

# Google 클라우드 플랫폼에 CSR1000v/C8000v 구축

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[프로젝트 설정](#)

[1단계. 계정의 유효한 활성 프로젝트를 확인합니다.](#)

[2단계. 새 VPC 및 서브넷을 생성합니다.](#)

[3단계. 가상 인스턴스 구축.](#)

[구축 확인](#)

[새 인스턴스에 원격으로 연결](#)

[Bash 터미널을 사용하여 CSR1000v/C8000v에 로그인](#)

[PuTTY를 사용하여 CSR1000v/C8000v에 로그인](#)

[SecureCRT를 사용하여 CSR1000v/C8000V에 로그인](#)

[추가 VM 로그인 방법](#)

[추가 사용자가 GCP의 CSR1000v/C8000v에 로그인하도록 권한 부여](#)

[새 사용자 이름/비밀번호 구성](#)

[SSH 키를 사용하여 새 사용자 구성](#)

[CSR1000v/C8000v에 로그인할 때 구성된 사용자 확인](#)

[문제 해결](#)

["Operation timed out" 오류 메시지가 표시되는 경우](#)

[암호가 필요한 경우](#)

[관련 정보](#)

## 소개

이 문서에서는 GCP(Google Cloud Platform)에서 Cisco Cloud Services Router 1000v(CSR1000v) 및 Catalyst 8000v(C800v) Edge Router를 구축하고 구성하는 절차에 대해 설명합니다.

기고자: Eric Garcia, Ricardo Neri, Cisco TAC 엔지니어

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 가상화 기술/가상 머신(VM)
- 클라우드 플랫폼

## 사용되는 구성 요소

- 프로젝트가 생성된 Google Cloud Platform에 대한 활성 서브스크립션
- GCP 콘솔
- GCP 마켓플레이스
- Bash 터미널, Putty 또는 SecureCRT
- 공개 및 개인 SSH(Secure Shell) 키

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

## 배경 정보

17.4.1부터 CSR1000v는 SDWAN 및 DNA 라이선싱과 같은 새로운 기능이 추가된 C8000v가 됩니다. 자세한 내용은 공식 제품 데이터시트를 확인하십시오.

[Cisco Cloud Services Router 1000v 데이터 시트](#)

[Cisco Catalyst 8000V Edge 소프트웨어 데이터 시트](#)

따라서 이 가이드는 CSR1000v 및 C8000v 라우터를 모두 설치하는 경우에 적용됩니다.

## 프로젝트 설정

**참고:** 이 문서가 작성되는 즉시 신규 사용자는 300USD의 무료 크레딧을 사용하여 1년 동안 프리 티어로 GCP를 완전히 살펴볼 수 있습니다. 이는 Google에서 정의하며 Cisco에서 관리하지 않습니다.

**참고:** 이 문서에서는 공용 및 개인 SSH 키를 생성해야 합니다. 자세한 내용은 [Google Cloud Platform에서 CSR1000v를 구축하려면 인스턴스 SSH 키 생성을 참조하십시오.](#)

### 1단계. 계정의 유효한 활성 프로젝트를 확인합니다.

계정에 유효한 활성 프로젝트가 있는지 확인하십시오. 이 프로젝트는 Compute Engine에 대한 권한이 있는 그룹과 연결되어 있어야 합니다.

이 예제 구축에서는 GCP에서 생성된 프로젝트가 사용됩니다.

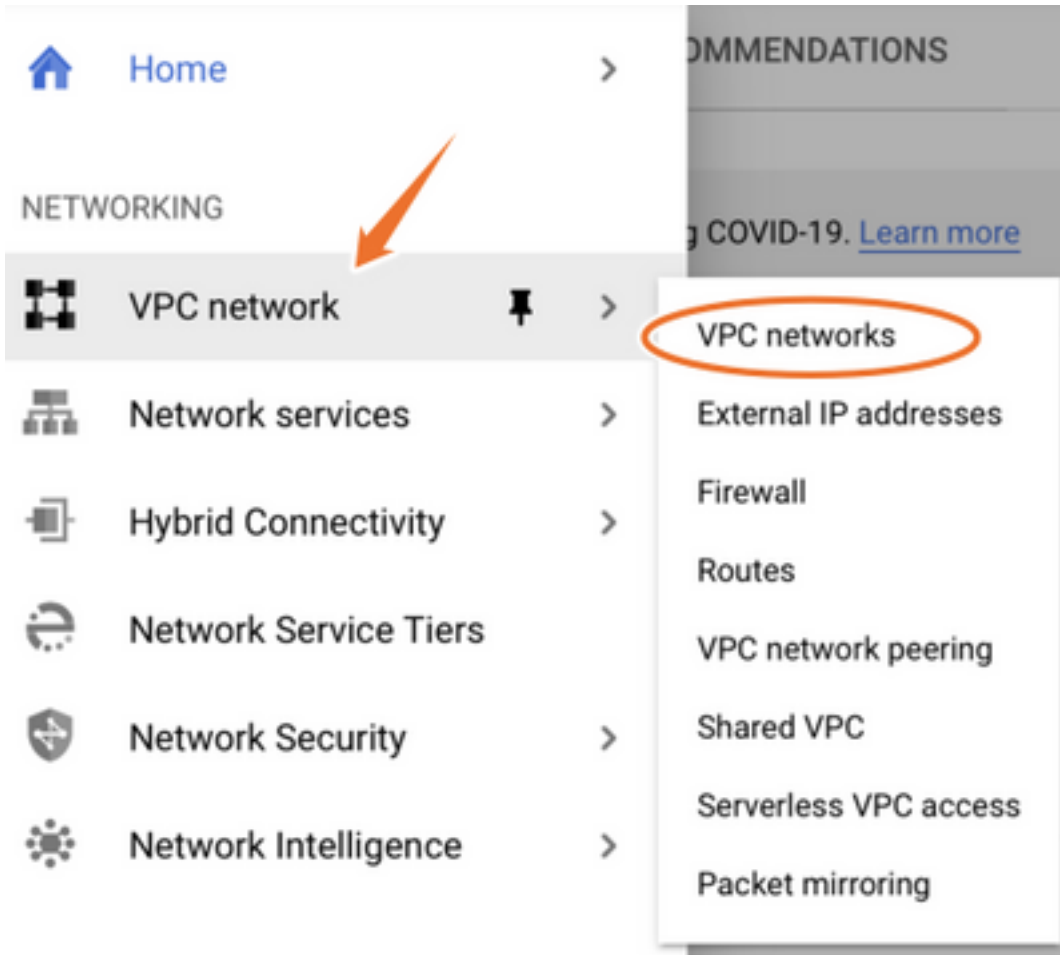
**참고:** 새 프로젝트를 만들려면 [프로젝트 만들기 및 관리](#)를 참조하십시오.

### 2단계. 새 VPC 및 서브넷을 생성합니다.

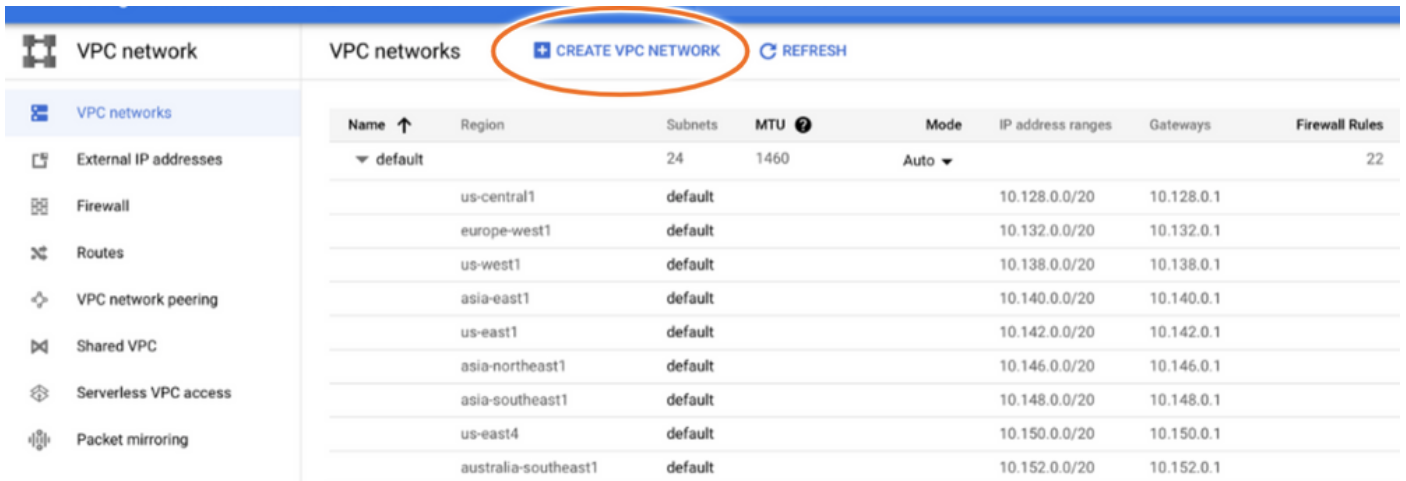
새 VPC(Virtual Private Cloud) 및 CSR1000v 인스턴스와 연결해야 하는 서브넷을 생성합니다.

기본 VPC 또는 이전에 생성한 VPC 및 서브넷을 사용할 수 있습니다.

콘솔 대시보드에서 이미지에 표시된 대로 VPC 네트워크 > VPC 네트워크를 선택합니다.



이미지에 표시된 대로 Create VPC Network를 선택합니다.



참고: 현재 CSR1000v는 GCP의 us-central 지역에만 구축됩니다.

이미지에 표시된 대로 VPC 이름을 구성합니다.

## ← Create a VPC network

Name \*

csr-vpc

Lowercase letters, numbers, hyphens allowed

Description

VPC와 연결된 서브넷 이름을 구성하고 region us-**central1**을 선택합니다.

이미지에 표시된 대로 us-central1 CIDR 10.128.0.0/20에 유효한 IP 주소 범위를 할당합니다.

다른 설정을 기본값으로 유지하고 **만들기** 단추를 선택합니다.

### 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

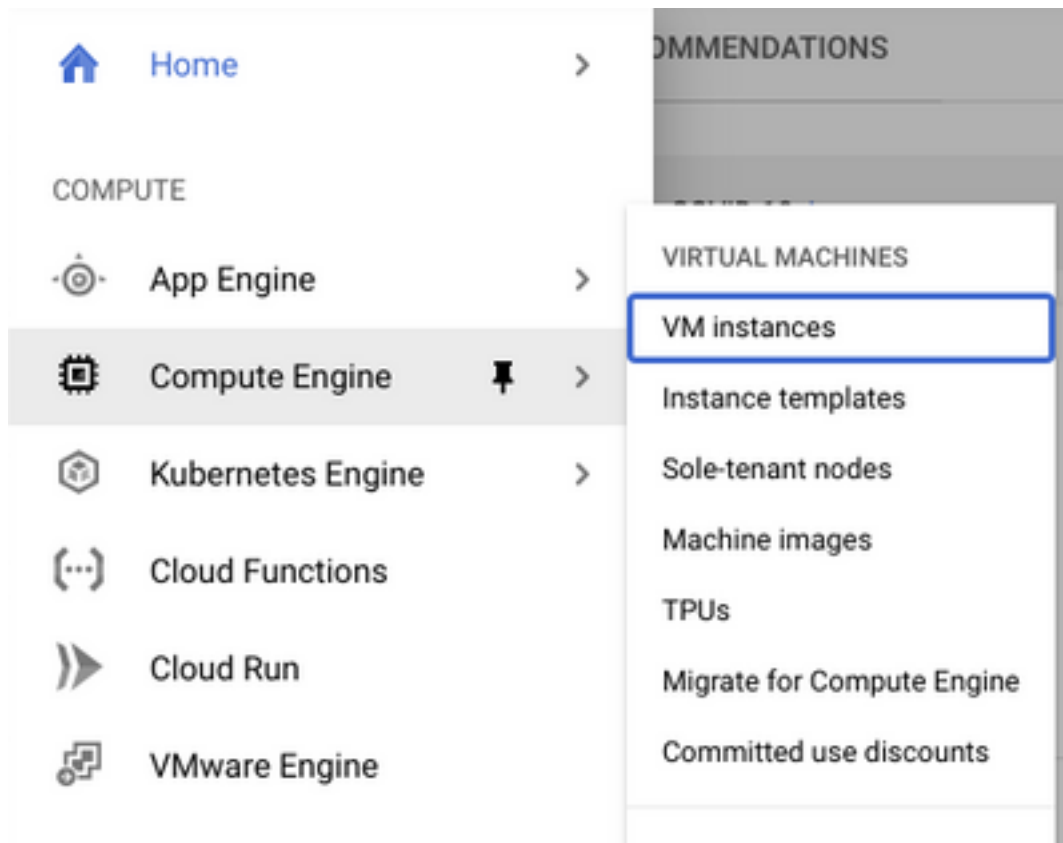
**참고:** "automatic"을 선택하면 GCP는 영역 CIDR 내에서 자동 유효 범위를 할당합니다.

생성 프로세스가 완료되면 이미지에 표시된 대로 새 VPC가 **VPC 네트워크** 섹션에 나타납니다.

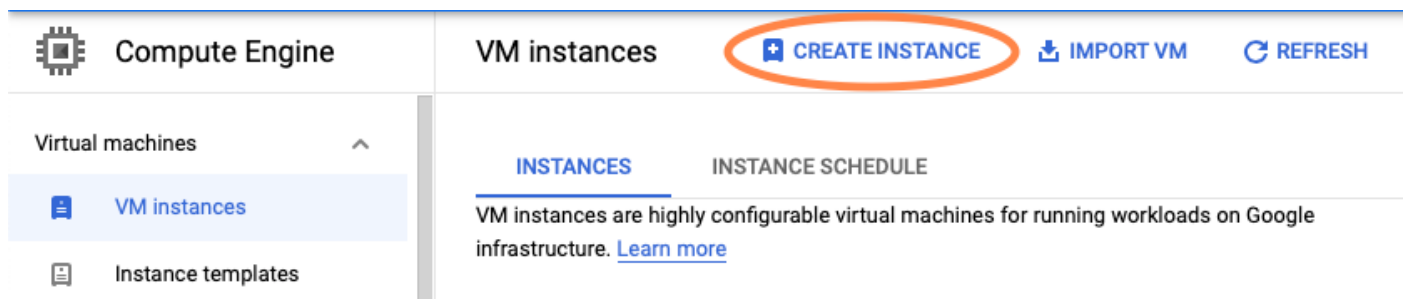
Name ↑	Region	Subnets	MTU ?	Mode	IP address ranges	Gateways
▼ csr-vpc		1	1460	Custom		
	us-central1	csr-subnet			<u>10.10.1.0/24</u>	<u>10.10.1.1</u>

### 3단계. 가상 인스턴스 구축.

Compute Engine 섹션에서 이미지에 표시된 대로 **Compute Engine > VM 인스턴스**를 선택합니다.



VM 대시보드에서, 이미지에 표시된 대로 **Create Instance** 탭을 선택합니다.



이미지에 표시된 대로 GCP 마켓플레이스를 사용하여 Cisco 제품을 표시합니다.

## ← 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

검색 표시줄에서 **Cisco CSR** 또는 **Catalyst C8000v**를 입력하고 요구 사항에 맞는 모델 및 버전을 선택하고 **Launch**를 선택합니다.

이 예제 구축에서 첫 번째 옵션은 이미지에 표시된 대로 선택되었습니다.

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

Marketplace &gt; "catalyst 8000v edge software - byol" &gt; Virtual machines

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

**참고:** BYOL은 "Bring Your Own License"를 의미합니다.

**참고:** 현재 GCP는 PAYG(Pay As You Go) 모델을 지원하지 않습니다.

GCP는 이미지에 표시된 대로 VM과 연결해야 하는 컨피그레이션 값을 입력해야 합니다.

이미지에 표시된 대로 GCP에서 CSR1000v/C8000v를 구축하려면 사용자 이름 및 SSH 공개 키가 필요합니다. SSH 키가 [생성되지](#) 않은 경우 [Google Cloud Platform에서 CSR1000v를 구축하려면 인스턴스 SSH 키 생성](#)을 참조하십시오.





## 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 ?

이전에 생성된 VPC 및 서브넷을 선택하고 외부 IP에서 Ephemeral을 선택하여 이미지에 표시된 대로 인스턴스와 연결된 Public IP를 설정합니다.

이 구성 후 시작 버튼을 선택합니다.

## 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

**참고:** SSH를 통해 CSR 인스턴스에 연결하려면 포트 22가 필요합니다. HTTP 포트는 선택 사항입니다.

구축이 완료되면 이미지에 표시된 대로 새 CSR1000v가 성공적으로 구축되었는지 확인하려면 **Compute Engine > VM 인스턴스**를 선택합니다.

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)	<span style="background-color: black; color: black;">[REDACTED]</span>	SSH ▾ ⋮

## 구축 확인

### 새 인스턴스에 원격으로 연결

GCP에서 CSR1000v/C8000V에 로그인하는 가장 일반적인 방법은 Bash 터미널, Putty 및 SecureCRT의 명령줄입니다. 이 섹션에서는 이전 방법과 연결하는 데 필요한 컨피그레이션을 제공합니다.

### Bash 터미널을 사용하여 CSR1000v/C8000v에 로그인

새 CSR에 원격으로 연결하는 데 필요한 구문은 다음과 같습니다.

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

예:

```
$ 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.
```

연결에 성공하면 CSR1000v 프롬프트가 표시됩니다.

```
$ 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
```

## PuTTY를 사용하여 CSR1000v/C8000v에 로그인

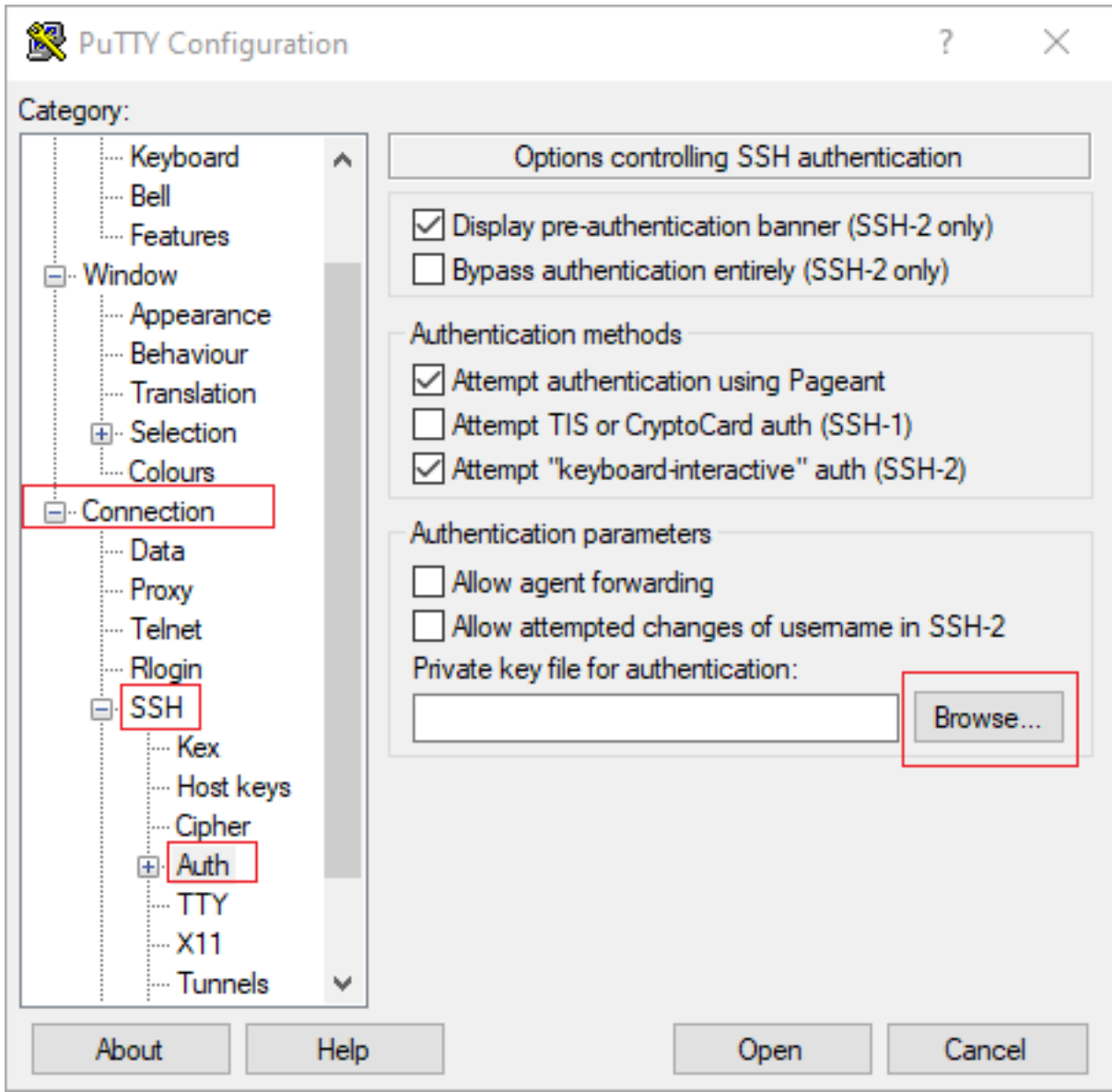
Putty에 연결하려면 PuTTYgen 응용 프로그램을 사용하여 개인 키를 PEM에서 PPK 형식으로 변환합니다.

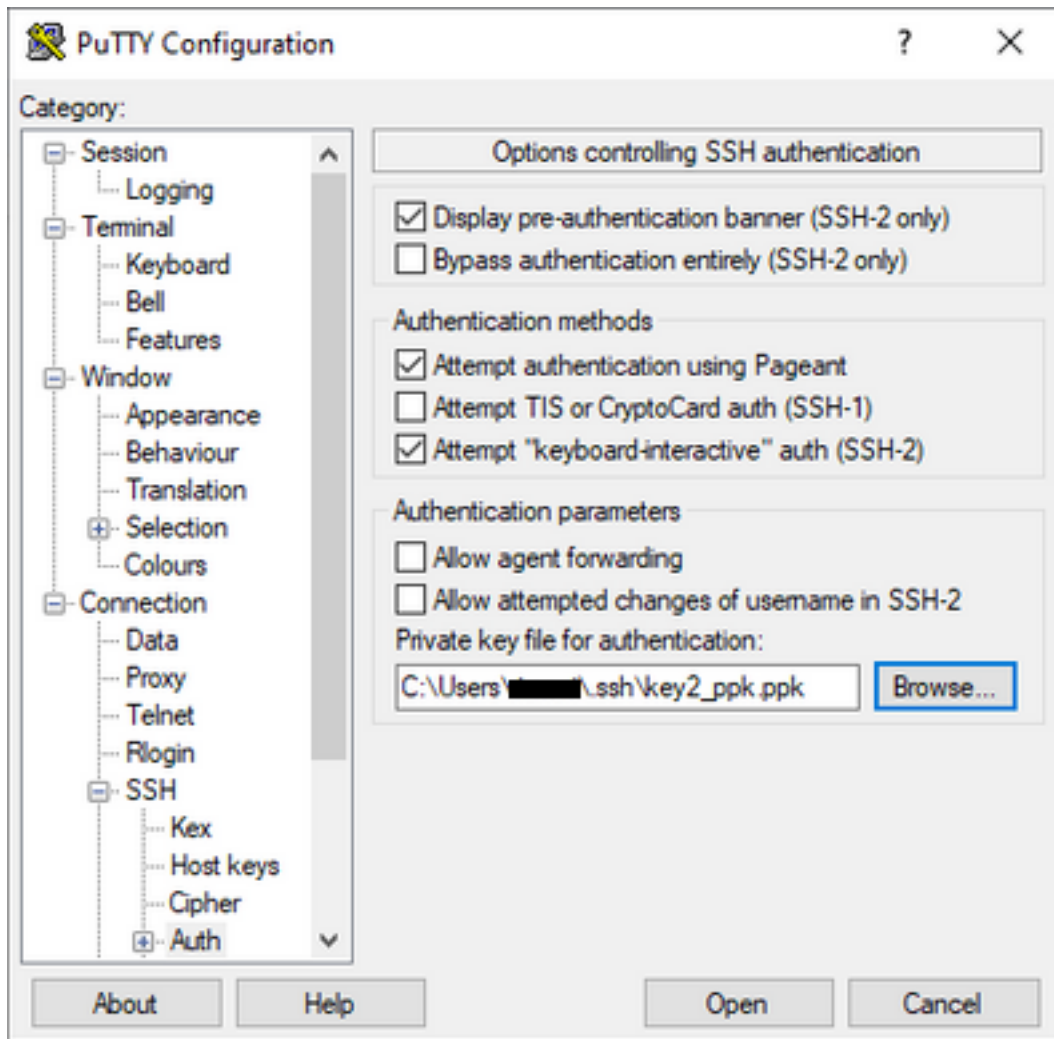
자세한 내용은 [PuTTYgen을 사용하여 Pem을 Ppk 파일로 변환](#)을 참조하십시오.

개인 키가 올바른 형식으로 생성되면 Putty에서 경로를 지정해야 합니다.

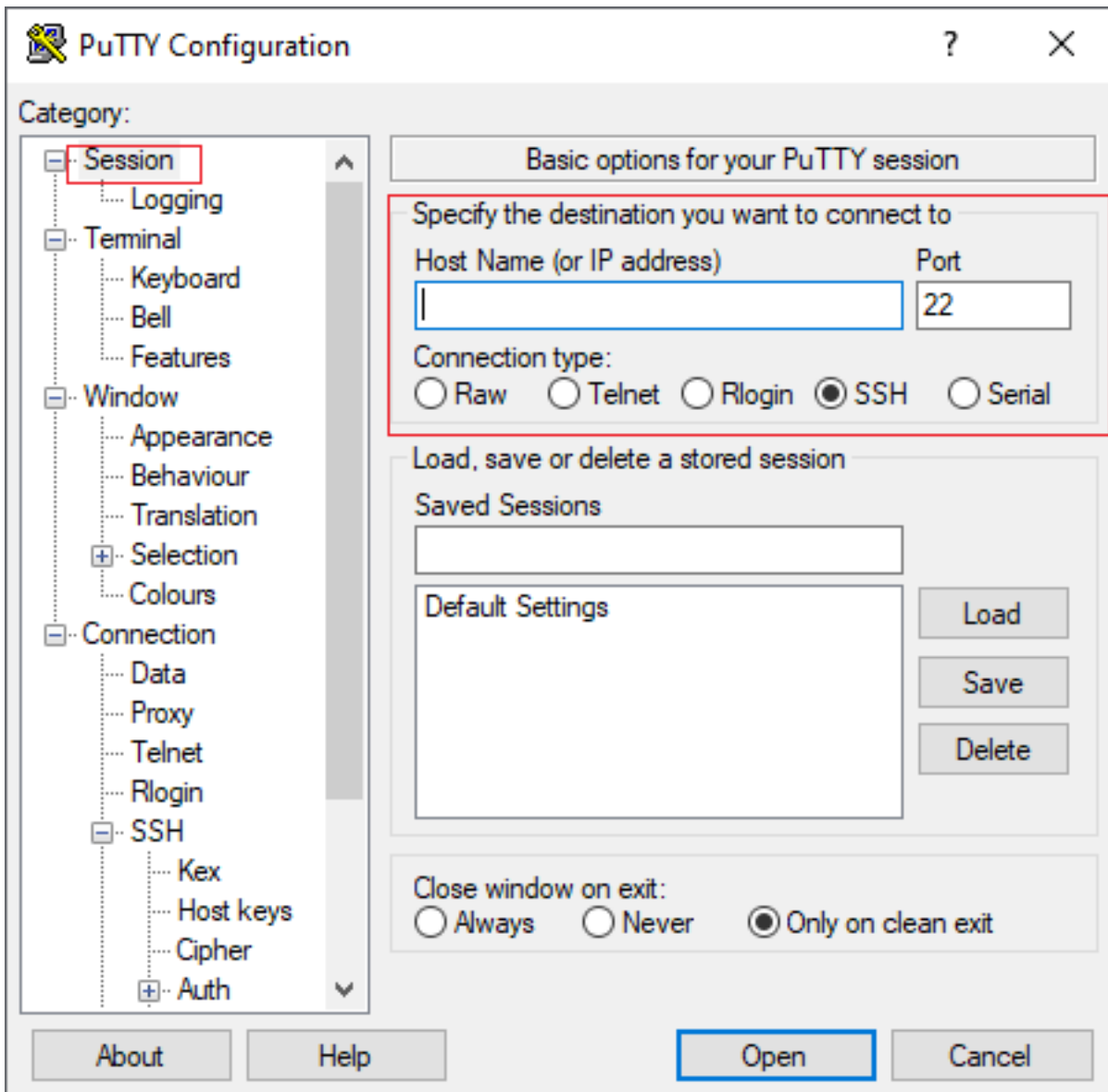
SSH 연결 메뉴의 auth 옵션에서 **Private key file for authentication(인증을 위한 개인 키 파일)**을 선택합니다.

키가 저장된 폴더를 찾아 만든 키를 선택합니다. 이 예에서 이미지는 Putty 메뉴의 그래픽 보기 및 원하는 상태를 보여줍니다.





적절한 키를 선택한 후 주 메뉴로 돌아가 이미지에 표시된 대로 CSR1000v 인스턴스의 외부 IP 주소를 사용하여 SSH를 통해 연결합니다.



**참고:** 생성된 SSH 키에 정의된 사용자 이름/비밀번호가 로그인을 요청합니다.

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

```
csr-cisco#
```

## SecureCRT를 사용하여 CSR1000v/C8000V에 로그인

SecureCRT에는 개인 키의 기본 형식인 PEM 형식의 개인 키가 필요합니다.

SecureCRT에서 메뉴의 개인 키에 대한 경로를 지정합니다.

**파일 > 빠른 연결 > 인증 > 암호 선택 취소 > 공개 키 > 등록 정보.**

이 그림에서는 예상 창을 보여 줍니다.

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

Use **session public key string**(세션 공개 키 문자열 사용) > Select **Use identity or certificate file**(ID 또는 인증서 파일 사용) > Select ...button > Select ...(선택...) 디렉토리를 선택하고 원하는 키를 선택한 다음 이미지에 표시된 대로 Select **OK**(확인 선택)를 선택합니다.

Public Key Properties

Use global public key setting  Use session public key setting

Session settings

- Use identity or certificate file
- Use a certificate from your personal CAPI store or a PKCS #11 provider DLL

C:\Users\...\.ssh\key2

OK

Cancel

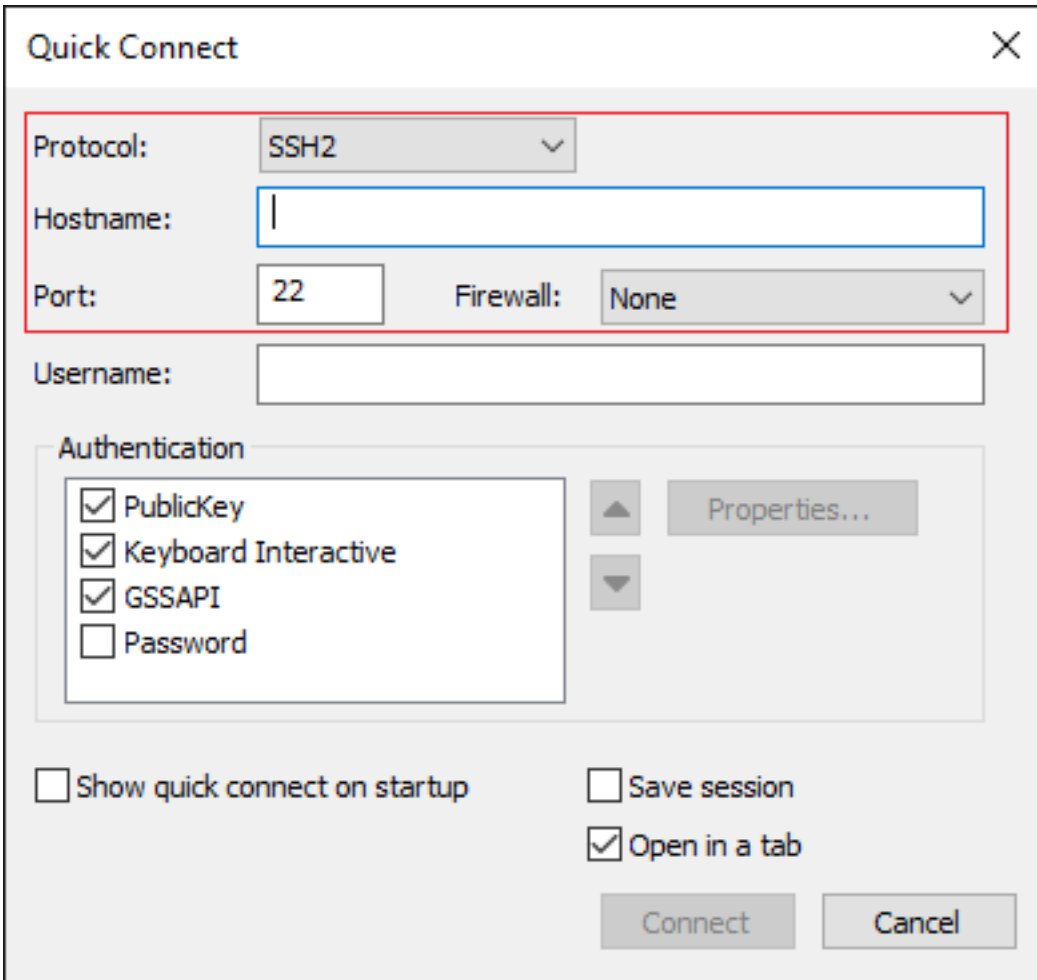
Use certificate as raw SSH2 key (server does not support X.509)

Fingerprint:

SHA-2: e0:82:1d:a8:67:45:eb:96:31:12:74:28:ac:1a:4b:fa:b6:6e:67:e9:85:c9:06:0d:3  
 SHA-1: 79:04:f3:8a:0f:99:57:ee:d0:6b:4f:84:bb:93:d3:d1:99:63:70:a3  
 MD5: da:82:5e:30:f8:22:ec:a0:04:18:71:7e:fe:de:40:63

Create Identity File... Upload Export Public Key... Change Passphrase...

마지막으로, 이미지에 표시된 대로 SSH를 통해 인스턴스의 외부 IP 주소에 연결합니다.



**참고:** 생성된 SSH 키에 정의된 사용자 이름/비밀번호가 로그인을 요청합니다.

```
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#
```

## 추가 VM 로그인 방법

**참고:** 자세한 내용은 [Linux VM에 연결 고급 방법](#) 설명서를 참조하십시오.

## 추가 사용자가 GCP의 CSR1000v/C8000v에 로그인하도록 권한 부여

CSR1000v 인스턴스에 로그인하면 다음 방법으로 추가 사용자를 구성할 수 있습니다.

### 새 사용자 이름/비밀번호 구성

다음 명령을 사용하여 새 사용자 및 비밀번호를 구성합니다.



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

예:

```
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#
```

이제 새 사용자가 CSR1000v/C8000v 인스턴스에 로그인할 수 있습니다.

## SSH 키를 사용하여 새 사용자 구성

CSR1000v 인스턴스에 액세스하려면 공개 키를 구성합니다. 인스턴스 메타데이터의 SSH 키는 CSR1000v에 대한 액세스를 제공하지 않습니다.

다음 명령을 사용하여 SSH 키로 새 사용자를 구성합니다.

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

**참고:** Cisco CLI의 최대 줄 길이는 254자입니다. 따라서 키 문자열이 이 제한에 맞지 않을 수 있습니다. 키 문자열을 터미널 라인에 맞게 래핑하는 것이 편리합니다. 이 제한을 극복하는 방법에 대한 자세한 내용은 [Google Cloud Platform에서 CSR1000v를 구축하기 위한 인스턴스 SSH 키 생성에서 설명합니다.](#)

```
$ fold -b -w 72 /mnt/c/Users/ricneri/.ssh/key2.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDldzZ/iJi3VeHs4qDoxOP67jebaGwC6vkC
n29bwsQ4CPJGVRLcVSNPcPPqVydiXVEOG8e9gFszkpk6c2meO+TRsSLiwHigv28lyw5xhn1U
ck/AYpy9E6TyEEu9w6Fz0xTG2Qheln9b5Les6K9PFP/mR6WUMbfmaFredV/sADnODPO+OfTK
/OZPg34DNfcFhglja5GzudRb3S4nBBhDzuVrVC9RbA4PHVMXrLbIfq1ks3PCVGotW1HxxTU4
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
AAAAB3NzaC1yc2EAAAADAQABAAQDldzZ/iJi3VeHs4qDoxOP67jebaGwC
csr-cisco(conf-ssh-pubkey-
data)#6vkCn29bwsQ4CPJGVRLcVSNPcPPqVydiXVEOG8e9gFszkpk6c2meO+TRsSLiwHigv28l
```

```
csr-cisco(conf-ssh-pubkey-
data)#yw5xhnlUck/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#
```

## CSR1000v/C8000v에 로그인할 때 구성된 사용자 확인

컨피그레이션이 제대로 설정되었는지 확인하려면 생성된 자격 증명으로 또는 추가 자격 증명으로 공개 키에 대한 개인 키 쌍으로 로그인하십시오.

라우터 측에서 터미널 IP 주소로 성공 로그인 로그를 참조하십시오.

```
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#
```

## 문제 해결

### "Operation timed out" 오류 메시지가 표시되는 경우

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

가능한 원인:

- 인스턴스가 배포를 완료하지 않았습니다.
- 공용 주소는 VM의 nic0에 할당된 주소가 아닙니다.

해결책:

VM 구축이 완료될 때까지 기다립니다. 일반적으로 CSR1000v 구축은 완료하는 데 최대 5분이 소요됩니다.

### 암호가 필요한 경우

비밀번호가 필요한 경우:

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

Password:

Password:

가능한 원인:

- 사용자 이름 또는 개인 키가 잘못되었습니다.

해결책:

- 사용자 이름이 CSR1000v/C8000v를 구축할 때 지정된 것과 동일한지 확인합니다.
- 프라이빗 키가 구축 시 포함했던 것과 동일한지 확인합니다.

## 관련 정보

- [Cisco Cloud Services Router 1000v 데이터 시트](#)
- [기술 지원 및 문서 - Cisco Systems](#)