AWS와 GCP 간 HA VPN 연결 구성

lswoo@mz.co.kr

Google | MEGAZONE CLOUD

Configuration step

관련 Document:
Google Cloud와 AWS 사이에 HA VPN 연결 빌드 | 클라우드 아키텍처 센터

1. Topology

2. HA VPN gateway 및 Cloud Router 생성

3. AWS virtual private gateways 생성

4. AWS site-to-site VPN connections 과 customer gateways 생성

5. AWS configuration files 다운로드

6. HA VPN gateway에 VPN tunnel 생성

7. 다운로드받은 AWS configuration file의 BGP IP 사용하여 Cloud Router에 BGP session 설정

0. 기본 VPN gateway 지원 중단

지원 중단된 구성

2021년 10월 31일부터는 다음 작업을 더 이상 수행할 수 없습니다.

- 정적 라우팅 (경로 기반 또는 정책 기반)을 사용하여 다른 기본 VPN 게이트웨이에 *연결*하는 기본 VPN 터널을 만듭니다.
- 정적 라우팅 (경로 기반 또는 정책 기반)을 사용하여 Google Cloud Virtual Private Cloud (VPC) 네트워크를 다른 클라우드 제공업체의 네트워크에 연결하는 기본 VPN 터널을 만듭니다.
- 동적 라우팅 (모든 구성)을 사용하여 새로운 기본 VPN 터널을 만듭니다.

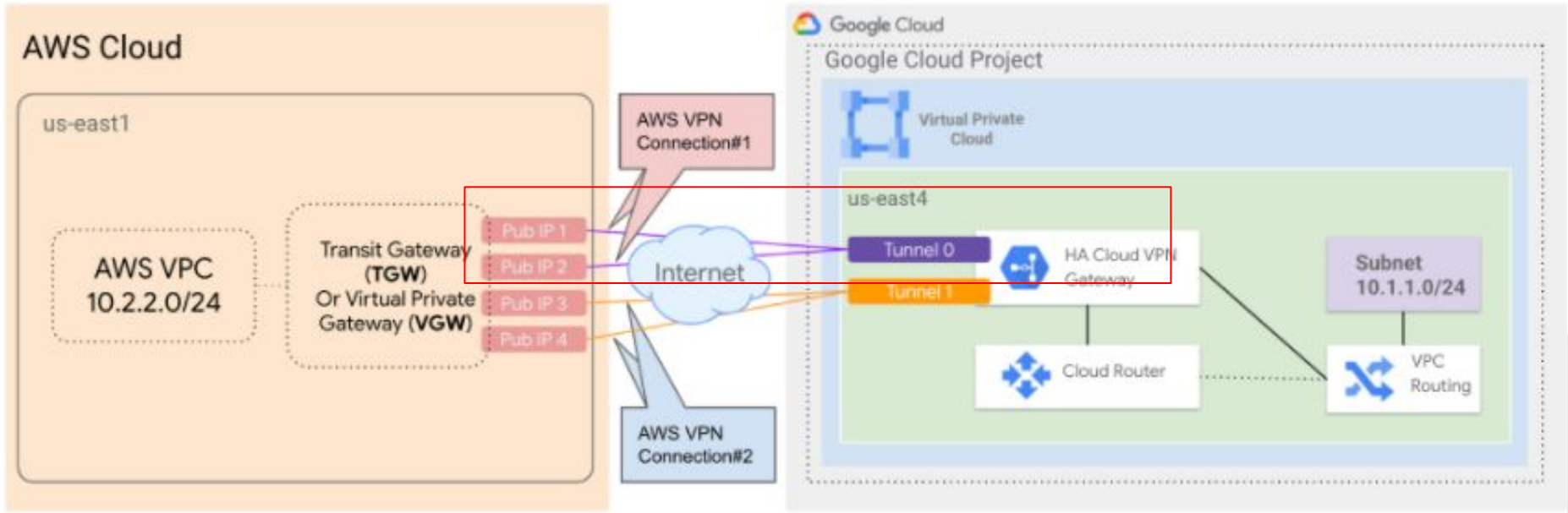
2021년 10월 31일부터 기본 VPN 게이트웨이를 사용한 Static routing은 지원 중단될 예정

-> Static routing VPN은 HA VPN 게이트웨이를 사용한 **Dynamic routing으로 변경**해야 함

지원 가능한 시나리오

- 1개의 AWS Gateway에서 나온 2개의 터널에서 1개의 HA VPN Gateway NIC에 연결
- 다른 하나의 AWS Gateway에서 나온 2개의 터널에서 나머지 1개의 HA VPN Gateway NIC에 연결
  ->
  총 2개의 AWS Gateway, 4개의 터널 지원 가능

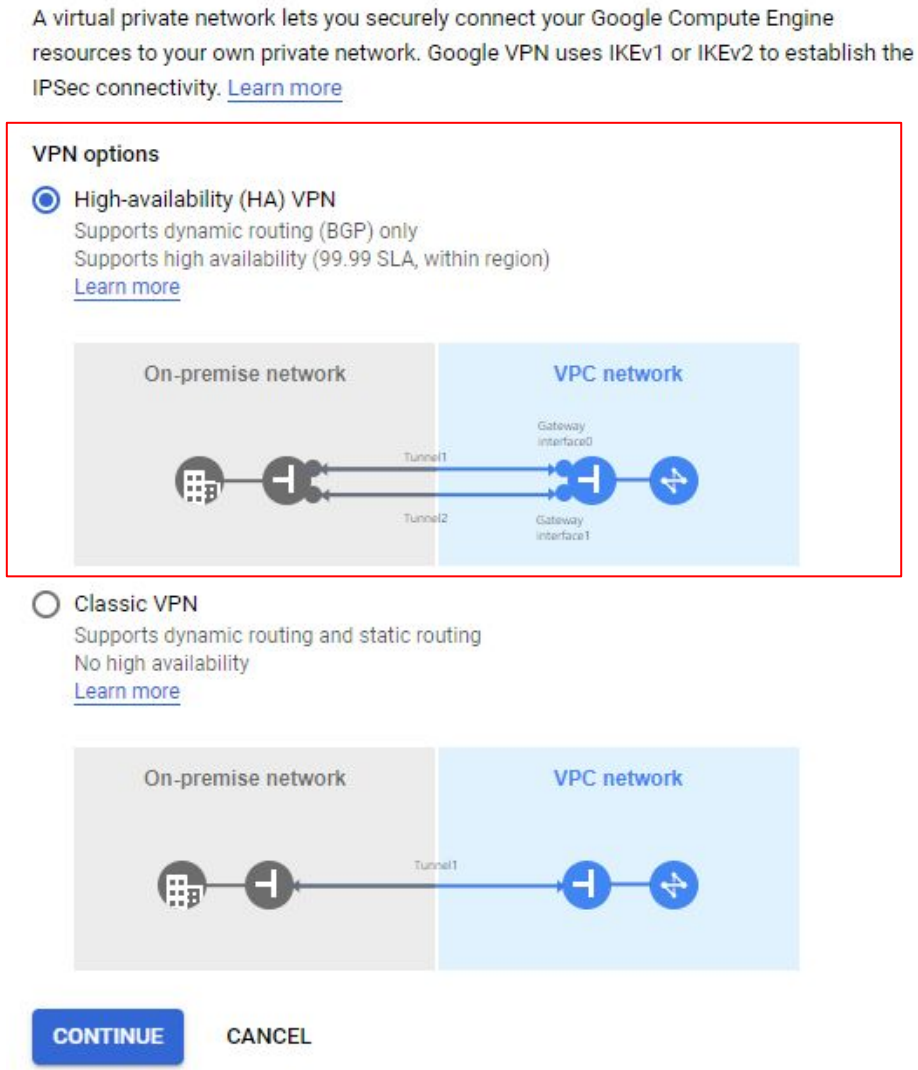
1. Topology



본 슬라이드에는 1개 Gateway, 2개 터널을 연결한 구성을 예제로 함.

상황에 따라 추가적인 Gateway 구성 가능

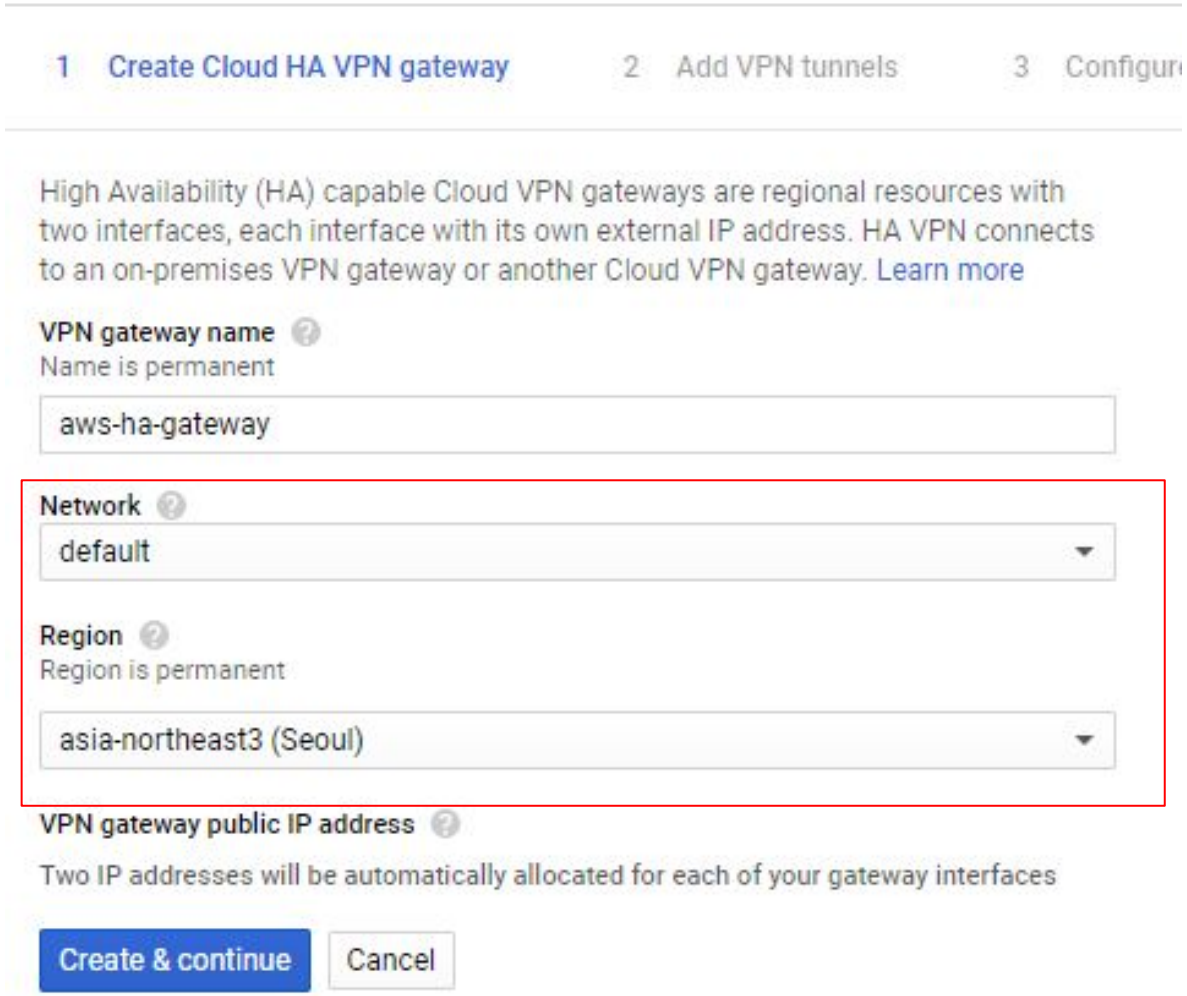
2. HA VPN gateway 및 Cloud Router 생성



High-availability (HA) VPN 선택

(Classic VPN의 static routing은 지원 중단)

2. HA VPN gateway 및 Cloud Router 생성

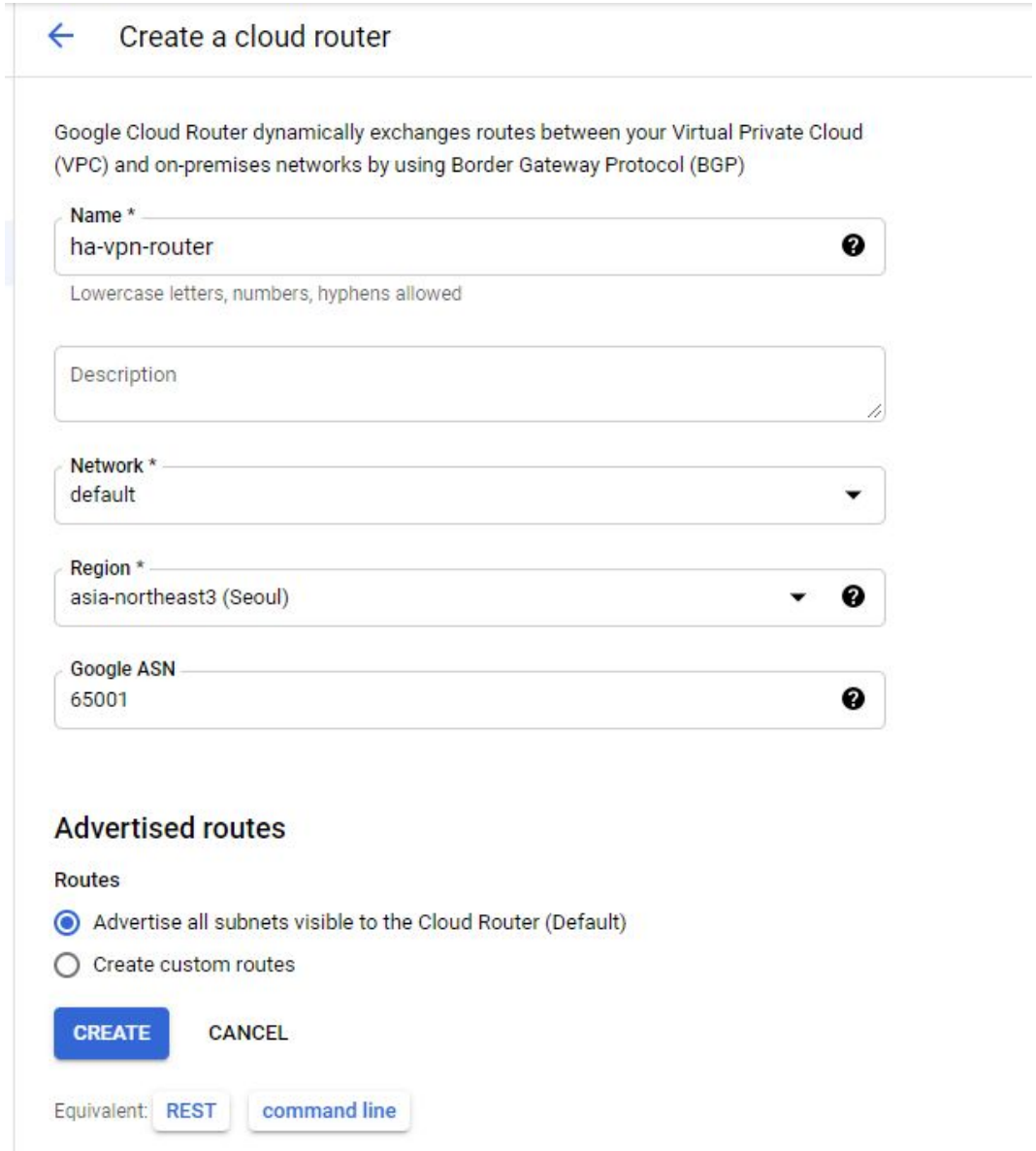


Cloud VPN Gateway 생성

Network : VPN을 구성할 VPN Network 선택

Region : VPN을 구성할 Region 선택

2. HA VPN gateway 및 Cloud Router 생성



Cloud Router 생성

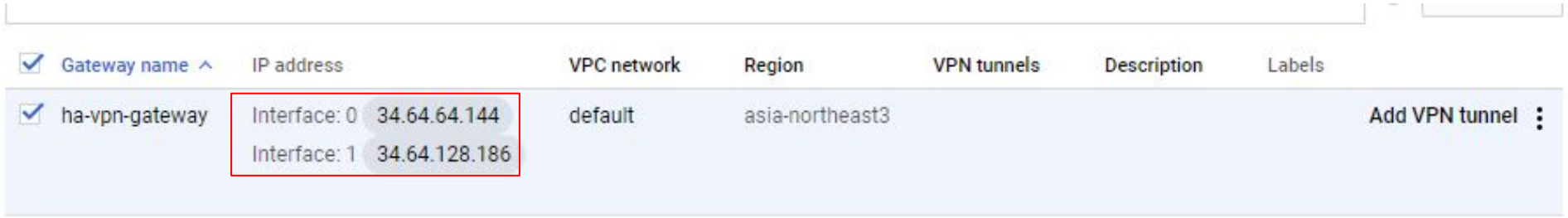
Network : Cloud Router를 생성할 VPC Network 선택, 이전과 동일

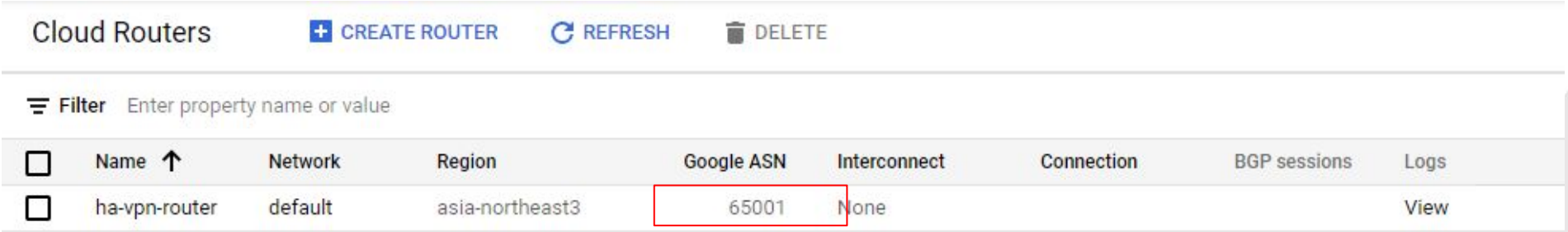
Region : Cloud Router를 생성할 Region 선택, 이전과 동일

Google ASN : ASN값 지정,
64512 - 65534, 4200000000 - 4294967294 중 선택

Routes : Default값 선택

2. HA VPN gateway 및 Cloud Router 생성





생성 후

1. HA Gateway의 Public IP address 2개
2. Cloud Router의 ASN

2가지 정보를 AWS 측에 넘겨준다.

3. AWS 리소스 생성

1. AWS측에서 Virtual private gateway 생성
   -> GCP Cloud Router와 **겹치지 않는** ASN을 지정해 생성할 것

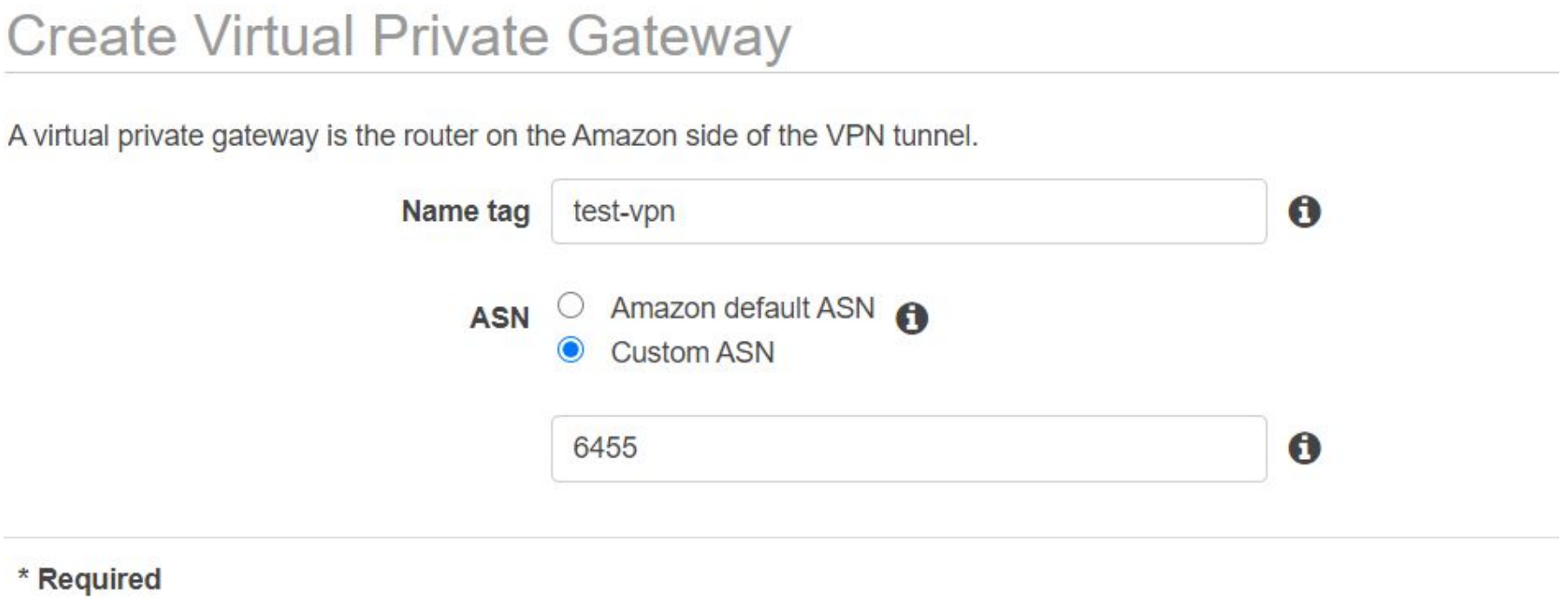
2. Customer gateway 생성
   -> IP address에 GCP HA Gateway의 IP address 중 하나 입력
   -> BGP ASN에 GCP Cloud Router의 ASN 입력

3. VPN Tunnel 생성
   ->IP range 자동으로 생성되도록 default로 생성

4. Virtual private gateway 하나 더 생성
   -> Customer gateway Ip를 GCP HA Gateway의 Ip address 중 남은 하나를 입력, 나머진 동일

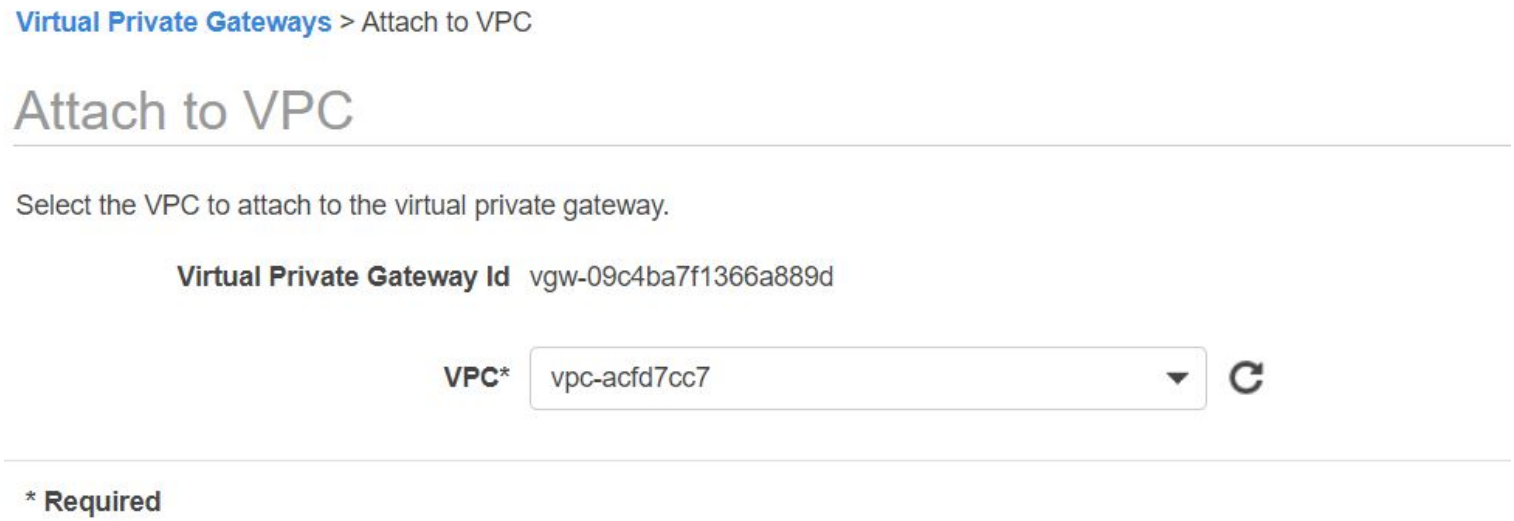
   ※ 생성을 마친 후 AWS configuration을 download받으면 GCP측에 편하게 정보를 제공할 수 있다.

3. AWS 리소스 생성



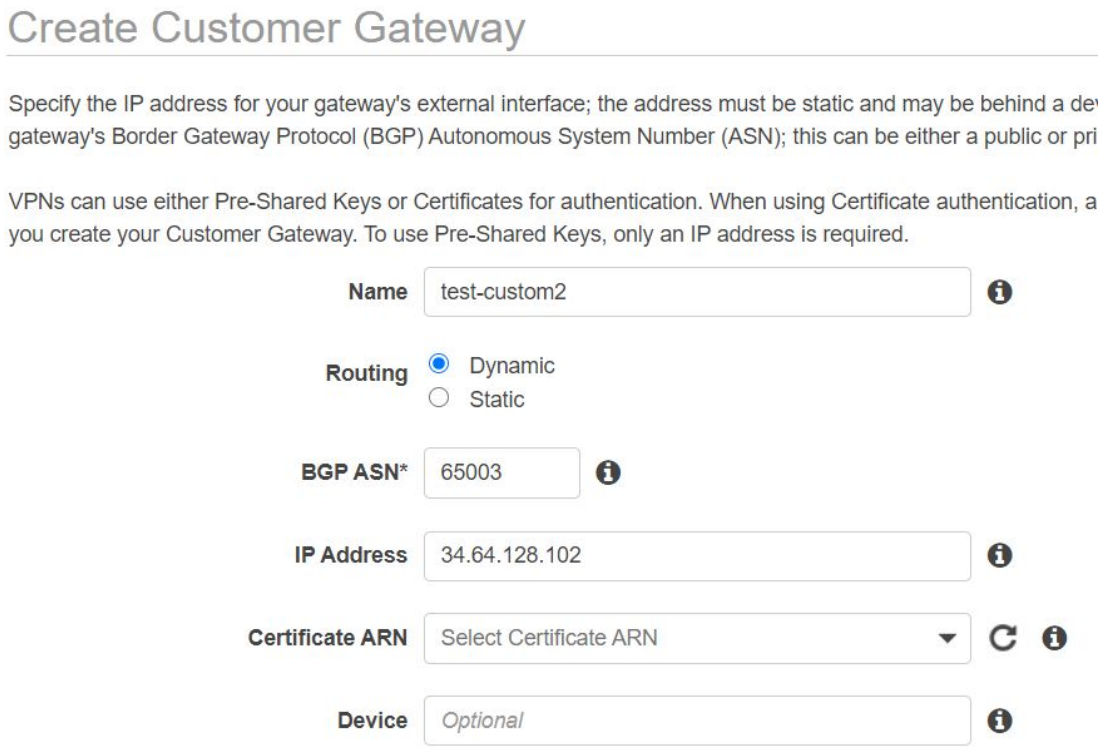
1. AWS측에서 Virtual private gateway 생성
   -> GCP Cloud Router와 **겹치지 않는** ASN을 지정해 생성할 것

3. AWS 리소스 생성



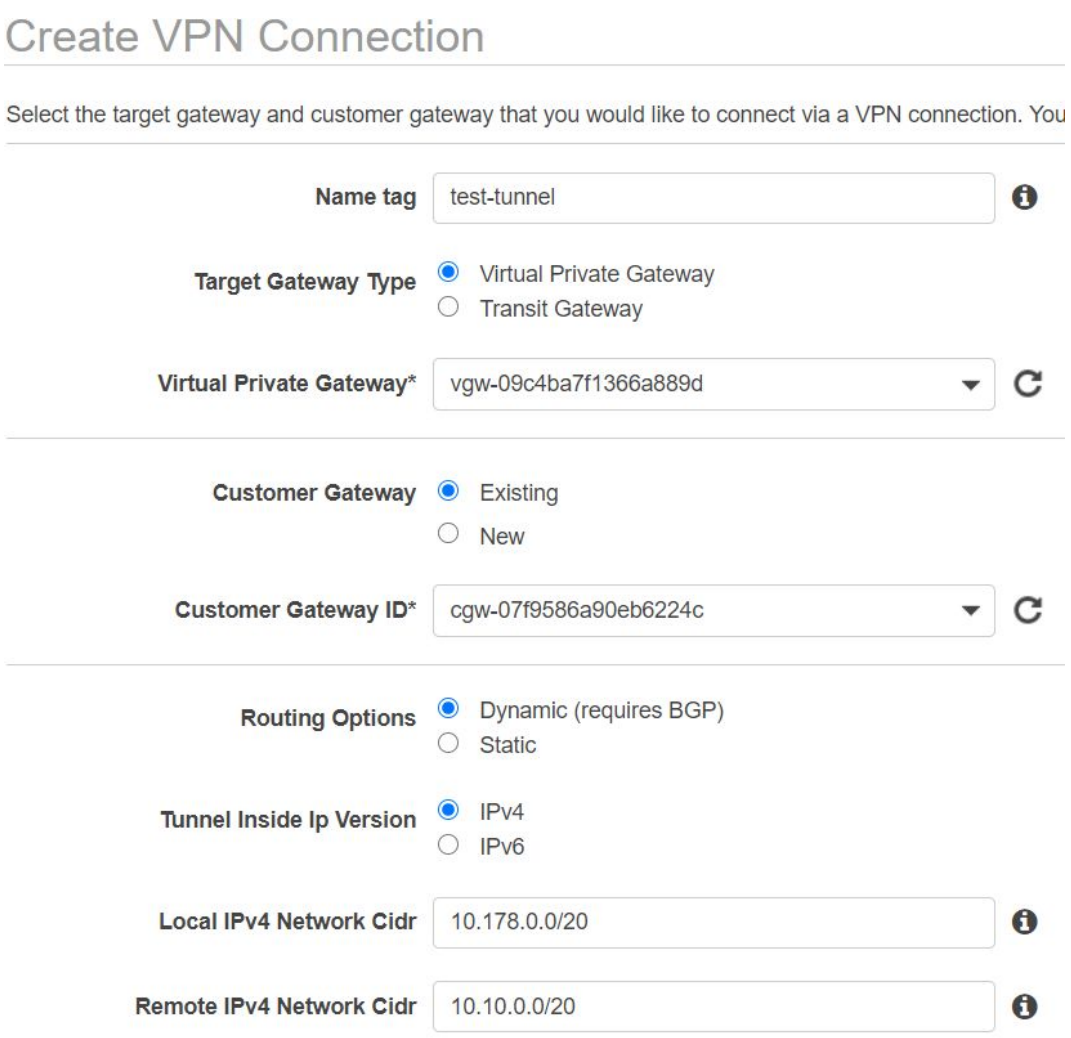
생성한 Virtual Private Gateways는 VPC에 attach한다.

3. AWS 리소스 생성



2. Customer gateway 생성
   -> IP address에 GCP HA Gateway의 IP address 중 하나 입력
   -> BGP ASN에 GCP Cloud Router의 ASN 입력

3. AWS 리소스 생성



3. VPN Tunnel 생성

Virtual Private Gateway : 생성한 Virtual Private Gateway 선택

Customer Gateway : 생성한 Customer Gateway 선택

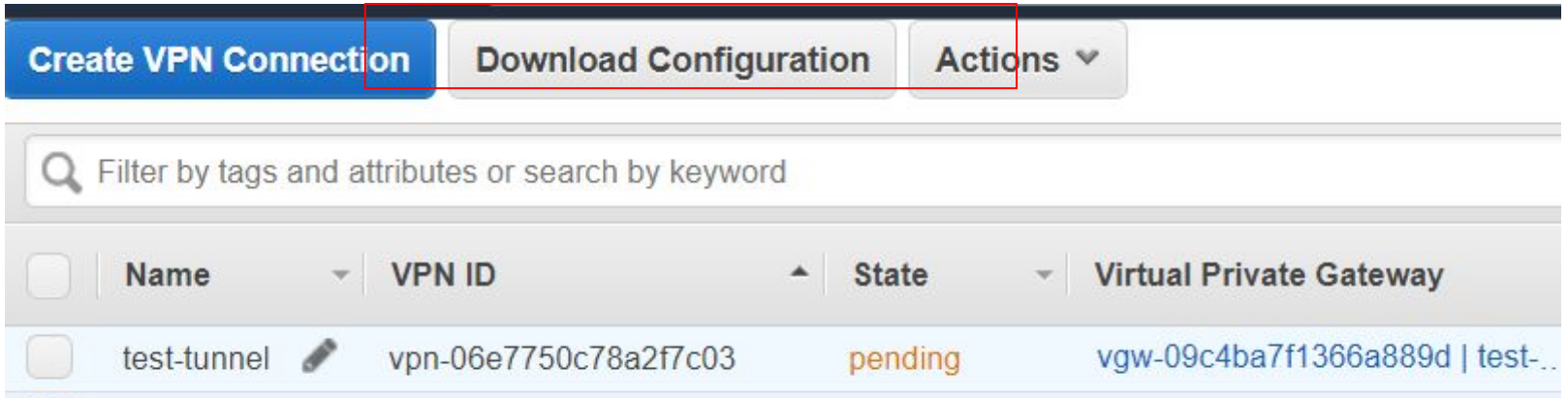
Routing Option : Dynamic

Local IPv4 Network Cidr : AWS측 VPC cidr

Remote IPv4 Network Cidr : GCP측 VPC cidr

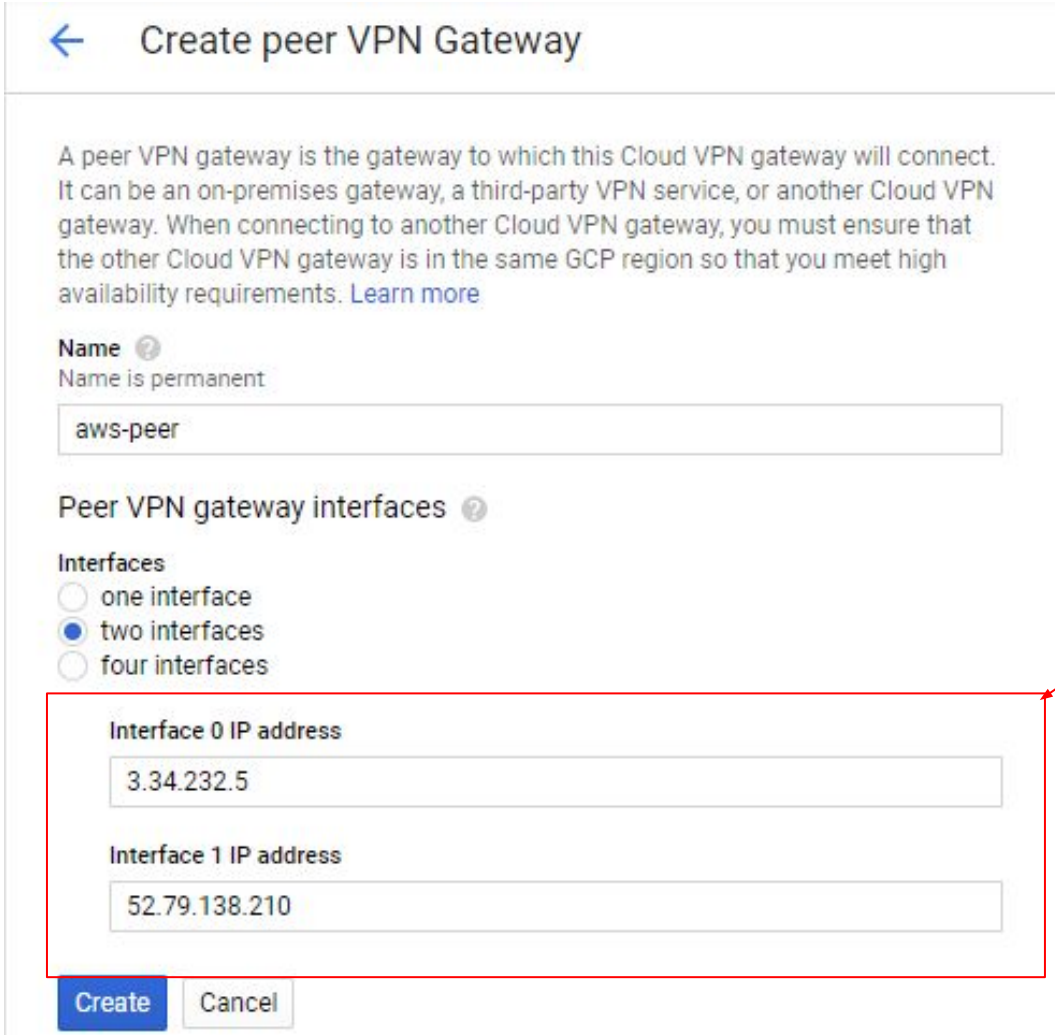
Tunnel은 default로 2개가 생성된다.
Tunnel option에서 IKEv2를 선택한다.
나머진 default

3. AWS 리소스 생성



※ 생성을 마친 후 AWS configuration을 download받으면 GCP측에 편하게 정보를 제공할 수 있다

4. GCP Peer gateway 생성



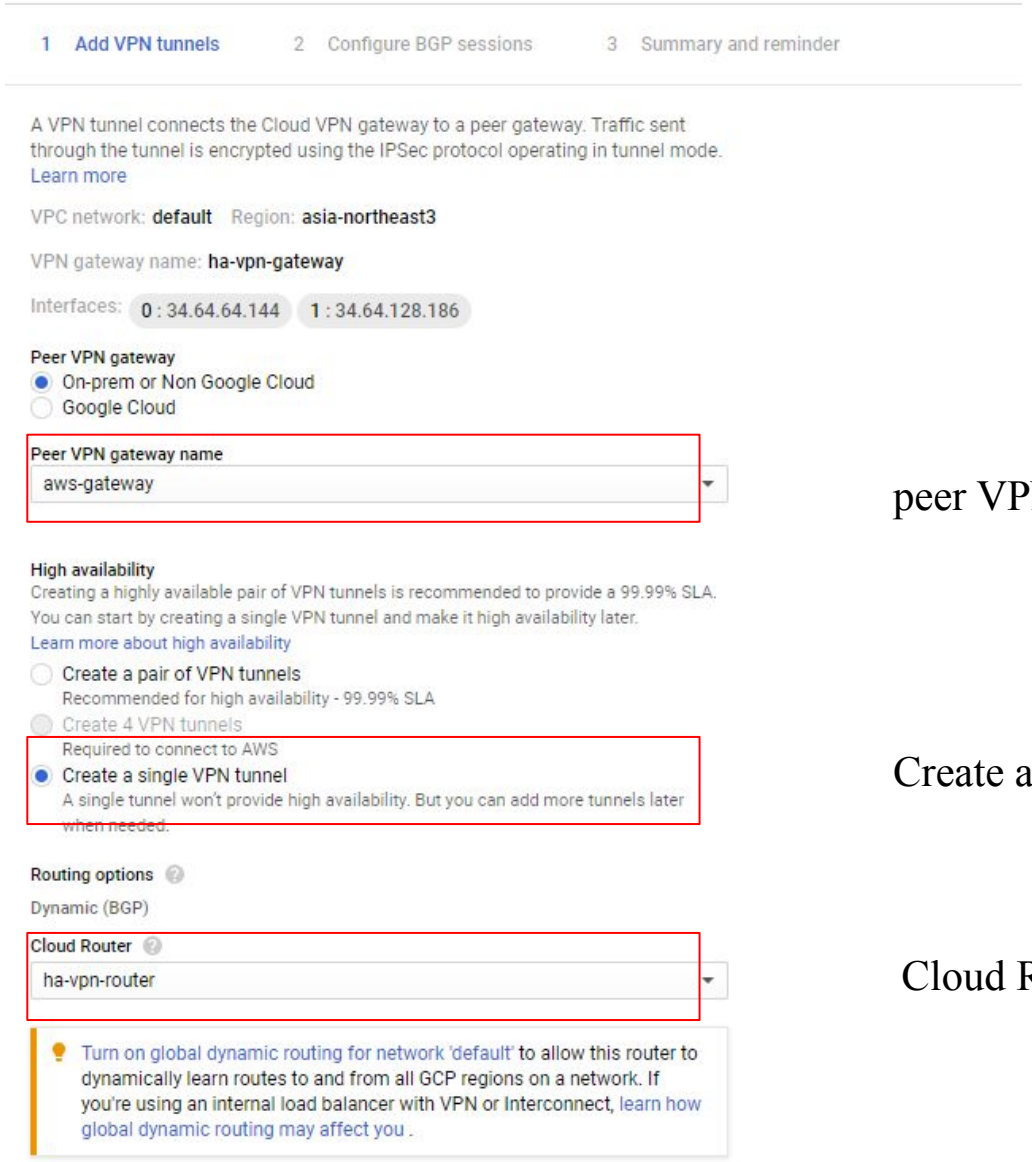
Tunnel Number	Outside IP Address	Inside IPv4 CIDR	In
Tunnel 1	13.124.62.151	169.254.138.168/30	-
Tunnel 2	52.78.221.188	169.254.79.112/30	-

GCP에서 peer gateway를 생성

AWS측 virtual gateway IP address 1

AWS측 virtual gateway IP address 2

5. GCP VPN Tunnel 생성

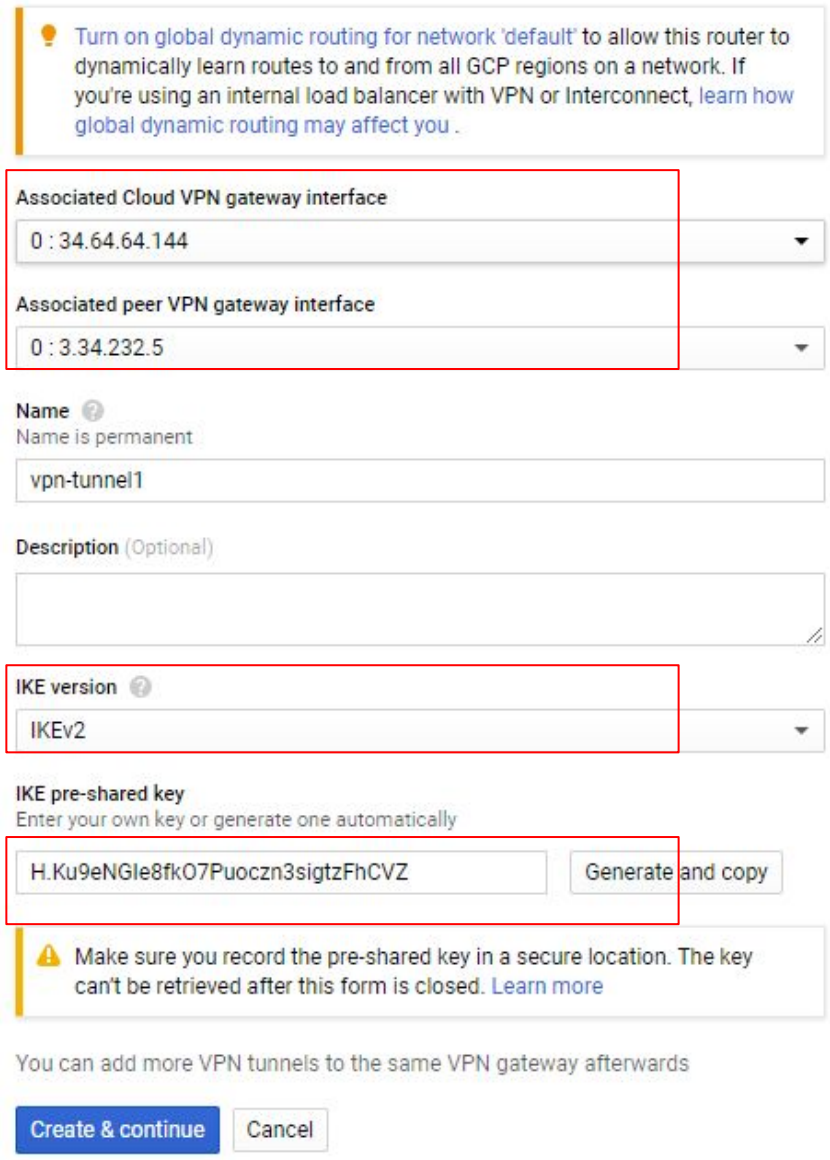


peer VPN gateway name : 이전에 생성한 peer gateway

Create a single VPN tunnel 체크

Cloud Router : 이전에 생성한 Cloud Router

5. GCP VPN Tunnel 생성



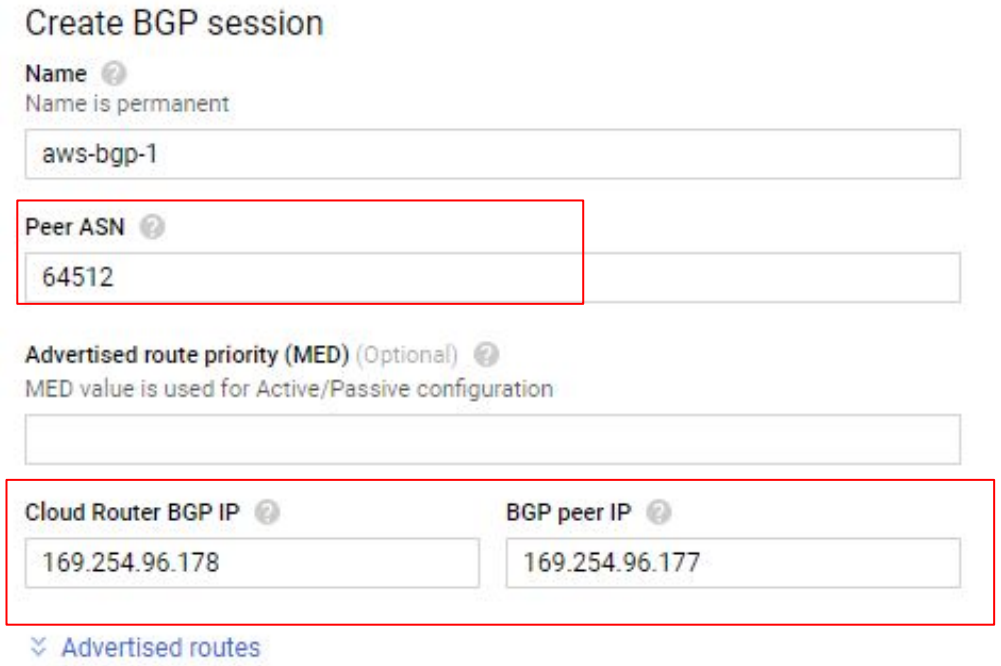
Associated Cloud VPN gateway interface :연결할 GCP측 VPN gateway interface (NIC 0)

Associated peer VPN gateway interface :연결할 AWS측 VPN gateway interface (NIC 0)

IKE version : IKEv2 체크

Pre-shared key : AWS에서 제공하는 Pre-shared key

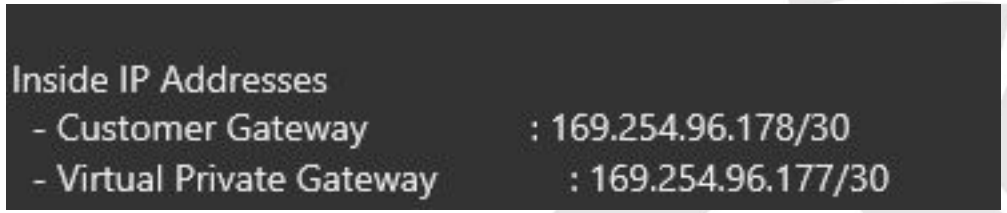
6. BGP Configuration 설정



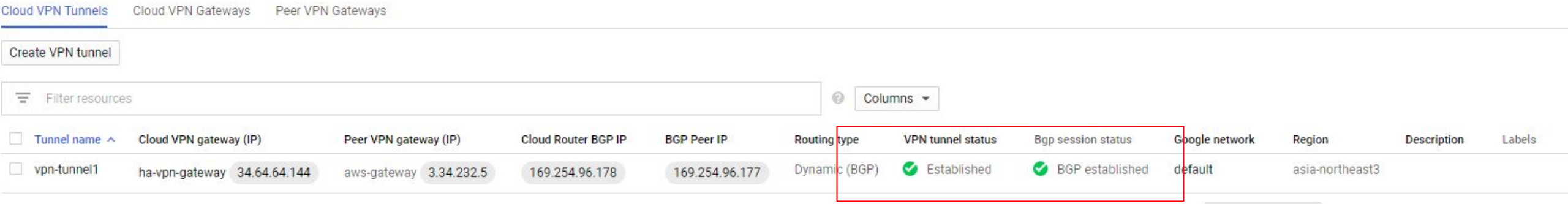
Peer ASN : AWS측에서 제공한 ASN

Cloud Router BGP IP : Customer Gateway /30 IP
BGP peer IP : Virtual Private Gateway /30 IP

-> AWS Configuration에서 참고

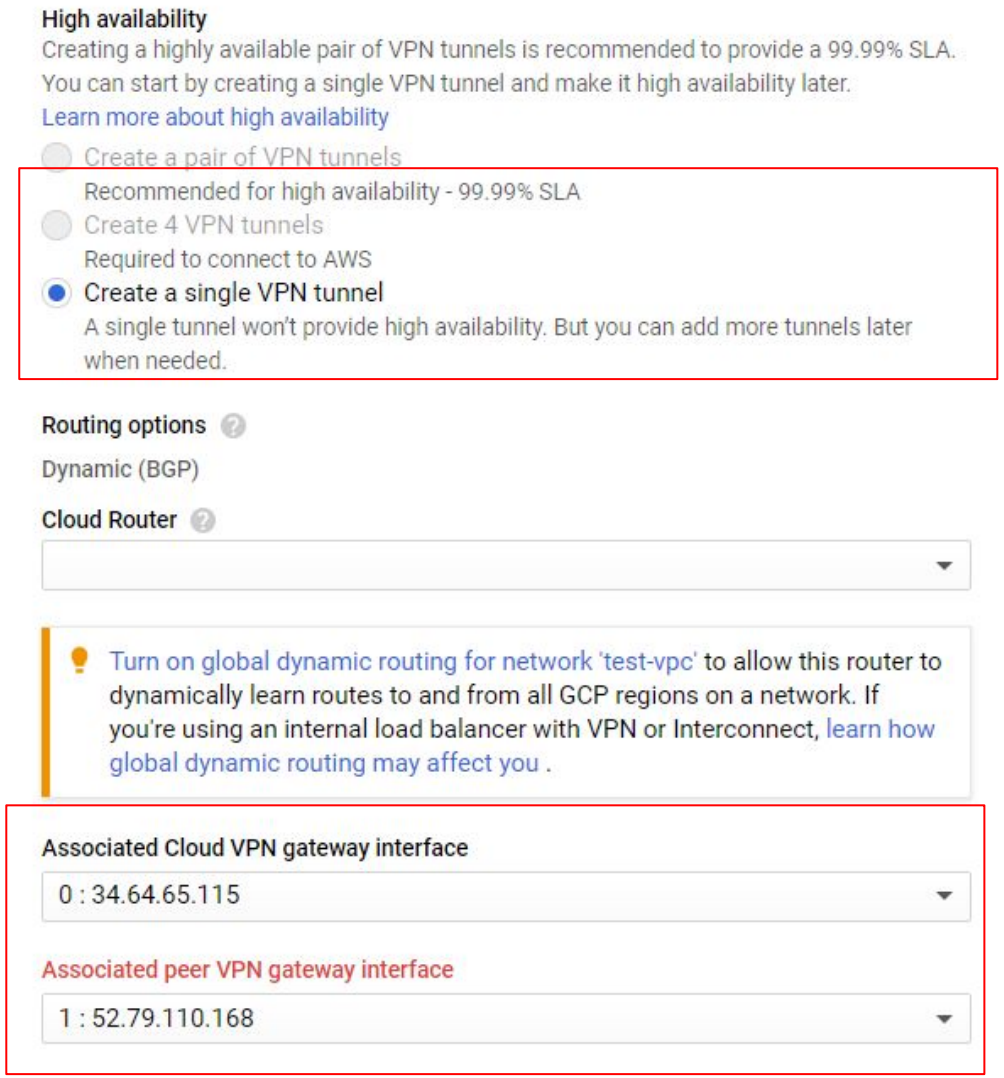


7. Connection 확인



VPN tunnel status : Established
Bgp session status : BGP established
가 뜨면 연결 성공

8. 추가 Tunnel 구성



Create a single VPN tunnel 선택

Associated Cloud VPN gateway interface : GCP측 VPN gateway interface (NIC 0)

Associated peer VPN gateway interface : AWS측 VPN gateway interface (NIC 1)

이후 bgp configuration도 동일하게 진행

8. 추가 Tunnel 구성

Cloud VPN Tunnels | Cloud VPN Gateways | Peer VPN Gateways

Create VPN tunnel

Filter resources | Columns

Tunnel name	Cloud VPN gateway (IP)	Peer VPN gateway (IP)	Cloud Router BGP IP	BGP Peer IP	Routing type	VPN tunnel status	Bgp session status	Google netw
test-tunnel1	test-ha-vpn 34.64.65.115	test-peer-aws 52.79.50.55	169.254.20.54	169.254.20.53	Dynamic (BGP)	Established	BGP established	test-vpc
test-tunnel2	test-ha-vpn 34.64.65.115	test-peer-aws 52.79.110.168	169.254.99.242	169.254.99.241	Dynamic (BGP)	Established	BGP established	test-vpc

두 Tunnel 모두 Established 되었다면 연결 성공

Thank you