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

Supported IKE ciphers

Cloud VPN supports the following ciphers and configuration parameters for peer VPN devices or VPN services. Cloud VPN auto-negotiates the connection as long as the peer side uses a supported IKE cipher setting.

For configuration instructions, see Configuring the peer VPN gateway (https://cloud.google.com/vpn/docs/how-to/configuring-peer-gateway).

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

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).
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
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
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)
- 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
← Networks and tunnel routing (https://cloud.google.com/vpn/docs/concepts/choosing-networks-routing)

Last updated December 4, 2019.