

AWS와 GCP 간 HA VPN 연결 구성

lswoo@mz.co.kr

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 연결하는 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.

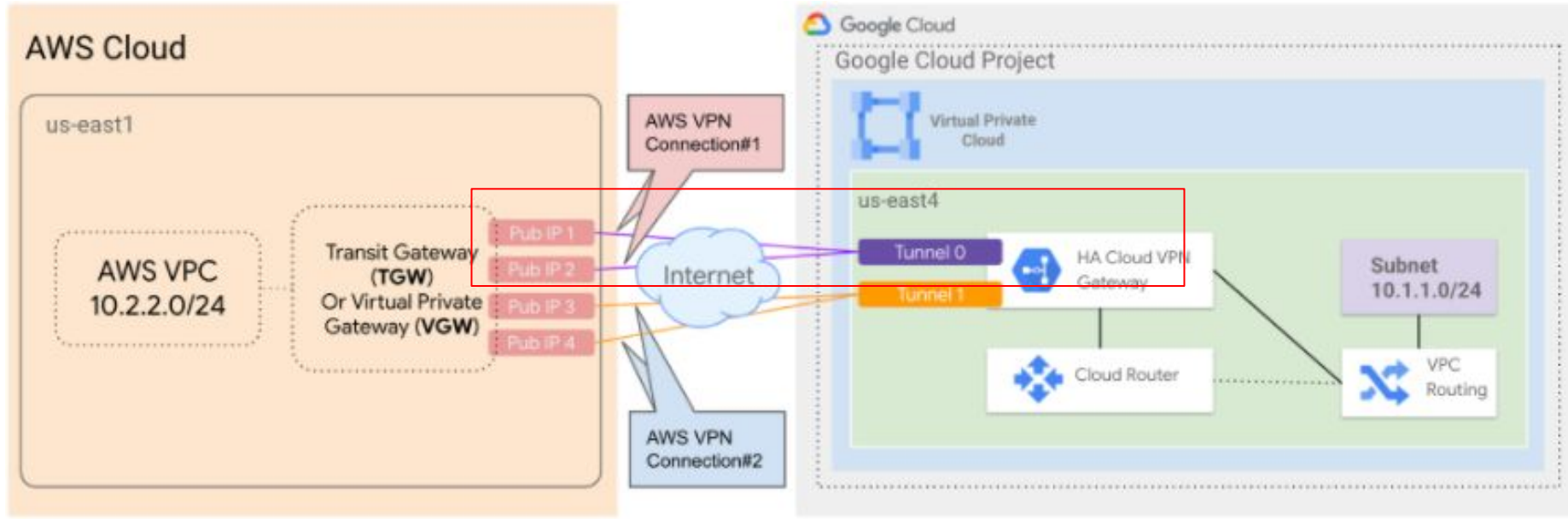
2021년 10월 31일부터 기본 VPN 게이트웨이를 사용한 Static routing은 지원 중단될 예정

-> Static routing VPN은 HA VPN 게이트웨이를 사용한 **Dynamic routing**으로 변경해야 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

A virtual private network lets you securely connect your Google Compute Engine resources to your own private network. Google VPN uses IKEv1 or IKEv2 to establish the IPSec connectivity. [Learn more](#)

VPN options

- ☒ **High-availability (HA) VPN**
Supports dynamic routing (BGP) only
Supports high availability (99.99 SLA, within region)
[Learn more](#)



- ☐ **Classic VPN**
Supports dynamic routing and static routing
No high availability
[Learn more](#)



CONTINUE

CANCEL

High-availability (HA) VPN 선택

(Classic VPN의 static routing은 지원 중단)

2. HA VPN gateway 및 Cloud Router 생성

1 Create Cloud HA VPN gateway

2 Add VPN tunnels

3 Configure

High Availability (HA) capable Cloud VPN gateways are regional resources with two interfaces, each interface with its own external IP address. HA VPN connects to an on-premises VPN gateway or another Cloud VPN gateway. [Learn more](#)

VPN gateway name ?
Name is permanent

Network ?
default

Region ?
Region is permanent

VPN gateway public IP address ?
Two IP addresses will be automatically allocated for each of your gateway interfaces

Create & continue

Cancel

Cloud VPN Gateway 생성

Network : VPN을 구성할 VPN Network 선택

Region : VPN을 구성할 Region 선택

2. HA VPN gateway 및 Cloud Router 생성

[←](#) Create a cloud router

Google Cloud Router dynamically exchanges routes between your Virtual Private Cloud (VPC) and on-premises networks by using Border Gateway Protocol (BGP)

Name *

ha-vpn-router

Lowercase letters, numbers, hyphens allowed

Description

Network *

default

Region *

asia-northeast3 (Seoul)

Google ASN

65001

Advertised routes

Routes

☒ Advertise all subnets visible to the Cloud Router (Default)

☐ Create custom routes

CREATE

CANCEL

Equivalent: [REST](#) [command line](#)

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

☒ Gateway name ^	IP address	VPC network	Region	VPN tunnels	Description	Labels
☒ ha-vpn-gateway	Interface: 0 34.64.64.144 Interface: 1 34.64.128.186	default	asia-northeast3			Add VPN tunnel ⋮

Cloud Routers + CREATE ROUTER REFRESH DELETE								
Filter Enter property name or value								
☐ Name ↑	Network	Region	Google ASN	Interconnect	Connection	BGP sessions	Logs	
☐ ha-vpn-router	default	asia-northeast3	65001	None			View	

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 **접치지 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

Create Virtual Private Gateway

A virtual private gateway is the router on the Amazon side of the VPN tunnel.

Name tag

test-vpn



ASN



Amazon default ASN



Custom ASN

6455



* Required

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

3. AWS 리소스 생성

[Virtual Private Gateways](#) > Attach to VPC

Attach to VPC

Select the VPC to attach to the virtual private gateway.

Virtual Private Gateway Id vgw-09c4ba7f1366a889d

VPC*

vpc-acfd7cc7



* Required

생성한 Virtual Private Gateways는 VPC에 attach한다.

3. AWS 리소스 생성

Create Customer Gateway

Specify the IP address for your gateway's external interface; the address must be static and may be behind a default gateway's Border Gateway Protocol (BGP) Autonomous System Number (ASN); this can be either a public or private IP address.

VPNs can use either Pre-Shared Keys or Certificates for authentication. When using Certificate authentication, a certificate must be created and associated with the gateway. To use Pre-Shared Keys, only an IP address is required.

Name	test-custom2	
Routing	☒ Dynamic ☐ Static	
BGP ASN*	65003	
IP Address	34.64.128.102	
Certificate ARN	Select Certificate ARN	 
Device	Optional	

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

Create VPN Connection

Select the target gateway and customer gateway that you would like to connect via a VPN connection. You

Name tag test-tunnel ⓘ

Target Gateway Type
☒ Virtual Private Gateway
☐ Transit Gateway

Virtual Private Gateway* vgw-09c4ba7f1366a889d ⌵ Ⓒ

Customer Gateway
☒ Existing
☐ New

Customer Gateway ID* cgw-07f9586a90eb6224c ⌵ Ⓒ

Routing Options
☒ Dynamic (requires BGP)
☐ Static

Tunnel Inside Ip Version
☒ IPv4
☐ IPv6

Local IPv4 Network Cidr 10.178.0.0/20 ⓘ

Remote IPv4 Network Cidr 10.10.0.0/20 ⓘ

3. VPN Tunnel 생성

Virtual Private Gateway : 생성한 Virtual Private Gateway 선택

Customer Gateway : 생성한 Customer Gateway 선택

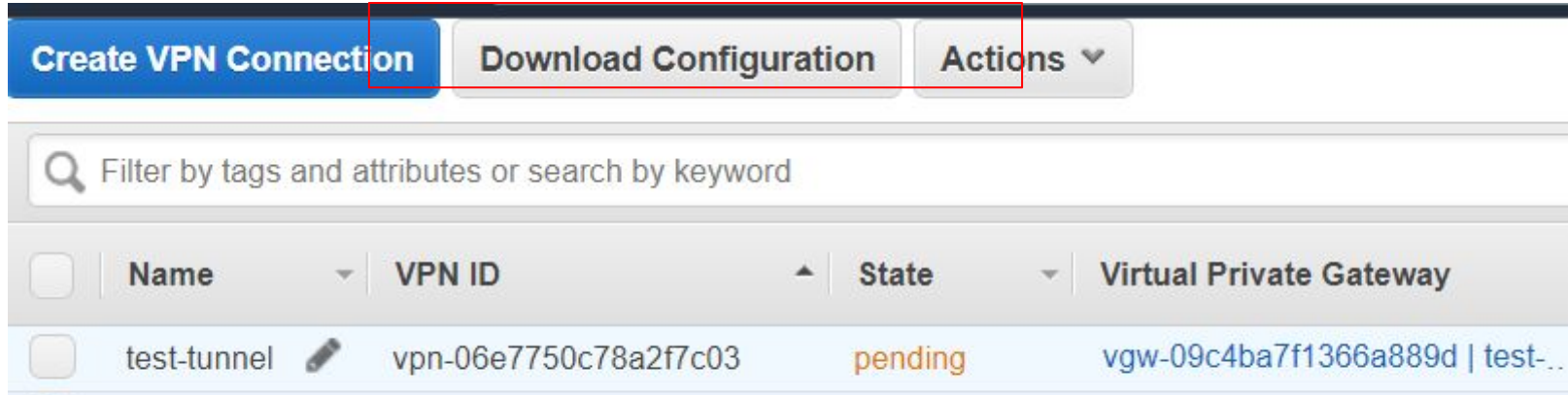
Routing Option : Dynamic

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

[←](#) Create peer VPN Gateway

A peer VPN gateway is the gateway to which this Cloud VPN gateway will connect. It can be an on-premises gateway, a third-party VPN service, or another Cloud VPN gateway. When connecting to another Cloud VPN gateway, you must ensure that the other Cloud VPN gateway is in the same GCP region so that you meet high availability requirements. [Learn more](#)

Name [?](#)
Name is permanent

Peer VPN gateway interfaces [?](#)

Interfaces

☐ one interface

☒ two interfaces

☐ four interfaces

Interface 0 IP address

Interface 1 IP address

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

1 Add VPN tunnels

2 Configure BGP sessions

3 Summary and reminder

A VPN tunnel connects the Cloud VPN gateway to a peer gateway. Traffic sent through the tunnel is encrypted using the IPSec protocol operating in tunnel mode. [Learn more](#)

VPC network: **default** Region: **asia-northeast3**

VPN gateway name: **ha-vpn-gateway**

Interfaces: **0** : 34.64.64.144 **1** : 34.64.128.186

Peer VPN gateway

☒ On-prem or Non Google Cloud
☐ Google Cloud

Peer VPN gateway name

aws-gateway

High availability
Creating a highly available pair of VPN tunnels is recommended to provide a 99.99% SLA. You can start by creating a single VPN tunnel and make it high availability later. [Learn more about high availability](#)

☐ Create a pair of VPN tunnels
Recommended for high availability - 99.99% SLA

☐ Create 4 VPN tunnels
Required to connect to AWS

☒ Create a single VPN tunnel
A single tunnel won't provide high availability. But you can add more tunnels later when needed.

Routing options ?
Dynamic (BGP)

Cloud Router ?

ha-vpn-router

Turn on global dynamic routing for network 'default' to allow this router to dynamically learn routes to and from all GCP regions on a network. If you're using an internal load balancer with VPN or Interconnect, [learn how global dynamic routing may affect you](#).

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

 Turn on global dynamic routing for network 'default' to allow this router to dynamically learn routes to and from all GCP regions on a network. If you're using an internal load balancer with VPN or Interconnect, [learn how global dynamic routing may affect you](#).

Associated Cloud VPN gateway interface
0 : 34.64.64.144

Associated peer VPN gateway interface
0 : 3.34.232.5

Name 
Name is permanent
vpn-tunnel1

Description (Optional)

IKE version 
IKEv2

IKE pre-shared key
Enter your own key or generate one automatically
H.Ku9eNGIe8fk07Puoczn3sigtzFhCVZ

 Make sure you record the pre-shared key in a secure location. The key can't be retrieved after this form is closed. [Learn more](#)

You can add more VPN tunnels to the same VPN gateway afterwards

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

Create BGP session

Name ?

Name is permanent

aws-bgp-1

Peer ASN ?

64512

Advertised route priority (MED) (Optional) ?

MED value is used for Active/Passive configuration

Cloud Router BGP IP ?

169.254.96.178

BGP peer IP ?

169.254.96.177

Advertised routes

Peer ASN : AWS측에서 제공한 ASN

Cloud Router BGP IP : Customer Gateway /30 IP

BGP peer IP : Virtual Private Gateway /30 IP

-> AWS Configuration에서 참고

Inside IP Addresses

- Customer Gateway : 169.254.96.178/30
- Virtual Private Gateway : 169.254.96.177/30

7. Connection 확인

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 network	Region	Description	Labels
☐ vpn-tunnel1	ha-vpn-gateway 34.64.64.144	aws-gateway 3.34.232.5	169.254.96.178	169.254.96.177	Dynamic (BGP)	✔ Established	✔ BGP established	default	asia-northeast3		

VPN tunnel status : Established

Bgp session status : BGP established

가 뜨면 연결 성공

8. 추가 Tunnel 구성

High availability

Creating a highly available pair of VPN tunnels is recommended to provide a 99.99% SLA.

You can start by creating a single VPN tunnel and make it high availability later.

[Learn more about high availability](#)

☐ Create a pair of VPN tunnels

Recommended for high availability - 99.99% SLA

☐ Create 4 VPN tunnels

Required to connect to AWS

☒ Create a single VPN tunnel

A single tunnel won't provide high availability. But you can add more tunnels later when needed.

Routing options ?

Dynamic (BGP)

Cloud Router ?



Turn on global dynamic routing for network 'test-vpc' to allow this router to dynamically learn routes to and from all GCP regions on a network. If you're using an internal load balancer with VPN or Interconnect, [learn how global dynamic routing may affect you](#).

Associated Cloud VPN gateway interface

0 : 34.64.65.115

Associated peer VPN gateway interface

1 : 52.79.110.168

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

