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

Using third-party VPNs with Cloud VPN

This page provides Google-tested interoperability guides and vendor-specific notes for peer
(https://cloud.google.com/vpn/docs/concepts/overview#peer-definition) third-party VPN devices or
services that you can use to connect to Cloud VPN
(https://cloud.google.com/vpn/docs/concepts/overview).

**Any third-party device or service that supports IPSEC and IKE versions 1 or 2 should be
compatible with Cloud VPN. For more information, see Supported IKE ciphers**
(https://cloud.google.com/vpn/docs/concepts/supported-ike-ciphers)**.**

Each Interop guide offers specific instructions for connecting the third-party VPN solution to
Cloud VPN.

If the third-party solution supports dynamic (BGP) routing, the guide includes configuration
instructions for Cloud Router (https://cloud.google.com/router/docs).

> **Note:** Guides on this page may refer to the Classic VPN configuration instead of HA VPN.

- Most peer VPN devices should be compatible with Cloud VPN. For general information
  about configuring peer VPN devices, see Configuring the Peer VPN Gateway
  (https://cloud.google.com/vpn/docs/how-to/configuring-peer-gateway).

- For a list of IKE ciphers and other configuration parameters used by Cloud VPN, see
  Supported IKE Ciphers (https://cloud.google.com/vpn/docs/concepts/supported-ike-ciphers).

Interop guides by vendor

This section lists interoperability guides by vendor in alphabetical order. Each guide covers how to use that vendor's VPN gateway solution with Cloud VPN.

See the vendor-specific notes section (#vendor-specific-notes) for detailed notes covering the vendors listed in this section.

A-L

- Alibaba Cloud VPN Gateway without redundancy
  (https://cloud.google.com/community/tutorials/using-cloud-vpn-with-alibaba-site-to-site/) —
  supports static routes only

- Alibaba Cloud VPN Gateway with redundancy
  (https://cloud.google.com/community/tutorials/using-cloud-vpn-with-alibaba-redundancy) —
  supports static routes only

- Amazon Web Services with HA VPN
  (https://cloud.google.com/community/tutorials/using-ha-vpn-with-aws) — supports dynamic
  routing with Cloud Router only

> ★ **Known issue**: When setting up VPN tunnels to AWS, using IKEv2 and setting up fewer IKE transform sets (https://cloud.google.com/vpn/docs/how-to/creating-ha-vpn#aws-known-issue) on the AWS side is required.

- Amazon Web Services with Classic VPN
  (https://cloud.google.com/files/CloudVPNGuide-UsingCloudVPNwithAmazonWebServices.pdf) —
  supports static routes or dynamic routing with Cloud Router

- Cisco ASA 5506H with HA VPN
  (https://cloud.google.com/community/tutorials/using-ha-vpn-with-cisco-asa) — supports dynamic
  routing with Cloud Router only

- Cisco ASA 5505 with Classic VPN
  (https://cloud.google.com/files/CloudVPNGuide-UsingCloudVPNwithCiscoASA.pdf) — supports
  static routes only

- Cisco ASR (https://cloud.google.com/community/tutorials/using-cloud-vpn-with-cisco-asr) —
  supports static routes or dynamic routing with Cloud Router

- Check Point security gateway
  (https://cloud.google.com/community/tutorials/using-cloud-vpn-with-checkpoint) — supports

static routes or dynamic routing with Cloud Router

- Fortinet FortiGate with HA VPN
  (https://cloud.google.com/community/tutorials/using-ha-vpn-with-fortigate) — supports dynamic
  routing with Cloud Router only

- Fortinet FortiGate 300C with Classic VPN
  (https://cloud.google.com/files/CloudVPNGuide-UsingCloudVPNwithFortinetFortiGate300C.pdf) —
  supports static routes or dynamic routing with Cloud Router

- Juniper SRX (https://cloud.google.com/community/tutorials/using-cloud-vpn-with-juniper-srx) —
  supports static routes or dynamic routing with Cloud Router

M–Z

- Microsoft Azure
  (https://cloud.google.com/files/CloudVPNGuide-UsingCloudVPNwithAzureVPN.pdf) — supports
  static routes only

- Palo Alto Networks PA-3020
  (https://cloud.google.com/files/CloudVPNGuide-UsingCloudVPNwithPaloAltoNetworksPA-3020.pdf)
  — supports static routes or dynamic routing with Cloud Router

- strongSwan (https://cloud.google.com/community/tutorials/using-cloud-vpn-with-strongswan) —
  supports dynamic routing with Cloud Router and BIRD (https://bird.network.cz/)

- VyOS (https://cloud.google.com/files/CloudVPNGuide-UsingCloudVPNwithVyOS.pdf) — supports
  static routes or dynamic routing with Cloud Router

Vendor-specific notes

Check Point

Check Point VPN implements IKEv2 by creating multiple Child Security Associations (SAs)
when you specify more than one CIDR per traffic selector. This implementation is incompatible
with Cloud VPN, which requires all CIDRs for the local traffic selector and all CIDRs for the
remote traffic selector to be located in a single Child SA. Refer to Traffic selector strategies
(https://cloud.google.com/vpn/docs/concepts/choosing-networks-routing#route-alignment) for
suggestions on how to create a compatible configuration.

Cisco

- If your VPN gateway runs Cisco IOS XE, make sure you're running version 16.6.3 (Everest) or later. Earlier versions have known problems with Phase 2 rekey events, which result in tunnels going down for a few minutes every few hours.

- Cisco ASA supports route-based VPN with Virtual Tunnel Interface (VTI) in IOS version 9.7(x) and later. See the Cisco ASA Series 9.7(x) Release Notes (https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/release/notes/asarn97.html) and the VTI chapter in the Cisco ASA Series VPN CLI Configuration Guide, 9.7 (https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/vpn/asa-97-vpn-config/vpn-vti.pdf) .

★ **Note:** IOS version 9.7 is not supported with ASA hardware version 5505, which has reached end-of-life status (https://www.cisco.com/c/en/us/products/collateral/security/asa-5505-adaptive-security-appliance/eos-eol-notice-c51-738642.html) . See the ASA compatibility matrix for more information. (https://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asamatrx.html)

- When using Cisco ASA devices with a Cloud VPN tunnel, you cannot configure more than one IP address range (CIDR block) for each of the local and remote traffic selectors. The reason is that Cisco ASA devices use a unique SA for each IP address range in a traffic selector, while Cloud VPN uses a single SA for all IP ranges in a traffic selector. See traffic selectors (https://cloud.google.com/vpn/docs/concepts/choosing-networks-routing#static-routing-networks) for more information.

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 monitoring metrics
  (https://cloud.google.com/vpn/docs/how-to/viewing-logs-metrics)

- Get troubleshooting help (https://cloud.google.com/vpn/docs/support/troubleshooting)