Cloud VPN (https://cloud.google.com/vpn/)
Documentation (https://cloud.google.com/vpn/docs/) Guides

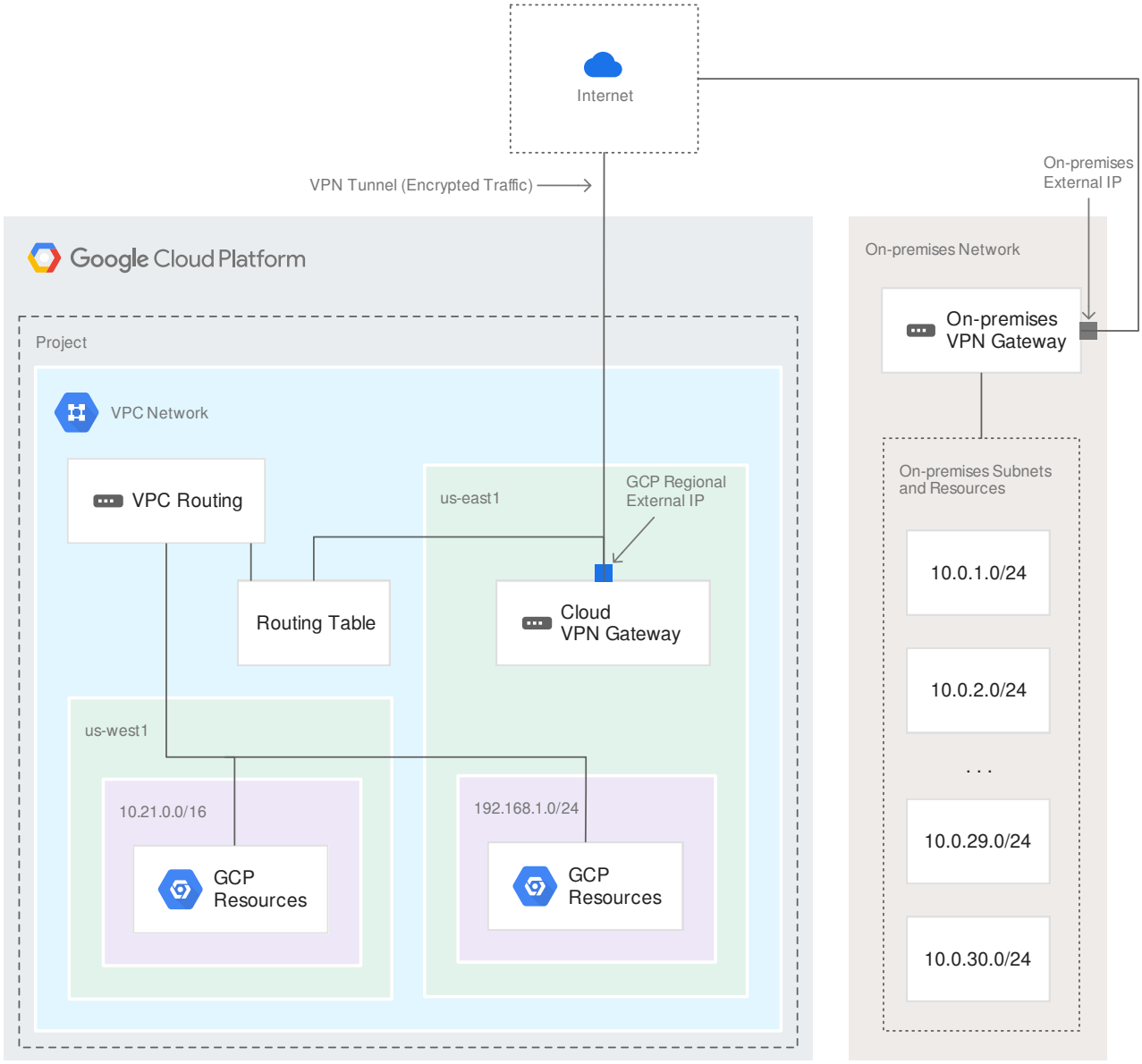
Classic VPN topologies

With Classic VPN, your on-premises hosts communicate through one or more IPsec VPN tunnels to Compute Engine Virtual Machine (VM) instances in your project's VPC networks.

Classic VPN supports site-to-site VPN as the simple topology shown below or with redundancy options (#redundancy-options).

Note: For information about HA VPN topologies, see the Cloud VPN Topologies page (https://cloud.google.com/vpn/docs/concepts/topologies).

The following diagram shows a simple VPN connection (https://cloud.google.com/vpn/docs/concepts/overview#connection) between a Classic VPN gateway and your peer (https://cloud.google.com/vpn/docs/concepts/overview/#peer-definition) VPN gateway.



(https://cloud.google.com/vpn/images/cloud-vpn-overview-01.svg)
VPN diagram (click to enlarge)

Redundancy and failover options

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.

Option 1: Moving to HA VPN

If your peer VPN gateway supports BGP (https://cloud.google.com/vpn/docs/concepts/overview#bgp-definition), the recommended option is to move to a highly-available (HA) Cloud VPN gateway (https://cloud.google.com/vpn/docs/how-to/moving-to-ha-vpn).

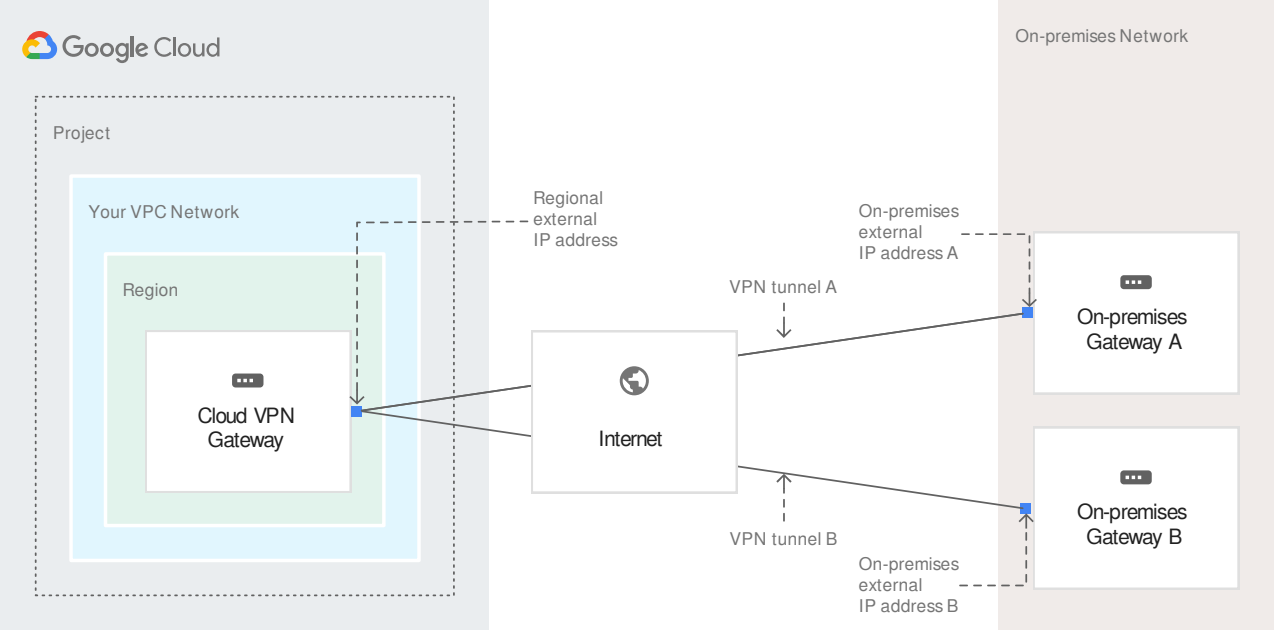
Option 2: Using a second peer VPN gateway

For Classic VPN, if your on-premises side is hardware based, having a second peer VPN gateway provides redundancy and failover on that side of the connection. A second physical gateway allows you to take one of the gateways offline for software upgrades or other scheduled maintenance. It also protects you in case of an outright failure in one of the devices.

To configure a tunnel from your Cloud VPN gateway to a second on-premises-side VPN gateway, do the following:

1. Configure a second on-premises VPN gateway and a tunnel.
2. Set up a second tunnel on your Cloud VPN gateway pointing to the second on-premises gateway.
3. Forward the same routes for the second tunnel as you did for the first. If you want both tunnels to balance traffic, set their route priorities (https://cloud.google.com/vpc/docs/routes) to be the same. If you want one tunnel to be primary, set a lower priority on the second tunnel.
4. If either VPN tunnel fails due to network issues along the path, or a problem with an on-premises gateway, the Cloud VPN gateway will continue sending traffic over the healthy tunnel and will automatically resume using both tunnels once the failed tunnel recovers.

For details about configuring redundancy with dynamic routing, see the Cloud Router redundancy page (https://cloud.google.com/router/docs/concepts/overview#redundant_cloud_vpn_tunnels).



(https://cloud.google.com/vpn/images/vpn-basic-2-on-prem.svg)
Redundant on-premises VPN gateways diagram (click to enlarge)

Increased throughput and load balancing options

Note: the solutions in this section for increasing throughput can be also used to load balance between two gateways as described for each option.

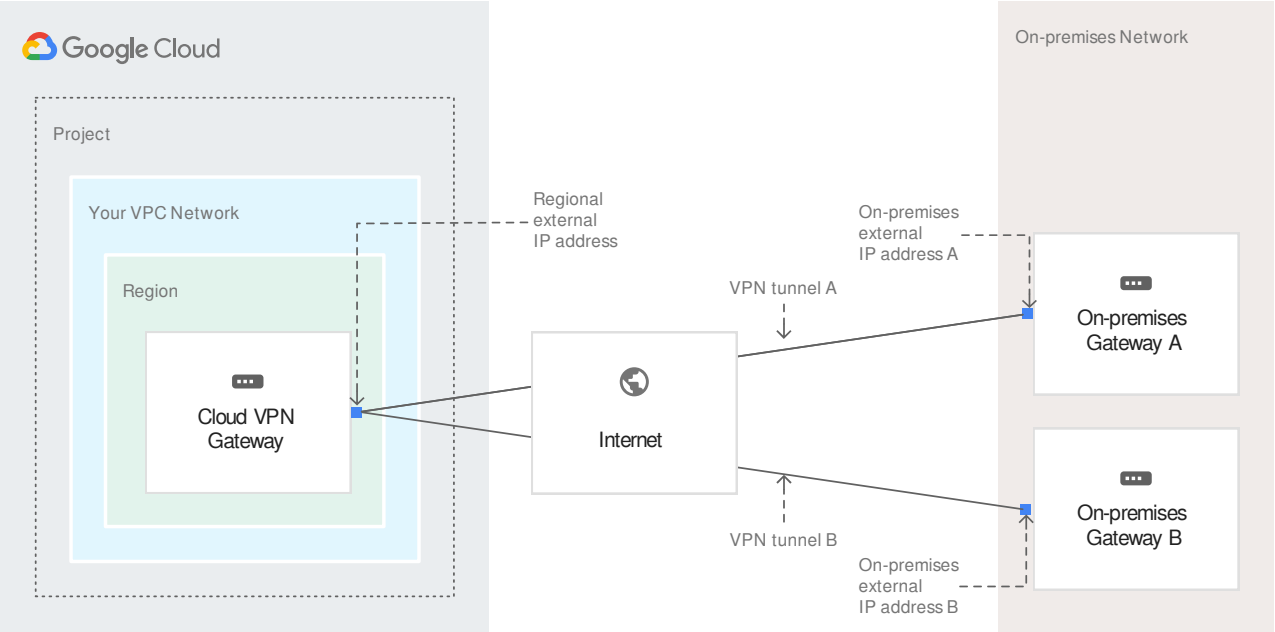
For information about VPN bandwidth, see the VPN Overview (https://cloud.google.com/vpn/docs/concepts/overview#network-bandwidth) and Calculating network throughput (https://cloud.google.com/community/tutorials/network-throughput).

There are three options for scaling a Cloud VPN configuration:

- Option 1: Scale the on-premises VPN gateway.
- Option 2: Scale the Cloud VPN gateway. If your on-premises VPN gateway's throughput capabilities are higher, and you want to scale higher throughput from the Cloud VPN gateway, you can set up a second Cloud VPN gateway.
- Option 3: Scale both the on-premises VPN gateway and the Cloud VPN gateway.

Option 1: Scale the on-premises VPN gateway

Set up a second on-premises VPN gateway device with a different public IP address. Create a second tunnel on your existing Cloud VPN gateway that forwards the same IP range, but pointing at the second on-premises gateway IP. Your Cloud VPN gateway automatically load balances between the configured tunnels. You can set up the VPN gateways to have multiple tunnels load balanced this way to increase the aggregate VPN connectivity throughput.

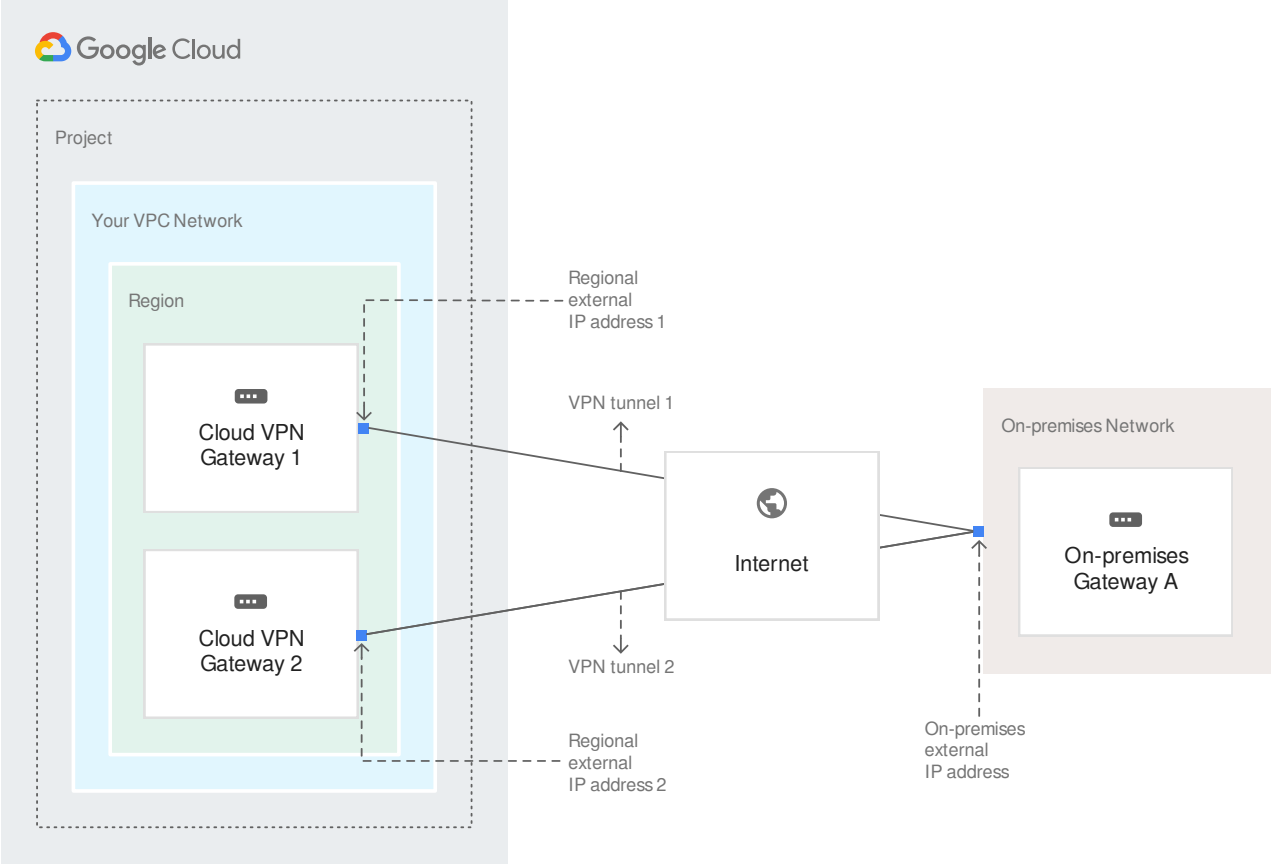


(https://cloud.google.com/vpn/images/vpn-basic-2-on-prem.svg)
Redundant on-premises VPN gateways diagram (click to enlarge)

Option 2: Scale the Cloud VPN gateway

Note: This configuration requires an on-premises VPN gateway that supports using equal-cost multi-path routing (ECMP (https://wikipedia.org/wiki/Equal-cost_multi-path_routing)) between two tunnels having the same on-premises IP ranges. Many software VPNs are not capable of this.

Add a second Cloud VPN gateway in the same region as the existing VPN gateway. The second Cloud VPN gateway can have a tunnel that points to the same IP address of the on-premises VPN gateway as the tunnel on the first gateway. Once configured, traffic to the on-premises VPN gateway is automatically load balanced between the two Cloud VPN gateways and tunnels.

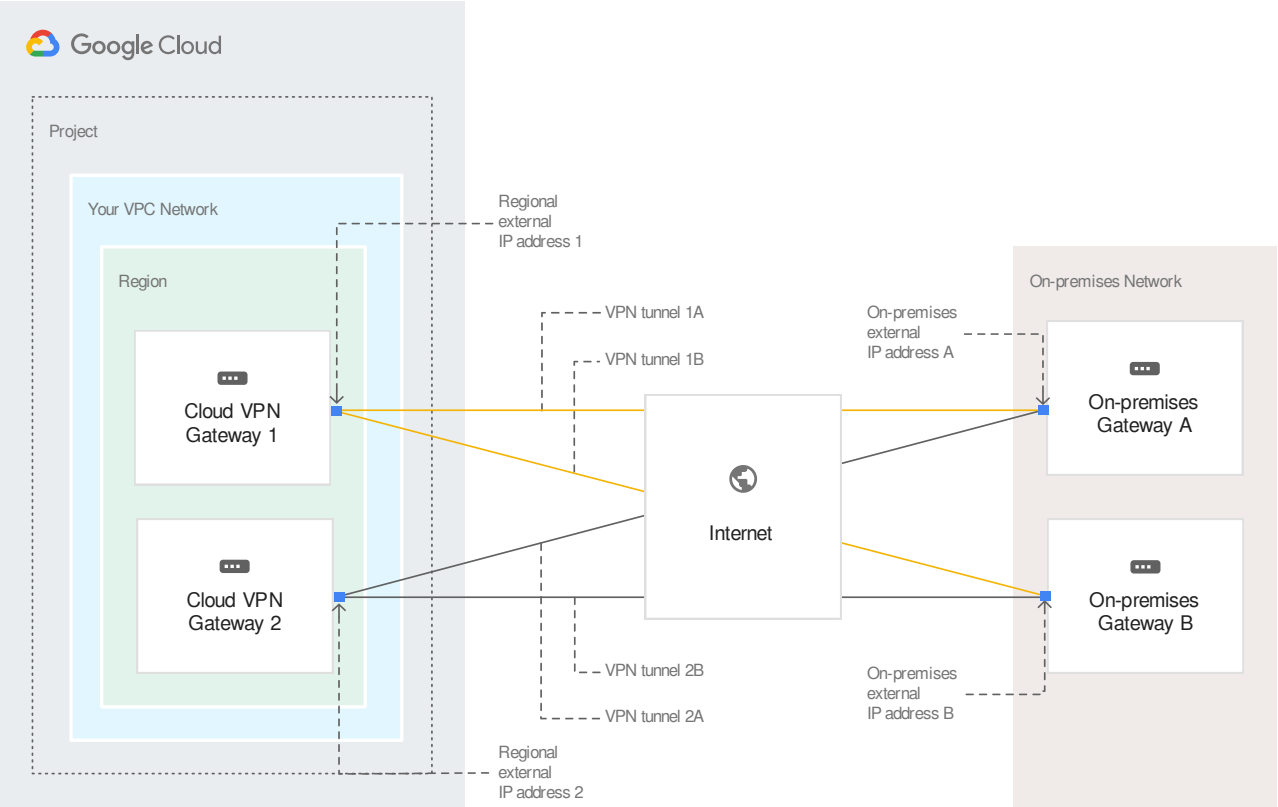


(https://cloud.google.com/vpn/images/vpn-basic-2-cloud-vpn.svg)
Redundant Cloud VPN gateways diagram (click to enlarge)

Option 3: Scale both the on-premises VPN gateway and the Cloud VPN gateway

Note: This configuration requires an on-premises VPN gateway that supports using equal-cost multi-path routing (ECMP (https://wikipedia.org/wiki/Equal-cost_multi-path_routing)) between two tunnels having the same on-premises IP ranges. Many software VPNs are not capable of this.

Combine options 1 and 2 mentioned above to scale throughput. If you have two on-premises VPN gateways and two Cloud VPN gateways, each Cloud VPN gateway can have a tunnel pointing at each on-premises VPN gateway public IP, giving you four load balanced tunnels between the VPN gateway, thereby potentially providing four times the bandwidth.



(https://cloud.google.com/vpn/images/vpn-basic-2-cloud-on-prem.svg)
Redundant Cloud VPN and on-premises VPN gateways diagram (click to enlarge)

For more information, see the tutorial Building high-throughput VPNs (https://cloud.google.com/solutions/building-high-throughput-vpns). You can increase the number of tunnels up to your project's quota. ECMP is used to balance traffic between tunnels.

What's next

More VPN concepts

For additional information on Cloud VPN concepts, use the navigation arrows at the bottom of the page to move to the next concept or use the following links:

- Learn about the basic concepts of Cloud VPN (https://cloud.google.com/vpn/docs/concepts/overview)
- Choosing VPN over other hybrid connectivity solutions (https://cloud.google.com/vpn/docs/concepts/choosing-a-hybrid-solution)

- Choosing a VPC network type and routing option (https://cloud.google.com/vpn/docs/concepts/choosing-networks-routing)
- Learn about MTU considerations (https://cloud.google.com/vpn/docs/concepts/mtu-considerations)

VPN related

- Create a custom Virtual Private Cloud network (https://cloud.google.com/vpc/docs/using-vpc#create-custom-network)
- Set up different types of Cloud VPN (https://cloud.google.com/vpn/docs/how-to/choosing-a-vpn)
- Maintain VPN tunnels and gateways (https://cloud.google.com/vpn/docs/how-to/maintaining-vpns)
- See Advanced Configurations (https://cloud.google.com/vpn/docs/concepts/advanced) for information on high-availability, high-throughput scenarios, or multiple subnet scenarios.
- View logs and monitoring metrics (https://cloud.google.com/vpn/docs/how-to/viewing-logs-metrics)
- Get troubleshooting help (https://cloud.google.com/vpn/docs/support/troubleshooting)

Previous
← MTU considerations (https://cloud.google.com/vpn/docs/concepts/mtu-considerations)

Last updated September 27, 2019.