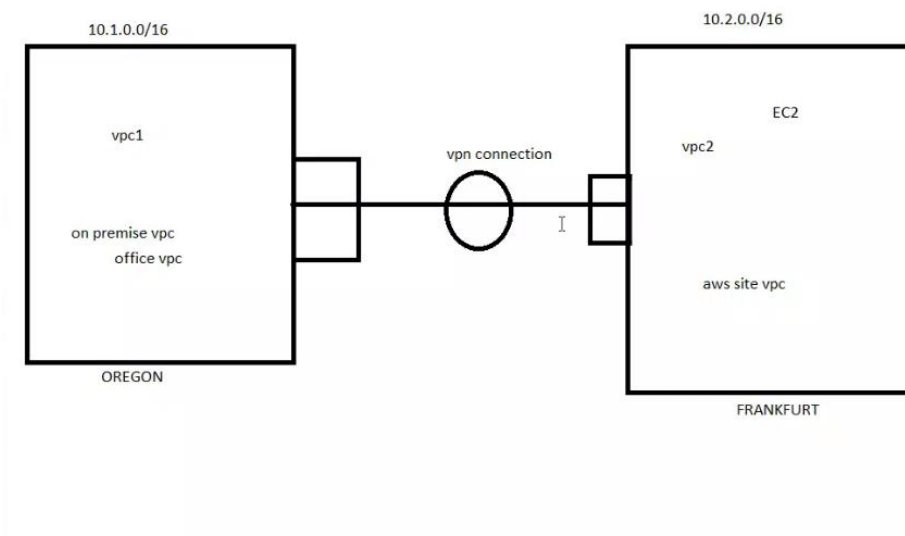


AWS SITE TO SITE VPN:

AWS Site-to-Site VPN is a way for companies to connect their office or data center to their resources on Amazon Web Services (AWS) securely. It's like a secret tunnel that allows data to travel between their own network and their resources on AWS without being intercepted by anyone else. This is helpful for businesses that want to use cloud resources like servers and databases, but still need to communicate with their own network in a secure way.

First create two **VPC** in different-different region:



First VPC:

The screenshot shows the 'VPC settings' page in the AWS console. It includes options for creating a VPC only or with other resources, a name tag field, and selections for IPv4 and IPv6 CIDR blocks. The IPv4 CIDR is set to 10.1.0.0/16, and the IPv6 option is set to 'No IPv6 CIDR block'. The tenancy is set to 'Default'.

VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

☒ VPC only ☐ VPC and more

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

neerajVPC1

IPv4 CIDR block [Info](#)
☒ IPv4 CIDR manual input
☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR
10.1.0.0/16

IPv6 CIDR block [Info](#)
☒ No IPv6 CIDR block
☐ IPAM-allocated IPv6 CIDR block
☐ Amazon-provided IPv6 CIDR block
☐ IPv6 CIDR owned by me

Tenancy [Info](#)
Default

The screenshot shows the 'vpc-0680bd77973628fa6 / neerajVPC1' details page. It includes a sidebar with navigation links for VPC dashboard, EC2 Global View, and various VPC resources. The main content area displays the VPC details in a table format, including VPC ID, State (Available), DNS hostnames (Disabled), DNS resolution (Enabled), Tenancy (Default), DHCP option set, Main route table, Main network ACL, IPv6 pool, IPv6 CIDR (Network border group), Network Address Usage metrics, Route 53 Resolver DNS Firewall rule groups, and Owner ID.

VPC dashboard ✕
EC2 Global View [New](#)
Filter by VPC:
[Select a VPC](#)

▼ Virtual private cloud
[Your VPCs](#) [New](#)
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections

▼ Security

VPC > Your VPCs > vpc-0680bd77973628fa6

vpc-0680bd77973628fa6 / neerajVPC1 [Actions](#)

Details [Info](#)

VPC ID vpc-0680bd77973628fa6	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-0a2d4be1404e52152	Main route table rtb-041b6f3d33f53ff8d	Main network ACL acl-0ccbc9345ff30854c
Default VPC No	IPv4 CIDR 10.1.0.0/16	IPv6 pool -	IPv6 CIDR (Network border group) -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID 528519205020	

[Resource map](#) [New](#) | [CIDRs](#) | [Flow logs](#) | [Tags](#)

Resource map [Info](#)

VPC [Show details](#)
Your AWS virtual network

Subnets (0)
Subnets within this VPC

Route tables (1)
Route network traffic to resour

Create Subnet:

aws

Services

Search

[Option+S]

Oregon

AWSPowerUserAccess/neeraj.panwar@cloudeq.com

Create subnet [Info](#)

VPC

VPC ID
Create subnets in this VPC.
vpc-0680bd77973628fa6 (neerajVPC1)

Associated VPC CIDRs
IPv4 CIDRs
10.1.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
neeraj-subnet-1
The name can be up to 256 characters long.
Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
No preference

CloudShell

Feedback

Language

© 2023, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

aws

Services

Search

[Option+S]

Oregon

AWSPowerUserAccess/neeraj.panwar@cloudeq.com

VPC dashboard

EC2 Global View

Filter by VPC:
Select a 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

Endpoints

Endpoint services

NAT gateways

Peering connections

VPC > Subnets > subnet-076ed8e0e50c1d76e

subnet-076ed8e0e50c1d76e / neeraj-subnet-1

Actions

Details

Subnet ID subnet-076ed8e0e50c1d76e	Subnet ARN arn:aws:ec2:us-west-2:528519205020:subnet/subnet-076ed8e0e50c1d76e	State Available	IPv4 CIDR 10.1.0.0/16
Available IPv4 addresses 65531	IPv6 CIDR -	Availability Zone us-west-2a	Availability Zone ID usw2-az1
Network border group us-west-2	VPC vpc-0680bd77973628fa6 neerajVPC1	Route table rtb-045d146d9be5cf87a neeraj-rt-1	Network ACL acl-0ccbc9345ff30854c
Default subnet No	Auto-assign public IPv4 address No	Auto-assign IPv6 address No	Auto-assign customer-owned IPv4 address No
Customer-owned IPv4 pool -	Outpost ID -	IPv4 CIDR reservations -	IPv6 CIDR reservations -
IPv6-only No	Hostname type IP name	Resource name DNS A record Disabled	Resource name DNS AAAA record Disabled
DNS64 Disabled			

Create Internet Gateway:

Services

Search

[Option+S]

Oregon

AWSPowerUserAccess/neeraj.panwar@cloudeq.com

Create internet gateway [Info](#)

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

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

neeraj-ig-1

Tags - optional

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.

Key

Value - optional

Q Name

X

Q neeraj-ig-1

X

Remove

Q Owner

X

Q neeraj.panwar@cloudeq.com

X

Remove

Add new tag

You can add 48 more tags.

Cancel

Create internet gateway

CloudShell

Feedback

Language

© 2023, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

Services

Search

[Option+S]

Oregon

AWSPowerUserAccess/neeraj.panwar@cloudeq.com

VPC dashboard

EC2 Global View

Filter by VPC:

Select a 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

Endpoints

Endpoint services

NAT gateways

Peering connections

Security

The following internet gateway was created: igw-04b347ae58617482a - neeraj-ig-1. You can now attach to a VPC to enable the VPC to communicate with the internet.

Attach to a VPC

VPC > Internet gateways > igw-04b347ae58617482a

igw-04b347ae58617482a / neeraj-ig-1

Actions

Details

Info

Internet gateway ID

State

VPC ID

Owner

igw-04b347ae58617482a

Detached

-

528519205020

Tags

Manage tags

Q Search tags

< 1 >

Key

Value

Owner

neeraj.panwar@cloudeq.com

Name

neeraj-ig-1

CloudShell

Feedback

Language

© 2023, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

Attach it to VPC:

The screenshot shows the AWS console interface for attaching an Internet Gateway to a VPC. The breadcrumb navigation is 'VPC > Internet gateways > Attach to VPC (igw-04b347ae58617482a)'. The main heading is 'Attach to VPC (igw-04b347ae58617482a)' with an 'Info' link. Below this is a 'VPC' section with the instruction: 'Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.' Underneath is an 'Available VPCs' section with the instruction: 'Attach the internet gateway to this VPC.' A search bar contains the text 'vpc-0680bd77973628fa6'. Below the search bar is a link for the 'AWS Command Line Interface command'. At the bottom of the dialog are 'Cancel' and 'Attach internet gateway' buttons.

VPC > Internet gateways > Attach to VPC (igw-04b347ae58617482a)

Attach to VPC (igw-04b347ae58617482a) [Info](#)

VPC
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs
Attach the internet gateway to this VPC.

[AWS Command Line Interface command](#)

[Cancel](#) [Attach internet gateway](#)

Create Route Table:

The screenshot shows the 'Create route table' form in the AWS console. The breadcrumb navigation is 'VPC > Route tables > Create route table'. The main heading is 'Create route table' with an 'Info' link. Below this is a description: 'A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.' The form is divided into two main sections: 'Route table settings' and 'Tags'. The 'Route table settings' section has a 'Name - optional' field with the value 'neeraj-rt-1' and a 'VPC' dropdown menu with the selected value 'vpc-0680bd77973628fa6 (neerajVPC1)'. The 'Tags' section has a table with two rows: one with 'Name' as the key and 'neeraj-rt-1' as the value, and another with 'Owner' as the key and 'neeraj.panwar@cloudeq.com' as the value. Each row has a 'Remove' button. At the bottom of the 'Tags' section is an 'Add new tag' button and a note: 'You can add 48 more tags.' At the bottom of the form are 'Cancel' and 'Create route table' buttons.

VPC > Route tables > Create route table

Create route table [Info](#)

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

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

VPC
The VPC to use for this route table.

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.

Key	Value - optional	
<input type="text" value="Name"/>	<input type="text" value="neeraj-rt-1"/>	Remove
<input type="text" value="Owner"/>	<input type="text" value="neeraj.panwar@cloudeq.com"/>	Remove

[Add new tag](#)
You can add 48 more tags.

[Cancel](#) [Create route table](#)

Virtual private cloud

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

NAT gateways

Peering connections

Route table rtb-045d146d9be5cf87a | neeraj-rt-1 was created successfully.

VPC > Route tables > rtb-045d146d9be5cf87a

rtb-045d146d9be5cf87a / neeraj-rt-1

You can now check network connectivity with Reachability Analyzer

Run Reachability Analyzer

Details Info

Route table ID
rtb-045d146d9be5cf87a

Main
No

Explicit subnet associations
-

Edge associations
-

VPC
vpc-0680bd77973628fa6 | neerajVPC1

Owner ID
528519205020

Routes Subnet associations Edge associations Route propagation Tags

Routes (1)

Filter routes

Both

1

Edit routes

CloudShell Feedback Language

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

VPC > Route tables > rtb-045d146d9be5cf87a > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.1.0.0/16	local	Active	No
0.0.0.0/0	igw-04b347ae58617482a	-	No

Add route

Remove

Cancel

Preview

Save changes

CloudShell Feedback Language

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Virtual private cloud

EC2 Global View

Filter by VPC:

Select a 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

Endpoints

Endpoint services

NAT gateways

Peering connections

Security

Updated routes for rtb-045d146d9be5cf87a / neeraj-rt-1 successfully

Details

Routes

Subnet associations

Edge associations

Route propagation

Tags

Explicit subnet associations (0)

Edit subnet associations

Find subnet association

< 1 >

No subnet associations

You do not have any subnet associations.

Subnets without explicit associations (1)

Edit subnet associations

Find subnet association

< 1 >

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
neeraj-subnet-1	subnet-076ed8e0e50c1d76e	10.1.0.0/16	-

CloudShell

Feedback

Language

© 2023, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

VPC

Route tables

rtb-045d146d9be5cf87a

Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/1)

Filter subnet associations

< 1 >

<input checked="" type="checkbox"/>	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/>	neeraj-subnet-1	subnet-076ed8e0e50c1d76e	10.1.0.0/16	-	Main (rtb-041b6f3d33f53ff8d)

Selected subnets

subnet-076ed8e0e50c1d76e / neeraj-subnet-1

Cancel

Save associations

CloudShell

Feedback

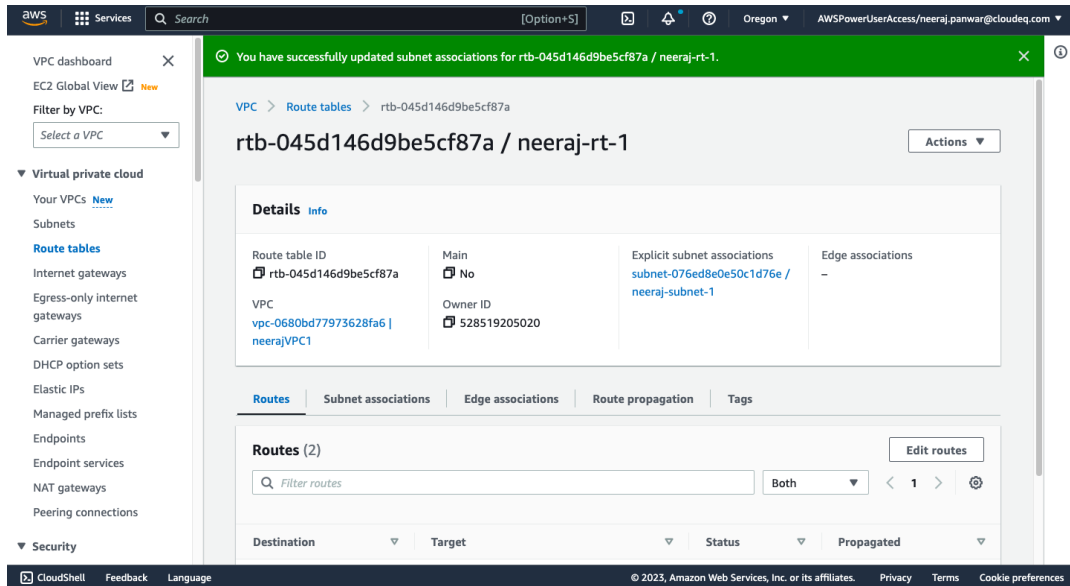
Language

© 2023, Amazon Web Services, Inc. or its affiliates.

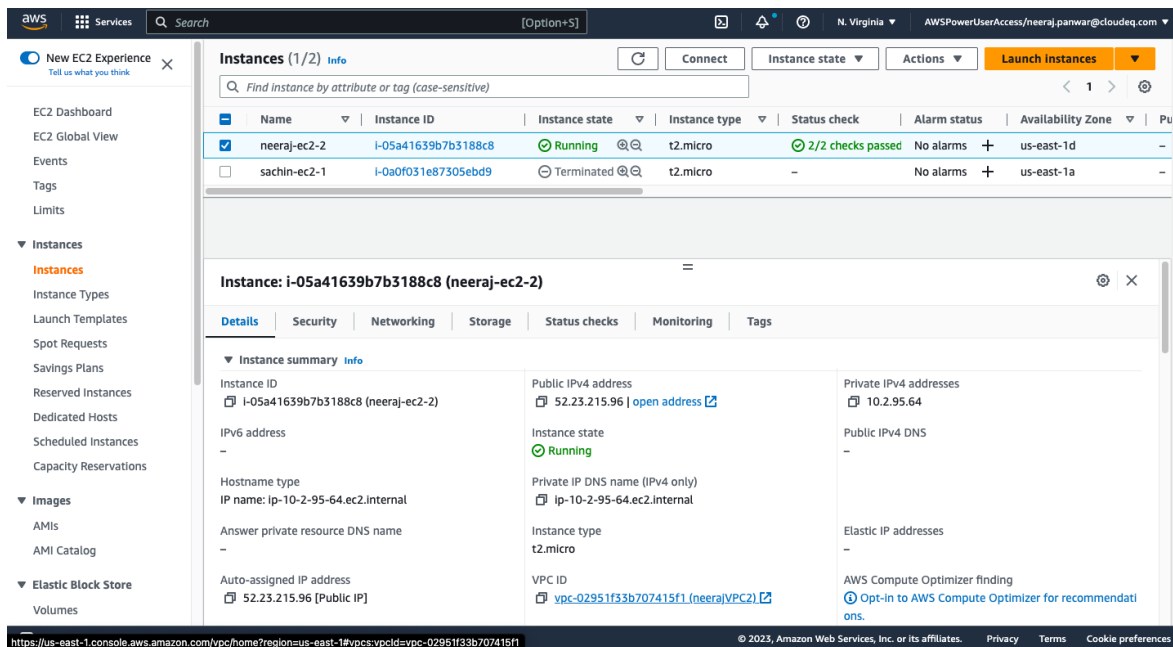
Privacy

Terms

Cookie preferences



Create EC2 Instance and Attach to VPC:



Create Second VPC:

The screenshot shows the AWS Management Console interface. On the left, the 'Virtual private cloud' section is expanded, showing 'Your VPCs' with a 'New' button. The main content area displays 'Your VPCs (1/4)' with a table listing VPCs. The 'neerajVPC2' is selected, and its details are shown below.

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
patyankvpc-1	vpc-0dcb202b2c2f4c93e	Available	10.0.0.0/16	-
neerajVPC2	vpc-02951f33b707415f1	Available	10.2.0.0/16	-
-	vpc-076eb9b0fa60396b5	Available	172.31.0.0/16	-
sachin-vpc-1	vpc-0f4ed21ac823a83e3	Available	10.1.0.0/16	-

vpc-02951f33b707415f1 / neerajVPC2

Details

VPC ID vpc-02951f33b707415f1	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-085ce0fb7e8ab7937	Main route table rtb-01dc5bcd7cbebd91	Main network ACL acl-06f1bd809ca506006
Default VPC No	IPv4 CIDR 10.2.0.0/16	IPv6 pool -	IPv6 CIDR (Network border group) -
Network Address Usage metrics	Route 53 Resolver DNS Firewall rule	Owner ID	

The screenshot shows the AWS Management Console interface. On the left, the 'Virtual private cloud' section is expanded, showing 'Internet gateways' with a 'New' button. The main content area displays 'Internet gateways' with a table listing gateways. The 'igw-0170d5416ac292ae7' is selected, and its details are shown below.

igw-0170d5416ac292ae7 / neeraj-ig-2

Details

Internet gateway ID igw-0170d5416ac292ae7	State Attached	VPC ID vpc-02951f33b707415f1 neerajVPC2	Owner 528519205020
--	-------------------	--	-----------------------

Tags

Key	Value
Name	neeraj-ig-2
Owner	neeraj.panwar@cloudeq.com

Create Site to site VPN

Create Customer Gateway:

The screenshot shows the 'Create Customer Gateway' form in the AWS console. The form is divided into several sections with input fields and labels.

Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.
neeraj-cg
Value must be 256 characters or less in length.

BGP ASN [Info](#)
The ASN of your customer gateway device.
65000
Value must be in 1 - 2147483647 range.

IP address [Info](#)
Specify the IP address for your customer gateway device's external interface.
52.23.215.96

Certificate ARN
The ARN of a private certificate provisioned in AWS Certificate Manager (ACM).
Select certificate ARN

Device - optional
Enter a name for the customer gateway device.
Enter device name

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.

The screenshot shows the 'Customer gateways' page in the AWS console. A green notification banner at the top states: 'You successfully created cgw-047814e75b8c2aad2 / neeraj-cg.' The page displays a table of customer gateways with one entry.

Customer gateways (1) [Info](#)

Filter customer gateways

Customer gateway ID: cgw-047814e75b8c2aad2

	Name	Customer gateway ID	State	BGP ASN	IP address
<input type="radio"/>	neeraj-cg	cgw-047814e75b8c2aad2	Available	65000	52.23.215.96

Select a customer gateway

Create Virtual Private Gateway:

Virtual private gateways (1/1) [Info](#)

Filter virtual private gateways

Virtual private gateway ID: vgw-09046268f23436062 [Clear filters](#)

Name	Virtual private gateway ID	State	Type	VPC
neeraj-vpg	vgw-09046268f23436062	Attached	ipsec.1	vpc-0680bd77973628fa6

vgw-09046268f23436062 / neeraj-vpg

[Details](#) [Tags](#)

Attach the VPC for virtual private gateway:

VPC > Virtual private gateways > vgw-09046268f23436062 > Attach to VPC

Attach to VPC [Info](#)

Details

Virtual private gateway ID
vgw-09046268f23436062

Available VPCs
Attach the virtual private gateway to this VPC.
vpc-0680bd77973628fa6 / neerajVPC1

[Cancel](#) [Attach to VPC](#)

Create Site to Site VPN:

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

neeraj-vpn
Value must be 256 characters or less in length.

Target gateway type [Info](#)

☒ Virtual private gateway
☐ Transit gateway
☐ Not associated

Virtual private gateway

vgw-09046268f23436062 / neeraj-vpg

Customer gateway [Info](#)

☒ Existing
☐ New

Customer gateway ID

cgw-047814e75b8c2aad2 / neeraj-cg

Routing options [Info](#)

☐ Dynamic (requires BGP)
☒ Static

Static IP prefixes [Info](#)

10.2.0.0/16

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.

Tunnel 1 options - optional [Info](#)

Tunnel 2 options - optional [Info](#)

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	
<input type="text" value="Name"/>	<input type="text" value="neeraj-vpn"/>	<input type="button" value="Remove"/>
<input type="text" value="Owner"/>	<input type="text" value="neeraj.panwar@cloudeq.com"/>	<input type="button" value="Remove"/>

You can add 48 more tags.

Virtual private cloud

EC2 Global View New

Filter by VPC:

Select a VPC

Virtual private cloud

Your VPCs New

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

NAT gateways

Peering connections

Security

Static

Local IPv4 network CIDR

0.0.0.0/0

Core network ARN

-

Static

Remote IPv4 network CIDR

0.0.0.0/0

Core network attachment ARN

-

Static

Local IPv6 network CIDR

-

Gateway association state

associated

Static

Remote IPv6 network CIDR

-

Outside IP address type

PublicIpv4

Tunnel details

Static routes

Tags

Tunnel state

Tunnel number	Outside IP address	Inside IPv4 CIDR	Inside IPv6 CIDR	Status	Last status change
Tunnel 1	34.211.9.27	169.254.57.192/30	-	Down	April 10, 2023, 12:06:48 (UTC+)
Tunnel 2	52.13.50.168	169.254.253.44/30	-	Down	April 10, 2023, 12:06:48 (UTC+)

Tunnel 1 options

Tunnel 2 options

CloudShell

Feedback

Language

© 2023, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

Services

Search

[Option+S]

N. Virginia

AWSPowerUserAccess/neeraj.panwar@cloudeq.com

Amazon Linux 2023

https://aws.amazon.com/linux/amazon-linux-2023

```
(ec2-user@ip-10-2-95-64 ~)$ sudo su
[root@ip-10-2-95-64 ~]# yum install openswan -y
Last metadata expiration check: 0:26:46 ago on Mon Apr 10 06:16:35 2023.
No match for argument: openswan
Error: Unable to find a match: openswan
[root@ip-10-2-95-64 ~]#
```

i-05a41639b7b3188c8 (neeraj-ec2-2)

PublicIPs: 52.23.215.96 PrivateIPs: 10.2.95.64

CloudShell

Feedback

Language

© 2023, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

aws

Services

Search

[Option+S]

Oregon

AWSPowerUserAccess/neeraj.panwar@cloudeq.com

Customer gateways

Virtual private gateways

Site-to-Site VPN connections

Client VPN endpoints

AWS Verified Access

Transit gateways

Verified Access instances

Verified Access trust providers

Verified Access groups

Verified Access endpoints

Transit gateways

Transit gateway attachments

Transit gateway policy tables

Transit gateway route tables

Transit gateway

VPN connections (1/1) Info

Actions

Download configuration

Create VPN connection

Filter VPN connections

< 1 >

Name	VPN ID	State	Virtual private gateway	Transit gateway
neeraj-vpn	vpn-02d75dd1649279de1	Available	vgw-09046268f23436062	-

vpn-02d75dd1649279de1 / neeraj-vpn

DetailsTunnel detailsStatic routesTags

CloudShell

Feedback

Language

© 2023, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences