Order of routes

This page describes how routes for Cloud VPN tunnels are interpreted in VPC and legacy networks. Review the Routes Overview (https://cloud.google.com/vpc/docs/routes) for important background information about routes in Google Cloud. This document assumes that you understand route applicability and order (https://cloud.google.com/vpc/docs/routes#instancerouting).

VPN routes

VPN routes define an *egress* path for traffic leaving your Google Cloud network:

- Cloud Router manages routes for each Cloud VPN tunnel that uses dynamic routing (https://cloud.google.com/vpn/docs/concepts/choosing-networks-routing#dynamic-routing). These routes cannot be edited or removed manually. The Cloud Router associated with the tunnel, based on the BGP advertisements of the peer VPN gateway, automatically creates and removes routes with destinations to peer (https://cloud.google.com/vpn/docs/concepts/overview#peer-definition) networks. The next hop for a dynamic route is the BGP IP address of the peer.
- Google Cloud creates a static route with a matching destination for each IP range in the remote traffic selector if you use the Cloud Console to create tunnels using one of the following Classic VPN gateways:
    - policy-based routing (https://cloud.google.com/vpn/docs/concepts/choosing-networks-routing#static-routing)
    - route-based VPNs (https://cloud.google.com/vpn/docs/concepts/choosing-networks-routing#static-routing) If you use `gcloud` commands to create VPN tunnels, you must manually create the

corresponding static routes. The next hop for a VPN static route is the appropriate Cloud VPN tunnel.

Routing examples

Google Cloud follows a specific procedure for selecting the next hop for a packet. The following examples illustrate how VPN routes work in conjunction with subnet routes. For more information about how Google Cloud selects a specific route, see Routing order (https://cloud.google.com/vpc/docs/routes#routeselection) in the VPC documentation.

In each example, `10.2.0.0/16` represents an on-premises network IP address range:

- **Google Cloud subnet with the same IP range**: If your Google Cloud network contains a subnet using the `10.2.0.0/16` range, Google Cloud does the following:
  - For a Cloud VPN tunnel that uses policy-based routing or route-based VPN, Google Cloud prevents you from creating a tunnel using this range if a remote traffic selector includes it.
  - For a Cloud VPN tunnel that uses dynamic routing, the associated Cloud Router ignores any advertised routes with a destination of `10.2.0.0/16`. Traffic destined for that range remains in Google Cloud.
- **Google Cloud subnet with a broader IP range**: If your Google Cloud network contains a subnet using a larger, encompassing IP range such as `10.0.0.0/8`, Google Cloud does the following:
  - For a Cloud VPN tunnel that uses policy-based routing or route-based VPN Google Cloud prevents you from creating a tunnel if a remote traffic selector includes `10.0.0.0/8` or a more specific range.
  - For a Cloud VPN tunnel that uses dynamic routing, the associated Cloud Router ignores any advertised routes with destinations that fit in `10.0.0.0/8` (including more specific ranges). All traffic destined for `10.0.0.0/8` remains in Google Cloud.
- **Google Cloud subnet with a narrower IP range**: If your Google Cloud network contains a subnet with a narrower, included IP range like `10.2.99.0/24`, you *can* create a Cloud VPN tunnel to the broader `10.2.0.0/16` range using any routing option: Traffic destined to `10.2.99.0/24` is still routed to the Google Cloud subnet. Traffic destined to `10.2.0.0/16` *but outside of* `10.2.99.0/24` (such as to `10.2.100.8`) is sent through the VPN tunnel.

With other VPN routes

If no destination is found with a subnet route, Google Cloud resolves routes for VPN tunnels in the following way:

- If the tunnel is not up, routes that use a Cloud VPN tunnel as a next hop are ignored.
- Google Cloud sends the packet to the next hop of the route with the most specific destination.
- If more than one route has the same most-specific destination, the priority of the route is used:
    - If a single route with the highest priority is available, the packet is sent to its next hop.
    - If more than one route has the same highest priority, the packet is delivered to the next hop of *either* route using ECMP. In this way, traffic is distributed among multiple next hops, so it is balanced among the applicable, available Cloud VPN tunnels. This balancing method is based on a hash, so all packets from the same flow use the same tunnel as long as that tunnel is up.

      To test ECMP behavior, use iperf3 (https://cloud.google.com/community/tutorials/network-throughput) to send multiple simultaneous TCP streams, ideally from multiple GCP VMs, through Cloud VPN tunnels.

      Using ICMP to "ping test" from one VM instance isn't sufficient to test ECMP-based egress through Cloud VPN tunnels, since only one tunnel is selected when you run `ping`. ICMP (ping) has no concept of ports and is a fixed protocol. Thus, ICMP provides a 2-tuple that contains only a source and destination IP address and that always selects a single tunnel.

When tunnels are down

When Cloud VPN tunnels are not available, Google Cloud interprets their associated routes as follows:

- If a Cloud VPN tunnel uses dynamic routing, its associated Cloud Router automatically removes the learned routes when the tunnel goes down. The learned routes are routes with a next hop of the BGP IP for the corresponding peer VPN gateway. Provided there are

no conflicts with subnet routes, the learned routes are re-added when the tunnel comes back up. Depending on your network, it can take the associated Cloud Router up to 40 seconds of processing time to remove them.

- Tunnels using policy-based routing or route-based VPNs have corresponding static routes. Google Cloud ignores static routes with next hops that point to Cloud VPN tunnels that are down.

If a second Cloud VPN tunnel provides an alternate path to the same destination, you should still expect packet loss whenever one Cloud VPN tunnel goes down. In-flight packets may be dropped, and dynamic routes are removed only after the associated Cloud Router has completed its processing.

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)
- 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
← Overview (https://cloud.google.com/vpn/docs/concepts/advanced)

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

Last updated November 22, 2019.