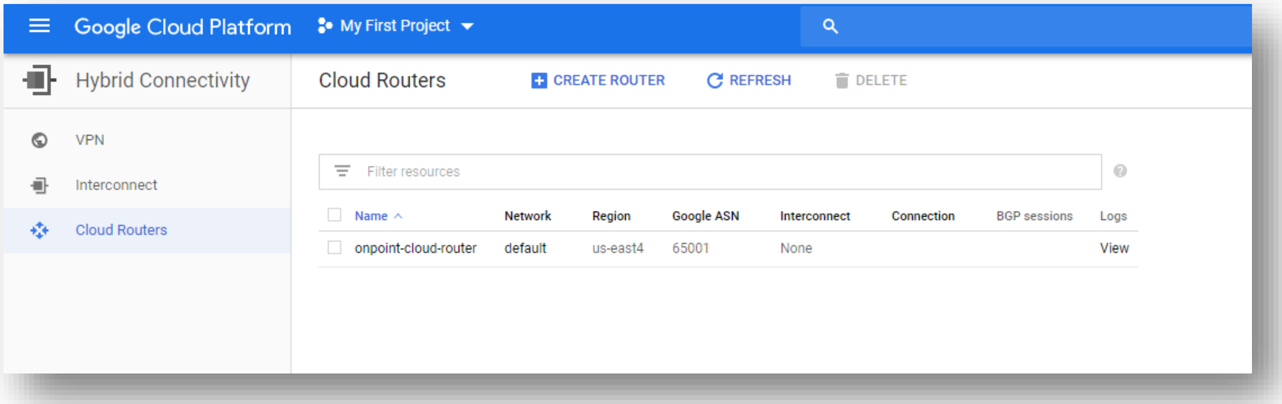
Site-to-Site Hybrid VPN Configuration

Overview

As more and more organizations are seeking to avoid vendor lock in and take advantage of specific cloud provider services, hybrid environments are becoming more popular. Being able to seamlessly and securely communicate between disparate environments is critical to streamlined operation. This guide walks through the process of creating a site to site virtual private network (VPN) connection between Google Cloud Platform (GCP) and Amazon Web Services (AWS) using dynamic routing.

Create GCP Cloud Router

The Google Cloud Router is a managed service that scales with network traffic and dynamically exchanges routes between GCP and your other environment. The cloud router also utilizes the Border Gateway Protocol (BGP), which automatically propagates changes between networks so there is no need to define static routes. This is critical when adding or removing services so that they can automatically communicate across the VPN. When setting up the cloud router, you will also need to define the Autonomous System Number (ASN), which the network uses to control routing and exchange routing information. The allowable range is 64512 - 65534, 4200000000 – 4294967294 (and cannot be changed after it is selected), and we selected **65001** for this case. When creating the cloud router, also specify “Advertise all subnets visible to the Cloud Router (Default)” to expose all subnets to BGP routing.

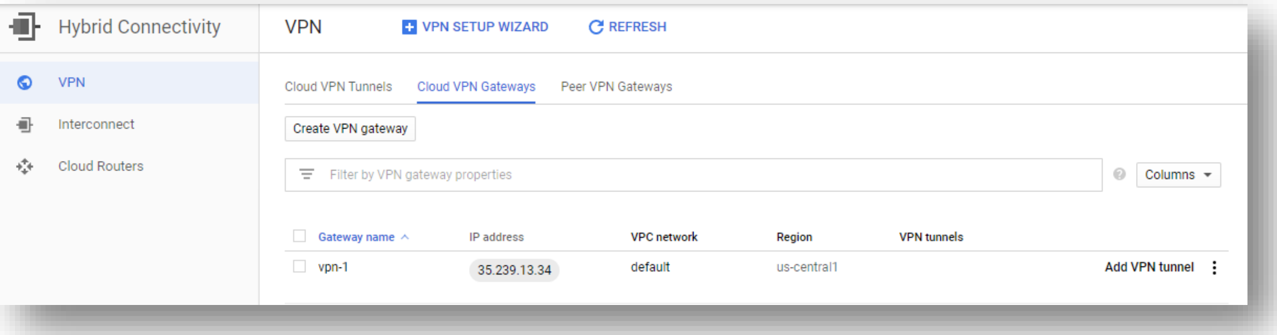


	Name	Network	Region	Google ASN	Interconnect	Connection	BGP sessions	Logs
□	onpoint-cloud-router	default	us-east4	65001	None			View

Create GCP Cloud VPN gateway

The GCP cloud VPN gateway is a classic VPN which has an external IP address and supports tunnels using BGP. We will specify two public interfaces on the AWS side to allow for redundant tunnels.

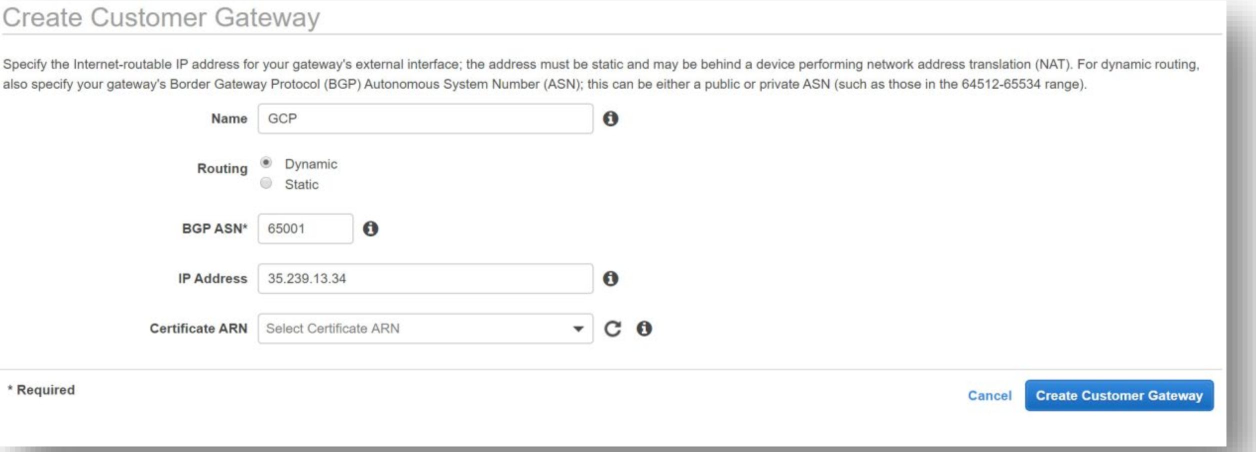
When you create the VPN, reserve a static public IP that will be used for the GCP side of the tunnel. This IP will be referenced when creating the tunnels from the AWS side.



Gateway name	IP address	VPC network	Region	VPN tunnels	
vpn-1	35.239.13.34	default	us-central1		Add VPN tunnel

Create AWS Customer Gateway

The Customer Gateway is a device that is the external side of the VPN connection; There are two tunnels between the customer gateway device and the virtual private gateway to provide increased availability. Set the ASN to 65001 (the value that was used on the GCP Cloud Router) and specify the IP of the GCP Cloud VPN


Create Customer Gateway

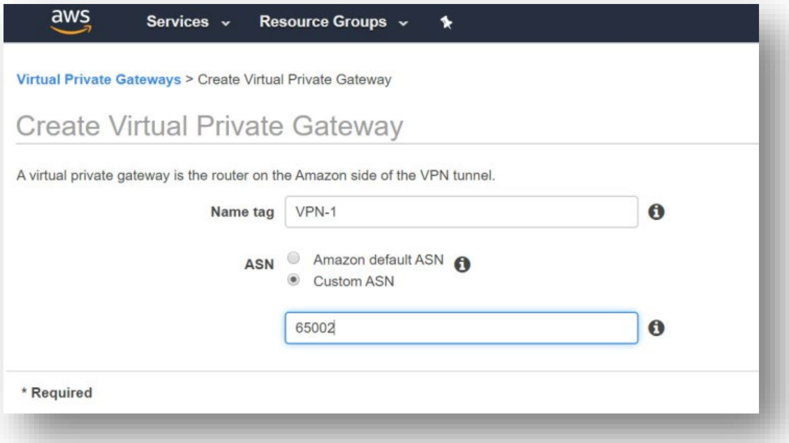
Specify the Internet-routable IP address for your gateway's external interface; the address must be static and may be behind a device performing network address translation (NAT). For dynamic routing, also specify your gateway's Border Gateway Protocol (BGP) Autonomous System Number (ASN); this can be either a public or private ASN (such as those in the 64512-65534 range).

Name	GCP
Routing	● Dynamic ○ Static
BGP ASN*	65001
IP Address	35.239.13.34
Certificate ARN	Select Certificate ARN

* Required

Create AWS Virtual Private Gateway

The AWS Virtual Private Gateway is the VPN concentrator on the Amazon side of the Site-to-Site VPN connection. Set the ASN to 65002 on the AWS side, create the gateway, and then attach it to a VPC



Virtual Private Gateways > Create Virtual Private Gateway

Create Virtual Private Gateway

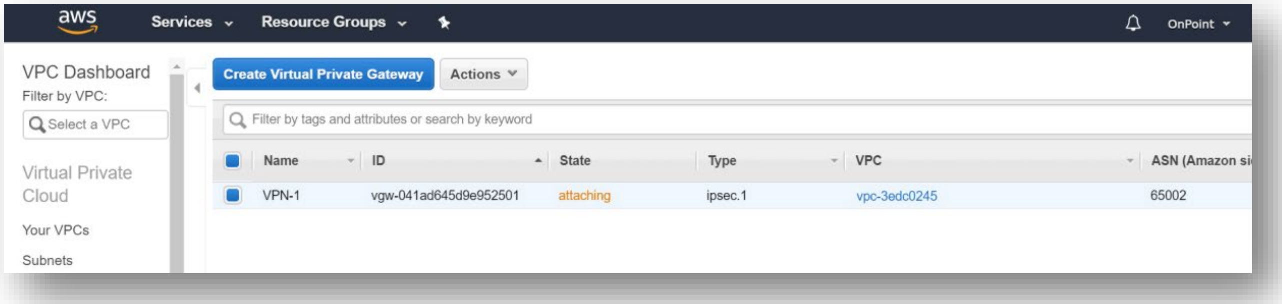
A virtual private gateway is the router on the Amazon side of the VPN tunnel.

Name tag: VPN-1

ASN: ○ Amazon default ASN ● Custom ASN

65002

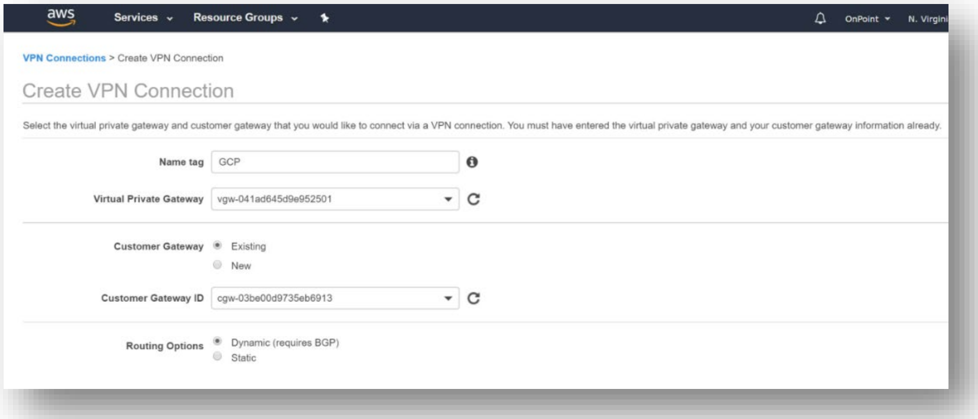
* Required



Name	ID	State	Type	VPC	ASN (Amazon si
VPN-1	vgw-041ad645d9e952501	attaching	ipsec.1	vpc-3edc0245	65002

Create AWS Site-to-Site VPN Connection

A Site-to-Site VPN connection is used to connect your remote network to a VPC. Each Site-to-Site VPN connection has two tunnels, with each tunnel using a unique virtual private gateway public IP address. It is important to configure both tunnels for redundancy. Select the Virtual Private Gateway and Customer Gateway that were created previously and select dynamic routing.



VPN Connections > Create VPN Connection

Create VPN Connection

Select the virtual private gateway and customer gateway that you would like to connect via a VPN connection. You must have entered the virtual private gateway and your customer gateway information already.

Name tag: GCP

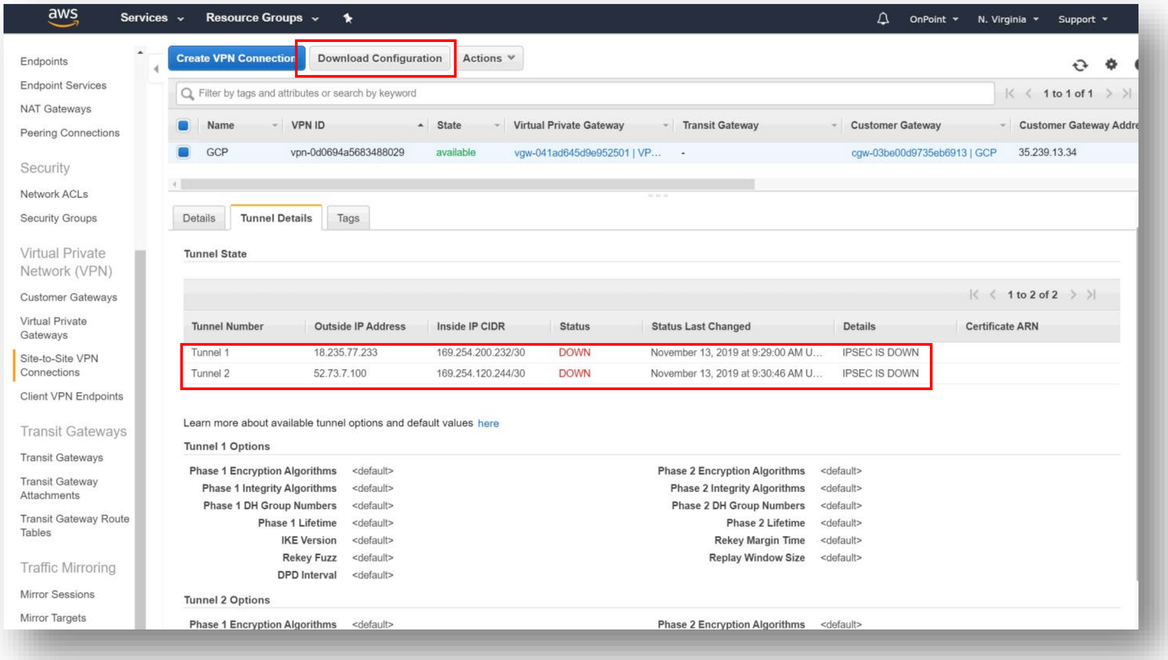
Virtual Private Gateway: vgw-041ad645d9e952501

Customer Gateway: ● Existing ○ New

Customer Gateway ID: cgw-03be00d9735eb6913

Routing Options: ● Dynamic (requires BGP) ○ Static

Leave the tunnel options as default, as AWS will generate Pre-Shares IPSEC keys and addresses for the tunnels automatically.



Name	VPN ID	State	Virtual Private Gateway	Transit Gateway	Customer Gateway	Customer Gateway Addre
GCP	vpn-0d0694a5683488029	available	vgw-041ad645d9e952501 | VP…	-	cgw-03be00d9735eb6913 | GCP	35.239.13.34

Tunnel State

Tunnel Number	Outside IP Address	Inside IP CIDR	Status	Status Last Changed	Details	Certificate ARN
Tunnel 1	18.235.77.233	169.254.200.232/30	DOWN	November 13, 2019 at 9:29:00 AM U…	IPSEC IS DOWN	
Tunnel 2	52.73.7.100	169.254.120.244/30	DOWN	November 13, 2019 at 9:30:46 AM U…	IPSEC IS DOWN	

Learn more about available tunnel options and default values here

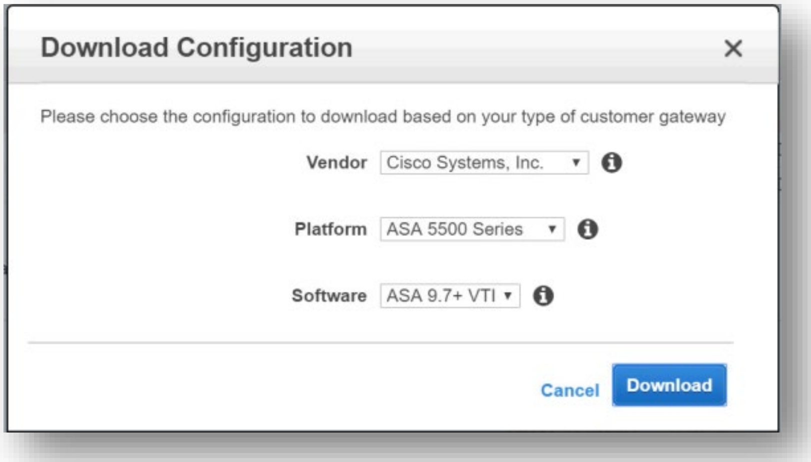
Tunnel 1 Options

Phase 1 Encryption Algorithms	<default>	Phase 2 Encryption Algorithms	<default>
Phase 1 Integrity Algorithms	<default>	Phase 2 Integrity Algorithms	<default>
Phase 1 DH Group Numbers	<default>	Phase 2 DH Group Numbers	<default>
Phase 1 Lifetime	<default>	Phase 2 Lifetime	<default>
IKE Version	<default>	Rekey Margin Time	<default>
Rekey Fuzz	<default>	Replay Window Size	<default>
DPD Interval	<default>		

Tunnel 2 Options

Phase 1 Encryption Algorithms	<default>	Phase 2 Encryption Algorithms	<default>

The links are showing down, as the GCP side of the tunnel has not been configured. The tunnel configuration information is generated by AWS and can be downloaded from the interface (as highlighted in the image above). Select the “Cisco Systems” vendor and then download



Download Configuration

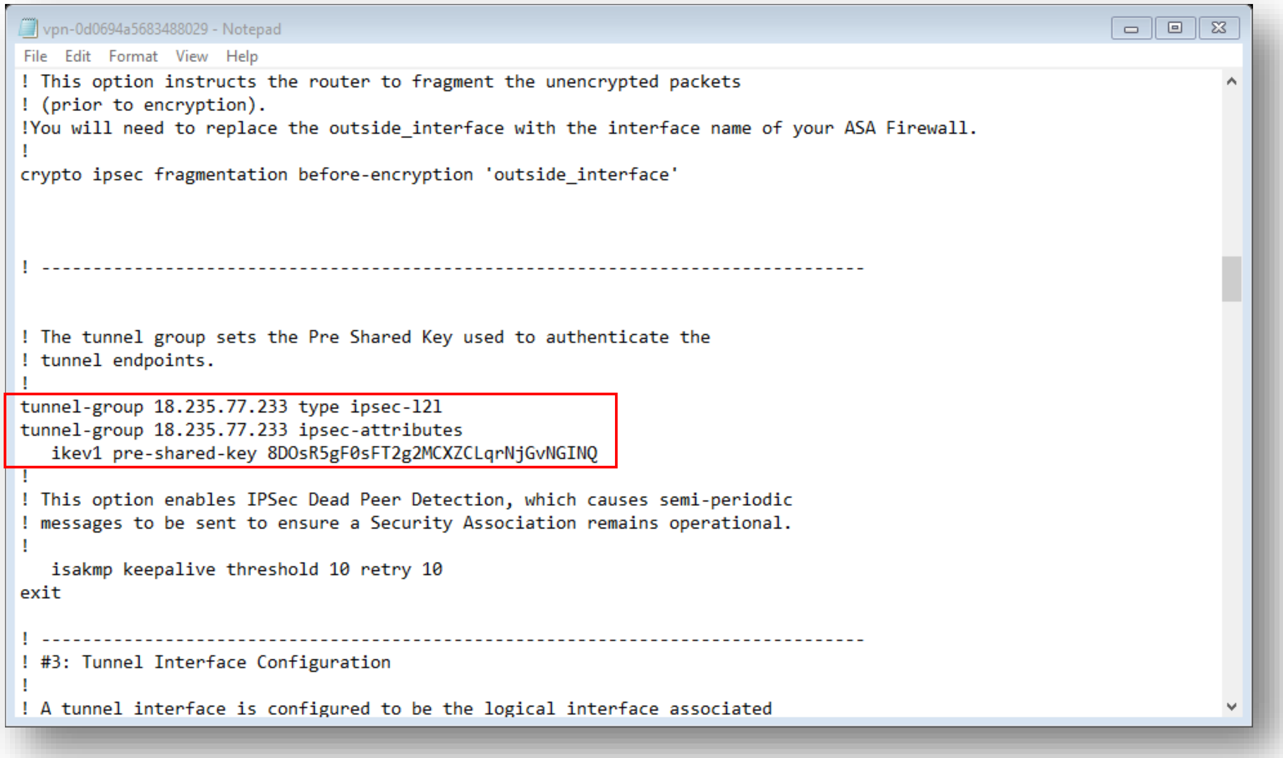
Please choose the configuration to download based on your type of customer gateway

Vendor: Cisco Systems, Inc.

Platform: ASA 5500 Series

Software: ASA 9.7+ VTI

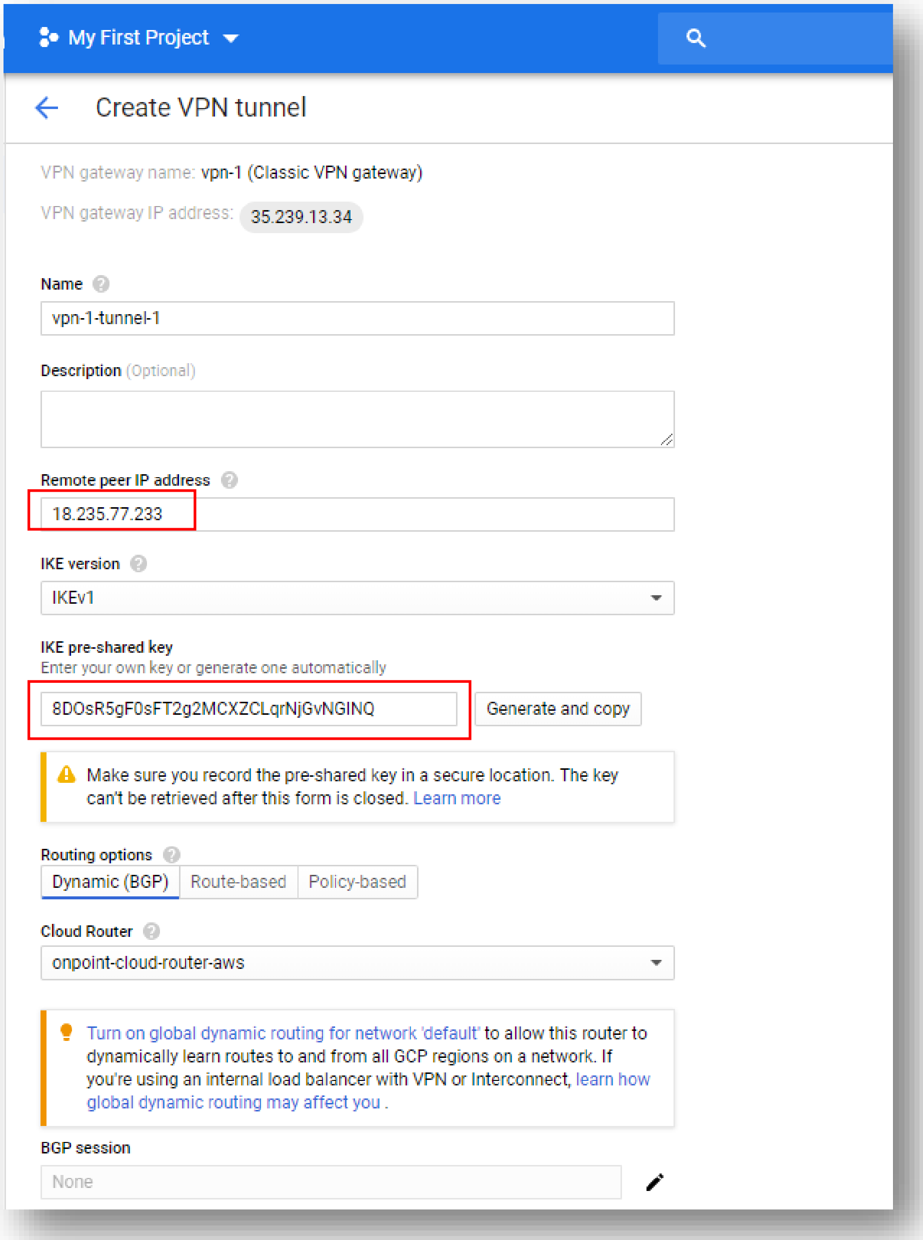
Open the text file and find the tunnel and associated pre-share key for both tunnels.



```
! This option instructs the router to fragment the unencrypted packets
! (prior to encryption).
!You will need to replace the outside_interface with the interface name of your ASA Firewall.
!
crypto ipsec fragmentation before-encryption 'outside_interface'



! --------------------------------------------------------------------------------


! The tunnel group sets the Pre Shared Key used to authenticate the
! tunnel endpoints.
!
tunnel-group 18.235.77.233 type ipsec-l2l
tunnel-group 18.235.77.233 ipsec-attributes
   ikev1 pre-shared-key 8DOsR5gF0sFT2g2MCXZCLqrNjGvNGINQ
!
! This option enables IPSec Dead Peer Detection, which causes semi-periodic
! messages to be sent to ensure a Security Association remains operational.
!
   isakmp keepalive threshold 10 retry 10
exit

! --------------------------------------------------------------------------------
! #3: Tunnel Interface Configuration
!
! A tunnel interface is configured to be the logical interface associated
```

Create GCP Cloud VPN Tunnels

In the GCP console, we can now create the other side of the tunnel using the data generated by AWS. Create a VPN tunnel, selecting the VPN gateway established earlier. Enter the remote peer address and IKE pre-shared key from AWS



VPN gateway name: vpn-1 (Classic VPN gateway)

VPN gateway IP address: 35.239.13.34

Name: vpn-1-tunnel-1

Description (Optional)

Remote peer IP address: 18.235.77.233

IKE version: IKEv1

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

8DOsR5gF0sFT2g2MCXZCLqrNjGvNGINQ

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

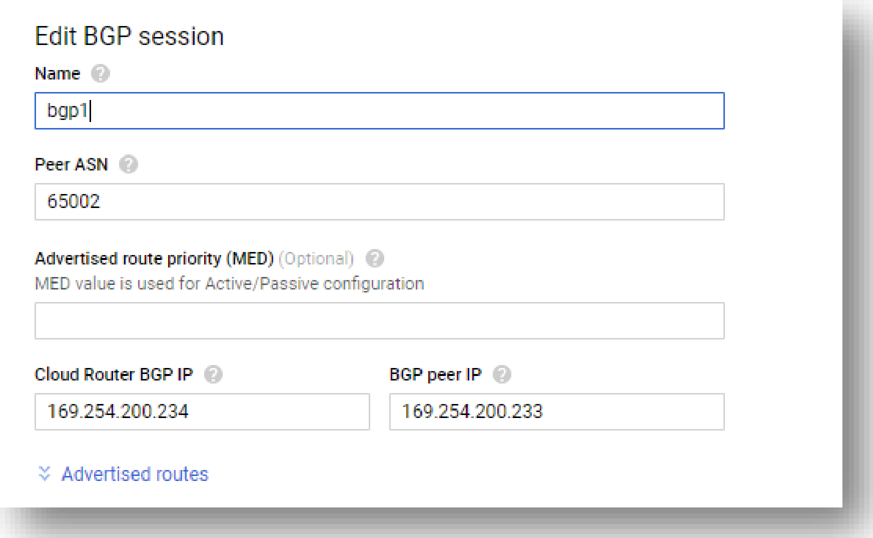
Routing options: Dynamic (BGP) | Route-based | Policy-based

Cloud Router: onpoint-cloud-router-aws

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 .

BGP session: None

Edit the BGP Session information and enter 65002 as the peer ASN (same as was defined in the AWS environment). Use the Inside IP CIDR value of 169.254.200.232/30 to populate the Cloud Router BGP IP (169.254.200.234) and the BGP peer IP (169.254.200.233)



Edit BGP session

Name: bgp1

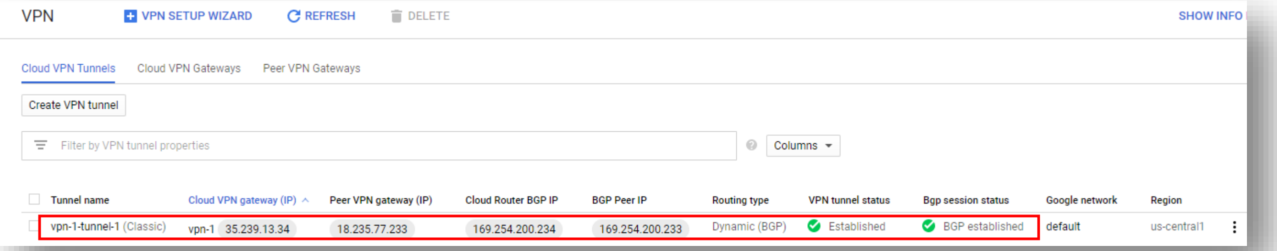
Peer ASN: 65002

Advertised route priority (MED) (Optional)
MED value is used for Active/Passive configuration

Cloud Router BGP IP: 169.254.200.234

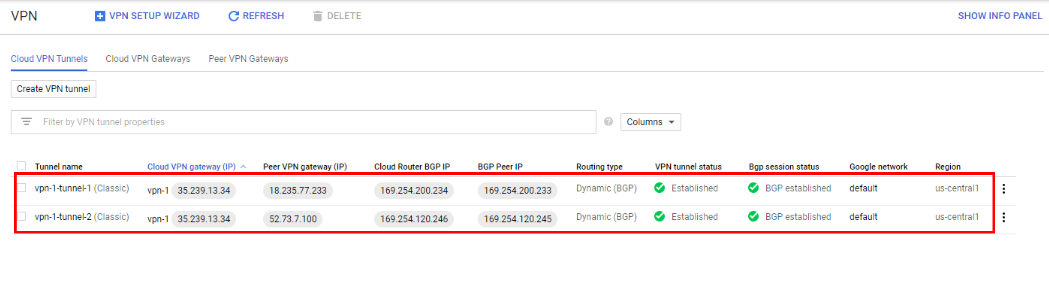
BGP peer IP: 169.254.200.233

Click “create”, and then after the tunnel is established you should see a successful tunnel



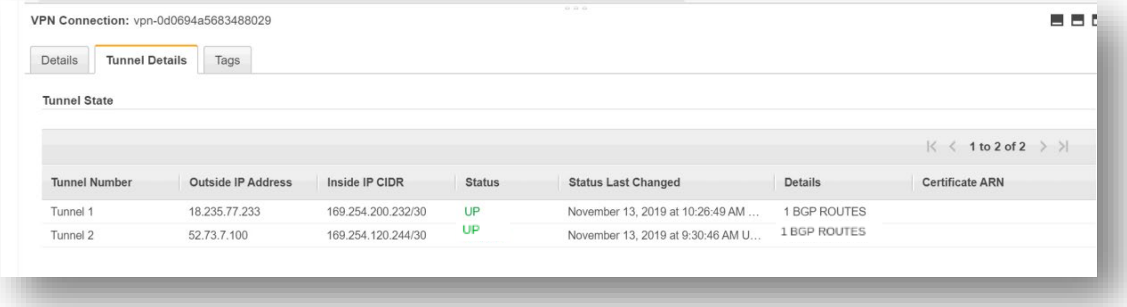
Tunnel name	Cloud VPN gateway (IP)	Peer VPN gateway (IP)	Cloud Router BGP IP	BGP Peer IP	Routing type	VPN tunnel status	Bgp session status	Google network	Region
vpn-1-tunnel-1 (Classic)	vpn-1 35.239.13.34	18.235.77.233	169.254.200.234	169.254.200.233	Dynamic (BGP)	✓ Established	✓ BGP established	default	us-central1

Create the second tunnel using the same steps with the second tunnel values and the interface should show both tunnels active



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
vpn-1-tunnel-1 (Classic)	vpn-1 35.239.13.34	18.235.77.233	169.254.200.234	169.254.200.233	Dynamic (BGP)	✓ Established	✓ BGP established	default	us-central1
vpn-1-tunnel-2 (Classic)	vpn-1 35.239.13.34	52.73.7.100	169.254.120.246	169.254.120.245	Dynamic (BGP)	✓ Established	✓ BGP established	default	us-central1

Check the AWS console to verify that the tunnels are up.



VPN Connection: vpn-0d0694a5683488029

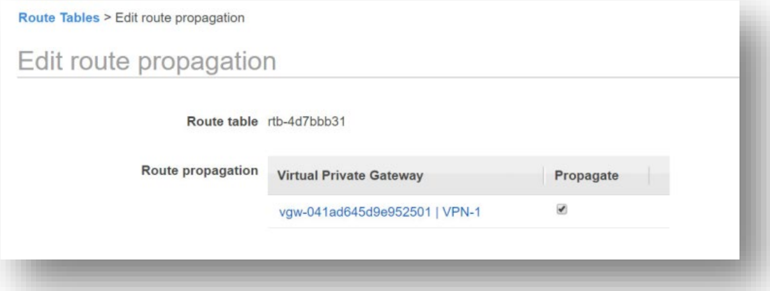
Tunnel State

1 to 2 of 2

Tunnel Number	Outside IP Address	Inside IP CIDR	Status	Status Last Changed	Details	Certificate ARN
Tunnel 1	18.235.77.233	169.254.200.232/30	UP	November 13, 2019 at 10:26:49 AM ...	1 BGP ROUTES	
Tunnel 2	52.73.7.100	169.254.120.244/30	UP	November 13, 2019 at 9:30:46 AM U...	1 BGP ROUTES	

Enable Route Propagation in AWS

The route table contains a set of rules that are used to determine where network traffic from your subnet or gateway is directed. Enabling route propagation will expose the subnets of the AWS VPC to the BGP and GCP Router.



Route Tables > Edit route propagation

Edit route propagation

Route table rtb-4d7bbb31

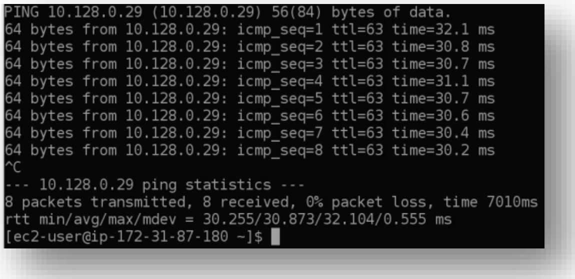
Route propagation

Virtual Private Gateway	Propagate
vgw-041ad645d9e952501 | VPN-1	☑

Testing the connection

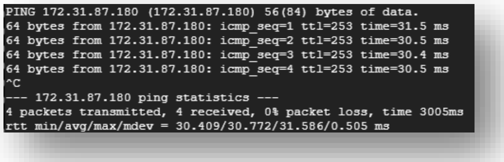
Once virtual machines are set up in both environments, you can verify the connection by pinging the internal IP address. Note: ensure that firewalls on both environments are configured to allow ICMP port access).

Ping from AWS to GCP



```
PING 10.128.0.29 (10.128.0.29) 56(84) bytes of data.
64 bytes from 10.128.0.29: icmp_seq=1 ttl=63 time=32.1 ms
64 bytes from 10.128.0.29: icmp_seq=2 ttl=63 time=30.8 ms
64 bytes from 10.128.0.29: icmp_seq=3 ttl=63 time=30.7 ms
64 bytes from 10.128.0.29: icmp_seq=4 ttl=63 time=31.1 ms
64 bytes from 10.128.0.29: icmp_seq=5 ttl=63 time=30.7 ms
64 bytes from 10.128.0.29: icmp_seq=6 ttl=63 time=30.6 ms
64 bytes from 10.128.0.29: icmp_seq=7 ttl=63 time=30.4 ms
64 bytes from 10.128.0.29: icmp_seq=8 ttl=63 time=30.2 ms
^C
--- 10.128.0.29 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7010ms
rtt min/avg/max/mdev = 30.255/30.873/32.104/0.555 ms
[ec2-user@ip-172-31-87-180 ~]$
```

Ping from GCP to AWS



```
PING 172.31.87.180 (172.31.87.180) 56(84) bytes of data.
64 bytes from 172.31.87.180: icmp_seq=1 ttl=253 time=31.5 ms
64 bytes from 172.31.87.180: icmp_seq=2 ttl=253 time=30.5 ms
64 bytes from 172.31.87.180: icmp_seq=3 ttl=253 time=30.4 ms
64 bytes from 172.31.87.180: icmp_seq=4 ttl=253 time=30.5 ms
^C
--- 172.31.87.180 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 30.409/30.772/31.586/0.505 ms
```

You should now be able to securely communicate between both environments!

About OnPoint

OnPoint Consulting, Inc. (OnPoint) delivers secure IT infrastructure, enterprise systems, cybersecurity and program management solutions for the U.S. federal government. Our specialized strategy, cyber and technology capabilities are changing the way our clients improve performance, effectively deliver results and manage risk. OnPoint holds ISO 9001:2015, ISO 20000-1:2011, ISO 27001:2013 certifications and a CMMI Maturity Level 3 rating.

OnPoint is a part of the Publicis Sapient platform, with access to industry leading AI tools and teams. Contact us at innovation@onpointcorp.com or visit onpointcorp.com to learn more about us and our services.