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

Networks and tunnel routing

This page describes supported Virtual Private Cloud networks and routing options.

Supported networks

Cloud VPN supports VPC custom networks, auto-mode networks (https://cloud.google.com/vpc/docs/vpc#subnet-ranges), and legacy networks (https://cloud.google.com/vpc/docs/legacy); however, you should consider the following best practices:

- **Use VPC networks instead of legacy networks.** Legacy networks do not support subnets; the entire network uses a single range of IP addresses. Legacy networks cannot be converted into VPC networks.
- **Use a custom mode VPC network.** VPC networks in custom mode provide you with full control over the range of IP addresses used by their subnets.
    - If you are connecting two VPC networks using Cloud VPN, at least one of them *must* be a custom mode network because auto mode networks use the same range of internal IP addresses (https://cloud.google.com/vpc/docs/vpc#ip-ranges) for their subnets.
    - Review the considerations for auto mode networks (https://cloud.google.com/vpc/docs/vpc#auto-mode-considerations) before using one with Cloud VPN. Auto mode networks automatically create a subnet in each Google Cloud region, including automatically creating new subnets in new regions as they are added. Avoid using the private IP addresses from the range used by auto mode

networks (https://cloud.google.com/vpc/docs/vpc#ip-ranges) in the network to which Cloud VPN tunnels connect.

Routing options for VPN tunnels

Classic VPN supports dynamic and static routing options for VPN tunnels, while HA VPN requires the dynamic routing option.

Dynamic routing uses the Border Gateway routing Protocol (BGP) (https://wikipedia.org/wiki/Border_Gateway_Protocol).

Dynamic (BGP) routing

Dynamic routing makes use of a Cloud Router (https://cloud.google.com/router/docs/concepts/overview) to automatically manage the exchange of routes using the BGP protocol. A BGP interface on a Cloud Router in the same region as the corresponding Cloud VPN tunnel manages this exchange. The Cloud Router adds and removes routes without requiring that the tunnel be deleted and re-created.

The dynamic routing mode (https://cloud.google.com/vpc/docs/vpc#routing_for_hybrid_networks) of your VPC network controls the behavior of all its Cloud Routers. This mode determines whether or not the routes learned from your peer network are only applied to Google Cloud resources in the same region as the VPN tunnel or if they are applied in all regions. You control the routes advertised by your peer router or gateway.

The dynamic routing mode also determines whether subnet routes from just the tunnel's region or all regions are shared with your peer router or gateway. In addition to these subnet routes, you can configure custom route advertisements (https://cloud.google.com/router/docs/how-to/advertising-overview) on a Cloud Router.

Static routing

Classic VPN tunnels support policy based and route based static routing options. Consider a static routing option only if you cannot use dynamic (BGP) routing or HA VPN.

- *Policy based routing*: Local IP ranges (left side) and remote IP ranges (right side) are defined as part of the tunnel creation process.

- *Route based VPN*: When you create a route based VPN using the Cloud Console, you only specify a list of remote IP ranges. Those ranges are *only* used to create routes in your VPC network to peer (https://cloud.google.com/vpn/docs/concepts/overview#peer-definition) resources.

Refer to traffic selectors (#static-routing-networks) for additional details about these two static routing options.

Note: The dynamic routing mode of a VPC network **only** affects the behavior of Cloud Routers. It does not affect Cloud VPN policy or route based tunnels.

Traffic selectors

A traffic selector defines a set of IP address ranges or CIDR blocks used to establish a VPN tunnel. These ranges are used as part of the IKE negotiation for the tunnel. Some literature refers to traffic selectors as “encryption domains.”

There are two types of traffic selectors:

- The **local traffic selector** defines the set of local IP ranges (CIDR blocks) from the perspective of the VPN gateway that emits the VPN tunnel. For Cloud VPN tunnels, the local traffic selector defines the set of primary and secondary subnet CIDRs for subnets (https://cloud.google.com/vpc/docs/vpc#vpc_networks_and_subnets) in the VPC network, representing the “left side” of the tunnel.
- The **remote traffic selector** defines the set of remote IP ranges (CIDR blocks) from the perspective of the VPN gateway emitting the VPN tunnel. For a Cloud VPN tunnel, the remote traffic selector is the “right side” or peer network.

Traffic selectors are an intrinsic part of a VPN tunnel, used to establish the IKE handshake. If either the local or remote CIDRs need to be changed, the Cloud VPN tunnel and its peer counterpart tunnel must be destroyed and re-created.

Important: In Google Cloud, a traffic selector (encryption domain) is *not* the same thing as a route. When you create a policy or route based Cloud VPN tunnel using the Cloud Console, Google Cloud automatically creates the necessary routes to peer networks in your VPC network. If you create a policy or route based Cloud VPN tunnel using `gcloud`, routes are *not* automatically created; you must create the custom static routes

manually. Refer to Creating a Classic VPN using static routing (https://cloud.google.com/vpn/docs/how-to/creating-static-vpns) for directions.

Routing options and traffic selectors

The IP range (CIDR block) values for local and remote traffic selectors depend on the routing option used by the Cloud VPN tunnel:

HA VPN tunnels				
Tunnel routing option	Local traffic selector	Remote traffic selector	Routes to the VPC network	Rou to t
Requires dynamic (BGP) routing	Always `0.0.0.0/0`	Always `0.0.0.0/0`	Unless modified by custom advertisements (https://cloud.google.com/router/docs/how-to/advertising-overview), the Cloud Router managing the BGP interface for the Cloud VPN tunnel shares the routes to the subnets in the VPC network according to the dynamic routing mode (https://cloud.google.com/vpc/docs/vpc#routing_for_hybrid_networks) of the network and quotas and limits for Cloud Router (https://cloud.google.com/router/quotas).	Sub (ht and (ht mar rou the (ht .
Classic VPN tunnels				
Tunnel routing option	Local traffic selector	Remote traffic selector	Routes to the VPC network	Rou to t
Dynamic (BGP) routing	Always `0.0.0.0/0`	Always `0.0.0.0/0`	Unless modified by custom advertisements (https://cloud.google.com/router/docs/how-to/advertising-overview), the Cloud Router managing the BGP interface for the Cloud VPN tunnel shares the routes to the subnets in the VPC network according to the dynamic routing mode (https://cloud.google.com/vpc/docs/vpc#routing_for_hybrid_networks) of the network and quotas and limits for Cloud Router (https://cloud.google.com/router/quotas).	Sub (ht and (ht mar rou the (ht .
Policy based routing	Configurable. See policy based	Required. See policy based	You must manually create and maintain the routes to the subnets in your VPC network on your peer routers.	Cus (ht are

	tunnels and traffic selectors (#static-routing-networks).	tunnels and traffic selectors (#static-routing-networks).		tun the crea rou (ht vpn for
Route based VPN	Always `0.0.0.0/0`	Always `0.0.0.0/0`	You must manually create and maintain the routes to the subnets in your VPC network on your peer routers.	Cus (ht are tun the crea rou (ht vpn for

Policy based tunnels and traffic selectors

This section describes special considerations for traffic selectors when you create policy based Classic VPN tunnels. It does not apply to any other type of Classic VPN or HA VPN tunnel.

You can choose to specify the **local traffic selector** of a policy based Cloud VPN tunnel when you create it:

- *Custom local traffic selector*: You can define the local traffic selector as a set of subnets in the VPC network or a set of RFC 1918 (https://tools.ietf.org/html/rfc1918) CIDRs that include desired IP ranges of subnets in the VPC network. IKEv1 limits local traffic selectors to a single CIDR (#ts-ip-ranges).
- Custom mode VPC networks (https://cloud.google.com/vpc/docs/vpc#subnet-ranges): You must specify a custom local traffic selector consisting of RFC 1918 CIDRs.
- Auto mode VPC networks (https://cloud.google.com/vpc/docs/vpc#subnet-ranges): If unspecified, the local traffic selector is the primary IP range (CIDR block) of the automatically-created subnet in the same region as the Cloud VPN tunnel. Auto mode networks have one subnet per region with well-defined IP ranges (https://cloud.google.com/vpc/docs/vpc#ip-ranges).

- Legacy networks (https://cloud.google.com/vpc/docs/legacy): If unspecified, the local traffic selector is defined as the entire RFC 1918 IP address range of the legacy network.

You must specify the **remote traffic selector** of a policy based Cloud VPN tunnel when you create it. If you create the Cloud VPN tunnel using the Cloud Console, custom static routes whose destinations correspond to the CIDRs of the remote traffic selector are automatically created. IKEv1 limits remote traffic selectors to a single CIDR (#ts-ip-ranges). See Creating a Classic VPN using static routing (https://cloud.google.com/vpn/docs/how-to/creating-static-vpns) for directions.

Important considerations for traffic selectors

Before you create a Cloud VPN policy based tunnel, consider the following:

- Most VPN gateways will only pass traffic through a VPN tunnel if the source IP of a packet fits in the tunnel's local traffic selector and if the destination IP of a packet fits in the tunnel's remote traffic selector. Some VPN devices do not enforce this requirement.
- Cloud VPN supports traffic selector CIDRs of `0.0.0.0/0` (any IP address). Consult the documentation that came with your peer VPN gateway to determine if it does as well. Creating a policy based VPN tunnel with both traffic selectors set to `0.0.0.0/0` is functionally equivalent to creating a route based VPN.
- Carefully review multiple CIDRs per traffic selector (#ts-ip-ranges) to learn how Cloud VPN implements IKEv1 and IKEv2 protocols.
- Cloud VPN disallows editing any traffic selectors after you have created a VPN. To change either the local or the remote traffic selector for a Cloud VPN tunnel, you must delete the tunnel then re-create it. You do **not** have to delete the Cloud VPN gateway, though.
- If you convert an auto mode VPC network to a custom mode VPC network, you might need to delete and re-create the Cloud VPN tunnel (but not the gateway), especially if you add custom subnets, remove any automatically-created subnets, or modify the secondary IP ranges of any subnet. You should avoid switching the mode of a VPC network that has existing Cloud VPN tunnels. Review the considerations for auto mode networks (https://cloud.google.com/vpc/docs/vpc#auto-mode-considerations) for suggestions.

Additionally, for consistent and predictable VPN behavior:

- Make both the local and remote traffic selectors as specific as possible.

- Make the Cloud VPN local traffic selector the same as the *remote traffic selector* configured for the corresponding tunnel on the peer VPN gateway.
- Make the Cloud VPN remote traffic selector the same as the *local traffic selector* configured for the corresponding tunnel on the on-premises VPN gateway.

Multiple CIDRs per traffic selector

When you create a policy based Classic VPN tunnel, you can specify multiple CIDRs per traffic selector if you use IKEv2. Cloud VPN *always* uses a single Child SA, regardless of IKE version.

The following table summarizes Cloud VPN support for multiple CIDRs per traffic selector in policy based VPN tunnels:

IKE Version	Multiple CIDRs per traffic selector
IKEv1	**No** The IKEv1 protocol only supports a single CIDR per Child Security Assocation (SA) as defined in RFC 2407 and RFC 2409. Because Cloud VPN requires a single Child SA per VPN tunnel, you can only supply a single CIDR for the local traffic selector and a single CIDR for the remote traffic selector when using IKEv1. Cloud VPN does **not** support creating a VPN tunnel using IKEv1 with multiple Child SAs, each with a single CIDR.
IKEv2	**Yes**, provided that all of following conditions are met: • Your peer VPN gateway uses a single Child Security Association (SA). All CIDRs for the local traffic selector and all CIDRs for the remote traffic selector **must** be in a single Child SA. • The number of CIDRs you configure does not cause IKE proposal packets to exceed Cloud VPN's maximum MTU of 1,460 bytes. Cloud VPN tunnels will not establish if IKE proposals exceed this MTU. • You don't exceed any restriction for the number of CIDRS supported by your on-premises gateway. Consult your gateway vendor's documentation for details. A best practice is to use 30 or fewer CIDRs per traffic selector so you don't create an IKE proposal packet that exceeds the maximum MTU.

Important: When using IKEv2, your peer VPN gateway *must* accept all of the CIDRs in each traffic selector using a single Child SA. Not all VPN gateways support this. VPN gateways that create a unique Child SA per

CIDR are **not** compatible with Cloud VPN. See traffic selector strategies (#route-alignment) for additional details.

Traffic selector strategies

Consider the following strategies if your on-premises VPN gateway creates multiple Child SAs per VPN tunnel or if multiple CIDRs per traffic selector would cause an IKE proposal for IKEv2 to exceed 1,460 bytes:

1. Use dynamic routing (#ts-tun-routing) for the VPN tunnel. If your peer VPN gateway supports BGP, both local and remote traffic selectors for the VPN tunnel are `0.0.0.0/0` by definition. Routes are exchanged automatically between the peer VPN gateway and the Cloud Router associated with your Cloud VPN tunnel. If you can use dynamic routing, consider HA VPN.
2. Use broad, single CIDR traffic selectors and static tunnel routing:
    - Use a route based VPN (#ts-tun-routing). Both traffic selectors are `0.0.0.0/0` by definition for route based VPNs. You can create routes that are more specific than the traffic selectors.
    - Use policy based routing (#ts-tun-routing) and configure the local and remote traffic selectors to be as broad as possible. For policy based Cloud VPN tunnels, you can create routes to on-premises networks in your VPC network whose destinations are more specific than the CIDR blocks specified in the remote traffic selectors. The simplest way to accomplish this is to create the routes separately from the VPN tunnels by following **`gcloud`** steps on the Creating a Classic VPN using static routing (https://cloud.google.com/vpn/docs/how-to/creating-static-vpns) page.
3. Create multiple Cloud VPN tunnels using policy based routing so that each tunnel only has one CIDR block for its local traffic selector and one CIDR block for its remote traffic selector. Configure the on-premises counterpart tunnel in a similar fashion. Cloud VPN supports multiple tunnels per gateway; however, using multiple tunnels has some implications:
    - Your peer VPN gateway must offer separate public IP addresses to which each Cloud VPN tunnel can connect. Tunnels on the same Classic VPN gateway must connect to unique peer gateway IP addresses. Your peer VPN gateway might also require that its tunnels connect to unique IP addresses. In some situations, you will need to create a separate Cloud VPN gateway per Cloud VPN tunnel.

- When you create route based or policy based Cloud VPN tunnels using the Cloud Console, routes to the peer network are automatically created in addition to the tunnel. If routes are automatically created for multiple VPN tunnels that each use the same remote traffic selectors — as the case will be if you create route based VPNs — you can have multiple routes in your VPC network, all with identical destinations but different next hops. This can lead to unpredictable or unexpected behavior as traffic is delivered to a VPN tunnel according to the applicability and order of routes (https://cloud.google.com/vpc/docs/routes#instancerouting). You must carefully create and review static routes in both your VPC network and your peer network if you don't use dynamic (BGP) tunnel routing.

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)
- Choose VPN over other hybrid connectivity solutions (https://cloud.google.com/vpn/docs/concepts/choosing-a-hybrid-solution)
- 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
← Cloud VPN topologies (https://cloud.google.com/vpn/docs/concepts/topologies)

Next
Supported IKE ciphers (https://cloud.google.com/vpn/docs/concepts/supported-ike-ciphers) →

Last updated December 4, 2019.