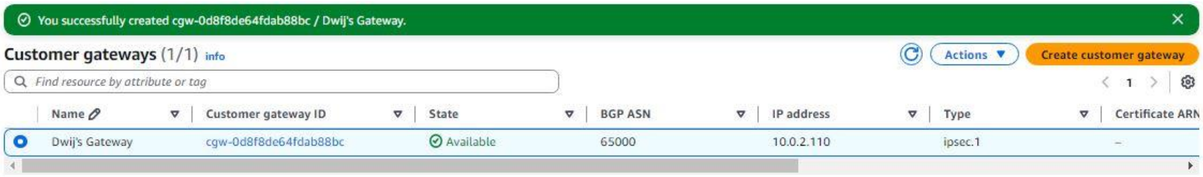
Day-9

……………………………………….

Today I have understood terms like tunneling, transit gateway, customer gateway and with the help of all of that I am going to perform a Site-To-Site VPN connection. It's just like peering but this can be done between On-Site Premises and AWS Architecture.

Here are the steps that I performed for Site-To-Site VPN connection:

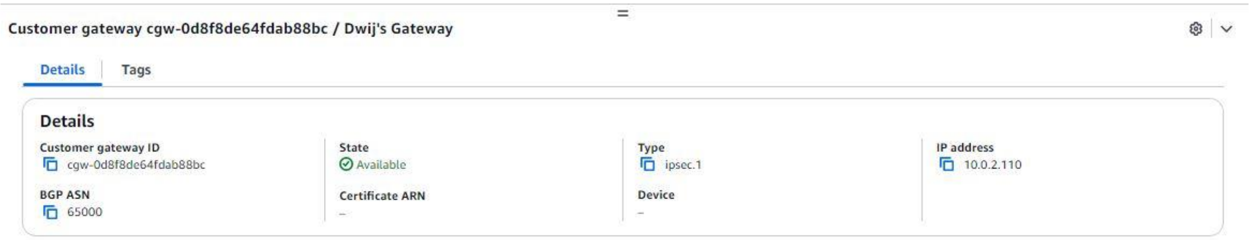
Create a customer gateway: Defines IP of customer to connect it to the route and tunnel.



You successfully created cgw-0d8f8de64fdab88bc / Dwij's Gateway.

Customer gateways (1/1) Info

	Name	Customer gateway ID	State	BGP ASN	IP address	Type	Certificate ARN
●	Dwij's Gateway	cgw-0d8f8de64fdab88bc	Available	65000	10.0.2.110	ipsec.1	–



Customer gateway cgw-0d8f8de64fdab88bc / Dwij's Gateway

Details

Customer gateway ID: cgw-0d8f8de64fdab88bc

BGP ASN: 65000

State: Available

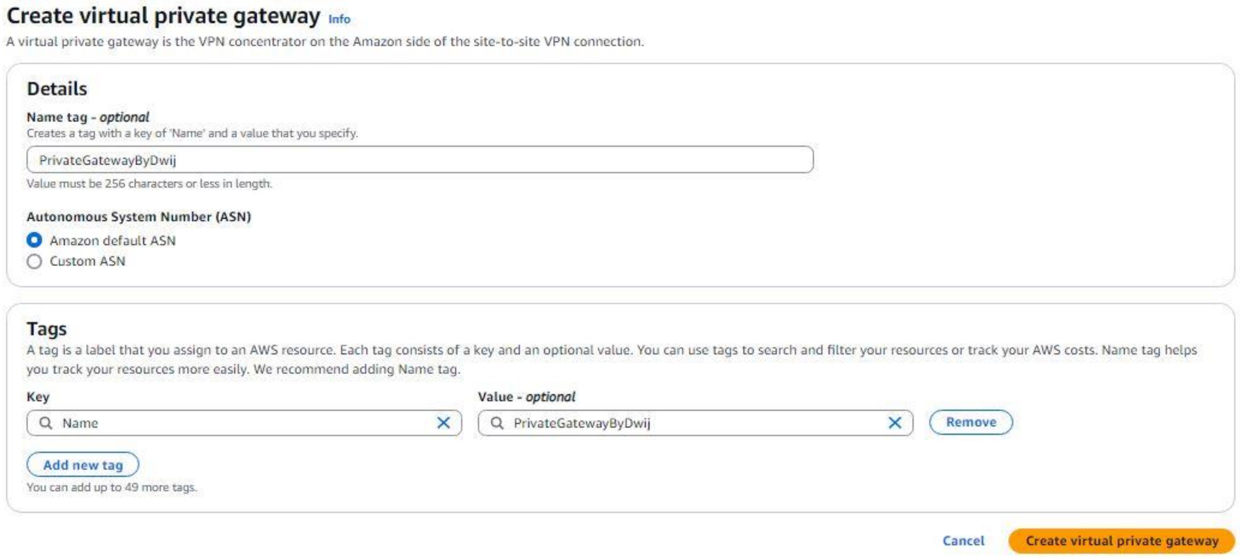
Certificate ARN: –

Type: ipsec.1

Device: –

IP address: 10.0.2.110

Creating a Virtual Private Gateway (VPG): VPG connects your on-premises network to your AWS VPC.



Create virtual private gateway Info

A virtual private gateway is the VPN concentrator on the Amazon side of the site-to-site VPN connection.

Details

Name tag - *optional*

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

PrivateGatewayByDwij

Value must be 256 characters or less in length.

Autonomous System Number (ASN)

● Amazon default ASN

○ Custom ASN

Tags

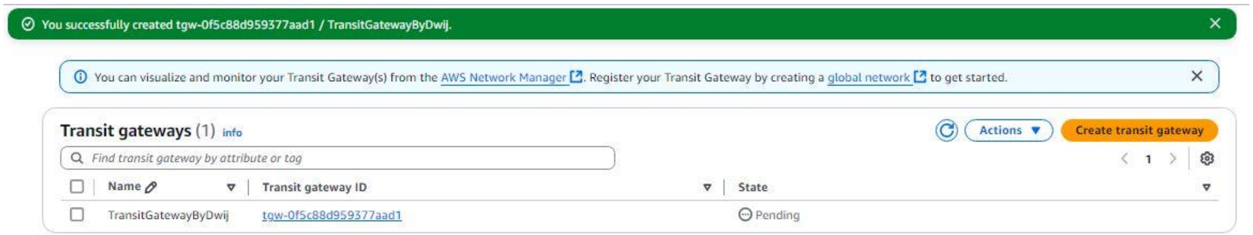
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs. Name tag helps you track your resources more easily. We recommend adding Name tag.

Key: Name

Value - *optional*: PrivateGatewayByDwij

You can add up to 49 more tags.

Creating a Transit Gateway:



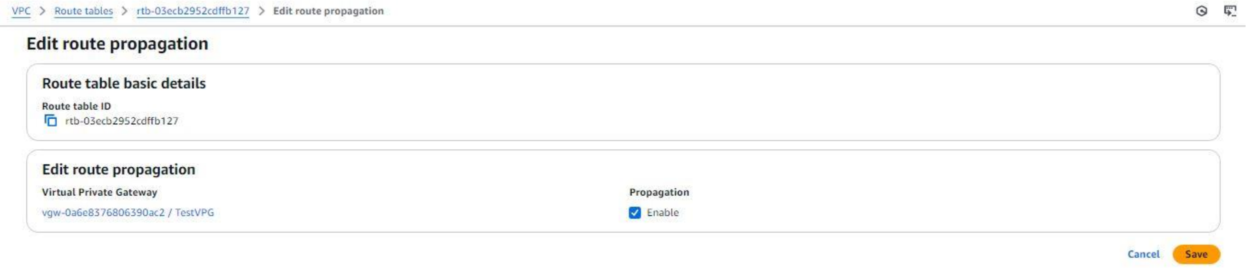
You successfully created tgw-0f5c88d959377aad1 / TransitGatewayByDwij.

You can visualize and monitor your Transit Gateway(s) from the AWS Network Manager. Register your Transit Gateway by creating a global network to get started.

Transit gateways (1)

Name	Transit gateway ID	State
TransitGatewayByDwij	tgw-0f5c88d959377aad1	Pending

Enabling Route Propagation:



VPC > Route tables > rtb-03ecb2952cdffb127 > Edit route propagation

Edit route propagation

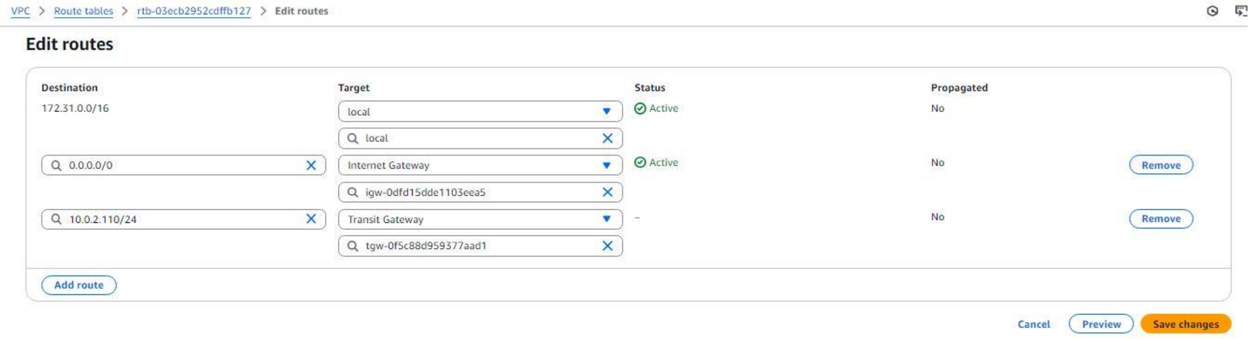
Route table basic details

Route table ID
rtb-03ecb2952cdffb127

Edit route propagation

Virtual Private Gateway	Propagation
vgw-0a6e8376806390ac2 / TestVPG	☑ Enable

Adding New route to Transit Gateway:

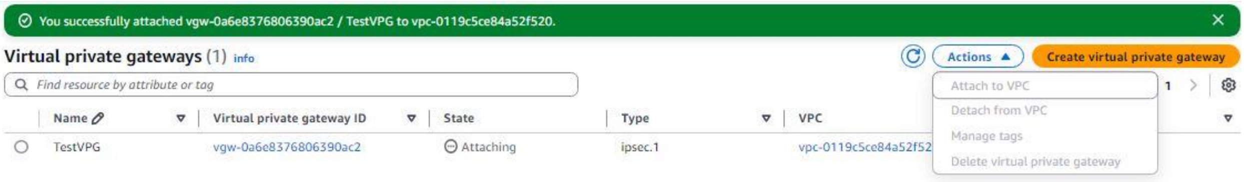


VPC > Route tables > rtb-03ecb2952cdffb127 > Edit routes

Edit routes

Destination	Target	Status	Propagated
172.31.0.0/16	local local	Active	No
0.0.0.0/0	Internet Gateway igw-0dfd15dde1103eea5	Active	No
10.0.2.110/24	Transit Gateway tgw-0f5c88d959377aad1	-	No

Attaching the Virtual Private Gateway to VPC:



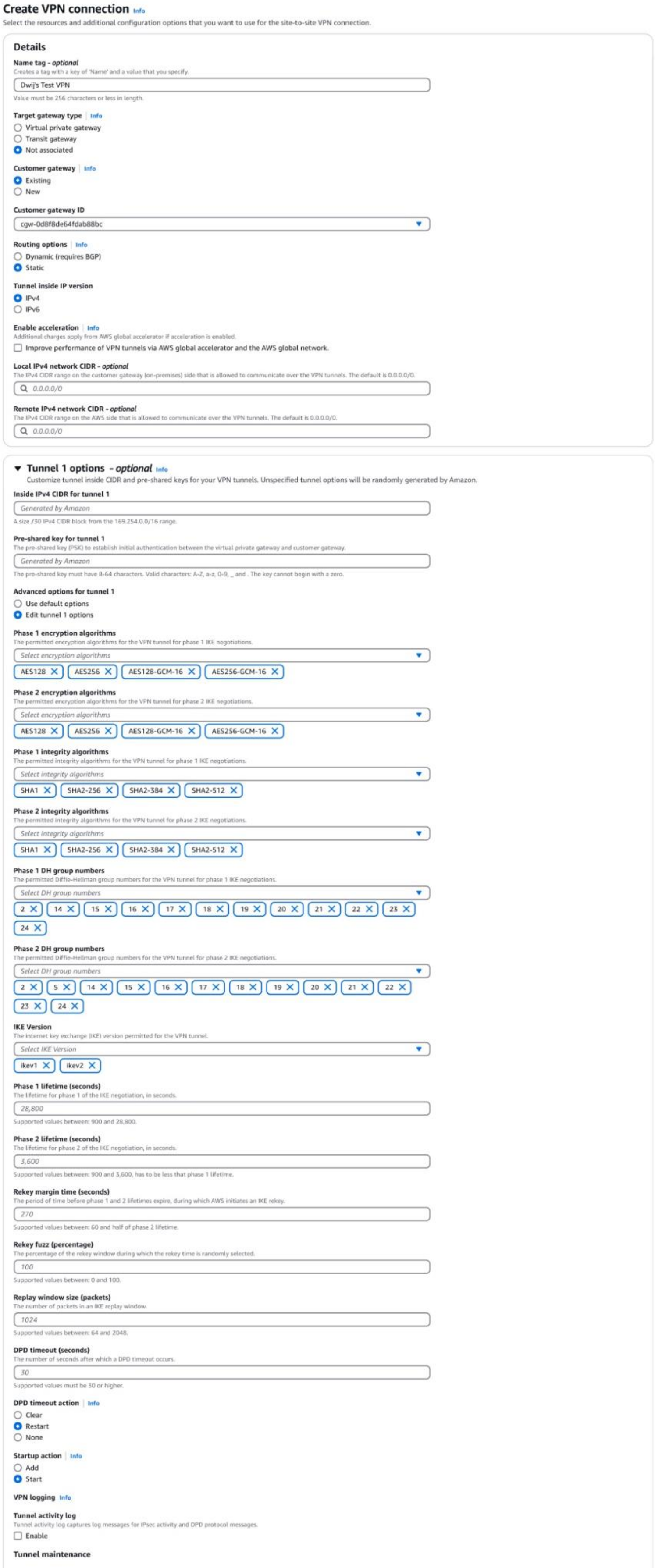
You successfully attached vgw-0a6e8376806390ac2 / TestVPG to vpc-0119c5ce84a52f520.

Virtual private gateways (1)

Name	Virtual private gateway ID	State	Type	VPC
TestVPG	vgw-0a6e8376806390ac2	Attaching	ipsec.1	vpc-0119c5ce84a52f52

info
Actions
Create virtual private gateway
Find resource by attribute or tag
Attach to VPC
Detach from VPC
Manage tags
Delete virtual private gateway
1

Creating VPN with the following config and tunneling:



Create VPN connection Info

Select the resources and additional configuration options that you want to use for the site-to-site VPN connection.

Details

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.
Dwij's Test VPN
Value must be 256 characters or less in length.

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

Customer gateway | Info
● Existing
○ New

Customer gateway ID
cgw-0d8f8de64fdab88bc ▼

Routing options | Info
○ Dynamic (requires BGP)
● Static

Tunnel inside IP version
● IPv4
○ IPv6

Enable acceleration | Info
Additional charges apply from AWS global accelerator if acceleration is enabled.
□ Improve performance of VPN tunnels via AWS global accelerator and the AWS global network.

Local IPv4 network CIDR - *optional*
The IPv4 CIDR range on the customer gateway (on-premises) side that is allowed to communicate over the VPN tunnels. The default is 0.0.0.0/0.
0.0.0.0/0

Remote IPv4 network CIDR - *optional*
The IPv4 CIDR range on the AWS side that is allowed to communicate over the VPN tunnels. The default is 0.0.0.0/0.
0.0.0.0/0

▼ Tunnel 1 options - *optional* Info
Customize tunnel inside CIDR and pre-shared keys for your VPN tunnels. Unspecified tunnel options will be randomly generated by Amazon.

Inside IPv4 CIDR for tunnel 1
Generated by Amazon
A size /30 IPv4 CIDR block from the 169.254.0.0/16 range.

Pre-shared key for tunnel 1
The pre-shared key (PSK) to establish initial authentication between the virtual private gateway and customer gateway.
Generated by Amazon
The pre-shared key must have 8-64 characters. Valid characters: A-Z, a-z, 0-9, _ and . The key cannot begin with a zero.

Advanced options for tunnel 1
○ Use default options
● Edit tunnel 1 options

Phase 1 encryption algorithms
The permitted encryption algorithms for the VPN tunnel for phase 1 IKE negotiations.
Select encryption algorithms ▼
AES128 ✕ | AES256 ✕ | AES128-GCM-16 ✕ | AES256-GCM-16 ✕

Phase 2 encryption algorithms
The permitted encryption algorithms for the VPN tunnel for phase 2 IKE negotiations.
Select encryption algorithms ▼
AES128 ✕ | AES256 ✕ | AES128-GCM-16 ✕ | AES256-GCM-16 ✕

Phase 1 integrity algorithms
The permitted integrity algorithms for the VPN tunnel for phase 1 IKE negotiations.
Select integrity algorithms ▼
SHA1 ✕ | SHA2-256 ✕ | SHA2-384 ✕ | SHA2-512 ✕

Phase 2 integrity algorithms
The permitted integrity algorithms for the VPN tunnel for phase 2 IKE negotiations.
Select integrity algorithms ▼
SHA1 ✕ | SHA2-256 ✕ | SHA2-384 ✕ | SHA2-512 ✕

Phase 1 DH group numbers
The permitted Diffie-Hellman group numbers for the VPN tunnel for phase 1 IKE negotiations.
Select DH group numbers ▼
2 ✕ | 14 ✕ | 15 ✕ | 16 ✕ | 17 ✕ | 18 ✕ | 19 ✕ | 20 ✕ | 21 ✕ | 22 ✕ | 23 ✕ | 24 ✕

Phase 2 DH group numbers
The permitted Diffie-Hellman group numbers for the VPN tunnel for phase 2 IKE negotiations.
Select DH group numbers ▼
2 ✕ | 5 ✕ | 14 ✕ | 15 ✕ | 16 ✕ | 17 ✕ | 18 ✕ | 19 ✕ | 20 ✕ | 21 ✕ | 22 ✕ | 23 ✕ | 24 ✕

IKE Version
The internet key exchange (IKE) version permitted for the VPN tunnel.
Select IKE Version ▼
ikev1 ✕ | ikev2 ✕

Phase 1 lifetime (seconds)
The lifetime for phase 1 of the IKE negotiation, in seconds.
28,800
Supported values between: 900 and 28,800.

Phase 2 lifetime (seconds)
The lifetime for phase 2 of the IKE negotiation, in seconds.
3,600
Supported values between: 900 and 3,600, has to be less that phase 1 lifetime.

Rekey margin time (seconds)
The period of time before phase 1 and 2 lifetimes expire, during which AWS initiates an IKE rekey.
270
Supported values between: 60 and half of phase 2 lifetime.

Rekey fuzz (percentage)
The percentage of the rekey window during which the rekey time is randomly selected.
100
Supported values between: 0 and 100.

Replay window size (packets)
The number of packets in an IKE replay window.
1024
Supported values between: 64 and 2048.

DPD timeout (seconds)
The number of seconds after which a DPD timeout occurs.
30
Supported values must be 30 or higher.

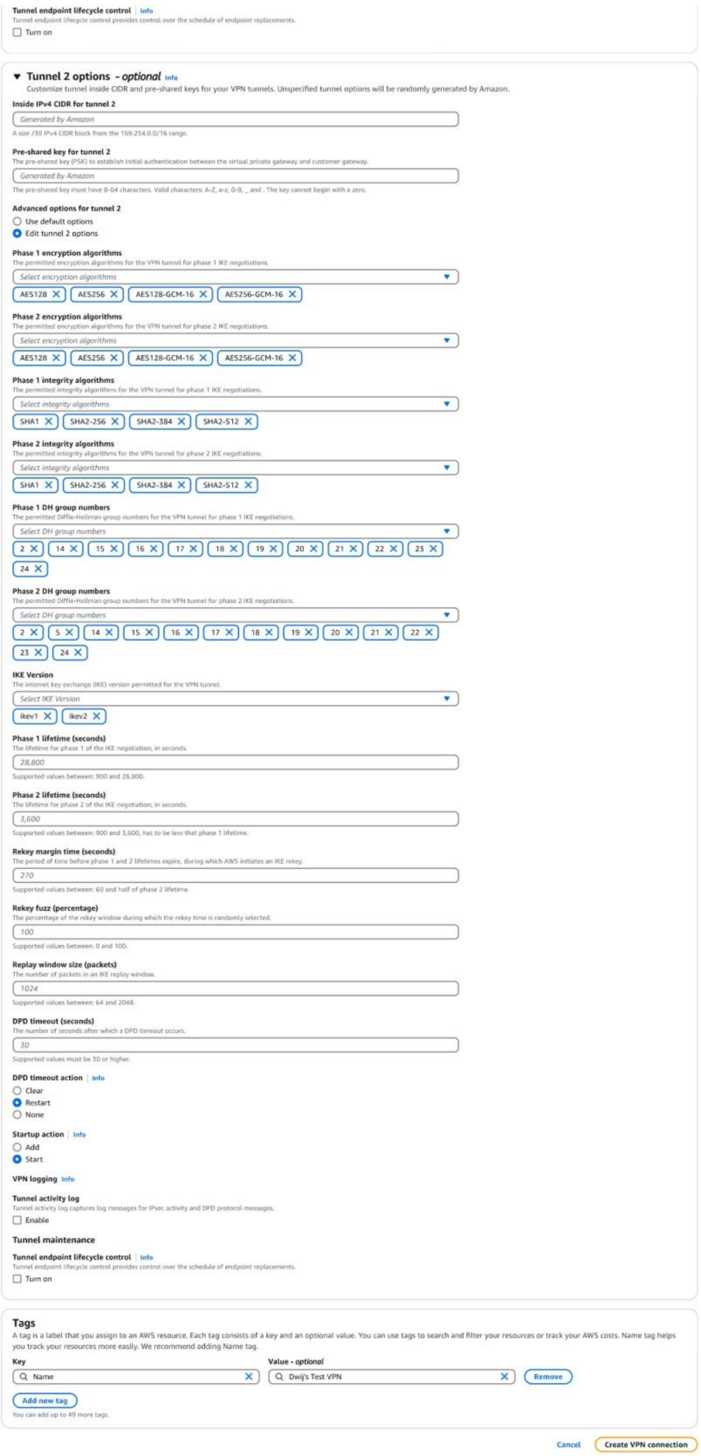
DPD timeout action | Info
○ Clear
● Restart
○ None

Startup action | Info
○ Add
● Start

VPN logging Info

Tunnel activity log
Tunnel activity log captures log messages for IPsec activity and DPD protocol messages.
□ Enable

Tunnel maintenance



Tunnel endpoint lifecycle control | Info

Tunnel endpoint lifecycle control provides control over the schedule of endpoint replacements.

□ Turn on

▼ Tunnel 2 options - *optional* Info

Customize tunnel inside CIDR and pre-shared keys for your VPN tunnels. Unspecified tunnel options will be randomly generated by Amazon.

Inside IPv4 CIDR for tunnel 2

Generated by Amazon

A size /30 IPv4 CIDR block from the 169.254.0.0/16 range.

Pre-shared key for tunnel 2

The pre-shared key (PSK) to establish initial authentication between the virtual private gateway and customer gateway.

Generated by Amazon

The pre-shared key must have 8-64 characters. Valid characters: A-Z, a-z, 0-9, _ and . The key cannot begin with a zero.

Advanced options for tunnel 2

○ Use default options
● Edit tunnel 2 options

Phase 1 encryption algorithms

The permitted encryption algorithms for the VPN tunnel for phase 1 IKE negotiations.

Select encryption algorithms ▼

AES128 ✕ AES256 ✕ AES128-GCM-16 ✕ AES256-GCM-16 ✕

Phase 2 encryption algorithms

The permitted encryption algorithms for the VPN tunnel for phase 2 IKE negotiations.

Select encryption algorithms ▼

AES128 ✕ AES256 ✕ AES128-GCM-16 ✕ AES256-GCM-16 ✕

Phase 1 integrity algorithms

The permitted integrity algorithms for the VPN tunnel for phase 1 IKE negotiations.

Select integrity algorithms ▼

SHA1 ✕ SHA2-256 ✕ SHA2-384 ✕ SHA2-512 ✕

Phase 2 integrity algorithms

The permitted integrity algorithms for the VPN tunnel for phase 2 IKE negotiations.

Select integrity algorithms ▼

SHA1 ✕ SHA2-256 ✕ SHA2-384 ✕ SHA2-512 ✕

Phase 1 DH group numbers

The permitted Diffie-Hellman group numbers for the VPN tunnel for phase 1 IKE negotiations.

Select DH group numbers ▼

2 ✕ 14 ✕ 15 ✕ 16 ✕ 17 ✕ 18 ✕ 19 ✕ 20 ✕ 21 ✕ 22 ✕ 23 ✕
24 ✕

Phase 2 DH group numbers

The permitted Diffie-Hellman group numbers for the VPN tunnel for phase 2 IKE negotiations.

Select DH group numbers ▼

2 ✕ 5 ✕ 14 ✕ 15 ✕ 16 ✕ 17 ✕ 18 ✕ 19 ✕ 20 ✕ 21 ✕ 22 ✕
23 ✕ 24 ✕

IKE Version

The internet key exchange (IKE) version permitted for the VPN tunnel.

Select IKE Version ▼

ikev1 ✕ ikev2 ✕

Phase 1 lifetime (seconds)

The lifetime for phase 1 of the IKE negotiation, in seconds.

28,800

Supported values between: 900 and 28,800.

Phase 2 lifetime (seconds)

The lifetime for phase 2 of the IKE negotiation, in seconds.

3,600

Supported values between: 900 and 3,600, has to be less that phase 1 lifetime.

Rekey margin time (seconds)

The period of time before phase 1 and 2 lifetimes expire, during which AWS initiates an IKE rekey.

270

Supported values between: 60 and half of phase 2 lifetime.

Rekey fuzz (percentage)

The percentage of the rekey window during which the rekey time is randomly selected.

100

Supported values between: 0 and 100.

Replay window size (packets)

The number of packets in an IKE replay window.

1024

Supported values between: 64 and 2048.

DPD timeout (seconds)

The number of seconds after which a DPD timeout occurs.

30

Supported values must be 30 or higher.

DPD timeout action | Info

○ Clear
● Restart
○ None

Startup action | Info

○ Add
● Start

VPN logging Info

Tunnel activity log

Tunnel activity log captures log messages for IPsec activity and DPD protocol messages.

□ Enable

Tunnel maintenance

Tunnel endpoint lifecycle control | Info

Tunnel endpoint lifecycle control provides control over the schedule of endpoint replacements.

□ Turn on

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs. Name tag helps you track your resources more easily. We recommend adding Name tag.

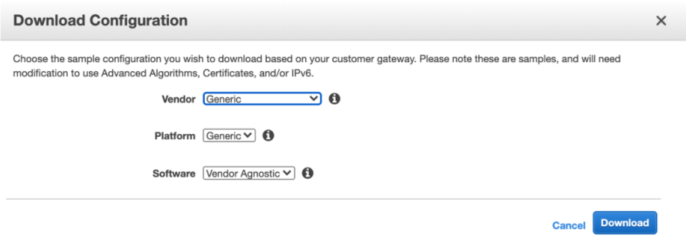
Key	Value - *optional*	
Name ✕	Dwij's Test VPN ✕	Remove

Add new tag

You can add up to 49 more tags.

Cancel Create VPN connection

Download Configuration:



Download Configuration

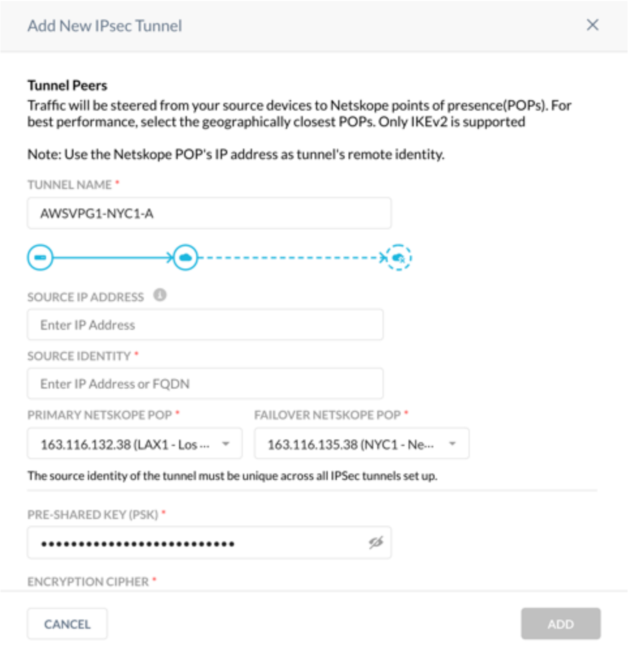
Choose the sample configuration you wish to download based on your customer gateway. Please note these are samples, and will need modification to use Advanced Algorithms, Certificates, and/or IPv6.

Vendor: Generic

Platform: Generic

Software: Vendor Agnostic

Example of adding Tunnel:



Add New IPsec Tunnel

Tunnel Peers

Traffic will be steered from your source devices to Netskope points of presence(POPs). For best performance, select the geographically closest POPs. Only IKEv2 is supported

Note: Use the Netskope POP's IP address as tunnel's remote identity.

TUNNEL NAME *: AWSVPG1-NYC1-A

SOURCE IP ADDRESS: Enter IP Address

SOURCE IDENTITY *: Enter IP Address or FQDN

PRIMARY NETSKOPE POP *: 163.116.132.38 (LAX1 - Los ...

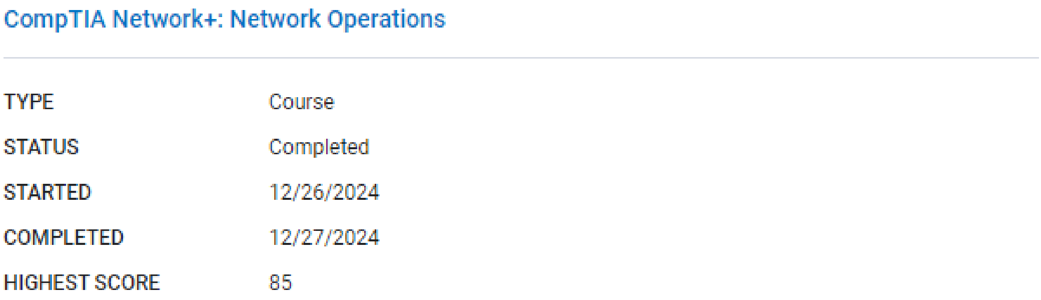
FAILOVER NETSKOPE POP *: 163.116.135.38 (NYC1 - Ne...

The source identity of the tunnel must be unique across all IPSec tunnels set up.

PRE-SHARED KEY (PSK) *: ••••••••••••••••••••••••••

ENCRYPTION CIPHER *

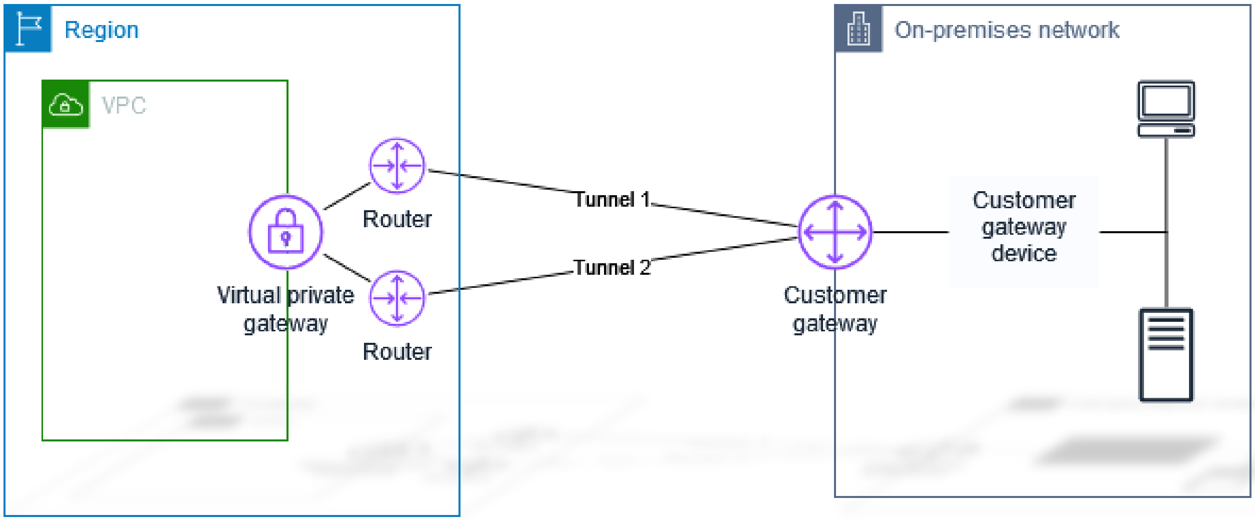
Apart than this, I also completed a small course on CompTIA Network+: Network Operations, from Infosys Springboard. I learned about network availability, including statistics and sensors. I explored the Simple Network Management Protocol (SNMP) and how to use network device logs like Syslog, Audit etc. I also learned environmental factors like temperature, humidity, and electrical issues as well as data centre's Hot aisle to cold aisle, problem with wirings etc. I learned about organizational documents and policies, and how to plan for incident response, disaster recovery. I explored hardening and security policy planning strategies, and the importance of maintaining essential documentation.



CompTIA Network+: Network Operations

TYPE	Course
STATUS	Completed
STARTED	12/26/2024
COMPLETED	12/27/2024
HIGHEST SCORE	85

The task given to analyze the following VPN Architecture:



Solution:

Here a VPC is created in an AWS Region and on the other side there is a Local On-Premises Network. They both need to be connected to each other for communication between them. So AWS creates a Virtual Private Gateway for traffic to enter which is connected to router which gives route to the traffic that is coming through the tunnels which are connected to the Customer Side gateway on the Local On-Premises.

AWS Components Needed:

Component	**Description**
Virtual Private Gateway (VPG)	Connects your on-premises network to your AWS VPC.
Customer Gateway	Defines IP of customer to connect it to the route and tunnel.
Virtual Private Cloud (VPC)	Your network in AWS where your resources are stored.
Routers	Devices that route traffic between your on-premises network and the VPN tunnels
Tunnel Connection	To transfer the network from one end point to another