Configuring the Peer VPN gateway

To complete your VPN configuration, you must configure the following resources on your peer (https://cloud.google.com/vpn/docs/concepts/overview#peer-definition) VPN gateway:

- Corresponding VPN tunnel(s) to Cloud VPN
- BGP sessions if you are using dynamic routing with Cloud Router.
  You must always configure BGP sessions for HA VPN gateways and for Classic VPN gateways with tunnels that use dynamic routing.
- Firewall rules
- IKE settings

All of these resources are described in this document.

See your peer gateway documentation or manufacturer for best practices when setting up your peer gateway. See the VPN Interop Guides page (https://cloud.google.com/vpn/docs/how-to/interop-guides) for guides that describe some supported third-party VPN devices and services.

External peer VPN gateway resources for HA VPN

For HA VPN gateway, you configure an external peer VPN gateway resource that represents your physical peer gateway in Google Cloud. You can also create this resource as a standalone resource and use it later.

To create an external peer VPN gateway, you need the following values from your physical peer gateway, which can also be a 3rd-party software-based gateway. The values for the external

peer VPN gateway resource must match the configuration on your physical peer gateway for the VPN to be established:

- The number of interfaces on your physical VPN gateway
- Public IP address or addresses for the peer gateway(s) or interfaces
- BGP endpoint IP address(es)
- The IKE preshared key
- The ASN number

To create a standalone external peer VPN gateway resource, do the following:

CONSOLE GCLOUD API

1. Go to the VPN page in the Google Cloud Console.
   GO TO THE VPN PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/HYBRID/VPN/LIST&TAB=PEERGA
2. Click the **Create peer VPN gateway** button.
3. Give the peer gateway a **Name**.
4. Select the number of interfaces your physical peer gateway has: `one`, `two`, or `four`.
5. Add the **Interface IP address** for each interface on your physical VPN gateway.
6. Click **Create**.

Configuring VPN tunnels

Consult the documentation for your peer VPN gateway to create corresponding tunnels for each Cloud VPN tunnel you've created.

For HA VPN, configure two tunnels on your peer gateway. One tunnel on the peer gateway should correspond to the Cloud VPN tunnel on interface 0, and another tunnel on the peer gateway should correspond to the Cloud VPN tunnel on interface 1.

Each tunnel on your peer gateway should also use a unique public IP address for your HA VPN gateway to use.

Configuring BGP sessions for dynamic routing

For dynamic routing only, configure your peer VPN gateway to support BGP sessions for the peer subnets you want to advertise to Cloud Router.

Use the ASNs and IP addresses of your Cloud Router, and the information from your Cloud VPN gateway, to configure your peer gateway.

You can use Cloud Router summary information to obtain the Google ASN, configured peer network ASN(s), and BGP IP addresses. See Viewing the Router Configuration (https://cloud.google.com/router/docs/how-to/viewing-configuration) to get the above information for your Cloud Router.

For HA VPN, note that the Google ASN, which is the peer ASN from the perspective of your peer VPN gateway, is the same for both tunnels.

Configuring firewall rules

For instructions on configuring firewall rules for your peer network, see Configuring Firewall Rules (https://cloud.google.com/vpn/docs/how-to/configuring-firewall-rules).

Configuring IKE

For dynamic, route based, and policy based routing, use the following instructions to configure IKE on your peer VPN gateway.

Configure the peer (https://cloud.google.com/vpn/docs/concepts/overview#peer-definition) VPN gateway and tunnel for IKE using the following parameters:

- For information about connecting Cloud VPN to some third-party VPN solutions, see the VPN Interoperability Guides (https://cloud.google.com/vpn/docs/how-to/interop-guides).
- For information on IPsec encryption and authentication settings, see Supported IKE Ciphers (https://cloud.google.com/vpn/docs/concepts/supported-ike-ciphers).

For IKEv1 and IKEv2:

Setting	Value
IPsec Mode	ESP+Auth Tunnel mode (Site-to-Site)
Auth Protocol	psk
Shared Secret	Also known as an IKE pre-shared key. Choose a strong password by following these guidelines (https://cloud.google.com/vpn/docs/how-to/generating-pre-shared-key). The shared secret is very sensitive as it allows access into your network.
Start	**`auto`** (peer device should automatically restart the connection if it drops)
PFS (Perfect Forward Secrecy)	on
DPD (Dead Peer Detection)	Recommended: **`Aggressive`**. DPD detects when the Cloud VPN restarts and routes traffic using alternate tunnels.
INITIAL_CONTACT (sometimes called uniqueids)	Recommended: **on** (sometimes called **`restart`**). The purpose is to detect restarts faster so that perceived downtime is reduced.
TSi (Traffic Selector - Initiator)	**Subnet networks:** the ranges specified by the **`--local-traffic-selector`** flag. If **`--local-traffic-selector`** was not specified because the VPN is in an auto mode VPC network and is announcing only the gateway's subnet, then that subnet range is used. **Legacy networks:** the range of the network.
TSr (Traffic Selector - Responder)	**IKEv2:** The destination ranges of all of the routes that have **`--next-hop-vpn-tunnel`** set to this tunnel. **IKEv1:** Arbitrarily, the destination range of one of the routes that has **`--next-hop-vpn-tunnel`** set to this tunnel.
MTU	The MTU of the peer VPN device must not exceed 1460 bytes. You must enable prefragmentation on your device, which means that packets must be fragmented first, then encapsulated. For more information, see Maximum Transmission Unit (MTU) considerations (https://cloud.google.com/vpn/docs/concepts/mtu-considerations).

Additional parameters for IKEv1 only:

Setting	Value
IKE/ISAKMP	aes128-sha1-modp1024
ESP	aes128-sha1

Setting	Value
PFS Algorithm	Group 2 (MODP_1024)

IKE cipher overview

The following IKE ciphers are supported for Classic VPN and HA VPN. There are two sections for IKEv2, one for ciphers using authenticated encryption with associated data (AEAD) (https://wikipedia.org/wiki/Authenticated_encryption), and one for ciphers that do not use AEAD.

Note: Cloud VPN operates in IPsec ESP Tunnel Mode.

IKEv2 ciphers that use AEAD

Phase 1

Cipher role	Cipher	Notes
Encryption & Integrity	• AES-GCM-8-128 • AES-GCM-8-192 • AES-GCM-8-256 • AES-GCM-12-128 • AES-GCM-12-192 • AES-GCM-12-256 • AES-GCM-16-128 • AES-GCM-16-192 • AES-GCM-16-256	In this list, the first number is the size of the ICV parameter in *bytes (octets)* and the second is the key length in *bits*. Some documentation might express the ICV parameter (the first number) in bits instead (8 becomes 64, 12 becomes 96, and 16 becomes 128).

Cipher role	Cipher	Notes
Pseudo-Random Function (PRF)	• PRF-AES128-XCBC • PRF-AES128-CMAC • PRF-HMAC-SHA1 • PRF-HMAC-MD5 • PRF-HMAC-SHA2-256 • PRF-HMAC-SHA2-384 • PRF-HMAC-SHA2-512	Many devices won't require an explicit PRF setting.
Diffie-Hellman (DH)	• modp_2048 (Group 14) • modp_2048_224 (modp_2048s224) • modp_2048_256 (modp_2048s256) • modp_1536 (Group 5) • modp_3072 (Group 15) • modp_4096 (Group 16) • modp_8192 (Group 18) • modp_1024 (Group 2) • modp_1024_160 (modp_1024s160)	Cloud VPN's proposal presents these key exchange algorithms in the order shown. Cloud VPN accepts any proposal that includes one or more of these algorithms in any order.
Phase 1 lifetime	36,000 seconds (10 hours)	—

Phase 2

Cipher role	Cipher	Notes

Cipher role	Cipher	Notes
Encryption & Integrity	• AES-GCM-16-128 • AES-GCM-16-256 • AES-GCM-16-192 • AES-GCM-12-128 • AES-GCM-8-128	Cloud VPN's proposal presents these algorithms in the order shown. Cloud VPN accepts any proposal that includes one or more of these algorithms, in any order. Note that the first number in each algorithm is the size of the ICV parameter in *bytes (octets)* and the second is its key length in *bits*. Some documentation might express the ICV parameter (the first number) in bits instead (8 becomes 64, 12 becomes 96, 16 becomes 128).
PFS Algorithm (required)	• modp_2048 (Group 14) • modp_2048_224 (modp_2048s224) • modp_2048_256 (modp_2048s256) • modp_1536 (Group 5) • modp_3072 (Group 15) • modp_4096 (Group 16) • modp_8192 (Group 18) • modp_1024 (Group 2) • modp_1024_160 (modp_1024s160)	Cloud VPN's proposal presents these key exchange algorithms in the order shown. Cloud VPN accepts any proposal that has one or more of these algorithms in any order.
Diffie-Hellman (DH)	Refer to Phase 1	If your VPN gateway requires DH settings for Phase 2, use the same settings you used for Phase 1.
Phase 2 lifetime	10,800 seconds (3 hours)	—

IKEv2 ciphers that don't use AEAD

Phase 1

Cipher role	Cipher	Notes

Cipher role	Cipher	Notes
Encryption	• AES-CBC-128 • AES-CBC-192 • AES-CBC-256 • 3DES-CBC • AES-XCBC-96 • AES-CMAC-96	Cloud VPN's proposal presents these symmetric encryption algorithms in the order shown. Cloud VPN accepts any proposal that use one or more of these algorithms, in any order.
Integrity	• HMAC-SHA1-96 • HMAC-MD5-96 • HMAC-SHA2-256-128 • HMAC-SHA2-384-192 • HMAC-SHA2-512-256	Cloud VPN's proposal presents these HMAC algorithms in the order shown. Cloud VPN accepts any proposal that has one or more of these algorithms, in any order. Documentation for your on-premises VPN gateway might use a slightly different name for the algorithm. For example, `HMAC-SHA2-512-256` might be referred to as just `SHA2-512` or `SHA-512`, dropping the truncation length number and other extraneous information.
Pseudo-Random Function (PRF)	• PRF-AES-128-XCBC • PRF-AES-128-CMAC • PRF-SHA1 • PRF-MD5 • PRF-SHA2-256 • PRF-SHA2-384 • PRF-SHA2-512	Many devices won't require an explicit PRF setting.

Cipher role	Cipher	Notes
Diffie-Hellman (DH)	• modp_2048 (Group 14) • modp_2048_224 (modp_2048s224) • modp_2048_256 (modp_2048s256) • modp_1536 (Group 5) • modp_3072 (Group 15) • modp_4096 (Group 16) • modp_8192 (Group 18) • modp_1024 (Group 2) • modp_1024_160 (modp_1024s160)	Cloud VPN's proposal presents these key exchange algorithms in the order shown. Cloud VPN accepts any proposal that contains one or more of these algorithms, in any order.
Phase 1 lifetime	36,000 seconds (10 hours)	—

Phase 2

Cipher role	Cipher	Notes
Encryption	• AES-CBC-128 • AES-CBC-256 • AES-CBC-192	Cloud VPN's proposal presents these symmetric encryption algorithms in the order shown. Cloud VPN accepts any proposal that contains one or more of these algorithms, in any order.
Integrity	• HMAC-SHA2-256-128 • HMAC-SHA2-512-256 • HMAC-SHA1-96	Cloud VPN's proposal presents these HMAC algorithms in the order shown. Cloud VPN accepts any proposal that contains one or more of these algorithms, in any order. Documentation for your on-premises VPN gateway might use a slightly different name for the algorithm. For example, `HMAC-SHA2-512-256` might be referred to as just `SHA2-512` or `SHA-512`, dropping the truncation length number and other extraneous information.

Cipher role	Cipher	Notes
PFS Algorithm (required)	• modp_2048 (Group 14) • modp_2048_224 (modp_2048s224) • modp_2048_256 (modp_2048s256) • modp_1536 (Group 5) • modp_3072 (Group 15) • modp_4096 (Group 16) • modp_8192 (Group 18) • modp_1024 (Group 2) • modp_1024_160 (modp_1024s160)	Cloud VPN's proposal presents these key exchange algorithms in the order shown. Cloud VPN accepts any proposal that contains one or more of these algorithms, in any order.
Diffie-Hellman (DH)	Refer to Phase 1.	If your VPN gateway requires DH settings for Phase 2, use the same settings that you used for Phase 1.
Phase 2 lifetime	10,800 seconds (3 hours)	—

IKEv1 ciphers

Phase 1

Cipher role	Cipher
Encryption	AES-CBC-128
Integrity	HMAC-SHA1-96
Pseudo-Random Function (PRF)	PRF-SHA1-96
Diffie-Hellman (DH)	modp_1024 (Group 2)
Phase 1 lifetime	36,600 seconds (10 hours, 10 minutes)

Phase 2

Cipher role	Cipher
Encryption	AES-CBC-128
Integrity	HMAC-SHA1-96
PFS Algorithm (required)	modp_1024 (Group 2)
Diffie-Hellman (DH)	If you need to specify DH for your VPN gateway, use the same setting that you used for Phase 1.
Phase 2 lifetime	10,800 seconds (3 hours)

What's next

- Learn about the basic concepts of Cloud VPN (https://cloud.google.com/vpn/docs/concepts/overview)
- See Advanced Configurations (https://cloud.google.com/vpn/docs/concepts/advanced) for information on high-availability, high-throughput scenarios, or multiple subnet scenarios.
- 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 metrics (https://cloud.google.com/vpn/docs/how-to/viewing-logs-metrics)
- Get troubleshooting help (https://cloud.google.com/vpn/docs/support/troubleshooting)

Previous
← Configuring firewall rules (https://cloud.google.com/vpn/docs/how-to/configuring-firewall-rules)

Next
Checking VPN status (https://cloud.google.com/vpn/docs/how-to/checking-vpn-status) →

Last updated December 4, 2019.