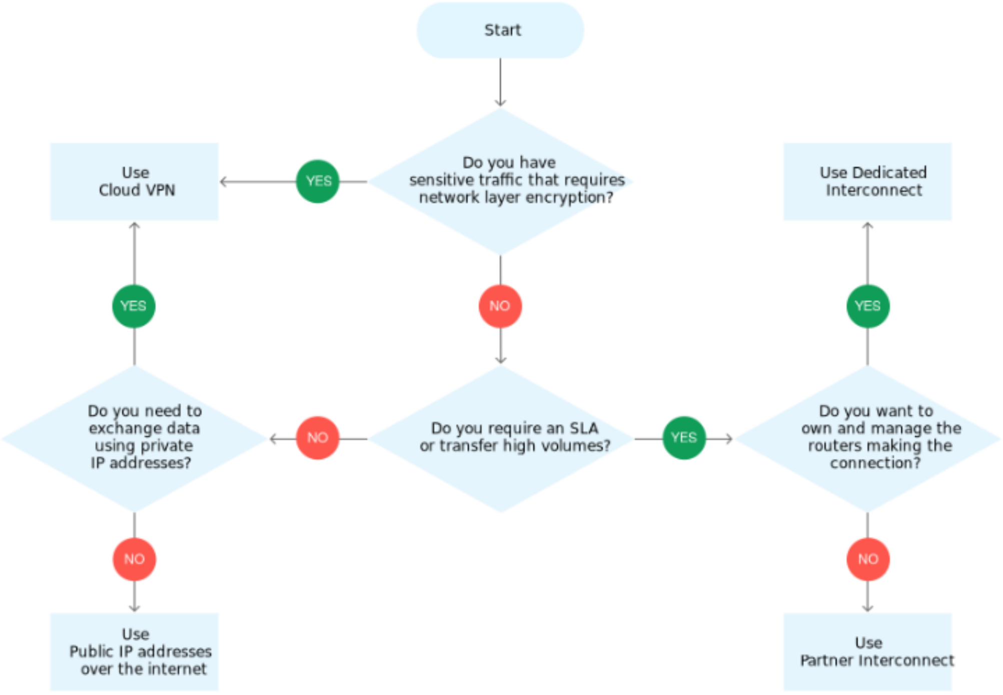
Hybrid Cloud

25 July 2021 16:45


Start
Do you have sensitive traffic that requires network layer encryption?
YES
Use Cloud VPN
NO
Do you require an SLA or transfer high volumes?
NO
Do you need to exchange data using private IP addresses?
YES
NO
Use Public IP addresses over the internet
YES
Do you want to own and manage the routers making the connection?
YES
Use Dedicated Interconnect
NO
Use Partner Interconnect

https://cloud.google.com/architecture/patterns-for-connecting-other-csps-with-gcp

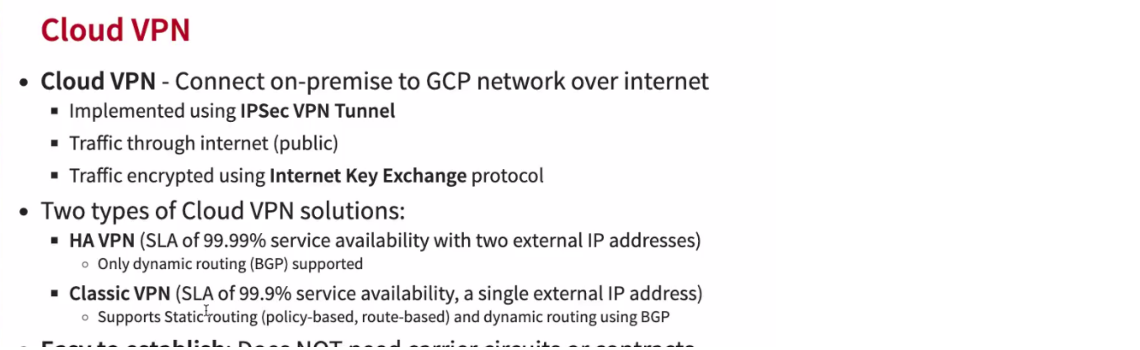
Cloud VPN

Step to speed up data transfer uing vpn

Create an additional VPN tunnel. Each VPN tunnel has a max speed of 3 Gbps. However, you can create multiple VPN tunnels to increase bandwidth.\

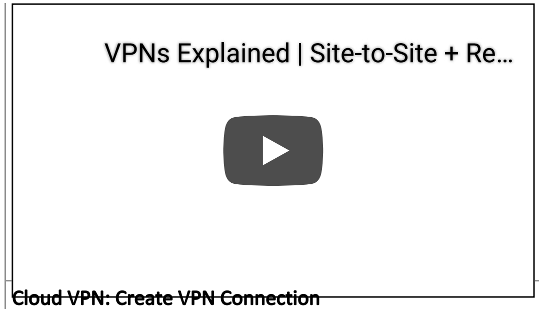
gateway can sustain up to 6 Gbps

VPNs Explained | Site-to-Site + Remote Access



Cloud VPN

- **Cloud VPN** - Connect on-premise to GCP network over internet
  - Implemented using **IPSec VPN Tunnel**
  - Traffic through internet (public)
  - Traffic encrypted using **Internet Key Exchange** protocol
- Two types of Cloud VPN solutions:
  - **HA VPN** (SLA of 99.99% service availability with two external IP addresses)
    - Only dynamic routing (BGP) supported
  - **Classic VPN** (SLA of 99.9% service availability, a single external IP address)
    - Supports Static routing (policy-based, route-based) and dynamic routing using BGP
- **Easy to establish:** Does NOT need carrier circuits or contracts



Cloud VPN: Create VPN Connection

Create VPN Gateway

```
gcloud compute vpn-gateways create NAME --network = NETWORK [ --description = DESCRIPTION ]
   [ --region = REGION ] [ GCLOUD_WIDE_FLAG … ]
```

https://cloud.google.com/sdk/gcloud/reference/compute/vpn-gateways/create

Create VPN Tunnel

```
gcloud compute vpn-tunnels create NAME --shared-secret = SHARED_SECRET
   ( --peer-address = PEER_ADDRESS   | --peer-external-gateway = PEER_EXTERNAL_GATEWAY   |
   --peer-gcp-gateway = PEER_GCP_GATEWAY   | --peer-gcp-gateway-region = PEER_GCP_GATEWAY_REGION )
   ( --target-vpn-gateway = TARGET_VPN_GATEWAY   |
   --target-vpn-gateway-region = TARGET_VPN_GATEWAY_REGION   | --vpn-gateway = VPN_GATEWAY   |
   --vpn-gateway-region = VPN_GATEWAY_REGION ) [ --description = DESCRIPTION ]
   [ --ike-version = IKE_VERSION ] [ --interface = INTERFACE ] [ --local-traffic-selector = CIDR ,[ CIDR ,
   …]] [ --peer-external-gateway-interface = PEER_EXTERNAL_GATEWAY_INTERFACE ] [ --region = REGION ]
   [ --remote-traffic-selector = CIDR ,[ CIDR ,…]] [ --router = ROUTER ] [ --router-region = ROUTER_REGION ]
   [ GCLOUD_WIDE_FLAG … ]
```

Detail: https://cloud.google.com/sdk/gcloud/reference/compute/vpn-tunnels/create

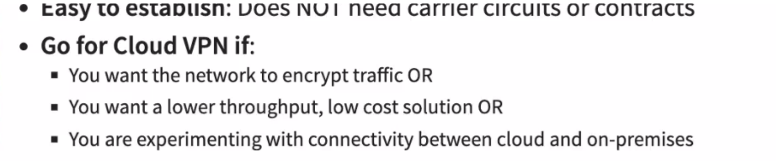
You want to establish a Compute Engine application in a single VPC across two regions. The application must communicate over VPN to an on-premises network. How should you deploy the VPN?

D. Deploy Cloud VPN Gateway in each region. Ensure that each region has at least one VPN tunnel to the on-premises peer gateway. (**VPN Gateway and tunnel are regional resources**)

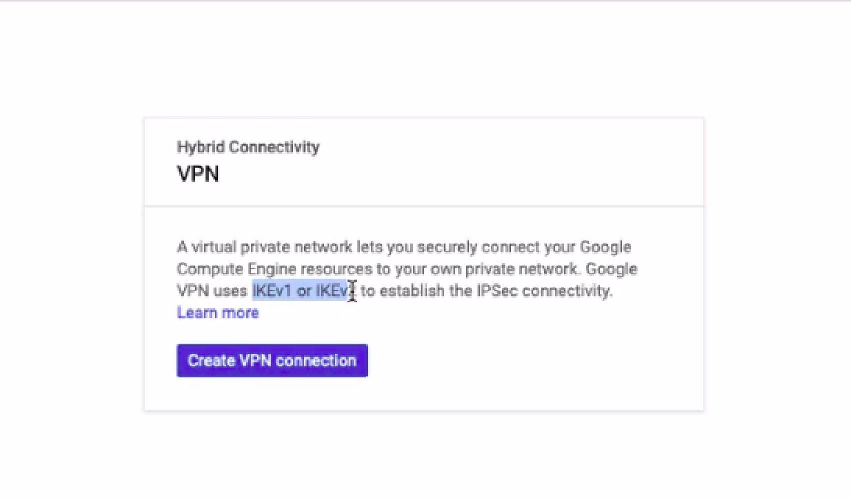
Recommended routing option

When using a single HA VPN gateway, we recommend using an active/passive routing configuration. With this configuration, the observed bandwidth capacity at the time of normal tunnel operation matches the bandwidth capacity observed during failover. This type of configuration is easier to manage because the observed bandwidth limit stays constant, except for the multiple gateway scenario described previously.

When using multiple HA VPN gateways, we recommend using an active/active routing configuration. With this configuration, the observed bandwidth capacity at the time of normal tunnel operation is twice that of the guaranteed bandwidth capacity. However, this configuration effectively underprovisions the tunnels and can cause dropped traffic in case of failover.



- **Easy to establish:** Does NOT need carrier circuits or contracts
- **Go for Cloud VPN if:**
  - You want the network to encrypt traffic OR
  - You want a lower throughput, low cost solution OR
  - You are experimenting with connectivity between cloud and on-premises

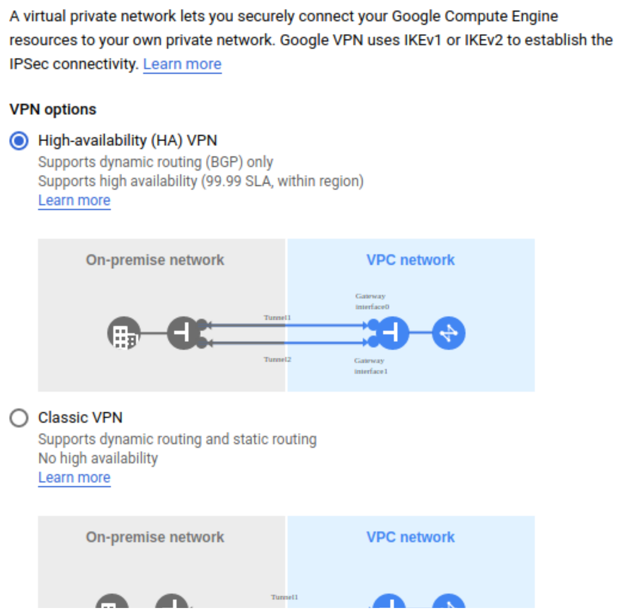


Hybrid Connectivity

VPN

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

HA VPN Setup



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

HA VPN to peer VPN gateways

There are three typical peer gateway configurations for HA VPN:

- An HA VPN gateway to two separate peer VPN devices, each with its own IP address
- An HA VPN gateway to one peer VPN device that uses two separate IP addresses
- An HA VPN gateway to one peer VPN device that uses one IP address

10GBps Throughput configuration using HA VPN

Following is an example of an HA VPN gateway with 10-Gbps throughput that uses the following Google Cloud resources:

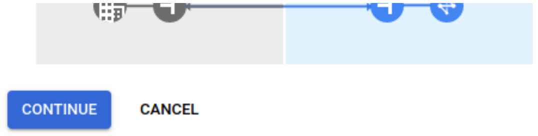
- 1 Cloud Router
- 4 HA VPN gateways with two tunnels each, for a total of 8 VPN tunnels
- 8 total BGP sessions

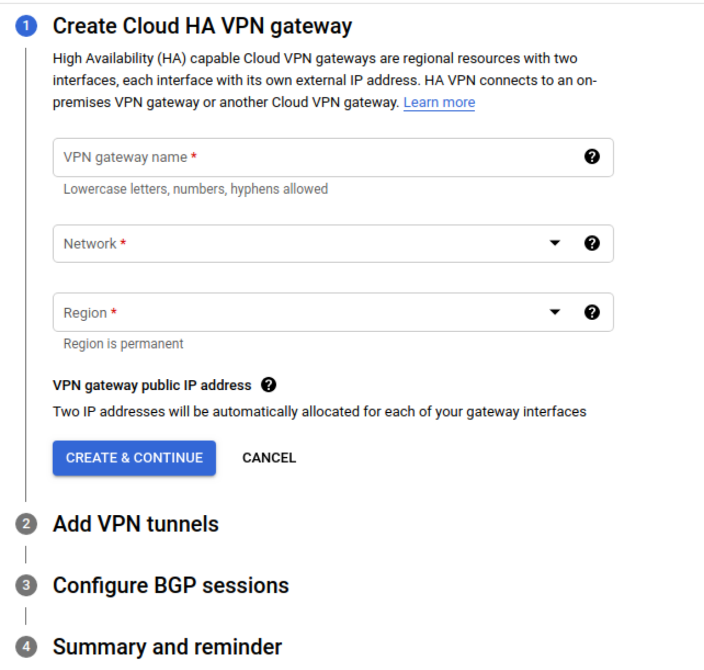
This configuration assumes an active/passive MED configuration for BGP sessions attached to interface 0 and interface 1 respectively on each gateway. That is, four interface 0 tunnels are active, and four interface 1 tunnels are passive.

Each Cloud VPN tunnel can support up to 3 Gbps total for ingress and egress. In this case, 3 Gbps is the maximum bandwidth and can only be achieved with an ideal traffic pattern; generally, we can safely say that 2.5 Gbps is ensured per tunnel. Therefore, the calculation is 4 * 2.5 = 10 Gbps

Classic VPN

Note: With Classic VPN, it is not possible to create two VPN tunnels within the same Cloud VPN gateway to the same destination VPN gateway. You can provide redundancy and failover for Classic VPN gateways by either moving to HA VPN or by using a second Classic VPN gateway.





1 Create Cloud HA VPN gateway

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 *
Lowercase letters, numbers, hyphens allowed

Network *

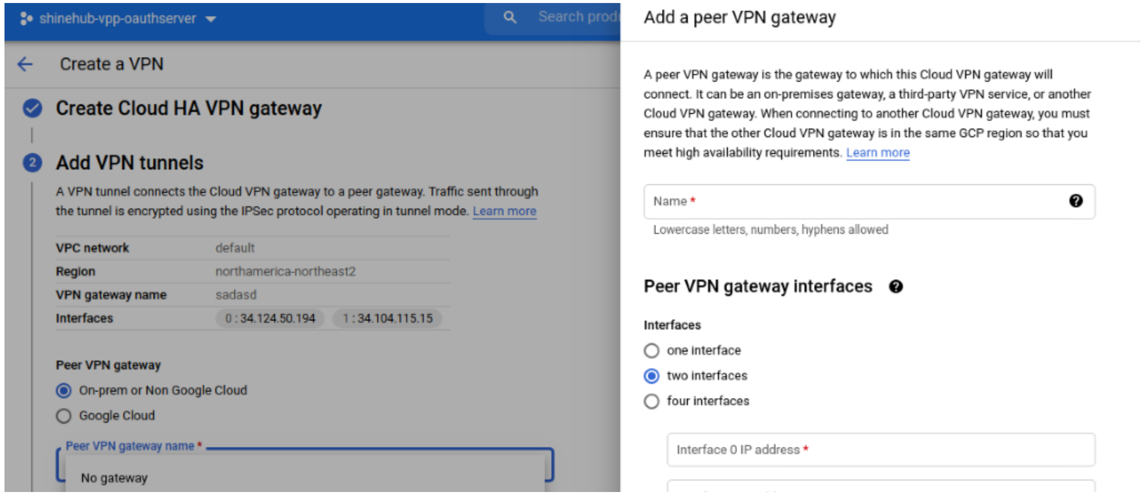
Region *
Region is permanent

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

2 Add VPN tunnels

3 Configure BGP sessions

4 Summary and reminder



Create a VPN

Create Cloud HA VPN gateway

2 Add VPN tunnels

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	northamerica-northeast2
VPN gateway name	sadasd
Interfaces	0 : 34.124.50.194 1 : 34.104.115.15

Peer VPN gateway
● On-prem or Non Google Cloud
○ Google Cloud

Peer VPN gateway name *
No gateway

Add a peer VPN gateway

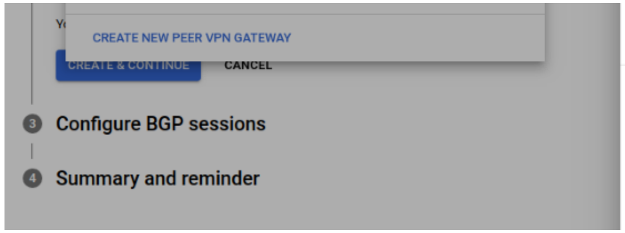
A peer VPN gateway is the gateway to which this Cloud VPN gateway will connect. It can be an on-premises gateway, a third-party VPN service, or another Cloud VPN gateway. When connecting to another Cloud VPN gateway, you must ensure that the other Cloud VPN gateway is in the same GCP region so that you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

Name *
Lowercase letters, numbers, hyphens allowed

Peer VPN gateway interfaces

Interfaces
○ one interface
● two interfaces
○ four interfaces

Interface 0 IP address *



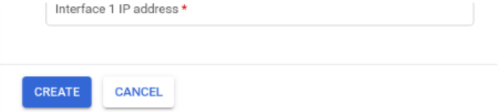
Y

CREATE NEW PEER VPN GATEWAY

CREATE & CONTINUE CANCEL

3 Configure BGP sessions

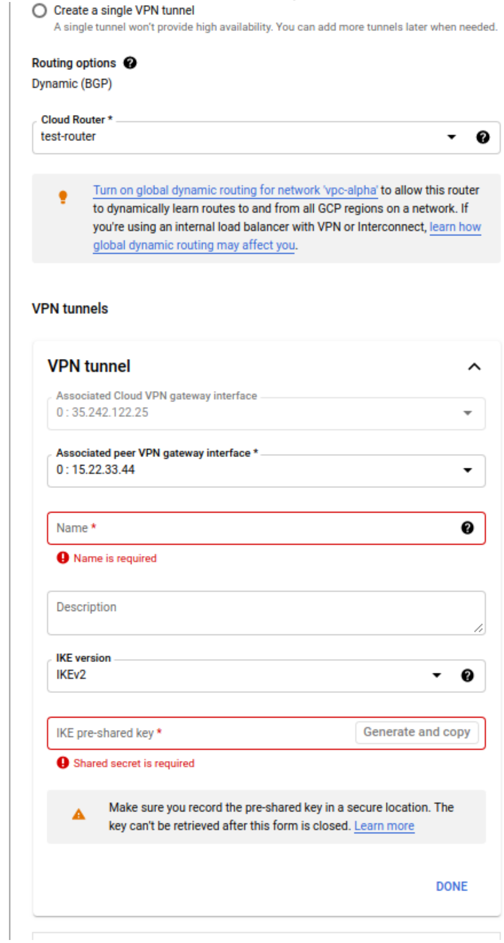
4 Summary and reminder



Interface 1 IP address *

CREATE CANCEL

We need to add two tunnel configuration



○ Create a single VPN tunnel

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

Routing options

Dynamic (BGP)

Cloud Router *: test-router

Turn on global dynamic routing for network 'vpc-alpha' 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.

VPN tunnels

VPN tunnel

Associated Cloud VPN gateway interface: 0 : 35.242.122.25

Associated peer VPN gateway interface *: 0 : 15.22.33.44

Name *

Name is required

Description

IKE version: IKEv2

IKE pre-shared key * Generate and copy

Shared secret is required

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

DONE

Configure BGP Session for single tunnel

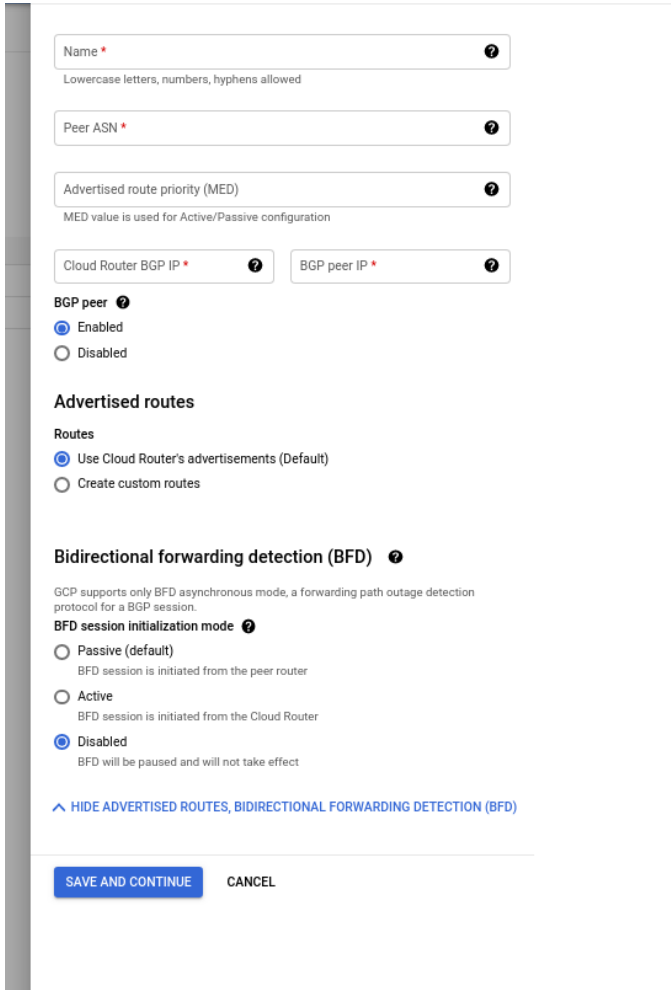
Peer ASN: The ASN for the on-premises side of the BGP session. The ASN can be public or private.

BGP Peer: The status of the BGP peer connection. If enabled, the peer connection can be established with routing information. If disabled, any active session with the peer is terminated and all associated routing information is removed.

BFD Session Initialization: The BFD session initiation mode for this BGP peer.

If set to Passive, the Cloud Router will wait for the peer router to initiate the BFD session for this BGP peer. If set to Active, the Cloud Router will initiate the BFD session for this BGP peer. If set to Disabled, BFD is disabled for this BGP peer.

Create BGP session



Name *
Lowercase letters, numbers, hyphens allowed

Peer ASN *

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

Cloud Router BGP IP *

BGP peer IP *

BGP peer
● Enabled
○ Disabled

Advertised routes

Routes
● Use Cloud Router's advertisements (Default)
○ Create custom routes

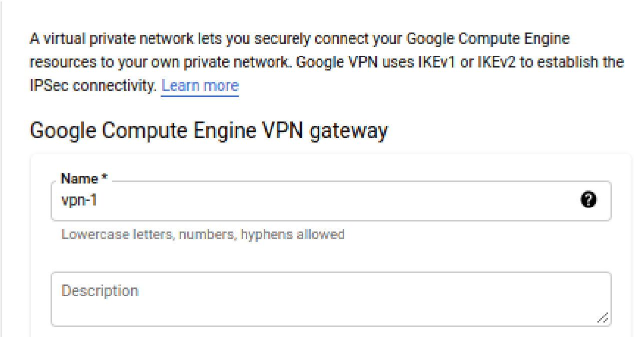
Bidirectional forwarding detection (BFD)

GCP supports only BFD asynchronous mode, a forwarding path outage detection protocol for a BGP session.

BFD session initialization mode
○ Passive (default)
BFD session is initiated from the peer router
○ Active
BFD session is initiated from the Cloud Router
● Disabled
BFD will be paused and will not take effect

HIDE ADVERTISED ROUTES, BIDIRECTIONAL FORWARDING DETECTION (BFD)
SAVE AND CONTINUE
CANCEL

Classic VPN Configuration

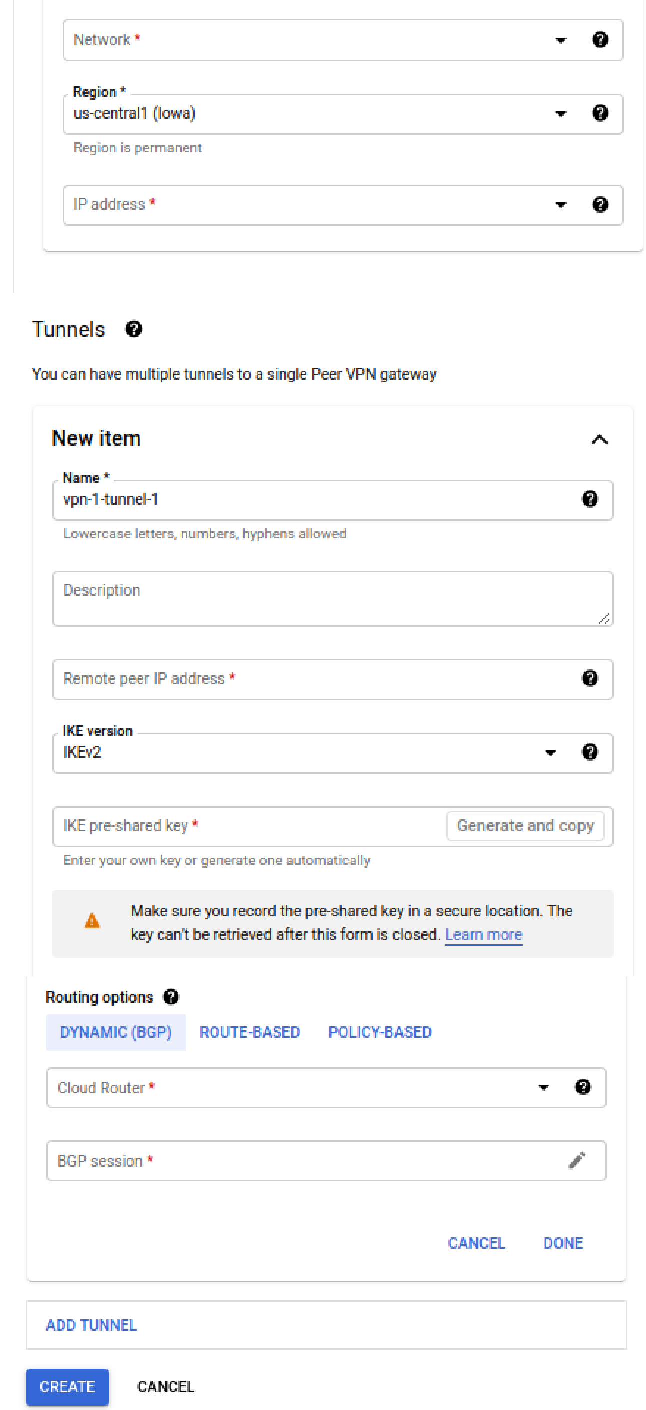


A virtual private network lets you securely connect your Google Compute Engine resources to your own private network. Google VPN uses IKEv1 or IKEv2 to establish the IPSec connectivity. Learn more

Google Compute Engine VPN gateway

Name *
vpn-1
Lowercase letters, numbers, hyphens allowed

Description



Network *

Region *
us-central1 (Iowa)
Region is permanent

IP address *

Tunnels

You can have multiple tunnels to a single Peer VPN gateway

New item

Name *
vpn-1-tunnel-1
Lowercase letters, numbers, hyphens allowed

Description

Remote peer IP address *

IKE version
IKEv2

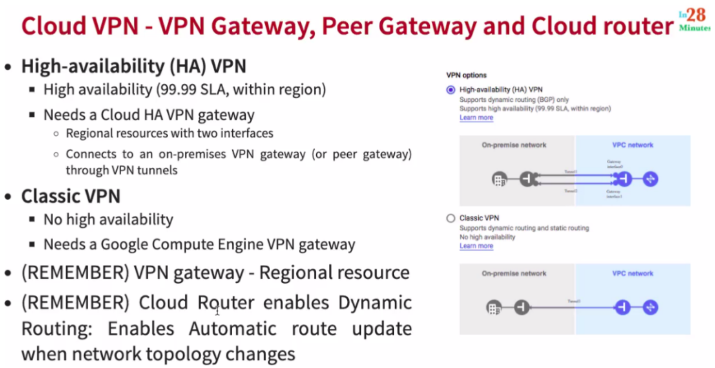
IKE pre-shared key *
Enter your own key or generate one automatically

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

Cloud Router *

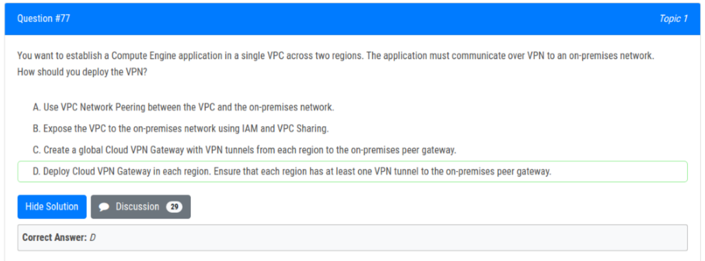
BGP session *



Cloud VPN - VPN Gateway, Peer Gateway and Cloud router

- High-availability (HA) VPN
  - High availability (99.99 SLA, within region)
  - Needs a Cloud HA VPN gateway
    - Regional resources with two interfaces
    - Connects to an on-premises VPN gateway (or peer gateway) through VPN tunnels
- Classic VPN
  - No high availability
  - Needs a Google Compute Engine VPN gateway
- (REMEMBER) VPN gateway - Regional resource
- (REMEMBER) Cloud Router enables Dynamic Routing: Enables Automatic route update when network topology changes

In28 Minutes
VPN options
● High-availability (HA) VPN
Supports dynamic routing (BGP) only
Supports high availability (99.99 SLA, within region)
Learn more
On-premise network
VPC network
○ Classic VPN
Supports dynamic routing and static routing
No high availability
Learn more
On-premise network
VPC network



Question #77 Topic 1

You want to establish a Compute Engine application in a single VPC across two regions. The application must communicate over VPN to an on-premises network.
How should you deploy the VPN?

A. Use VPC Network Peering between the VPC and the on-premises network.

B. Expose the VPC to the on-premises network using IAM and VPC Sharing.

C. Create a global Cloud VPN Gateway with VPN tunnels from each region to the on-premises peer gateway.

D. Deploy Cloud VPN Gateway in each region. Ensure that each region has at least one VPN tunnel to the on-premises peer gateway.

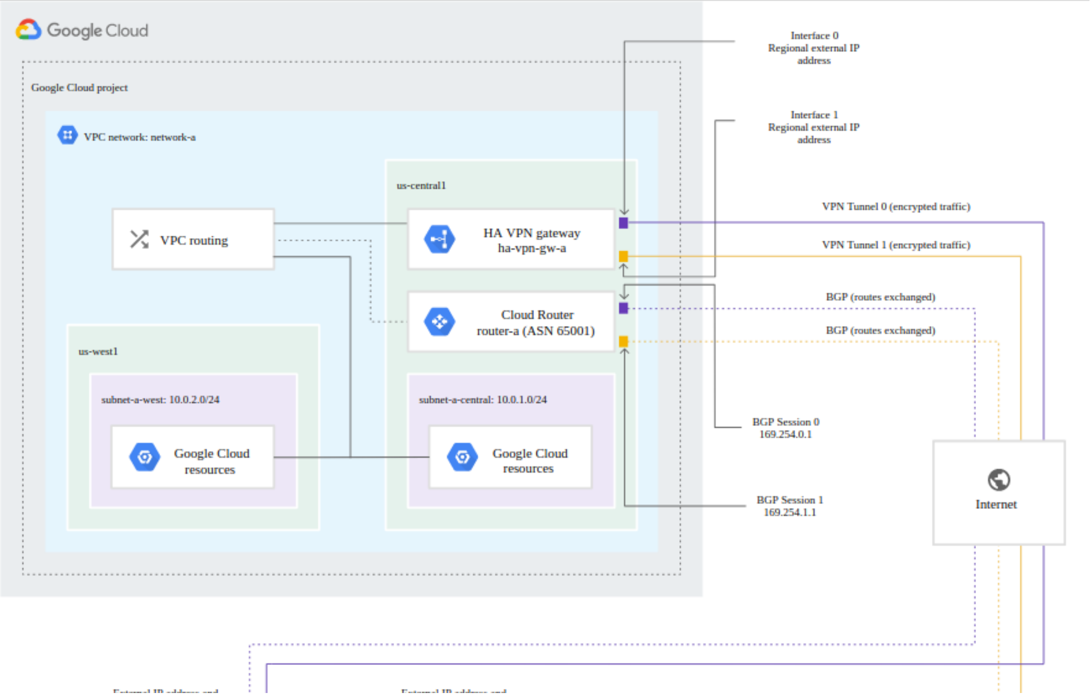
Correct Answer: *D*

HA VPN Requirement

HA VPN requirements

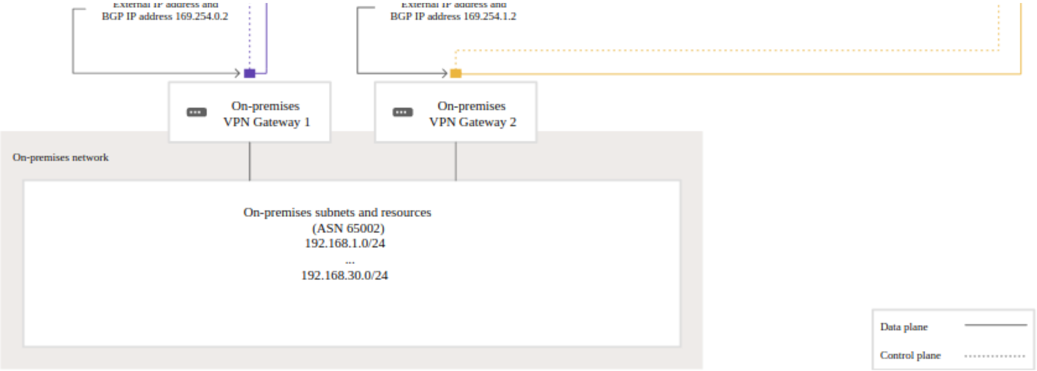
Your Cloud VPN configuration must meet the following requirements to achieve a service-level availability of 99.99% for HA VPN:

- When you connect an HA VPN gateway to your peer gateway, 99.99% availability is guaranteed only on the Google Cloud side of the connection. End-to-end availability is subject to proper configuration of the peer VPN gateway.
- If both sides are Google Cloud gateways and are properly configured, end-to-end 99.99% availability is guaranteed.
- **To achieve high availability when both VPN gateways are located in VPC networks, you must use two HA VPN gateways, and both of them must be located in the same region.**
  Even though both gateways must be located in the same region, if your VPC network uses *global dynamic routing mode*, the routes to the subnets that the gateways share with each other can be located in any region. If your VPC network uses *regional dynamic routing mode*, only routes to subnets in the same region are shared with the peer network. Learned routes are applied only to subnets in the same region as the VPN tunnel.
  For more information, see Dynamic routing mode.
- HA VPN rejects Google Cloud IP addresses when they are configured in an external VPN gateway resource—for example, using the external IP address of a VM instance as the external IP address for the external VPN gateway resource. The only supported HA VPN topology between Google Cloud networks is where HA VPN is



used on both sides, as documented in Creating an HA VPN between Google Cloud networks.

- Configure two VPN tunnels from the perspective of the Cloud VPN gateway:
  - If you have *two peer VPN gateway devices*, each of the tunnels from each interface on the Cloud VPN gateway must be connected to its own peer gateway.
  - If you have *a single peer VPN gateway device with two interfaces*, each of the tunnels from each interface on the Cloud VPN gateway must be connected to its own interface on the peer gateway.
  - If you have *a single peer VPN gateway device with a single interface*, both of the tunnels from each interface on the Cloud VPN gateway must be connected to the same interface on the peer gateway.
- A peer VPN device must be configured with adequate redundancy. The device vendor specifies the details of an adequately redundant configuration, which might include multiple hardware instances. For details, see the vendor documentation for the peer VPN device.
  If two peer devices are required, each peer device must be connected to a different HA VPN gateway interface. If the peer side is another cloud provider like AWS, VPN connections must be configured with adequate redundancy on the AWS side as well.
- Your peer VPN gateway device must support dynamic (BGP) routing.

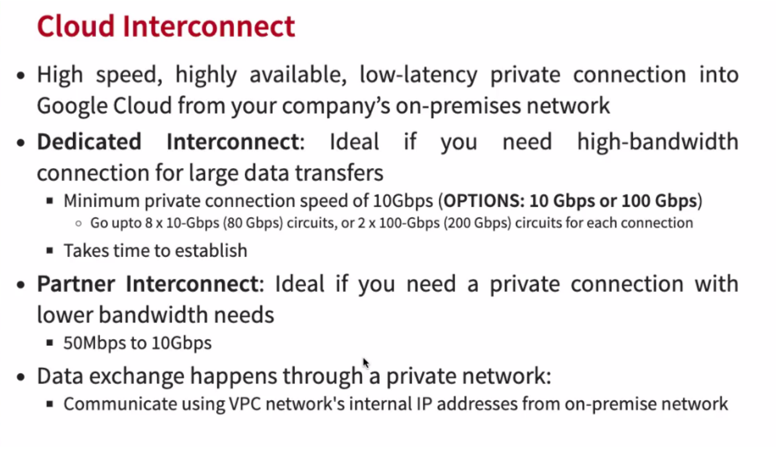

External IP address and BGP IP address 169.254.0.2
External IP address and BGP IP address 169.254.1.2
On-premises VPN Gateway 1
On-premises VPN Gateway 2
On-premises network
On-premises subnets and resources
(ASN 65002)
192.168.1.0/24
...
192.168.30.0/24
Data plane
Control plane

Active/Active and Active/Passive Configuration

If a Cloud VPN tunnel goes down, it restarts automatically. If an entire virtual VPN device fails, Cloud VPN automatically instantiates a new one with the same configuration. The new gateway and tunnel connect automatically.

VPN tunnels connected to HA VPN gateways must use dynamic (BGP) routing. Depending on the way that you configure route priorities for HA VPN tunnels, you can create an active/active or active/passive routing configuration. For both of these routing configurations, both VPN tunnels remain active.

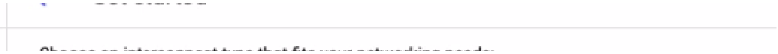
Cloud Interconnect



Cloud Interconnect

- High speed, highly available, low-latency private connection into Google Cloud from your company's on-premises network
- **Dedicated Interconnect**: Ideal if you need high-bandwidth connection for large data transfers
  - Minimum private connection speed of 10Gbps (**OPTIONS: 10 Gbps or 100 Gbps**)
    - Go upto 8 x 10-Gbps (80 Gbps) circuits, or 2 x 100-Gbps (200 Gbps) circuits for each connection
  - Takes time to establish
- **Partner Interconnect**: Ideal if you need a private connection with lower bandwidth needs
  - 50Mbps to 10Gbps
- Data exchange happens through a private network:
  - Communicate using VPC network's internal IP addresses from on-premise network

Create Interconnect



Dedicated Interconnect Redundancy

If you have a single Dedicated Interconnect connection, you can create a second one so that you have redundant connections. Google recommends redundancy so that if one connection fails, the other connection can continue to serve traffic.

To create a redundant Interconnect connection, you must create it in the same metropolitan area (city) as the existing one, but in a different edge availability domain (metro availability zone). If you don't, the connections won't be redundant.

When there is a requirement to upload a file of size 10TB Dedicated interconnect is always better as with normal internet connection for example 100MBPs it will take 27hrs to upload.

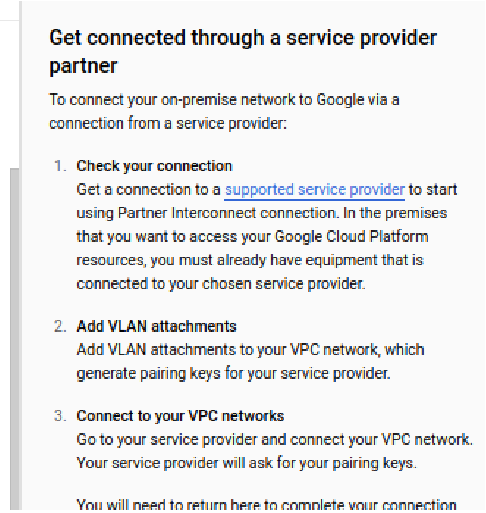
Direct Peering exists outside of Google Cloud. Unless you need to access Google Workspace applications, the recommended methods of access to Google Cloud are Dedicated Interconnect or Partner Interconnect.

Edge availaibility domain: Each metropolitan area has at least two zones called *edge availability domains*. These domains provide isolation during scheduled maintenance, which means that two domains in the same metro are not down for maintenance at the same time. This isolation is important when you're building for redundancy.

Partner Interconnect Redundancy

99.99% availability requires at least four VLAN attachments across two metros, one in each edge availability domain (metro availability zone). You also need two Cloud Routers (one in each Google Cloud region of a VPC network). Associate one Cloud Router with each pair of VLAN attachments. You must also enable global routing for the VPC network.

Partner Interconnect Connection Process



Get connected through a service provider partner

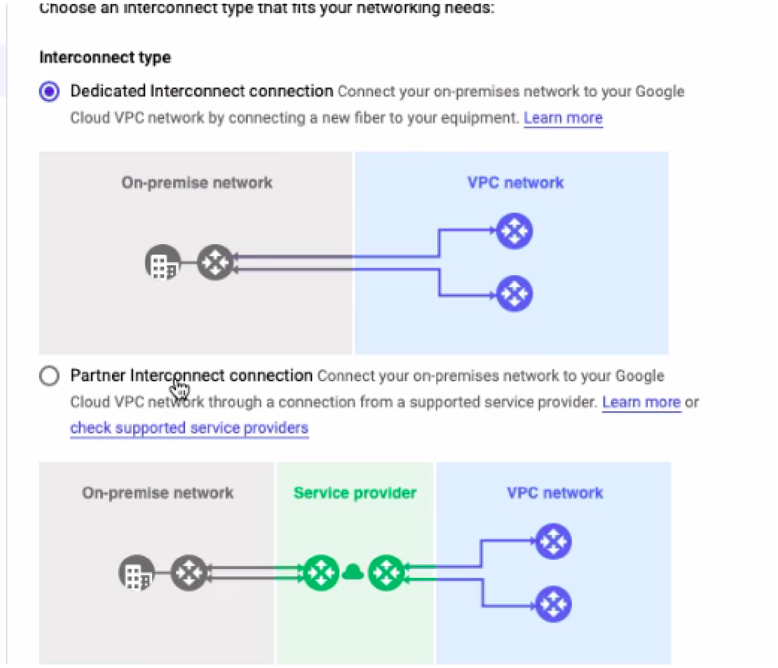
To connect your on-premise network to Google via a connection from a service provider:

1. Check your connection
   Get a connection to a supported service provider to start using Partner Interconnect connection. In the premises that you want to access your Google Cloud Platform resources, you must already have equipment that is connected to your chosen service provider.

2. Add VLAN attachments
   Add VLAN attachments to your VPC network, which generate pairing keys for your service provider.

3. Connect to your VPC networks
   Go to your service provider and connect your VPC network. Your service provider will ask for your pairing keys.

   You will need to return here to complete your connection

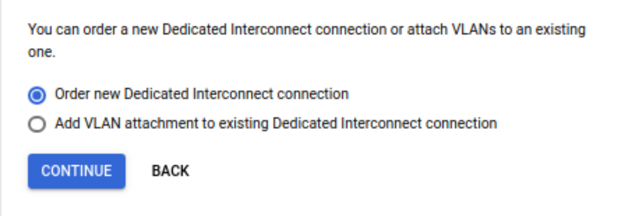


Choose an interconnect type that fits your networking needs:

Interconnect type

● Dedicated Interconnect connection Connect your on-premises network to your Google Cloud VPC network by connecting a new fiber to your equipment. Learn more

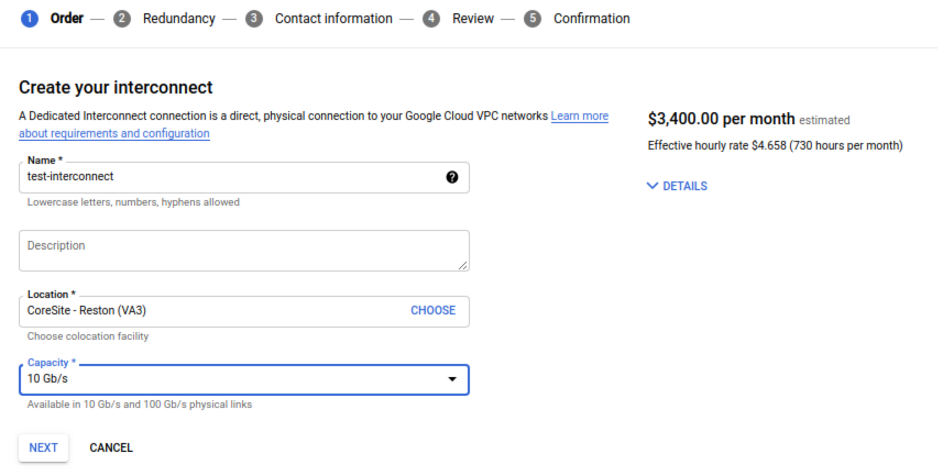
○ Partner Interconnect connection Connect your on-premises network to your Google Cloud VPC network through a connection from a supported service provider. Learn more or check supported service providers



You can order a new Dedicated Interconnect connection or attach VLANs to an existing one.

● Order new Dedicated Interconnect connection

○ Add VLAN attachment to existing Dedicated Interconnect connection



1 Order — 2 Redundancy — 3 Contact information — 4 Review — 5 Confirmation

Create your interconnect

A Dedicated Interconnect connection is a direct, physical connection to your Google Cloud VPC networks Learn more about requirements and configuration

Name *
test-interconnect
Lowercase letters, numbers, hyphens allowed

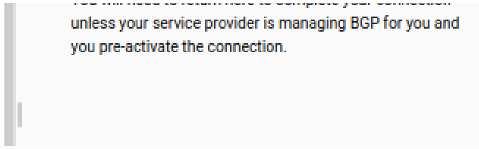
Description

Location *
CoreSite - Reston (VA3)
Choose colocation facility

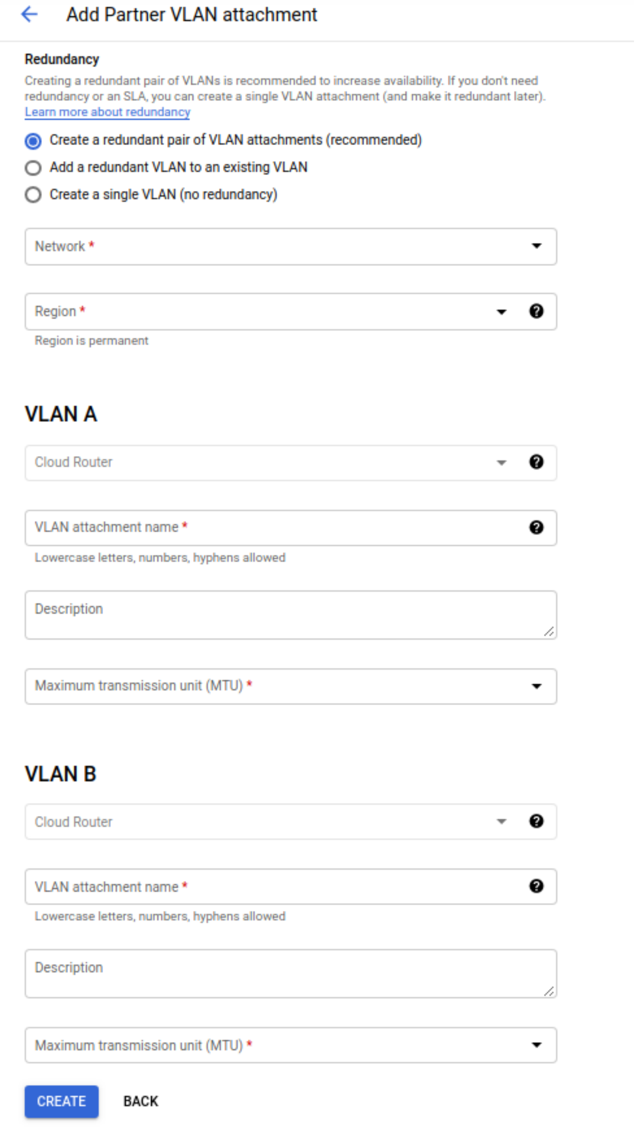
Capacity *
10 Gb/s
Available in 10 Gb/s and 100 Gb/s physical links

$3,400.00 per month estimated

Effective hourly rate $4.658 (730 hours per month)



You will need to return here to complete your connection unless your service provider is managing BGP for you and you pre-activate the connection.



← Add Partner VLAN attachment

Redundancy

Creating a redundant pair of VLANs is recommended to increase availability. If you don't need redundancy or an SLA, you can create a single VLAN attachment (and make it redundant later).
Learn more about redundancy

- ● Create a redundant pair of VLAN attachments (recommended)
- ○ Add a redundant VLAN to an existing VLAN
- ○ Create a single VLAN (no redundancy)

Network *

Region *
Region is permanent

VLAN A

Cloud Router

VLAN attachment name *
Lowercase letters, numbers, hyphens allowed

Description

Maximum transmission unit (MTU) *

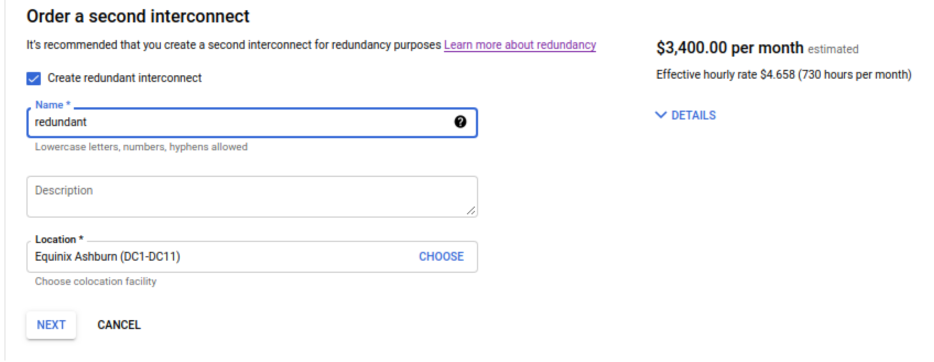
VLAN B

Cloud Router

VLAN attachment name *
Lowercase letters, numbers, hyphens allowed

Description

Maximum transmission unit (MTU) *



Order a second interconnect

It's recommended that you create a second interconnect for redundancy purposes Learn more about redundancy

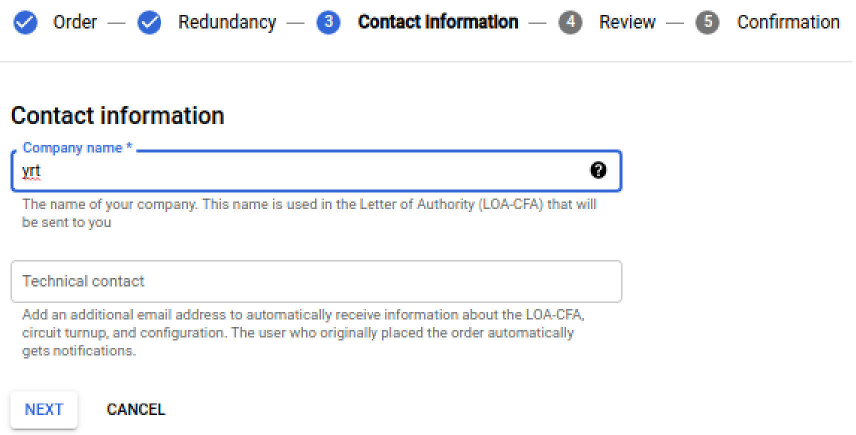
☑ Create redundant interconnect

Name *: redundant
Lowercase letters, numbers, hyphens allowed

Description

Location *: Equinix Ashburn (DC1-DC11)
Choose colocation facility

$3,400.00 per month estimated
Effective hourly rate $4.658 (730 hours per month)

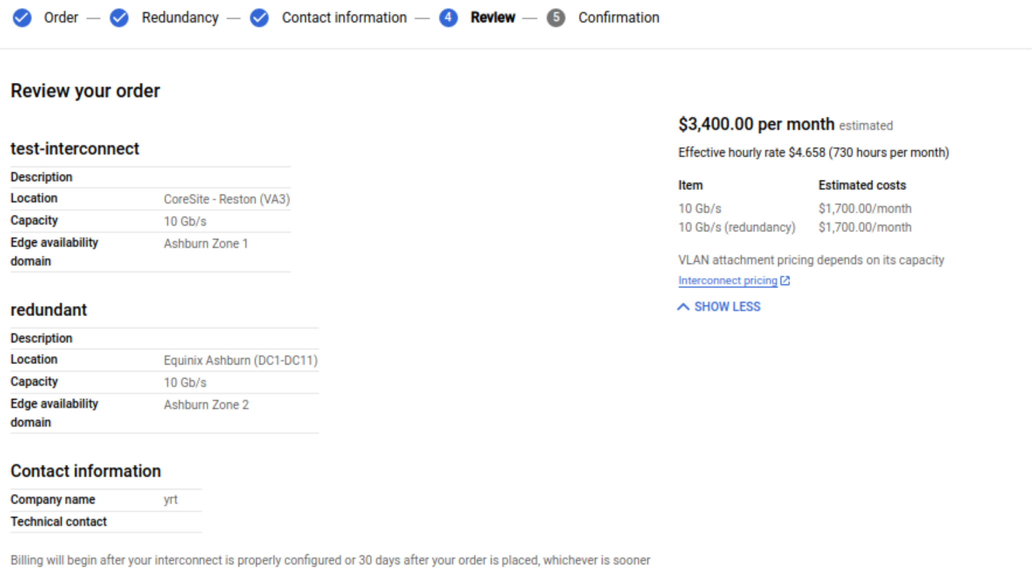


Order — Redundancy — 3 Contact information — 4 Review — 5 Confirmation

Contact information

Company name *: yrt
The name of your company. This name is used in the Letter of Authority (LOA-CFA) that will be sent to you

Technical contact
Add an additional email address to automatically receive information about the LOA-CFA, circuit turnup, and configuration. The user who originally placed the order automatically gets notifications.



Order — Redundancy — Contact information — 4 Review — 5 Confirmation

Review your order

test-interconnect

Description	
Location	CoreSite - Reston (VA3)
Capacity	10 Gb/s
Edge availability domain	Ashburn Zone 1

redundant

Description	
Location	Equinix Ashburn (DC1-DC11)
Capacity	10 Gb/s
Edge availability domain	Ashburn Zone 2

Contact information

Company name	yrt
Technical contact	

Billing will begin after your interconnect is properly configured or 30 days after your order is placed, whichever is sooner

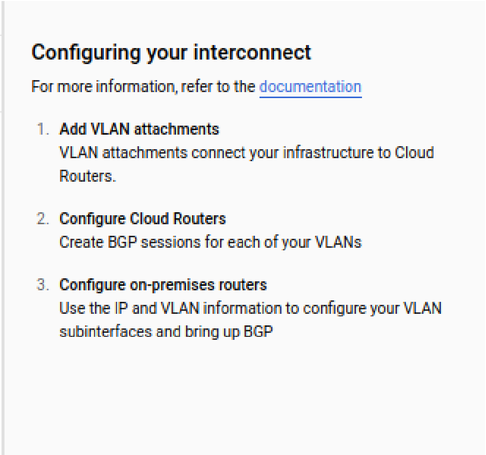
$3,400.00 per month estimated
Effective hourly rate $4.658 (730 hours per month)

Item	Estimated costs
10 Gb/s	$1,700.00/month
10 Gb/s (redundancy)	$1,700.00/month

VLAN attachment pricing depends on its capacity
Interconnect pricing

VLAN Attachment

VLAN attachments (also known as interconnectAttachments) determine which Virtual Private Cloud (VPC) networks can reach your on-premises network through a Dedicated Interconnect connection. You can create VLAN attachments over connections that have passed all tests and are ready to use.

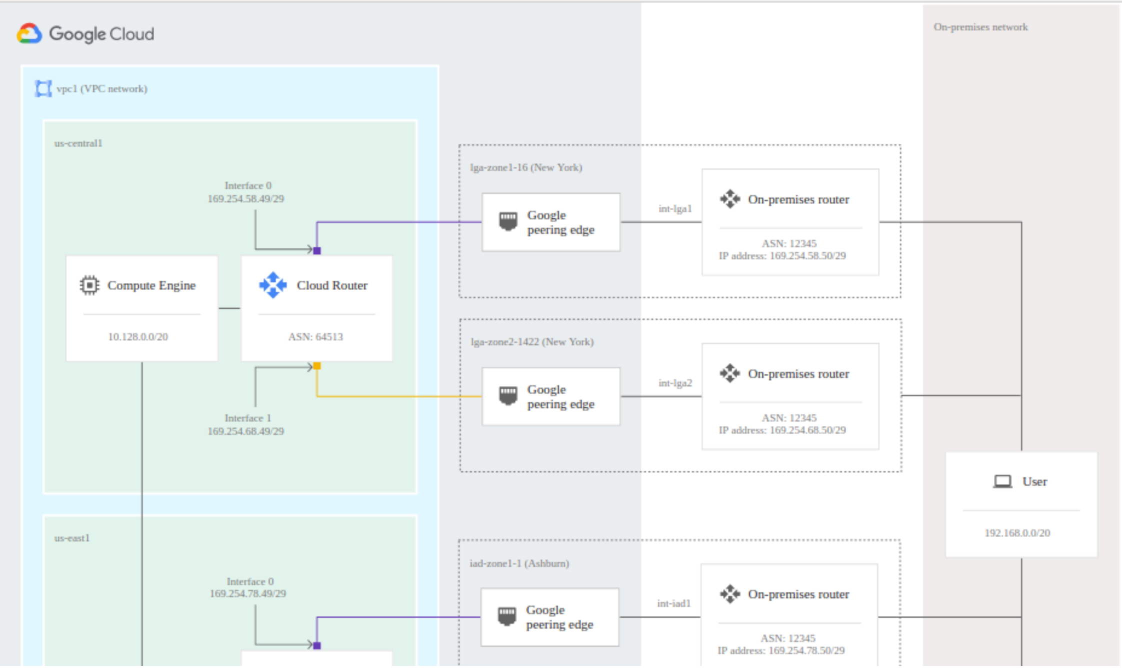


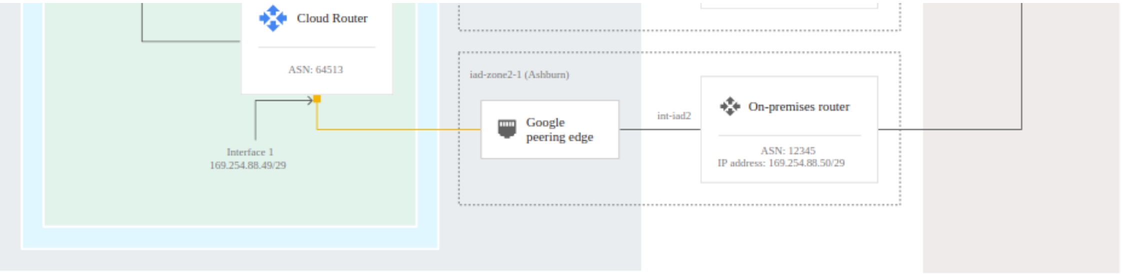
Configuring your interconnect

For more information, refer to the documentation

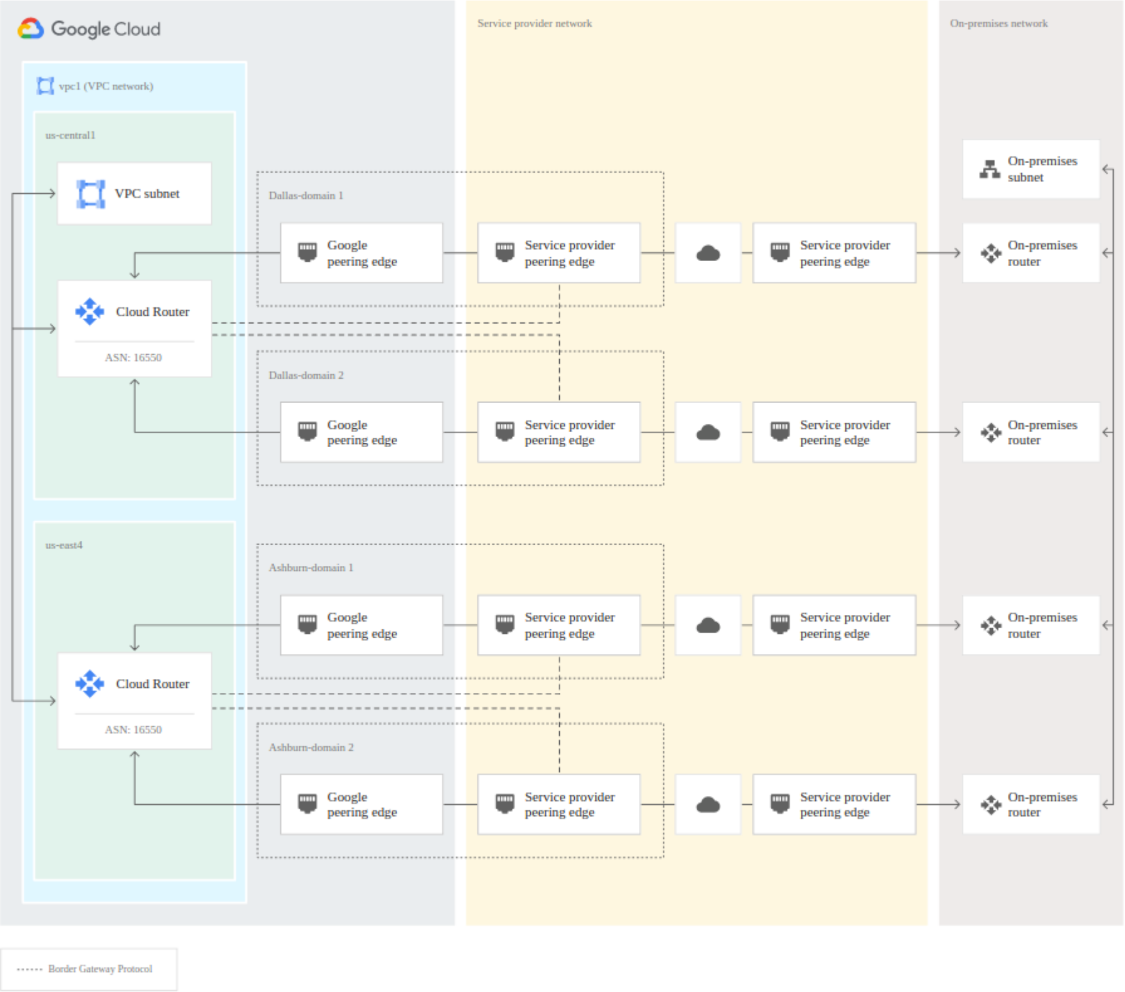
1. **Add VLAN attachments**
   VLAN attachments connect your infrastructure to Cloud Routers.
2. **Configure Cloud Routers**
   Create BGP sessions for each of your VLANs
3. **Configure on-premises routers**
   Use the IP and VLAN information to configure your VLAN subinterfaces and bring up BGP

Dedicated interconnect redundant setup

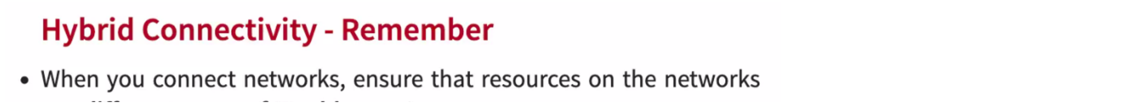




Partner Interconnect Redundancy

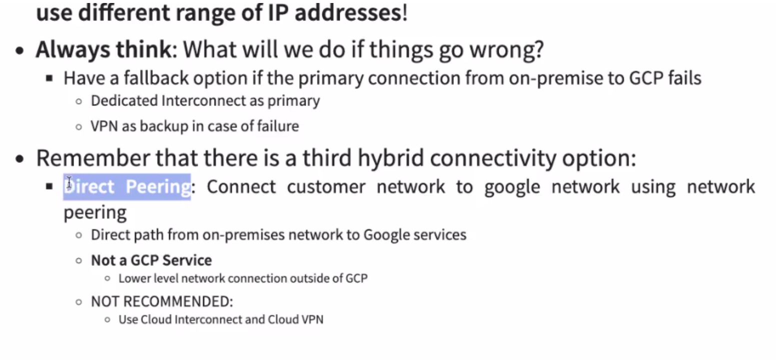


Hybrid Connection Best Practice



Hybrid Connectivity - Remember

- When you connect networks, ensure that resources on the networks

	 **use different range of IP addresses!** • **Always think:** What will we do if things go wrong? ▪ Have a fallback option if the primary connection from on-premise to GCP fails ○ Dedicated Interconnect as primary ○ VPN as backup in case of failure • Remember that there is a third hybrid connectivity option: ▪ Direct Peering: Connect customer network to google network using network peering ○ Direct path from on-premises network to Google services ○ **Not a GCP Service** ○ Lower level network connection outside of GCP ○ NOT RECOMMENDED: ○ Use Cloud Interconnect and Cloud VPN
Access google private servicesfrom on-promise "You must configure routes so that Google API traffic is forwarded through your Cloud VPN or Cloud Interconnect connection, firewall rules on your on-premises firewall to allow the outgoing traffic, and DNS so that traffic to Google APIs resolves to the IP range you've added to your routes." "You can use Cloud Router Custom Route Advertisement to announce the Restricted Google APIs IP addresses through Cloud Router to your on-premises network. The Restricted Google APIs IP range is 199.36.153.4/30. While this is technically a public IP range, Google does not announce it publicly. This IP range is only accessible to hosts that can reach your Google Cloud projects through internal IP ranges, such as through a Cloud VPN or Cloud Interconnect connection."	