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

Advanced configurations

This page describes advanced configuration details necessary for high-availability, high throughput, or multiple subnet VPN scenarios. The Cloud VPN overview (https://cloud.google.com/vpn/docs/concepts/overview) describes the basic concepts of Cloud VPN.

Advanced settings and configurations

While you can configure the VPN types described in Choosing a VPN routing option (https://cloud.google.com/vpn/docs/how-to/choosing-a-vpn) using only the steps outlined in the set-up instructions, the more advanced configurations listed above require additional details.

Order of routes

It is possible to create a VPN tunnel that has the same IP range as another tunnel, a subset of the other tunnel's range, or a superset of the other tunnel's range.

For details, see Configuring VPN tunnels with overlapping IP ranges (https://cloud.google.com/vpn/docs/concepts/order-of-routes).

Configuring IKE, including multiple subnet support

You can view detailed information about how Cloud VPN supports multiple IKE ciphers at Supported IKE ciphers (https://cloud.google.com/vpn/docs/concepts/supported-ike-ciphers).

You can view detailed information about how Cloud VPN supports multiple IP ranges in each traffic selector

(https://cloud.google.com/vpn/docs/concepts/choosing-networks-routing#static-routing-networks) when
using IKEv2 at Multiple IP ranges
 (https://cloud.google.com/vpn/docs/concepts/choosing-networks-routing#ts-ip-ranges) in Networks
and tunnel routing (https://cloud.google.com/vpn/docs/concepts/choosing-networks-routing).

UDP encapsulation

Cloud VPN *only* supports one-to-one NAT via UDP encapsulation for NAT-Traversal (NAT-T).
One-to-many NAT and port-based address translation are *not* supported. In other words, Cloud
VPN *cannot* connect to multiple peer
 (https://cloud.google.com/vpn/docs/concepts/overview#peer-definition) VPN gateways that share a
single public IP address.

When using one-to-one NAT, a peer VPN gateway *must* be configured to identify itself using a
public IP address, not its internal (private) address. When you configure a Cloud VPN tunnel to
connect to a peer VPN gateway, you specify an external IP address. Cloud VPN expects an on-
premises VPN gateway to use its external IP address for its identity.

For more details about VPN gateways behind one-to-one NAT, refer to the troubleshooting page
 (https://cloud.google.com/vpn/docs/support/troubleshooting#gateways_behind_nat).

Maximum Transfer Unit (MTU) considerations

The Cloud VPN MTU size is 1460. See MTU Considerations
 (https://cloud.google.com/vpn/docs/concepts/mtu-considerations) for a description of how to
configure your peer VPN gateway to support this MTU size, if required.

High availability, failover, and higher-throughput VPNs

HA VPN is the recommended method of implementing highly-available and higher-throughput
VPNs. If your peer VPN gateway supports BGP, you can configure an HA VPN gateway with a
99.99% uptime SLA (https://cloud.google.com/vpn/docs/concepts/topologies) using an active/active
or active/passive (https://cloud.google.com/vpn/docs/concepts/overview#active) tunnel
configuration.

Caution: It is recommended that you use an Active/Passive configuration only with **one** HA VPN gateway. If
you use an Active/Passive configuration across **multiple HA VPN gateways**, with an active and passive

tunnel pair configured on each gateway, HA VPN doesn't use the passive tunnels for failover until all of the active tunnels on all gateways have failed. Configuring multiple gateways with an Active/Passive configuration can cause bandwidth loss.

For Classic VPN gateways, you can provide VPN redundancy and failover by using these options (https://cloud.google.com/vpn/docs/concepts/classic-topologies#vpn-throughput). However, you receive a 99.9% availability SLA for this configuration.

What's next?

- Learn about the basic concepts of Cloud VPN
  (https://cloud.google.com/vpn/docs/concepts/overview)

- 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)

- 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)

Next

Order of routes (https://cloud.google.com/vpn/docs/concepts/order-of-routes)