



PROJECT TITLE: “Hybrid Cloud Secure Site-to-Site VPN between AWS and GCP”

PROJECT OVERVIEW:

The objective of this project was to establish a **secure and reliable communication channel** between AWS and Google Cloud Platform (GCP) environments to enable **hybrid cloud operations, resource sharing, disaster recovery, and failover mechanisms** across cloud platforms. The solution was aimed at **supporting business continuity**, reducing vendor lock-in, and **enabling multi-cloud workload distribution**.

The project was initiated to establish a **secure and reliable communication link** between an organisation’s **on-premise data centre** and its newly adopted **AWS cloud environment**. The organisation needed to extend its internal services (like databases, file servers, and internal applications) hosted on-premises to the cloud without exposing them to the Internet.

A **Site-to-Site VPN** was chosen as the solution to securely route internal traffic between both networks, ensuring data confidentiality, integrity, and availability.

PURPOSE:

The purpose of this project was to **enable secure, scalable, and resilient communication between cloud environments hosted on AWS and GCP**. Organizations are increasingly adopting **multi-cloud strategies** to leverage the unique advantages of different cloud providers, reduce vendor lock-in, and optimize costs. Enable secure, encrypted communication between isolated Virtual Private Clouds (VPCs) hosted in Amazon Web Services (AWS) and Google Cloud Platform (GCP), allowing seamless interoperability, hybrid cloud deployment, and disaster recovery between the two cloud environments.

A multinational company decided to adopt a **multi-cloud strategy** to:

- Leverage GCP’s analytics capabilities (e.g., BigQuery).
- Use AWS for scalable application hosting and storage (e.g., S3, EC2).
- Maintain **data and service connectivity** between both environments.

They needed **secure communication** between these two clouds over the internet using **IPsec VPN tunnels** for a **reliable and encrypted hybrid cloud network**.

ABOUT VPN:

AWS Site-to-Site VPN is a fully-managed service that creates a secure connection between your data centre or branch office and your AWS resources using IP Security (IPSec) tunnels. When using Site-to-Site VPN, you can connect to both your Amazon Virtual Private Clouds (VPC) as well as AWS Transit Gateway, and two tunnels per connection are used for increased redundancy.



For globally distributed applications, the Accelerated Site-to-Site VPN option provides even greater performance by working with AWS Global Accelerator to intelligently route your traffic to the nearest AWS network endpoint with the best performance.

Types of VPN in Cloud Networking

1. Site-to-Site VPN

- Connects **two networks** (e.g., AWS VPC and GCP VPC) over the internet.
- Uses **IPSec (Internet Protocol Security)** for encryption and authentication.
- Ideal for **Hybrid or Multi-Cloud Architectures**.

2. Client-to-Site VPN

- Connects an individual user's device to a private cloud network.
- Used for remote user access (e.g., employees working from home).

3. Cloud Provider VPN

- Managed VPN services from cloud vendors (e.g., **AWS Site-to-Site VPN, GCP Cloud VPN**) that simplify setup and maintenance.

TECHNOLOGIES USED:

AWS Services:

Amazon VPC

- Virtual Private Gateway (VGW)
- Customer Gateway (CGW)
- Site-to-Site VPN
- EC2
- CloudWatch

GCP Services:

- Google Cloud VPC
- Cloud VPN Gateway
- Cloud Router
- Compute Engine

Security & Networking Tools:

- IPsec (IKEv2)
- BGP (Border Gateway Protocol)
- Cloud Firewalls (AWS Security Groups, GCP Firewall Rules)

**ROLES AND RESPONSIBILITIES:**

- Designed and provisioned secure network topology across AWS and GCP.
- Configured VPN gateways and routing (static/BGP).
- Automated VPN deployment using **Terraform and CLI scripts**.
- Implemented logging, monitoring, and alerting systems.
- Ensured compliance with security policies and standards (IPSec encryption, firewall rules).
- Performed connectivity testing, latency benchmarking, and performance tuning.

SCOPE OF THE PROJECT:

- Establish a **resilient Site-to-Site VPN tunnel** between AWS and GCP.
- Enable **cross-cloud communication** for critical workloads (APIs, microservices, databases).
- Provide **high availability** and **automatic failover** using dual tunnels and BGP.
- Implement **infrastructure automation** for repeatable deployments across dev, test, and prod.
- Support **hybrid multi-cloud data replication**, centralized logging, and disaster recovery.

PROBLEM IT SOLVED:

- Removed the dependency on less secure and unreliable public internet access to AWS services.
- Solved latency and packet loss issues faced with legacy third-party connectivity tools.
- Addressed compliance and data security requirements by encrypting data in transit.
- Improved access control and network visibility for IT and DevOps teams.

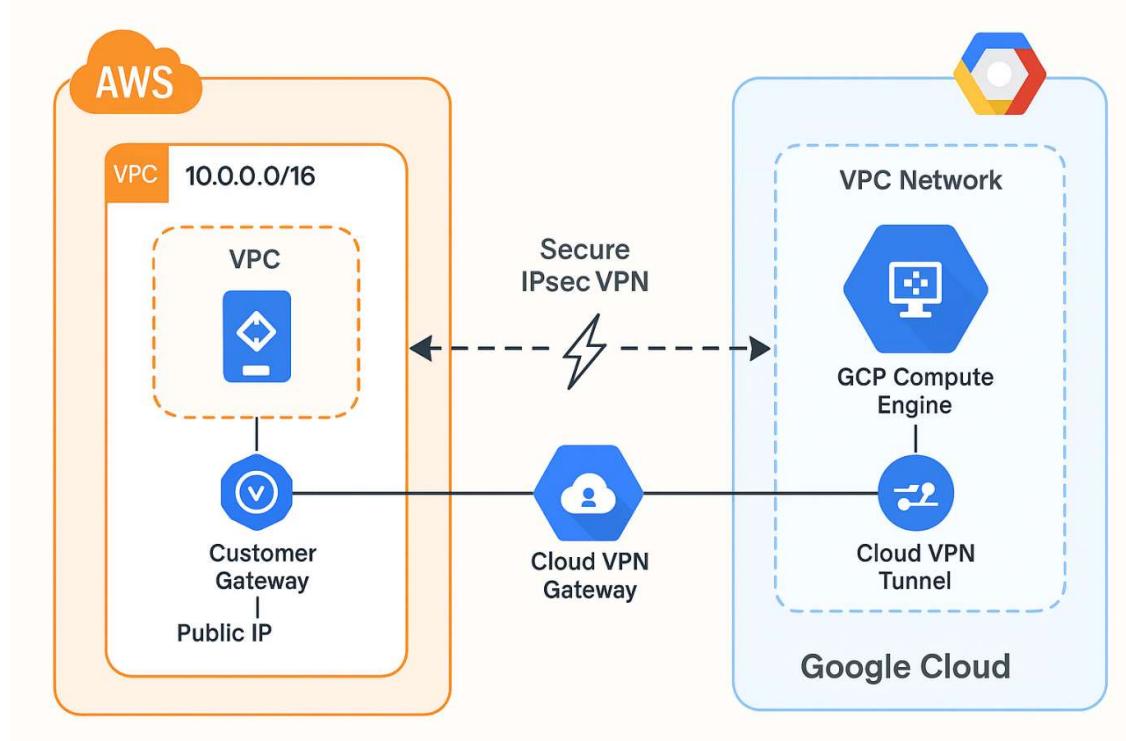
BUSINESS BENEFITS:

- **Secure cross-cloud data flow:** Enabled seamless and encrypted communication between AWS and GCP workloads using IPSec tunnels.
- **Reduced costs:** Leveraged cost-effective VPN and routing solutions, minimizing the need for expensive direct connectivity (e.g., Direct Connect, Interconnect).
- **Improved efficiency:** Automated VPN setup with Terraform and CLI tools reduced manual configuration time by over 60%.
- **Reduced downtime:** Implemented dual IPSec tunnels with BGP for high availability and quick failover between clouds.



- **Enhanced security:** Used strong encryption protocols (IPSec/IKEv2) to ensure data confidentiality, integrity, and secure key exchange.
- **Improved scalability:** Designed a flexible, cloud-agnostic architecture that supports scaling workloads across both AWS and GCP as needed.

AWS VPN: SET UP SITE-TO-SITE VPN ARCHITECTURE





Step-by-Step Guide

Prerequisites:

First, we need to create the foundational infrastructure required for establishing secure Site-to-Site VPN connectivity between the AWS Cloud and the on-premises network (GCP).

STEP 1: Create a VPC in AWS

Go to the VPC Dashboard in AWS Console.

- **VPC Name: AWS-VPN-Hybrid**
- **IPv4 CIDR : 10.0.0.0/16**
- **Select Remaining Default**
- **Create VPC on AWS**

The screenshot shows the AWS VPC Dashboard. On the left, there's a sidebar with options like EC2 Global View, Filter by VPC, Virtual private cloud, Your VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, Carrier gateways, DHCP option sets, Elastic IPs, Managed prefix lists, NAT gateways, and Peering connections. The main area displays 'Your VPCs (1/2)' with a table. The table has columns: Name, VPC ID, State, Block Public Access, IPv4 CIDR, and If. It shows two rows: one for a default VPC and one for 'AWS-VPN-Hybrid' (selected). Below the table, a detailed view for 'vpc-0bad9b5db8b5dd7d6 / AWS-VPN-Hybrid' is shown. The 'Details' tab is selected, displaying information such as VPC ID (vpc-0bad9b5db8b5dd7d6), State (Available), Block Public Access (Off), DNS hostnames (Disabled), and DHCP option set (dopt-0a29ae1800ecf70e6). Other tabs include Resource map, CIDs, Flow logs, Tags, and Integrations.



Go to the VPC Dashboard in AWS Console.

- Go to Subnet
- Select VPC: AWS-VPN-Hybrid
- Subnet 1: aws-vpn-public-subnet
- AZs: us-east-1a
- IPv4 CIDR: 10.0.1.0/24
- Subnet 2 aws-vpn-public-subnet
- AZs: us-east-1b
- IPv4 CIDR: 10.0.2.0/24
- Select Remaining Default
- Create Subnet

The screenshot shows the AWS VPC Subnets dashboard. On the left, there's a sidebar with options like EC2 Global View, Virtual private cloud (selected), Subnets, Route tables, Internet gateways, Egress-only internet gateways, Carrier gateways, DHCP option sets, Elastic IPs, Managed prefix lists, NAT gateways, and Peering connections. The main area is titled "Subnets (2/2) Info". It displays two subnets in a table:

Name	Subnet ID	State	VPC	Block Public
aws-vpn-Private-subnet	subnet-03b665a9eb9873357	Available	vpc-0bad9b5db8b5dd7d6 AW...	Off
aws-vpn-Public-subnet	subnet-0ca10c1b3175dac20	Available	vpc-0bad9b5db8b5dd7d6 AW...	Off

At the bottom of the main area, it says "Subnets: subnet-03b665a9eb9873357, subnet-0ca10c1b3175dac20". The browser address bar shows "us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#subnets;subnetId=subnet-0ca10c1b3175dac20;subnet-03b665a9eb9873357".

Go to the VPC Dashboard in AWS Console.

- Go to Internet gateway
- Create Internet gateway
- Name: AWS-VPN-Hybrid-igw
- Click create
- Go to actions attach to VPC
- Select the VPC and attach Internet gateway

AWS -SITE-TO-SITE VPN



The screenshot shows the AWS VPC Dashboard. On the left, there's a sidebar for 'Virtual private cloud' with options like 'Your VPCs', 'Subnets', 'Route tables', 'Internet gateways', and 'Carrier gateways'. The main area displays 'Internet gateways (1/2)'. A table lists two entries:

Name	Internet gateway ID	State	VPC ID
igw-0583d1b15a82fec1d	Attached	vpc-0591948495ad013b7	
AWS-VPN-Hybrid-igw	igw-044dea2f3136e5ec8	Attached	vpc-0bad9b5db8b5dd7d6 AWS-VPN-Hybrid

Below the table, a detailed view for 'igw-044dea2f3136e5ec8 / AWS-VPN-Hybrid-igw' is shown with tabs for 'Details' and 'Tags'. The 'Details' tab shows the following information:

Internet gateway ID	State	VPC ID	Owner
igw-044dea2f3136e5ec8	Attached	vpc-0bad9b5db8b5dd7d6 AWS-VPN-Hybrid	637423525126

The bottom of the screen shows the Windows taskbar with various pinned icons.

The screenshot shows the 'Attach to VPC (igw-044dea2f3136e5ec8)' dialog. It has a 'VPC' section where users can attach an internet gateway to a VPC. A search bar is provided to find available VPCs, with 'vpc-0bad9b5db8b5dd7d6' selected. There's also a link for 'AWS Command Line Interface command'. At the bottom are 'Cancel' and 'Attach internet gateway' buttons.



Go to the VPC Dashboard in AWS Console.

- Go to Route Tables
- RT 1: AWS-VPN-Hybrid-Public-rt
- Select VPC
- Create route table



- **RT 2: AWS-VPN-Hybrid-Private-rt**
- **Select VPC**
- **Create route table**

Name	Route table ID	Expli...	Edge...	Main	VPC	Owner ID
-	rtb-0558b936e2d143478	-	-	Yes	vpc-0591948495ad013b7	637423525126
<input checked="" type="checkbox"/> AWS-VPN-Hybrid-Public-rt	rtb-094a38740cc4507ed	-	-	No	vpc-Obad9b5db8b5dd7d6 AW...	637423525126
-	rtb-058cb072cdc9262ee	-	-	Yes	vpc-Obad9b5db8b5dd7d6 AW...	637423525126
<input checked="" type="checkbox"/> AWS-VPN-Hybrid-Private-rt	rtb-05bc3a619d43beb0f	-	-	No	vpc-Obad9b5db8b5dd7d6 AW...	637423525126

Route tables: rtb-094a38740cc4507ed, rtb-05bc3a619d43beb0f

Go to public route table associate only public subnet

- **Click on Subnet Associations**
- **Edit Subnet associations**
- **Select Public Subnet**
- **Save associations**
- **Go to private Route Table**
- **Click on Subnet Associations**
- **Edit Subnet associations**
- **Select Private Subnet**
- **Save associations**

AWS -SITE-TO-SITE VPN



VPC | us-east-1 IP Subnet Calculator

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#EditRouteTableSubnetAssociations:RouteTableId=rtb-094a38740cc4507ed

Feed | LinkedIn | google-it-automati... | Google | Xe Currency Convers... | The WoW Foundati... | Free Online Cron Ex... | AutoLt Scripting Ex...

Search [Alt+S] | United States (N. Virginia) | Tejaswini Yadav | All Bookmarks

VPC > Route tables > rtb-094a38740cc4507ed > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/2)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
aws-vpn-Private-subnet	subnet-03b665a9eb987...	10.0.2.0/24	-	Main (rtb-058cb072cd9262ee)
<input checked="" type="checkbox"/> aws-vpn-Public-subnet	subnet-0ca10c1b3175d...	10.0.1.0/24	-	Main (rtb-058cb072cd9262ee)

Selected subnets

subnet-0ca10c1b3175dac20 / aws-vpn-Public-subnet X

Cancel Save associations

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

ENG IN 10:48 PM 15-05-2025

VPC | us-east-1 IP Subnet Calculator

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#RouteTables:sort=desc:tag:Name

Feed | LinkedIn | google-it-automati... | Google | Xe Currency Convers... | The WoW Foundati... | Free Online Cron Ex... | AutoLt Scripting Ex...

CloudShell Feedback

Route tables (1/4) Info

Name	Route table ID	Explicit subnet associations	Edge...
AWS-VPN-Hybrid-Public-rt	rtb-094a38740cc4507ed	subnet-0ca10c1b3175dac20 / aws-vpn-Public-subnet	↑
<input checked="" type="checkbox"/> AWS-VPN-Hybrid-Private-rt	rtb-05bc3a619d43beb0f	subnet-03b665a9eb9873357 / aws-vpn-Private-subnet	↑
-	rtb-058cb072cd9262ee	-	↓
-	rtb-058cb072cd9262ee	-	↓

rtb-05bc3a619d43beb0f / AWS-VPN-Hybrid-Private-rt

Details Routes Subnet associations Edge associations Route propagation Tags

Details

Route table ID	Main	Explicit subnet associations	Edge associations
----------------	------	------------------------------	-------------------

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

CloudShell Feedback

ENG IN 10:50 PM 15-05-2025



- Go to Route tables
- Go to Public Route Table
- Click on edit routes
- Add routes 0.0.0.0/0
- Select the Internet gateway
- Click Save changes

The screenshot shows the AWS VPC dashboard with the 'Route tables' section selected. A modal window is open, titled 'Updated routes for rtb-094a38740cc4507ed / AWS-VPN-Hybrid-Public-rt successfully'. The modal displays details about the route table, including its ID (rtb-094a38740cc4507ed), VPC (vpc-0bad9b5db8b5dd7d6 | AWS-VPN-Hybrid), and owner ID (637423525126). It also shows explicit subnet associations (subnet-0ca1b3175dac20 / aws-vpn-Public-subnet) and edge associations. Below the modal, the 'Routes' tab is selected, showing two routes: one to the internet gateway (igw-044dea2f3136e5ec8) and one to the local subnet (10.0.0.0/16).

Create Two EC2 Instance:

- EC2 1 Name: AWS-VPN-Private-EC2
 - Amazon Linux Machine
 - Instatance type: t2 micro
 - Key pair: aws-key.pem
 - Select VPC
 - Select Subnet Private
 - Create security group: All ICMP – IPv4 , Anywhere
 - Launch Instance
- EC2 1 Name: AWS-VPN-Public-EC2
 - Amazon Linux Machine
 - Instatance type: t2 micro
 - Key pair: aws-key.pem
 - Select VPC
 - Select Subnet Public
 - Enable Public IP
 - Create security group: All ICMP – IPv4 , Anywhere
 - Launch Instance

AWS -SITE-TO-SITE VPN



The screenshot shows the AWS VPC Console with the 'Launch an instance' wizard. In the 'Inbound Security Group Rules' section, there is one rule defined:

Type	Protocol	Port range
ssh	TCP	22

The 'Source type' is set to 'Anywhere'. The summary on the right indicates 1 instance will be launched, using the 'Amazon Linux 2 Kernel 5.10 AMI' and 't2.micro' instance type.

Both Private and Public EC2 Instance Created:

The screenshot shows the AWS EC2 Instances page. The left sidebar is expanded to show 'Instances' and 'Images'. The main pane displays two instances:

Name	Instance ID	Instance state	Status check	Alarm status	Availability
AWS-VPN-Public-EC2	i-0565317eadf51d161	Running	2/2 checks passed	View alarms +	us-east-1a
AWS-VPN-Private-EC2	i-00bdbb40622cfe163	Running	2/2 checks passed	View alarms +	us-east-1b

Below the instances, it says '2 instances selected'. Monitoring tabs are visible at the bottom.



customer gateway

- Name: **aws-gcp-cgw-1**
- BGP ASN: **64512**
- IP address: **35.242.36.121**
- Select default
- Create customer gateway

- Name: **aws-gcp-cgw-2**
- BGP ASN: **64512**
- IP address: **35.220.36.67**
- Select default
- Create customer gateway

The screenshot shows the AWS VPC dashboard with the 'Customer gateways' section selected. The table lists two customer gateways:

Name	Customer gateway ID	State	BGP ASN	IP address
aws-gcp-cgw-2	cgw-0206a8ebf3f65ca7	Available	64512	35.220.36.67
aws-gcp-cgw-1	cgw-01389b8bf34ac7138	Available	64512	35.242.36.121

Below the table, a detailed view is shown for the gateway with ID cgw-01389b8bf34ac7138. The details include:

- Customer gateway ID: cgw-01389b8bf34ac7138
- State: Available
- Type: ipsec.1
- IP address: 35.242.36.121
- BGP ASN: 64512
- Certificate ARN: (not visible)
- Device: (not visible)

CREATE VIRTUAL PRIVATE GATEWAY

- Name: **aws-gcp-vpgw**
- Amazon ASN : **64513**
- Create Virtual Private gateway
- Attach to VPC

AWS -SITE-TO-SITE VPN



The screenshot shows the AWS VPC dashboard with the 'Virtual private gateways' section. A single gateway named 'aws-gcp-vgw' is listed, which is detached from a VPC. The gateway ID is 'vgw-0343d5f43c54ccdee'. The details page for this gateway is also visible.

Name	Virtual private gateway ID	State	Type	VPC
aws-gcp-vgw	vgw-0343d5f43c54ccdee	Detached	ipsec.1	-

The screenshot shows the 'Attach to VPC' dialog box. It requires the selection of a virtual private gateway (selected) and a target VPC (selected). The target VPC is 'vpc-0bad9b5db8b5dd7d6 / AWS-VPN-Hybrid'. The 'Attach to VPC' button is highlighted in orange.

AWS -SITE-TO-SITE VPN



The screenshot shows the AWS VPC dashboard with the 'Virtual private gateways' section. A table lists one gateway: 'aws-gcp-vpgw' (vgw-0343d5f43c54ccdee), which is 'Attached' to 'vpc-0bad9b5db8b5dd7d6'. The table has columns for Name, Virtual private gateway ID, State, Type, and VPC.

Name	Virtual private gateway ID	State	Type	VPC
aws-gcp-vpgw	vgw-0343d5f43c54ccdee	Attached	ipsec.1	vpc-0bad9b5db8b5dd7d6 AW

- **Create VPN Connection**
- **Select site -to-site-connections**
- **Create two VPN Connections and meanwhile attached to VPN gateway**

The screenshot shows the 'Create VPN connection' form. It includes fields for 'Name tag - optional' (set to 'aws-gcp-vpn-01'), 'Target gateway type' (set to 'Virtual private gateway'), 'Virtual private gateway' (set to 'vgw-0343d5f43c54ccdee'), 'Customer gateway' (set to 'Existing'), 'Customer gateway ID' (set to 'cgw-01389b8bf34ac7138'), and 'Routing options' (set to 'Dynamic (requires BGP)').

AWS -SITE-TO-SITE VPN



VPC | us-east-1 Instances | EC2 IP Subnet Calc... Architecture Arcency App how to generate Create SSH keys +

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateVpnConnection:

(6) Feed | LinkedIn google-it-automati... Google Xe Currency Conver... The WoW Foundati... Free Online Cron Ex... AutoLt Scripting Ex...

aws Search [Alt+S] United States (N. Virginia) Tejaswini Yadav

VPN > VPN connections > Create VPN connection

Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.

Value must be 256 characters or less in length.

Target gateway type | Info
 Virtual private gateway
 Transit gateway
 Not associated

Virtual private gateway

Customer gateway | Info
 Existing
 New

Customer gateway ID

Routing options | Info
 Dynamic (requires BGP)
 Static

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 12:40 PM 16-05-2025

File Explorer Task View Taskbar

Here two tunnels are Down in Status need to set up tunnel connectivity:

VPC | us-east-1 Instances | EC2 IP Subnet Calc... Architecture Arcency App how to generate Create SSH keys +

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#VpnConnections:VpnConnectionId=vpn-06cca5ee945df76e8

(6) Feed | LinkedIn google-it-automati... Google Xe Currency Conver... The WoW Foundati... Free Online Cron Ex... AutoLt Scripting Ex...

aws Search [Alt+S] United States (N. Virginia) Tejaswini Yadav

VPC dashboard < Actions Download configuration Create VPN connection

Find resource by attribute or tag

Name	VPN ID	State	Virtual private gateway	Transit gateway
aws-gcp-vpn-01	vpn-037a4c5787b71933a	Available	vgw-0343d5f43c54ccdee	-
aws-gcp-vpn-02	vpn-06cca5ee945df76e8	Pending	vgw-0343d5f43c54ccdee	-

VPN connection vpn-037a4c5787b71933a / aws-gcp-vpn-01

Tunnel state

Tunnel number	Outside IP address	Inside IPv4 CIDR	Inside IPv6 CIDR	Status	Last status change	De
Tunnel 1	3.219.12.29	169.254.88.136/30	-	Down	May 16, 2025, 12:42:12 (UTC+05:30)	IPS
Tunnel 2	3.221.50.251	169.254.101.40/30	-	Down	May 16, 2025, 12:42:10 (UTC+05:30)	IPS

Tunnel 1 options

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 12:44 PM 16-05-2025

File Explorer Task View Taskbar

AWS -SITE-TO-SITE VPN



VPC connections (1/2) [Actions](#) [Download configuration](#) [Create VPN connection](#)

Name	VPN ID	State	Virtual private gateway	Transit gateway
aws-gcp-vpn-02	vpn-06cca5ee945df76e8	Available	vgw-0343d5f43c54ccdee	-
aws-gcp-vpn-01	vpn-037a4c5787b71933a	Available	vgw-0343d5f43c54ccdee	-

Tunnel state

Tunnel number	Outside IP address	Inside IPv4 CIDR	Inside IPv6 CIDR	Status	Last status change	De
Tunnel 1	3.219.12.29	169.254.88.136/30	-	Down	May 16, 2025, 12:42:12 (UTC+05:30)	IPS
Tunnel 2	3.221.50.251	169.254.101.40/30	-	Down	May 16, 2025, 12:42:10 (UTC+05:30)	IPS

Tunnel 1 options

Select the VPN Connection click on Downloads configuration make the changes as below and download from two VPN connections

Download configuration

Choose the sample configuration you wish to download based on your customer gateway. Please note these are samples, and will need modification to use Advanced Algorithms, Certificates, and/or IPv6.

Vendor

The manufacturer of the customer gateway device (for example, Cisco Systems, Inc.).

Generic

Platform

The class of the customer gateway device (for example, J-Series).

Generic

Software

The operating system running on the customer gateway device (for example, ScreenOS).

Vendor Agnostic

IKE version

The IKE version you are using for your VPN connection.

ikev2

[Cancel](#) [Download](#)



Output Result:

Name	VPN ID	State	Virtual private gateway	Transit gateway	Customer gateway
aws-gcp-vpn-002	vpn-0d75cdc3d4b2bf6b2	Available	vgw-055a62a1311410692	-	cgw-06f14e9c7a9c79147
aws-gcp-vpn-001	vpn-04cda4380dd43abda	Available	vgw-055a62a1311410692	-	cgw-00a5f8a9e4f327f68
aws-gcp-vpn-02	vpn-0f4778ea489b999c9	Deleted	vgw-00f1a72a8dadaa026	-	cgw-0206a8ebf3f665ca7
aws-gcp-vpn-01	vpn-096a9f7fa573750e4	Deleted	vgw-00f1a72a8dadaa026	-	cgw-01389b8bf34ac7138

Tunnel state								
Tunnel number	Outside IP address	Inside IPv4 CIDR	Inside IPv6 CIDR	Status	Last status change	Details	Certificate ARN	
Tunnel 1	3.213.11.148	169.254.10.176/30	-	Up	May 17, 2025, 12:27:48 (UTC+05:30)	2 BGP ROUTES	-	
Tunnel 2	54.235.43.37	169.254.73.80/30	-	Up	May 17, 2025, 12:27:37 (UTC+05:30)	2 BGP ROUTES	-	

STEP 1: Create a VPC in GCP

Go to the VPC Dashboard in GCP Console.

- **VPC Name: gcp-vpc-hybrid**
- **Enable two rules: Allow icmp and allow ssh**
- **Dynamic Routing Mode: Regional**
- **Best Path selection mode: Legacy**
- **Select Remaining Default**
- **Create VPC on GCP**

AWS -SITE-TO-SITE VPN



The screenshot shows the 'Create a VPC network' page in the AWS Cloud console. On the left, a sidebar lists various VPC-related options like IP addresses, Internal ranges, Bring your own IP, Firewall, Routes, VPC network peering, Shared VPC, Serverless VPC access, Packet mirroring, and VPC Flow Logs. The main area is titled 'Create a VPC network' and shows the 'IPv4 firewall rules' section. It lists several rules:

Name	Type	Targets	Filters	Protocols / ports	Action	Priority ↑	Edit
gcp-vpn-hybrid-allow-custom	Ingress	Apply to all	IP ranges: all		Allow	65,534	Edit
gcp-vpn-hybrid-allow-icmp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	icmp	Allow	65,534	
gcp-vpn-hybrid-allow-rdp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:3389	Allow	65,534	
gcp-vpn-hybrid-allow-ssh	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow	65,534	
gcp-vpn-hybrid-deny-all-ingress	Ingress	Apply to all	IP ranges: all		Deny	65,535	
gcp-vpn-hybrid-allow-all-egress	Egress	Apply to all	IP ranges: all		Allow	65,535	

Below this, there's an 'Advanced dynamic routing configuration' section with a note about configuration of the dynamic routing mechanism used by the VPC network.

The screenshot shows the 'VPC networks' page in the AWS Cloud console. The left sidebar is identical to the previous screenshot. The main area shows a table of VPC networks:

Name	Subnets	MTU	Mode	IPv6 ULA range	Gateways	Firewall rules	Global dynamic routing	Ne
default	41	1460	Auto			4	Off	
gcp-vpn-hybrid	0	1460	Custom			2	Off	

A message at the top states 'SMTP port 25 disallowed in this project. [Learn more](#)'.

Go to the VPC Dashboard in GCP Console.

- Go to Subnet
- Select VPC: gcp-vpn-hybrid
- Select option Subnet click on add Subnet
- Subnet 1: gcp-vpn-hybrid-public-subnet
- Region : asia-east1
- IPv4 CIDR: 21.0.1.0/24
- Click add Subnet

AWS -SITE-TO-SITE VPN



- **Subnet 2: gcp-vpn-hybrid-private-subnet**
- **Region: asia-east1**
- **IPv4 CIDR: 21.0.2.0/24**
- **Click add Subnet**

The screenshot shows the Google Cloud VPC Network details page for the network 'gcp-vpn-hybrid'. The left sidebar lists various network components like IP addresses, internal ranges, and routes. The main panel displays the 'Subnets' tab, which lists two subnets:

Name	Region	Stack Type	Primary IPv4 range
gcp-vpn-hybrid-private-subnet	asia-east1	IPv4 (single-stack)	21.0.2.0/24
gcp-vpn-hybrid-public-subnet	asia-east1	IPv4 (single-stack)	21.0.1.0/24

A right-hand sidebar titled 'Select a subnet' contains the message 'Please select at least one resource.'

- **Click on Routes**
- **All the default routes available in GCP**

AWS -SITE-TO-SITE VPN



The screenshot shows the VPC network details page for 'gcp-vpn-hybrid'. The 'Routes' tab is selected. A dropdown menu shows the region as 'asia-east1 (Taiwan)'. The table lists three routes:

Status	Name ↑	Type	IP version	Destination IP range	Priority	Scope limits	Next hop
✓	default-route-68aa7ccfeb807a4	Static	IPv4	0.0.0.0/0	1000	—	Default internet gateway
✓	default-router-3c69d93a188c37cc	Subnet	IPv4	21.0.1.0/24	0	—	Network gcp-vpn-hybrid
✓	default-router-r-948397893d81f276	Subnet	IPv4	21.0.2.0/24	0	—	Network gcp-vpn-hybrid

Create VM Instance in GCP Console

- Name : **gcp-vpn-public-vm**
- Region : **asia-east1 (Taiwan)**
- Machine : **E2**
- Network interfaces : **gcp-vpn-hybrid**
- Subnetwork : **gcp-vpn-hybrid-public-subnet IPv4 (21.0.1.0/24)**
- Security: Add Public SSH key

The screenshot shows the VM instances page for 'Compute Engine'. The 'Instances' tab is selected. A table lists one instance:

Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External IP	Connect
✓	gcp-vpn-public-vm	asia-east1-c			21.0.1.3 (nic0) 10.140.0.2 (nic1)	34.81.62.182 (nic0) 35.194.186.2 (nic1)	SSH

AWS -SITE-TO-SITE VPN



- **Create Router**
- **Name : gcp-vpn-router**
- **ASN Number: 64512**

Router details – Network Conn... +

← → ⌂ console.cloud.google.com/hybrid/routers/details/asia-east1/gcp-vpn-router?project=endless-set-459906-f0&hl=en&inv=1&invId=AbxI3Q

Google Cloud My First Project router Search All Bookmarks

Network Connectivity / Routers / Router: gcp-vpn-router

Router details Edit Delete

gcp-vpn-router

Overview Advertised and learned routes Best routes

Router overview

Network	gcp-vpn-hybrid
Region	asia-east1
Interconnect encryption	Unencrypted
Cloud Router ASN	64512
BGP peer keepalive interval	20 seconds
BGP identifier	Automatic
Tags	-

Advertised route configuration

BGP sessions will advertise these routes if no other configuration is specified

Advertisement mode

ENG IN 07:45 AM 17-05-2025

- **Create VPN**
- **Select High Availability VPN**
- **Click continue**
- **VPN Gateway: gcp-aws-vpn-gateway**
- **Select VPC network**

AWS -SITE-TO-SITE VPN



Screenshot of the Google Cloud Platform Network Connectivity / VPN / Select VPN page. The left sidebar shows Network Connectivity, VPN, Interconnect, and Cloud Router. The main content area is titled "Create a VPN" and describes a virtual private network connecting On-premise network and VPC network via Tunnel1 and Tunnel2. It highlights High-availability (HA) VPN, supports dynamic routing (BGP) only, high availability (99.9% SLA), and IPv4/IPv6 traffic. A diagram shows two routers connected by two tunnels to a central gateway interface. Below the diagram, "Classic VPN" is also mentioned.

**Note down the IP address generate in further steps we need:

IPs: 0 : 35.242.36.121 1 : 35.220.36.67

Screenshot of the Google Cloud Platform Network Connectivity / VPN / Create a VPN page. The left sidebar shows Network Connectivity, VPN, Interconnect, and Cloud Router. The main content area is titled "Create a VPN" and lists steps: 1. Create Cloud HA VPN gateway (selected), 2. Add VPN tunnels (highlighted), 3. Configure BGP sessions, 4. Summary and reminder. The "Add VPN tunnels" section details a VPN tunnel between a VPC network (gcp-vpn-hybrid) in the asia-east1 region and a VPN gateway named gcp-aws-vpn-gateway. The VPN gateway IP is IPv4, and the interfaces are 0 : 35.242.36.121 and 1 : 35.220.36.67. The "Peer VPN gateway" section includes options for On-prem or Non Google Cloud, Google Cloud VPN Gateway, and Compute Engine VMs with external IP addresses.

AWS -SITE-TO-SITE VPN



Screenshot of the Google Cloud Platform Network Connectivity Center - VPN - Create a VPN interface.

Name: gcp-aws-vpn-gateway

Peer VPN gateway IP version: IPv4

Interfaces:

- one interface
- two interfaces
- four interfaces**

Interface 0 IP address: 3.219.12.29

Interface 1 IP address: 3.221.50.251

Interface 2 IP address: 3.212.35.239

Interface 3 IP address: 54.198.193.129

Create Cancel

Screenshot of the Google Cloud Platform Network Connectivity Center - VPN - Add VPN tunnel interface.

Add VPN tunnels

Configure BGP sessions

Summary and reminder

Create BGP session

IPv4 BGP session

Name: bgp2

Peer ASN: 64513

Advertised route priority (MED): MED value is used for Active/Passive configuration

Multiprotocol BGP

BGP sessions are set up over IPv4, exchanging IPv4 and IPv6 addresses

Enable IPv6 traffic: You need to enable IPv6 traffic to allocate BGP next hops for IPv6 traffic.

Allocate BGP IPv4 address

Save and continue Cancel

AWS -SITE-TO-SITE VPN



After few the all-tunnel start connected AWS cloud

The screenshot shows the Google Cloud Network Connectivity VPN page. The left sidebar has 'Network Connectivity' expanded, with 'VPN' selected. Under 'VPN', there are 'Cloud VPN tunnels', 'Cloud VPN gateways', and 'Peer VPN gateways'. A 'Create VPN tunnel' button is visible. The main area displays 'VPN tunnels' with the following data:

Name	Cloud VPN gateway (IP)	Peer VPN gateway (IP)	Cloud Router BGP IP address	Peer BGP IP address	Actions
tunnel-1	gcp-aws-vpn-gateway 35.242.36.121	gcp-aws-vpn-gateway 3.219.12.29	169.254.90.214	169.254.90.213	⋮
tunnel-2	gcp-aws-vpn-gateway 35.242.36.121	gcp-aws-vpn-gateway 3.221.50.251	169.254.175.2	169.254.175.1	⋮
tunnel-3	gcp-aws-vpn-gateway 35.220.36.67	gcp-aws-vpn-gateway 3.212.35.239	169.254.26.26	169.254.26.25	⋮
tunnel-4	gcp-aws-vpn-gateway 35.220.36.67	gcp-aws-vpn-gateway 54.198.193.129	169.254.232.50	169.254.232.49	⋮

The screenshot shows the Google Cloud Network Connectivity VPN page. The left sidebar has 'Network Connectivity' expanded, with 'VPN' selected. Under 'VPN', there are 'Cloud VPN tunnels', 'Cloud VPN gateways', and 'Peer VPN gateways'. A 'Create VPN tunnel' button is visible. The main area displays 'VPN tunnels' with the following data:

Cloud Router BGP IP address	Peer BGP IP address	VPN tunnel status	BGP session status	Flow log configs	VPC	Actions
169.254.10.178	169.254.10.177	Established	BGP established	gcp	⋮	
169.254.73.82	169.254.73.81	Established	BGP established	gcp	⋮	
169.254.160.242	169.254.160.241	Established	BGP established	gcp	⋮	
169.254.85.142	169.254.85.141	Established	BGP established	gcp	⋮	

AWS -SITE-TO-SITE VPN



Screenshot of the Google Cloud Platform VPC Network details page for the 'gcp-vpn-hybrid' network.

The page shows two subnets:

Name	Region	Stack Type	Primary IPv4 range	Secondary IPv4 ranges	IPv6 ranges	R	N
gcp-vpn-hybrid-private-subnet	asia-east1	IPv4 (single-stack)	21.0.2.0/24				
gcp-vpn-hybrid-public-subnet	asia-east1	IPv4 (single-stack)	21.0.1.0/24				

AWS - SITE-TO-SITE VPN



SSH-in-browser

```

ssh.cloud.google.com/v2/ssh/projects/endless-set-459906-f0/zones/asia-east1-c/instances/gcp-vpn-public-vm?authuser=0&hl=en_US&p...
ssh.cloud.google.com/v2/ssh/projects/endless-set-459906-f0/zones/asia-east1-c/instances/gcp-vpn-public-vm?authuser=0&hl=en_US&p...
SSH-in-browser
8740cc4507ed
AutoIt Scripting Ex...
United States (N. Virginia) Tejaswini Yadav
Oc1b3175dac20 / blic-subnet
Tags Both Edit routes < 1 > Propagated No Yes
Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
12:44 PM 17-05-2025

```

SSH-in-browser

```

ssh.cloud.google.com/v2/ssh/projects/endless-set-459906-f0/zones/asia-east1-c/instances/gcp-vpn-public-vm?authuser=0&hl=en_US&p...
ssh.cloud.google.com/v2/ssh/projects/endless-set-459906-f0/zones/asia-east1-c/instances/gcp-vpn-public-vm?authuser=0&hl=en_US&p...
SSH-in-browser
8740cc4507ed
AutoIt Scripting Ex...
United States (N. Virginia) Tejaswini Yadav
Oc1b3175dac20 / blic-subnet
Tags Both Edit routes < 1 > Propagated No Yes
Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
12:44 PM 17-05-2025

```

SSH-in-browser

```

ssh.cloud.google.com/v2/ssh/projects/endless-set-459906-f0/zones/asia-east1-c/instances/gcp-vpn-public-vm?authuser=0&hl=en_US&p...
ssh.cloud.google.com/v2/ssh/projects/endless-set-459906-f0/zones/asia-east1-c/instances/gcp-vpn-public-vm?authuser=0&hl=en_US&p...
SSH-in-browser
8740cc4507ed
AutoIt Scripting Ex...
United States (N. Virginia) Tejaswini Yadav
Oc1b3175dac20 / blic-subnet
Tags Both Edit routes < 1 > Propagated No Yes
Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
12:44 PM 17-05-2025

```



HAPPY LEARNING

Regards,
Tejaswini J

<https://github.com/tejaswiniyadav/Site-to-Site-VPN->

THANK YOU