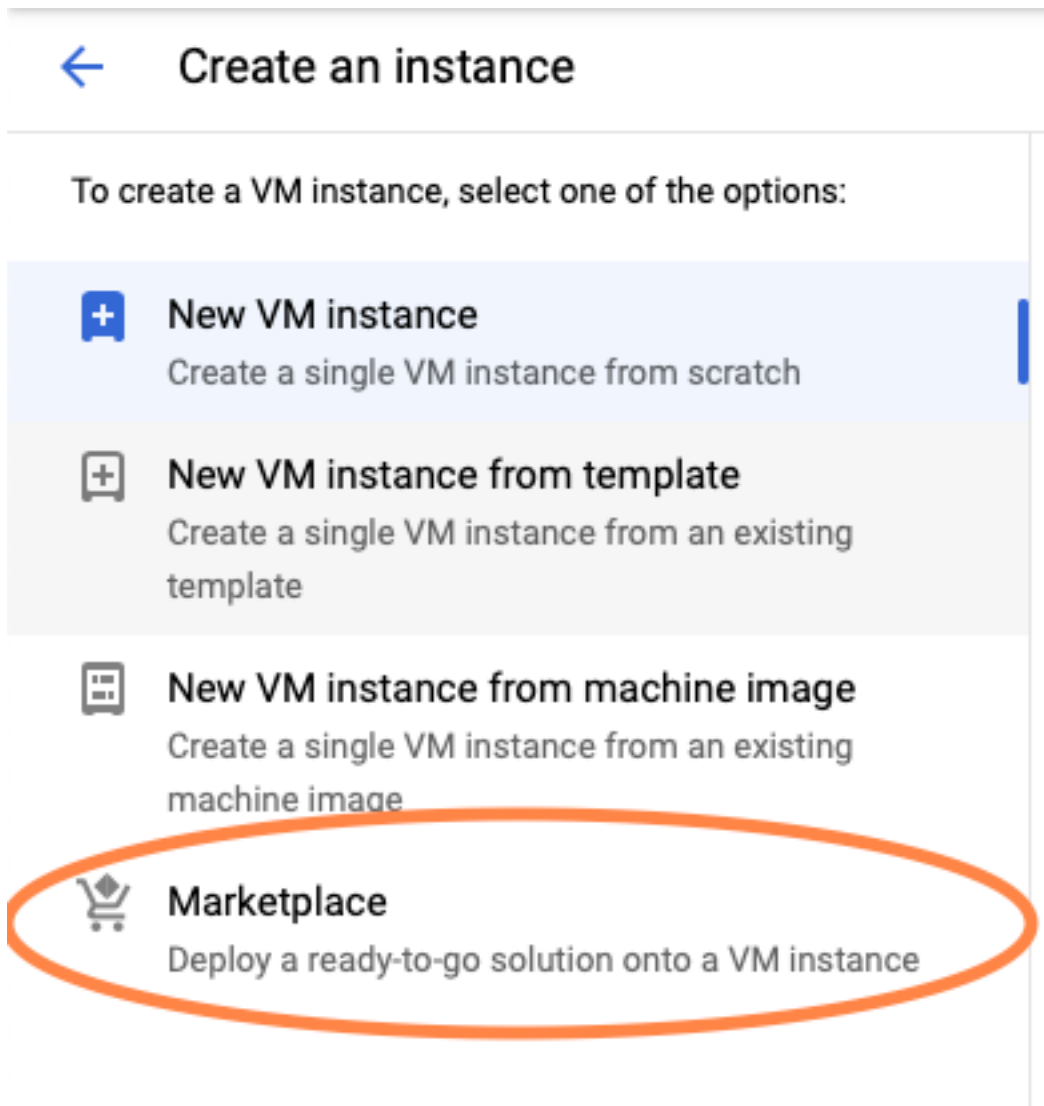
Selecteer in het gedeelte **Computing Engine** de optie **Computing Engine > VM-instellingen** zoals in de afbeelding.



Selecteer eenmaal in het **VM dashboard** het tabblad **Instance maken** zoals in de afbeelding wordt weergegeven.



Gebruik een GCP-marktplaats zoals in de afbeelding, om Cisco-producten weer te geven.



Typ in de zoekbalk **Cisco CSR** of **Catalyst C8000v** een model en een versie die passen bij uw vereisten en selecteer **Start**.

Voor deze voorbeeldplaatsing, werd de eerste optie geselecteerd zoals in de afbeelding.

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 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

**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

**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

**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

Filter Type to filter

Category ^

Compute (1)


Networking (1)

Type

Virtual machines

Virtual machines

1 result



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

Opmerking: BYOL staat voor "Breng je eigen licentie".

Opmerking: momenteel ondersteunt GCP niet het betalingsmodel (PAYG).

GCP moet de configuratiewaarden invoeren die bij de VM moeten worden gekoppeld, zoals in de afbeelding wordt getoond:

Er is een gebruikersnaam en SSH-openbare sleutel vereist om een CSR1000v/C8000v in GCP in te zetten zoals in de afbeelding. Raadpleeg [Generate an Instance SSH Key om CSR1000v te implementeren in Google Cloud Platform](#) indien de SSH-toetsen niet zijn gemaakt.



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 ?

Selecteer de VPC en het type dat vóór gecreëerd is en kies Ephemeral in externe IP, om een openbare IP te hebben geassocieerd met de instantie zoals getoond in het beeld.

Nadat dit is ingesteld. Selecteer de knop **Start**.

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

Opmerking: Port 22 is nodig om verbinding te maken met de CSR-instantie via SSH. De HTTP poort is optioneel.

Nadat de implementatie is voltooid, selecteert u **Computing Engine > VM instanties** om te controleren of de nieuwe CSR1000v met succes is ingezet zoals in de afbeelding wordt getoond.

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 type="checkbox"/> <input checked="" type="checkbox"/> csr-cisco	us-central1-f			10.10.1.2 (nic0)	[REDACTED]	SSH ⌵ ⋮

Controleer de implementatie

Connect op afstand met het nieuwe exemplaar

De meest gebruikelijke methoden om in te loggen op een CSR1000v/C8000V in GCP zijn de opdrachtregel in een Bash-terminal, Putty en SecureCRT. In dit gedeelte dient u de configuratie in te stellen die nodig is voor de aansluiting op de vorige methoden.

Meld u aan bij CSR1000v/C8000v met Bash-terminal

De syntaxis die nodig is om extern aan de nieuwe CSR te verbinden is:

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

Voorbeeld:

```
$ 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.
```

Als de verbinding succesvol is, wordt de CSR1000v-prompt weergegeven

```
$ 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
```

Inloggen op CSR1000v/C8000v met PuTTY

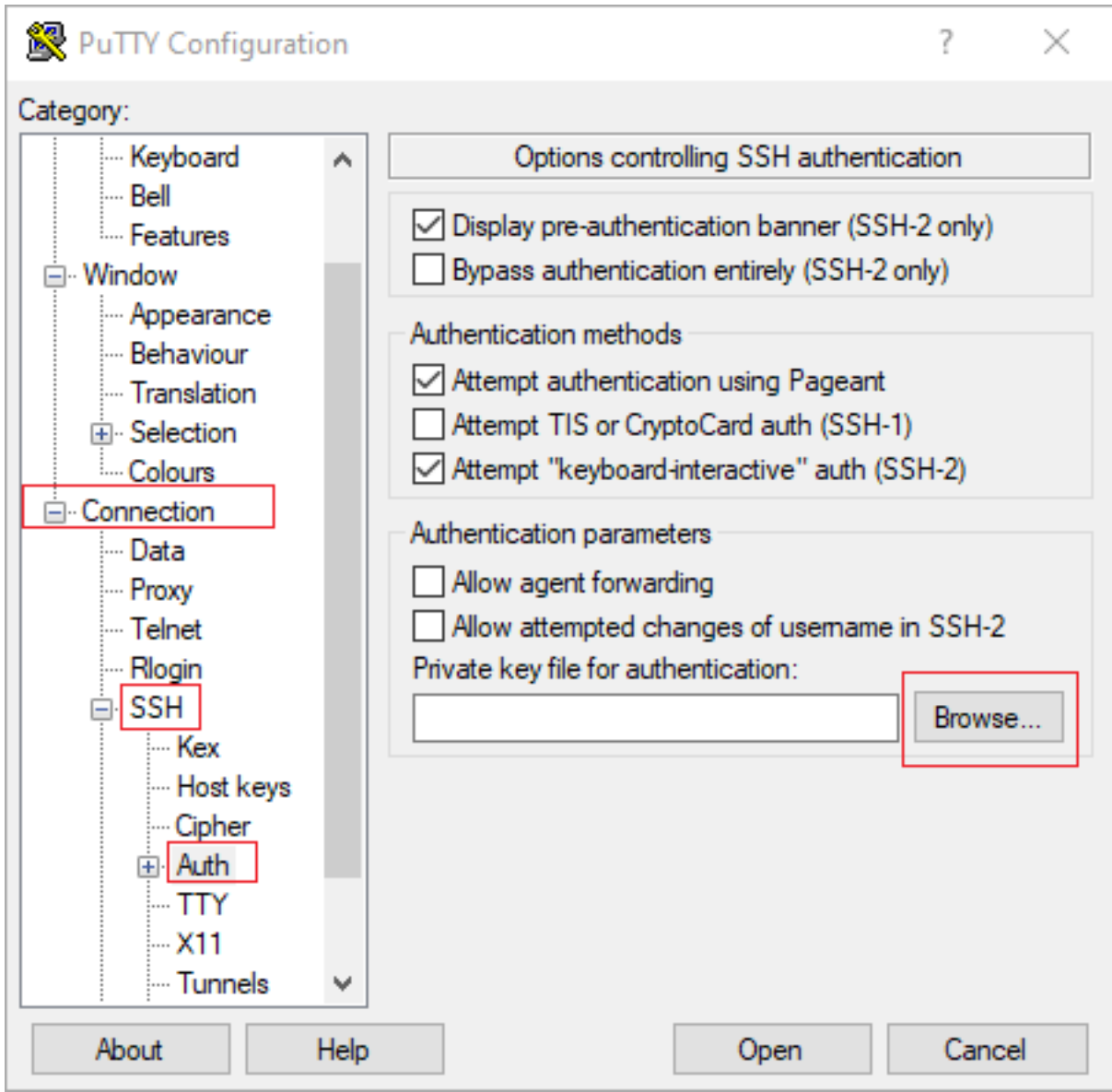
Gebruik de PuTTYgen-toepassing om de privé-toets van PEM naar PPK-formaat om te zetten.

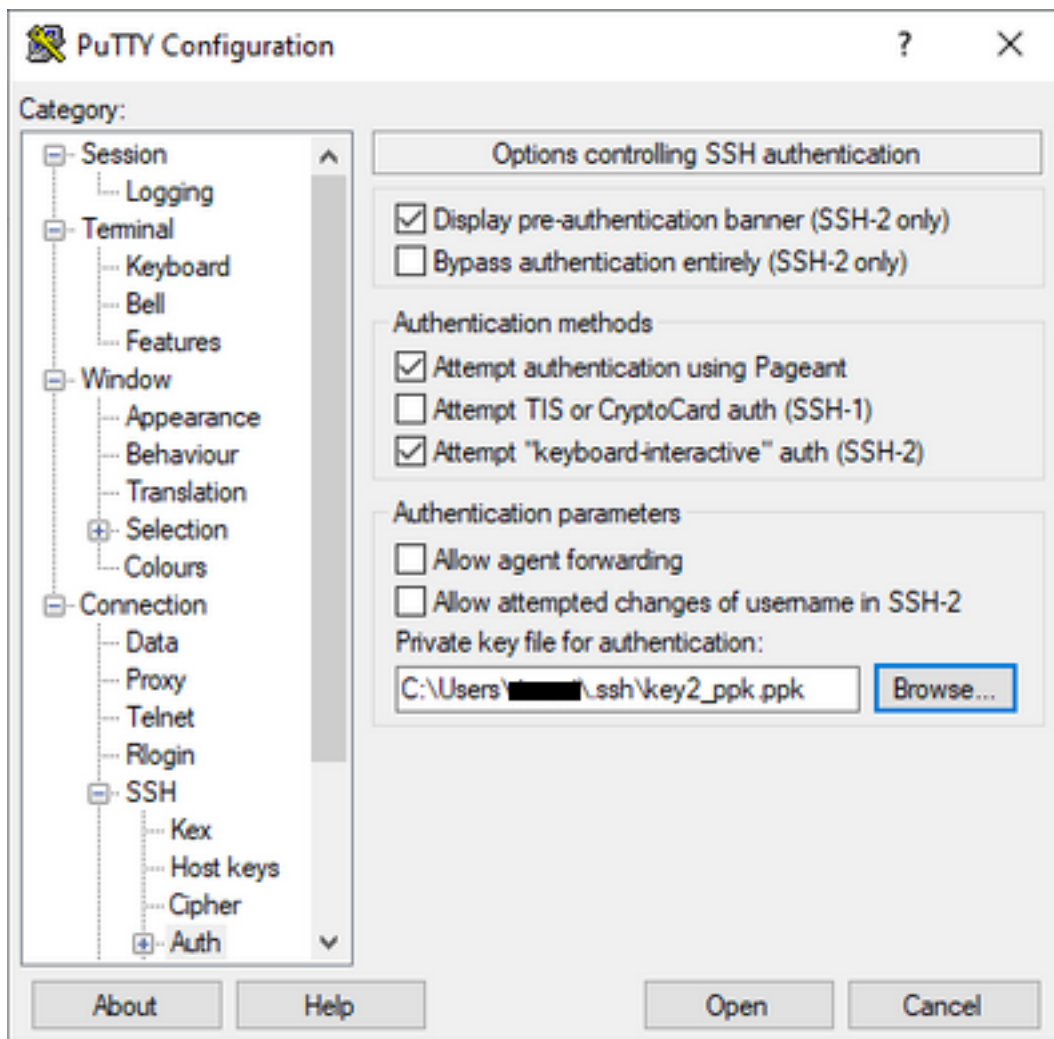
Raadpleeg het gedeelte [PDF-bestand converteren naar PPP-bestand met PuTTYgen](#) voor meer informatie.

Zodra de privétoets in de juiste indeling is gegenereerd, moet u het pad in Poetin specificeren.

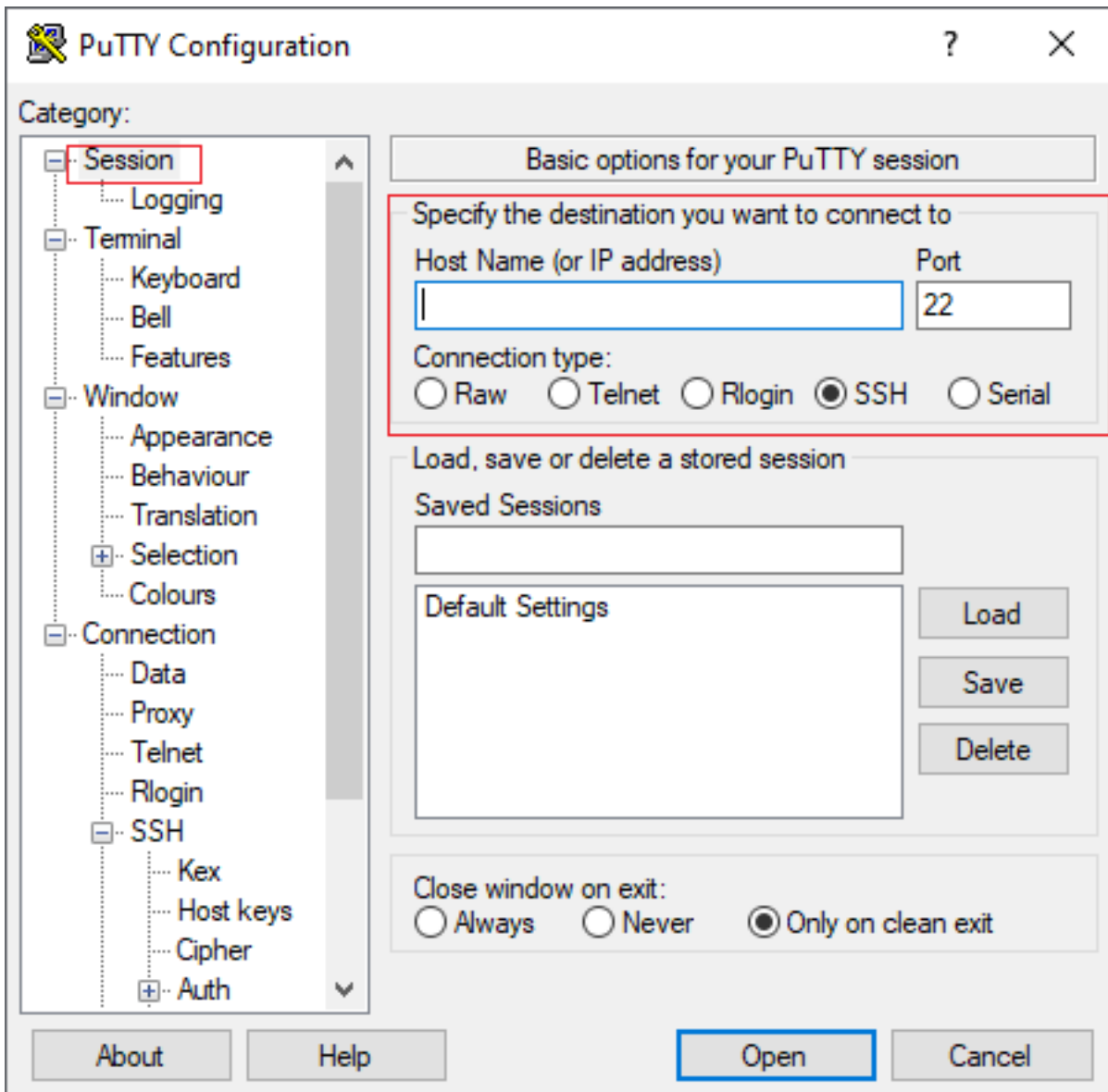
Selecteer het **Private key file voor authenticatie** in de autooptie van het SSH **connectie** menu.

Bladeren naar de map waarin de toets is opgeslagen en selecteer de nieuwe toets. In dit voorbeeld tonen de beelden de grafische weergave van het Putty menu en de gewenste status:





Zodra de juiste toets is geselecteerd, keert u terug naar het hoofdmenu en gebruikt u het externe IP-adres van de CSR1000v-instantie voor aansluiting via SSH zoals in de afbeelding.



Opmerking: Gebruikersnaam/wachtwoord die is gedefinieerd in de gegenereerde SSH-toetsen wordt gevraagd in te loggen.

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

```
csr-cisco#
```

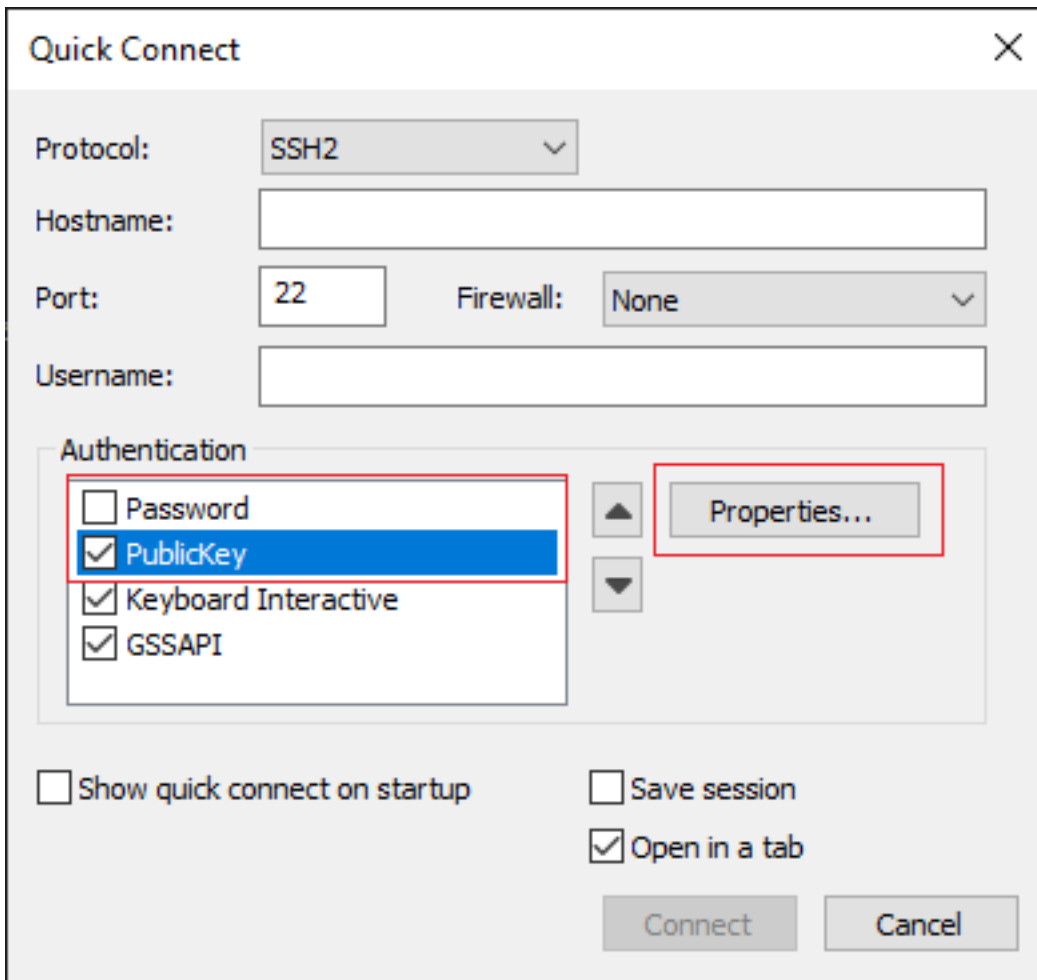
Meld u aan bij CSR1000v/C800V met SecureCRT

SecureCRT vereist de privé-toets in PEM-formaat, het standaardformaat voor de particuliere toetsen.

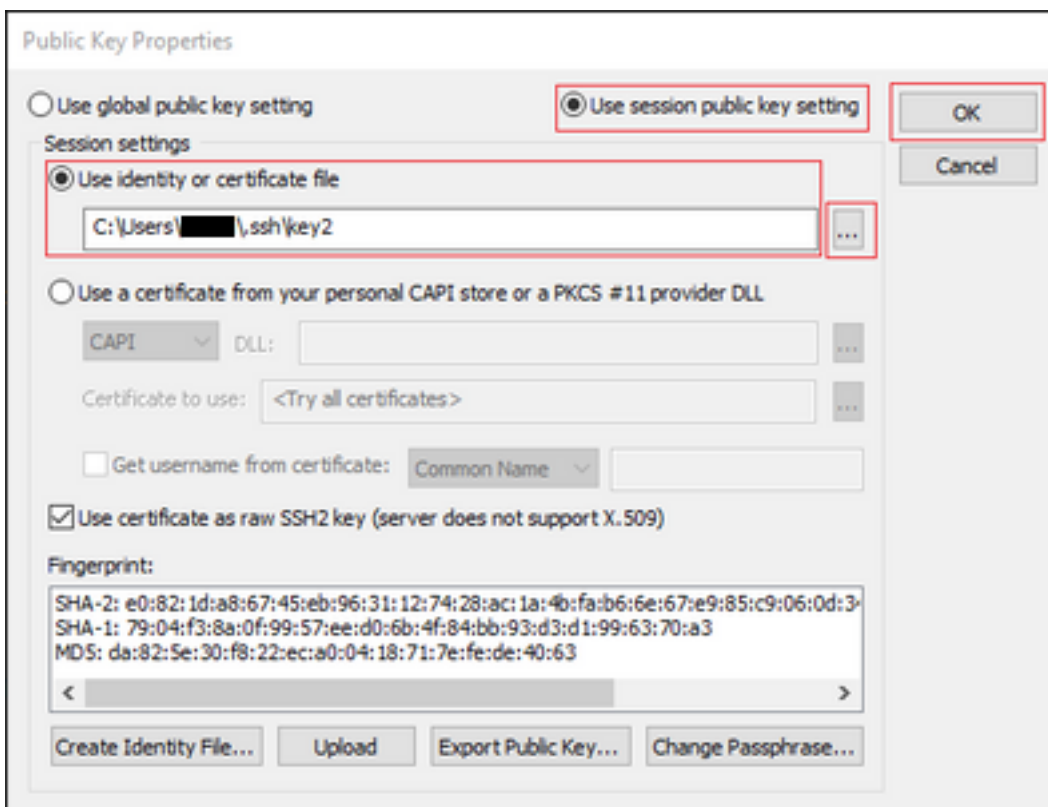
Specificeer in SecureCRT het pad naar de privé-toets in het menu:

Bestand > Quick Connect > Verificatie > Wachtwoord voor uitschakelen > Openbare sleutel > Eigenschappen.

De afbeelding toont het verwachte venster:



Selecteer **Use sessie public key string** > Select **Use Identity of certificate file** > Select ... toets > Navigeren in naar de folder en selecteer de gewenste toets > Select **OK** zoals getoond in de afbeelding.



Sluit tot slot aan op het externe IP-adres van de instantie via SSH zoals in de afbeelding.

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

Opmerking: Gebruikersnaam/wachtwoord die is gedefinieerd in de gegenereerde SSH-toetsen wordt gevraagd in te loggen.

```
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#

Aanvullende VM-inlogmethoden

Opmerking: Raadpleeg [Connect met Linux VMs met behulp van geavanceerde methodologische documentatie](#).

Geef extra gebruikers toestemming om in te loggen op CSR1000v/C800v in GCP

Na inloggen op de instantie CSR1000v is geslaagd, is het mogelijk om extra gebruikers met deze methoden te configureren:

Een nieuwe gebruikersnaam/wachtwoord configureren

Gebruik deze opdrachten om een nieuwe gebruiker en een nieuw wachtwoord te configureren:

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

Voorbeeld:

```
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#
```

Een nieuwe gebruiker kan nu inloggen bij de instantie CSR1000v/C8000v.

Een nieuwe gebruiker met SSH-toets configureren

Configureer de openbare sleutel om toegang tot de instantie CSR1000v te krijgen. SSH-toetsen in de metagegevens bieden geen toegang tot CSR1000v.

Gebruik deze opdrachten om een nieuwe gebruiker met een SSH-toets te configureren:

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

Opmerking: De maximum lijnlengte bij Cisco CLI is 254 tekens zodat de key string mogelijk niet past bij deze beperking, is het handig om de key string te wikkelen om een terminale lijn te gebruiken. De details over het overwinnen van deze beperking worden uitgelegd in [Generate an Instance SSH Key om CSR1000v te implementeren in Google Cloud Platform](#)

```
$ fold -b -w 72 /mnt/c/Users/ricneri/.ssh/key2.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDldzZ/iJi3VeHs4qDoxOP67jebaGwC6vkC
n29bwSQ4CPJGVRLcVSNPcPPqVydiXVEOG8e9gFszkpk6c2meO+TRsSLiwHigv28lyw5xhn1U
ck/AYpy9E6TyEEu9w6Fz0xTG2Qhe1n9b5Les6K9PFP/mR6WUMbfmaFredV/sADnODPO+OfTK
/OZPg34DNfcFhglja5GzudRb3S4nBBhDzuVrVC9RbA4PHVMXrLbIfqlks3PCVGOtW1HxxTU4
FckmEAg4NEqMVLsm26nLvrNK6z71RmcIKZzCST+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
AAAAB3NzaC1yc2EAAAADAQABAAQDldzZ/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/OZPg34DNfcFhglja5GzudRb3S4nBBhDzuVrVC9RbA4PHVMXrLbIfq1k
csr-cisco(conf-ssh-pubkey-
data)#s3PCVG0tW1HxxTU4FCkmEAg4NEqMVLsm26nLvrNK6z71RMcIKZZcST+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#
```

Controleer de ingestelde gebruikers op inloggen bij CSR1000v/C8000v

Om te bevestigen dat de configuratie juist is ingesteld, logt u in met de aangelegde geloofsbrieven of met het privé belangrijkste paar voor de openbare sleutel met de extra lichtgelovigen.

Van de routerkant, zie het succesvolle logbestand met het uiteindelijke IP-adres.

```
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#
```

Problemen oplossen

Als de foutmelding "Handeling ingesteld op out" wordt weergegeven.

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

Mogelijke oorzaken:

- De installatie is nog niet klaar.
- Het Openbaar adres is niet het adres dat is toegewezen aan nic0 in de VM.

Oplossing:

Wacht tot de VM-implementatie voltooid is. Gewoonlijk duurt een CSR1000v-implementatie tot 5 minuten om te voltooien.

Als een wachtwoord vereist is

Als er een wachtwoord is vereist:

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

Password:

Password:

Mogelijke oorzaak:

- De gebruikersnaam of privé-toets is onjuist.

Oplossing:

- Zorg ervoor dat de gebruikersnaam dezelfde is die is opgegeven toen CSR1000v/C8000v werd ingezet.
- Zorg ervoor dat de privé-toets hetzelfde is als u op de invoeringstijd hebt opgenomen.

Gerelateerde informatie

- [Cisco Cloud-services router 1000v dataplaat](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)