# Versa Networks SASE Gateway Integration with AWS Cloud

## About This Document

This document provides AWS Cloud integration options and low-level configuration for integrating a SASE solution with AWS cloud infrastructure. It covers multiple Integration options involving SASE gateways, AWS native networking services, and SD-WAN devices to deliver secure, optimized connectivity to workloads hosted in AWS. The guidance is based on Concerto 12.2.1, Director 22.1.4, and VOS 22.1.4

## Document Information

| | |
|---|---|
| **Title** | **Versa Networks SASE Gateway Integration with AWS Cloud** |
| **Author** | Versa Professional Services |
| **Version** | V 1.0 |

## Disclaimer

Information contained in this document regarding Versa Networks (the Company) is considered proprietary.

## Before you begin

Before you proceed with the steps outlined in this document, please ensure you've met the following prerequisites.

- The provider administrator must complete your tenant configuration. If you haven't received this information, please contact your Managed Service Provider or Account Manager for assistance.
- You have the Enterprise Administrator (Tenant Admin) credentials for the Versa SASE portal, also called the Concerto User Interface.

## Contents

## Introduction to Public Cloud

A public cloud is a cloud computing model where IT infrastructure like servers, networking, and storage resources are offered as virtual resources accessible over the internet. Public cloud providers deliver services under three main models, often referred to as the Cloud Service Models: IaaS, PaaS, and SaaS

**Infrastructure as a Service**: IaaS offers the basic building blocks of IT infrastructure — delivered over the internet. It allows users to rent virtualized computing resources like:

- Virtual Machines (VMs)
- Storage (Block, File, Object)
- Networks (VPCs, Load Balancers, IPs)

**Common Use Cases:**

- Hosting websites or enterprise applications
- Running development/test environments
- Backup and disaster recovery solutions

## Terminologies used:

1. **VPC:** Virtual Private Cloud
   VPC is a virtual network environment that allows you to launch AWS resources in a logically isolated section of the AWS Cloud. It's like having your own virtual network within AWS, offering you control over your IP address range, subnets, and networking configurations.
2. **IGW:** Internet Gateway
   IGW is a key component of a Virtual Private Cloud (VPC) that allows resources within the VPC to communicate with the internet. It facilitates both inbound and outbound traffic between your VPC and the outside world.
3. **EC2:** Elastic Compute Cloud
   EC2 is a web service within Amazon Web Services (AWS) that provides virtual servers called instances. These instances allow users to run applications on the AWS cloud, offering scalable and secure computing capacity on demand.
4. **Security Groups:**
   Security Groups act as virtual firewalls, controlling the flow of network traffic to and from EC2 instances within a VPC. They are a key part of AWS's security, helping to ensure only authorized traffic can reach your instances. Security Groups work by defining rules that specify which types of traffic (TCP, UDP, ICMP) and on which ports are allowed to pass through.
5. **VPN:** Virtual Private Network

VPN enables secure connections between your on-premises network, remote offices, and the AWS cloud. It provides encrypted tunnels for data transmission, enhancing security and privacy. AWS Site-to-Site VPN connects on-premises networks to an AWS VPC.

6. **VGW:** Virtual Private Gateway

   VGW is a VPN concentrator that provides the AWS side endpoint for a Site-to-Site VPN connection between your on-premises network and your AWS Virtual Private Cloud (VPC). It's crucial for establishing a secure tunnel between your VPC and external networks.

7. **TGW:** Transit Gateway

   TGW is a managed service that simplifies network connectivity within and between AWS regions and on-premises networks. Think of it as a central hub that connects multiple VPCs (Virtual Private Clouds) and other network resources.

## Cloud Integration Options

When customer workloads are hosted in the public cloud, secure access from remote users or on-prem sites is essential. SASE Gateway integration ensures encrypted connectivity, centralized policy enforcement, and Zero Trust access. To achieve this, there are three common integration models based on architecture and scale.

1. Option 1 - VGW
2. Option 2 - TGW
3. Option 3 – Versa SDWAN

To achieve the above use cases, we require the below components from AWS to integrate with an on-prem SASE (Secure Access Service Edge) gateway.

1. VPC (Virtual Private Cloud)
2. Subnets
3. Route Tables
4. Elastic IP
5. Internet Gateway (IGW) (if needed for public access)
6. Virtual Private Gateway (VGW)
7. Customer Gateway (CGW)
8. VPN Connection
9. Security Groups & NACLs

## Creating a VPC:

Amazon Virtual Private Cloud (VPC) is a logically isolated section of the AWS Cloud where you can launch AWS resources in a custom-defined virtual network.

**Purpose of VPC:**

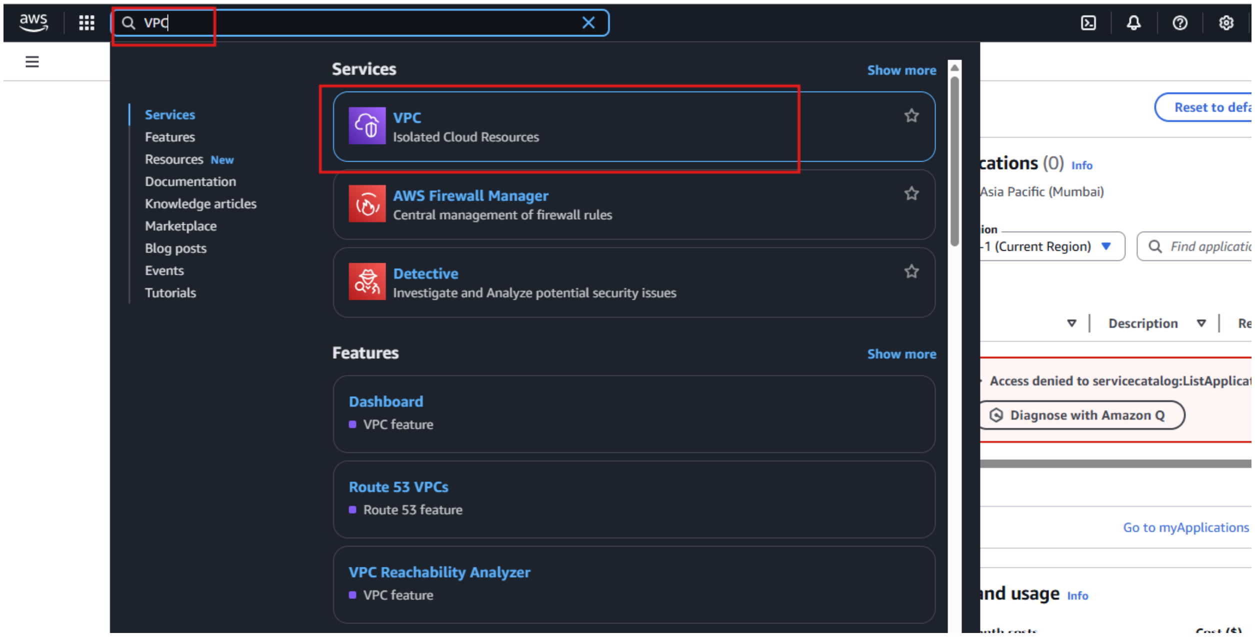
- Network Control: Define your own IP address ranges, subnets, and route tables.

- Security: Use security groups and network ACLs to control traffic in and out of resources.
- Connectivity Options: Connect to the internet, other AWS services, or on-prem networks via VPN or Direct Connect.
- Isolation & Customization: Achieve granular control over how your workloads communicate within and outside AWS.

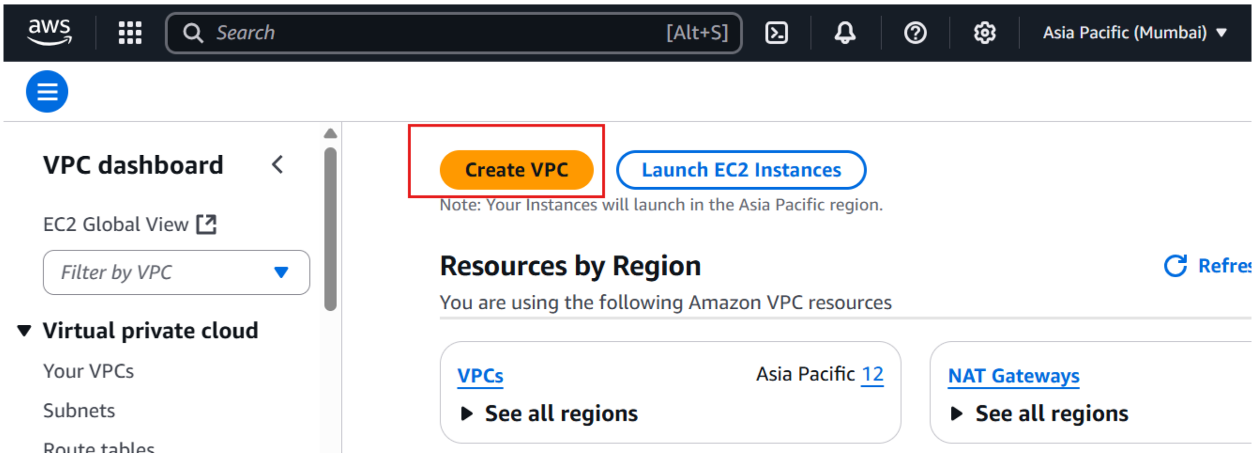
**Common Use Cases:**

- Hosting secure web applications
- Creating hybrid cloud environments
- Isolating production and development environments

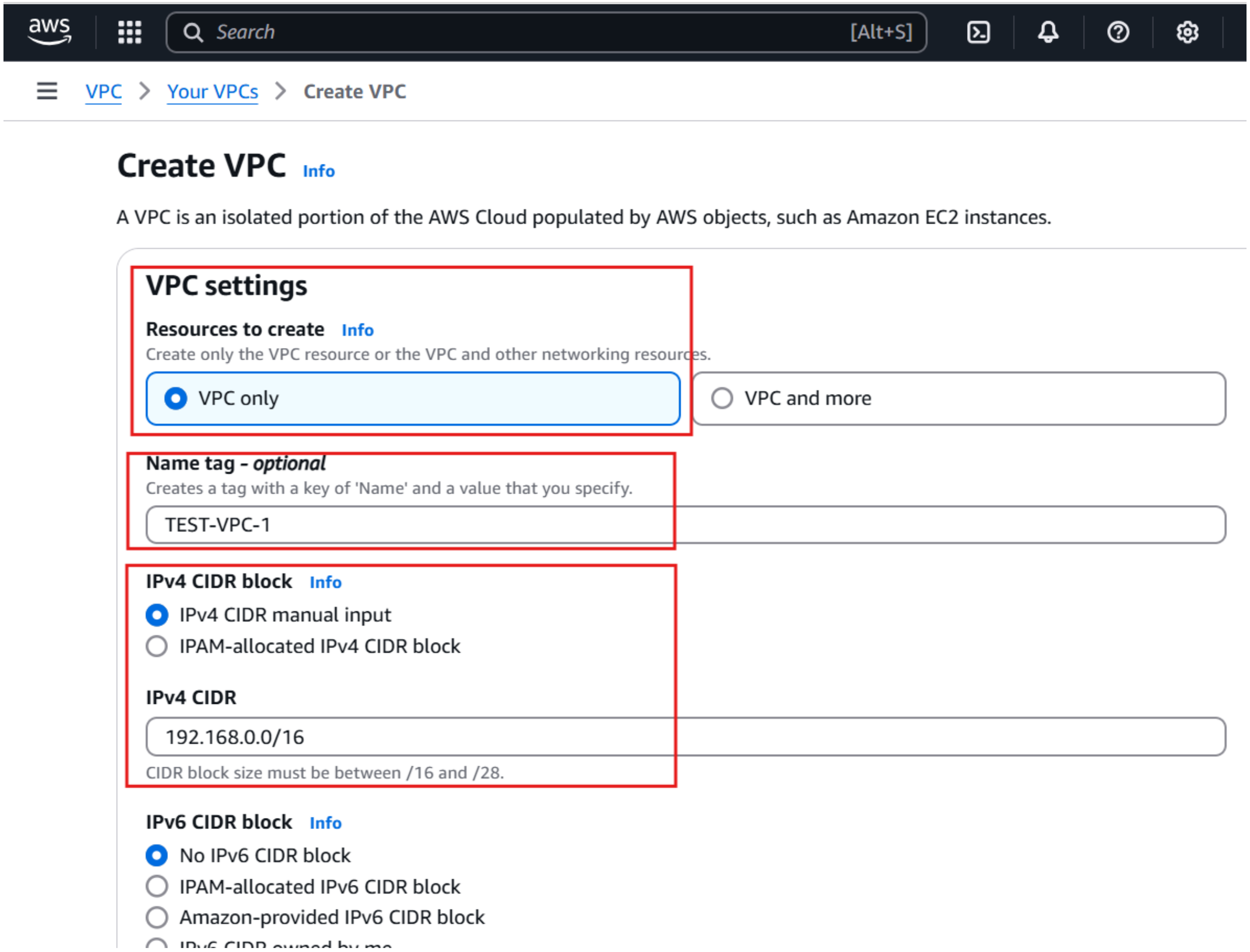
To create a VPC in AWS, type VPC in the search bar and select VPC.



Click on “Create VPC” to create a new VPC.



Under VPC Settings select “VPC only”, provide a Name-tag and the IPv4 CIDR block used inside the VPC, then click on “Create VPC”.



## Create VPC

Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

### 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.

TEST-VPC-1

**IPv4 CIDR block** Info

● IPv4 CIDR manual input

○ IPAM-allocated IPv4 CIDR block

**IPv4 CIDR**

192.168.0.0/16

CIDR block size must be between /16 and /28.

**IPv6 CIDR block** Info

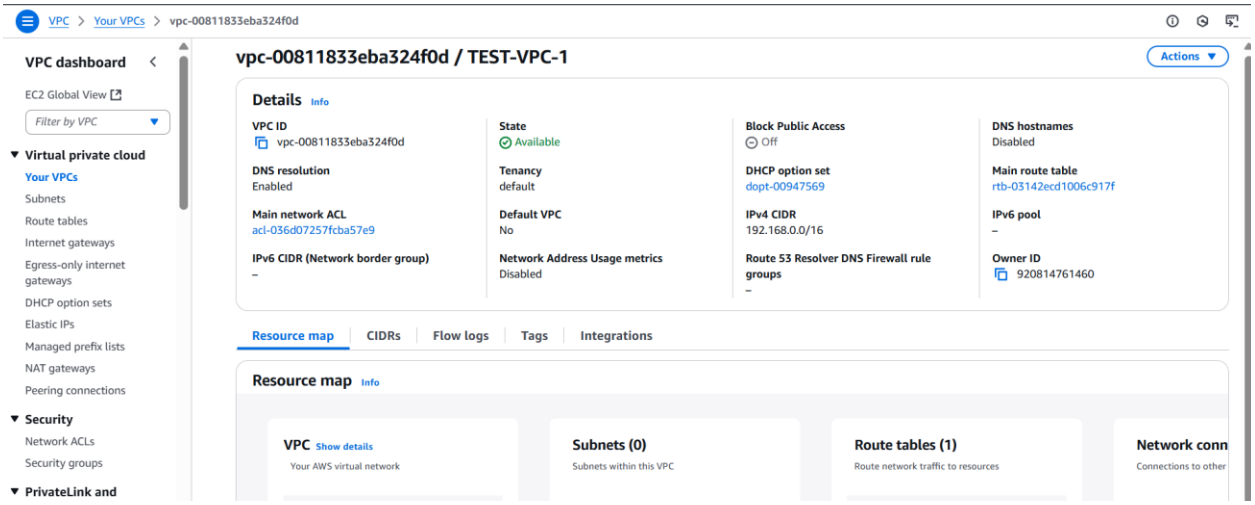
● No IPv6 CIDR block

○ IPAM-allocated IPv6 CIDR block

○ Amazon-provided IPv6 CIDR block

○ IPv6 CIDR owned by me

Once VPC is created, the state will be shown as “Available”.



VPC > Your VPCs > vpc-00811833eba324f0d

vpc-00811833eba324f0d / TEST-VPC-1

Details Info

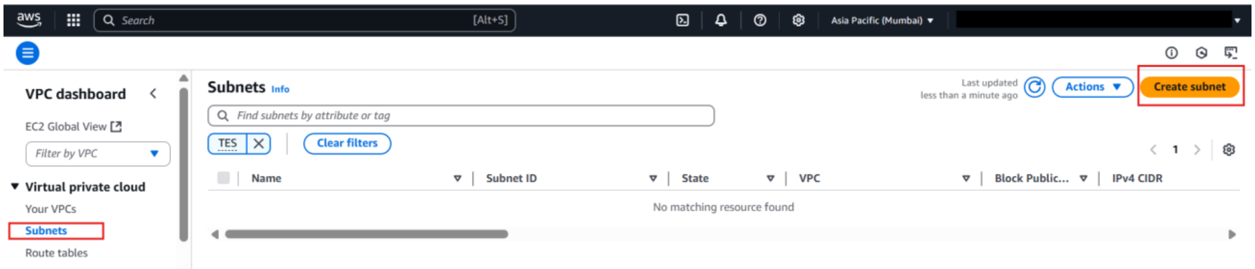
| VPC ID | State | Block Public Access | DNS hostnames |
|---|---|---|---|
| vpc-00811833eba324f0d | Available | Off | Disabled |
| **DNS resolution** | **Tenancy** | **DHCP option set** | **Main route table** |
| Enabled | default | dopt-00947569 | rtb-03142ecd1006c917f |
| **Main network ACL** | **Default VPC** | **IPv4 CIDR** | **IPv6 pool** |
| acl-036d07257fcba57e9 | No | 192.168.0.0/16 | – |
| **IPv6 CIDR (Network border group)** | **Network Address Usage metrics** | **Route 53 Resolver DNS Firewall rule groups** | **Owner ID** |
| – | Disabled | – | 920814761460 |

## Creating Subnets:

A subnet is a range of IP addresses in your VPC. You can create AWS resources, such as EC2 instances, in specific subnets. When you create a subnet in AWS, certain IP addresses within the subnet's CIDR block are reserved and cannot be assigned to resources. These reservations ensure proper network operation and management.

- **Reserved IP addresses** in an AWS subnet are five addresses AWS sets aside for network operations (e.g., network ID, router, DNS, and broadcast).
  - Example: In a 10.0.0.0/24 subnet, the reserved IPs are:
    10.0.0.0, 10.0.0.1, 10.0.0.2, 10.0.0.3, and 10.0.0.255.
- The remaining IP addresses in the subnet's CIDR block are available for assignment to AWS resources, such as EC2 instances. For example, in a /24 subnet (which contains 256 IP addresses), after reserving 5 addresses, 251 IP addresses are usable.

To create Subnets, under VPC dashboard, go to Virtual private Cloud → Subnets → Create Subnet.



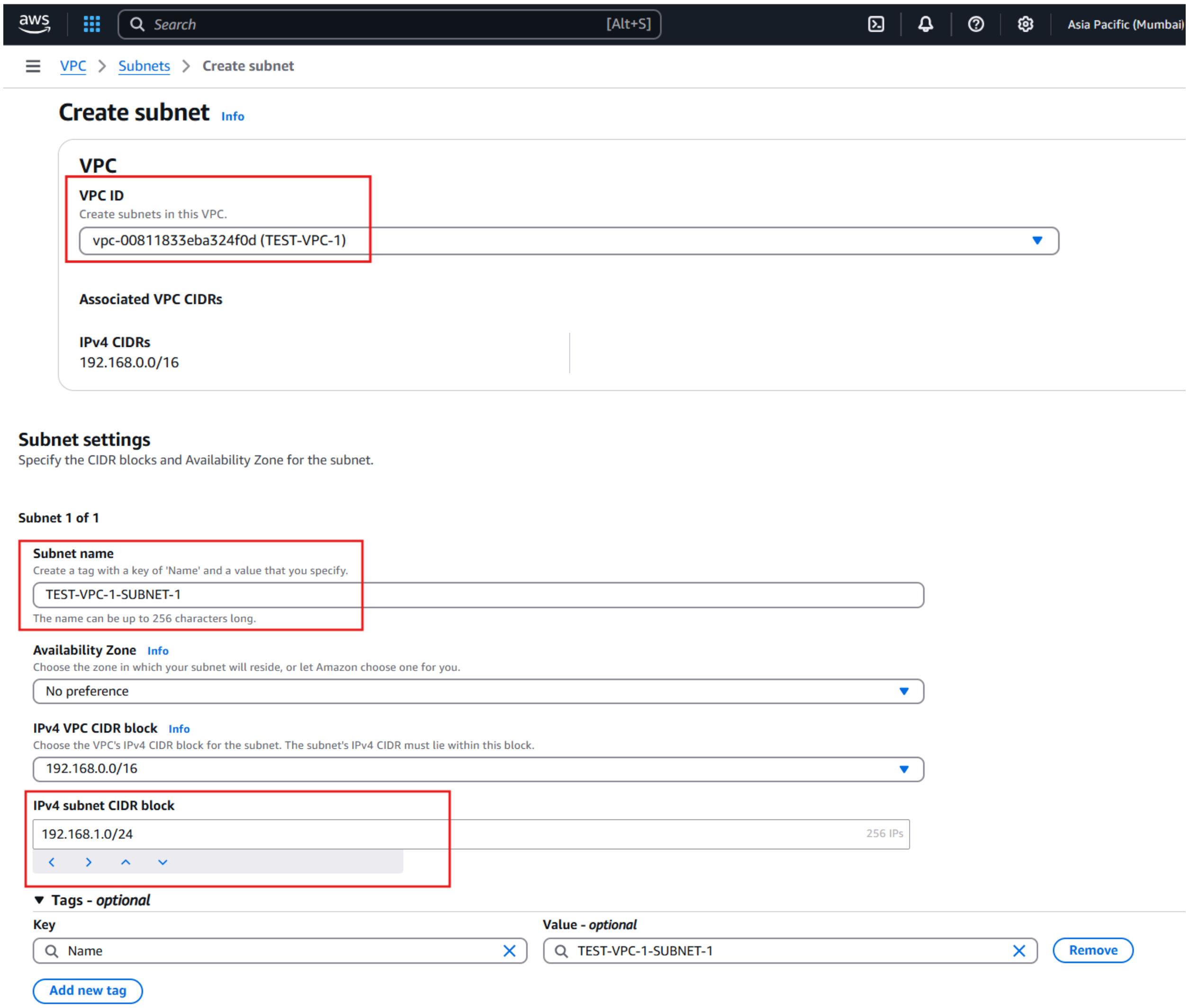
[redacted]

| | Name | Subnet ID | State | VPC | Block Public... | IPv4 CIDR |
|---|---|---|---|---|---|---|

No matching resource found

Selecting VPC under VPC ID will open Subnet settings.

Under Subnet settings, provide the Subnet name and the IPv4 subnet CIDR block.



Create subnet Info

VPC

VPC ID
Create subnets in this VPC.
vpc-00811833eba324f0d (TEST-VPC-1)

Associated VPC CIDRs

IPv4 CIDRs
192.168.0.0/16

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.
TEST-VPC-1-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

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
192.168.0.0/16

IPv4 subnet CIDR block
192.168.1.0/24 256 IPs

▼ Tags - *optional*

| Key | Value - *optional* |
|---|---|
| Name | TEST-VPC-1-SUBNET-1 |

## Creating IGW for the VPC:

An Internet Gateway is a horizontally scaled, redundant, and highly available AWS-managed component that allows communication between instances in your VPC public subnets and the internet.

**Purpose in This Use Case:**

While the main connectivity between AWS and the on-prem SASE gateway is established using VGW/TGW through IPsec site-to-site tunnels/SDWAN, an IGW may still be used in this scenario for:

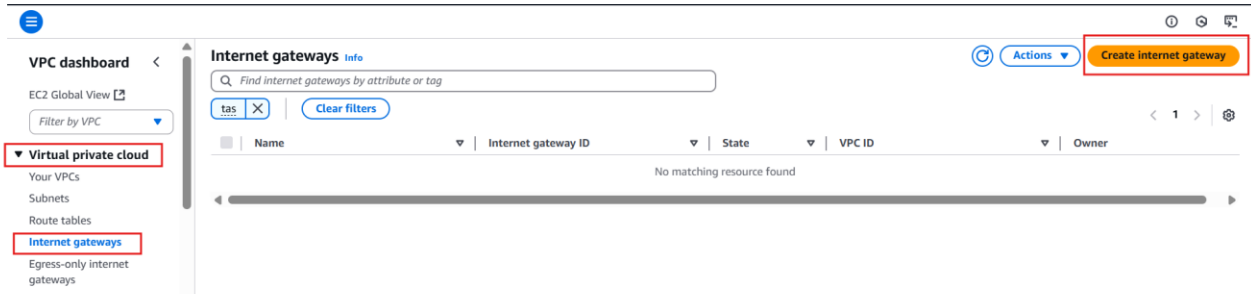
- Allowing public internet access for instances in the public subnet (e.g., for updates, management, or outbound monitoring).
- Supporting hybrid architecture where internet-bound traffic from AWS resources not routed through the IPsec tunnel is handled via IGW.

**Key Points:**

- IGW must be attached to the VPC.

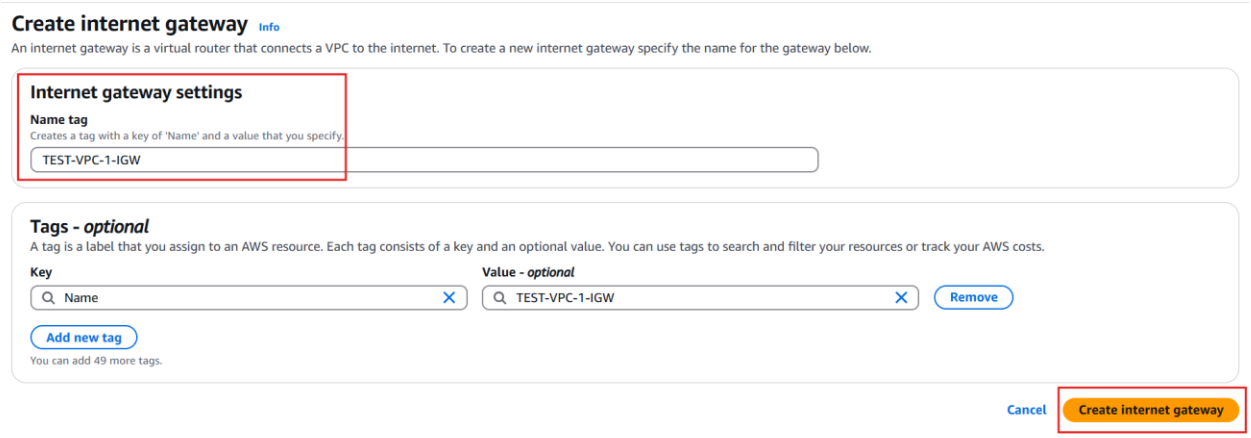
- Route tables of public subnets must have a route to the IGW (typically 0.0.0.0/0).
- Instances must have public IPs or Elastic IPs to communicate externally via IGW.

To create IGW, under VPC dashboard select “Internet gateways” then click on “Create Internet gateway”.



No matching resource found

Under Internet gateway settings, provide Name tag and click on “Create Internet gateway”.



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: TEST-VPC-1-IGW

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

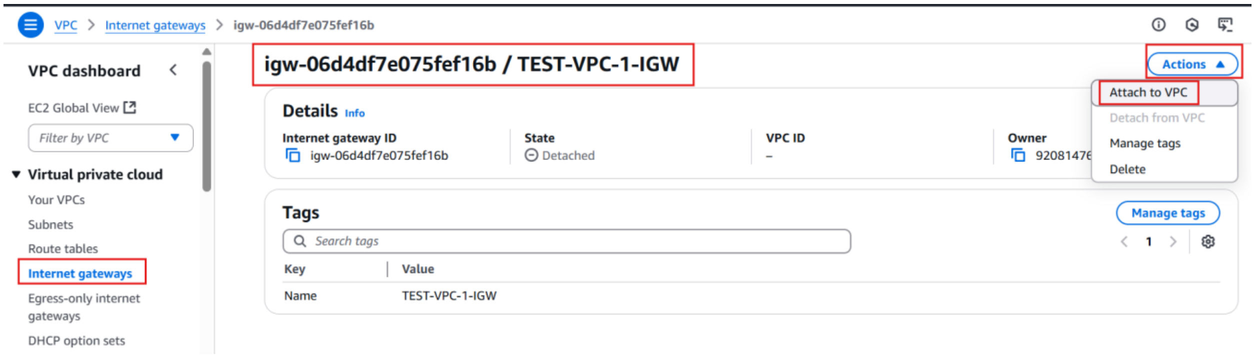
Tags - *optional*

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* |
|---|---|
| Name | TEST-VPC-1-IGW |

You can add 49 more tags.

To Attach IGW to VPC, under “Actions” click on “Attach to VPC”



igw-06d4df7e075fef16b / TEST-VPC-1-IGW

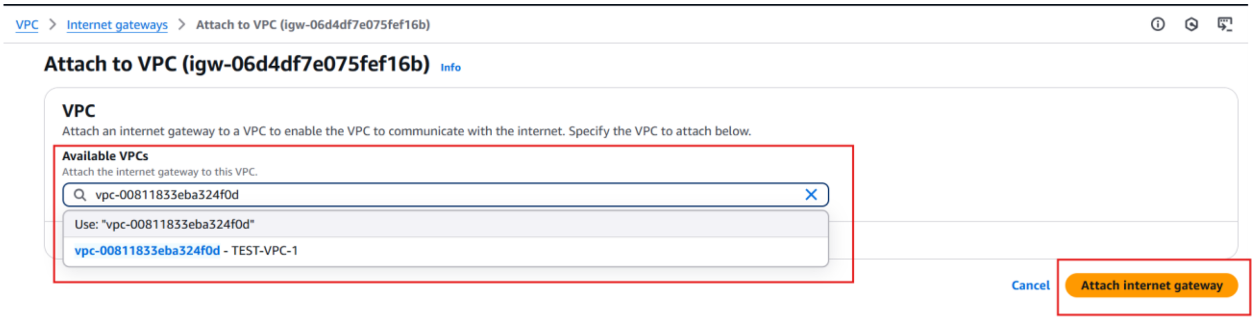
Details Info

| Internet gateway ID | State | VPC ID | Owner |
|---|---|---|---|
| igw-06d4df7e075fef16b | Detached | – | 9208147€ |

Tags

| Key | Value |
|---|---|
| Name | TEST-VPC-1-IGW |

Select the VPC under Available VPCs and click on "Attach Internet gateway”.



VPC > Internet gateways > Attach to VPC (igw-06d4df7e075fef16b)

Attach to VPC (igw-06d4df7e075fef16b) 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

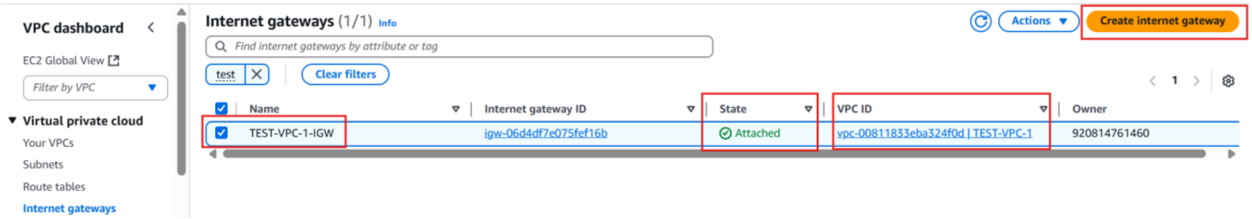
Attach the internet gateway to this VPC.

vpc-00811833eba324f0d

Use: "vpc-00811833eba324f0d"

vpc-00811833eba324f0d - TEST-VPC-1

Once attached the state and the VPC ID will be shown.

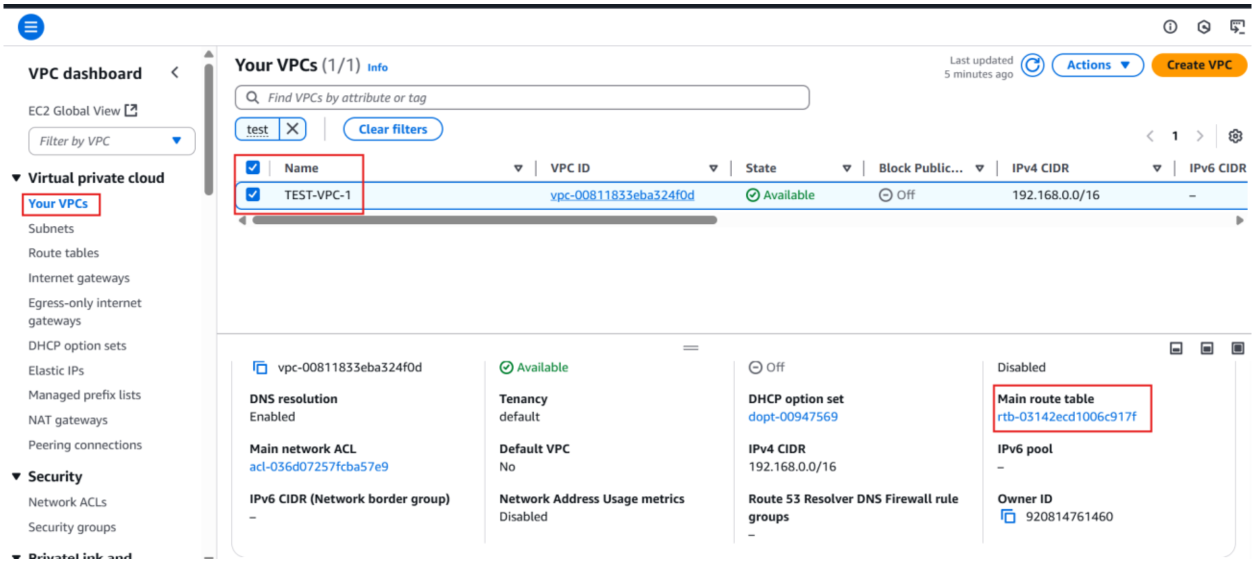


Internet gateways (1/1) Info

| Name | Internet gateway ID | State | VPC ID | Owner |
|---|---|---|---|---|
| TEST-VPC-1-IGW | igw-06d4df7e075fef16b | Attached | vpc-00811833eba324f0d \| TEST-VPC-1 | 920814761460 |

For instances with Public IPs in the VPC to break out to internet, we need a default route with IGW as next hop.

To identify the Route table, under Virtual private cloud, select the VPC you have created and click on the “Main route table”



Your VPCs (1/1) Info

| Name | VPC ID | State | Block Public... | IPv4 CIDR | IPv6 CIDR |
|---|---|---|---|---|---|
| TEST-VPC-1 | vpc-00811833eba324f0d | Available | Off | 192.168.0.0/16 | – |

vpc-00811833eba324f0d | Available | Off | Disabled

DNS resolution
Enabled

Tenancy
default

DHCP option set
dopt-00947569

Main route table
rtb-03142ecd1006c917f

Main network ACL
acl-036d07257fcba57e9

Default VPC
No

IPv4 CIDR
192.168.0.0/16

IPv6 pool
–

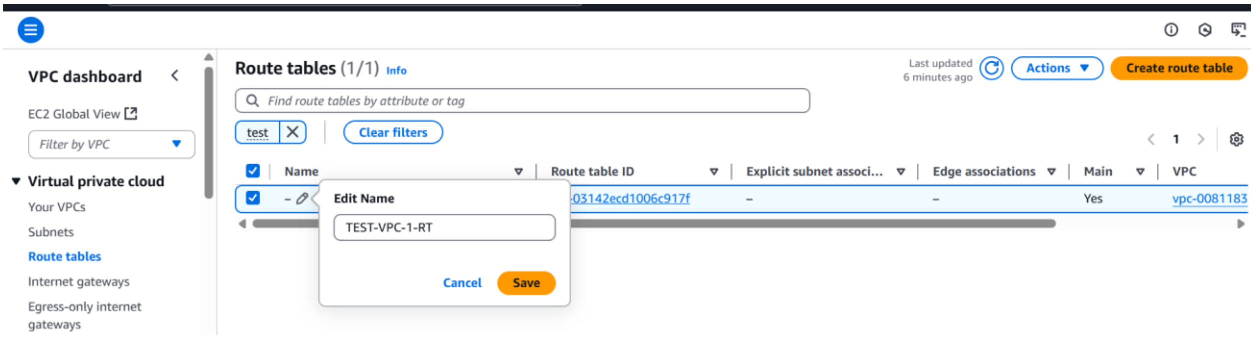
IPv6 CIDR (Network border group)
–

Network Address Usage metrics
Disabled

Route 53 Resolver DNS Firewall rule groups
–

Owner ID
920814761460

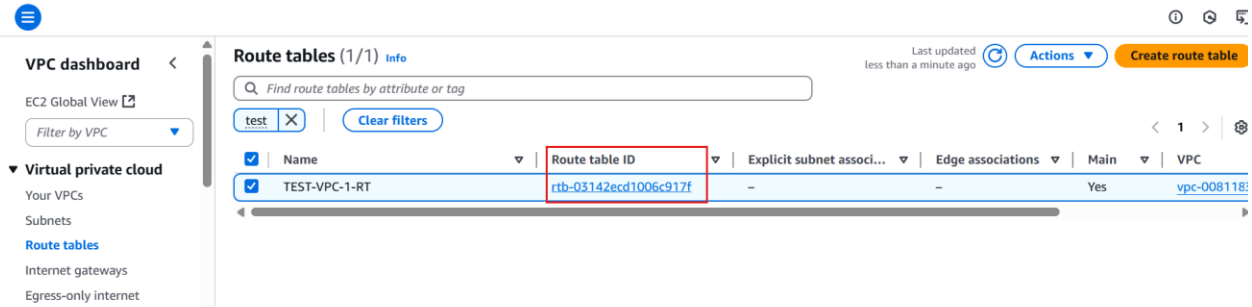
This will open the main route table of your VPC. Provide the name to the Route table.



| Name | Route table ID | Explicit subnet associ... | Edge associations | Main | VPC |
|---|---|---|---|---|---|
| – | -03142ecd1006c917f | – | – | Yes | vpc-0081183 |

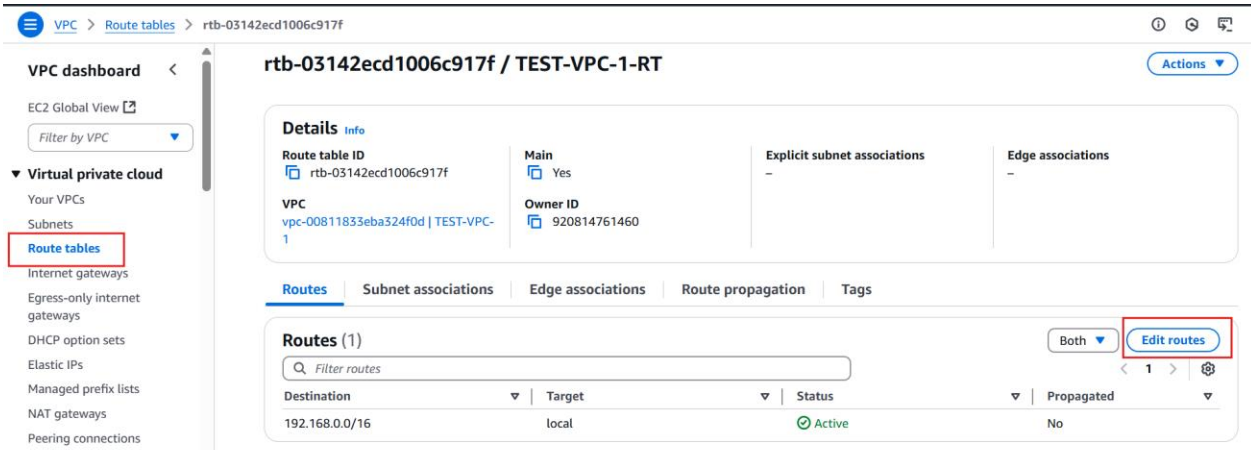
Edit Name: TEST-VPC-1-RT

Click on the Route Table ID:



| Name | Route table ID | Explicit subnet associ... | Edge associations | Main | VPC |
|---|---|---|---|---|---|
| TEST-VPC-1-RT | rtb-03142ecd1006c917f | – | – | Yes | vpc-008118 |

To update the routing table, click on “Edit routes”.



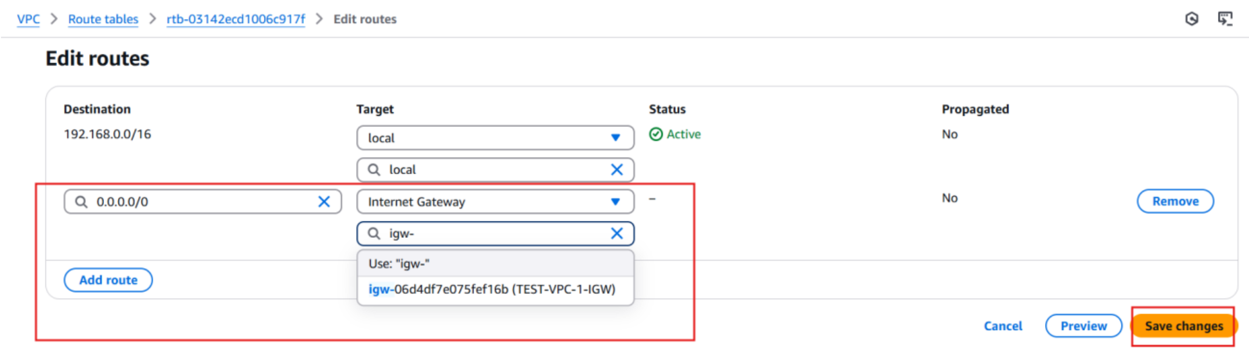
rtb-03142ecd1006c917f / TEST-VPC-1-RT

Details Info

Route table ID: rtb-03142ecd1006c917f
Main: Yes
Explicit subnet associations: –
Edge associations: –
VPC: vpc-00811833eba324f0d | TEST-VPC-1
Owner ID: 920814761460

| Destination | Target | Status | Propagated |
|---|---|---|---|
| 192.168.0.0/16 | local | ✓ Active | No |

Under Edit routes, add the default route 0.0.0.0/0 with the Target as the Internet Gateway which we have created and save the changes.

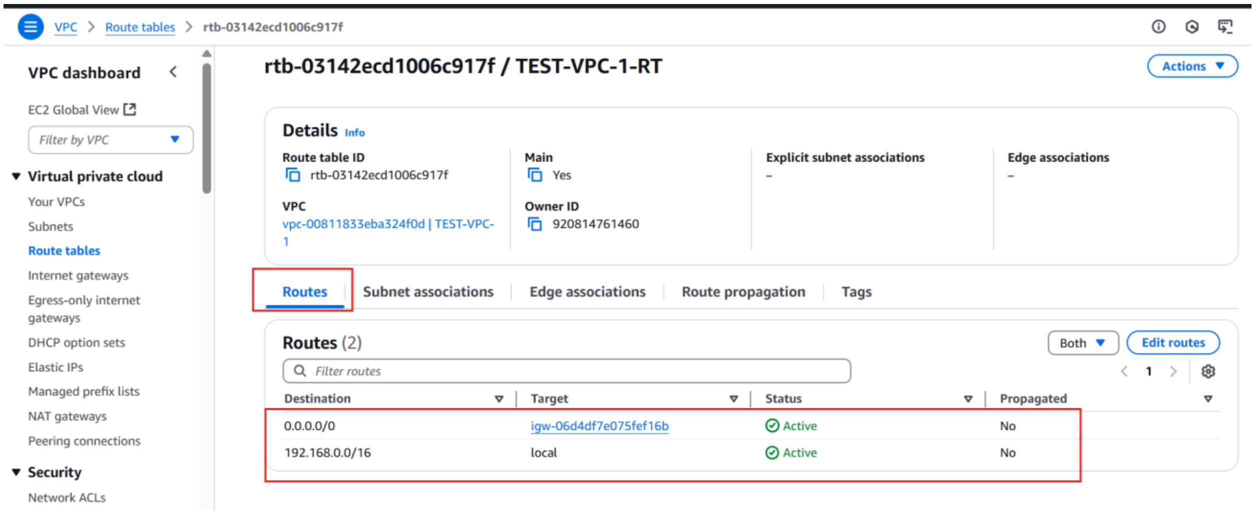


VPC > Route tables > rtb-03142ecd1006c917f > Edit routes

Edit routes

| Destination | Target | Status | Propagated |
|---|---|---|---|
| 192.168.0.0/16 | local<br>local | Active | No |
| 0.0.0.0/0 | Internet Gateway<br>igw-<br>Use: "igw-"<br>igw-06d4df7e075fef16b (TEST-VPC-1-IGW) | - | No |

Once update you should be able to view the routes.



VPC > Route tables > rtb-03142ecd1006c917f

rtb-03142ecd1006c917f / TEST-VPC-1-RT

Details Info

Route table ID: rtb-03142ecd1006c917f
Main: Yes
Explicit subnet associations: –
Edge associations: –
VPC: vpc-00811833eba324f0d | TEST-VPC-1
Owner ID: 920814761460

Routes (2)

| Destination | Target | Status | Propagated |
|---|---|---|---|
| 0.0.0.0/0 | igw-06d4df7e075fef16b | Active | No |
| 192.168.0.0/16 | local | Active | No |

## Creating EC2 instance in the VPC:

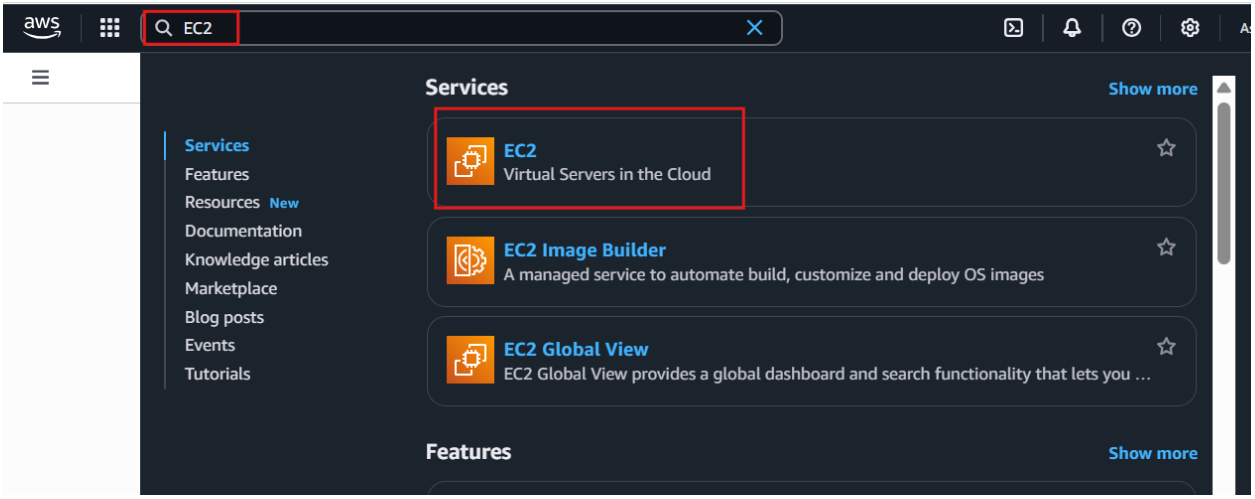
EC2 Instance is a scalable virtual server in the AWS Cloud used to run applications, network functions, and custom workloads.

**Purpose in This Use Case:**

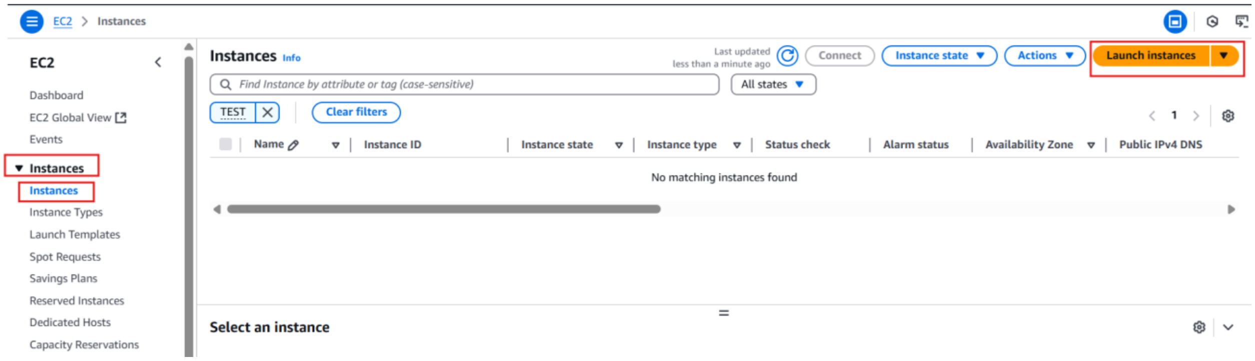
Server Hosting in AWS:
EC2 instances are used to host applications or services that need to communicate with on-premises environments over secure hybrid connectivity (via VGW/TGW and IPsec).

SD-WAN Appliance Deployment:
An EC2 instance is configured as a virtual SD-WAN edge device, enabling overlay connectivity between AWS and the on-prem SASE infrastructure.

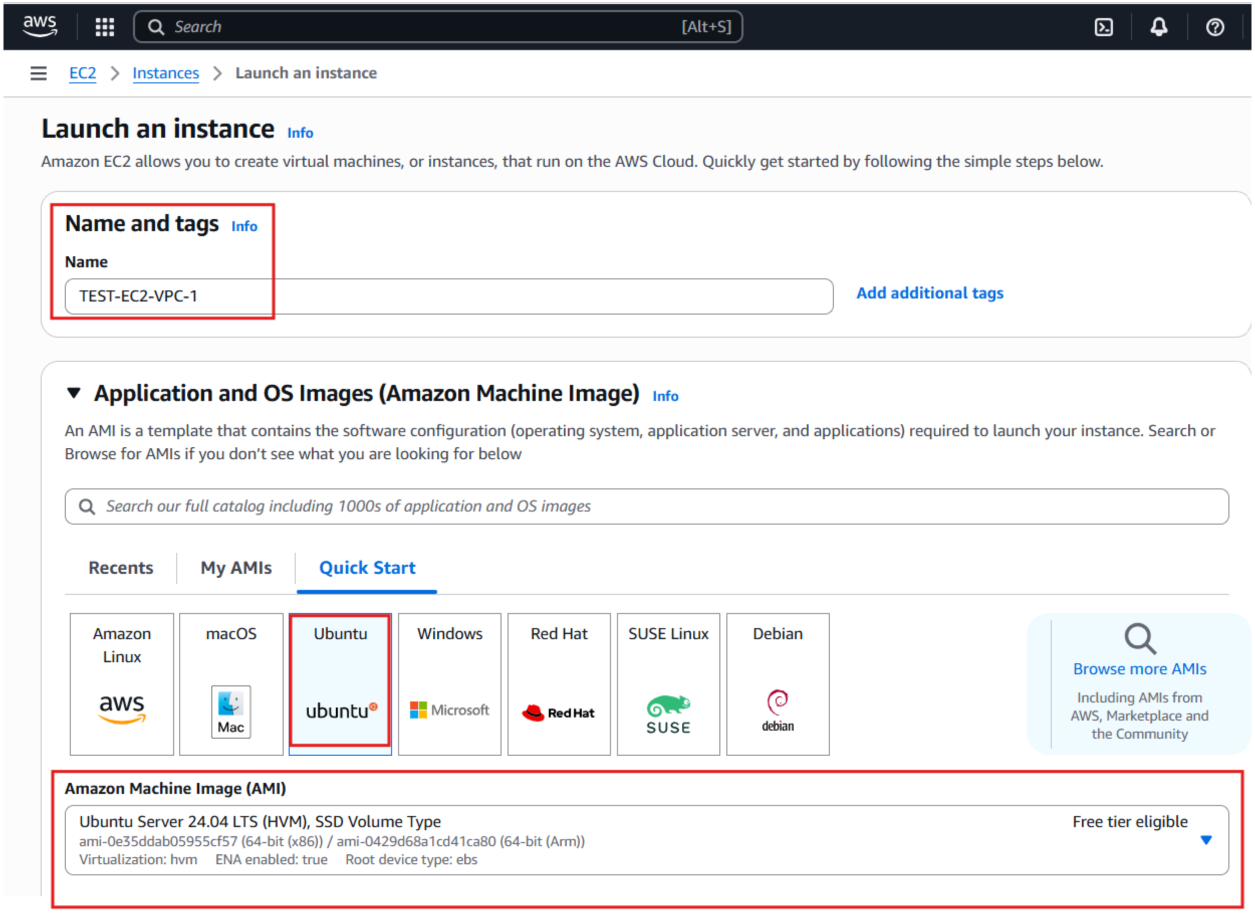
To create an EC2 instance in AWS, type EC2 in the search bar and select EC2.


aws
EC2
Services
Show more
Services
Features
Resources New
Documentation
Knowledge articles
Marketplace
Blog posts
Events
Tutorials
EC2
Virtual Servers in the Cloud
EC2 Image Builder
A managed service to automate build, customize and deploy OS images
EC2 Global View
EC2 Global View provides a global dashboard and search functionality that lets you ...
Features
Show more

Under Instances select Instances and click on "Launce Instances".



Under "Names and tags" provide name to the EC2 instance, under "Application and OS Images" → Quick Start select the AMI as per the requirement.



EC2 > Instances > Launch an instance

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name: TEST-EC2-VPC-1

Add additional tags

Application and OS Images (Amazon Machine Image) Info

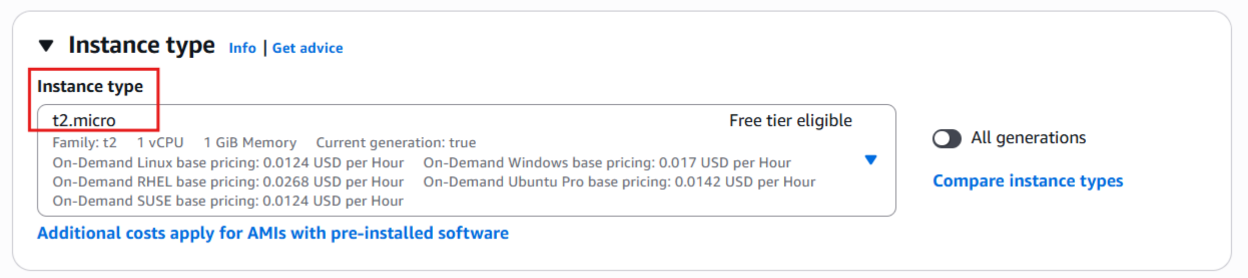
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images
Recents
My AMIs
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
SUSE Linux
Debian
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type — Free tier eligible
ami-0e35ddab05955cf57 (64-bit (x86)) / ami-0429d68a1cd41ca80 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

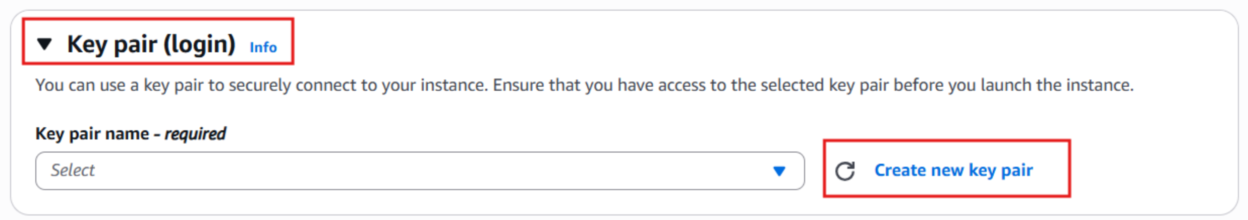
Under Instance type select the instance as per the requirement.



Instance type Info | Get advice

Instance type: t2.micro — Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux base pricing: 0.0124 USD per Hour On-Demand Windows base pricing: 0.017 USD per Hour
On-Demand RHEL base pricing: 0.0268 USD per Hour On-Demand Ubuntu Pro base pricing: 0.0142 USD per Hour
On-Demand SUSE base pricing: 0.0124 USD per Hour

Under Key pair click on “Create new Key pair”.

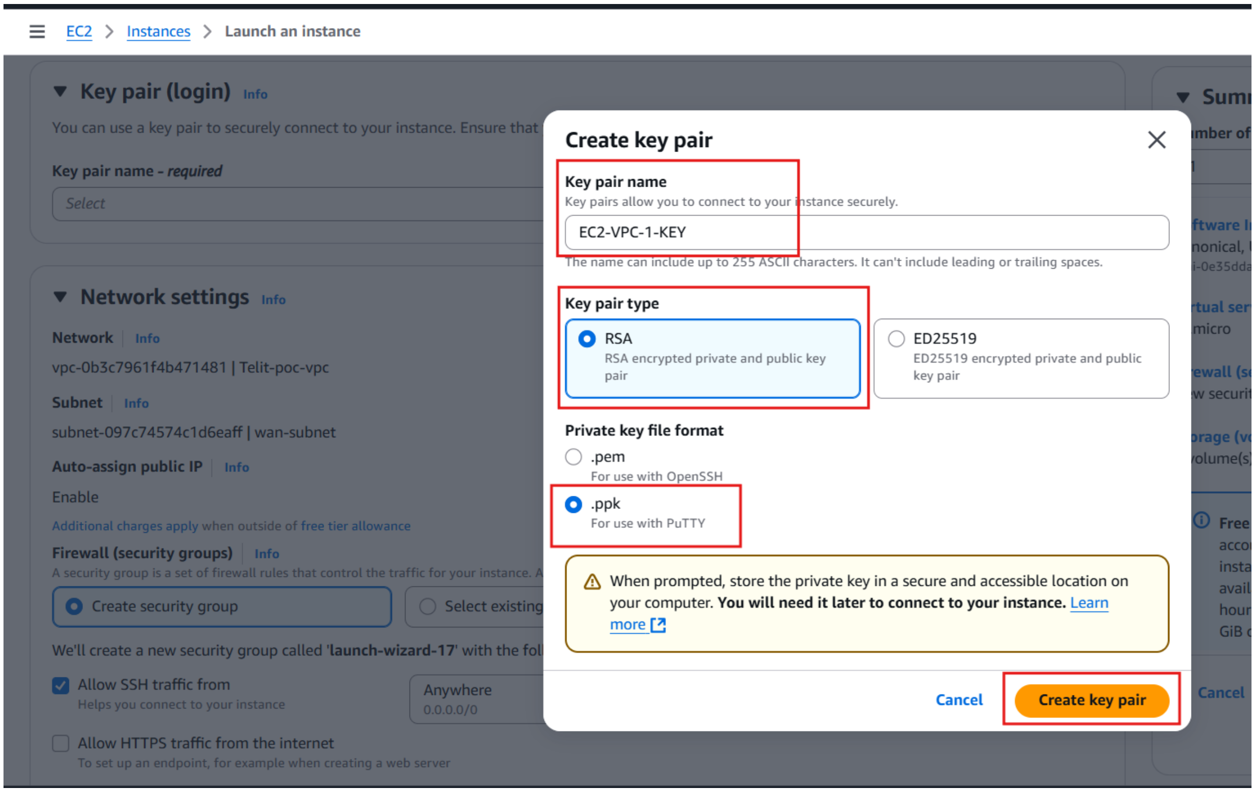


Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*: Select

Under “Create key pair” select “RSA” and the private key file format as “.ppk” and click on “Create key pair”. This key is used to access the EC2 instance using ssh.



EC2 > Instances > Launch an instance

▼ Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that

Key pair name - *required*

Select

▼ Network settings Info

Network | Info

vpc-0b3c7961f4b471481 | Telit-poc-vpc

Subnet | Info

subnet-097c74574c1d6eaff | wan-subnet

Auto-assign public IP | Info

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) | Info

A security group is a set of firewall rules that control the traffic for your instance. A

● Create security group ○ Select existing

We'll create a new security group called '**launch-wizard-17**' with the fol

☑ Allow SSH traffic from
Helps you connect to your instance — Anywhere 0.0.0.0/0

□ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

**Create key pair**

**Key pair name**

Key pairs allow you to connect to your instance securely.

EC2-VPC-1-KEY

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

**Key pair type**

● RSA
RSA encrypted private and public key pair

○ ED25519
ED25519 encrypted private and public key pair

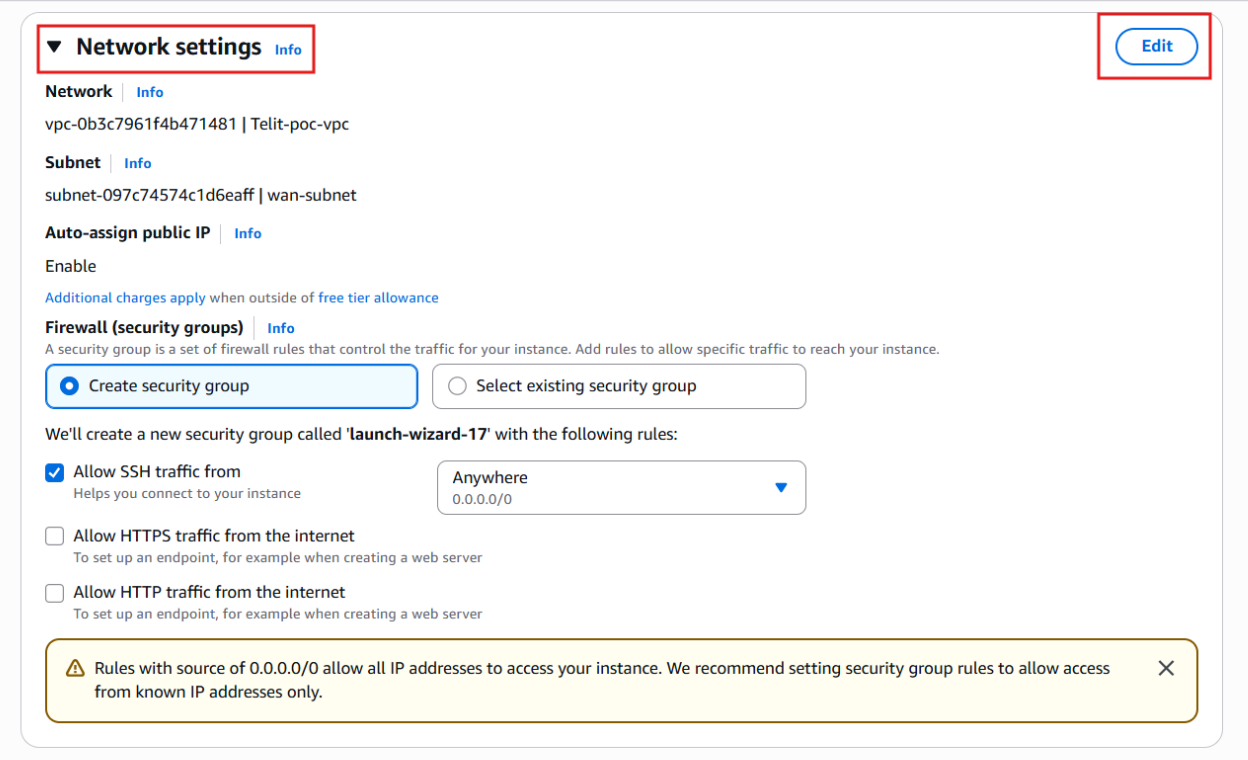
**Private key file format**

○ .pem
For use with OpenSSH

● .ppk
For use with PuTTY

⚠ When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** Learn more

Under “Network settings” click on Edit.



▼ **Network settings** Info

**Network** | Info

vpc-0b3c7961f4b471481 | Telit-poc-vpc

**Subnet** | Info

subnet-097c74574c1d6eaff | wan-subnet

**Auto-assign public IP** | Info

Enable

Additional charges apply when outside of free tier allowance

**Firewall (security groups)** | Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

We'll create a new security group called '**launch-wizard-17**' with the following rules:

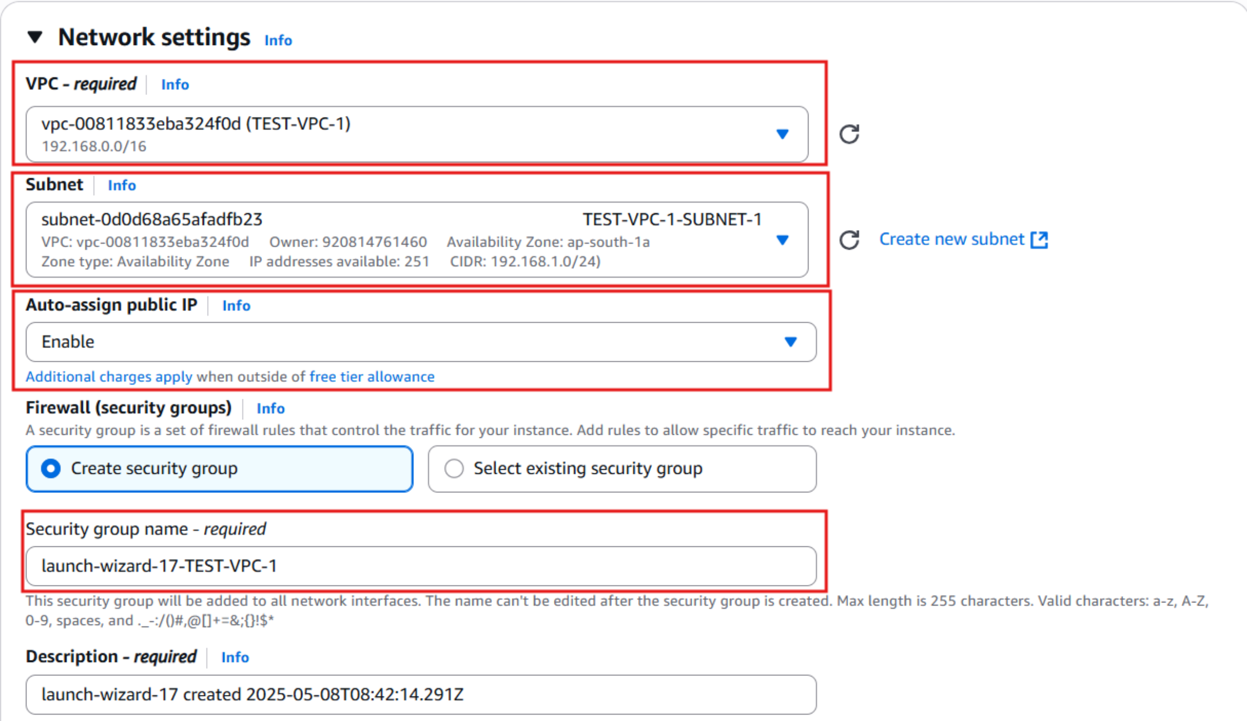
☑ Allow SSH traffic from
Helps you connect to your instance — Anywhere 0.0.0.0/0

□ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

□ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Under VPC, select the VPC which you have created, select the required subnet , Enable Public IP if required and modify the security group name.



▼ Network settings Info

VPC - *required* | Info

vpc-00811833eba324f0d (TEST-VPC-1)
192.168.0.0/16

Subnet | Info

subnet-0d0d68a65afadfb23 TEST-VPC-1-SUBNET-1
VPC: vpc-00811833eba324f0d Owner: 920814761460 Availability Zone: ap-south-1a
Zone type: Availability Zone IP addresses available: 251 CIDR: 192.168.1.0/24)

Create new subnet

Auto-assign public IP | Info

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) | Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

Security group name - *required*

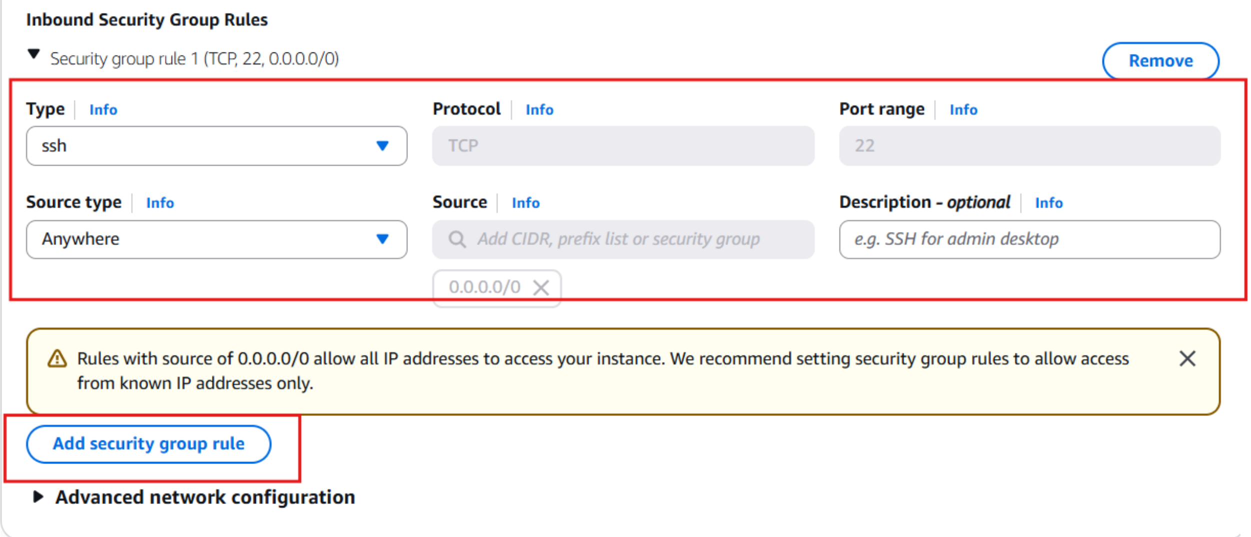
launch-wizard-17-TEST-VPC-1

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - *required* | Info

launch-wizard-17 created 2025-05-08T08:42:14.291Z

By default, ssh from Outside is allowed and all the outbound traffic from EC2 instance is allowed.



Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)

Remove

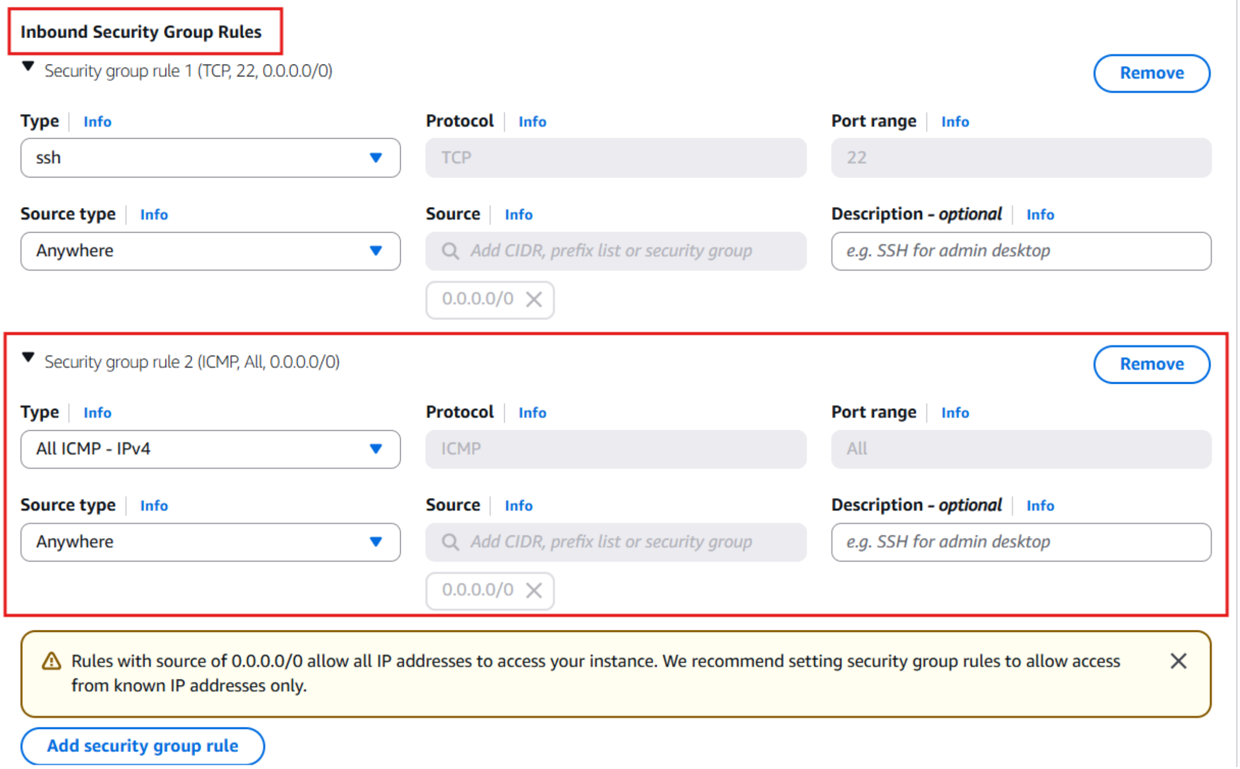
| | | |
|---|---|---|
| Type \| Info | Protocol \| Info | Port range \| Info |
| ssh | TCP | 22 |
| Source type \| Info | Source \| Info | Description - *optional* \| Info |
| Anywhere | Add CIDR, prefix list or security group<br>0.0.0.0/0 ✕ | e.g. SSH for admin desktop |

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. ✕

Add security group rule

▶ Advanced network configuration

We can edit the "Inbound Security Group Rules" as per our requirement.



**Inbound Security Group Rules**

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)

Type: ssh

Protocol: TCP

Port range: 22

Source type: Anywhere

Source: 0.0.0.0/0

Description - *optional*: e.g. SSH for admin desktop

▼ Security group rule 2 (ICMP, All, 0.0.0.0/0)

Type: All ICMP - IPv4

Protocol: ICMP

Port range: All

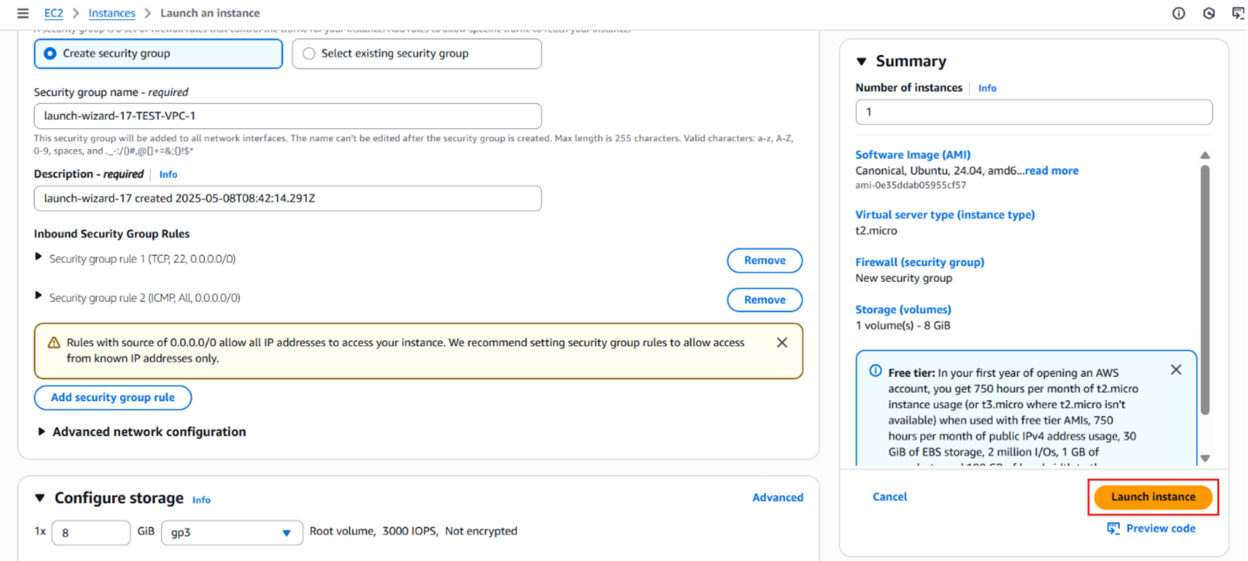
Source type: Anywhere

Source: 0.0.0.0/0

Description - *optional*: e.g. SSH for admin desktop

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Once all the above configuration is complete, Click on “Launch instance”.



EC2 > Instances > Launch an instance

● Create security group ○ Select existing security group

Security group name - *required*: launch-wizard-17-TEST-VPC-1

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - *required*: launch-wizard-17 created 2025-05-08T08:42:14.291Z

**Inbound Security Group Rules**

▶ Security group rule 1 (TCP, 22, 0.0.0.0/0)

▶ Security group rule 2 (ICMP, All, 0.0.0.0/0)

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

▶ **Advanced network configuration**

▼ **Configure storage**

1x 8 GiB gp3 Root volume, 3000 IOPS, Not encrypted

▼ **Summary**

Number of instances: 1

Software Image (AMI): Canonical, Ubuntu, 24.04, amd6...read more ami-0e35ddab05955cf57

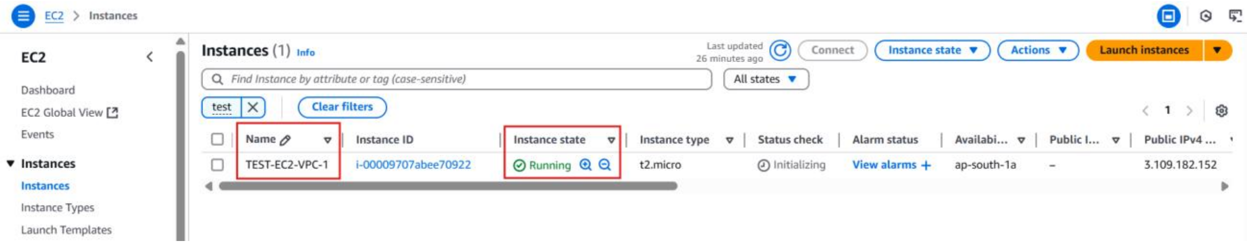
Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

ⓘ **Free tier:** In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of

After instance is launched, make sure the “Instance state” is Running.



EC2 > Instances

**Instances** (1)

Last updated 26 minutes ago

Find Instance by attribute or tag (case-sensitive) | All states

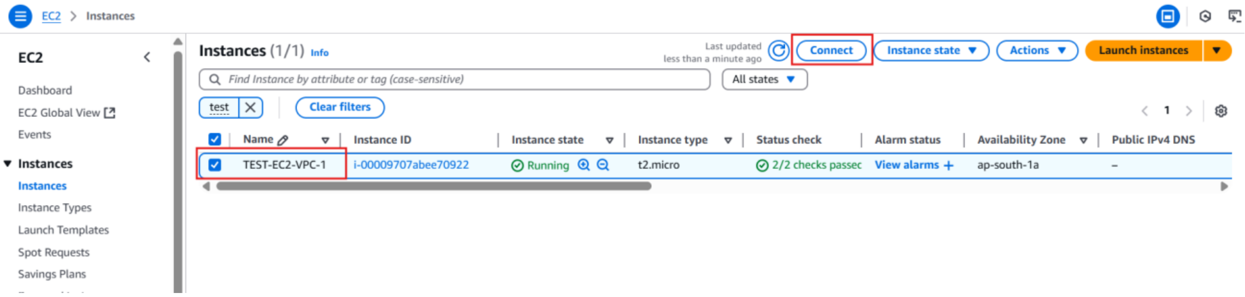
test ✕

| □ | Name | Instance ID | Instance state | Instance type | Status check | Alarm status | Availabi... | Public I... | Public IPv4 ... |
|---|---|---|---|---|---|---|---|---|---|
| □ | TEST-EC2-VPC-1 | i-00009707abee70922 | ✓ Running | t2.micro | Initializing | View alarms + | ap-south-1a | – | 3.109.182.152 |

# Accessing EC2 instance:

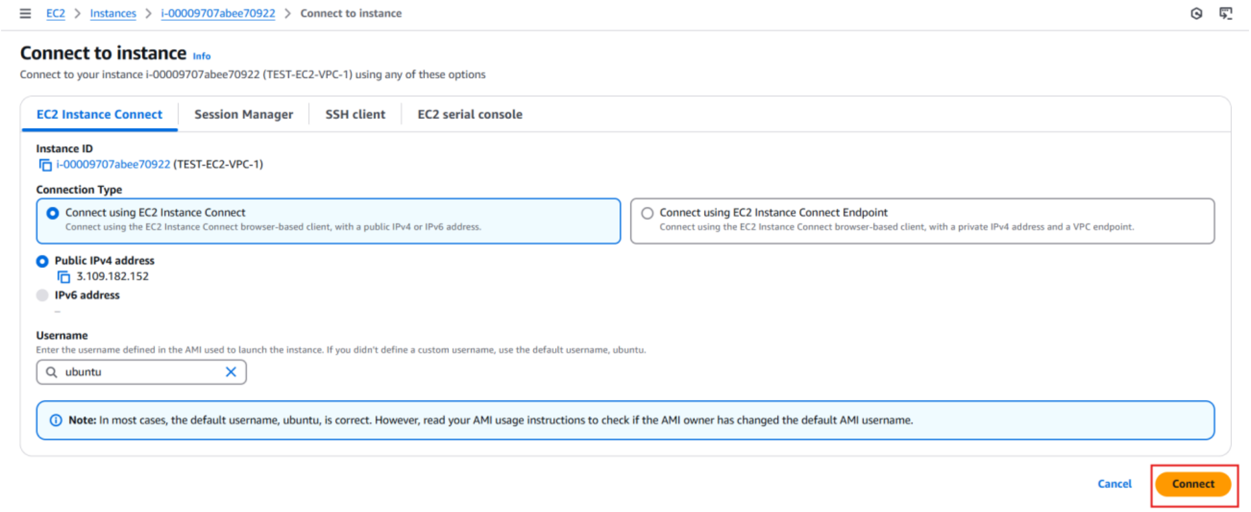
## Accessing through AWS Dashboard:

EC2 instance can be accessed directly through AWS by clicking on Connect.



| ☑ | Name | Instance ID | Instance state | Instance type | Status check | Alarm status | Availability Zone | Public IPv4 DNS |
|---|---|---|---|---|---|---|---|---|
| ☑ | TEST-EC2-VPC-1 | i-00009707abee70922 | Running | t2.micro | 2/2 checks passec | View alarms + | ap-south-1a | – |

Select the Connection type as “Connect using EC2 Instance Connect” and then click on Connect.



Connect to instance Info

Connect to your instance i-00009707abee70922 (TEST-EC2-VPC-1) using any of these options

Instance ID

i-00009707abee70922 (TEST-EC2-VPC-1)

Connection Type

● Connect using EC2 Instance Connect
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 or IPv6 address.

○ Connect using EC2 Instance Connect Endpoint
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

● Public IPv4 address
3.109.182.152

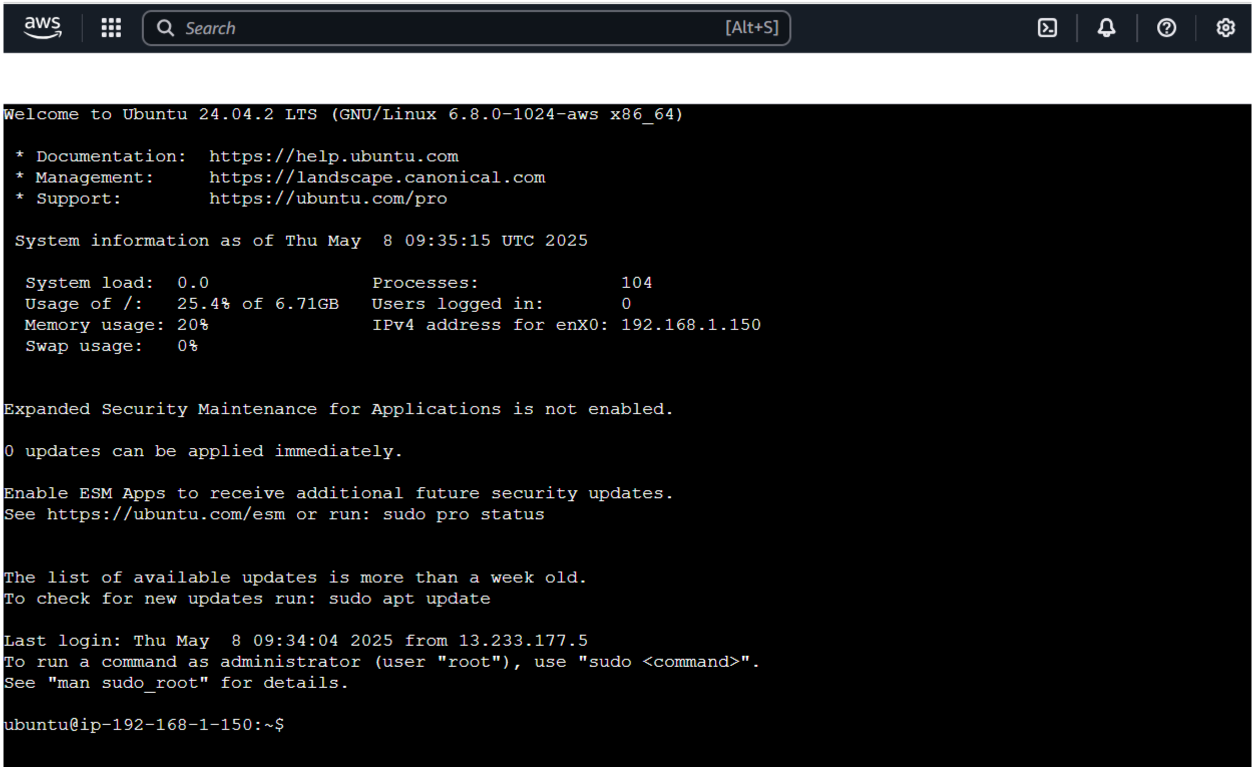
○ IPv6 address
–

Username

Enter the username defined in the AMI used to launch the instance. If you didn't define a custom username, use the default username, ubuntu.

ubuntu

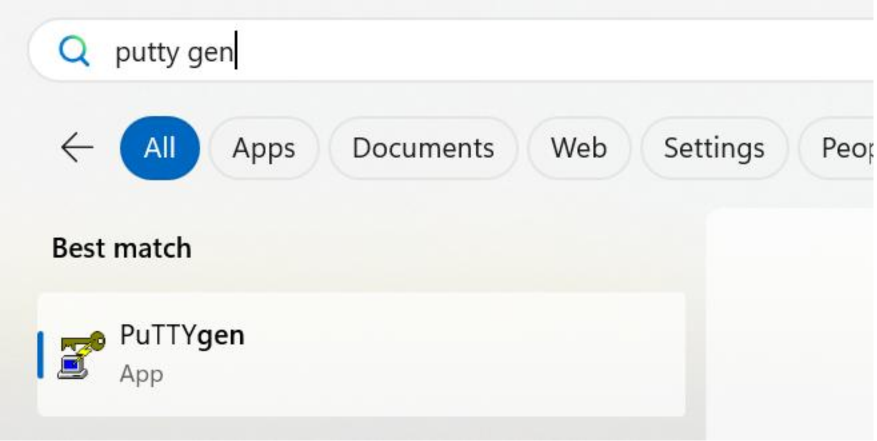
**Note:** In most cases, the default username, ubuntu, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.



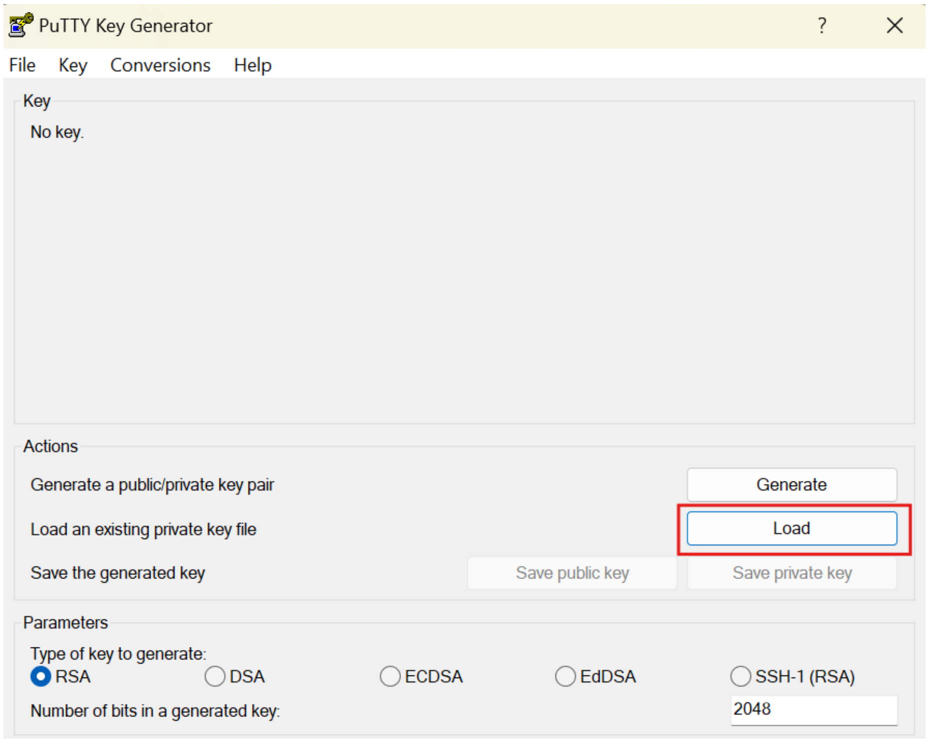
```
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-1024-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Thu May  8 09:35:15 UTC 2025

  System load:  0.0               Processes:             104
  Usage of /:   25.4% of 6.71GB   Users logged in:       0
  Memory usage: 20%               IPv4 address for enX0: 192.168.1.150
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Thu May  8 09:34:04 2025 from 13.233.177.5
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-192-168-1-150:~$
```

### Accessing through Putty:

1. From the “Start” menu, choose “All Programs” → PuTTYgen.



2. Under “Type of key to generate”, choose “RSA” and Click on “Load”. By default, PuTTYgen displays the files, select the “ppk” file that got generated while creating EC2 instance.



Key

No key.

Actions

Generate a public/private key pair

Load an existing private key file

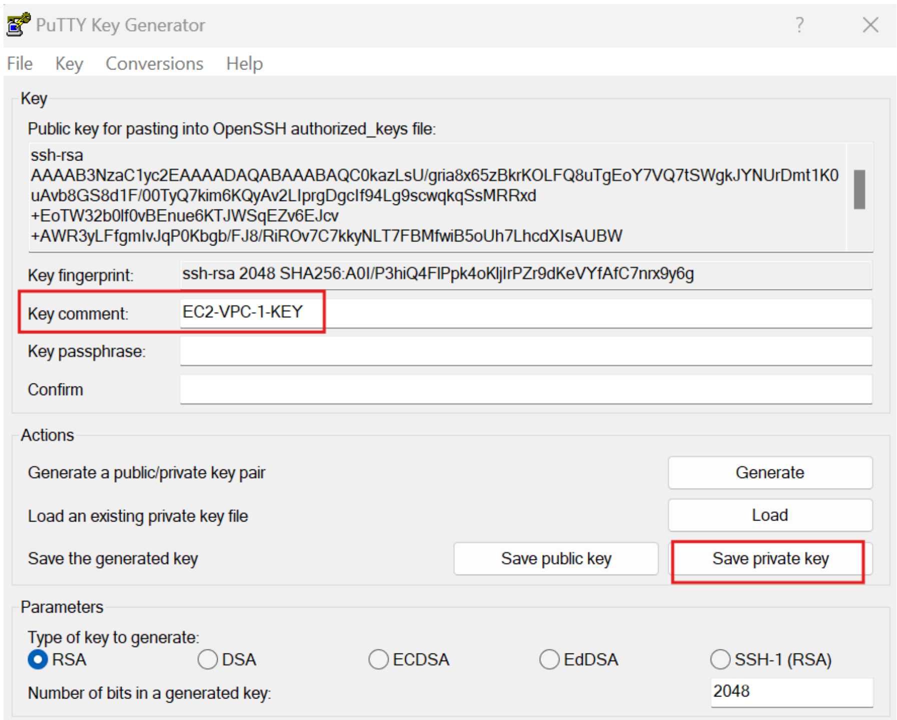
Save the generated key

Parameters

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ EdDSA ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Once the file is loaded click on “Save Private key”.



Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC0kazLsU/gria8x65zBkrKOLFQ8uTgEoY7VQ7tSWgkJYNUrDmt1K0
uAvb8GS8d1F/00TyQ7kim6KQyAv2LIprgDgcIf94Lg9scwqkqSsMRRxd
+EoTW32b0lf0vBEnue6KTJWSqEZv6EJcv
+AWR3yLFfgmIvJqP0Kbgb/FJ8/RiROv7C7kkyNLT7FBMfwiB5oUh7LhcdXIsAUBW
```

Key fingerprint: ssh-rsa 2048 SHA256:A0I/P3hiQ4FIPpk4oKljIrPZr9dKeVYfAfC7nrx9y6g

Key comment: EC2-VPC-1-KEY

Key passphrase:

Confirm

Actions

Generate a public/private key pair

Load an existing private key file

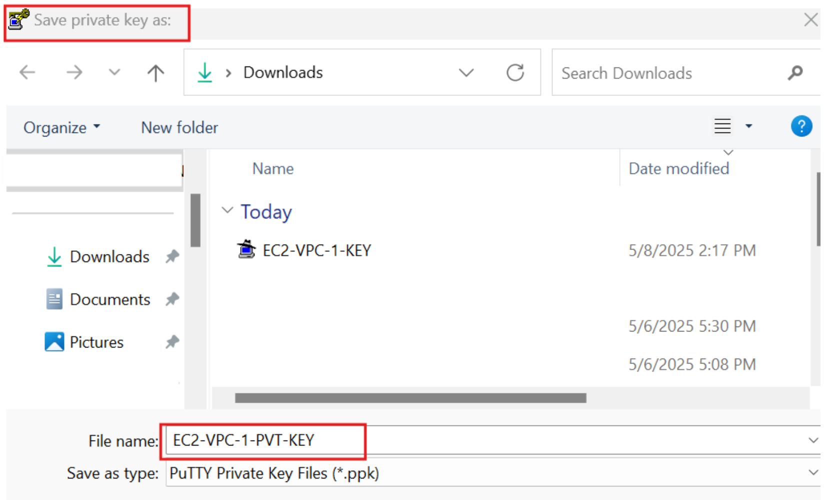
Save the generated key

Parameters

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ EdDSA ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

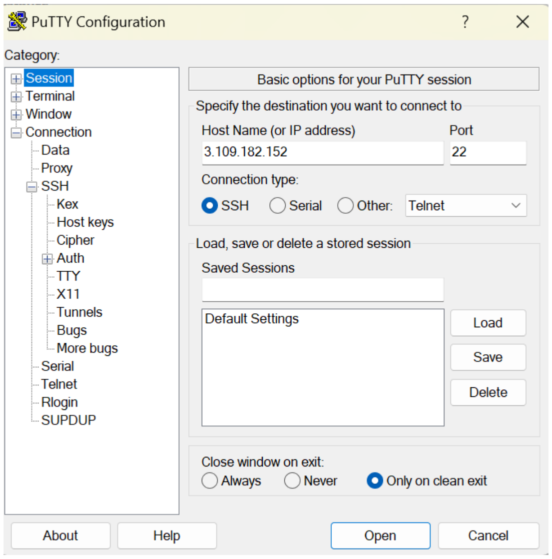
Save the key to your PC.



File name: EC2-VPC-1-PVT-KEY

Save as type: PuTTY Private Key Files (*.ppk)

Now open putty, provide the IP address of the EC2 instance and under “Auth” click on Credentials and browse for the private key, then click on “Open”.



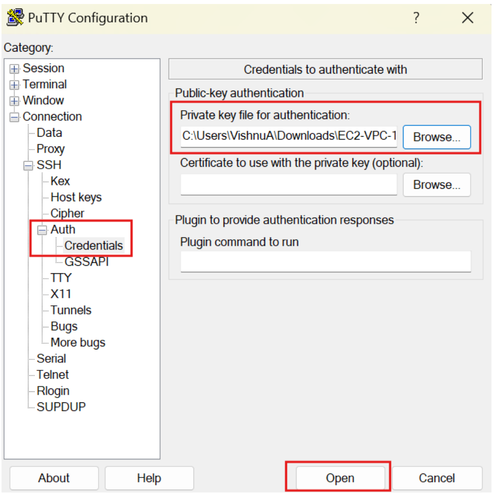
Specify the destination you want to connect to

Host Name (or IP address): 3.109.182.152

Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

Close window on exit: ○ Always ○ Never ● Only on clean exit

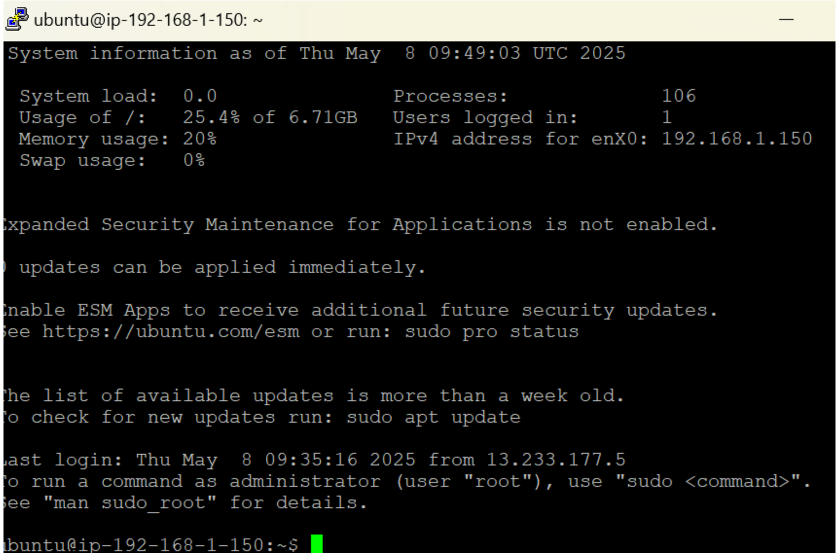


Public-key authentication

Private key file for authentication: C:\Users\VishnuA\Downloads\EC2-VPC-1

Certificate to use with the private key (optional):

Login with username ubuntu:

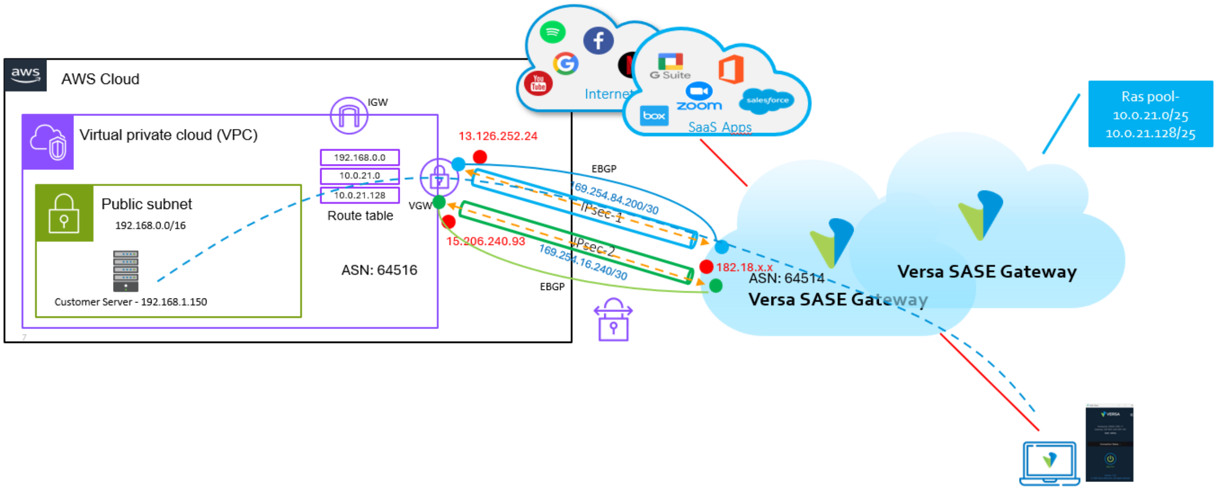


```
System information as of Thu May  8 09:49:03 UTC 2025

 System load:  0.0               Processes:             106
 Usage of /:   25.4% of 6.71GB   Users logged in:       1
 Memory usage: 20%               IPv4 address for enX0: 192.168.1.150
 Swap usage:   0%


xpanded Security Maintenance for Applications is not enabled.

 updates can be applied immediately.

nable ESM Apps to receive additional future security updates.
ee https://ubuntu.com/esm or run: sudo pro status


he list of available updates is more than a week old.
o check for new updates run: sudo apt update

ast login: Thu May  8 09:35:16 2025 from 13.233.177.5
o run a command as administrator (user "root"), use "sudo <command>".
ee "man sudo_root" for details.

buntu@ip-192-168-1-150:~$
```

## Option 1 – VGW

A site-to-site IPsec VPN is established between the SASE Gateway and the AWS VPC using a Virtual Private Gateway (VGW). The tunnels are configured for high availability, and dynamic route exchange is performed over the IPsec connection using eBGP between VGW and SASE GW.

This Option is used when you have a single VPC and requires a simple, direct, and cost-effective IPsec tunnel to connect SASE GW with AWS.

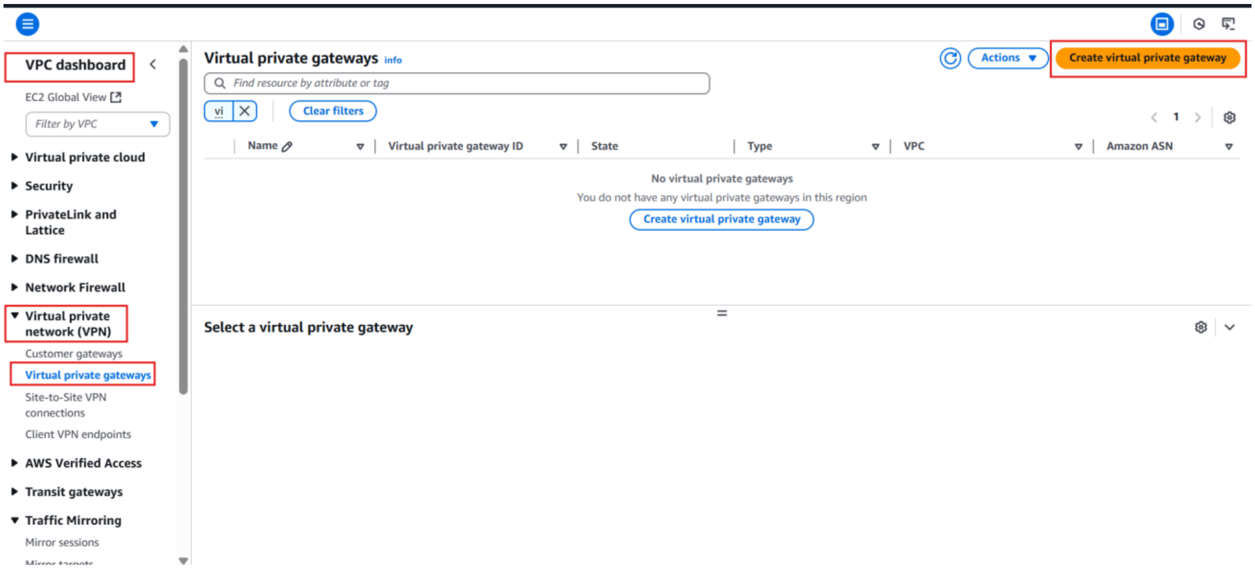


**Note:** Refer Section 4 to 7 for creating VPC, Subnets, IGW and EC2 Instance.

# AWS Configuration:

## Creating Virtual Private Gateway:

Under VPC Dashboard Go to “Virtual private network” → “Virtual private gateways” and click on “Create virtual private gateway”.

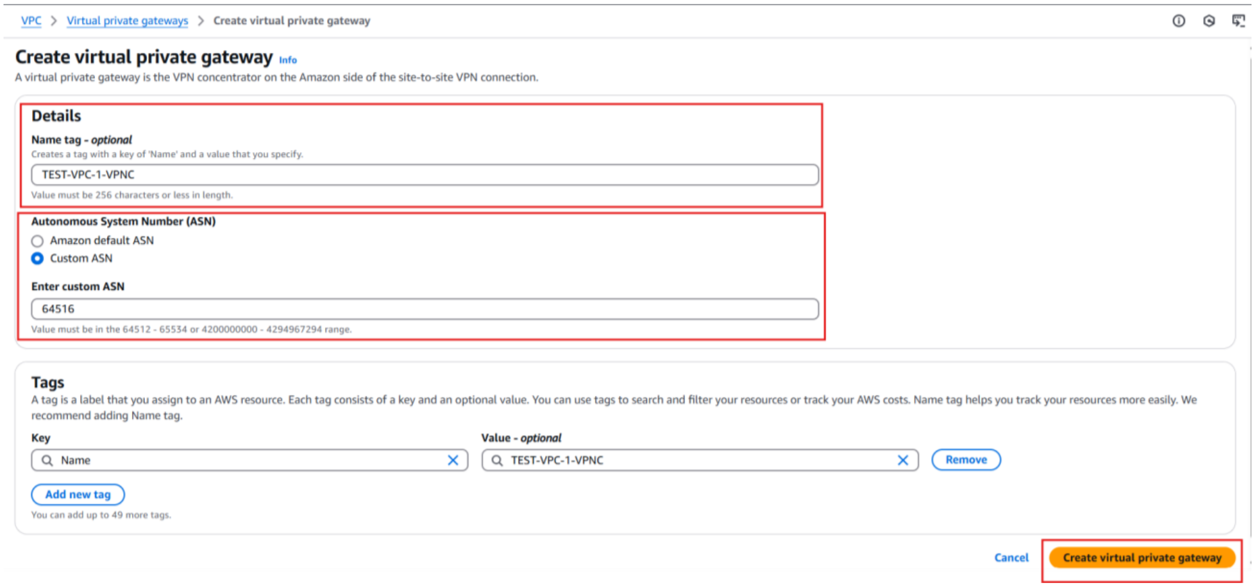


No virtual private gateways

You do not have any virtual private gateways in this region

Create virtual private gateway

Under Details, provide a Name tag, Custom ASN which will be used on AWS Virtual private gateway for BGP and click on “Create Virtual private gateway”.



VPC > Virtual private gateways > Create virtual private gateway

**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.

TEST-VPC-1-VPNC

Value must be 256 characters or less in length.

Autonomous System Number (ASN)

○ Amazon default ASN

● Custom ASN

Enter custom ASN

64516

Value must be in the 64512 - 65534 or 4200000000 - 4294967294 range.

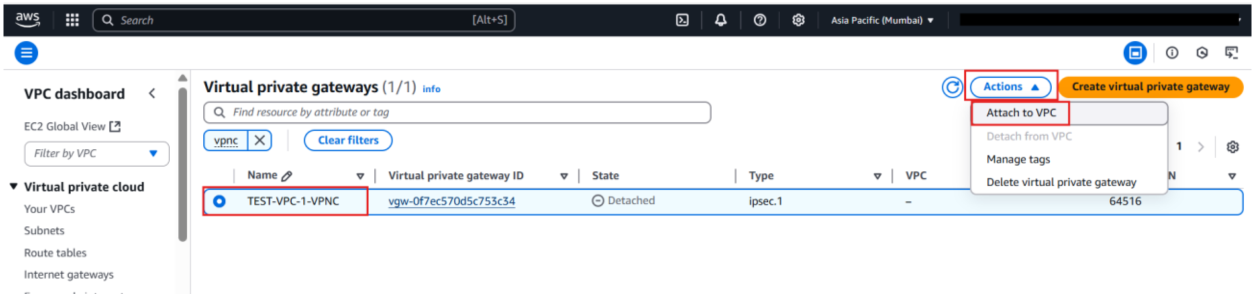
**Tags**

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 | TEST-VPC-1-VPNC |

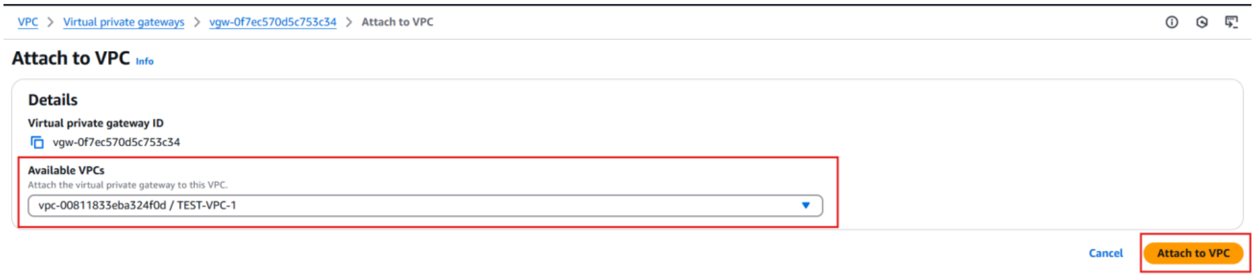
You can add up to 49 more tags.

Once created, VGW needs to be attached with a VPC. To Attach, select the created Virtual Private gateway and click on Actions → Attach to VPC.



| | Name | Virtual private gateway ID | State | Type | VPC | Amazon ASN |
|---|---|---|---|---|---|---|
| ● | TEST-VPC-1-VPNC | vgw-0f7ec570d5c753c34 | Detached | ipsec.1 | – | 64516 |

Select the VPC under “Available VPSs” and click on “Attach to VPC”.

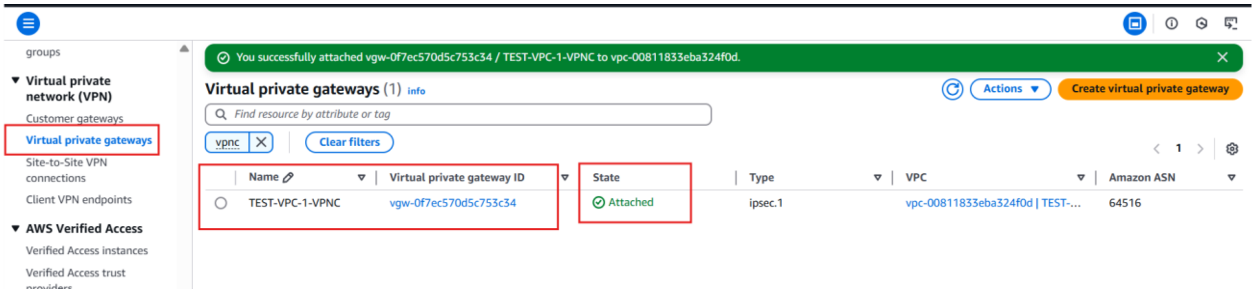

VPC > Virtual private gateways > vgw-0f7ec570d5c753c34 > Attach to VPC
Attach to VPC Info
Cancel
Attach to VPC

Details

Virtual private gateway ID: vgw-0f7ec570d5c753c34

Available VPCs
Attach the virtual private gateway to this VPC.
vpc-00811833eba324f0d / TEST-VPC-1

Once created you will be able to see the State as “Attached”.


groups
▾ Virtual private network (VPN)
Customer gateways
Virtual private gateways
Site-to-Site VPN connections
Client VPN endpoints
▾ AWS Verified Access
Verified Access instances
Verified Access trust providers
Virtual private gateways (1) Info
Find resource by attribute or tag
vpnc ✕
Clear filters
Actions ▾
Create virtual private gateway

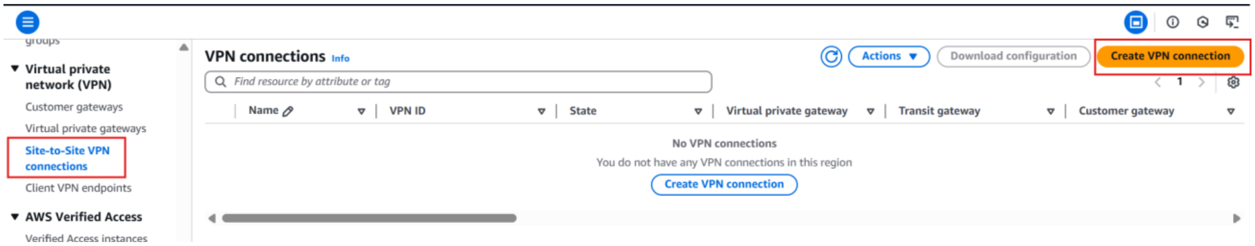
You successfully attached vgw-0f7ec570d5c753c34 / TEST-VPC-1-VPNC to vpc-00811833eba324f0d.

| | Name | Virtual private gateway ID | State | Type | VPC | Amazon ASN |
|---|---|---|---|---|---|---|
| ○ | TEST-VPC-1-VPNC | vgw-0f7ec570d5c753c34 | Attached | ipsec.1 | vpc-00811833eba324f0d \| TEST-... | 64516 |

## Create Site to Site Tunnels:

Once the VGW is created, we have to create site to site tunnels towards SASE-GWs.

Under “VPN” select “Site-To-Site VPN Connections” and click on “Create VPN Connection”.

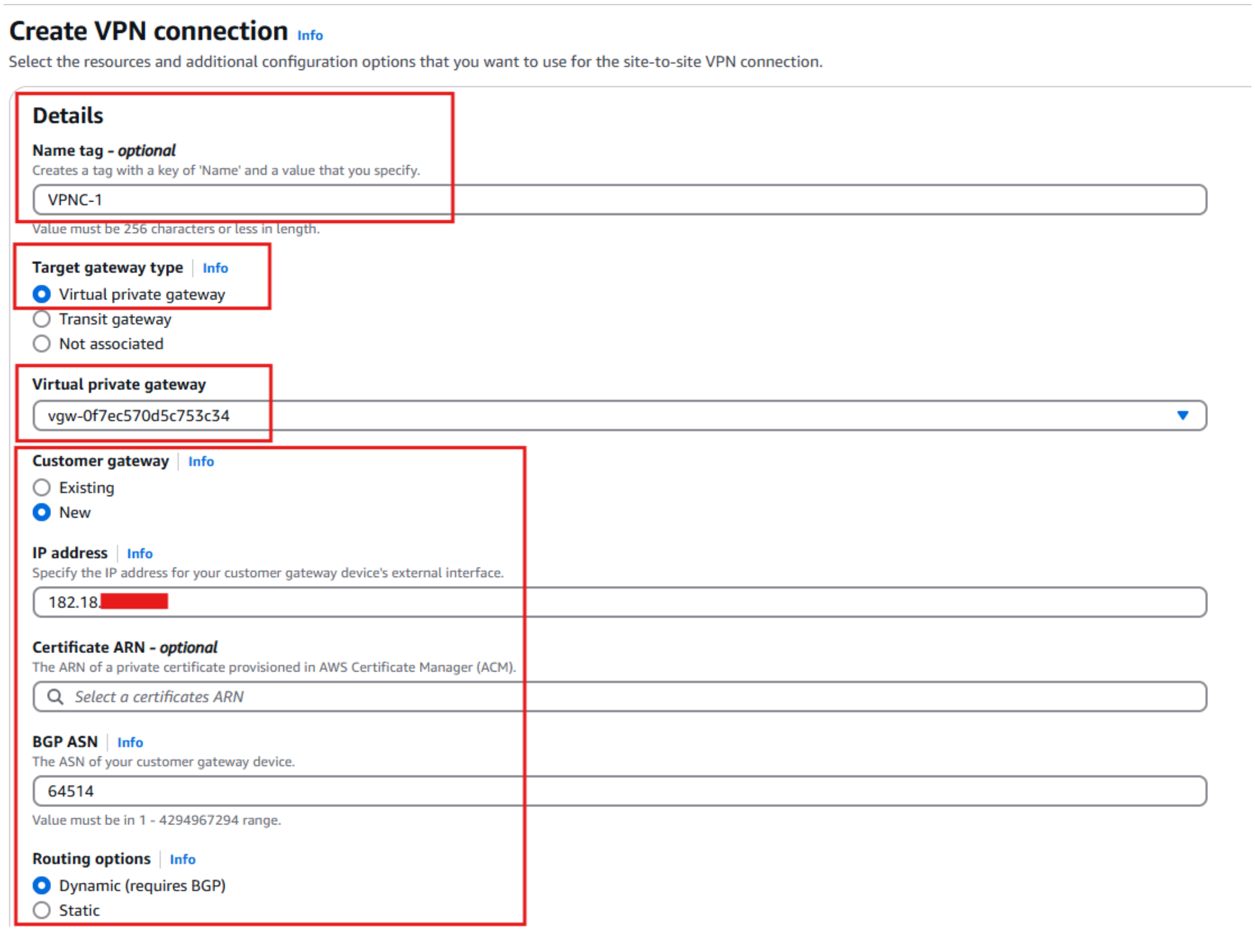


| Name | VPN ID | State | Virtual private gateway | Transit gateway | Customer gateway |
|---|---|---|---|---|---|

No VPN connections
You do not have any VPN connections in this region

Under Details, provide the “Name tag”, Under “Target gateway type” select “Virtual private gateway” and select the created VGW from the dropdown.

Under “Customer gateway” click on “New” and provide the “IP address” of the SASE-GW to which IP-sec tunnels are to be formed and under BGP ASN provide the AS number of the SASE-GW.



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.

VPNC-1

Value must be 256 characters or less in length.

Target gateway type | Info

● Virtual private gateway

○ Transit gateway

○ Not associated

Virtual private gateway

vgw-0f7ec570d5c753c34

Customer gateway | Info

○ Existing

● New

IP address | Info

Specify the IP address for your customer gateway device's external interface.

182.18[redacted]

Certificate ARN - *optional*

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

*Select a certificates ARN*

BGP ASN | Info

The ASN of your customer gateway device.

64514

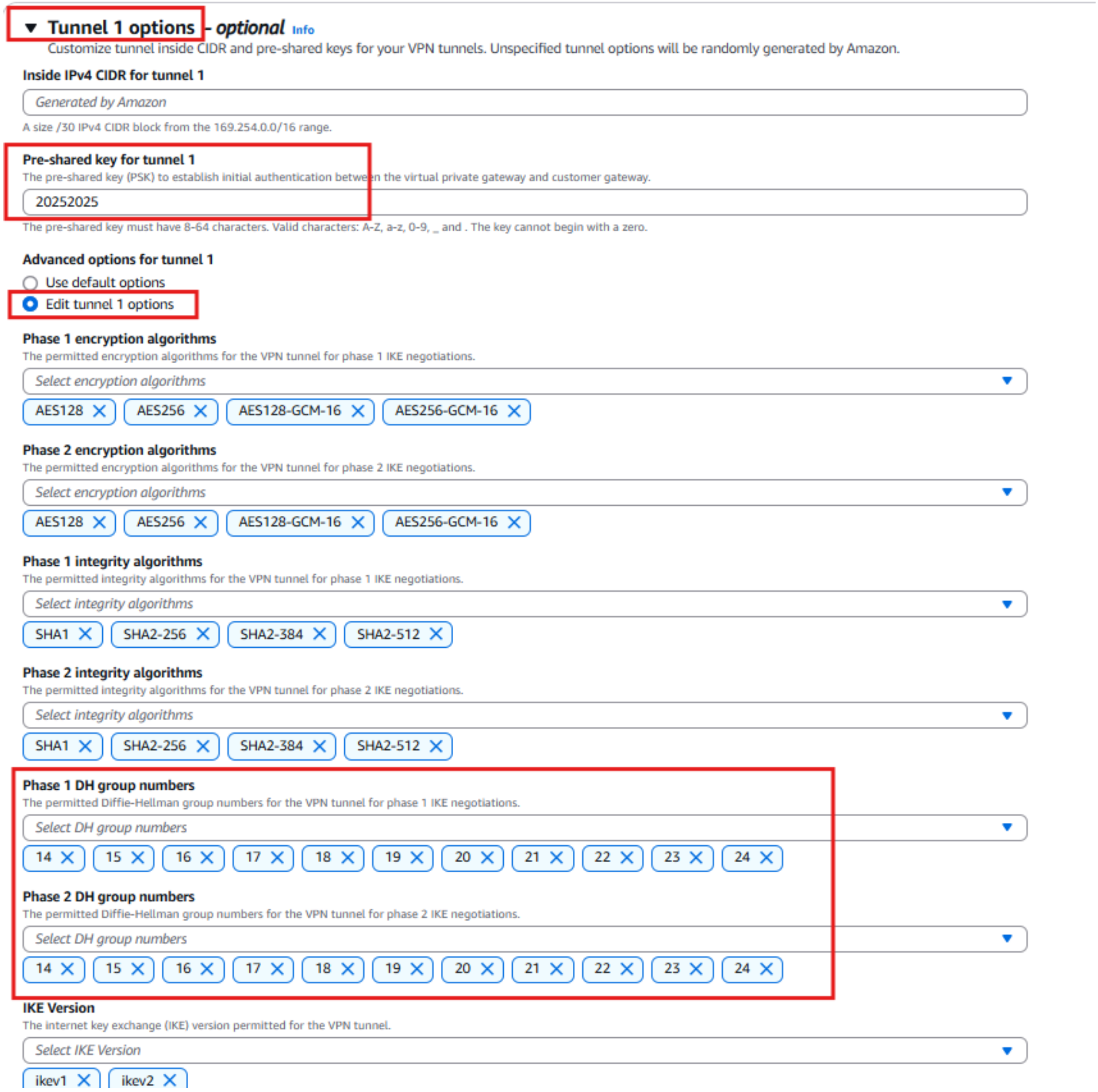
Value must be in 1 - 4294967294 range.

Routing options | Info

● Dynamic (requires BGP)

○ Static

Under Tunnel Options, configure pre-shared key and under "Advanced options for tunnel 1" select "Edit tunnel 1 options" and remove DH-group 2 and 5 from the DH-Group numbers.



▼ 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.

20252025

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* ▼

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* ▼

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

**IKE Version**

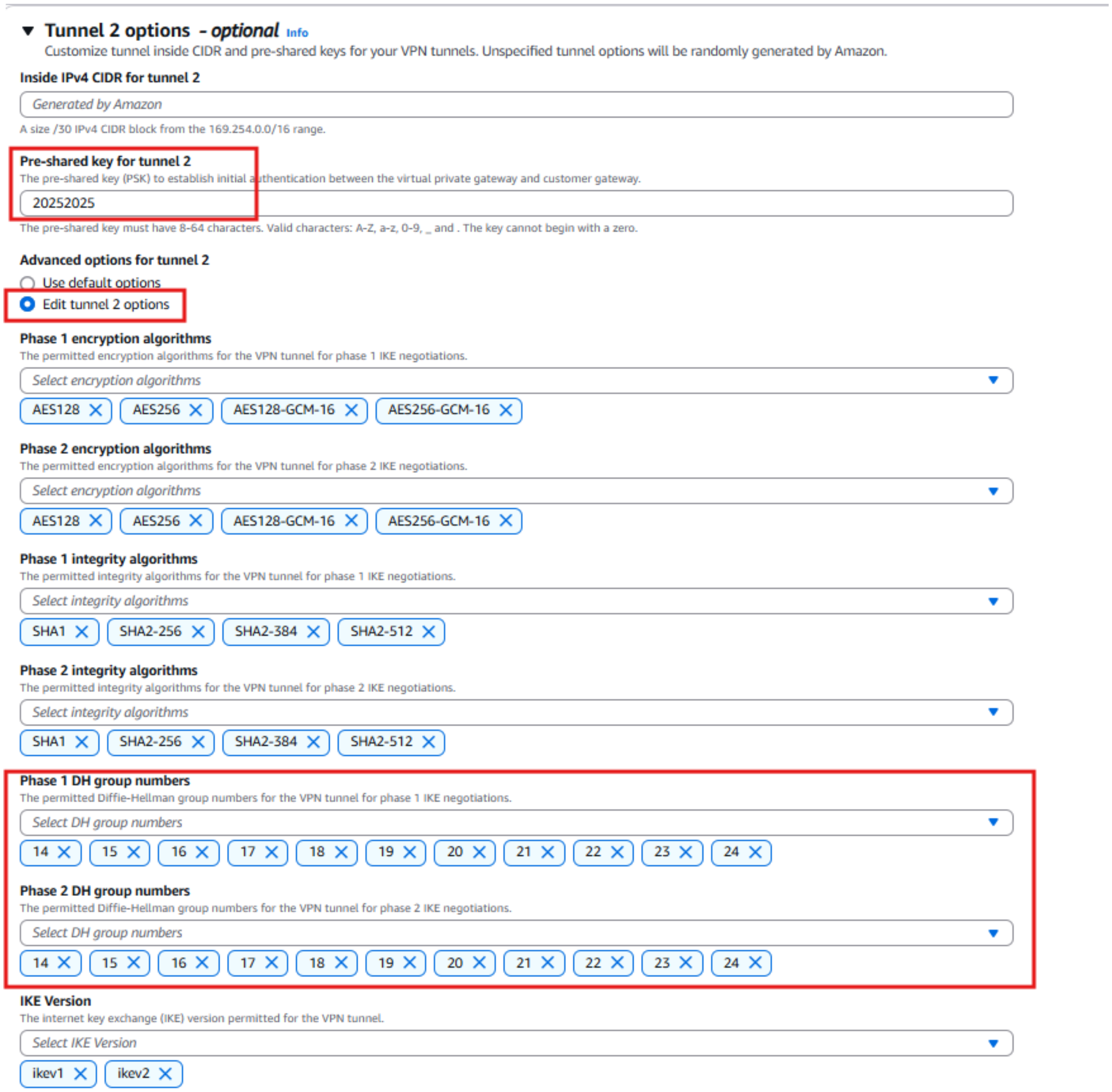
The internet key exchange (IKE) version permitted for the VPN tunnel.

*Select IKE Version* ▼

ikev1 ✕ ikev2 ✕

Tunnel 2 options:

Under Tunnel 2 Options, configure Pre-Shared key and under “Advanced options for tunnel 2” select “Edit tunnel 1 options” and remove DH-group 2 and 5 from the DH-Group numbers.



▼ **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.

20252025

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* ▼

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* ▼

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

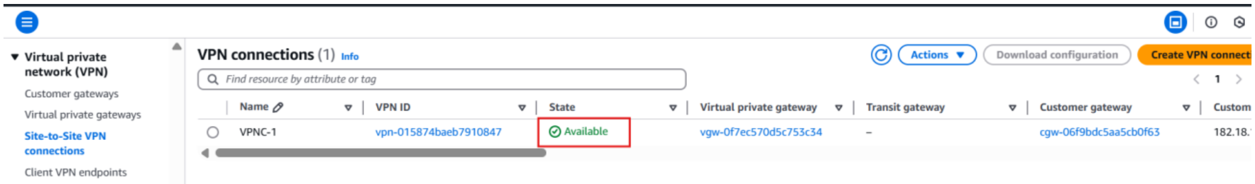
**IKE Version**

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

*Select IKE Version* ▼

ikev1 ✕ ikev2 ✕

Once done Click on Create VPN Connection, this will show the state as Available.

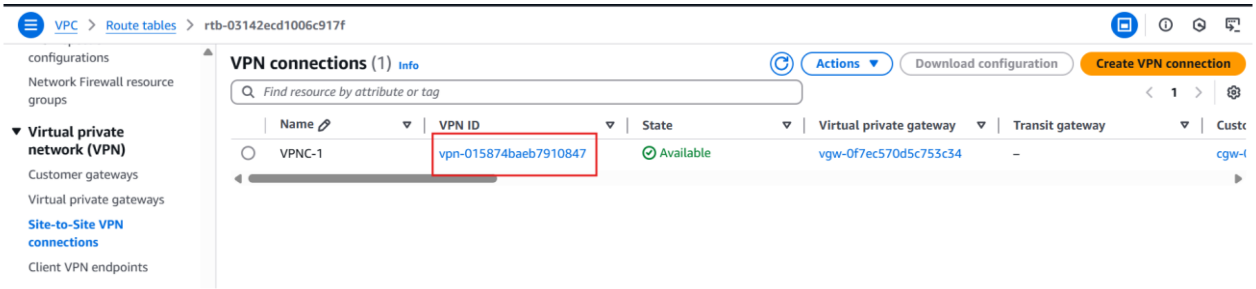


**VPN connections** (1) Info

*Find resource by attribute or tag*

| | Name | VPN ID | State | Virtual private gateway | Transit gateway | Customer gateway | Custom |
|---|---|---|---|---|---|---|---|
| ○ | VPNC-1 | vpn-015874baeb7910847 | ✓ Available | vgw-0f7ec570d5c753c34 | – | cgw-06f9bdc5aa5cb0f63 | 182.18. |

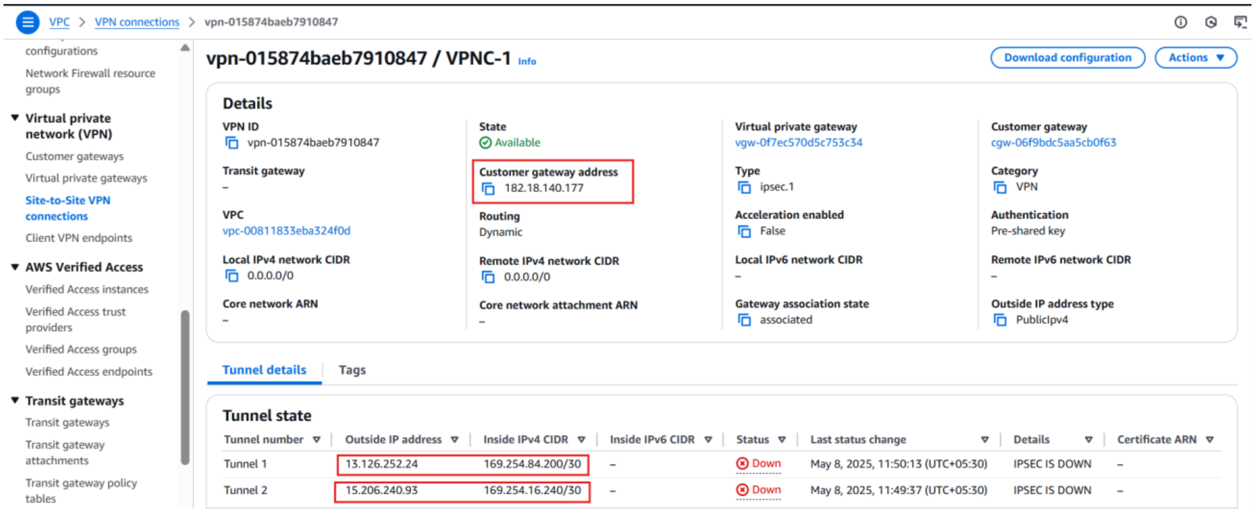
To view the IPsec “Inside” and “Outside” IP address, click on the VPN-ID of Site-to-Site VPN connections under “Virtual private network”.


VPC > Route tables > rtb-03142ecd1006c917f
configurations
Network Firewall resource groups
Virtual private network (VPN)
Customer gateways
Virtual private gateways
Site-to-Site VPN connections
Client VPN endpoints
Actions
Download configuration
Create VPN connection
Find resource by attribute or tag
1

VPN connections (1) Info

|  | Name | VPN ID | State | Virtual private gateway | Transit gateway | Custo |
|---|---|---|---|---|---|---|
| ○ | VPNC-1 | vpn-015874baeb7910847 | Available | vgw-0f7ec570d5c753c34 | – | cgw-( |

"Tunnel details" will provide you "Outside IP address" and the "Inside IPv4 CIDR".


VPC > VPN connections > vpn-015874baeb7910847
configurations
Network Firewall resource groups
Virtual private network (VPN)
Customer gateways
Virtual private gateways
Site-to-Site VPN connections
Client VPN endpoints
AWS Verified Access
Verified Access instances
Verified Access trust providers
Verified Access groups
Verified Access endpoints
Transit gateways
Transit gateways
Transit gateway attachments
Transit gateway policy tables
Download configuration
Actions
Tunnel details
Tags

vpn-015874baeb7910847 / VPNC-1 Info

Details

| | | | |
|---|---|---|---|
| VPN ID<br>vpn-015874baeb7910847 | State<br>Available | Virtual private gateway<br>vgw-0f7ec570d5c753c34 | Customer gateway<br>cgw-06f9bdc5aa5cb0f63 |
| Transit gateway<br>– | Customer gateway address<br>182.18.140.177 | Type<br>ipsec.1 | Category<br>VPN |
| VPC<br>vpc-00811833eba324f0d | Routing<br>Dynamic | Acceleration enabled<br>False | Authentication<br>Pre-shared key |
| Local IPv4 network CIDR<br>0.0.0.0/0 | Remote IPv4 network CIDR<br>0.0.0.0/0 | Local IPv6 network CIDR<br>– | Remote IPv6 network CIDR<br>– |
| Core network ARN<br>– | Core network attachment ARN<br>– | Gateway association state<br>associated | Outside IP address type<br>PublicIpv4 |

Tunnel state

| Tunnel number | Outside IP address | Inside IPv4 CIDR | Inside IPv6 CIDR | Status | Last status change | Details | Certificate ARN |
|---|---|---|---|---|---|---|---|
| Tunnel 1 | 13.126.252.24 | 169.254.84.200/30 | – | Down | May 8, 2025, 11:50:13 (UTC+05:30) | IPSEC IS DOWN | – |
| Tunnel 2 | 15.206.240.93 | 169.254.16.240/30 | – | Down | May 8, 2025, 11:49:37 (UTC+05:30) | IPSEC IS DOWN | – |

From the above generated Inside IPv4 CIDR the first IP will be used by AWS and the other IP will be configured on VOS.

**Example:**

Tunnel 1:

Outside IP – 13.126.252.24

Inside IPv4 CIDR - 169.254.84.200/30

AWS Side: 169.254.84.201/30

VOS Side: 169.254.84.202/30

Tunnel 2:

Outside IP - 15.206.240.93

Inside IPv4 CIDR – 169.254.16.240/30

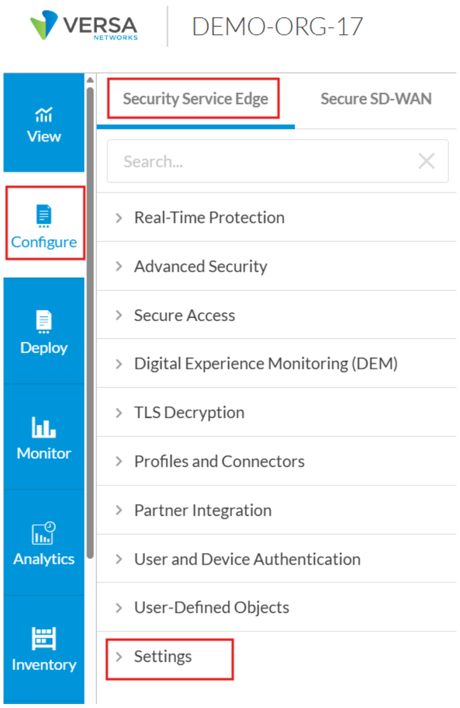
AWS Side: 169.254.16.241/30

VOS Side: 169.254.16.242/30

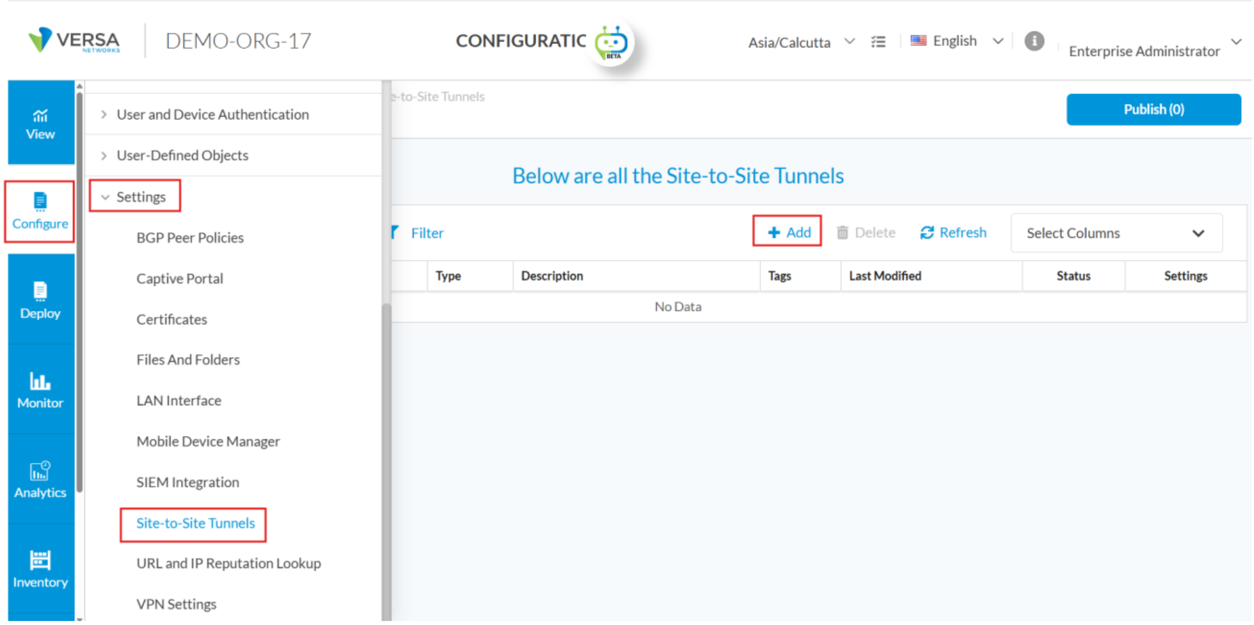
## SASE-GW Configuration:

### Configure Site to Site Tunnels:

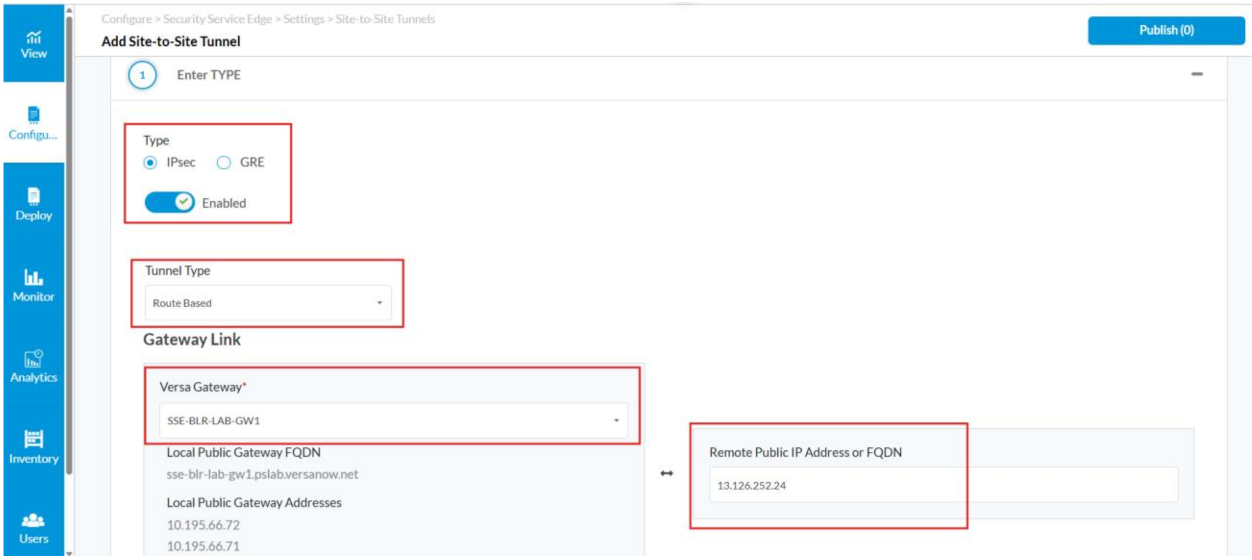
To Configure Site-to-Site Tunnels, Go to Configure →Secure Service Edge → Settings.



Under “Settings” go to “Site-to-Site Tunnels” and click on “Add”.



Under “Enter TYPE”, provide the Type as IPSec, “Tunnel Type” as “Route Based” and Select the Versa Gateway with has the IP 182.18.x.x, provide the Remote Public IP address and click on Next.



Configure > Security Service Edge > Settings > Site-to-Site Tunnels

Add Site-to-Site Tunnel

1 Enter TYPE

Type: ● IPsec ○ GRE

Enabled

Tunnel Type: Route Based

Gateway Link

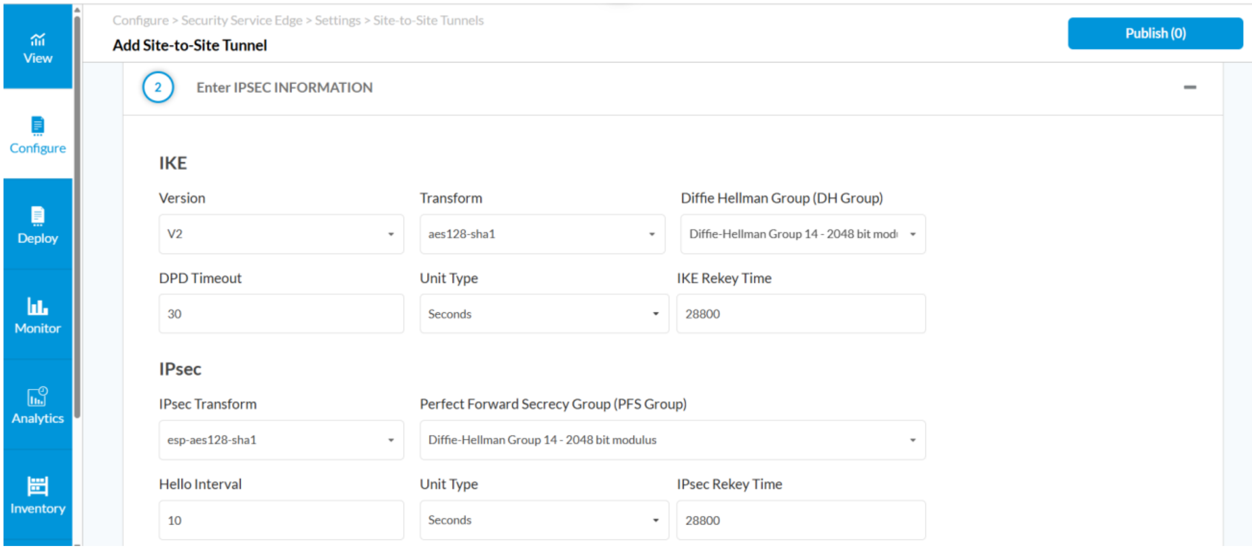
Versa Gateway*: SSE-BLR-LAB-GW1

Local Public Gateway FQDN: sse-blr-lab-gw1.pslab.versanow.net

Local Public Gateway Addresses: 10.195.66.72, 10.195.66.71

Remote Public IP Address or FQDN: 13.126.252.24

Under "Enter IPSEC INFORMATION" configure the Ike and IPsec parameters. The snip below shows the default values.



Configure > Security Service Edge > Settings > Site-to-Site Tunnels

Add Site-to-Site Tunnel

2 Enter IPSEC INFORMATION

IKE

| Version | Transform | Diffie Hellman Group (DH Group) |
|---|---|---|
| V2 | aes128-sha1 | Diffie-Hellman Group 14 - 2048 bit modi |

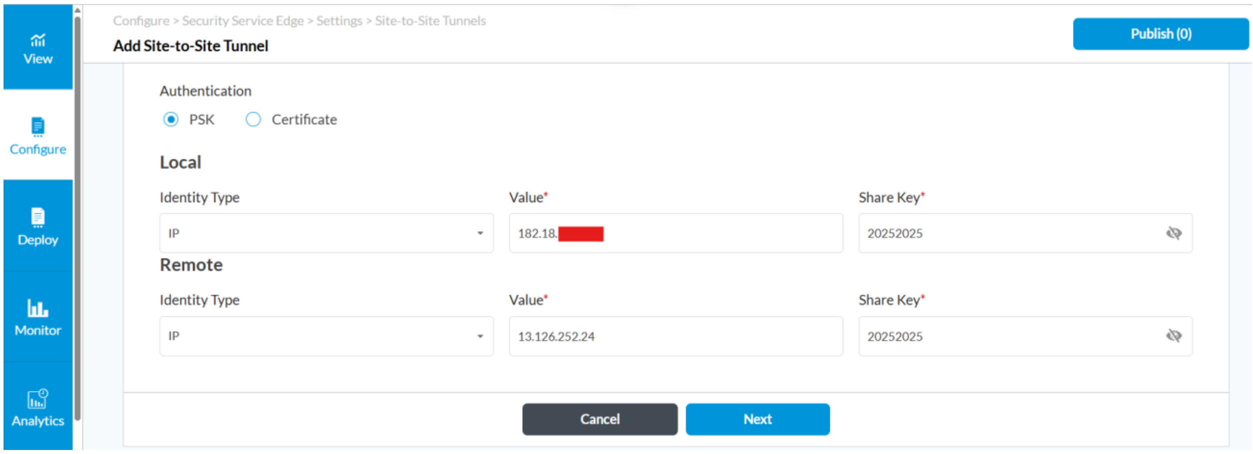
| DPD Timeout | Unit Type | IKE Rekey Time |
|---|---|---|
| 30 | Seconds | 28800 |

IPsec

| IPsec Transform | Perfect Forward Secrecy Group (PFS Group) |
|---|---|
| esp-aes128-sha1 | Diffie-Hellman Group 14 - 2048 bit modulus |

| Hello Interval | Unit Type | IPsec Rekey Time |
|---|---|---|
| 10 | Seconds | 28800 |

Under "Authentication", select "PSK", Under Local and Remote provide the Identity type as IP and give the Public IP's of SASE-GW, the Public IP address of Tunnel-1 and under Share key provide the PSK.



Configure > Security Service Edge > Settings > Site-to-Site Tunnels

Add Site-to-Site Tunnel

Authentication: ● PSK ○ Certificate

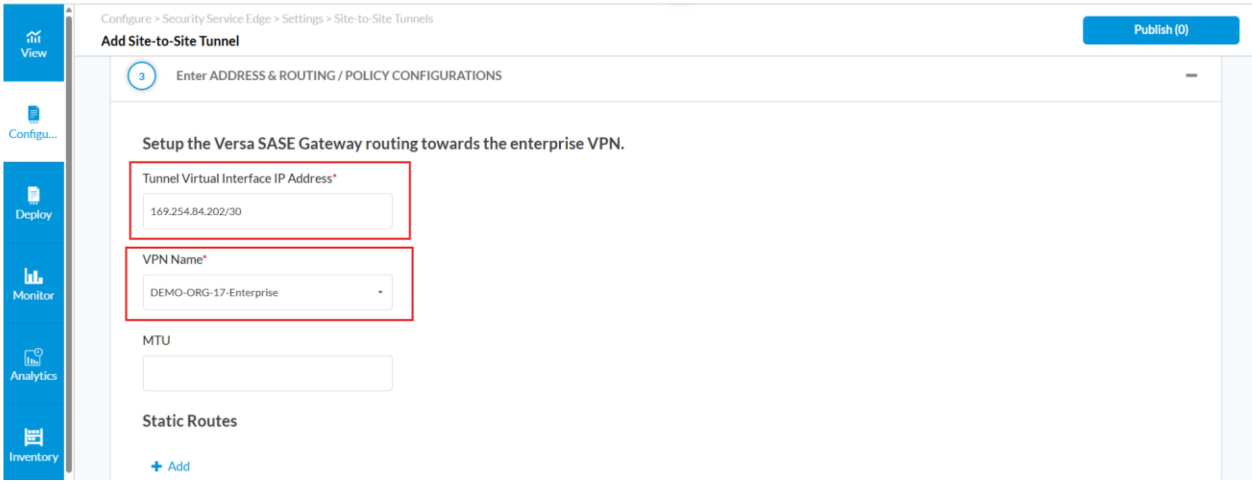
Local

| Identity Type | Value* | Share Key* |
|---|---|---|
| IP | 182.18.[redacted] | 20252025 |

Remote

| Identity Type | Value* | Share Key* |
|---|---|---|
| IP | 13.126.252.24 | 20252025 |

Under "Tunnel Virtual interface IP Address" provide the IP's generated by AWS as shown in the example above and under "VPN Name" provide the respective Enterprise VPN Name.


View
Configu...
Deploy
Monitor
Analytics
Inventory
Configure > Security Service Edge > Settings > Site-to-Site Tunnels
Publish (0)
3
−
+ Add

Add Site-to-Site Tunnel

Enter ADDRESS & ROUTING / POLICY CONFIGURATIONS

Setup the Versa SASE Gateway routing towards the enterprise VPN.

Tunnel Virtual Interface IP Address*: 169.254.84.202/30

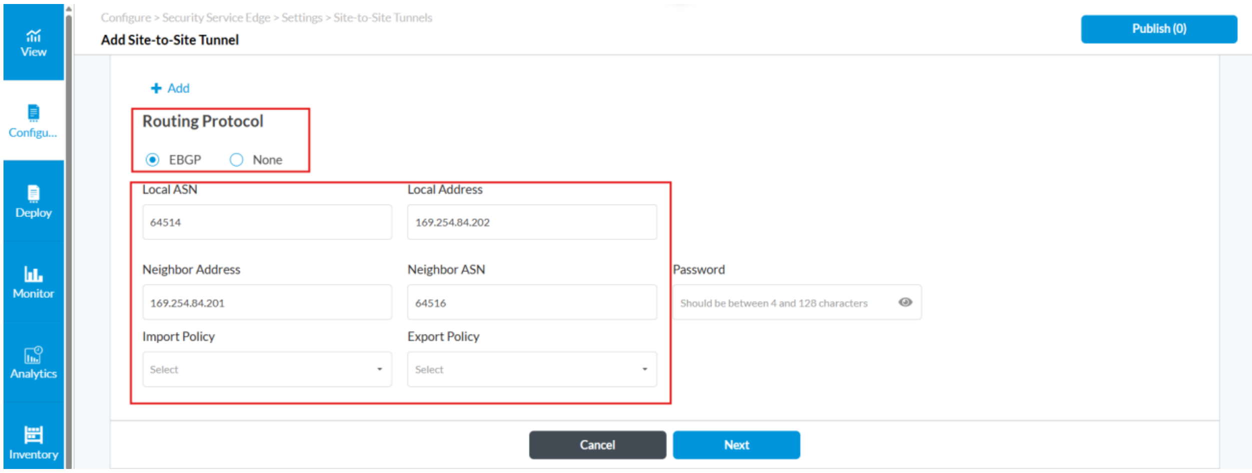
VPN Name*: DEMO-ORG-17-Enterprise

MTU

Static Routes

Under "Routing Protocol" select EBGP and under Local ASN, Local Address, Neighbor Address and Neighbor ASN provide the respective configuration.

| | |
|---|---|
| Local ASN | 64514 |
| Local Address | 169.254.84.202 |
| Remote ASN | 64516 |
| Neighbor Address | 169.254.84.201 |



Add Site-to-Site Tunnel

Routing Protocol

● EBGP ○ None

Local ASN: 64514

Local Address: 169.254.84.202

Neighbor Address: 169.254.84.201

Neighbor ASN: 64516

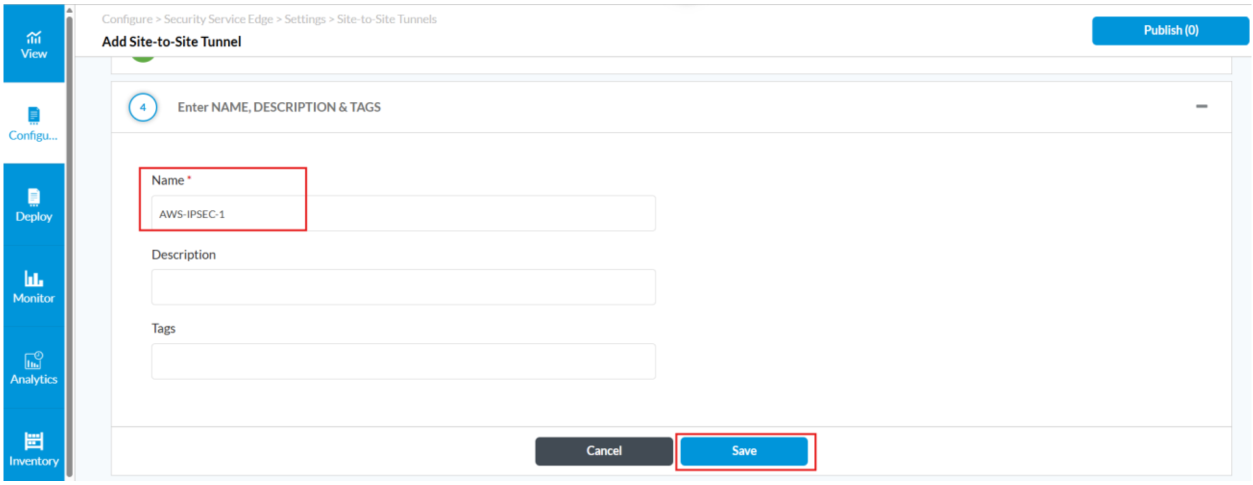
Password: Should be between 4 and 128 characters

Import Policy: Select

Export Policy: Select

Note: The Local and Neighbor Address will be your IPsec Tunnel interfaces.

Under "Enter NAME, DESCRIPTION & TAGS" provide the Name to the IPSec tunnel.



Configure > Security Service Edge > Settings > Site-to-Site Tunnels

Add Site-to-Site Tunnel

4 Enter NAME, DESCRIPTION & TAGS

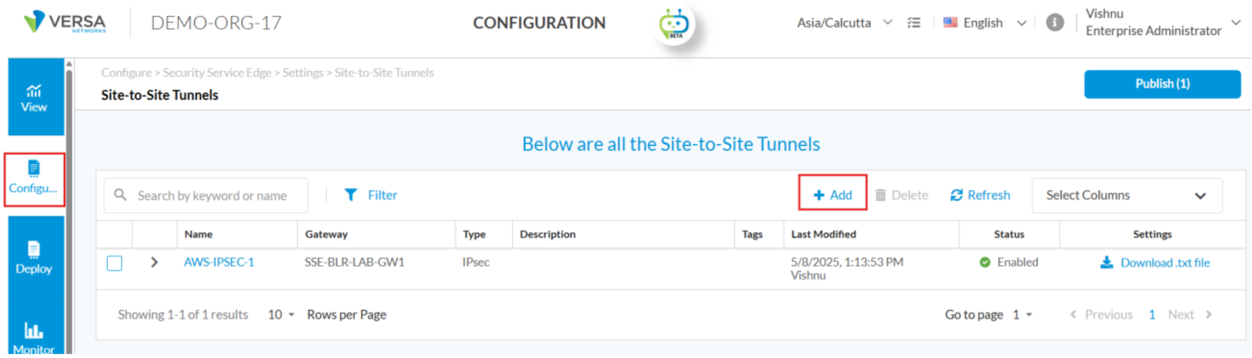
Name *: AWS-IPSEC-1

Description:

Tags:

Since AWS has two IPsec tunnels for Redundancy, create one more IPsec tunnel on SASE-GW.

Under “Settings” go to “Site-to-Site Tunnels” and click on “Add”.



Configure > Security Service Edge > Settings > Site-to-Site Tunnels

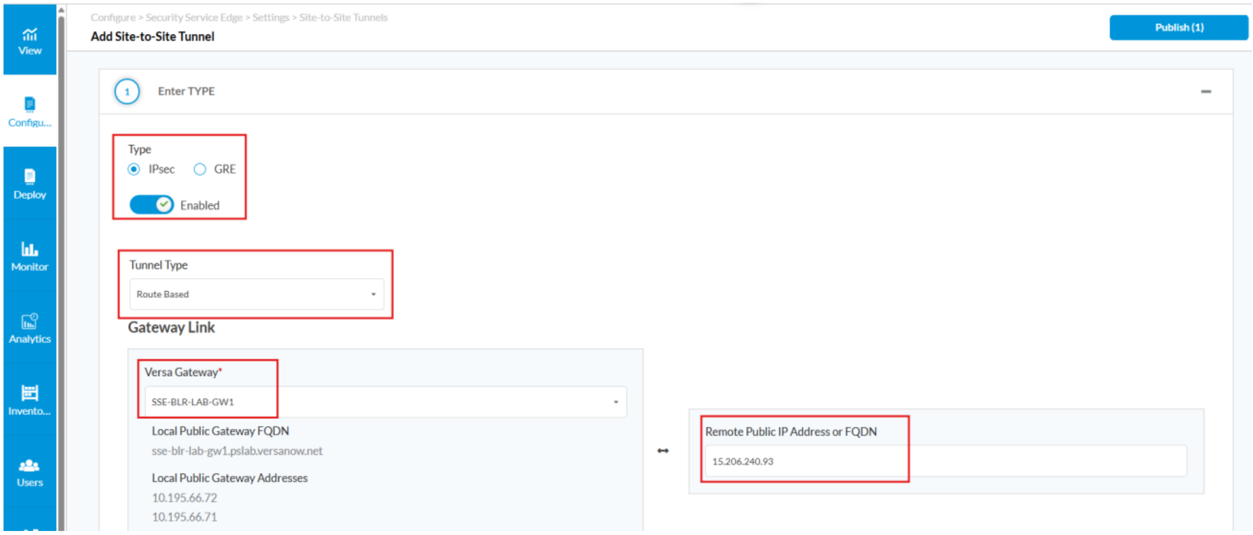
Site-to-Site Tunnels

Below are all the Site-to-Site Tunnels

| Name | Gateway | Type | Description | Tags | Last Modified | Status | Settings |
|---|---|---|---|---|---|---|---|
| AWS-IPSEC-1 | SSE-BLR-LAB-GW1 | IPsec | | | 5/8/2025, 1:13:53 PM<br>Vishnu | Enabled | Download .txt file |

Showing 1-1 of 1 results 10 Rows per Page Go to page 1 Previous 1 Next

Under “Enter TYPE”, provide the Type as IPSec, “Tunnel Type” as “Route Based” and Select the Versa Gateway with has the IP 182.18.x.x, provide the Remote Public IP address and click on Next.



Configure > Security Service Edge > Settings > Site-to-Site Tunnels

Add Site-to-Site Tunnel

1 Enter TYPE

Type: ● IPsec ○ GRE

Enabled

Tunnel Type: Route Based

Gateway Link

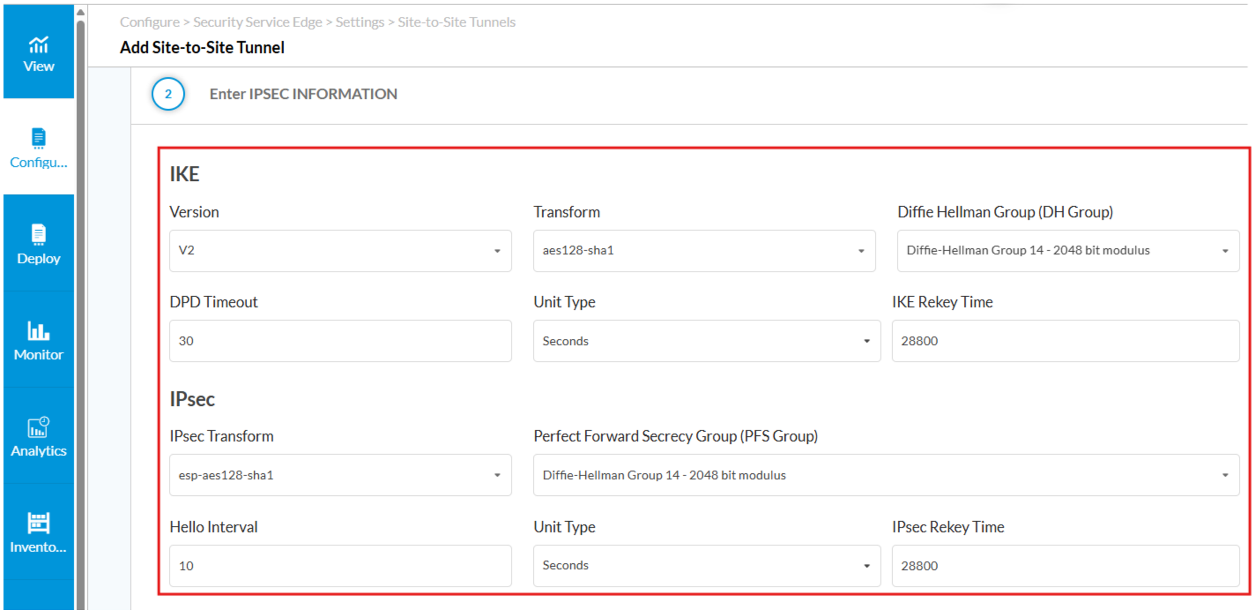
Versa Gateway*: SSE-BLR-LAB-GW1

Local Public Gateway FQDN: sse-blr-lab-gw1.pslab.versanow.net

Local Public Gateway Addresses: 10.195.66.72, 10.195.66.71

Remote Public IP Address or FQDN: 15.206.240.93

Under “Enter IPSEC INFORMATION” configure the Ike and IPsec parameters. The snip below shows the default values.



Configure > Security Service Edge > Settings > Site-to-Site Tunnels

Add Site-to-Site Tunnel

2 Enter IPSEC INFORMATION

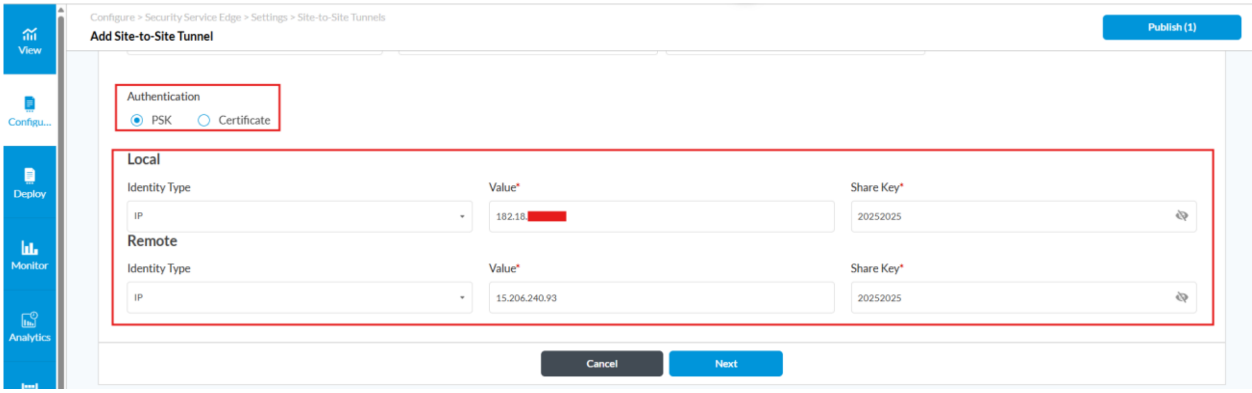
**IKE**

| | | |
|---|---|---|
| Version: V2 | Transform: aes128-sha1 | Diffie Hellman Group (DH Group): Diffie-Hellman Group 14 - 2048 bit modulus |
| DPD Timeout: 30 | Unit Type: Seconds | IKE Rekey Time: 28800 |

**IPsec**

| | | |
|---|---|---|
| IPsec Transform: esp-aes128-sha1 | Perfect Forward Secrecy Group (PFS Group): Diffie-Hellman Group 14 - 2048 bit modulus | |
| Hello Interval: 10 | Unit Type: Seconds | IPsec Rekey Time: 28800 |

Under “Authentication”, select “PSK”, Under Local and Remote provide the Identity type as IP and give the Public IP’s of SASE-GW, the Public IP address of Tunnel-1 and under Share key provide the PSK.



Configure > Security Service Edge > Settings > Site-to-Site Tunnels

Add Site-to-Site Tunnel

Authentication
● PSK ○ Certificate

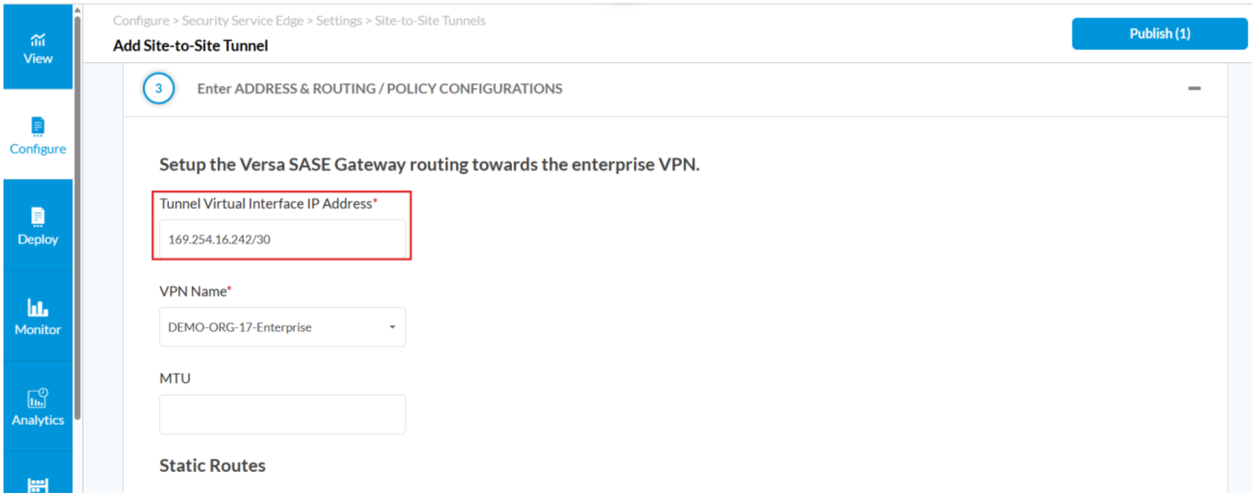
**Local**

| Identity Type | Value* | Share Key* |
|---|---|---|
| IP | 182.18.[redacted] | 20252025 |

**Remote**

| Identity Type | Value* | Share Key* |
|---|---|---|
| IP | 15.206.240.93 | 20252025 |

Under “Tunnel Virtual interface IP Address” provide the IP’s generated by AWS as shown in the example above and under “VPN Name” provide the respective Enterprise VPN Name.



Configure > Security Service Edge > Settings > Site-to-Site Tunnels

Add Site-to-Site Tunnel

3 Enter ADDRESS & ROUTING / POLICY CONFIGURATIONS

Setup the Versa SASE Gateway routing towards the enterprise VPN.

Tunnel Virtual Interface IP Address*: 169.254.16.242/30

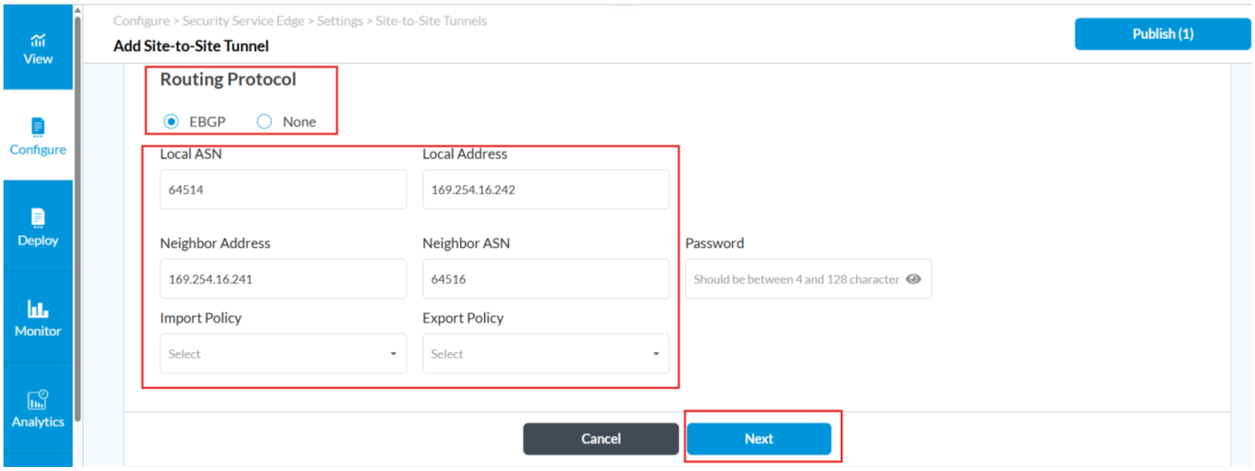
VPN Name*: DEMO-ORG-17-Enterprise

MTU:

Static Routes

Under “Routing Protocol” select EBGP and under Local ASN, Local Address, Neighbor Address and Neighbor ASN provide the respective configuration.

| | |
|---|---|
| Local ASN | 64514 |
| Local Address | 169.254.16.242 |
| Remote ASN | 64516 |
| Neighbor Address | 169.254.16.241 |



Routing Protocol

● EBGP ○ None

Local ASN: 64514

Local Address: 169.254.16.242

Neighbor Address: 169.254.16.241

Neighbor ASN: 64516

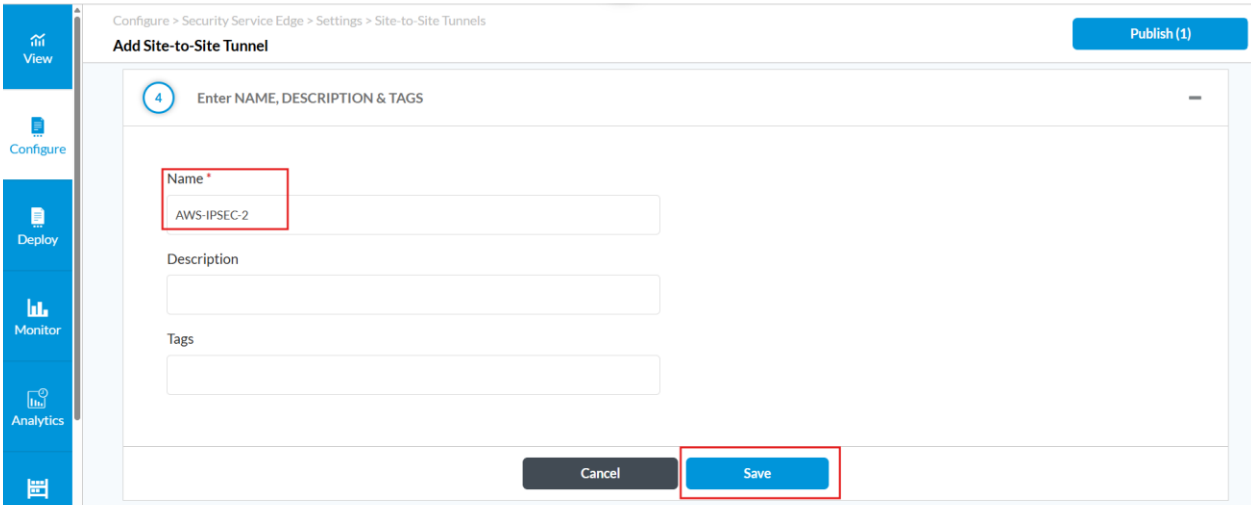
Password: Should be between 4 and 128 character

Import Policy: Select

Export Policy: Select

Note: The Local and Neighbor Address will be your IPsec Tunnel interfaces.

Under “Enter NAME, DESCRIPTION & TAGS” provide the Name to the IPSec tunnel.


View
Configure
Deploy
Monitor
Analytics
Configure > Security Service Edge > Settings > Site-to-Site Tunnels
Add Site-to-Site Tunnel
Publish (1)
4
Enter NAME, DESCRIPTION & TAGS

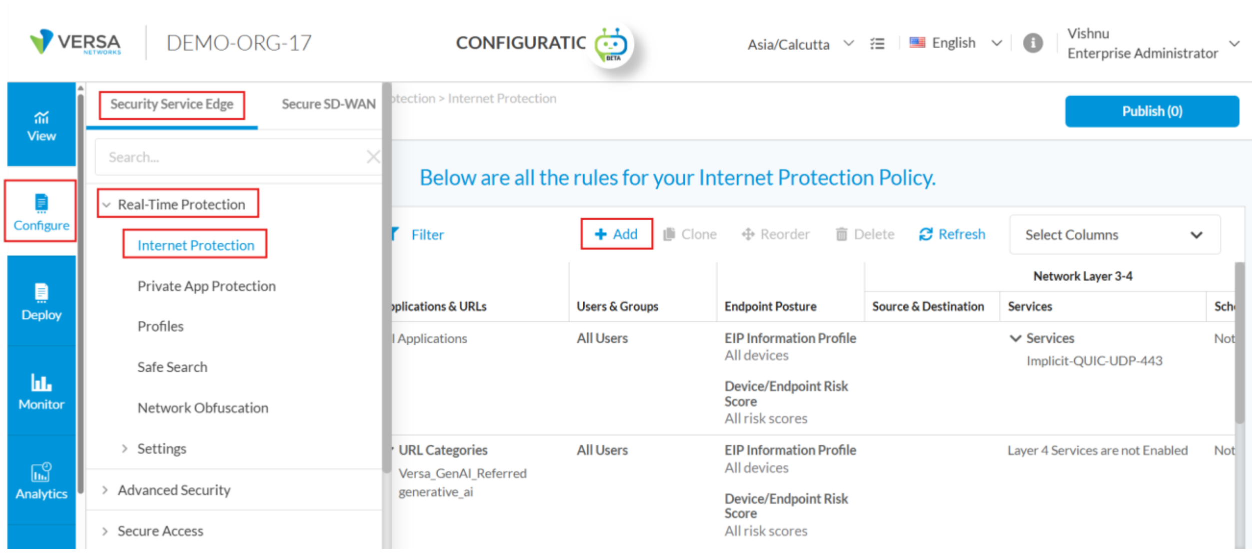
Name *: AWS-IPSEC-2

Description:

Tags:

### Configuring Secure Access Rule:

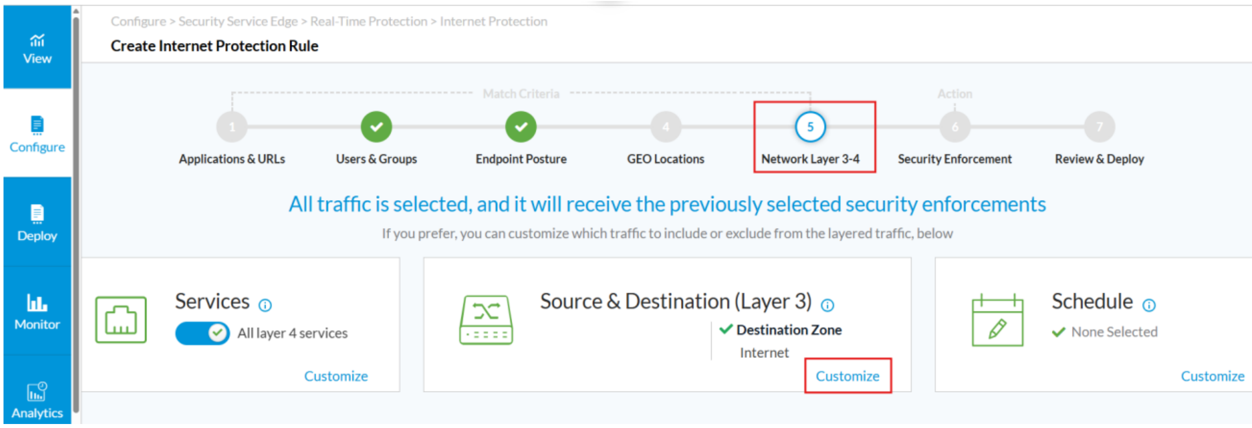
To Create a secure access rule for allowing traffic from SASE clients to AWS EC2 through IPSec tunnels, Go to Configure → Secure Service Edge → Real-Time Protection → Internet Protection and click on “Add”.



Below are all the rules for your Internet Protection Policy.

| plications & URLs | Users & Groups | Endpoint Posture | Source & Destination | Services | Sch |
|---|---|---|---|---|---|
| l Applications | All Users | EIP Information Profile<br>All devices<br>Device/Endpoint Risk Score<br>All risk scores | | Services<br>Implicit-QUIC-UDP-443 | Not |
| URL Categories<br>Versa_GenAI_Referred<br>generative_ai | All Users | EIP Information Profile<br>All devices<br>Device/Endpoint Risk Score<br>All risk scores | | Layer 4 Services are not Enabled | Not |

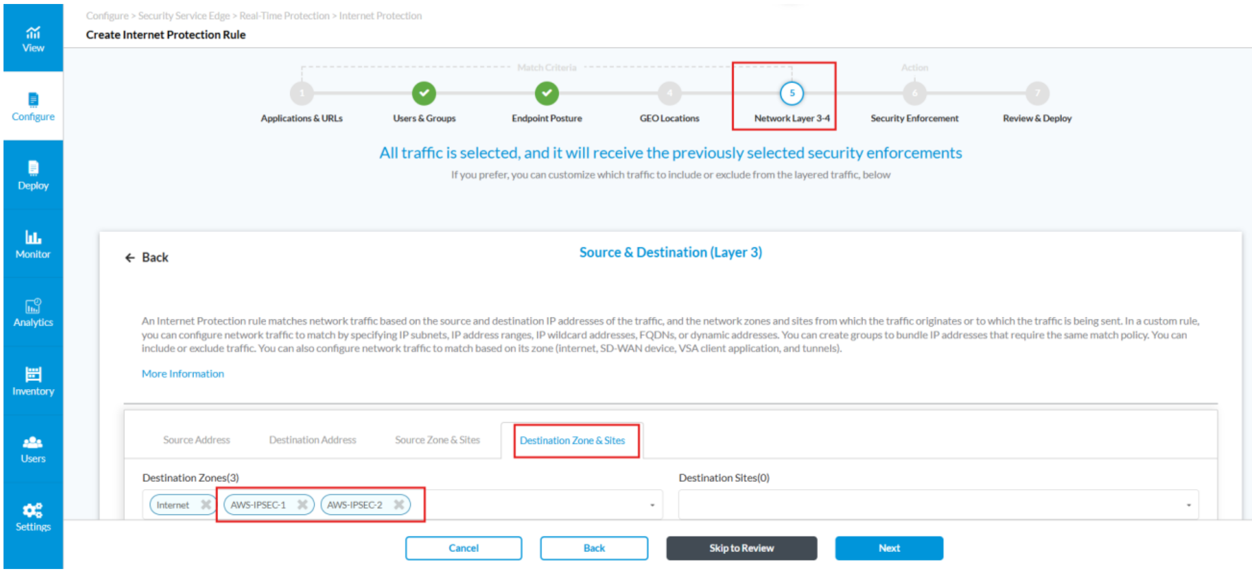
Under “Network Layer 3-4” go to “Source & Destination (Layer 3)” and click on “Customize”.



All traffic is selected, and it will receive the previously selected security enforcements

If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

Under “Destination Zone & Sites” configure “AWS-IPsec-1” and “AWS-IPSEC-2”.



All traffic is selected, and it will receive the previously selected security enforcements

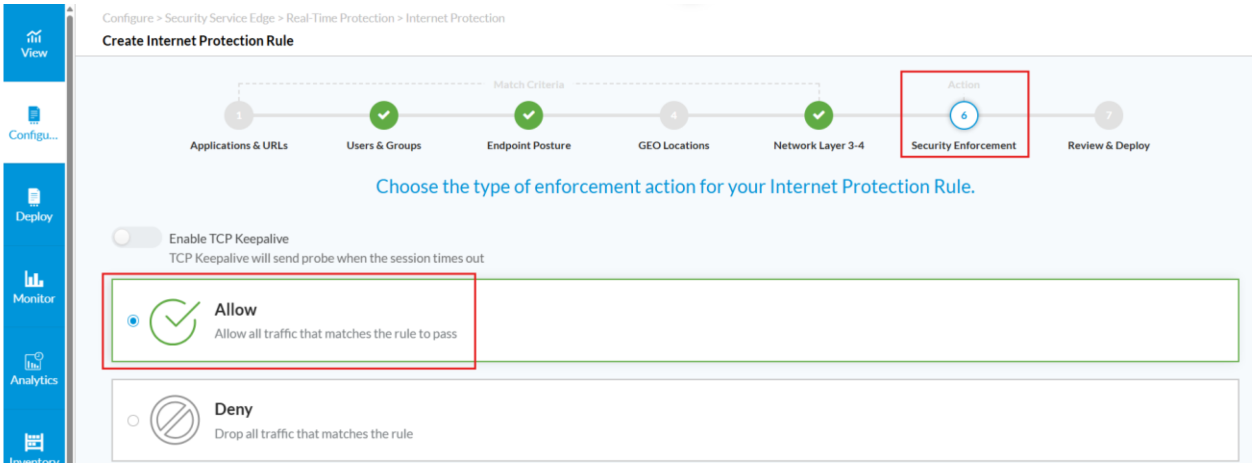
If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

An Internet Protection rule matches network traffic based on the source and destination IP addresses of the traffic, and the network zones and sites from which the traffic originates or to which the traffic is being sent. In a custom rule, you can configure network traffic to match by specifying IP subnets, IP address ranges, IP wildcard addresses, FQDNs, or dynamic addresses. You can create groups to bundle IP addresses that require the same match policy. You can include or exclude traffic. You can also configure network traffic to match based on its zone (internet, SD-WAN device, VSA client application, and tunnels).

Destination Zones(3): Internet, AWS-IPSEC-1, AWS-IPSEC-2

Destination Sites(0):

Under “Security Enforcement” Configure the action as “Allow”.



Configure > Security Service Edge > Real-Time Protection > Internet Protection

Create Internet Protection Rule

Choose the type of enforcement action for your Internet Protection Rule.

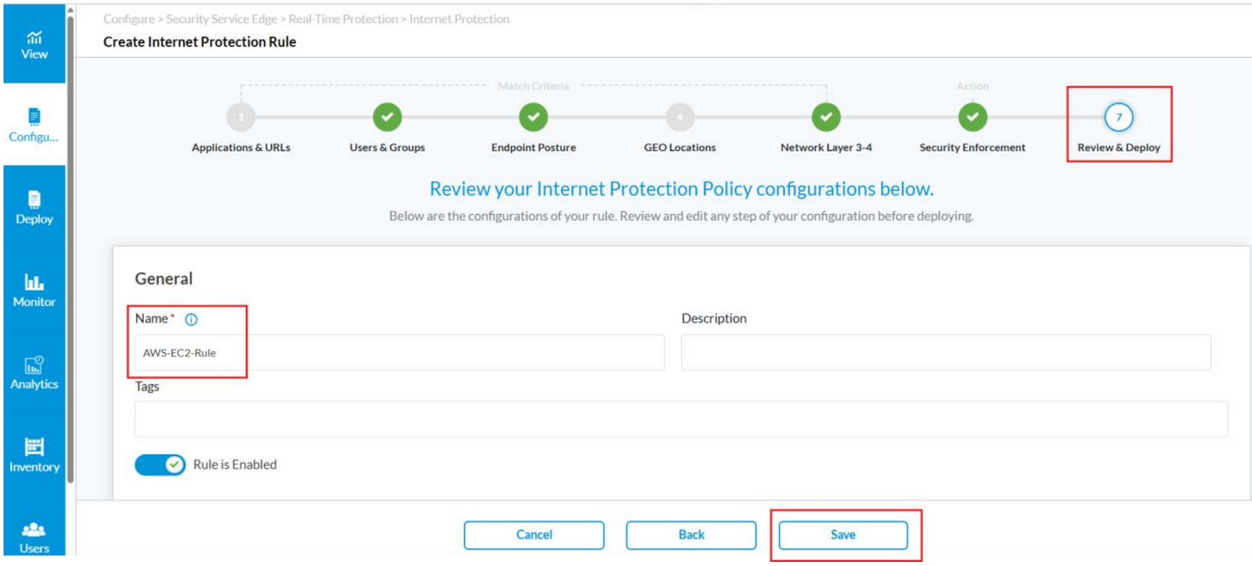
Enable TCP Keepalive
TCP Keepalive will send probe when the session times out

● Allow
Allow all traffic that matches the rule to pass

○ Deny
Drop all traffic that matches the rule

Note: Security Enforcement can be configured as per the requirement.

Under "Review and Deploy" provide the "Name" for the Internet Protection Rule.



Configure > Security Service Edge > Real-Time Protection > Internet Protection

Create Internet Protection Rule

Review your Internet Protection Policy configurations below.

Below are the configurations of your rule. Review and edit any step of your configuration before deploying.

General

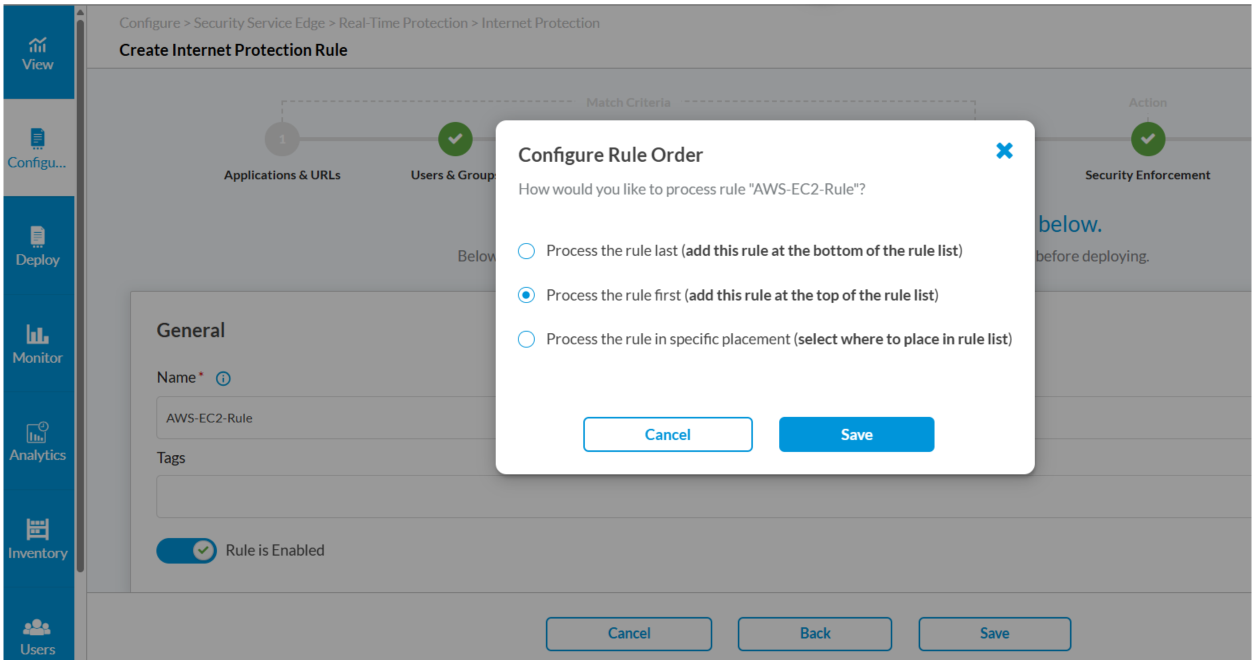
Name*: AWS-EC2-Rule

Description:

Tags:

Rule is Enabled

Under "Configure the Rule Order" place the rule at the top.



Configure > Security Service Edge > Real-Time Protection > Internet Protection

Create Internet Protection Rule

General

Name* : AWS-EC2-Rule

Tags

Rule is Enabled

Configure Rule Order

How would you like to process rule "AWS-EC2-Rule"?

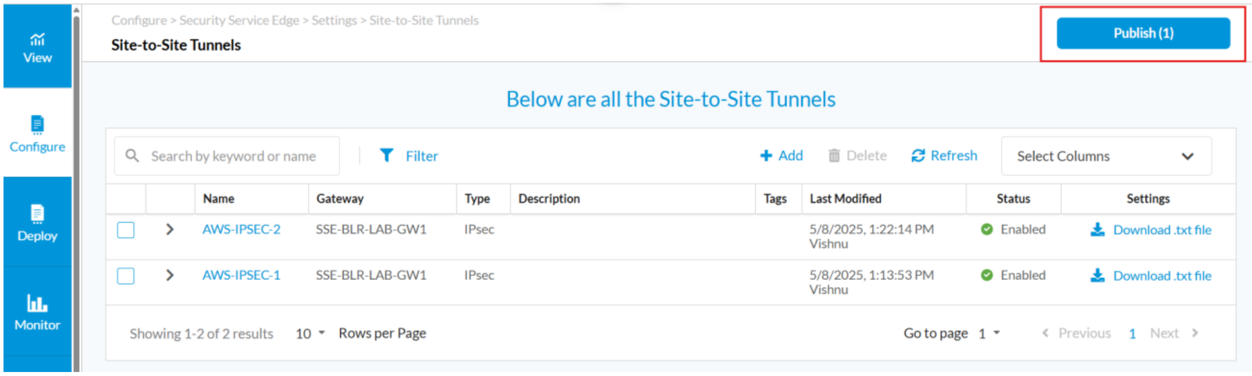
○ Process the rule last (**add this rule at the bottom of the rule list**)

● Process the rule first (**add this rule at the top of the rule list**)

○ Process the rule in specific placement (**select where to place in rule list**)

Cancel Save

Once the configuration is complete Publish the Configuration to SASE Gateways.



Configure > Security Service Edge > Settings > Site-to-Site Tunnels

Site-to-Site Tunnels

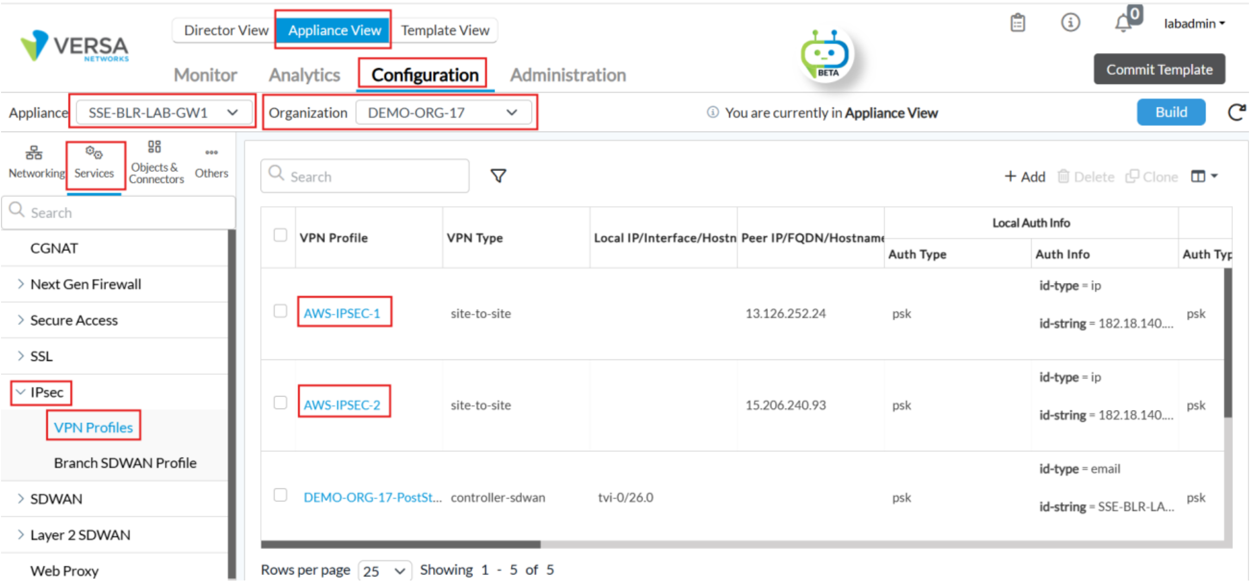
Below are all the Site-to-Site Tunnels

| | | Name | Gateway | Type | Description | Tags | Last Modified | Status | Settings |
|---|---|---|---|---|---|---|---|---|---|
| □ | > | AWS-IPSEC-2 | SSE-BLR-LAB-GW1 | IPsec | | | 5/8/2025, 1:22:14 PM<br>Vishnu | Enabled | Download .txt file |
| □ | > | AWS-IPSEC-1 | SSE-BLR-LAB-GW1 | IPsec | | | 5/8/2025, 1:13:53 PM<br>Vishnu | Enabled | Download .txt file |

Showing 1-2 of 2 results 10 Rows per Page Go to page 1 Previous 1 Next

IPSec on AWS is always a responder, so we need to modify the SASE Gateway IPsec from “Re-sponder” to “Auto” on both the IPsec Tunnels.

Under “Appliance View” go to respective SASE GW and under “Configure” go to “Services” → IPsec → VPN Profiles and select the VPN Profile configured for AWS.



Appliance: SSE-BLR-LAB-GW1

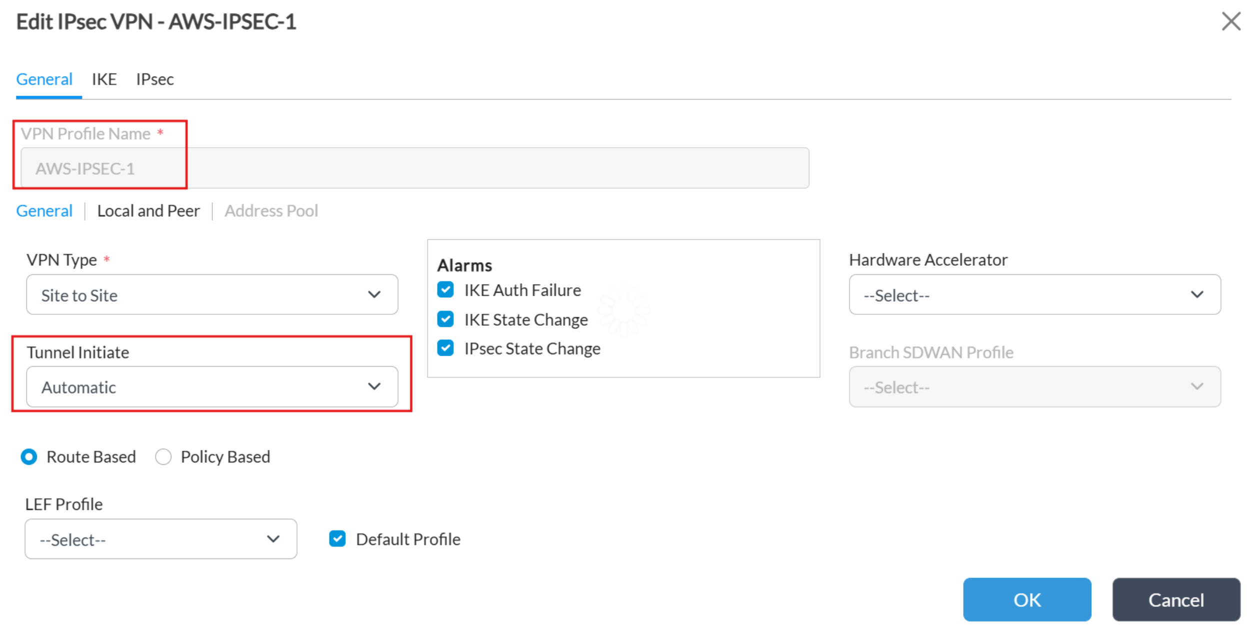
Organization: DEMO-ORG-17

You are currently in **Appliance View**

| | VPN Profile | VPN Type | Local IP/Interface/Hostn | Peer IP/FQDN/Hostname | Local Auth Info | | |
|---|---|---|---|---|---|---|---|
| | | | | | Auth Type | Auth Info | Auth Typ |
| □ | AWS-IPSEC-1 | site-to-site | | 13.126.252.24 | psk | **id-type** = ip<br>**id-string** = 182.18.140.... | psk |
| □ | AWS-IPSEC-2 | site-to-site | | 15.206.240.93 | psk | **id-type** = ip<br>**id-string** = 182.18.140.... | psk |
| □ | DEMO-ORG-17-PostSt... | controller-sdwan | tvi-0/26.0 | | psk | **id-type** = email<br>**id-string** = SSE-BLR-LA... | psk |

Rows per page 25 Showing 1 - 5 of 5

Under “General”, change the “Tunnel Initiate” to “Automatic” for both AWS-IPSEC-1 and AWS-IPSEC-2.



Edit IPsec VPN - AWS-IPSEC-1

VPN Profile Name * AWS-IPSEC-1

VPN Type * Site to Site

Tunnel Initiate Automatic

Alarms
☑ IKE Auth Failure
☑ IKE State Change
☑ IPsec State Change

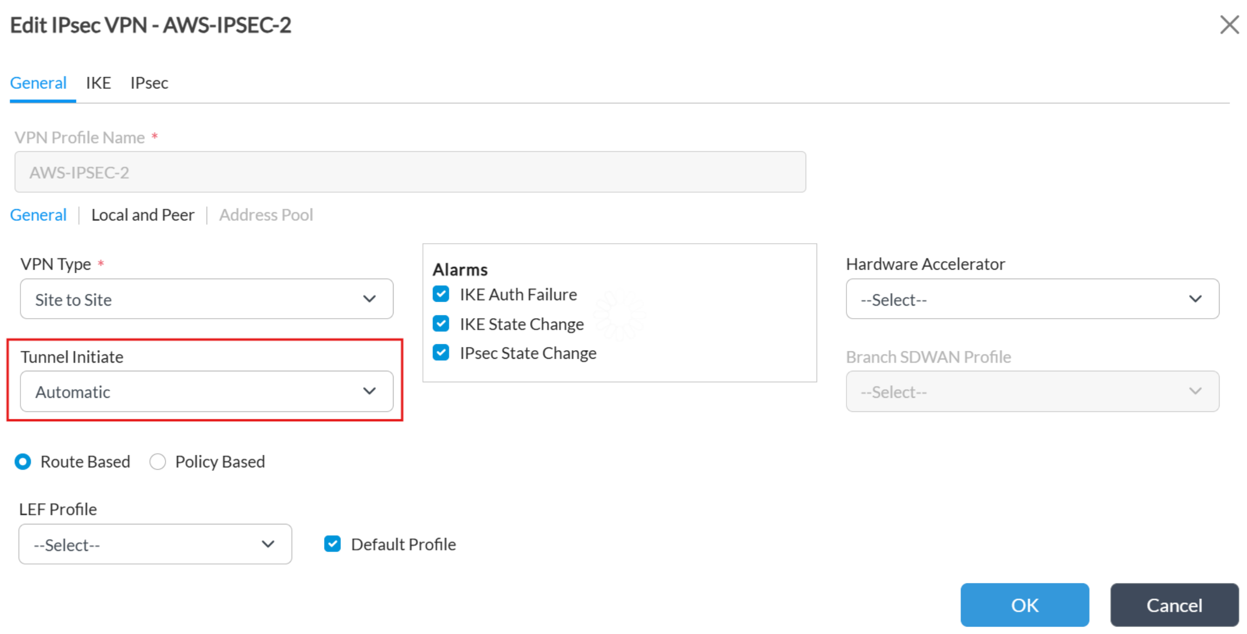
Hardware Accelerator --Select--

Branch SDWAN Profile --Select--

● Route Based ○ Policy Based

LEF Profile --Select--

☑ Default Profile



Edit IPsec VPN - AWS-IPSEC-2

General | IKE | IPsec

VPN Profile Name *: AWS-IPSEC-2

General | Local and Peer | Address Pool

VPN Type *: Site to Site

Tunnel Initiate: Automatic

Alarms
☑ IKE Auth Failure
☑ IKE State Change
☑ IPsec State Change

Hardware Accelerator: --Select--

Branch SDWAN Profile: --Select--

● Route Based ○ Policy Based

LEF Profile: --Select--

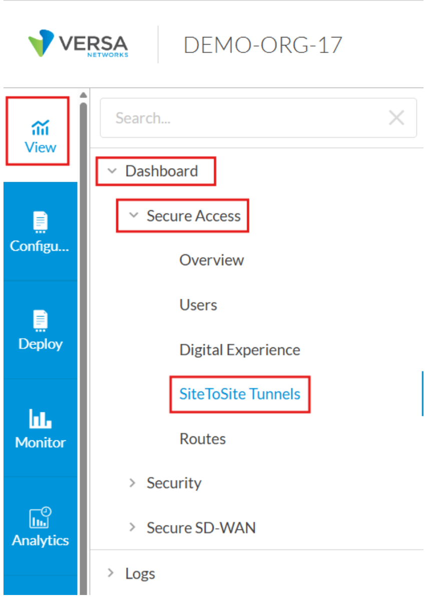
☑ Default Profile

Once the above configuration is complete you can view the IPsec Tunnel status, BGP status on AWS and Concerto.

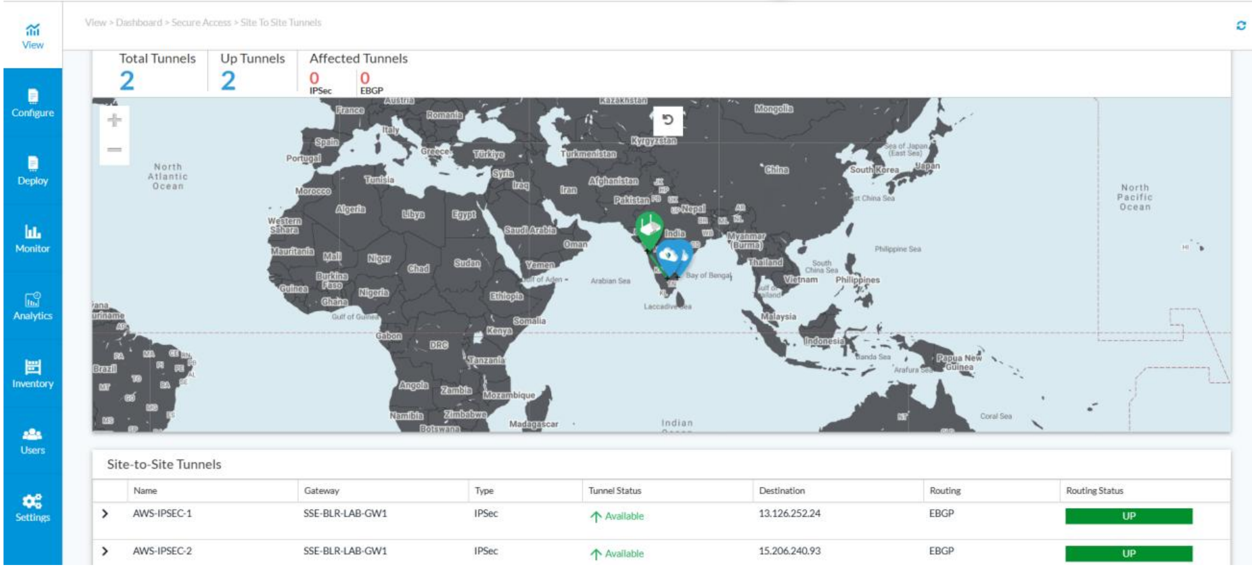
## Verifying IPsec and BGP status:

### Concerto:

Go to View → Dashboard → Secure Access → Site to Site Tunnels.



Under Site-to-Site Tunnels, check the Tunnel and Routing Status.



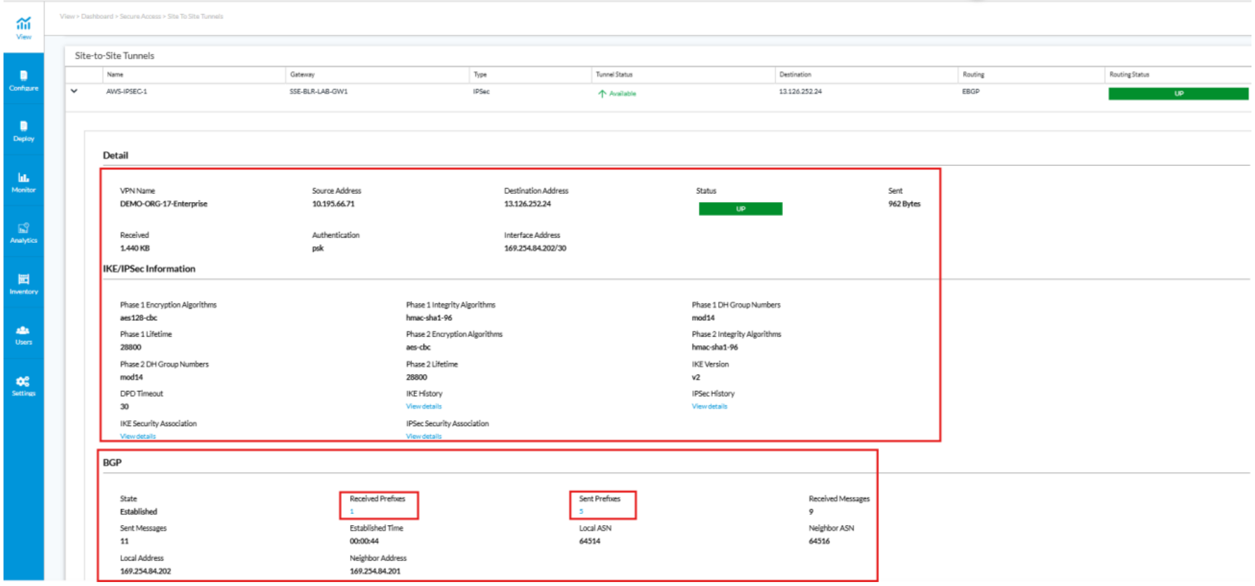
View > Dashboard > Secure Access > Site To Site Tunnels

Total Tunnels 2 | Up Tunnels 2 | Affected Tunnels 0 IPSec 0 EBGP

Site-to-Site Tunnels

| | Name | Gateway | Type | Tunnel Status | Destination | Routing | Routing Status |
|---|---|---|---|---|---|---|---|
| > | AWS-IPSEC-1 | SSE-BLR-LAB-GW1 | IPSec | ↑ Available | 13.126.252.24 | EBGP | UP |
| > | AWS-IPSEC-2 | SSE-BLR-LAB-GW1 | IPSec | ↑ Available | 15.206.240.93 | EBGP | UP |

Expanding the Tunnel will show detailed information about the IPsec tunnels and BGP.



View > Dashboard > Secure Access > Site To Site Tunnels

Site-to-Site Tunnels

| | Name | Gateway | Type | Tunnel Status | Destination | Routing | Routing Status |
|---|---|---|---|---|---|---|---|
| ⌄ | AWS-IPSEC-1 | SSE-BLR-LAB-GW1 | IPSec | ↑ Available | 13.126.252.24 | EBGP | UP |

Detail

VPN Name: DEMO-ORG-17-Enterprise
Source Address: 10.195.66.71
Destination Address: 13.126.252.24
Status: UP
Sent: 962 Bytes
Received: 1.440 KB
Authentication: psk
Interface Address: 169.254.84.202/30

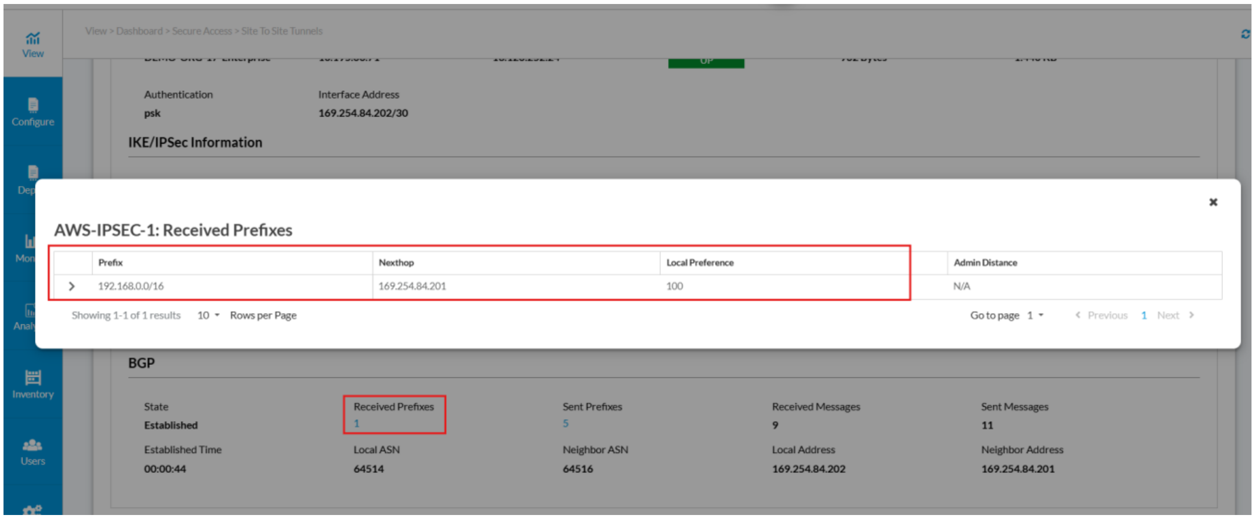
IKE/IPSec Information

Phase 1 Encryption Algorithms: aes128-cbc
Phase 1 Integrity Algorithms: hmac-sha1-96
Phase 1 DH Group Numbers: mod14
Phase 1 Lifetime: 28800
Phase 2 Encryption Algorithms: aes-cbc
Phase 2 Integrity Algorithms: hmac-sha1-96
Phase 2 DH Group Numbers: mod14
Phase 2 Lifetime: 28800
IKE Version: v2
DPD Timeout: 30
IKE History: View details
IPSec History: View details
IKE Security Association: View details
IPSec Security Association: View details

BGP

State: Established
Received Prefixes: 1
Sent Prefixes: 5
Received Messages: 9
Sent Messages: 11
Established Time: 00:00:44
Local ASN: 64514
Neighbor ASN: 64516
Local Address: 169.254.84.202
Neighbor Address: 169.254.84.201

Routes Sent and Received can be viewed by clicking on Received Prefixes and Sent Prefixes.



View > Dashboard > Secure Access > Site To Site Tunnels

Authentication
psk

Interface Address
169.254.84.202/30

IKE/IPSec Information

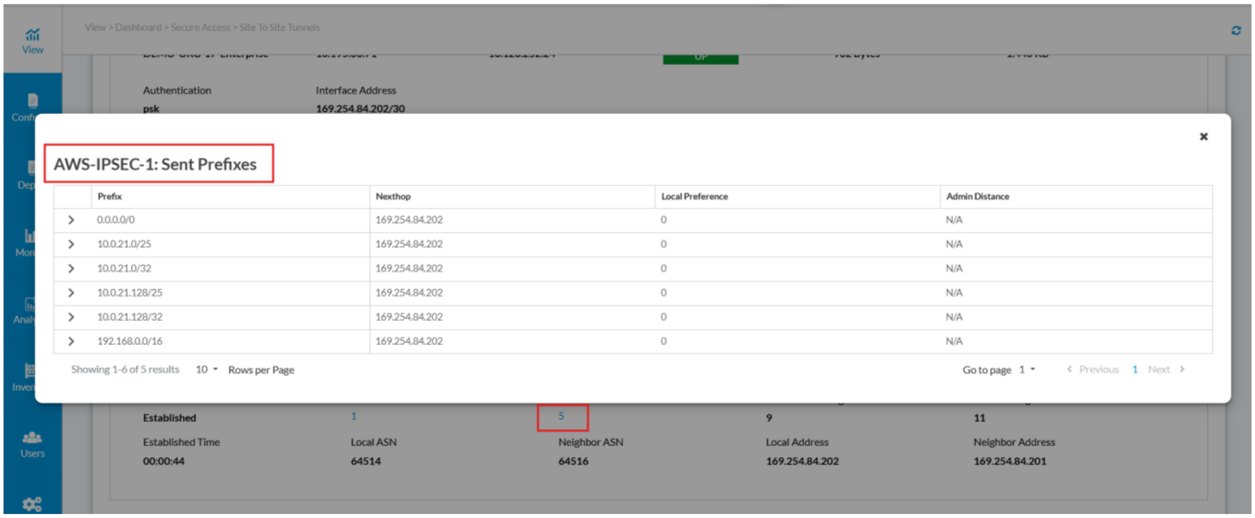
AWS-IPSEC-1: Received Prefixes

| | Prefix | Nexthop | Local Preference | Admin Distance |
|---|---|---|---|---|
| > | 192.168.0.0/16 | 169.254.84.201 | 100 | N/A |

Showing 1-1 of 1 results 10 Rows per Page Go to page 1 Previous 1 Next

BGP

| State | Received Prefixes | Sent Prefixes | Received Messages | Sent Messages |
|---|---|---|---|---|
| Established | 1 | 5 | 9 | 11 |
| **Established Time** | **Local ASN** | **Neighbor ASN** | **Local Address** | **Neighbor Address** |
| 00:00:44 | 64514 | 64516 | 169.254.84.202 | 169.254.84.201 |



View > Dashboard > Secure Access > Site To Site Tunnels

Authentication
psk

Interface Address
169.254.84.202/30

AWS-IPSEC-1: Sent Prefixes

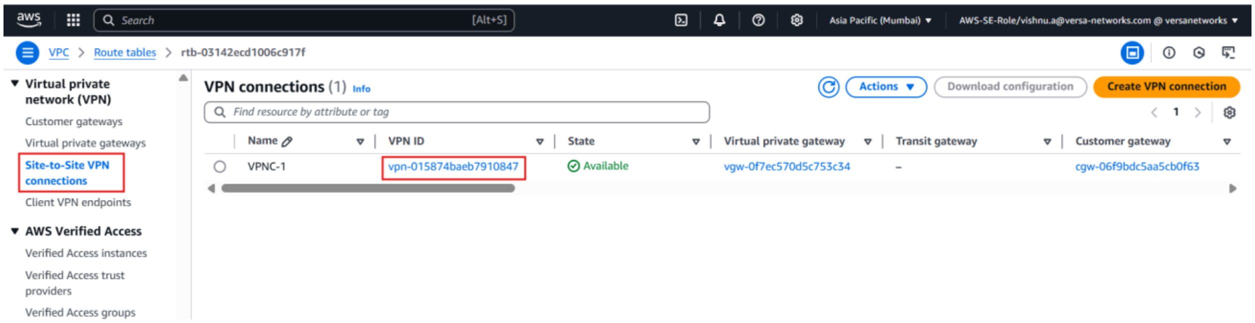
| | Prefix | Nexthop | Local Preference | Admin Distance |
|---|---|---|---|---|
| > | 0.0.0.0/0 | 169.254.84.202 | 0 | N/A |
| > | 10.0.21.0/25 | 169.254.84.202 | 0 | N/A |
| > | 10.0.21.0/32 | 169.254.84.202 | 0 | N/A |
| > | 10.0.21.128/25 | 169.254.84.202 | 0 | N/A |
| > | 10.0.21.128/32 | 169.254.84.202 | 0 | N/A |
| > | 192.168.0.0/16 | 169.254.84.202 | 0 | N/A |

Showing 1-6 of 5 results 10 Rows per Page Go to page 1 Previous 1 Next

| | | | | |
|---|---|---|---|---|
| Established | 1 | 5 | 9 | 11 |
| Established Time | Local ASN | Neighbor ASN | Local Address | Neighbor Address |
| 00:00:44 | 64514 | 64516 | 169.254.84.202 | 169.254.84.201 |

## AWS:

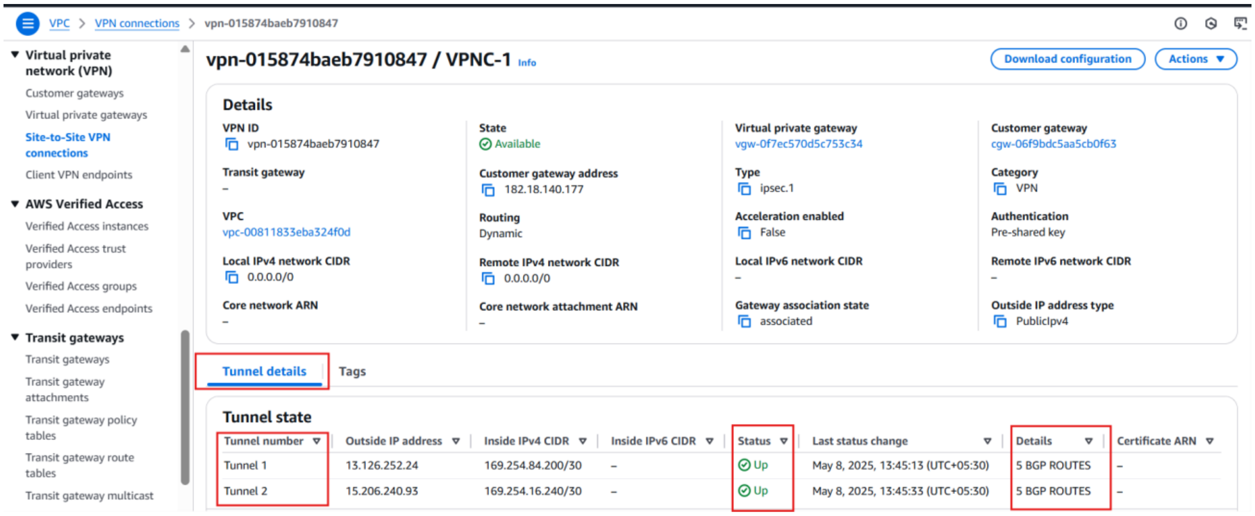
To view IPsec Tunnel status, go to "Virtual Private Network" → "Site to Site VPN connection" and click on VPN ID.


aws
Search [Alt+S]
Asia Pacific (Mumbai)
AWS-SE-Role/vishnu.a@versa-networks.com @ versanetworks
VPC > Route tables > rtb-03142ecd1006c917f
Virtual private network (VPN)
Customer gateways
Virtual private gateways
Site-to-Site VPN connections
Client VPN endpoints
AWS Verified Access
Verified Access instances
Verified Access trust providers
Verified Access groups
Actions
Download configuration
Create VPN connection
Find resource by attribute or tag

VPN connections (1) Info

| | Name | VPN ID | State | Virtual private gateway | Transit gateway | Customer gateway |
|---|---|---|---|---|---|---|
| ○ | VPNC-1 | vpn-015874baeb7910847 | Available | vgw-0f7ec570d5c753c34 | – | cgw-06f9bdc5aa5cb0f63 |

Tunnel details will show the Tunnel state and the BGP Routes received.



VPC > VPN connections > vpn-015874baeb7910847

Virtual private network (VPN)
- Customer gateways
- Virtual private gateways
- Site-to-Site VPN connections
- Client VPN endpoints

AWS Verified Access
- Verified Access instances
- Verified Access trust providers
- Verified Access groups
- Verified Access endpoints

Transit gateways
- Transit gateways
- Transit gateway attachments
- Transit gateway policy tables
- Transit gateway route tables
- Transit gateway multicast

vpn-015874baeb7910847 / VPNC-1 Info

Download configuration | Actions ▼

Details

| | | | |
|---|---|---|---|
| VPN ID<br>vpn-015874baeb7910847 | State<br>✓ Available | Virtual private gateway<br>vgw-0f7ec570d5c753c34 | Customer gateway<br>cgw-06f9bdc5aa5cb0f63 |
| Transit gateway<br>– | Customer gateway address<br>182.18.140.177 | Type<br>ipsec.1 | Category<br>VPN |
| VPC<br>vpc-00811833eba324f0d | Routing<br>Dynamic | Acceleration enabled<br>False | Authentication<br>Pre-shared key |
| Local IPv4 network CIDR<br>0.0.0.0/0 | Remote IPv4 network CIDR<br>0.0.0.0/0 | Local IPv6 network CIDR<br>– | Remote IPv6 network CIDR<br>– |
| Core network ARN<br>– | Core network attachment ARN<br>– | Gateway association state<br>associated | Outside IP address type<br>PublicIpv4 |

Tunnel details | Tags

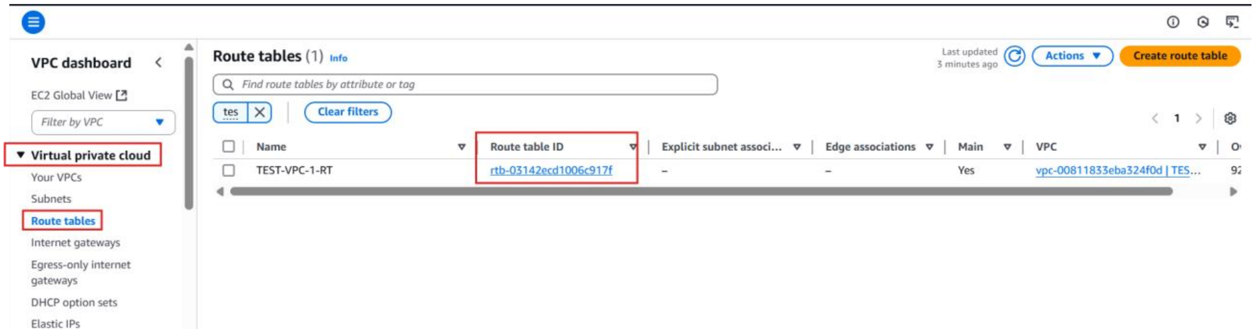
Tunnel state

| Tunnel number | Outside IP address | Inside IPv4 CIDR | Inside IPv6 CIDR | Status | Last status change | Details | Certificate ARN |
|---|---|---|---|---|---|---|---|
| Tunnel 1 | 13.126.252.24 | 169.254.84.200/30 | – | ✓ Up | May 8, 2025, 13:45:13 (UTC+05:30) | 5 BGP ROUTES | – |
| Tunnel 2 | 15.206.240.93 | 169.254.16.240/30 | – | ✓ Up | May 8, 2025, 13:45:33 (UTC+05:30) | 5 BGP ROUTES | – |

## BGP in AWS:

For BGP routes to get installed from Virtual Private GW to the Main route table we need to propagate the routes.

To Propagate the Routes, go to Virtual Private Cloud → Route tables and select the Main Route table of your VPC.



VPC dashboard

EC2 Global View

Filter by VPC ▼

Virtual private cloud
- Your VPCs
- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- DHCP option sets
- Elastic IPs

Route tables (1) Info

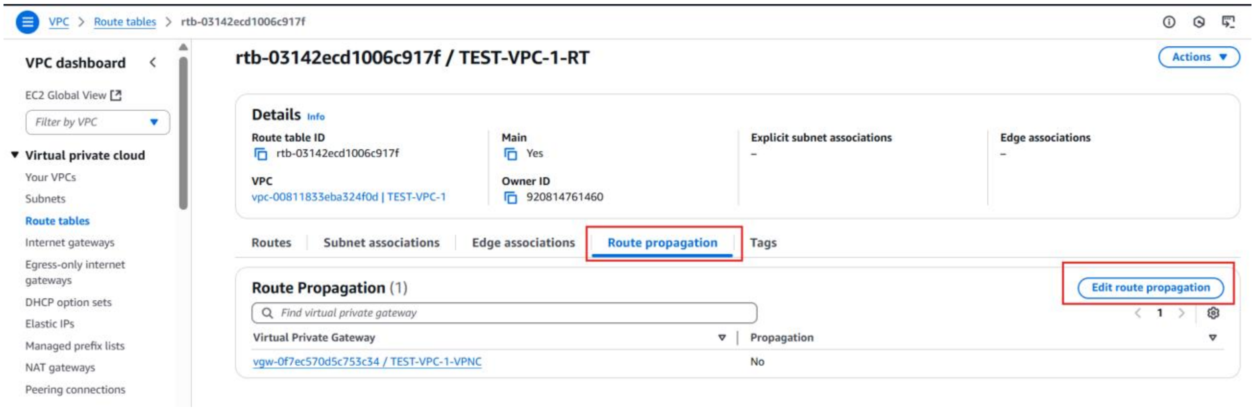
Last updated 3 minutes ago | Actions ▼ | Create route table

Find route tables by attribute or tag

tes ✕ | Clear filters

| □ | Name | Route table ID | Explicit subnet associ... | Edge associations | Main | VPC | O |
|---|---|---|---|---|---|---|---|
| □ | TEST-VPC-1-RT | rtb-03142ecd1006c917f | – | – | Yes | vpc-00811833eba324f0d \| TES... | 92 |

Once clicking on "Route Table ID", under Route Propagation click on "Edit route Propagation".



VPC > Route tables > rtb-03142ecd1006c917f

VPC dashboard

EC2 Global View

Filter by VPC ▼

Virtual private cloud
- Your VPCs
- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- NAT gateways
- Peering connections

rtb-03142ecd1006c917f / TEST-VPC-1-RT

Actions ▼

Details Info

| | | | |
|---|---|---|---|
| Route table ID<br>rtb-03142ecd1006c917f | Main<br>Yes | Explicit subnet associations<br>– | Edge associations<br>– |
| VPC<br>vpc-00811833eba324f0d \| TEST-VPC-1 | Owner ID<br>920814761460 | | |

Routes | Subnet associations | Edge associations | Route propagation | Tags

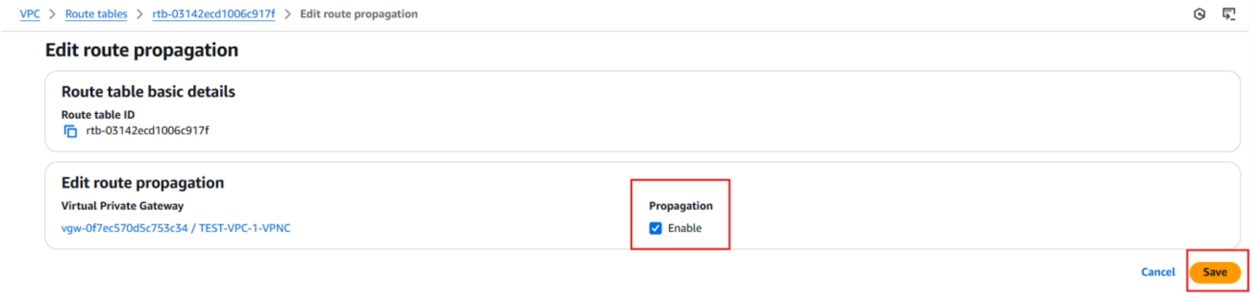
Route Propagation (1)

Edit route propagation

Find virtual private gateway

| Virtual Private Gateway | Propagation |
|---|---|
| vgw-0f7ec570d5c753c34 / TEST-VPC-1-VPNC | No |

Under "Edit route Propagation" enable the Propagation and save.



VPC > Route tables > rtb-03142ecd1006c917f > Edit route propagation

## Edit route propagation

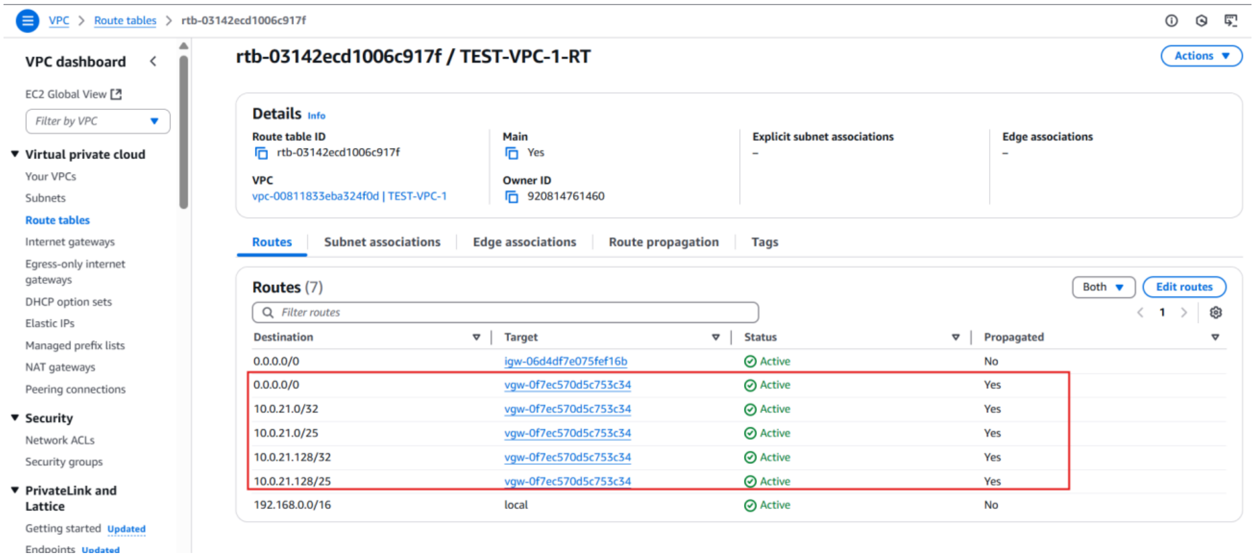
**Route table basic details**

Route table ID: rtb-03142ecd1006c917f

**Edit route propagation**

| Virtual Private Gateway | Propagation |
|---|---|
| vgw-0f7ec570d5c753c34 / TEST-VPC-1-VPNC | ☑ Enable |

Once done, you should be able to see the Propagated routes from VGW.



VPC > Route tables > rtb-03142ecd1006c917f

**rtb-03142ecd1006c917f / TEST-VPC-1-RT**

**Details** Info

Route table ID: rtb-03142ecd1006c917f

Main: Yes

Explicit subnet associations: –

Edge associations: –

VPC: vpc-00811833eba324f0d | TEST-VPC-1

Owner ID: 920814761460

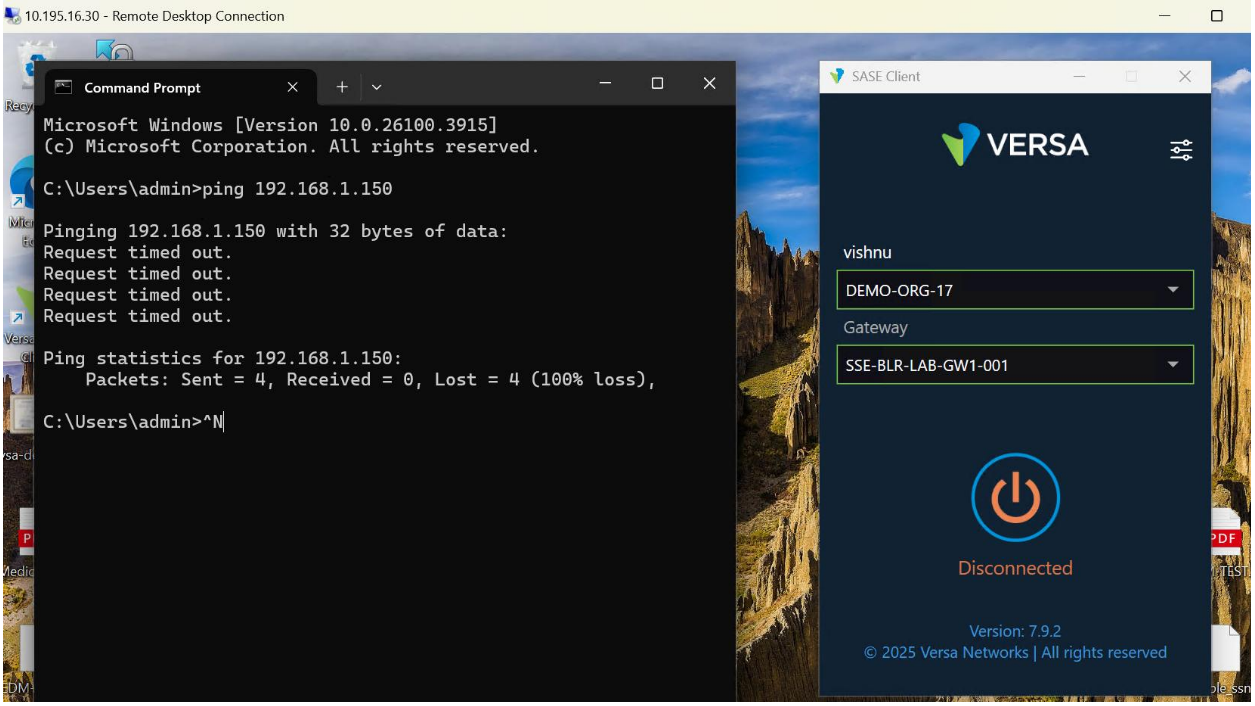
**Routes** (7)

| Destination | Target | Status | Propagated |
|---|---|---|---|
| 0.0.0.0/0 | igw-06d4df7e075fef16b | ✓ Active | No |
| 0.0.0.0/0 | vgw-0f7ec570d5c753c34 | ✓ Active | Yes |
| 10.0.21.0/32 | vgw-0f7ec570d5c753c34 | ✓ Active | Yes |
| 10.0.21.0/25 | vgw-0f7ec570d5c753c34 | ✓ Active | Yes |
| 10.0.21.128/32 | vgw-0f7ec570d5c753c34 | ✓ Active | Yes |
| 10.0.21.128/25 | vgw-0f7ec570d5c753c34 | ✓ Active | Yes |
| 192.168.0.0/16 | local | ✓ Active | No |

## Verifying Connectivity:

Accessing EC2 instance with IP: 192.168.1.150 from PC connected to SASE Client.

When the SASE Client is not connected to the Gateway we were unable to reach the EC2 instance in AWS over Private IP.



```
Microsoft Windows [Version 10.0.26100.3915]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>ping 192.168.1.150

Pinging 192.168.1.150 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.150:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\admin>^N
```

vishnu

DEMO-ORG-17

Gateway

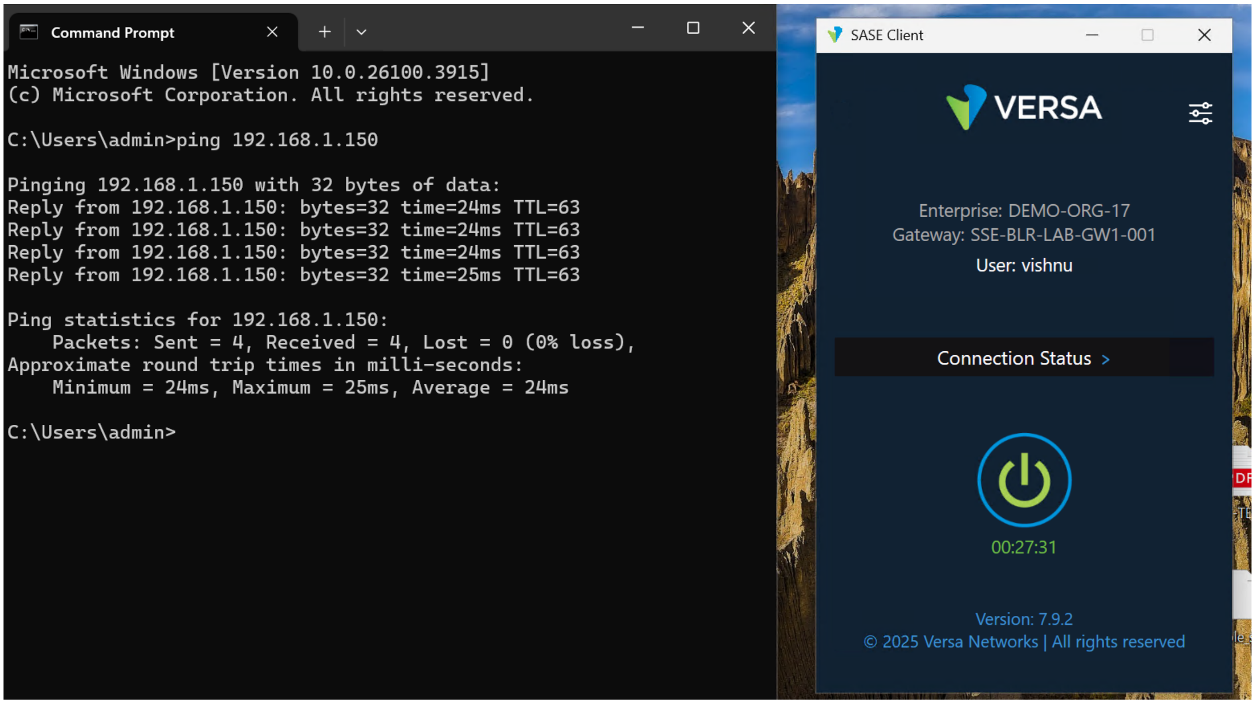
SSE-BLR-LAB-GW1-001

Disconnected

Version: 7.9.2

© 2025 Versa Networks | All rights reserved

When the SASE Client is connected to the Gateway we were able to reach the EC2 instance in AWS over Private IP.



```
Microsoft Windows [Version 10.0.26100.3915]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>ping 192.168.1.150

Pinging 192.168.1.150 with 32 bytes of data:
Reply from 192.168.1.150: bytes=32 time=24ms TTL=63
Reply from 192.168.1.150: bytes=32 time=24ms TTL=63
Reply from 192.168.1.150: bytes=32 time=24ms TTL=63
Reply from 192.168.1.150: bytes=32 time=25ms TTL=63

Ping statistics for 192.168.1.150:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 25ms, Average = 24ms

C:\Users\admin>
```

Enterprise: DEMO-ORG-17
Gateway: SSE-BLR-LAB-GW1-001
User: vishnu

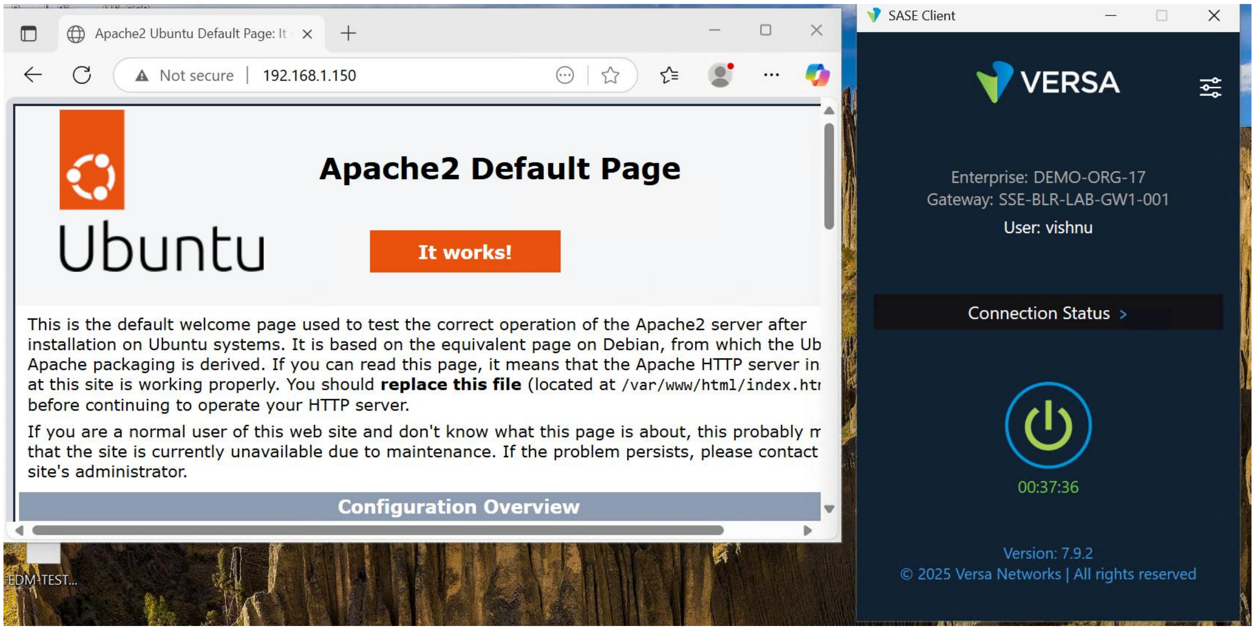
Connection Status >

00:27:31

Version: 7.9.2

© 2025 Versa Networks | All rights reserved

If the EC2 instance is a webserver then you should be able to access the webpage over Private IP.



Apache2 Default Page

Ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ub Apache packaging is derived. If you can read this page, it means that the Apache HTTP server in at this site is working properly. You should **replace this file** (located at `/var/www/html/index.htr` before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably m that the site is currently unavailable due to maintenance. If the problem persists, please contact site's administrator.

Configuration Overview

Enterprise: DEMO-ORG-17
Gateway: SSE-BLR-LAB-GW1-001
User: vishnu

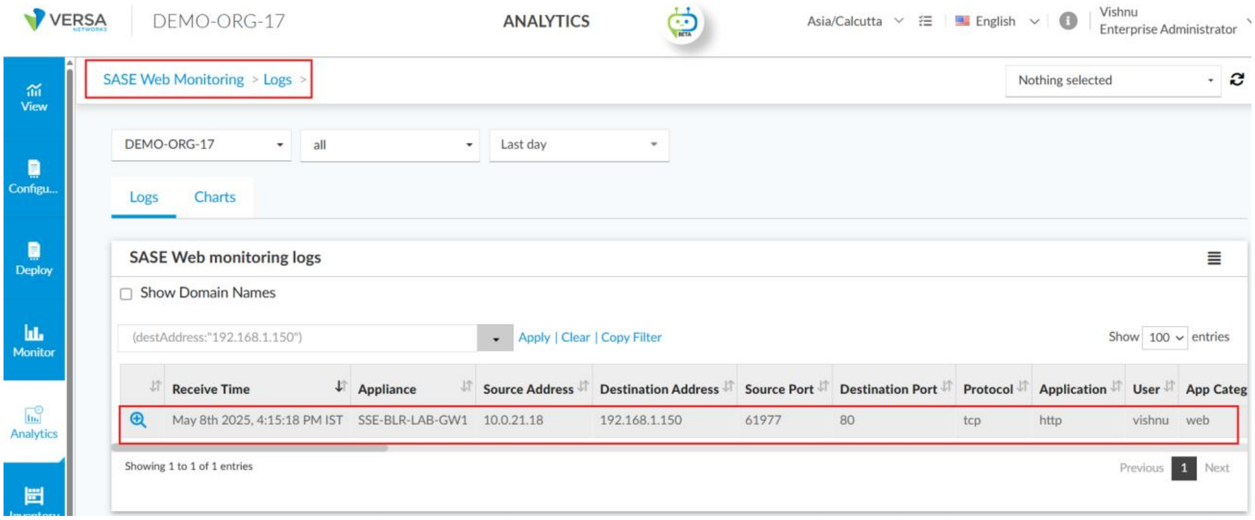
Connection Status >

00:37:36

Version: 7.9.2
© 2025 Versa Networks | All rights reserved

**SASE-WEB LOGS on Analytics:**

Go to Analytics →Logs → SASE Web Monitoring, select the respective Organization and the SASE Gateway.



DEMO-ORG-17 | all | Last day

SASE Web monitoring logs

□ Show Domain Names

(destAddress:"192.168.1.150")

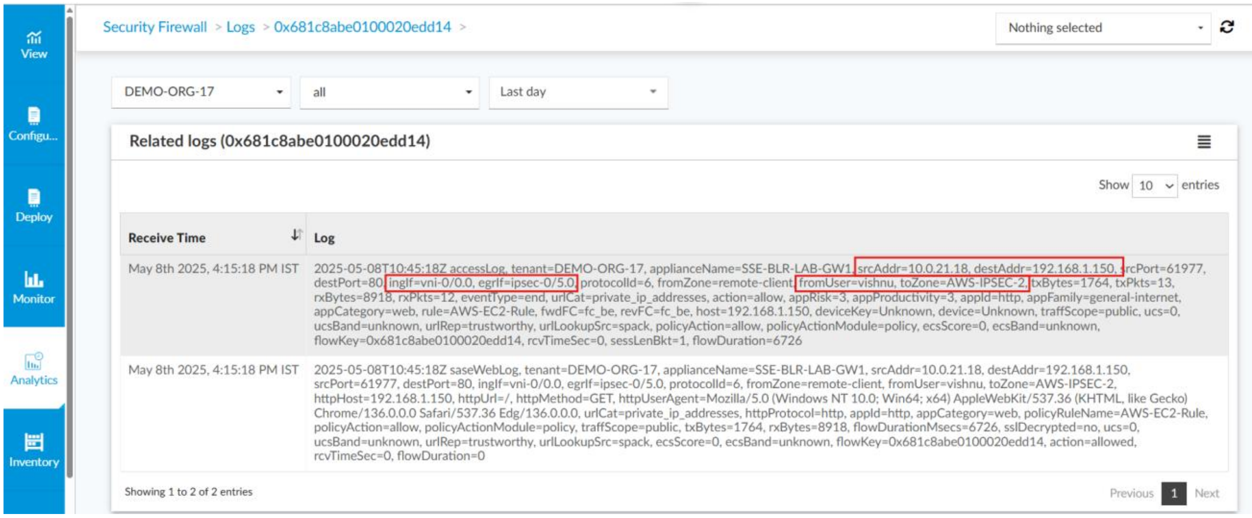
Show 100 entries

| | Receive Time | Appliance | Source Address | Destination Address | Source Port | Destination Port | Protocol | Application | User | App Categ |
|---|---|---|---|---|---|---|---|---|---|---|
| | May 8th 2025, 4:15:18 PM IST | SSE-BLR-LAB-GW1 | 10.0.21.18 | 192.168.1.150 | 61977 | 80 | tcp | http | vishnu | web |

Showing 1 to 1 of 1 entries

Firewall Logs on Concerto (If enabled):

Go to Analytics → Logs → Firewall and select the respective Organization and the SASE Gateway.



Related logs (0x681c8abe0100020edd14)

Show 10 entries

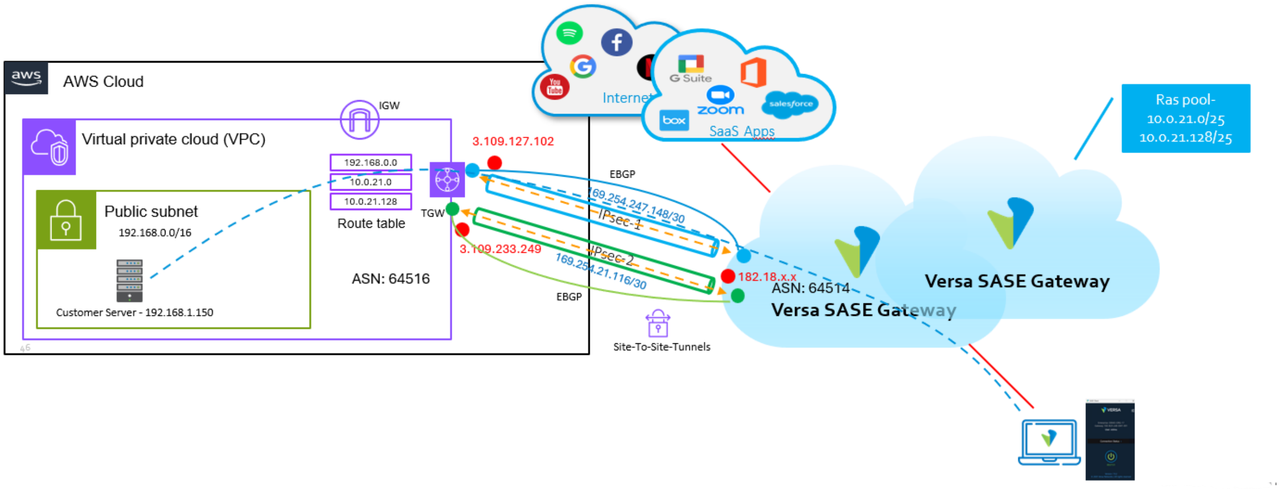
| Receive Time | Log |
|---|---|
| May 8th 2025, 4:15:18 PM IST | 2025-05-08T10:45:18Z accessLog, tenant=DEMO-ORG-17, applianceName=SSE-BLR-LAB-GW1, srcAddr=10.0.21.18, destAddr=192.168.1.150, srcPort=61977, destPort=80, inglf=vni-0/0.0, egrlf=ipsec-0/5.0, protocolId=6, fromZone=remote-client, fromUser=vishnu, toZone=AWS-IPSEC-2, txBytes=1764, txPkts=13, rxBytes=8918, rxPkts=12, eventType=end, urlCat=private_ip_addresses, action=allow, appRisk=3, appProductivity=3, appId=http, appFamily=general-internet, appCategory=web, rule=AWS-EC2-Rule, fwdFC=fc_be, revFC=fc_be, host=192.168.1.150, deviceKey=Unknown, device=Unknown, traffScope=public, ucs=0, ucsBand=unknown, urlRep=trustworthy, urlLookupSrc=spack, policyAction=allow, policyActionModule=policy, ecsScore=0, ecsBand=unknown, flowKey=0x681c8abe0100020edd14, rcvTimeSec=0, sessLenBkt=1, flowDuration=6726 |
| May 8th 2025, 4:15:18 PM IST | 2025-05-08T10:45:18Z saseWebLog, tenant=DEMO-ORG-17, applianceName=SSE-BLR-LAB-GW1, srcAddr=10.0.21.18, destAddr=192.168.1.150, srcPort=61977, destPort=80, inglf=vni-0/0.0, egrlf=ipsec-0/5.0, protocolId=6, fromZone=remote-client, fromUser=vishnu, toZone=AWS-IPSEC-2, httpHost=192.168.1.150, httpUrl=/, httpMethod=GET, httpUserAgent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36 Edg/136.0.0.0, urlCat=private_ip_addresses, httpProtocol=http, appId=http, appCategory=web, policyRuleName=AWS-EC2-Rule, policyAction=allow, policyActionModule=policy, traffScope=public, txBytes=1764, rxBytes=8918, flowDurationMsecs=6726, sslDecrypted=no, ucs=0, ucsBand=unknown, urlRep=trustworthy, urlLookupSrc=spack, ecsScore=0, ecsBand=unknown, flowKey=0x681c8abe0100020edd14, action=allowed, rcvTimeSec=0, flowDuration=0 |

Showing 1 to 2 of 2 entries

## Option 2 - TGW:

In this scenario, site-to-site IPsec VPN is established between the SASE Gateway and the AWS Transit Gateway (TGW). The VPC is attached to the TGW, and dynamic route exchange is performed over the IPsec connection using eBGP between TGW and SASW GW.

This Option is used when you need to connect SASE GW to multiple VPCs or regions with centralized routing and scalable architecture.

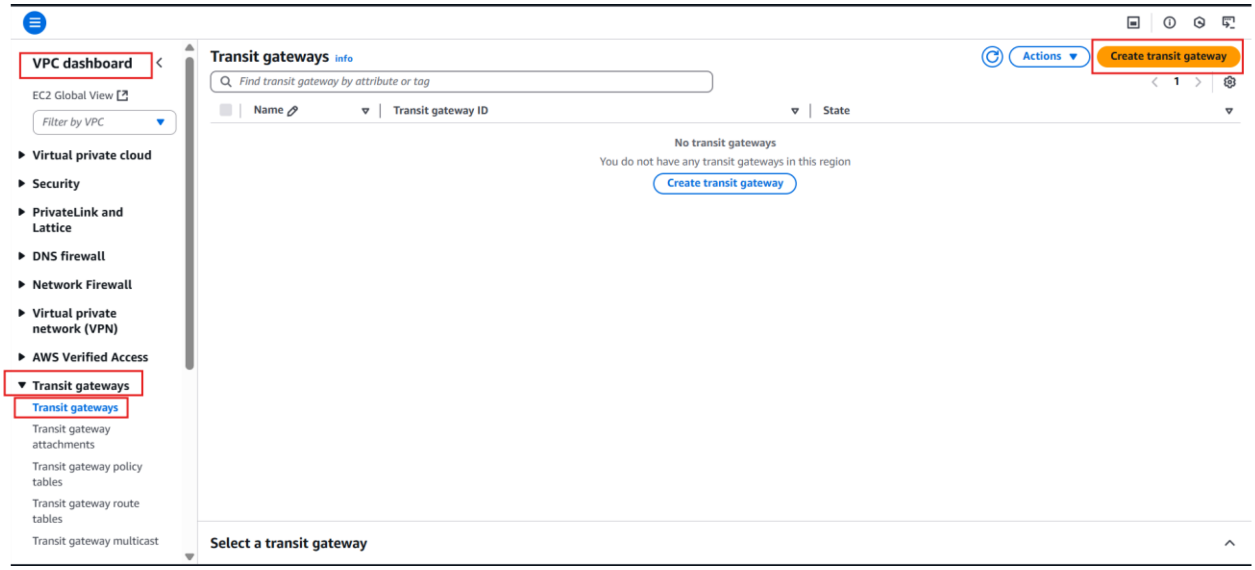


**Note**: Refer Section 4 to 7 for creating VPC, Subnets, IGW and EC2 Instance.

### AWS Configuration:

#### Creating AWS Transit Gateway:

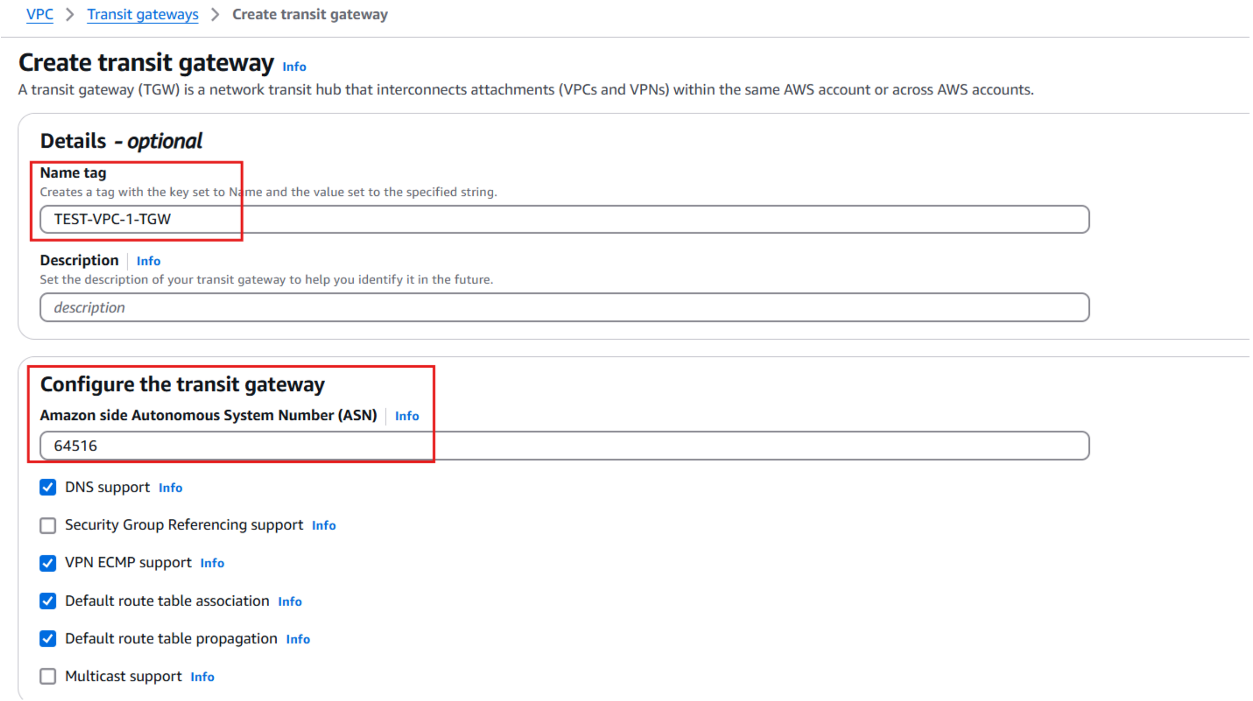
Under “VPC dashboard” go to “Transit gateways” → Transit gateways and click on “Create transit gateway”.



No transit gateways

You do not have any transit gateways in this region

Under Details,  provide “Name tag”, “ASN” for Transit gateway and then click on “Create Transit Gateway”



Create transit gateway Info

A transit gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same AWS account or across AWS accounts.

Details - *optional*

Name tag

Creates a tag with the key set to Name and the value set to the specified string.

TEST-VPC-1-TGW

Description Info

Set the description of your transit gateway to help you identify it in the future.

description

Configure the transit gateway

Amazon side Autonomous System Number (ASN) Info

64516

☑ DNS support Info

□ Security Group Referencing support Info

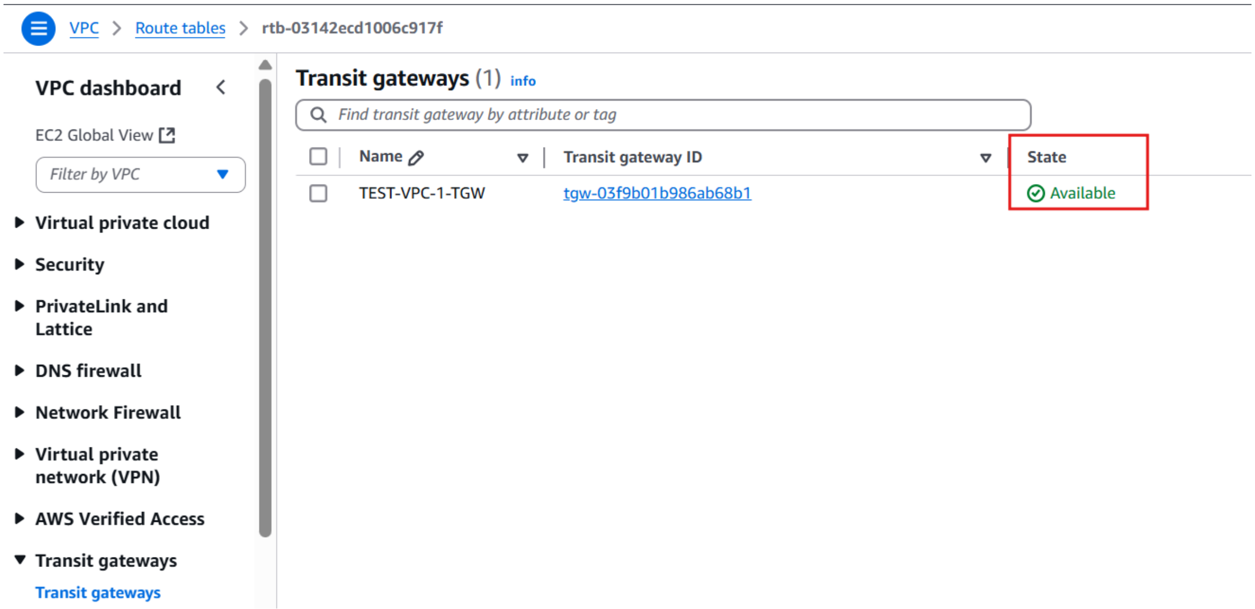
☑ VPN ECMP support Info

☑ Default route table association Info

☑ Default route table propagation Info

□ Multicast support Info

Once created it will show the state as Available.



VPC > Route tables > rtb-03142ecd1006c917f

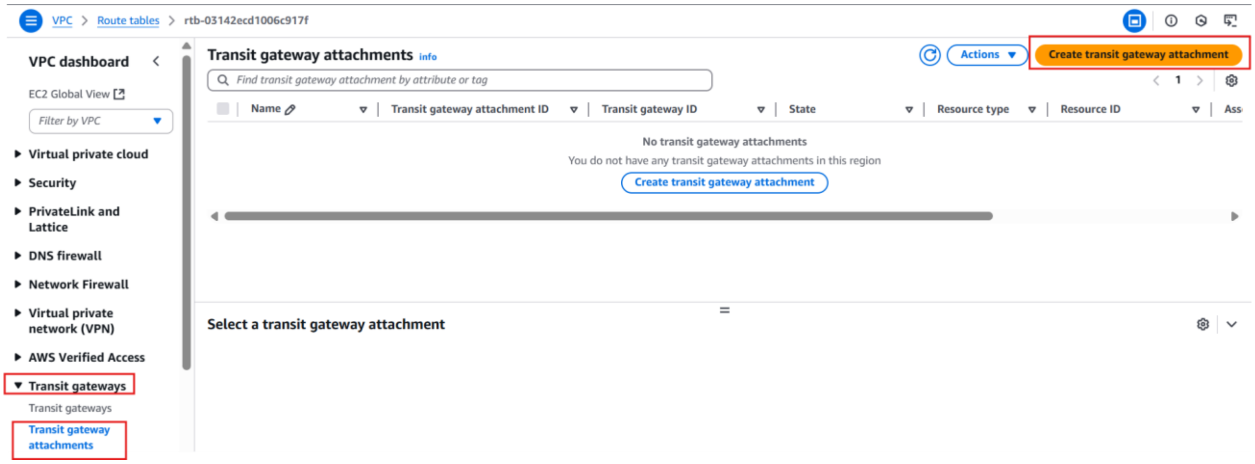
Transit gateways (1) info

Find transit gateway by attribute or tag

| □ | Name | Transit gateway ID | State |
|---|---|---|---|
| □ | TEST-VPC-1-TGW | tgw-03f9b01b986ab68b1 | Available |

## Creating TGW attachment:

Under VPC dashboard, go to “Transit gateway” → “Transit gateway attachments” and click on “Create transit gateway attachment”.



VPC > Route tables > rtb-03142ecd1006c917f

Transit gateway attachments info

Find transit gateway attachment by attribute or tag

| □ | Name | Transit gateway attachment ID | Transit gateway ID | State | Resource type | Resource ID | Ass |
|---|---|---|---|---|---|---|---|

No transit gateway attachments

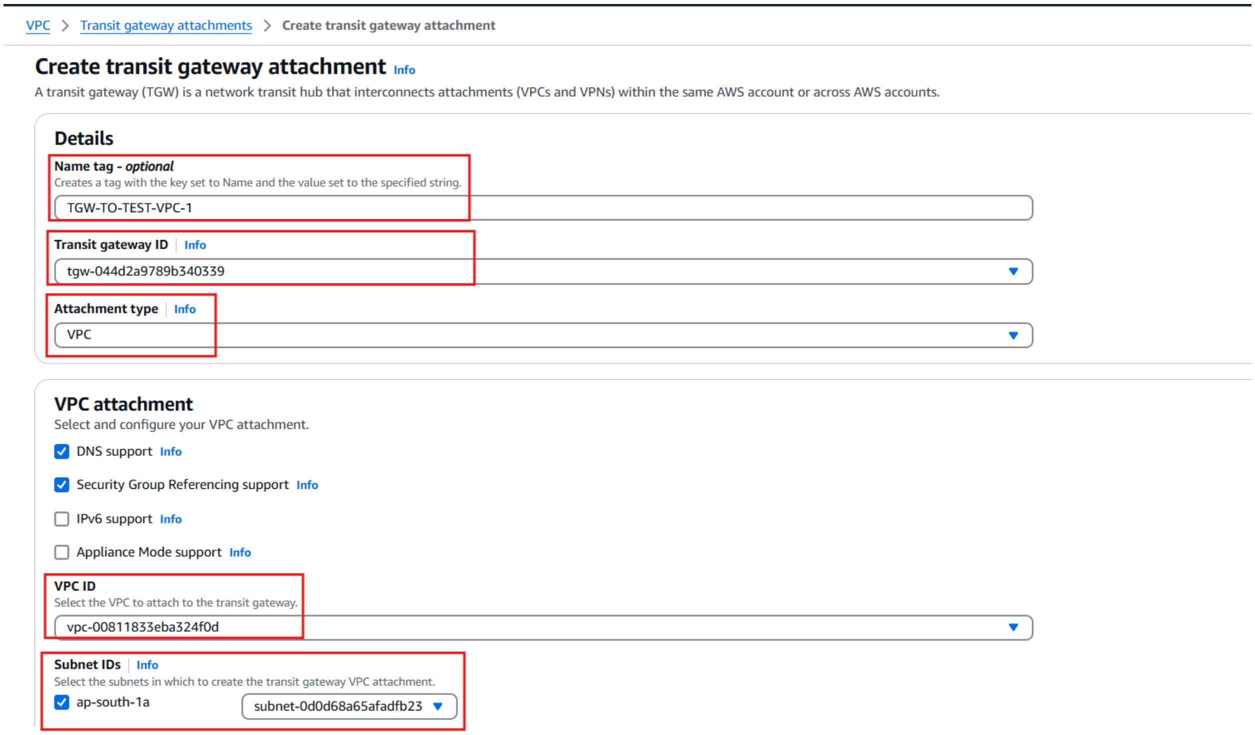
You do not have any transit gateway attachments in this region

Select a transit gateway attachment

Under Name-tag provide a name to the TGW Attachment, from Transit gateway ID dropdown select the TGW which we created. Under “Attachment type” select the attachment type as VPC.

Under the VPC Attachment select the VPC which you want to attach to the TGW (TEST-VPC-1) and select the subnet.

Click on “Create transit gateway attachment” to Create an attachment between TGW and the AWS VPC.



VPC > Transit gateway attachments > Create transit gateway attachment

## Create transit gateway attachment Info

A transit gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same AWS account or across AWS accounts.

**Details**

**Name tag - *optional***
Creates a tag with the key set to Name and the value set to the specified string.
TGW-TO-TEST-VPC-1

**Transit gateway ID** Info
tgw-044d2a9789b340339

**Attachment type** Info
VPC

**VPC attachment**
Select and configure your VPC attachment.

☑ DNS support Info

☑ Security Group Referencing support Info

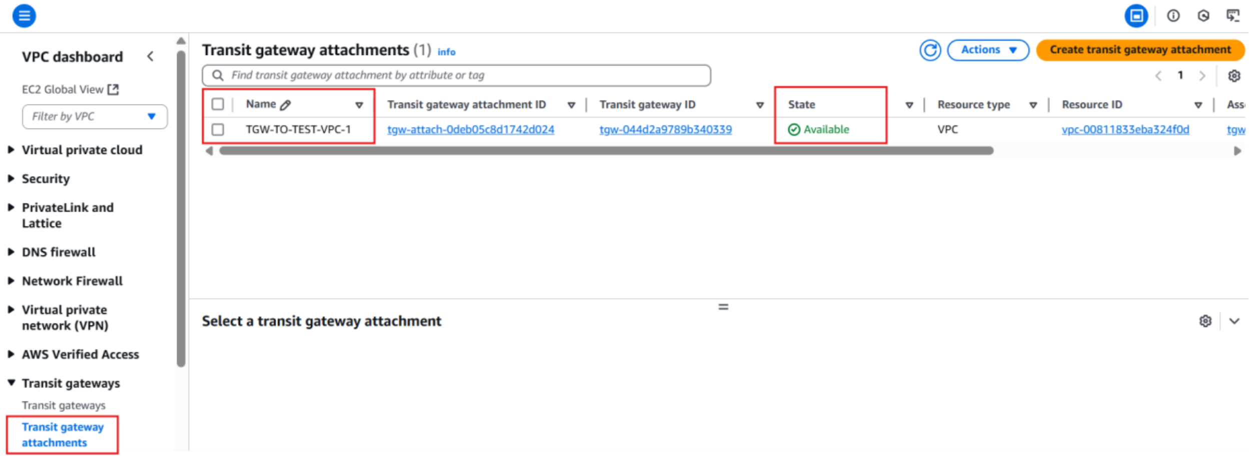
□ IPv6 support Info

□ Appliance Mode support Info

**VPC ID**
Select the VPC to attach to the transit gateway.
vpc-00811833eba324f0d

**Subnet IDs** Info
Select the subnets in which to create the transit gateway VPC attachment.
☑ ap-south-1a subnet-0d0d68a65afadfb23

Once created it will show the state as available.



**Transit gateway attachments** (1) info

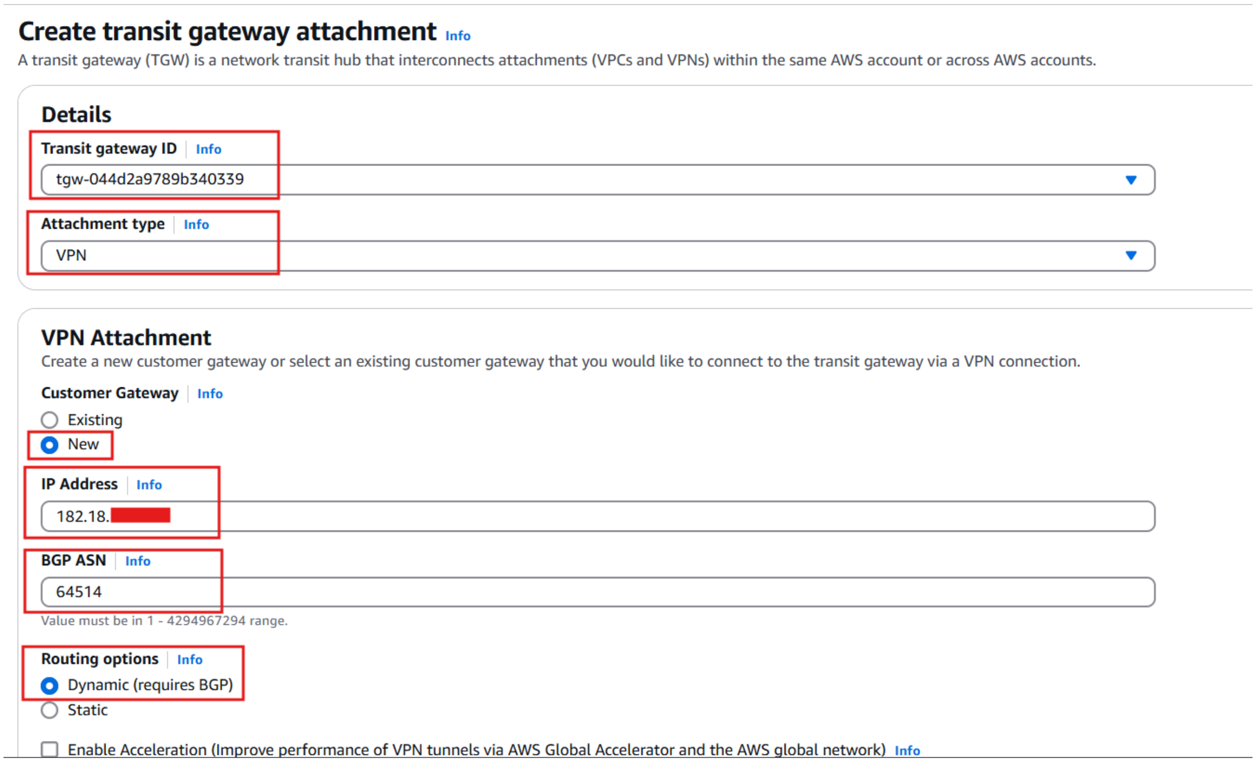
| □ | Name | Transit gateway attachment ID | Transit gateway ID | State | Resource type | Resource ID | Ass |
|---|---|---|---|---|---|---|---|
| □ | TGW-TO-TEST-VPC-1 | tgw-attach-0deb05c8d1742d024 | tgw-044d2a9789b340339 | ✓ Available | VPC | vpc-00811833eba324f0d | tgw |

Create another attachment that connects TGW to the on prem SASE GW through IPSec.

Under VPC dashboard, go to “Transit gateway” → “Transit gateway attachments” and click on “Create transit gateway attachment”.

Under “Details” provide the TGW ID which we created. Under “Attachment type” select the attachment type as VPN.

Under “Customer gateway” click on “New” and provide the “IP address” of the SASE-GW to which IPsec tunnels are to be formed and under BGP ASN provide the AS number of the SASE-GW.



Create transit gateway attachment Info

A transit gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same AWS account or across AWS accounts.

Details

Transit gateway ID | Info

tgw-044d2a9789b340339

Attachment type | Info

VPN

VPN Attachment

Create a new customer gateway or select an existing customer gateway that you would like to connect to the transit gateway via a VPN connection.

Customer Gateway | Info

○ Existing
● New

IP Address | Info

182.18.[redacted]

BGP ASN | Info

64514

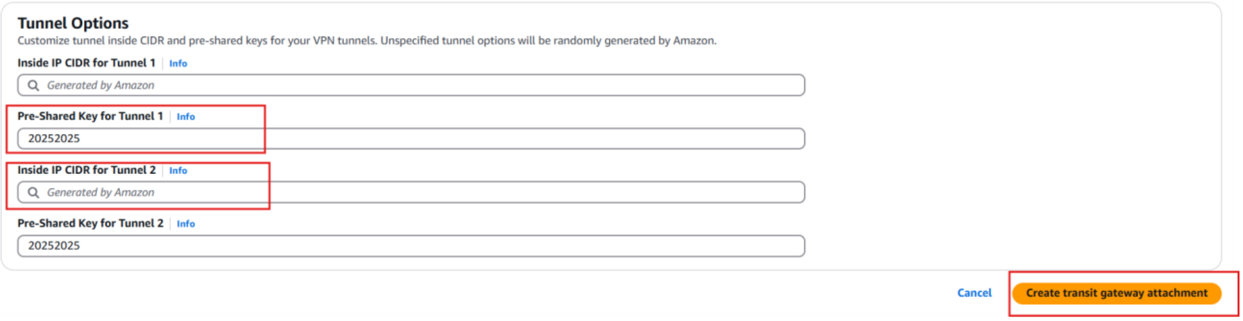
Value must be in 1 - 4294967294 range.

Routing options | Info

● Dynamic (requires BGP)
○ Static

□ Enable Acceleration (Improve performance of VPN tunnels via AWS Global Accelerator and the AWS global network) Info

Under Tunnel options provide the PSK for IPsec tunnels. (if not provided AWS will generate a random key).



Tunnel Options

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

Inside IP CIDR for Tunnel 1 | Info

Generated by Amazon

Pre-Shared Key for Tunnel 1 | Info

20252025

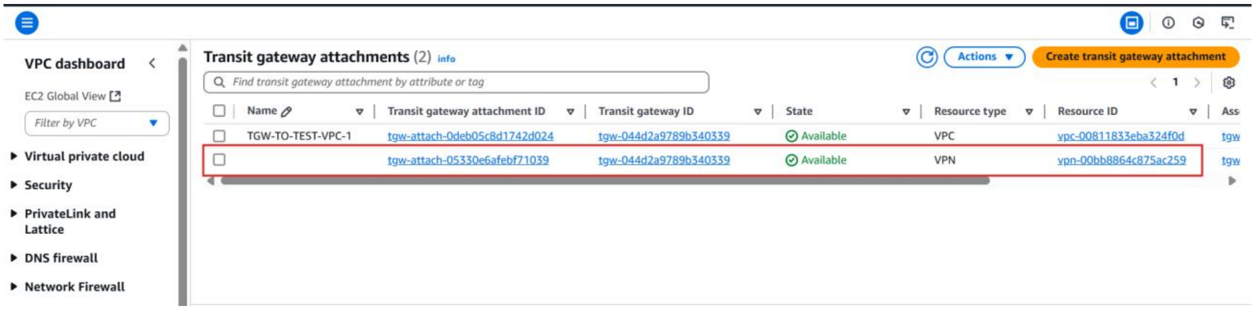
Inside IP CIDR for Tunnel 2 | Info

Generated by Amazon

Pre-Shared Key for Tunnel 2 | Info

20252025

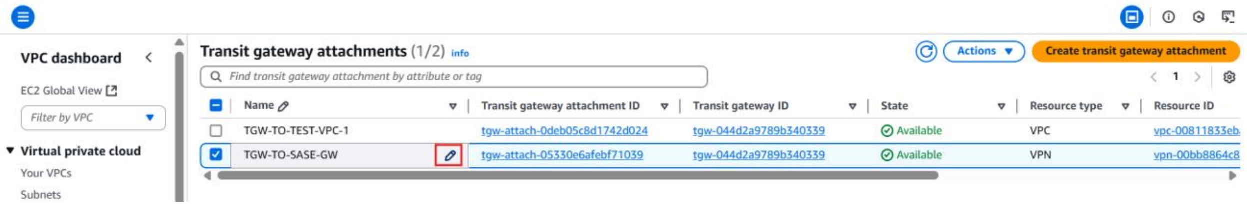
Once created it will show the state as Available.



Transit gateway attachments (2) Info

| | Name | Transit gateway attachment ID | Transit gateway ID | State | Resource type | Resource ID | Ass |
|---|---|---|---|---|---|---|---|
| □ | TGW-TO-TEST-VPC-1 | tgw-attach-0deb05c8d1742d024 | tgw-044d2a9789b340339 | Available | VPC | vpc-00811833eba324f0d | tgw |
| □ | | tgw-attach-05330e6afebf71039 | tgw-044d2a9789b340339 | Available | VPN | vpn-00bb8864c875ac259 | tgw |

Provide a name to the Transit gateway attachment by clicking on Edit icon.

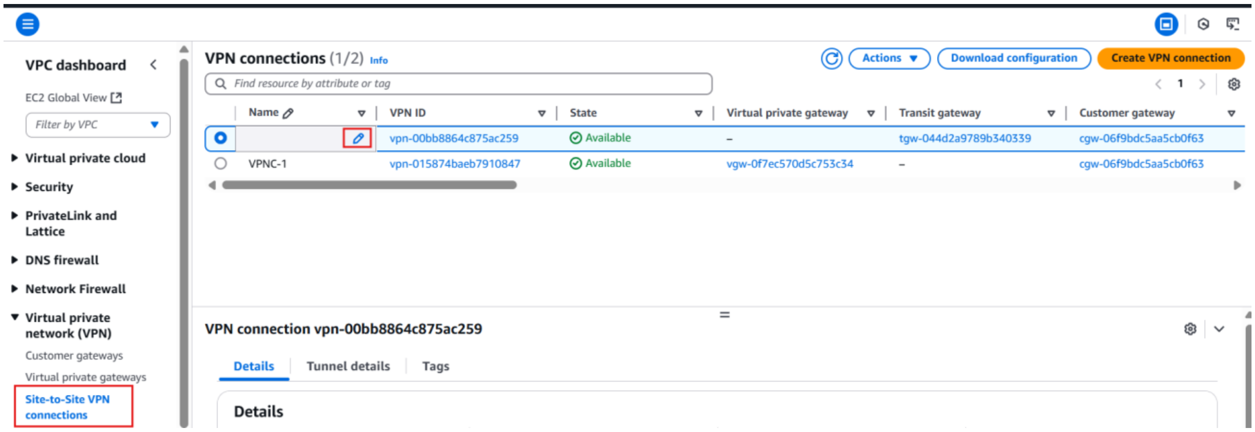


Transit gateway attachments (1/2) Info

| | Name | Transit gateway attachment ID | Transit gateway ID | State | Resource type | Resource ID |
|---|---|---|---|---|---|---|
| □ | TGW-TO-TEST-VPC-1 | tgw-attach-0deb05c8d1742d024 | tgw-044d2a9789b340339 | Available | VPC | vpc-00811833eb |
| ☑ | TGW-TO-SASE-GW | tgw-attach-05330e6afebf71039 | tgw-044d2a9789b340339 | Available | VPN | vpn-00bb8864c8 |

Creating a TGW attachment with type VPN will automatically create two Site-to-Site VPN Connections under VPC-Dashboard → VPN → Site-to-Site VPN Connections.

Under VPC Dashboard, go to Virtual Private Network → click on Site-to-Site VPN Connections and provide a name to it.

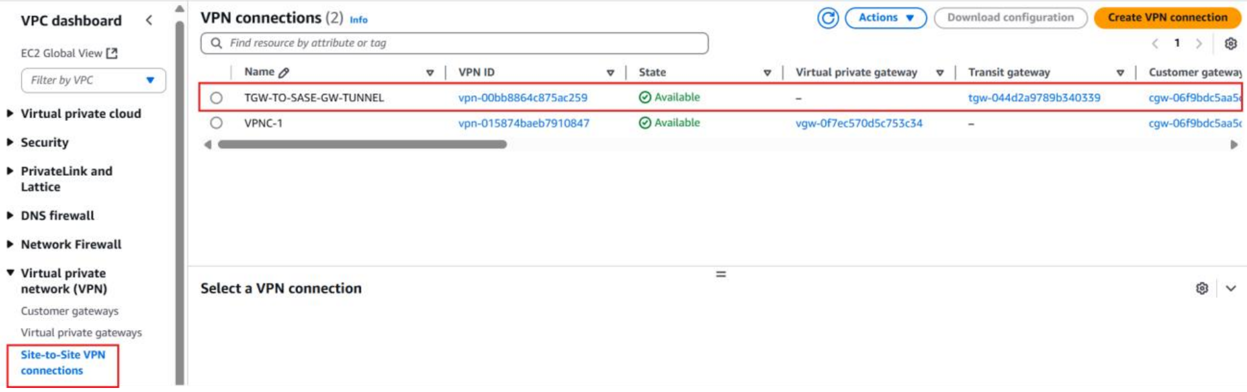


VPN connections (1/2) Info

| | Name | VPN ID | State | Virtual private gateway | Transit gateway | Customer gateway |
|---|---|---|---|---|---|---|
| ● | | vpn-00bb8864c875ac259 | Available | – | tgw-044d2a9789b340339 | cgw-06f9bdc5aa5cb0f63 |
| ○ | VPNC-1 | vpn-015874baeb7910847 | Available | vgw-0f7ec570d5c753c34 | – | cgw-06f9bdc5aa5cb0f63 |

VPN connection vpn-00bb8864c875ac259

Details

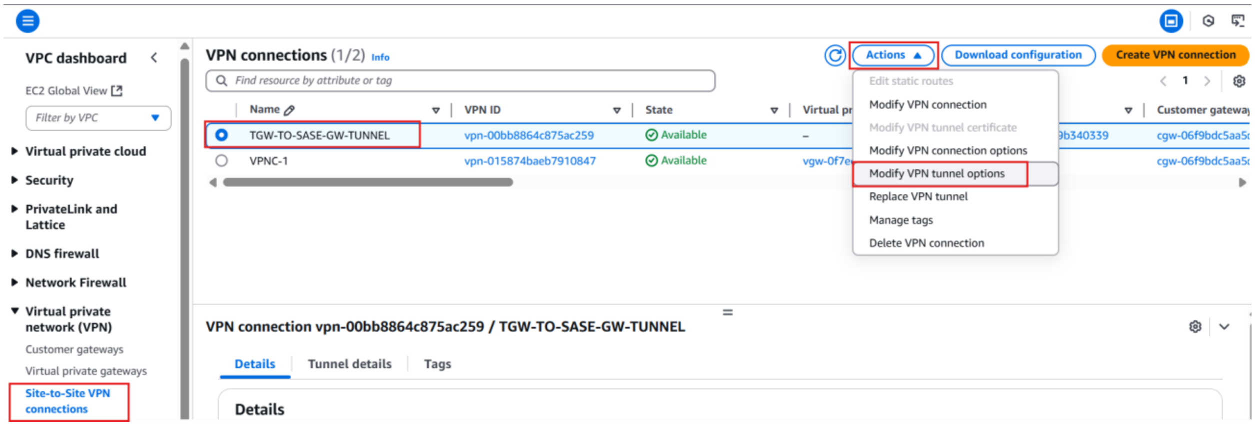


VPN connections (2) Info

| | Name | VPN ID | State | Virtual private gateway | Transit gateway | Customer gateway |
|---|---|---|---|---|---|---|
| ○ | TGW-TO-SASE-GW-TUNNEL | vpn-00bb8864c875ac259 | Available | – | tgw-044d2a9789b340339 | cgw-06f9bdc5aa5 |
| ○ | VPNC-1 | vpn-015874baeb7910847 | Available | vgw-0f7ec570d5c753c34 | – | cgw-06f9bdc5aa5 |

Select a VPN connection

Site-To-Site tunnels configured on SASE GW though Concerto has a Minimum version from DH group-14 as a security best practice. So, we need to remove DH Group 2 and 5 from IPsec Tunnel configuration on AWS.



VPN connections (1/2) Info

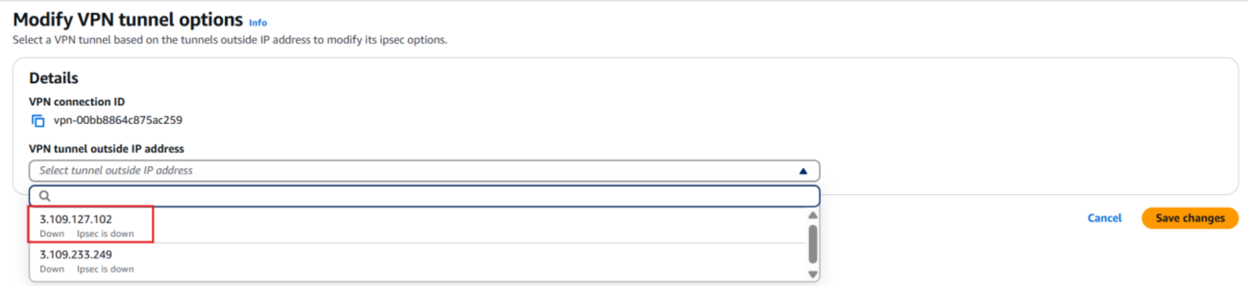
Find resource by attribute or tag

| | Name | VPN ID | State | Virtual pr | | Customer gatewa |
|---|---|---|---|---|---|---|
| ● | TGW-TO-SASE-GW-TUNNEL | vpn-00bb8864c875ac259 | Available | – | 9b340339 | cgw-06f9bdc5aa5 |
| ○ | VPNC-1 | vpn-015874baeb7910847 | Available | vgw-0f7e | | cgw-06f9bdc5aa5 |

VPN connection vpn-00bb8864c875ac259 / TGW-TO-SASE-GW-TUNNEL

Details

Under Modify VPN tunnel options select the first Outside IP.



Modify VPN tunnel options Info

Select a VPN tunnel based on the tunnels outside IP address to modify its ipsec options.

Details

VPN connection ID

vpn-00bb8864c875ac259

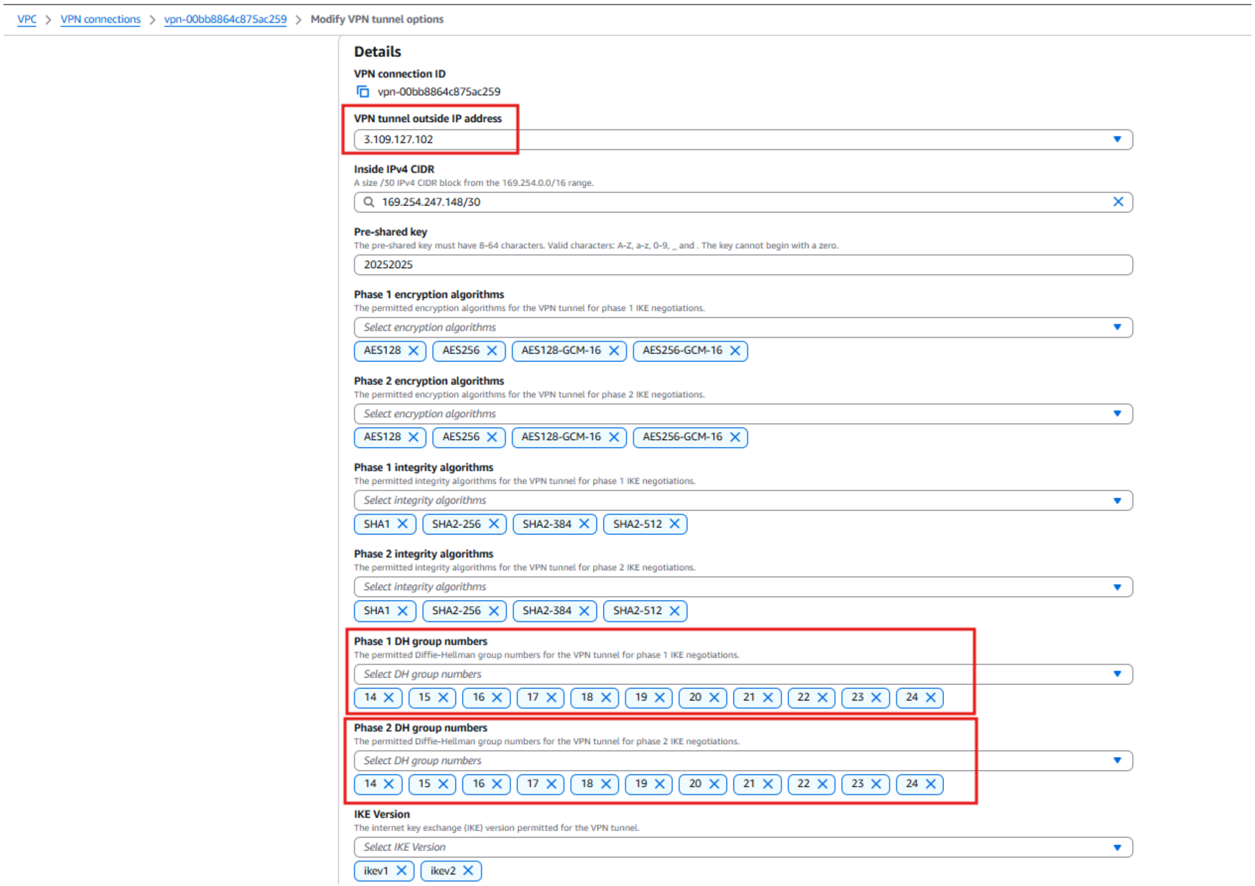
VPN tunnel outside IP address

Select tunnel outside IP address

3.109.127.102
Down Ipsec is down

3.109.233.249
Down Ipsec is down

Remove DH Group 2 and 5 from IPsec Tunnel configuration and click on “Save changes” and wait for the state to change from Modifying to Available.



VPC > VPN connections > vpn-00bb8864c875ac259 > Modify VPN tunnel options

**Details**

VPN connection ID
vpn-00bb8864c875ac259

VPN tunnel outside IP address
3.109.127.102

Inside IPv4 CIDR
A size /30 IPv4 CIDR block from the 169.254.0.0/16 range.
169.254.247.148/30

Pre-shared key
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.
20252025

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

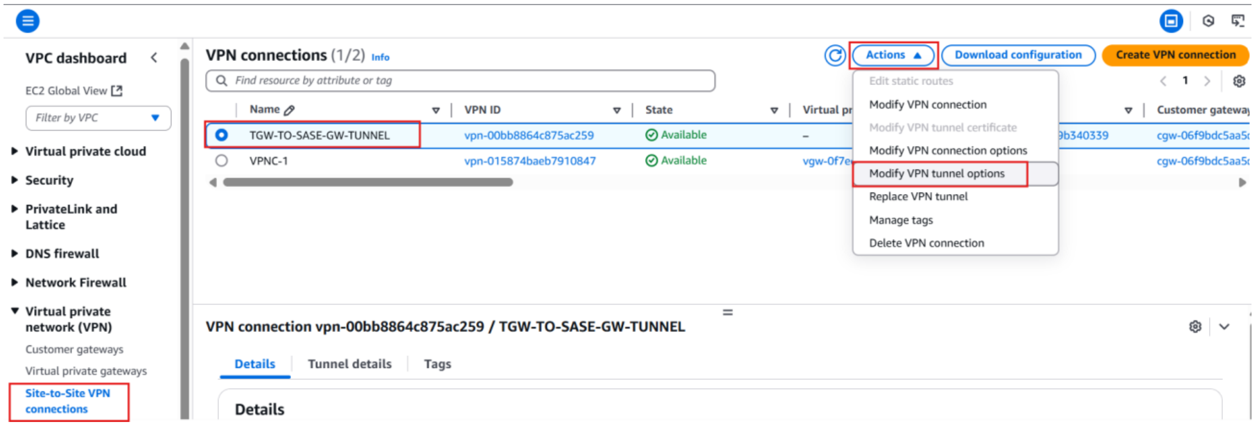
Phase 2 integrity algorithms
The permitted integrity algorithms for the VPN tunnel for phase 2 IKE negotiations.
Select integrity algorithms
SHA1, SHA2-256, SHA2-384, SHA2-512

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

Once complete repeat the same process for the second Outside IP.



VPN connections (1/2) Info

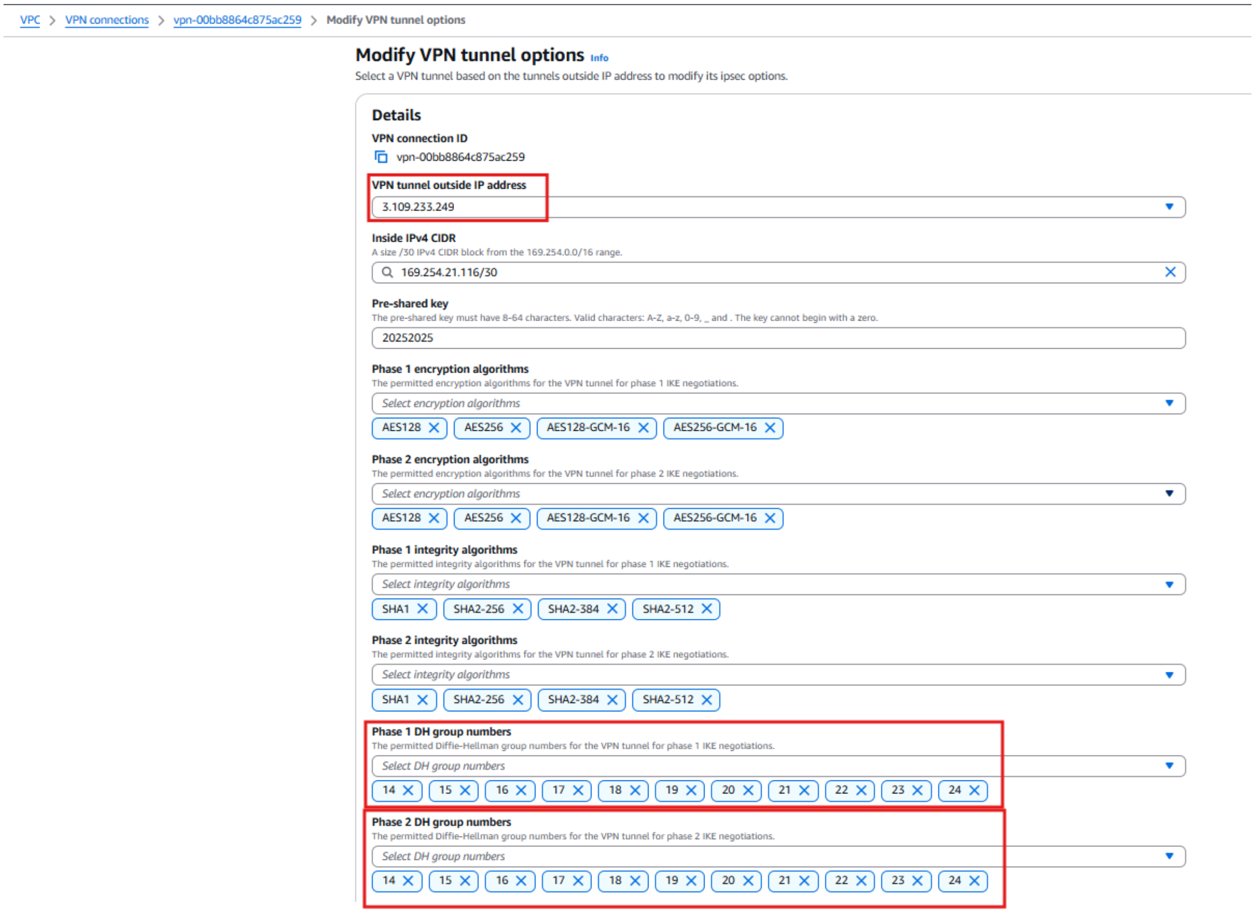
Find resource by attribute or tag

| | Name | VPN ID | State | Virtual pr | | Customer gateway |
|---|---|---|---|---|---|---|
| ● | TGW-TO-SASE-GW-TUNNEL | vpn-00bb8864c875ac259 | Available | – | 9b340339 | cgw-06f9bdc5aa5 |
| ○ | VPNC-1 | vpn-015874baeb7910847 | Available | vgw-0f7e | | cgw-06f9bdc5aa5 |

VPN connection vpn-00bb8864c875ac259 / TGW-TO-SASE-GW-TUNNEL

Details

After removing DH Group 2 and 5 from IPsec Tunnel configuration, click on “save changes” and wait for the state to change from Modifying to Available.



VPC > VPN connections > vpn-00bb8864c875ac259 > Modify VPN tunnel options

## Modify VPN tunnel options Info

Select a VPN tunnel based on the tunnels outside IP address to modify its ipsec options.

**Details**

**VPN connection ID**
vpn-00bb8864c875ac259

**VPN tunnel outside IP address**
3.109.233.249

**Inside IPv4 CIDR**
A size /30 IPv4 CIDR block from the 169.254.0.0/16 range.
169.254.21.116/30

**Pre-shared key**
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.
20252025

**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 ✕

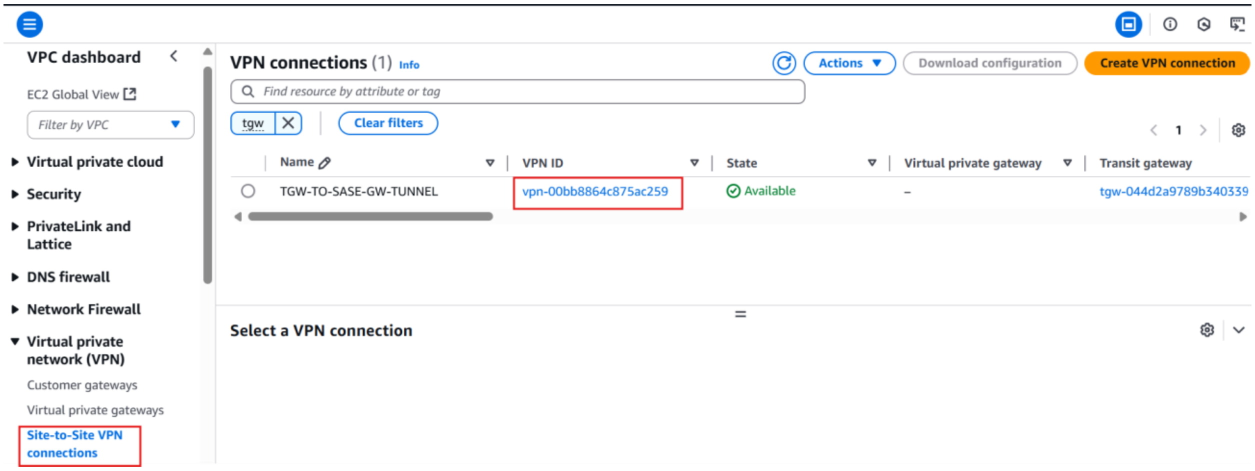
**Phase 1 integrity algorithms**
The permitted integrity algorithms for the VPN tunnel for phase 1 IKE negotiations.
Select integrity algorithms
SHA1 ✕ SHA2-256 ✕ SHA2-384 ✕ SHA2-512 ✕

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

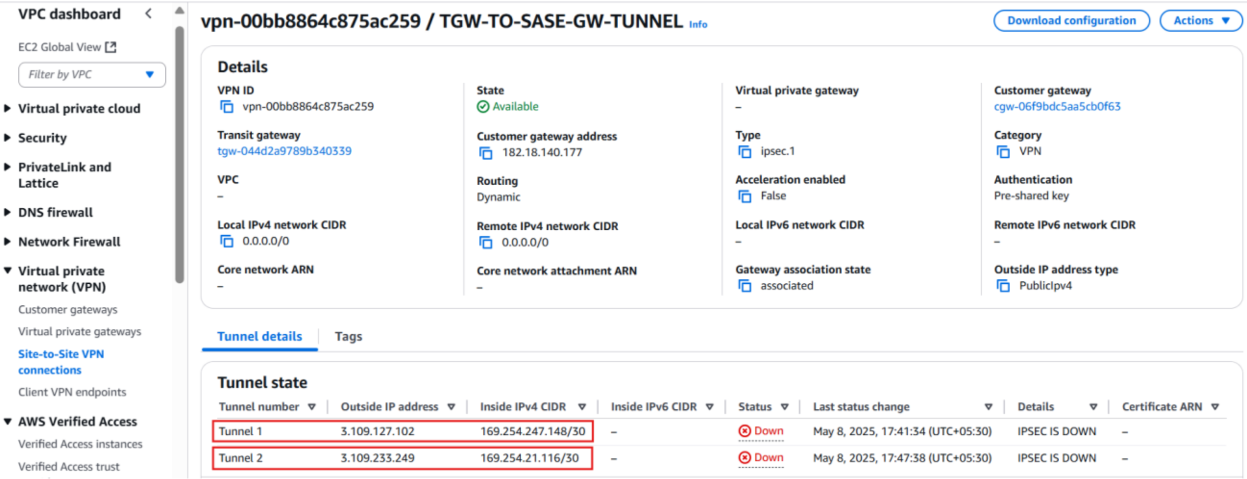
To Identify the tunnel parameters, under VPC dashboard → VPN → Site-to-Site VPN connections, click on the VPN ID of Site-to-Site VPN Connection.



**VPN connections** (1) Info

| Name | VPN ID | State | Virtual private gateway | Transit gateway |
|---|---|---|---|---|
| TGW-TO-SASE-GW-TUNNEL | vpn-00bb8864c875ac259 | Available | – | tgw-044d2a9789b340339 |

This will show the Tunnel information under “Tunnel details”.



vpn-00bb8864c875ac259 / TGW-TO-SASE-GW-TUNNEL

Details

VPN ID: vpn-00bb8864c875ac259
State: Available
Virtual private gateway: –
Customer gateway: cgw-06f9bdc5aa5cb0f63
Transit gateway: tgw-044d2a9789b340339
Customer gateway address: 182.18.140.177
Type: ipsec.1
Category: VPN
VPC: –
Routing: Dynamic
Acceleration enabled: False
Authentication: Pre-shared key
Local IPv4 network CIDR: 0.0.0.0/0
Remote IPv4 network CIDR: 0.0.0.0/0
Local IPv6 network CIDR: –
Remote IPv6 network CIDR: –
Core network ARN: –
Core network attachment ARN: –
Gateway association state: associated
Outside IP address type: PublicIpv4

Tunnel state

| Tunnel number | Outside IP address | Inside IPv4 CIDR | Inside IPv6 CIDR | Status | Last status change | Details | Certificate ARN |
|---|---|---|---|---|---|---|---|
| Tunnel 1 | 3.109.127.102 | 169.254.247.148/30 | – | Down | May 8, 2025, 17:41:34 (UTC+05:30) | IPSEC IS DOWN | – |
| Tunnel 2 | 3.109.233.249 | 169.254.21.116/30 | – | Down | May 8, 2025, 17:47:38 (UTC+05:30) | IPSEC IS DOWN | – |

From the above generated “Inside IPv4 CIDR” the first IP will be used by AWS and the other IP will be configured on VOS.

**Example:**

Tunnel 1:

Outside IP – 3.109.127.102

Inside IPv4 CIDR - 169.254.247.148/30

AWS Side: 169.254.247.149 /30

VOS Side: 169.254.247.150/30

Tunnel 2:

Outside IP - 3.109.233.249

Inside IPv4 CIDR – 169.254.21.116/30

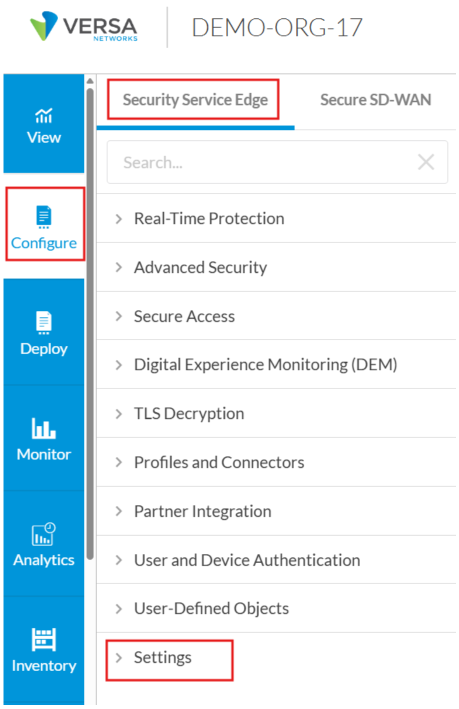
AWS Side: 169.254.21.117/30

VOS Side: 169.254.21.118/30

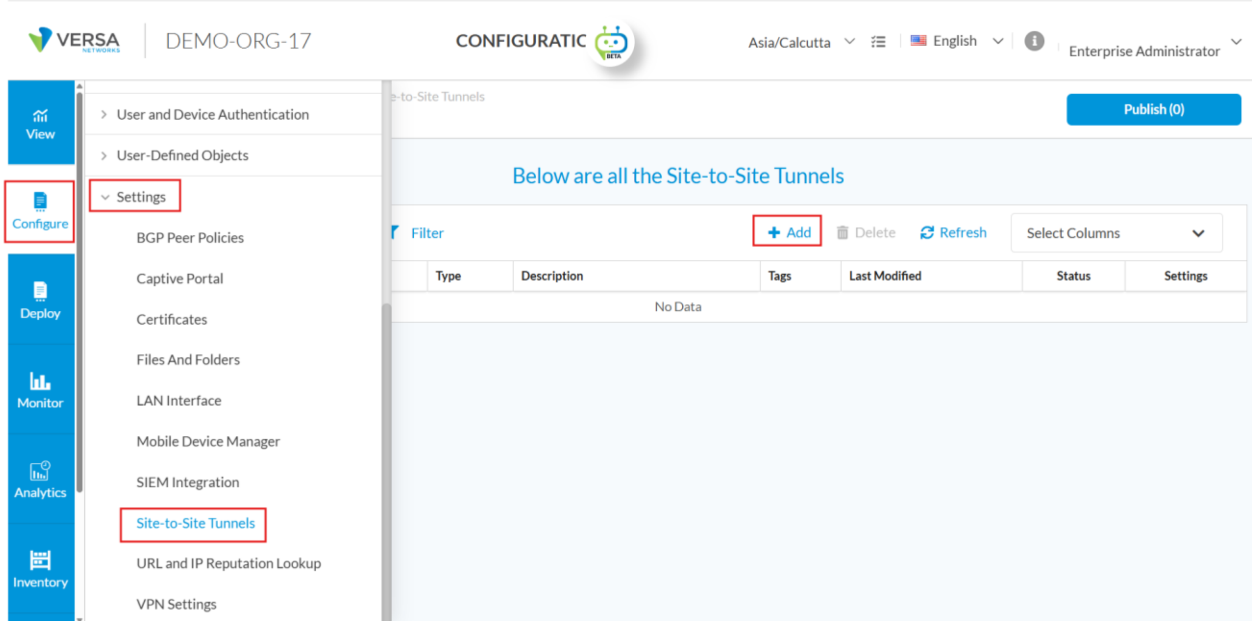
## SASE-GW Configuration:

### Configure Site to Site Tunnels:

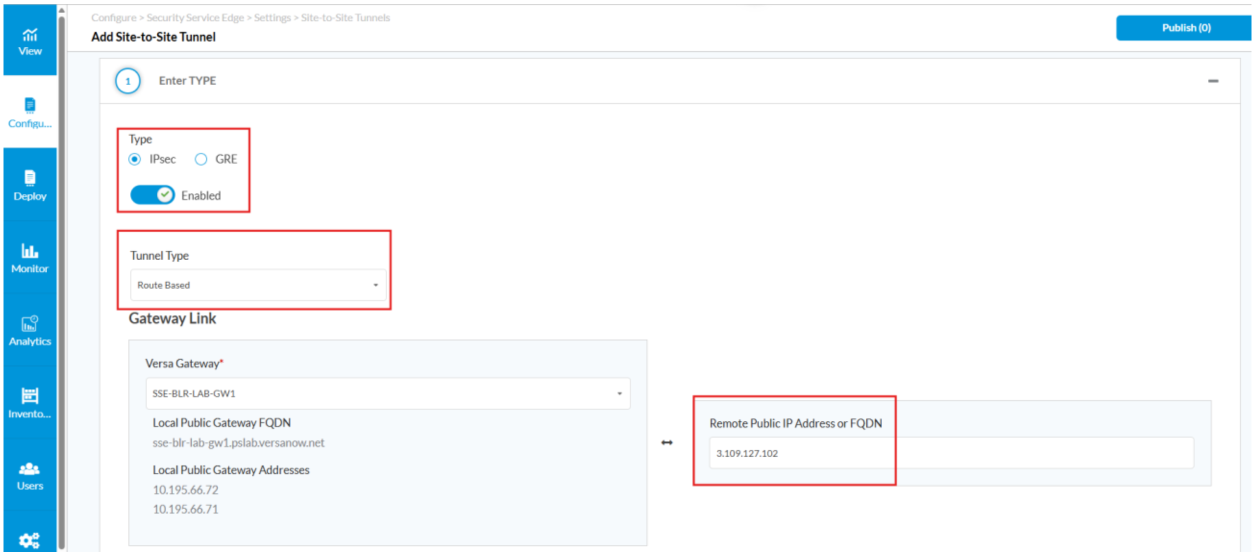
To Configure Site-to-Site Tunnels, Go to Configure →Secure Service Edge → Settings.



Under “Settings” go to “Site-to-Site Tunnels” and click on “Add”.



Under “Enter TYPE”, provide the Type as IPSec, “Tunnel Type” as “Route Based” and Select the Versa Gateway with has the IP 182.18.x.x, provide the Remote Public IP address and click on Next.



Configure > Security Service Edge > Settings > Site-to-Site Tunnels

Add Site-to-Site Tunnel

1 Enter TYPE

Type

● IPsec ○ GRE

Enabled

Tunnel Type: Route Based

Gateway Link

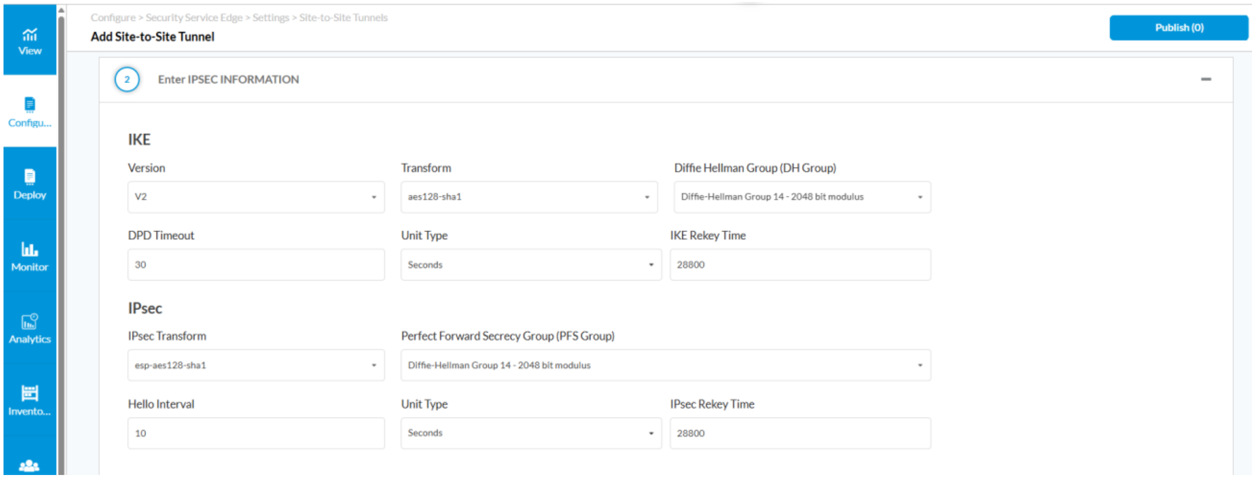
Versa Gateway*: SSE-BLR-LAB-GW1

Local Public Gateway FQDN: sse-blr-lab-gw1.pslab.versanow.net

Local Public Gateway Addresses: 10.195.66.72, 10.195.66.71

Remote Public IP Address or FQDN: 3.109.127.102

Under “Enter IPSEC INFORMATION” configure the Ike and IPsec parameters. The snip below shows the default values.



Configure > Security Service Edge > Settings > Site-to-Site Tunnels

Add Site-to-Site Tunnel

2 Enter IPSEC INFORMATION

IKE

Version: V2

Transform: aes128-sha1

Diffie Hellman Group (DH Group): Diffie-Hellman Group 14 - 2048 bit modulus

DPD Timeout: 30

Unit Type: Seconds

IKE Rekey Time: 28800

IPsec

IPsec Transform: esp-aes128-sha1

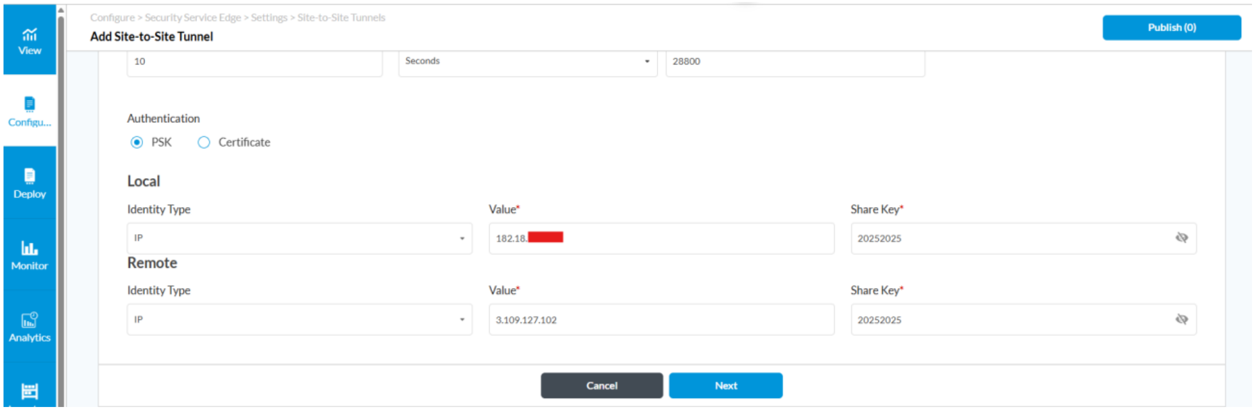
Perfect Forward Secrecy Group (PFS Group): Diffie-Hellman Group 14 - 2048 bit modulus

Hello Interval: 10

Unit Type: Seconds

IPsec Rekey Time: 28800

Under “Authentication”, select “PSK”, Under Local and Remote provide the Identity type as IP and give the Public IP’s of SASE-GW, the Public IP address of Tunnel-1 and under Share key provide the PSK.



Configure > Security Service Edge > Settings > Site-to-Site Tunnels

Add Site-to-Site Tunnel

10 | Seconds | 28800

Authentication

● PSK ○ Certificate

Local

Identity Type: IP

Value*: 182.18[redacted]

Share Key*: 20252025

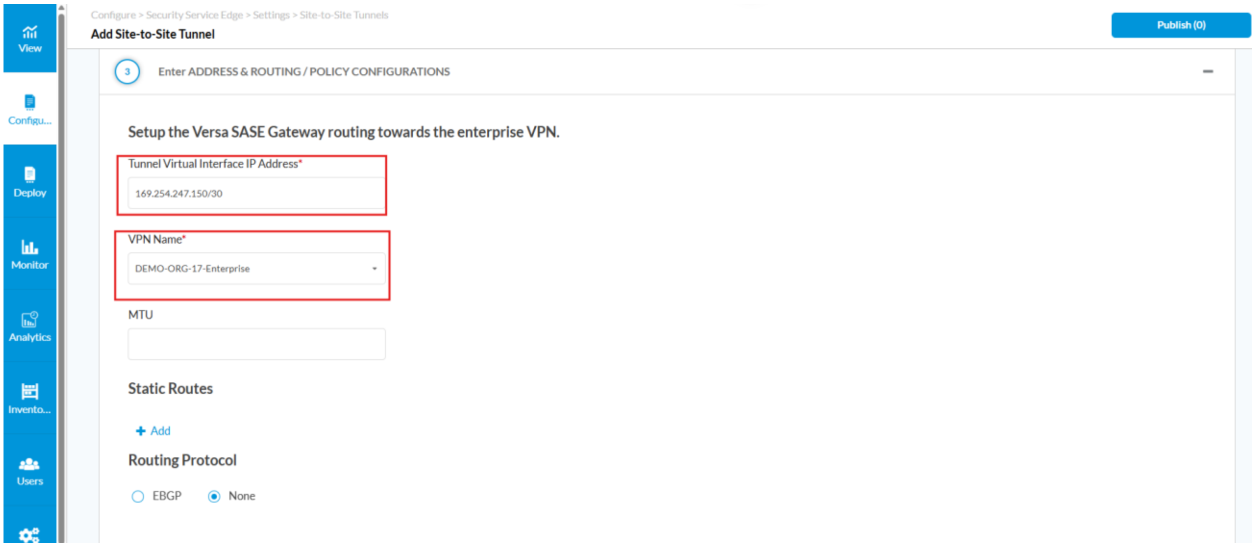
Remote

Identity Type: IP

Value*: 3.109.127.102

Share Key*: 20252025

Under “Tunnel Virtual interface IP Address” provide the IP’s generated by AWS as shown in the example above and under “VPN Name” provide the respective Enterprise VPN Name.


View
Configu...
Deploy
Monitor
Analytics
Invento...
Users
Configure > Security Service Edge > Settings > Site-to-Site Tunnels
Publish (0)
3

Add Site-to-Site Tunnel

Enter ADDRESS & ROUTING / POLICY CONFIGURATIONS

Setup the Versa SASE Gateway routing towards the enterprise VPN.

Tunnel Virtual Interface IP Address*: 169.254.247.150/30

VPN Name*: DEMO-ORG-17-Enterprise

MTU:

Static Routes

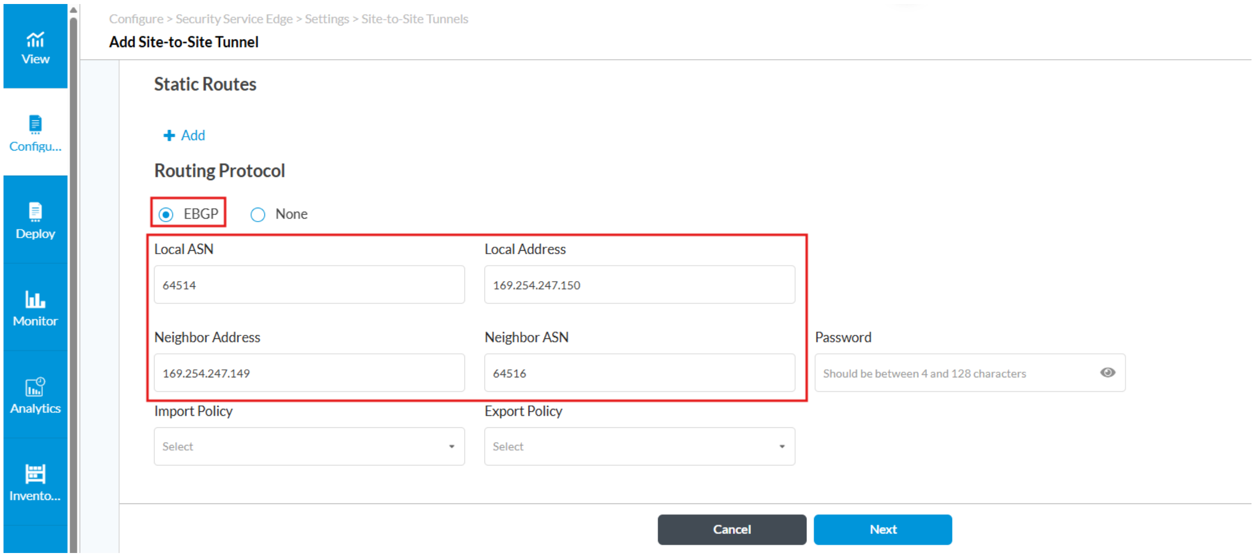
+ Add

Routing Protocol

○ EBGP ● None

Under “Routing Protocol” select EBGP and under Local ASN, Local Address, Neighbor Address and Neighbor ASN provide the respective configuration.

| | |
|---|---|
| Local ASN | 64514 |
| Local Address | 169.254.247.148 |
| Remote ASN | 64516 |
| Neighbor Address | 169.254.247.149 |


View
Configu...
Deploy
Monitor
Analytics
Invento...
Configure > Security Service Edge > Settings > Site-to-Site Tunnels
Cancel
Next

Add Site-to-Site Tunnel

Static Routes

+ Add

Routing Protocol

● EBGP ○ None

Local ASN: 64514

Local Address: 169.254.247.150

Neighbor Address: 169.254.247.149

Neighbor ASN: 64516

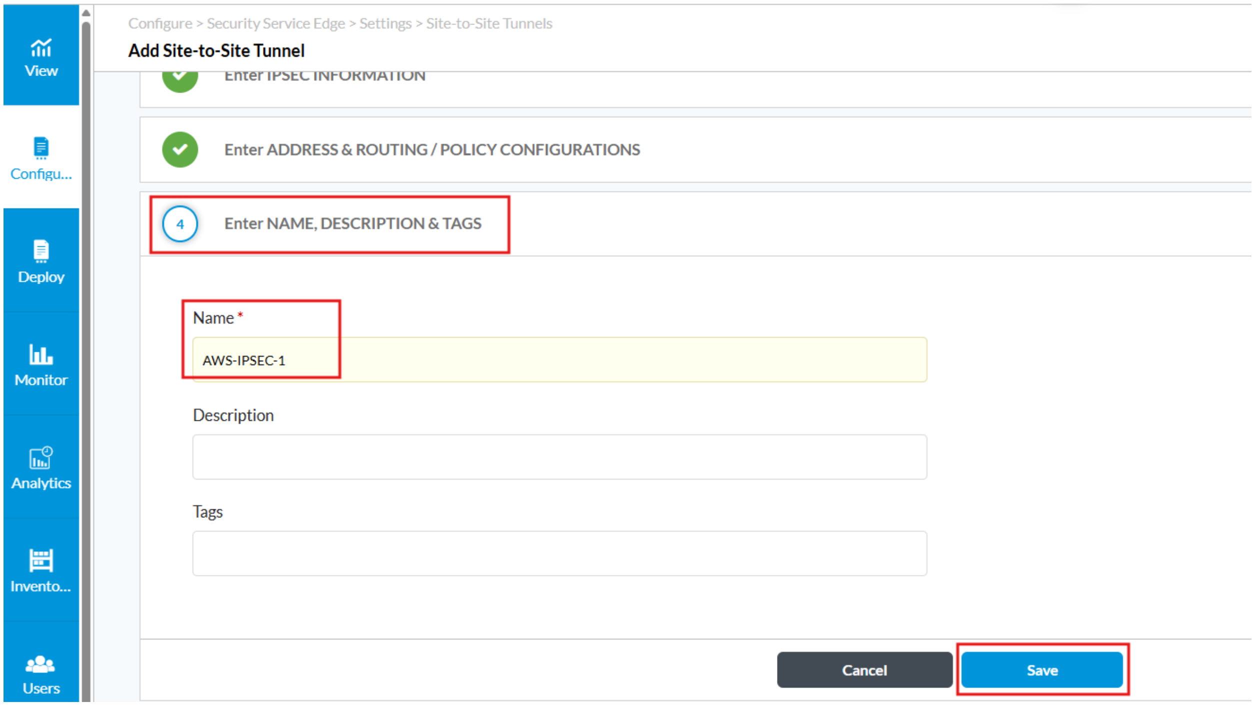
Password: Should be between 4 and 128 characters

Import Policy: Select

Export Policy: Select

**Note**: The Local and Neighbor Address will be your IPsec Tunnel interfaces.

Under “Enter NAME, DESCRIPTION & TAGS” provide the Name to the IPSec tunnel.



Configure > Security Service Edge > Settings > Site-to-Site Tunnels

Add Site-to-Site Tunnel

Enter IPSEC INFORMATION

Enter ADDRESS & ROUTING / POLICY CONFIGURATIONS

4 Enter NAME, DESCRIPTION & TAGS

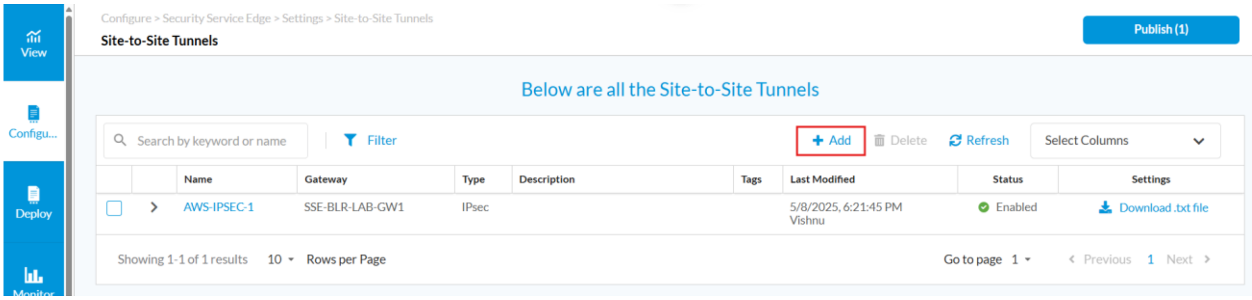
Name *: AWS-IPSEC-1

Description

Tags

Since AWS has two IPsec tunnels for Redundancy, create one more IPsec tunnel on SASE-GW.

Under “Settings” go to “Site-to-Site Tunnels” and click on “Add”.



Configure > Security Service Edge > Settings > Site-to-Site Tunnels

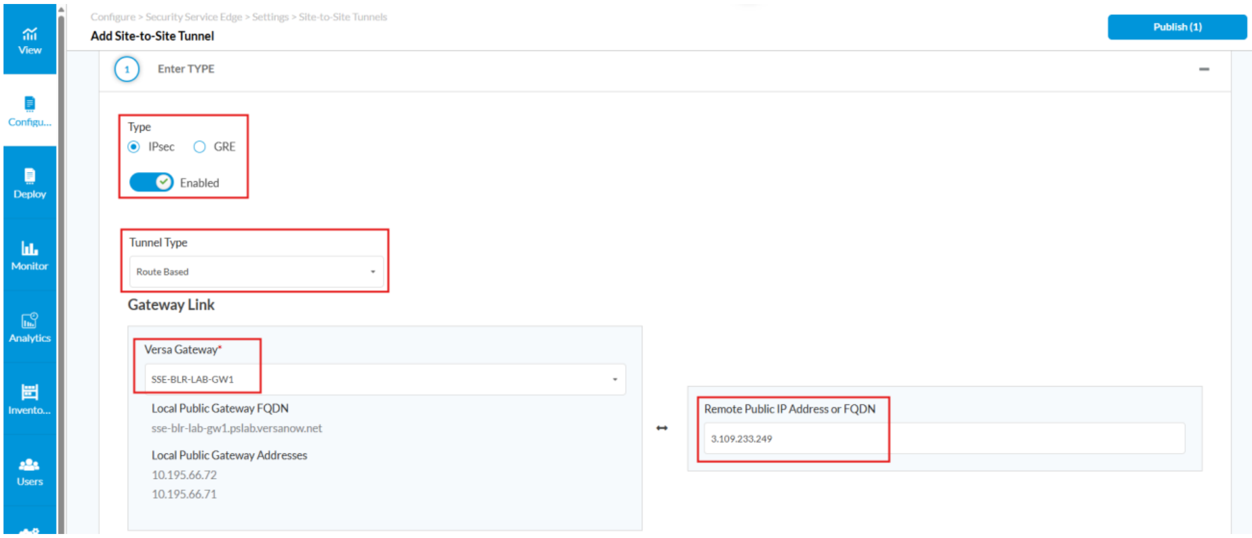
Site-to-Site Tunnels

Below are all the Site-to-Site Tunnels

| | Name | Gateway | Type | Description | Tags | Last Modified | Status | Settings |
|---|---|---|---|---|---|---|---|---|
| □ › | AWS-IPSEC-1 | SSE-BLR-LAB-GW1 | IPsec | | | 5/8/2025, 6:21:45 PM<br>Vishnu | ✓ Enabled | Download .txt file |

Showing 1-1 of 1 results 10 Rows per Page Go to page 1 ‹ Previous 1 Next ›

Under “Enter TYPE”, provide the Type as IPSec, “Tunnel Type” as “Route Based” and Select the Versa Gateway with has the IP 182.18.x.x, provide the Remote Public IP address and click on Next.



Configure > Security Service Edge > Settings > Site-to-Site Tunnels

Add Site-to-Site Tunnel

1 Enter TYPE

Type: ● IPsec ○ GRE

Enabled

Tunnel Type: Route Based

Gateway Link

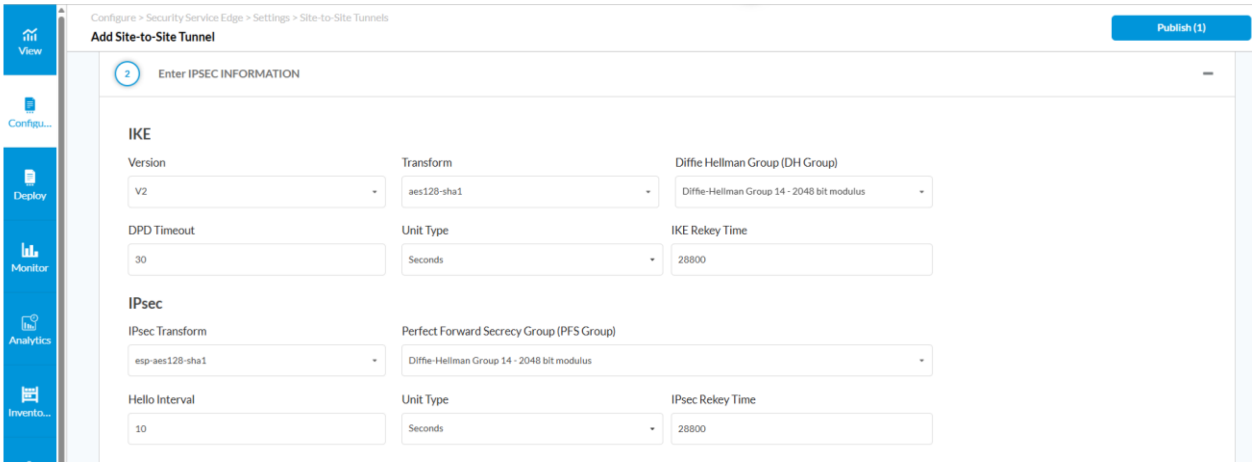
Versa Gateway*: SSE-BLR-LAB-GW1

Local Public Gateway FQDN: sse-blr-lab-gw1.pslab.versanow.net

Local Public Gateway Addresses: 10.195.66.72, 10.195.66.71

Remote Public IP Address or FQDN: 3.109.233.249

Under “Enter IPSEC INFORMATION” configure the Ike and IPsec parameters. The snip below shows the default values.



Configure > Security Service Edge > Settings > Site-to-Site Tunnels

Add Site-to-Site Tunnel

2 Enter IPSEC INFORMATION

IKE

Version: V2

Transform: aes128-sha1

Diffie Hellman Group (DH Group): Diffie-Hellman Group 14 - 2048 bit modulus

DPD Timeout: 30

Unit Type: Seconds

IKE Rekey Time: 28800

IPsec

IPsec Transform: esp-aes128-sha1

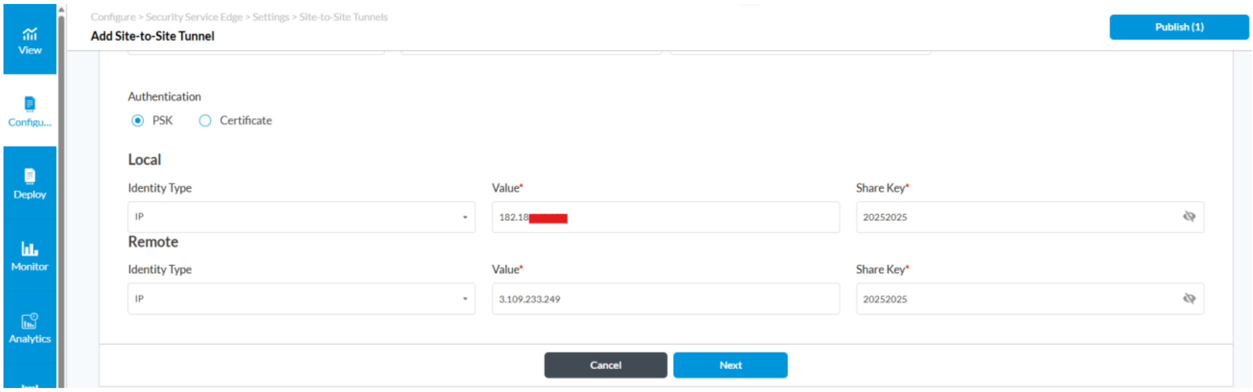
Perfect Forward Secrecy Group (PFS Group): Diffie-Hellman Group 14 - 2048 bit modulus

Hello Interval: 10

Unit Type: Seconds

IPsec Rekey Time: 28800

Under “Authentication”, select “PSK”, Under Local and Remote provide the Identity type as IP and give the Public IP’s of SASE-GW, the Public IP address of Tunnel-1 and under Share key provide the PSK.



Configure > Security Service Edge > Settings > Site-to-Site Tunnels

Add Site-to-Site Tunnel

Authentication

● PSK ○ Certificate

Local

Identity Type: IP

Value*: 182.18[redacted]

Share Key*: 20252025

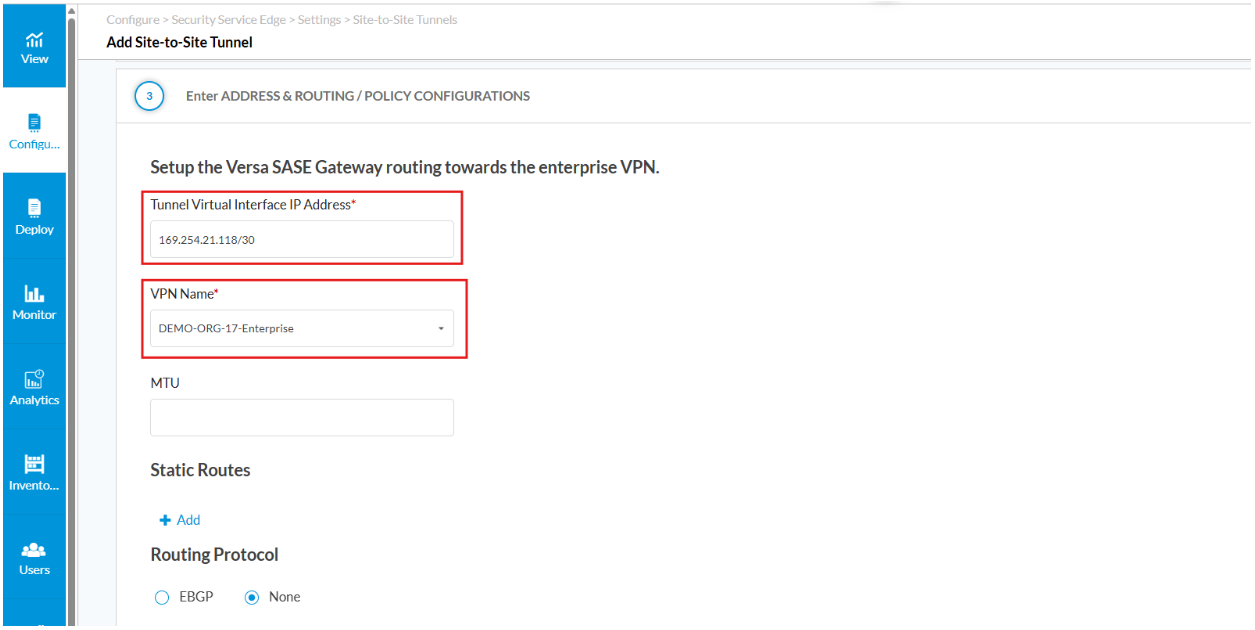
Remote

Identity Type: IP

Value*: 3.109.233.249

Share Key*: 20252025

Under “Tunnel Virtual interface IP Address” provide the IP’s generated by AWS as shown in the example above and under “VPN Name” provide the respective Enterprise VPN Name.



Configure > Security Service Edge > Settings > Site-to-Site Tunnels

Add Site-to-Site Tunnel

3 Enter ADDRESS & ROUTING / POLICY CONFIGURATIONS

Setup the Versa SASE Gateway routing towards the enterprise VPN.

Tunnel Virtual Interface IP Address*: 169.254.21.118/30

VPN Name*: DEMO-ORG-17-Enterprise

MTU

Static Routes

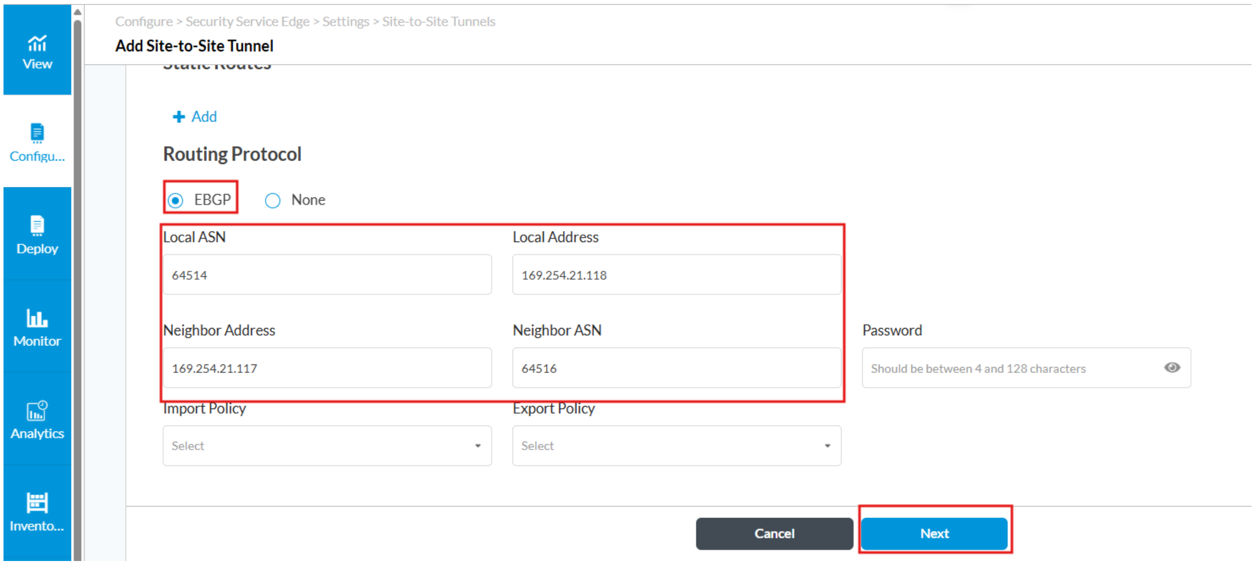
+ Add

Routing Protocol

○ EBGP ● None

Under "Routing Protocol" select EBGP and under Local ASN, Local Address, Neighbor Address and Neighbor ASN provide the respective configuration.

| | |
|---|---|
| Local ASN | 64514 |
| Local Address | 169.254.21.118 |
| Remote ASN | 64516 |
| Neighbor Address | 169.254.21.117 |



Configure > Security Service Edge > Settings > Site-to-Site Tunnels

Add Site-to-Site Tunnel

+ Add

Routing Protocol

● EBGP ○ None

Local ASN: 64514

Local Address: 169.254.21.118

Neighbor Address: 169.254.21.117

Neighbor ASN: 64516

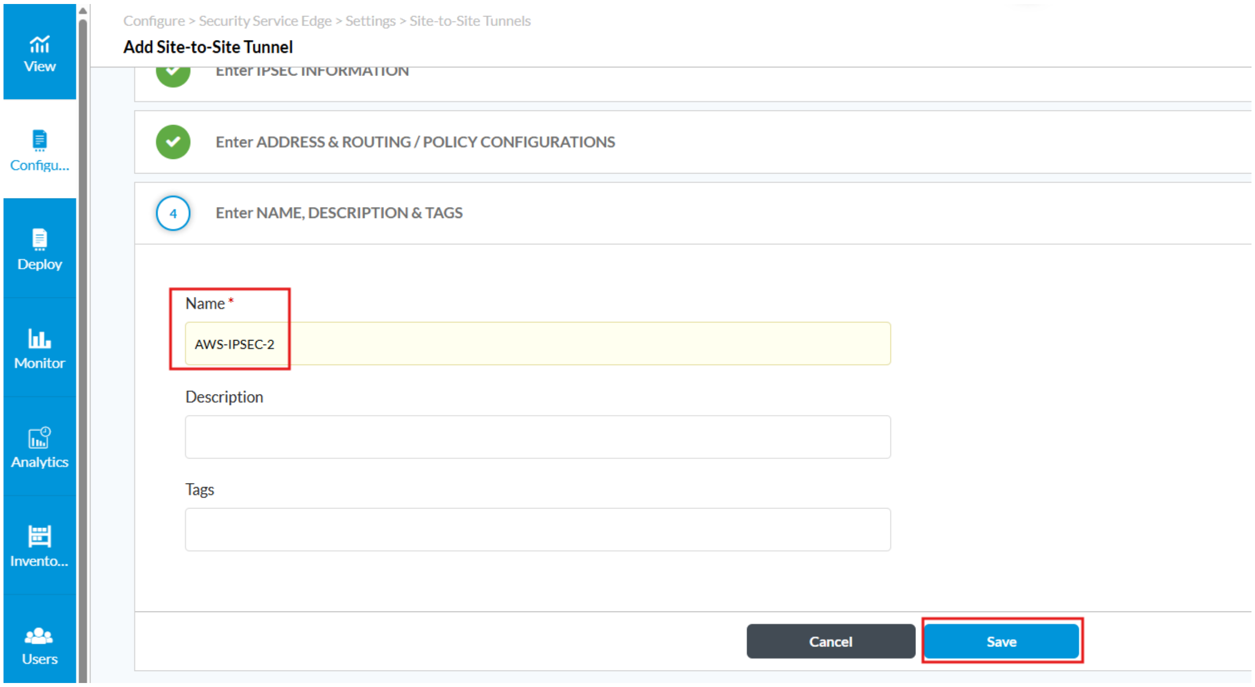
Password: Should be between 4 and 128 characters

Import Policy: Select

Export Policy: Select

**Note**: The Local and Neighbor Address will be your IPsec Tunnel interfaces.

Under "Enter NAME, DESCRIPTION & TAGS" provide the Name to the IPSec tunnel.



Configure > Security Service Edge > Settings > Site-to-Site Tunnels

Add Site-to-Site Tunnel

Enter IPSEC INFORMATION

Enter ADDRESS & ROUTING / POLICY CONFIGURATIONS

4 Enter NAME, DESCRIPTION & TAGS

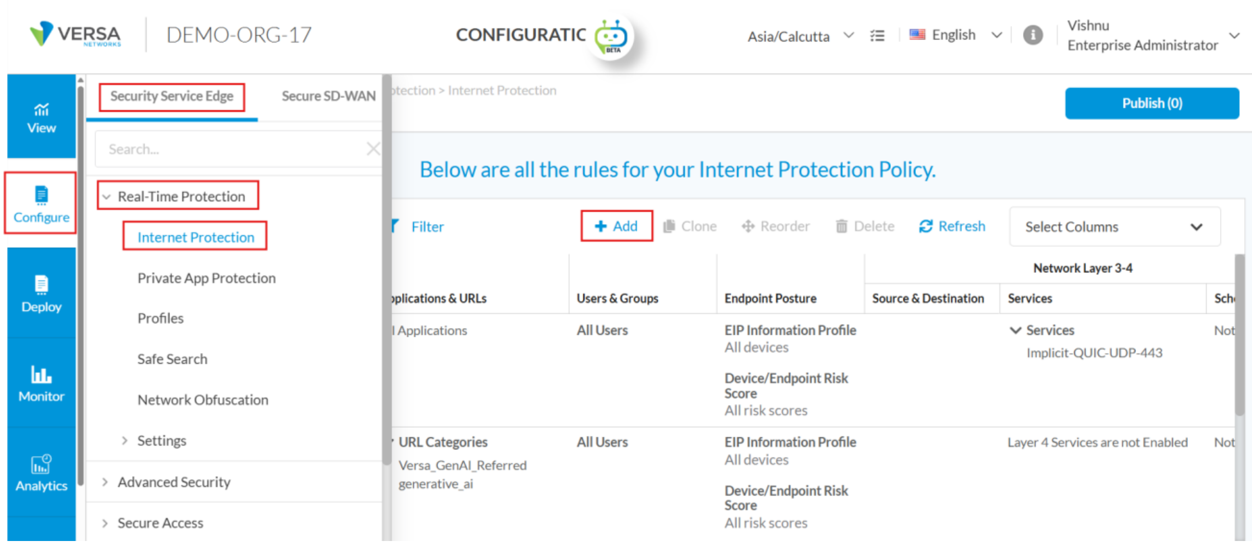
Name * AWS-IPSEC-2

Description

Tags

## Configuring Secure Access Rule:

To Create a secure access rule for allowing traffic from SASE clients to AWS EC2 through IPSec tunnels, Go to Configure → Secure Service Edge → Real-Time Protection → Internet Protection and click on "Add".

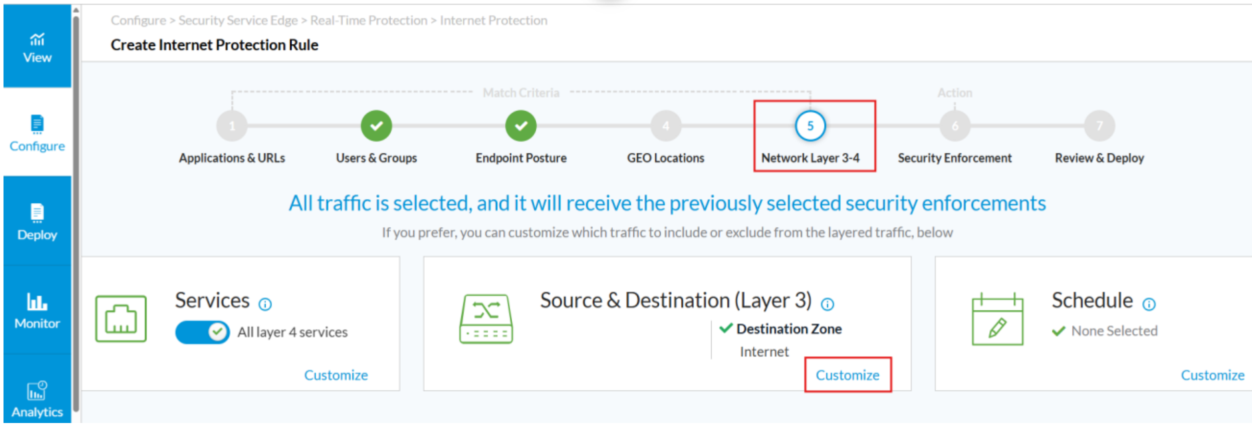


otection > Internet Protection

Below are all the rules for your Internet Protection Policy.

| pplications & URLs | Users & Groups | Endpoint Posture | Network Layer 3-4 |  | Sch |
|---|---|---|---|---|---|
|  |  |  | Source & Destination | Services |  |
| l Applications | All Users | EIP Information Profile<br>All devices<br>Device/Endpoint Risk Score<br>All risk scores |  | Services<br>Implicit-QUIC-UDP-443 | Not |
| URL Categories<br>Versa_GenAI_Referred<br>generative_ai | All Users | EIP Information Profile<br>All devices<br>Device/Endpoint Risk Score<br>All risk scores |  | Layer 4 Services are not Enabled | Not |

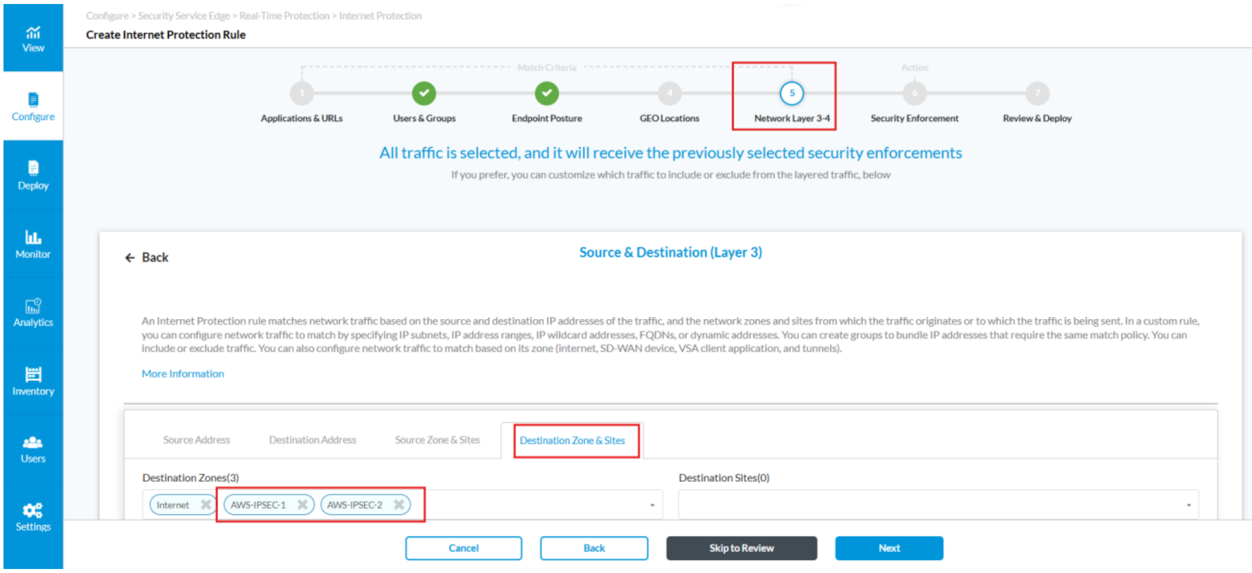
Under "Network Layer 3-4" go to "Source & Destination (Layer 3)" and click on "Customize".



All traffic is selected, and it will receive the previously selected security enforcements

If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

Under “Destination Zone & Sites” configure “AWS-IPsec-1” and “AWS-IPSEC-2”.



All traffic is selected, and it will receive the previously selected security enforcements

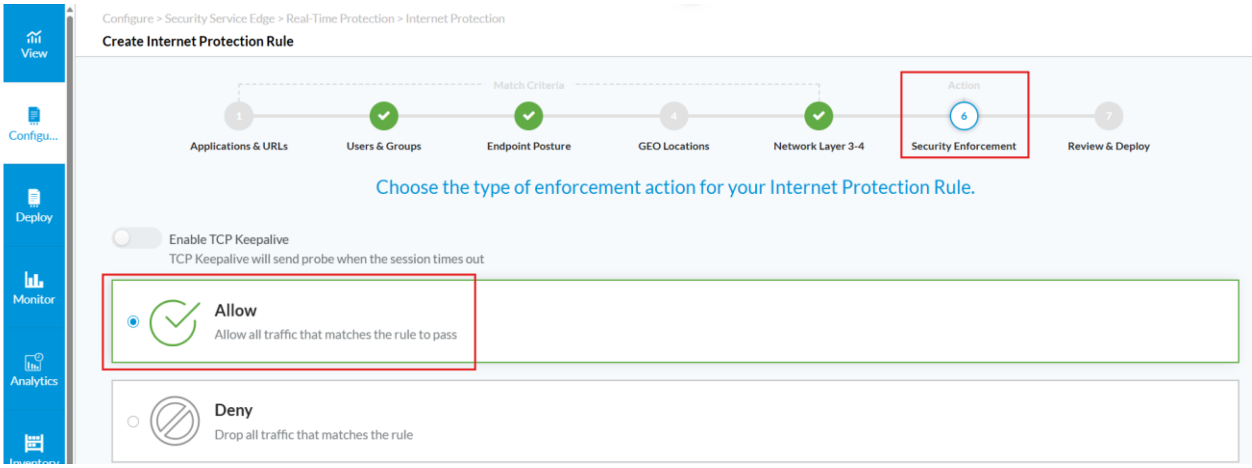
If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

An Internet Protection rule matches network traffic based on the source and destination IP addresses of the traffic, and the network zones and sites from which the traffic originates or to which the traffic is being sent. In a custom rule, you can configure network traffic to match by specifying IP subnets, IP address ranges, IP wildcard addresses, FQDNs, or dynamic addresses. You can create groups to bundle IP addresses that require the same match policy. You can include or exclude traffic. You can also configure network traffic to match based on its zone (internet, SD-WAN device, VSA client application, and tunnels).

Destination Zones(3): Internet, AWS-IPSEC-1, AWS-IPSEC-2

Destination Sites(0)

Under “Security Enforcement” Configure the action as “Allow”.



Choose the type of enforcement action for your Internet Protection Rule.

Enable TCP Keepalive

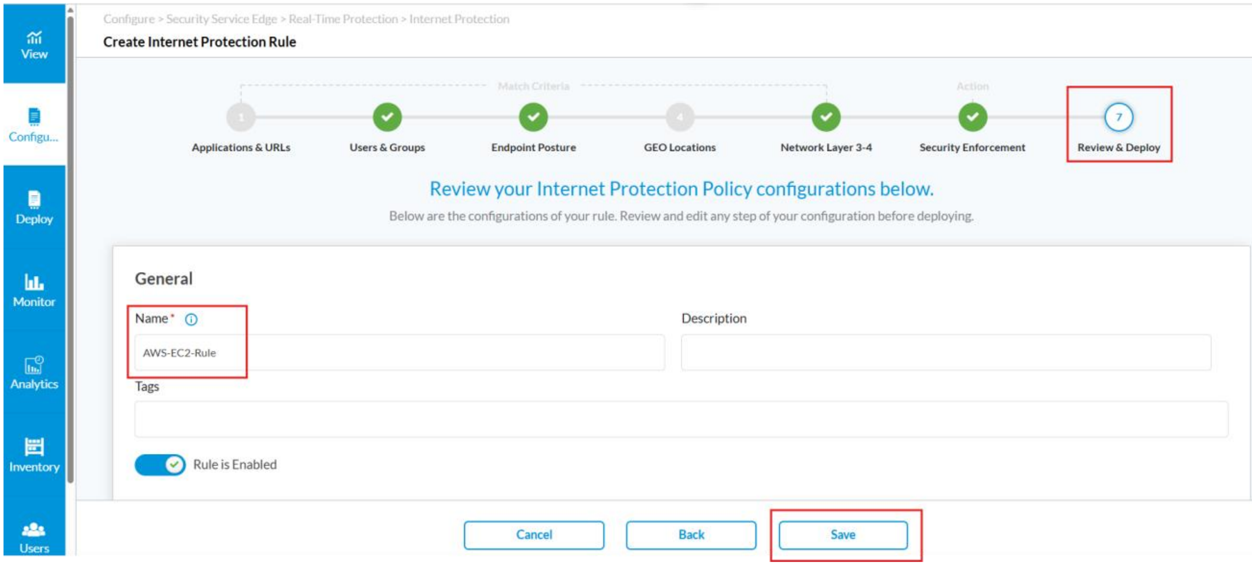
TCP Keepalive will send probe when the session times out

● Allow
Allow all traffic that matches the rule to pass

○ Deny
Drop all traffic that matches the rule

Note: Security Enforcement can be configured as per the requirement.

Under “Review and Deploy” provide the “Name” for the Internet Protection Rule.



Configure > Security Service Edge > Real-Time Protection > Internet Protection

Create Internet Protection Rule

Review your Internet Protection Policy configurations below.

Below are the configurations of your rule. Review and edit any step of your configuration before deploying.

General

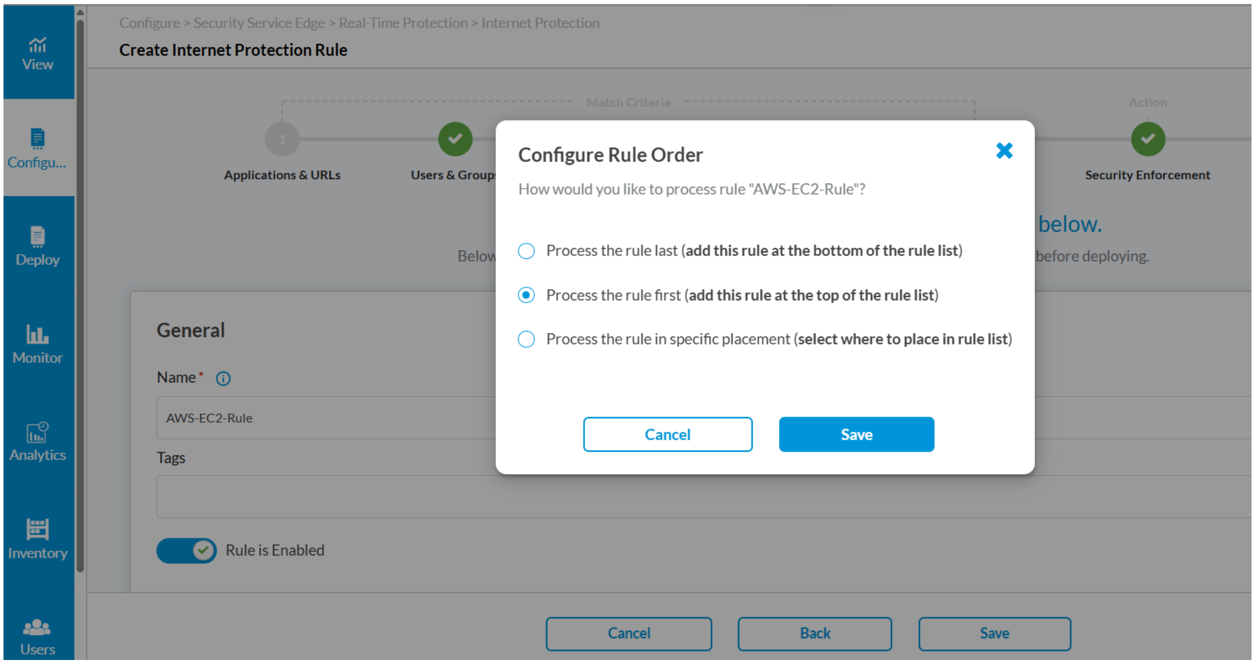
Name*: AWS-EC2-Rule

Description:

Tags:

Rule is Enabled

Under “Configure the Rule Order” place the rule at the top.



Configure > Security Service Edge > Real-Time Protection > Internet Protection

Create Internet Protection Rule

Configure Rule Order

How would you like to process rule "AWS-EC2-Rule"?

○ Process the rule last (**add this rule at the bottom of the rule list**)

● Process the rule first (**add this rule at the top of the rule list**)

○ Process the rule in specific placement (**select where to place in rule list**)

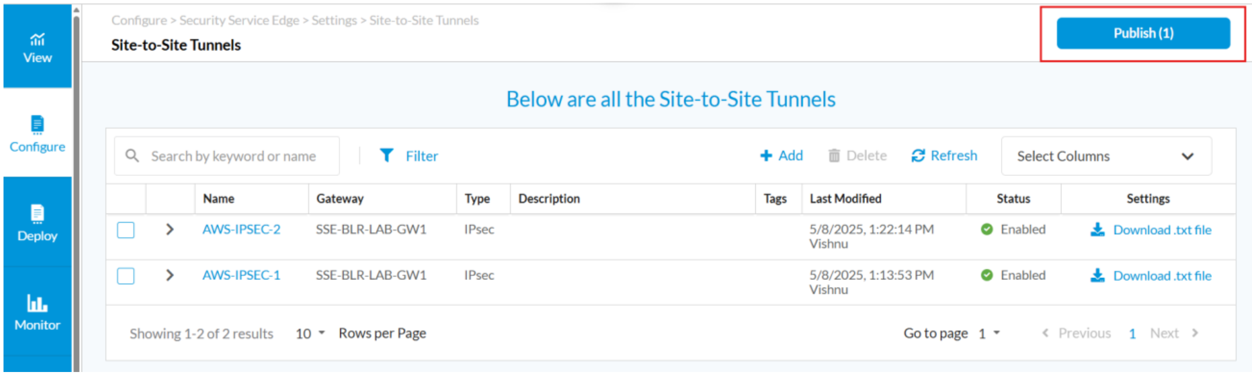
General

Name*: AWS-EC2-Rule

Tags

Rule is Enabled

Once the configuration is complete Publish the Configuration to SASE Gateways.



Configure > Security Service Edge > Settings > Site-to-Site Tunnels

Site-to-Site Tunnels

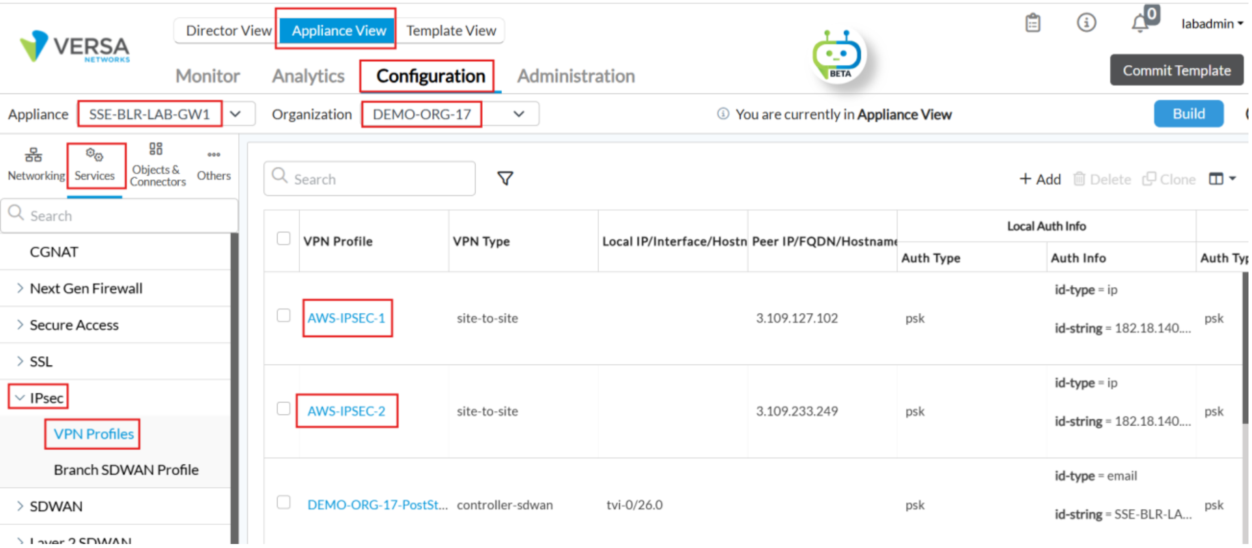
Below are all the Site-to-Site Tunnels

| Name | Gateway | Type | Description | Tags | Last Modified | Status | Settings |
|---|---|---|---|---|---|---|---|
| AWS-IPSEC-2 | SSE-BLR-LAB-GW1 | IPsec | | | 5/8/2025, 1:22:14 PM<br>Vishnu | Enabled | Download .txt file |
| AWS-IPSEC-1 | SSE-BLR-LAB-GW1 | IPsec | | | 5/8/2025, 1:13:53 PM<br>Vishnu | Enabled | Download .txt file |

Showing 1-2 of 2 results 10 Rows per Page Go to page 1 Previous 1 Next

IPSec on AWS is always a responder, so we need to modify the SASE Gateway IPsec from "Responder" to "Auto" on both the IPsec Tunnels.

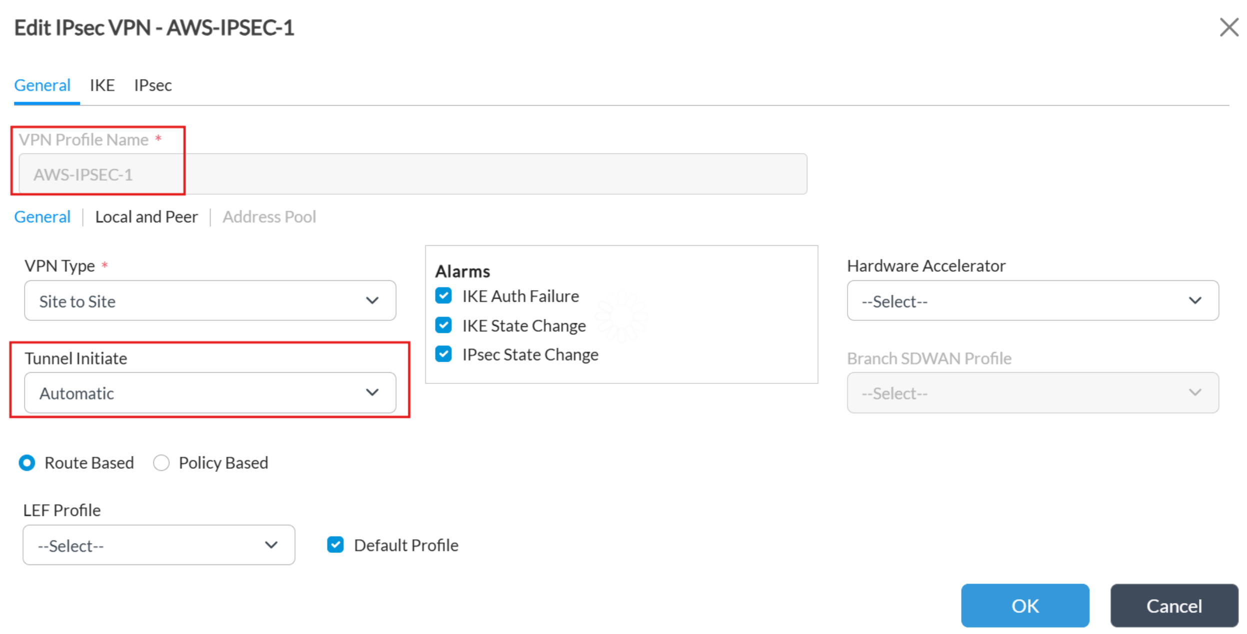
Under "Appliance View" go to respective SASE GW and under "Configure" go to "Services" → IPsec → VPN Profiles and select the VPN Profile configured for AWS.



Appliance SSE-BLR-LAB-GW1 Organization DEMO-ORG-17 You are currently in Appliance View

| VPN Profile | VPN Type | Local IP/Interface/Hostn | Peer IP/FQDN/Hostname | Local Auth Info | | Auth Typ |
|---|---|---|---|---|---|---|
| | | | | Auth Type | Auth Info | |
| AWS-IPSEC-1 | site-to-site | | 3.109.127.102 | psk | id-type = ip<br>id-string = 182.18.140.... | psk |
| AWS-IPSEC-2 | site-to-site | | 3.109.233.249 | psk | id-type = ip<br>id-string = 182.18.140.... | psk |
| DEMO-ORG-17-PostSt... | controller-sdwan | tvi-0/26.0 | | psk | id-type = email<br>id-string = SSE-BLR-LA... | psk |

Under "General", change the "Tunnel Initiate" to "Automatic" for both AWS-IPSEC-1 and AWS-IPSEC-2.



Edit IPsec VPN - AWS-IPSEC-1

VPN Profile Name *: AWS-IPSEC-1

VPN Type *: Site to Site

Tunnel Initiate: Automatic

Alarms
☑ IKE Auth Failure
☑ IKE State Change
☑ IPsec State Change

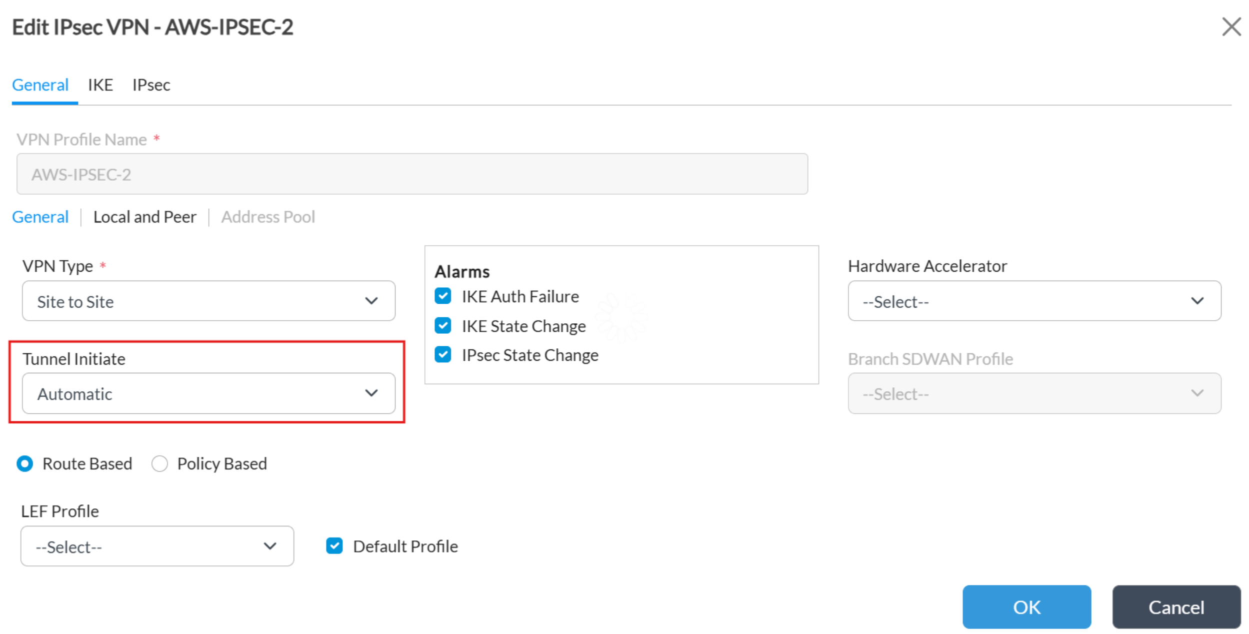
Hardware Accelerator: --Select--

Branch SDWAN Profile: --Select--

● Route Based ○ Policy Based

LEF Profile: --Select--

☑ Default Profile



Edit IPsec VPN - AWS-IPSEC-2

VPN Profile Name *: AWS-IPSEC-2

VPN Type *: Site to Site

Tunnel Initiate: Automatic

Alarms
☑ IKE Auth Failure
☑ IKE State Change
☑ IPsec State Change

Hardware Accelerator: --Select--

Branch SDWAN Profile: --Select--

● Route Based ○ Policy Based

LEF Profile: --Select--

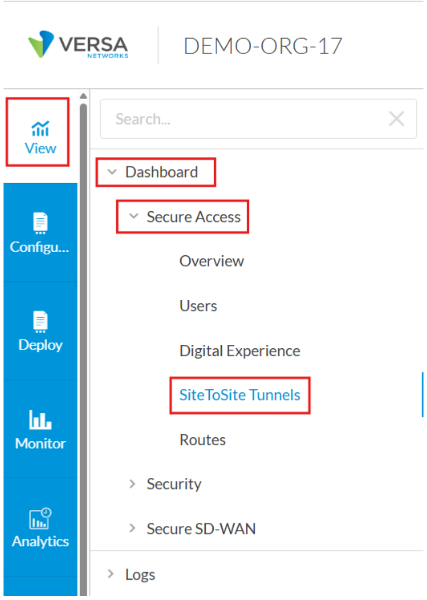
☑ Default Profile

Once the above configuration is complete you can view the IPsec and Tunnel status and BGP status on AWS and Concerto.

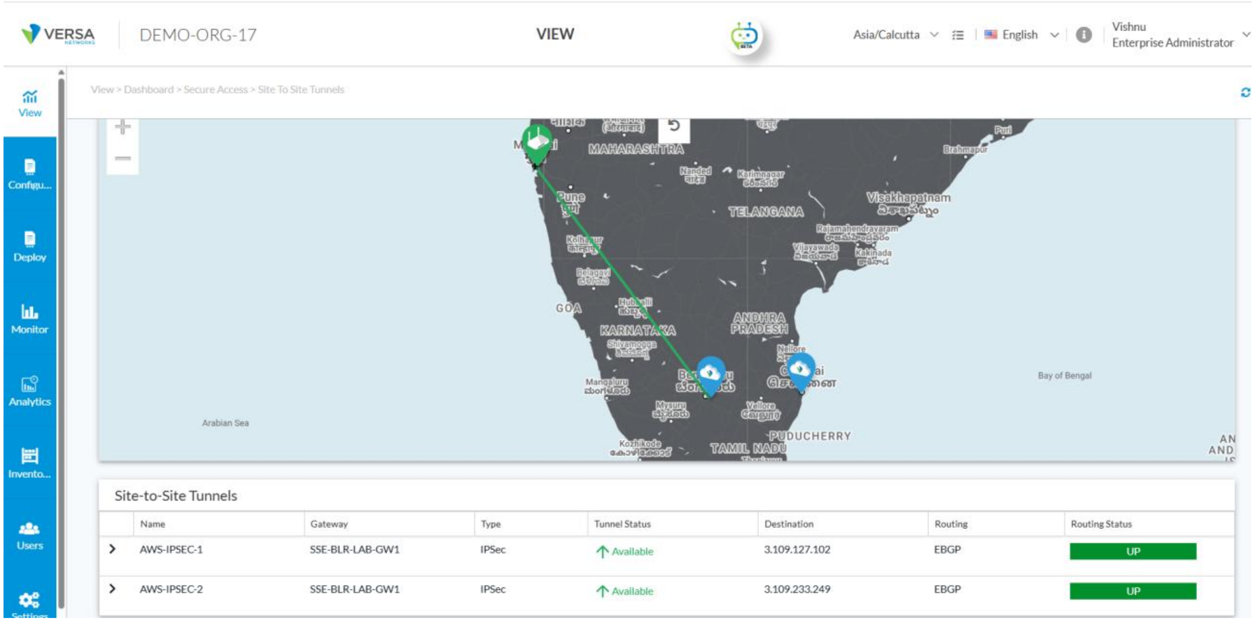
## Verifying IPsec and BGP status:

### Concerto:

Go to View → Dashboard → Secure Access → Site to Site Tunnels.



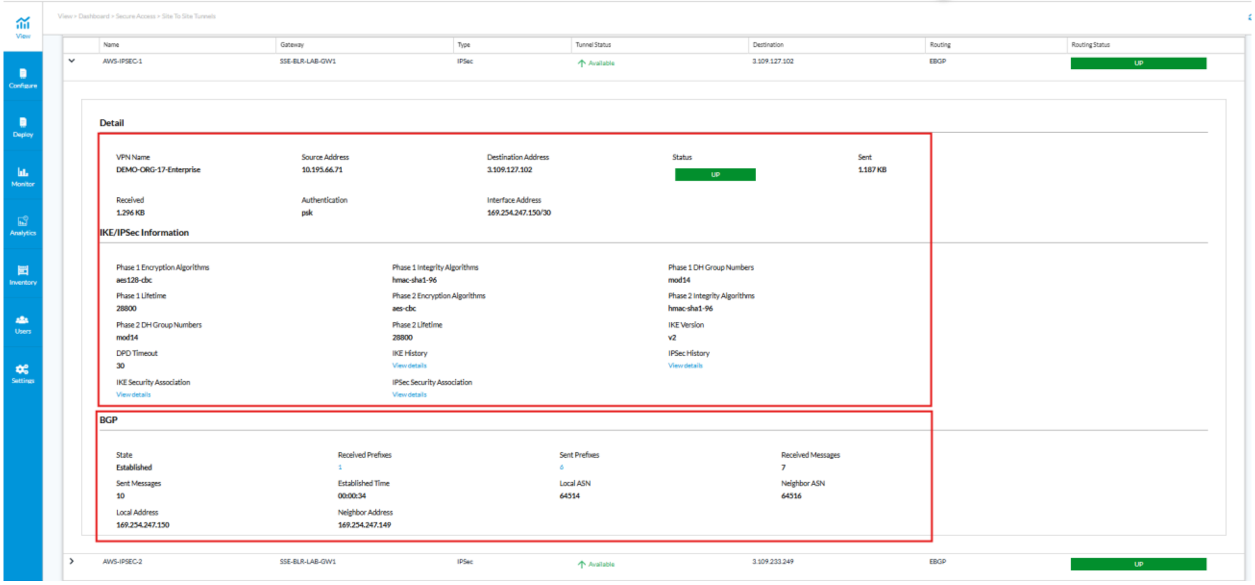
Under Site-to-Site Tunnels, check the Tunnel and Routing Status.



Site-to-Site Tunnels

| | Name | Gateway | Type | Tunnel Status | Destination | Routing | Routing Status |
|---|---|---|---|---|---|---|---|
| > | AWS-IPSEC-1 | SSE-BLR-LAB-GW1 | IPSec | ↑ Available | 3.109.127.102 | EBGP | UP |
| > | AWS-IPSEC-2 | SSE-BLR-LAB-GW1 | IPSec | ↑ Available | 3.109.233.249 | EBGP | UP |

Expanding the Tunnel will show detailed information about the IPsec tunnels and BGP.



View > Dashboard > Secure Access > Site To Site Tunnels

| | Name | Gateway | Type | Tunnel Status | Destination | Routing | Routing Status |
|---|---|---|---|---|---|---|---|
| ⌄ | AWS-IPSEC-1 | SSE-BLR-LAB-GW1 | IPSec | ↑ Available | 3.109.127.102 | EBGP | UP |

Detail

VPN Name
DEMO-ORG-17-Enterprise

Source Address
10.195.66.71

Destination Address
3.109.127.102

Status
UP

Sent
1.187 KB

Received
1.296 KB

Authentication
psk

Interface Address
169.254.247.150/30

IKE/IPSec Information

Phase 1 Encryption Algorithms
aes128-cbc

Phase 1 Integrity Algorithms
hmac-sha1-96

Phase 1 DH Group Numbers
mod14

Phase 1 Lifetime
28800

Phase 2 Encryption Algorithms
aes-cbc

Phase 2 Integrity Algorithms
hmac-sha1-96

Phase 2 DH Group Numbers
mod14

Phase 2 Lifetime
28800

IKE Version
v2

DPD Timeout
30

IKE History
View details

IPSec History
View details

IKE Security Association
View details

IPSec Security Association
View details

BGP

State
Established

Received Prefixes
1

Sent Prefixes
6

Received Messages
7

Sent Messages
10

Established Time
00:00:34

Local ASN
64514

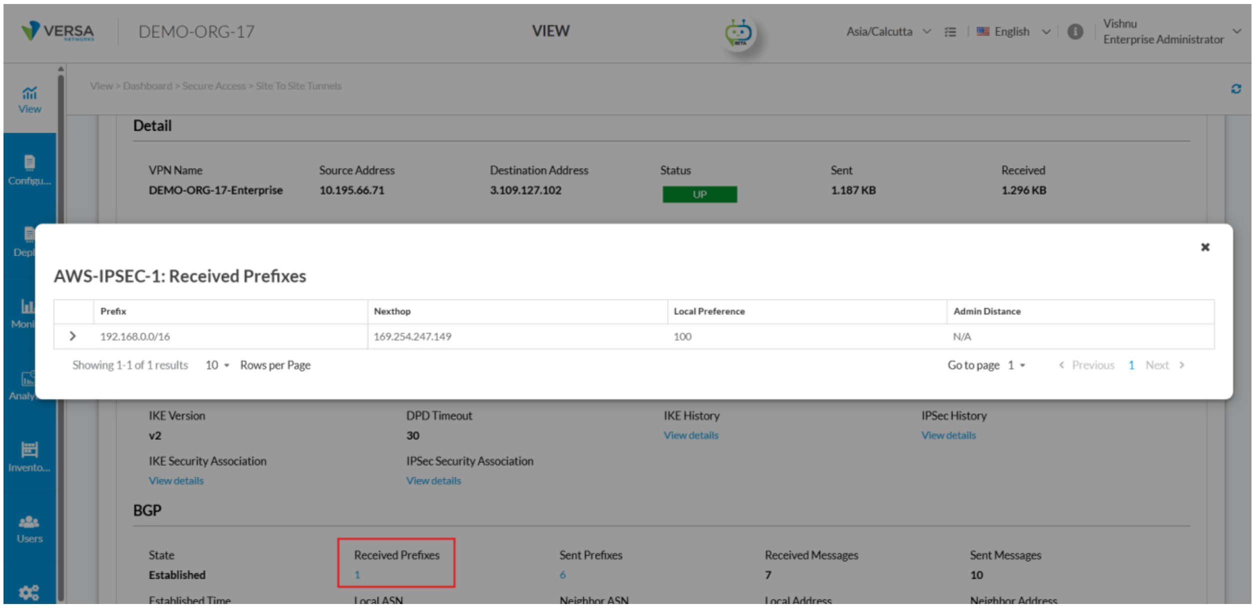
Neighbor ASN
64516

Local Address
169.254.247.150

Neighbor Address
169.254.247.149

| | Name | Gateway | Type | Tunnel Status | Destination | Routing | Routing Status |
|---|---|---|---|---|---|---|---|
| › | AWS-IPSEC-2 | SSE-BLR-LAB-GW1 | IPSec | ↑ Available | 3.109.233.249 | EBGP | UP |

Routes Sent and Received can be viewed by clicking on Received Prefixes and Sent Prefixes.



View > Dashboard > Secure Access > Site To Site Tunnels

Detail

VPN Name
DEMO-ORG-17-Enterprise

Source Address
10.195.66.71

Destination Address
3.109.127.102

Status
UP

Sent
1.187 KB

Received
1.296 KB

AWS-IPSEC-1: Received Prefixes

| | Prefix | Nexthop | Local Preference | Admin Distance |
|---|---|---|---|---|
| › | 192.168.0.0/16 | 169.254.247.149 | 100 | N/A |

Showing 1-1 of 1 results  10 ▾ Rows per Page  Go to page 1 ▾  ‹ Previous 1 Next ›

IKE Version
v2

DPD Timeout
30

IKE History
View details

IPSec History
View details

IKE Security Association
View details

IPSec Security Association
View details

BGP

State
Established

Received Prefixes
1

Sent Prefixes
6

Received Messages
7

Sent Messages
10

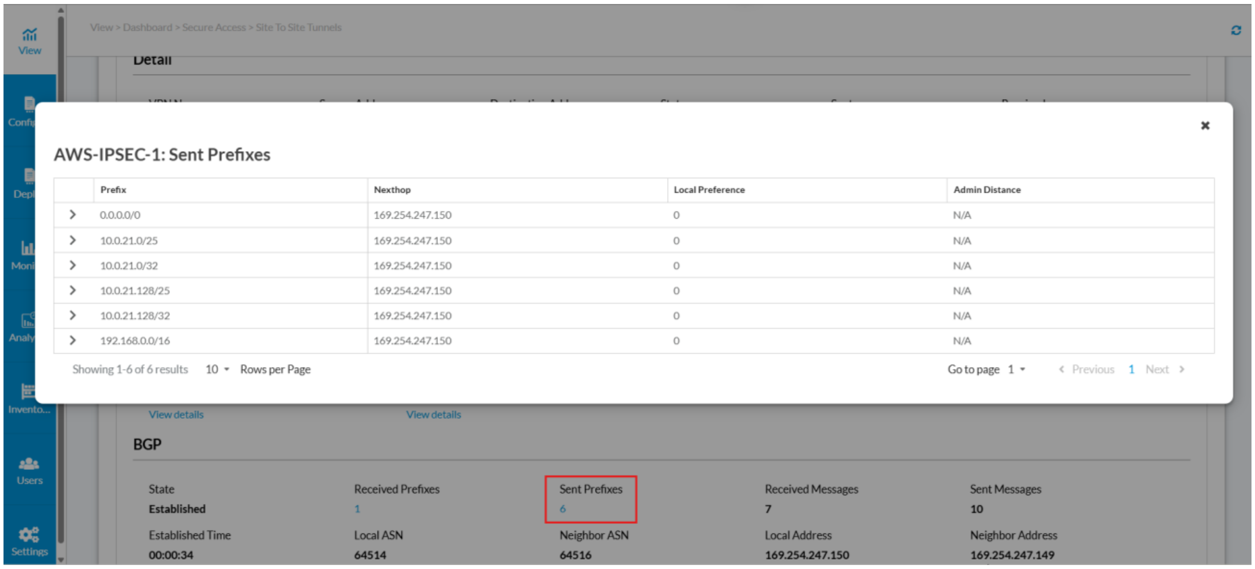
Established Time

Local ASN

Neighbor ASN

Local Address

Neighbor Address



View > Dashboard > Secure Access > Site To Site Tunnels

Detail

**AWS-IPSEC-1: Sent Prefixes**

| | Prefix | Nexthop | Local Preference | Admin Distance |
|---|---|---|---|---|
| > | 0.0.0.0/0 | 169.254.247.150 | 0 | N/A |
| > | 10.0.21.0/25 | 169.254.247.150 | 0 | N/A |
| > | 10.0.21.0/32 | 169.254.247.150 | 0 | N/A |
| > | 10.0.21.128/25 | 169.254.247.150 | 0 | N/A |
| > | 10.0.21.128/32 | 169.254.247.150 | 0 | N/A |
| > | 192.168.0.0/16 | 169.254.247.150 | 0 | N/A |

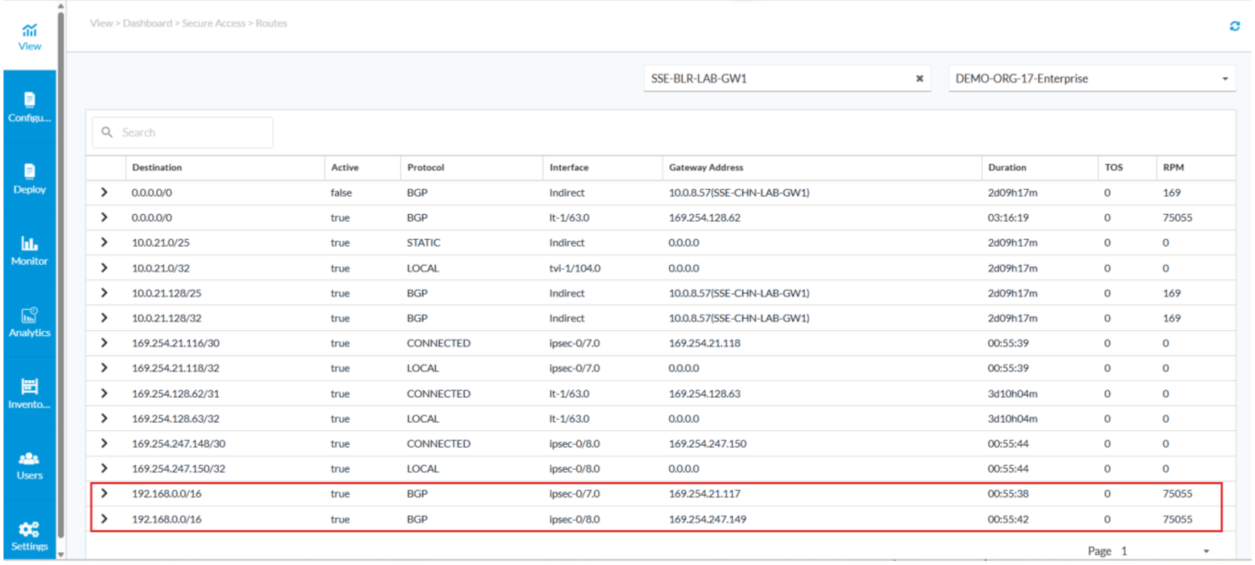
Showing 1-6 of 6 results 10 Rows per Page — Go to page 1 < Previous 1 Next >

View details View details

BGP

| State | Received Prefixes | Sent Prefixes | Received Messages | Sent Messages |
|---|---|---|---|---|
| Established | 1 | 6 | 7 | 10 |
| **Established Time** | **Local ASN** | **Neighbor ASN** | **Local Address** | **Neighbor Address** |
| 00:00:34 | 64514 | 64516 | 169.254.247.150 | 169.254.247.149 |

Routing Table on SASE-GW can be viewed from “View” → Dashboard → Secure Access → Routes.



View > Dashboard > Secure Access > Routes

SSE-BLR-LAB-GW1 — DEMO-ORG-17-Enterprise

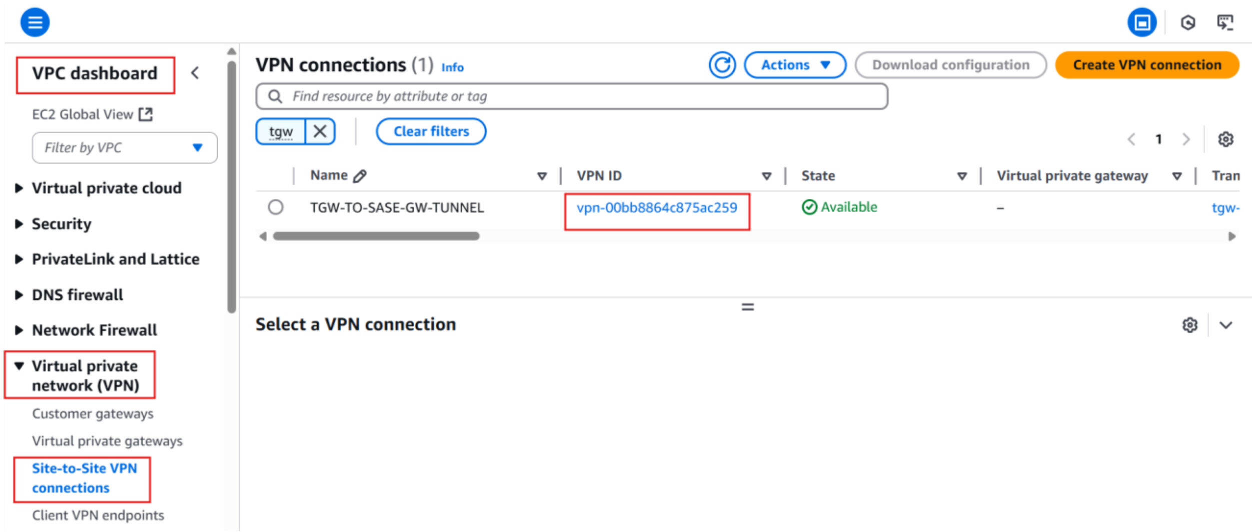
Search

| | Destination | Active | Protocol | Interface | Gateway Address | Duration | TOS | RPM |
|---|---|---|---|---|---|---|---|---|
| > | 0.0.0.0/0 | false | BGP | Indirect | 10.0.8.57(SSE-CHN-LAB-GW1) | 2d09h17m | 0 | 169 |
| > | 0.0.0.0/0 | true | BGP | lt-1/63.0 | 169.254.128.62 | 03:16:19 | 0 | 75055 |
| > | 10.0.21.0/25 | true | STATIC | Indirect | 0.0.0.0 | 2d09h17m | 0 | 0 |
| > | 10.0.21.0/32 | true | LOCAL | tvi-1/104.0 | 0.0.0.0 | 2d09h17m | 0 | 0 |
| > | 10.0.21.128/25 | true | BGP | Indirect | 10.0.8.57(SSE-CHN-LAB-GW1) | 2d09h17m | 0 | 169 |
| > | 10.0.21.128/32 | true | BGP | Indirect | 10.0.8.57(SSE-CHN-LAB-GW1) | 2d09h17m | 0 | 169 |
| > | 169.254.21.116/30 | true | CONNECTED | ipsec-0/7.0 | 169.254.21.118 | 00:55:39 | 0 | 0 |
| > | 169.254.21.118/32 | true | LOCAL | ipsec-0/7.0 | 0.0.0.0 | 00:55:39 | 0 | 0 |
| > | 169.254.128.62/31 | true | CONNECTED | lt-1/63.0 | 169.254.128.63 | 3d10h04m | 0 | 0 |
| > | 169.254.128.63/32 | true | LOCAL | lt-1/63.0 | 0.0.0.0 | 3d10h04m | 0 | 0 |
| > | 169.254.247.148/30 | true | CONNECTED | ipsec-0/8.0 | 169.254.247.150 | 00:55:44 | 0 | 0 |
| > | 169.254.247.150/32 | true | LOCAL | ipsec-0/8.0 | 0.0.0.0 | 00:55:44 | 0 | 0 |
| > | 192.168.0.0/16 | true | BGP | ipsec-0/7.0 | 169.254.21.117 | 00:55:38 | 0 | 75055 |
| > | 192.168.0.0/16 | true | BGP | ipsec-0/8.0 | 169.254.247.149 | 00:55:42 | 0 | 75055 |

Page 1

## AWS:

To view IPsec Tunnel status, Under VPC dashboard, go to “Virtual Private Network” → “Site to Site VPN connection” and click on VPN ID

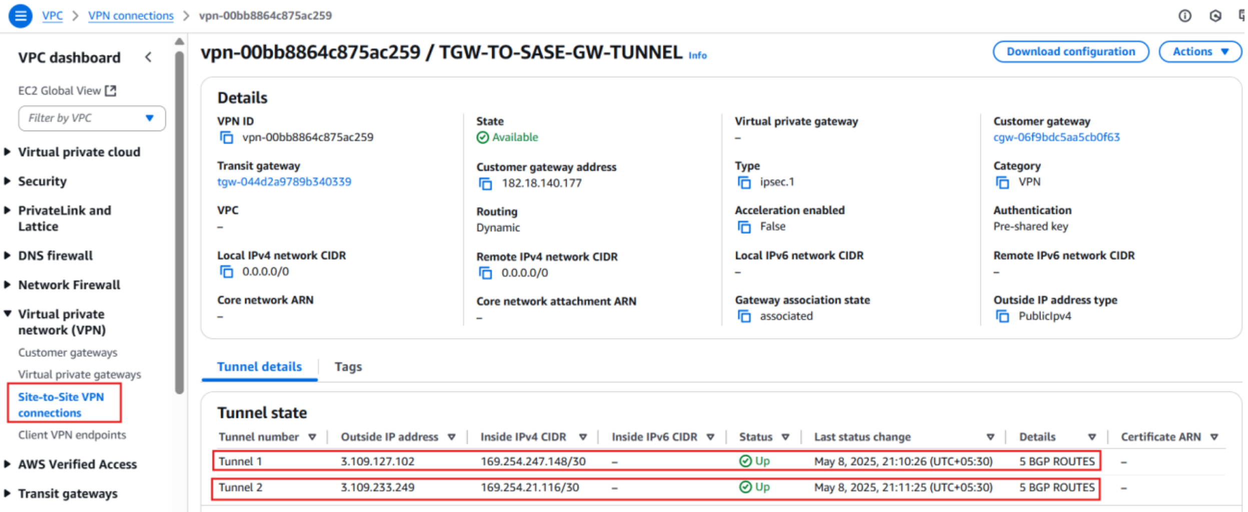


VPN connections (1) Info

| | Name | VPN ID | State | Virtual private gateway | Tran |
|---|---|---|---|---|---|
| ○ | TGW-TO-SASE-GW-TUNNEL | vpn-00bb8864c875ac259 | Available | – | tgw- |

Select a VPN connection

Tunnel details will show the Tunnel state and the BGP Routes received.



vpn-00bb8864c875ac259 / TGW-TO-SASE-GW-TUNNEL Info

Details

| | | | |
|---|---|---|---|
| VPN ID<br>vpn-00bb8864c875ac259 | State<br>Available | Virtual private gateway<br>– | Customer gateway<br>cgw-06f9bdc5aa5cb0f63 |
| Transit gateway<br>tgw-044d2a9789b340339 | Customer gateway address<br>182.18.140.177 | Type<br>ipsec.1 | Category<br>VPN |
| VPC<br>– | Routing<br>Dynamic | Acceleration enabled<br>False | Authentication<br>Pre-shared key |
| Local IPv4 network CIDR<br>0.0.0.0/0 | Remote IPv4 network CIDR<br>0.0.0.0/0 | Local IPv6 network CIDR<br>– | Remote IPv6 network CIDR<br>– |
| Core network ARN<br>– | Core network attachment ARN<br>– | Gateway association state<br>associated | Outside IP address type<br>PublicIpv4 |

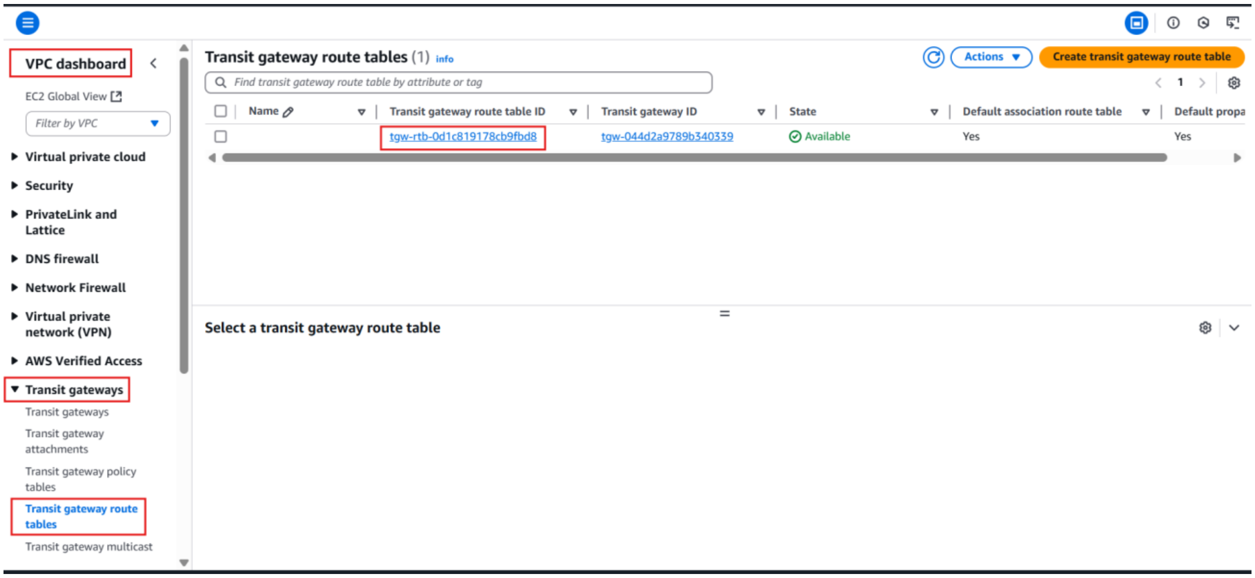
Tunnel state

| Tunnel number | Outside IP address | Inside IPv4 CIDR | Inside IPv6 CIDR | Status | Last status change | Details | Certificate ARN |
|---|---|---|---|---|---|---|---|
| Tunnel 1 | 3.109.127.102 | 169.254.247.148/30 | – | Up | May 8, 2025, 21:10:26 (UTC+05:30) | 5 BGP ROUTES | – |
| Tunnel 2 | 3.109.233.249 | 169.254.21.116/30 | – | Up | May 8, 2025, 21:11:25 (UTC+05:30) | 5 BGP ROUTES | – |

## Routing in AWS:

Since we have established BGP between TGW and SASE GW, we should be able to see the routes in TGW routing table.

To view the Routes, under VPC dashboard, go to Transit gateways →Transit gateway route tables and click ok Transit gateway route table ID.

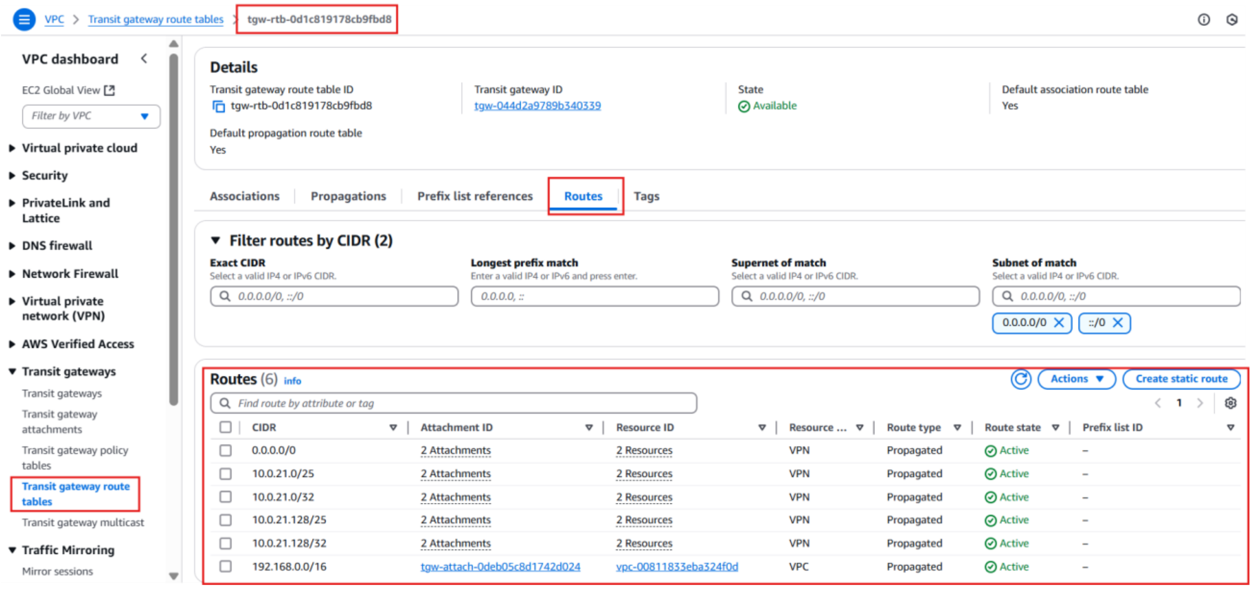


VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Security
PrivateLink and Lattice
DNS firewall
Network Firewall
Virtual private network (VPN)
AWS Verified Access
Transit gateways
Transit gateways
Transit gateway attachments
Transit gateway policy tables
Transit gateway route tables
Transit gateway multicast
Actions
Create transit gateway route table
Find transit gateway route table by attribute or tag
1
Select a transit gateway route table

Transit gateway route tables (1) info

| Name | Transit gateway route table ID | Transit gateway ID | State | Default association route table | Default propa |
|---|---|---|---|---|---|
| | tgw-rtb-0d1c819178cb9fbd8 | tgw-044d2a9789b340339 | Available | Yes | Yes |

Under TGW route table, click on routes to view the routes received from the SASE Gateway through EBGP.



Details

Transit gateway route table ID: tgw-rtb-0d1c819178cb9fbd8
Transit gateway ID: tgw-044d2a9789b340339
State: Available
Default association route table: Yes
Default propagation route table: Yes

Filter routes by CIDR (2)

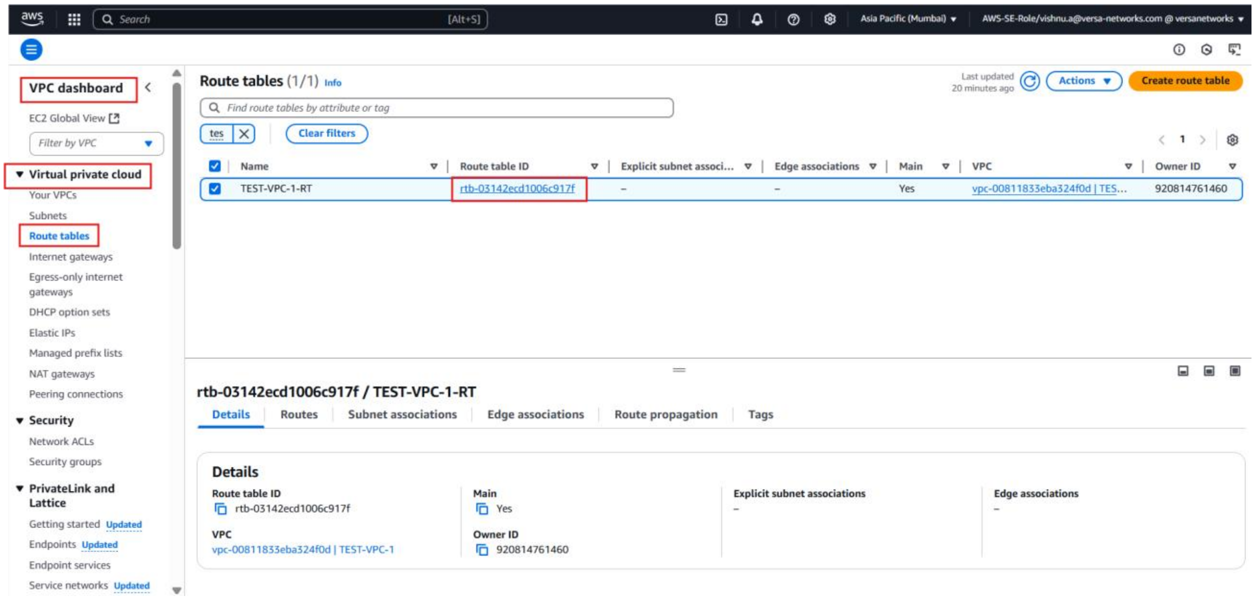
Exact CIDR: Select a valid IP4 or IPv6 CIDR. 0.0.0.0/0, ::/0
Longest prefix match: Enter a valid IP4 or IPv6 and press enter. 0.0.0.0, ::
Supernet of match: Select a valid IP4 or IPv6 CIDR. 0.0.0.0/0, ::/0
Subnet of match: Select a valid IP4 or IPv6 CIDR. 0.0.0.0/0, ::/0 — 0.0.0.0/0 ✕ ::/0 ✕

Routes (6) info

| CIDR | Attachment ID | Resource ID | Resource ... | Route type | Route state | Prefix list ID |
|---|---|---|---|---|---|---|
| 0.0.0.0/0 | 2 Attachments | 2 Resources | VPN | Propagated | Active | – |
| 10.0.21.0/25 | 2 Attachments | 2 Resources | VPN | Propagated | Active | – |
| 10.0.21.0/32 | 2 Attachments | 2 Resources | VPN | Propagated | Active | – |
| 10.0.21.128/25 | 2 Attachments | 2 Resources | VPN | Propagated | Active | – |
| 10.0.21.128/32 | 2 Attachments | 2 Resources | VPN | Propagated | Active | – |
| 192.168.0.0/16 | tgw-attach-0deb05c8d1742d024 | vpc-00811833eba324f0d | VPC | Propagated | Active | – |

For an EC2 instance to reach the subnets connected to SASE GW we need to create a static route towards TGW on the Main Routing table of VPC.

Under VPC dashboard, go to Virtual Private Cloud → Route tables and select the Main Route table of your VPC.



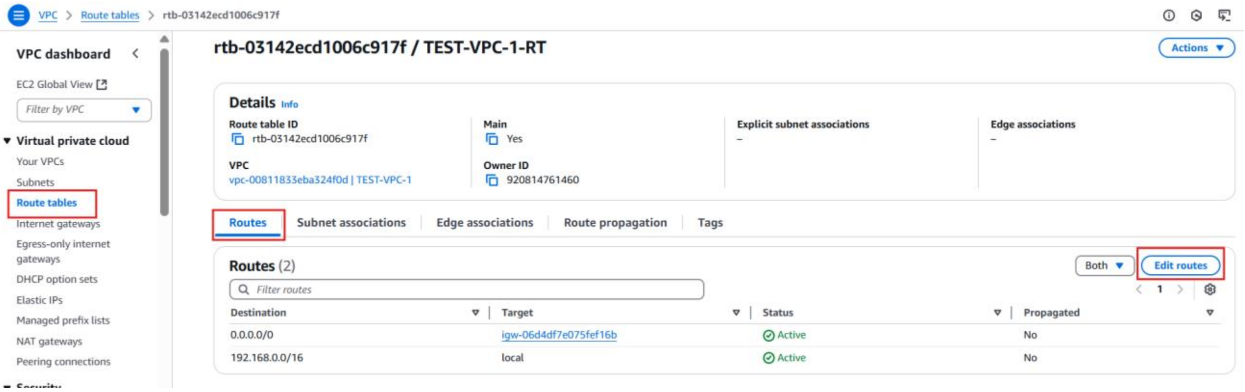
| ☑ | Name | Route table ID | Explicit subnet associ... | Edge associations | Main | VPC | Owner ID |
|---|---|---|---|---|---|---|---|
| ☑ | TEST-VPC-1-RT | rtb-03142ecd1006c917f | – | – | Yes | vpc-00811833eba324f0d \| TES... | 920814761460 |

rtb-03142ecd1006c917f / TEST-VPC-1-RT

Details

Route table ID: rtb-03142ecd1006c917f
Main: Yes
Explicit subnet associations: –
Edge associations: –
VPC: vpc-00811833eba324f0d | TEST-VPC-1
Owner ID: 920814761460

Once clicking on “Route Table ID”, under Routes click on “Edit routes”.



rtb-03142ecd1006c917f / TEST-VPC-1-RT

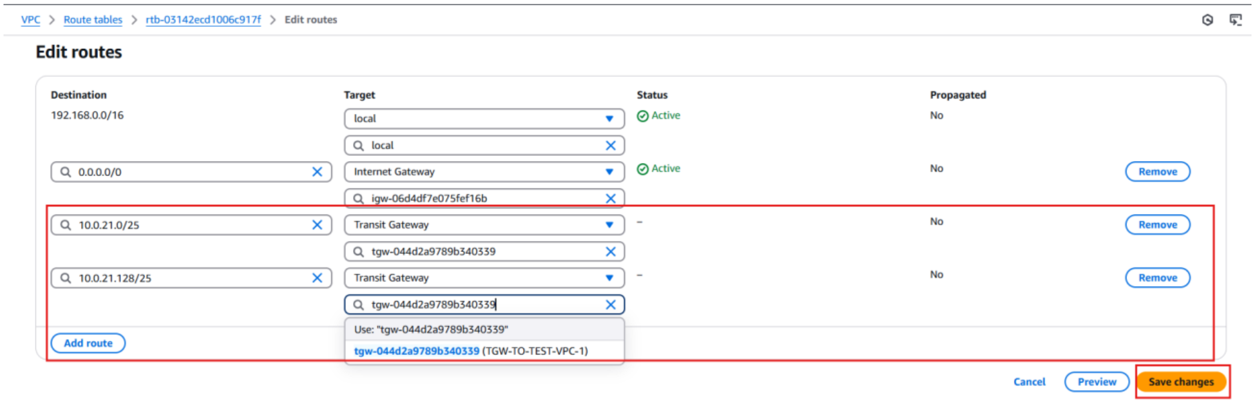
Details Info

Route table ID: rtb-03142ecd1006c917f
Main: Yes
Explicit subnet associations: –
Edge associations: –
VPC: vpc-00811833eba324f0d | TEST-VPC-1
Owner ID: 920814761460

Routes (2)

| Destination | Target | Status | Propagated |
|---|---|---|---|
| 0.0.0.0/0 | igw-06d4df7e075fef16b | Active | No |
| 192.168.0.0/16 | local | Active | No |

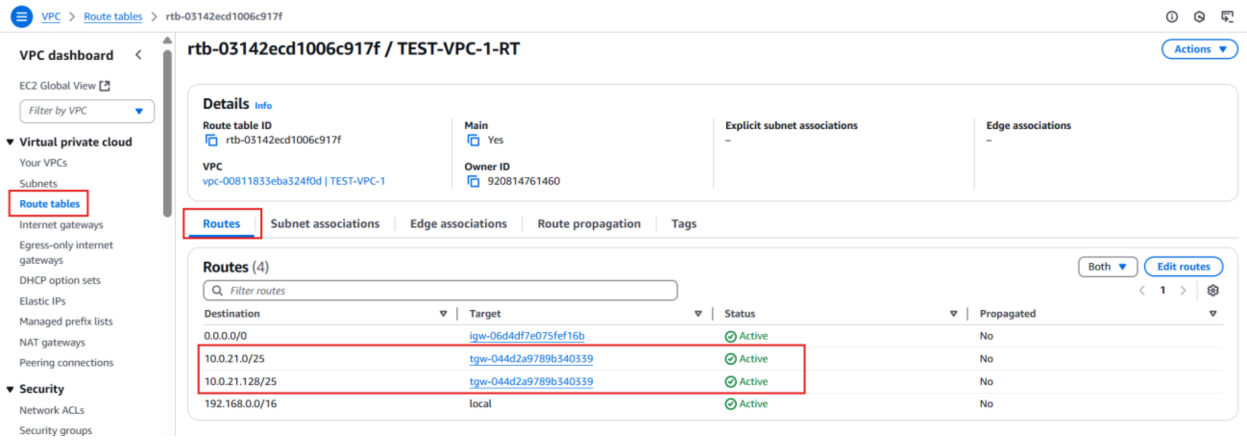
Under destination add the SASE Client pools with the target as TGW and save the changes.


VPC > Route tables > rtb-03142ecd1006c917f > Edit routes
Remove
Add route
Use: "tgw-044d2a9789b340339"
tgw-044d2a9789b340339 (TGW-TO-TEST-VPC-1)
Cancel
Preview
Save changes

Edit routes

| Destination | Target | Status | Propagated |
|---|---|---|---|
| 192.168.0.0/16 | local<br>local | Active | No |
| 0.0.0.0/0 | Internet Gateway<br>igw-06d4df7e075fef16b | Active | No |
| 10.0.21.0/25 | Transit Gateway<br>tgw-044d2a9789b340339 | - | No |
| 10.0.21.128/25 | Transit Gateway<br>tgw-044d2a9789b340339 | - | No |

Once saved the routes should be visible in the Mian Routing table of VPC.



rtb-03142ecd1006c917f / TEST-VPC-1-RT

Details Info

Route table ID: rtb-03142ecd1006c917f
Main: Yes
Explicit subnet associations: –
Edge associations: –
VPC: vpc-00811833eba324f0d | TEST-VPC-1
Owner ID: 920814761460

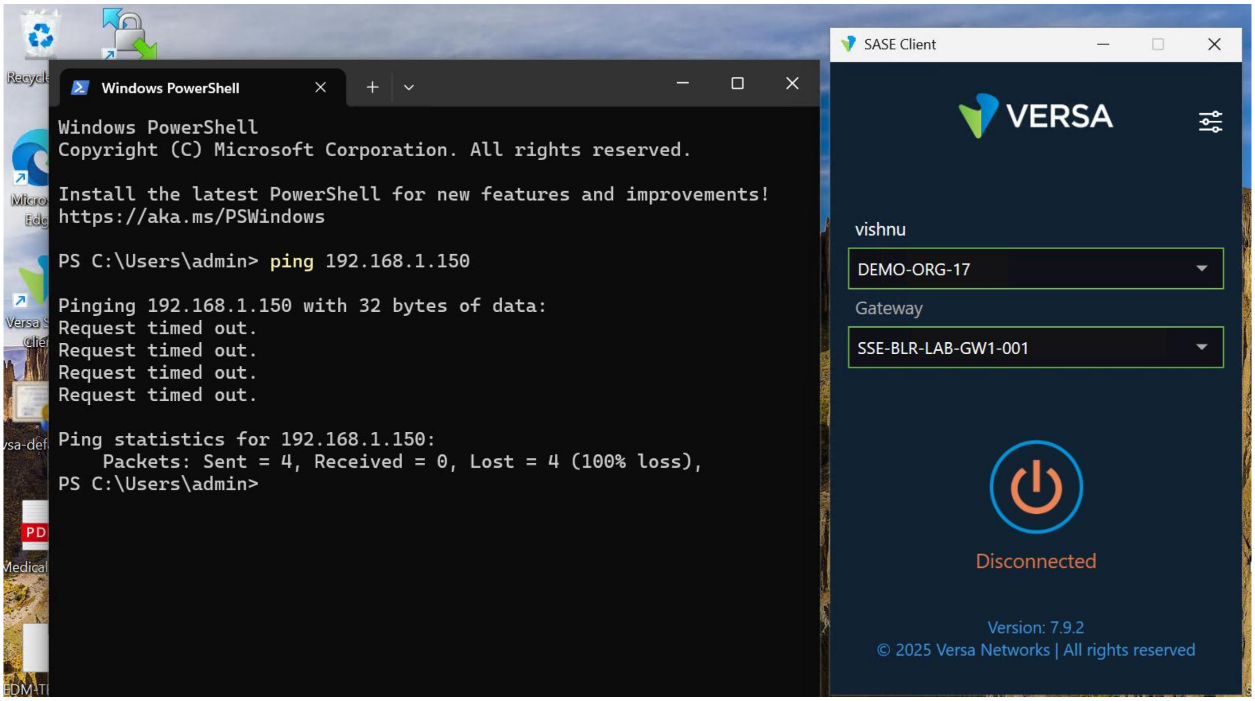
Routes (4)

| Destination | Target | Status | Propagated |
|---|---|---|---|
| 0.0.0.0/0 | igw-06d4df7e075fef16b | Active | No |
| 10.0.21.0/25 | tgw-044d2a9789b340339 | Active | No |
| 10.0.21.128/25 | tgw-044d2a9789b340339 | Active | No |
| 192.168.0.0/16 | local | Active | No |

## Verifying Connectivity:

Accessing EC2 instance with IP: 192.168.1.150 from PC connected to SASE Client.

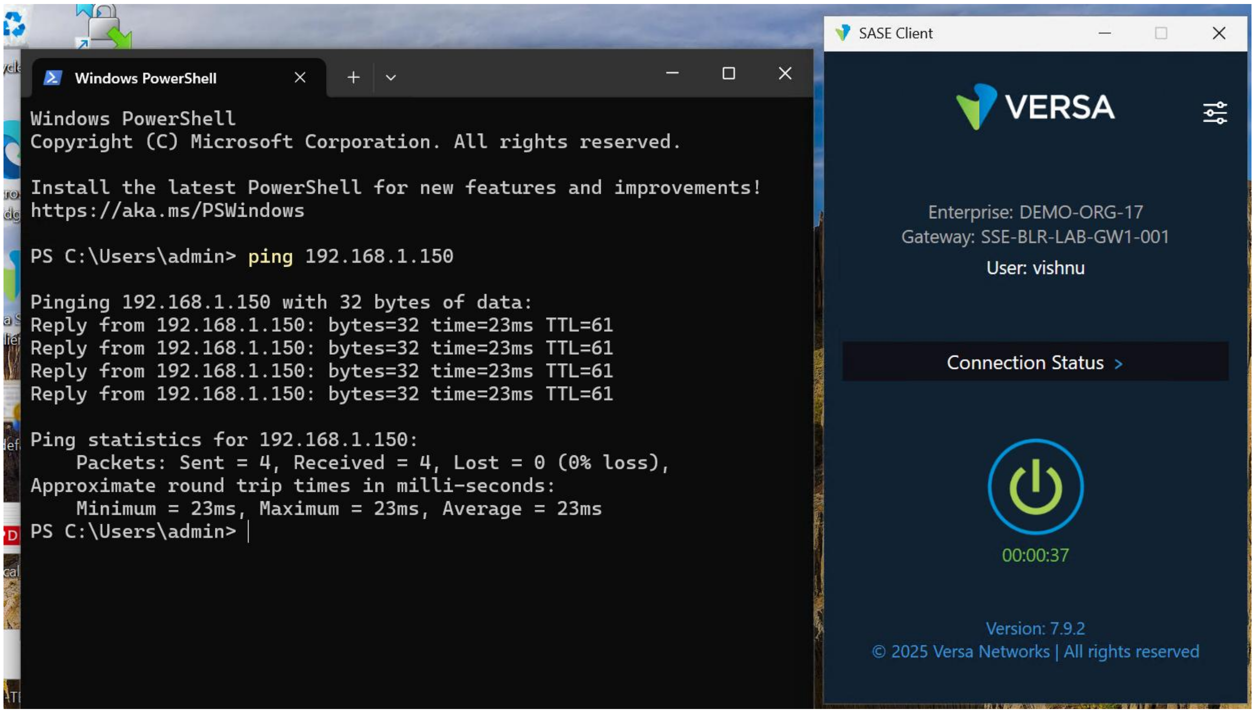
When the SASE Client is not connected to the Gateway, we were unable to reach the EC2 instance in AWS over Private IP.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\admin> ping 192.168.1.150

Pinging 192.168.1.150 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.150:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\admin>
```

vishnu: DEMO-ORG-17
Gateway: SSE-BLR-LAB-GW1-001
Disconnected

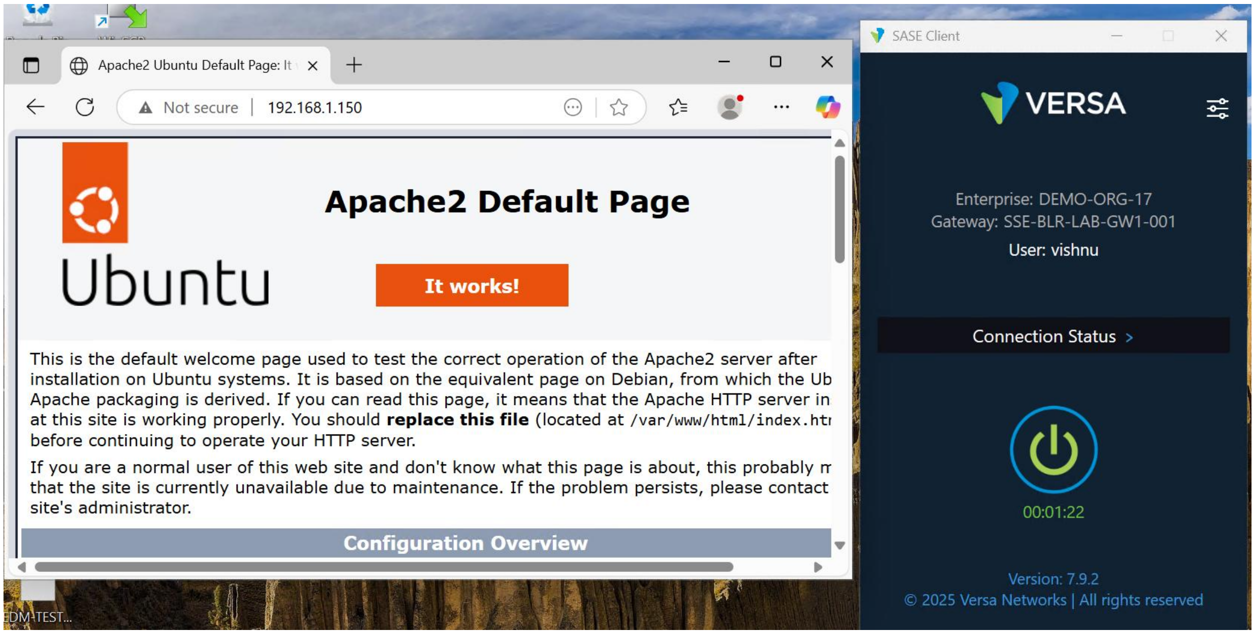
When the SASE Client is connected to the Gateway we were able to reach the EC2 instance in AWS over Private IP.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\admin> ping 192.168.1.150

Pinging 192.168.1.150 with 32 bytes of data:
Reply from 192.168.1.150: bytes=32 time=23ms TTL=61
Reply from 192.168.1.150: bytes=32 time=23ms TTL=61
Reply from 192.168.1.150: bytes=32 time=23ms TTL=61
Reply from 192.168.1.150: bytes=32 time=23ms TTL=61

Ping statistics for 192.168.1.150:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 23ms, Maximum = 23ms, Average = 23ms
PS C:\Users\admin>
```

Enterprise: DEMO-ORG-17
Gateway: SSE-BLR-LAB-GW1-001
User: vishnu

If the EC2 instance is a webserver then you should be able to access the webpage over Private IP.



Apache2 Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ub Apache packaging is derived. If you can read this page, it means that the Apache HTTP server in at this site is working properly. You should **replace this file** (located at `/var/www/html/index.htı` before continuing to operate your HTTP server.

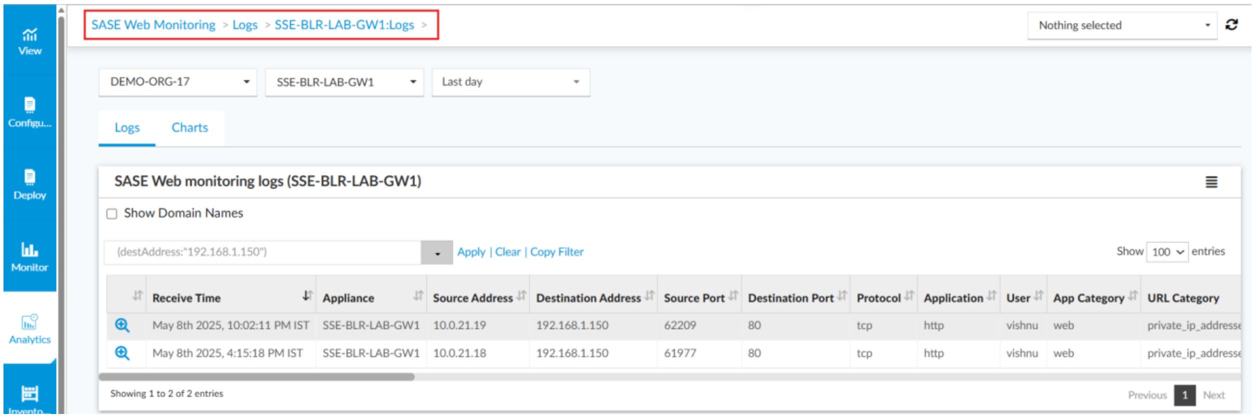
If you are a normal user of this web site and don't know what this page is about, this probably m that the site is currently unavailable due to maintenance. If the problem persists, please contact site's administrator.

Enterprise: DEMO-ORG-17
Gateway: SSE-BLR-LAB-GW1-001
User: vishnu

Apache2 Ubuntu Default Page: It
Not secure | 192.168.1.150
Ubuntu
Configuration Overview
SASE Client
VERSA
Connection Status >
00:01:22
Version: 7.9.2
© 2025 Versa Networks | All rights reserved

### SASE-WEB LOGS on Analytics:

Go to Analytics →Logs → SASE Web Monitoring, select the respective Organization and the SASE Gateway.



SASE Web monitoring logs (SSE-BLR-LAB-GW1)

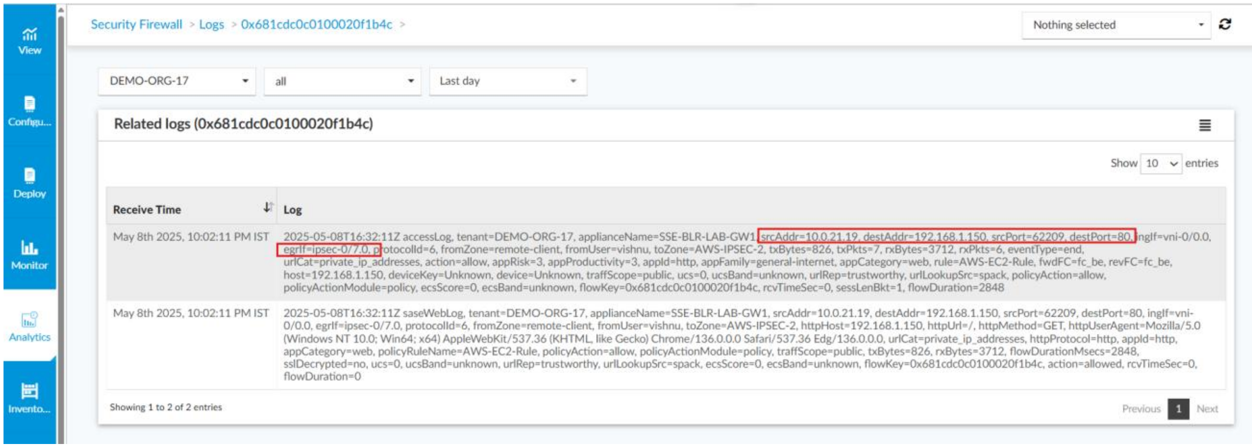
(destAddress:"192.168.1.150")

| | Receive Time | Appliance | Source Address | Destination Address | Source Port | Destination Port | Protocol | Application | User | App Category | URL Category |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | May 8th 2025, 10:02:11 PM IST | SSE-BLR-LAB-GW1 | 10.0.21.19 | 192.168.1.150 | 62209 | 80 | tcp | http | vishnu | web | private_ip_addresse |
| | May 8th 2025, 4:15:18 PM IST | SSE-BLR-LAB-GW1 | 10.0.21.18 | 192.168.1.150 | 61977 | 80 | tcp | http | vishnu | web | private_ip_addresse |

Showing 1 to 2 of 2 entries

Firewall Logs on Concerto (If enabled):

Go to Analytics → Logs → Firewall and select the respective Organization and the SASE Gateway.



Related logs (0x681cdc0c0100020f1b4c)

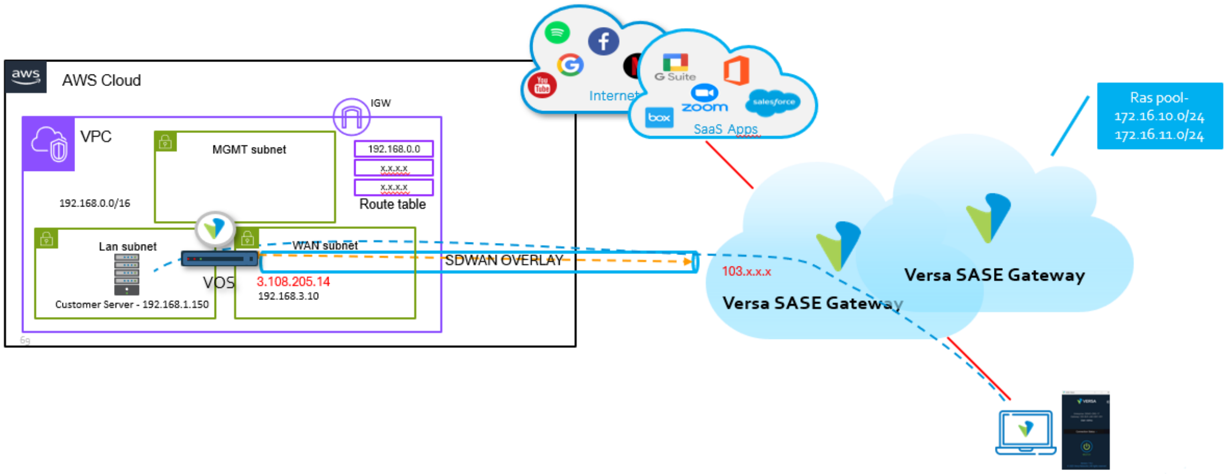
| Receive Time | Log |
|---|---|
| May 8th 2025, 10:02:11 PM IST | 2025-05-08T16:32:11Z accessLog, tenant=DEMO-ORG-17, applianceName=SSE-BLR-LAB-GW1, srcAddr=10.0.21.19, destAddr=192.168.1.150, srcPort=62209, destPort=80, ingIf=vni-0/0.0, egrIf=ipsec-0/7.0, protocolId=6, fromZone=remote-client, fromUser=vishnu, toZone=AWS-IPSEC-2, txBytes=826, txPkts=7, rxBytes=3712, rxPkts=6, eventType=end, urlCat=private_ip_addresses, action=allow, appRisk=3, appProductivity=3, appId=http, appFamily=general-internet, appCategory=web, rule=AWS-EC2-Rule, fwdFC=fc_be, revFC=fc_be, host=192.168.1.150, deviceKey=Unknown, device=Unknown, traffScope=public, ucs=0, ucsBand=unknown, urlRep=trustworthy, urlLookupSrc=spack, policyAction=allow, policyActionModule=policy, ecsScore=0, ecsBand=unknown, flowKey=0x681cdc0c0100020f1b4c, rcvTimeSec=0, sessLenBkt=1, flowDuration=2848 |
| May 8th 2025, 10:02:11 PM IST | 2025-05-08T16:32:11Z saseWebLog, tenant=DEMO-ORG-17, applianceName=SSE-BLR-LAB-GW1, srcAddr=10.0.21.19, destAddr=192.168.1.150, srcPort=62209, destPort=80, ingIf=vni-0/0.0, egrIf=ipsec-0/7.0, protocolId=6, fromZone=remote-client, fromUser=vishnu, toZone=AWS-IPSEC-2, httpHost=192.168.1.150, httpUrl=/, httpMethod=GET, httpUserAgent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36 Edg/136.0.0.0, urlCat=private_ip_addresses, httpProtocol=http, appId=http, appCategory=web, policyRuleName=AWS-EC2-Rule, policyAction=allow, policyActionModule=policy, traffScope=public, txBytes=826, rxBytes=3712, flowDurationMsecs=2848, sslDecrypted=no, ucs=0, ucsBand=unknown, urlRep=trustworthy, urlLookupSrc=spack, ecsScore=0, ecsBand=unknown, flowKey=0x681cdc0c0100020f1b4c, action=allowed, rcvTimeSec=0, flowDuration=0 |

Showing 1 to 2 of 2 entries

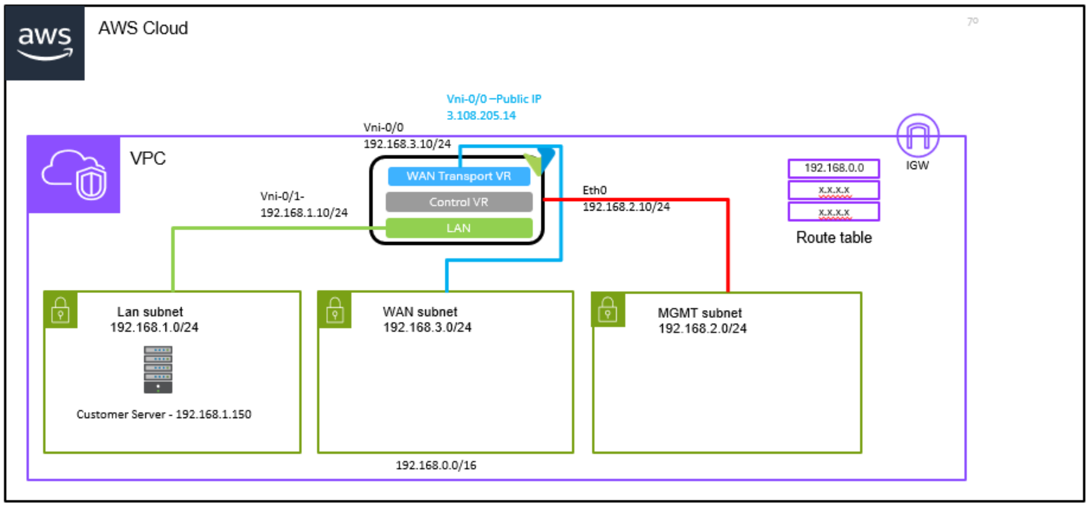
## Option 3 – Versa SDWAN

In this scenario, a dynamic IPsec tunnel is established between the SASE Gateway and the SD-WAN Branch in AWS VPC. The SD-WAN device is responsible for routing traffic between the SASE Client connected to SASE GW and the backend servers hosted in the VPC.

This option can be used when you already have an SD-WAN fabric, and you want to leverage SD-WAN capabilities.



**VOS Topology in AWS:**



## AWS Configuration:

To deploy VOS in AWS we need to create subnets for VOS.

**Note:** Refer Section 4 to 7 for creating VPC, Subnets, IGW and EC2 Instance

### Creating Subnets:

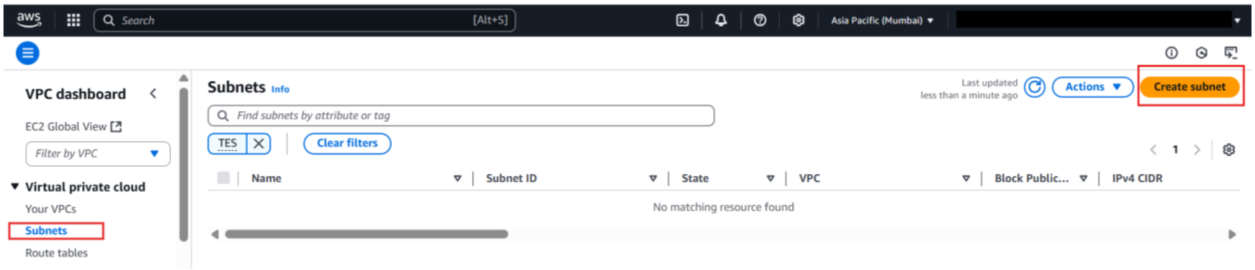
Under the existing VPC create new subnets for VOS.

- Subnet-1—For management interfaces – 192.168.2.10/24

- Subnet-2—For WAN transport interfaces – 192.168.3.10/24
- Subnet-3—For LAN (client-side) interfaces – 192.168.1.10/24

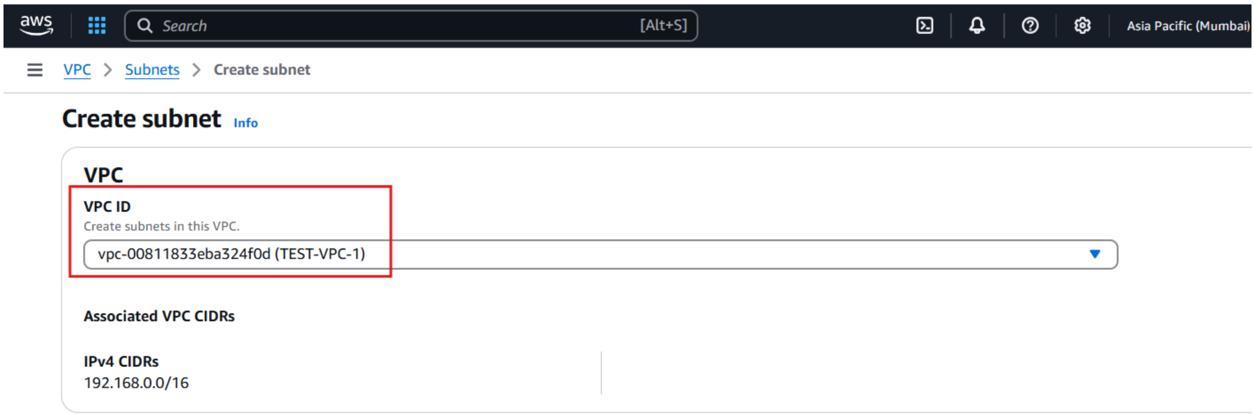
To create Subnets, under VPC dashboard, go to Virtual private Cloud → Subnets → Create Subnet.

Creating Management Subnet.



No matching resource found

Selecting VPC under VPC ID will open Subnet settings.



Create subnet Info

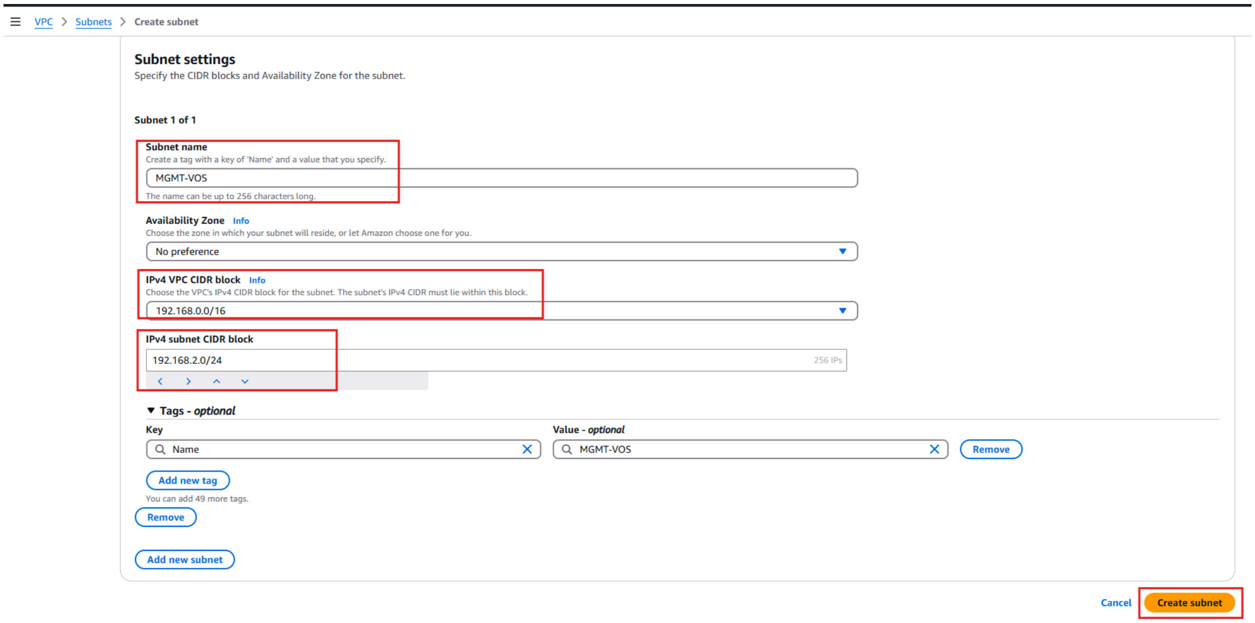
VPC

VPC ID
Create subnets in this VPC.
vpc-00811833eba324f0d (TEST-VPC-1)

Associated VPC CIDRs

IPv4 CIDRs
192.168.0.0/16

Under Subnet settings, provide the Subnet name and the IPv4 subnet CIDR block.



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.
MGMT-VOS
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

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
192.168.0.0/16

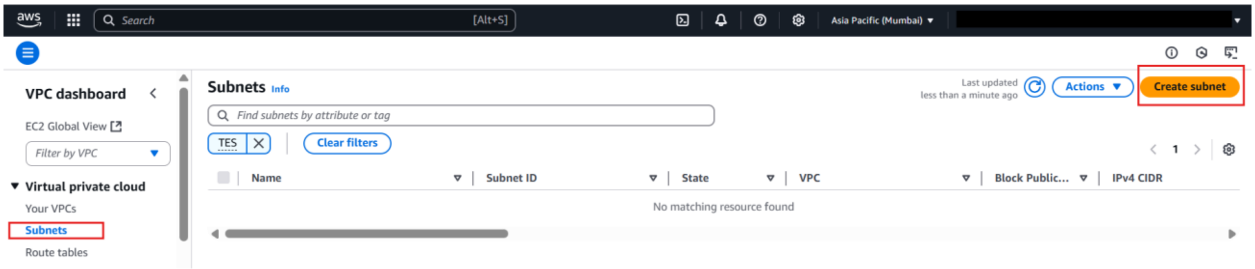
IPv4 subnet CIDR block
192.168.2.0/24 256 IPs

Tags - *optional*

| Key | Value - *optional* |
|---|---|
| Name | MGMT-VOS |

You can add 49 more tags.

Creating WAN Subnet.



[redacted]

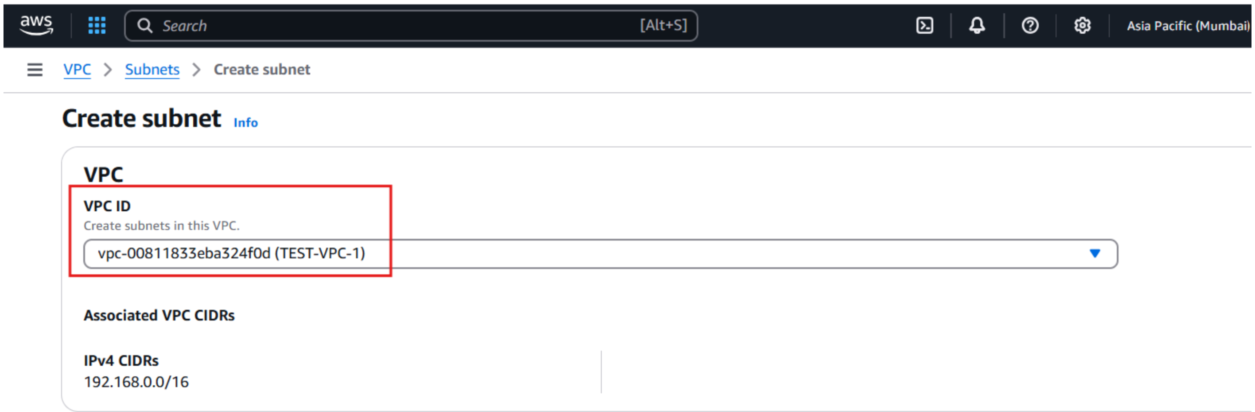
Subnets Info

Last updated less than a minute ago

| □ | Name | Subnet ID | State | VPC | Block Public... | IPv4 CIDR |
|---|---|---|---|---|---|---|

No matching resource found

Selecting VPC under VPC ID will open Subnet settings.



Create subnet Info

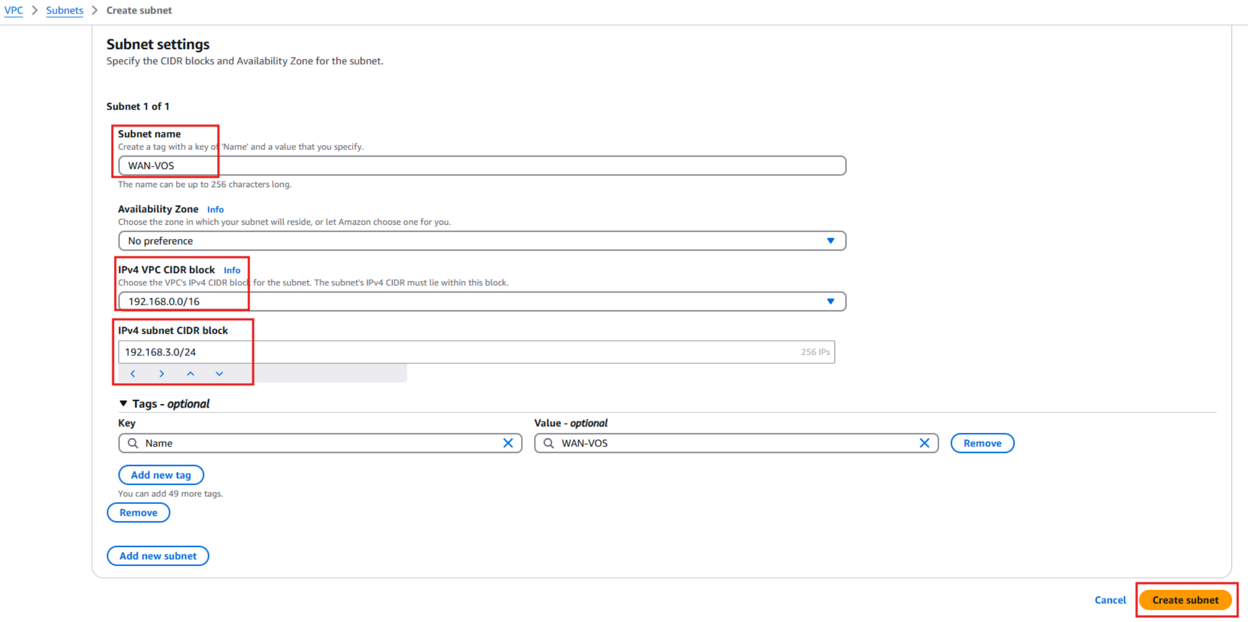
VPC

VPC ID
Create subnets in this VPC.
vpc-00811833eba324f0d (TEST-VPC-1)

Associated VPC CIDRs

IPv4 CIDRs
192.168.0.0/16

Under Subnet settings, provide the Subnet name and the IPv4 subnet CIDR block.



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.
WAN-VOS
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

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
192.168.0.0/16

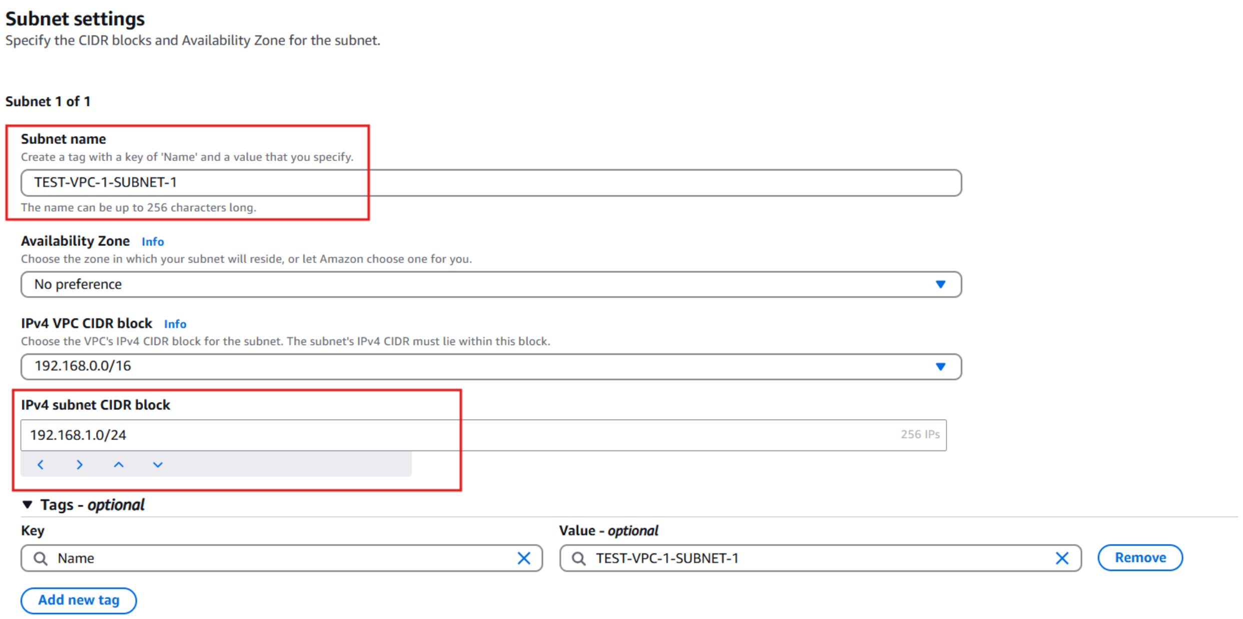
IPv4 subnet CIDR block
192.168.3.0/24 256 IPs

▼ Tags - *optional*

| Key | Value - *optional* |
|---|---|
| Name | WAN-VOS |

You can add 49 more tags.

For LAN subnet we will be reusing the Subnet (TEST-VPC-1-SUBNET-1) which we created earlier as we have EC2 instance already deployed with that subnet.



**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.
TEST-VPC-1-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

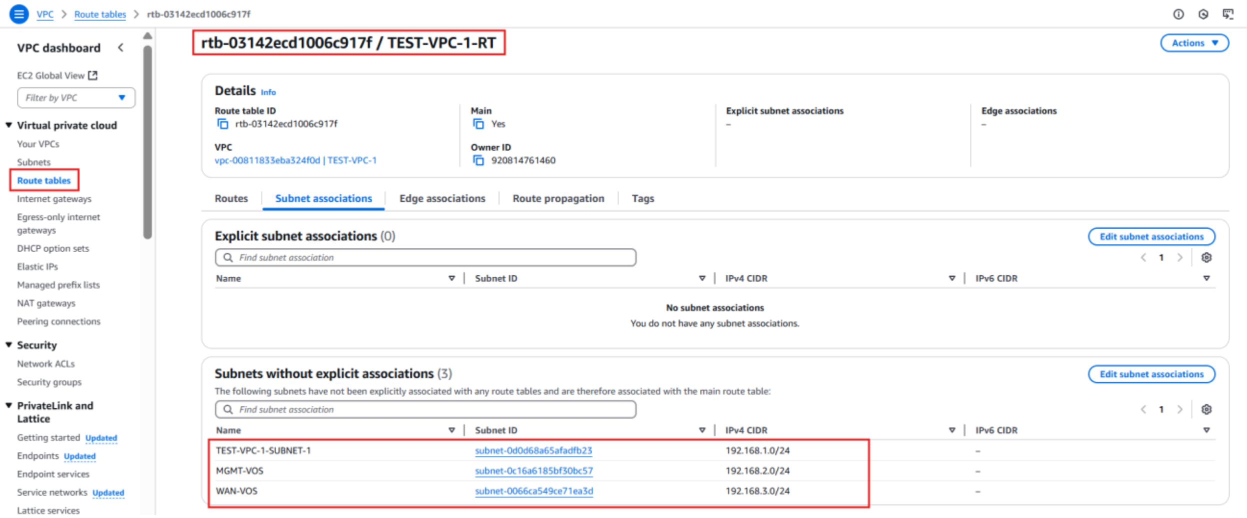
IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
192.168.0.0/16

IPv4 subnet CIDR block
192.168.1.0/24 256 IPs

▼ Tags - *optional*

| Key | Value - *optional* |
|---|---|
| Name | TEST-VPC-1-SUBNET-1 |

Once subnets are created, check the associations in the Main route table.



**rtb-03142ecd1006c917f / TEST-VPC-1-RT**

Details Info

Route table ID: rtb-03142ecd1006c917f
Main: Yes
Explicit subnet associations: –
Edge associations: –
VPC: vpc-00811833eba324f0d | TEST-VPC-1
Owner ID: 920814761460

Explicit subnet associations (0)

| Name | Subnet ID | IPv4 CIDR | IPv6 CIDR |
|---|---|---|---|

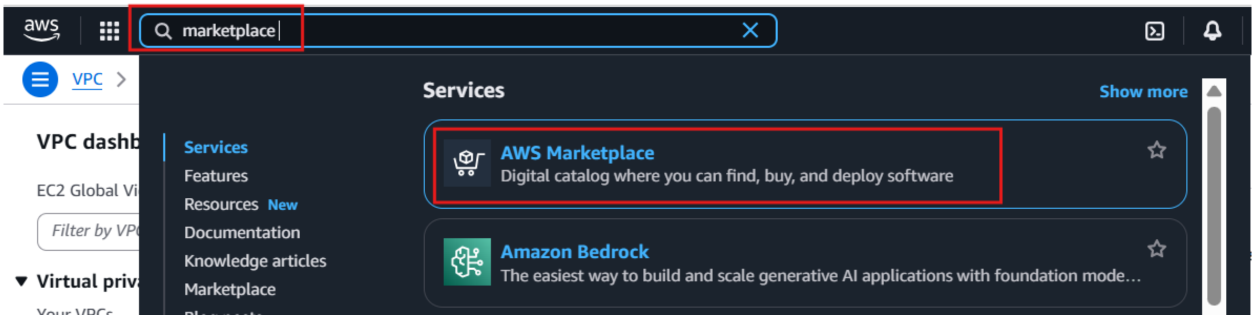
No subnet associations
You do not have any subnet associations.

Subnets without explicit associations (3)
The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

| Name | Subnet ID | IPv4 CIDR | IPv6 CIDR |
|---|---|---|---|
| TEST-VPC-1-SUBNET-1 | subnet-0d0d68a65afadfb23 | 192.168.1.0/24 | – |
| MGMT-VOS | subnet-0c16a6185bf30bc57 | 192.168.2.0/24 | – |
| WAN-VOS | subnet-0066ca549ce71ea3d | 192.168.3.0/24 | – |

## Deploying VOS as EC2 Instance in AWS:

Navigate to the AWS Management Console page, search for Marketplace, and click AWS Marketplace.

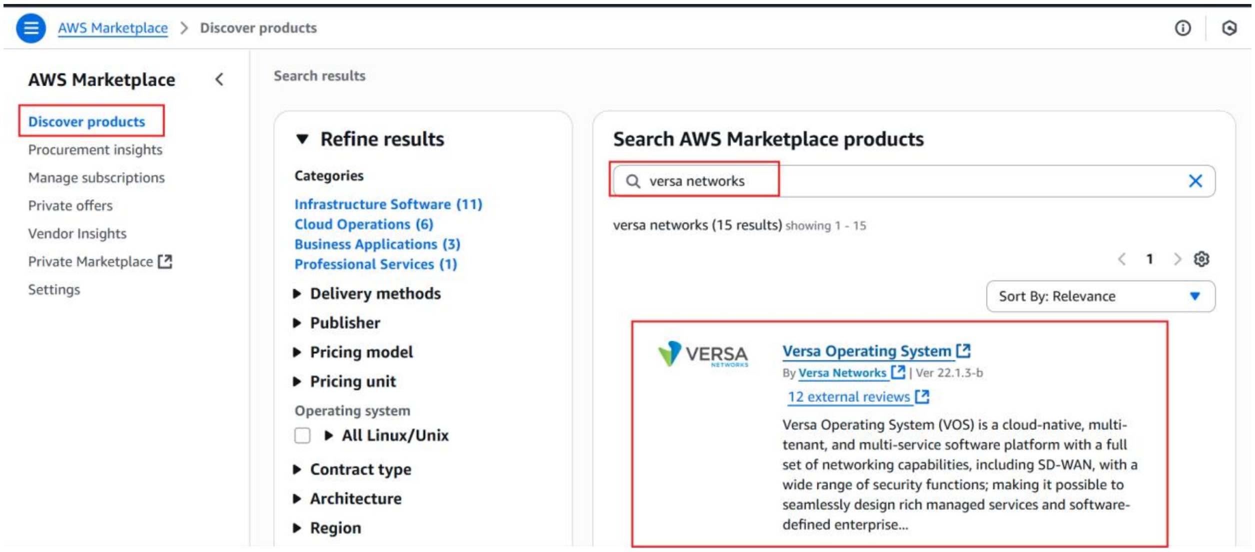


Services

**AWS Marketplace**
Digital catalog where you can find, buy, and deploy software

**Amazon Bedrock**
The easiest way to build and scale generative AI applications with foundation mode...

Under AWS Marketplace, select Discover products and search for “versa networks” and select “Versa Operating System”.



AWS Marketplace > Discover products

**AWS Marketplace**

- Discover products
- Procurement insights
- Manage subscriptions
- Private offers
- Vendor Insights
- Private Marketplace
- Settings

Search results

**Refine results**

Categories

- Infrastructure Software (11)
- Cloud Operations (6)
- Business Applications (3)
- Professional Services (1)

- Delivery methods
- Publisher
- Pricing model
- Pricing unit

Operating system

□ All Linux/Unix

- Contract type
- Architecture
- Region

**Search AWS Marketplace products**

versa networks

versa networks (15 results) showing 1 - 15

Sort By: Relevance

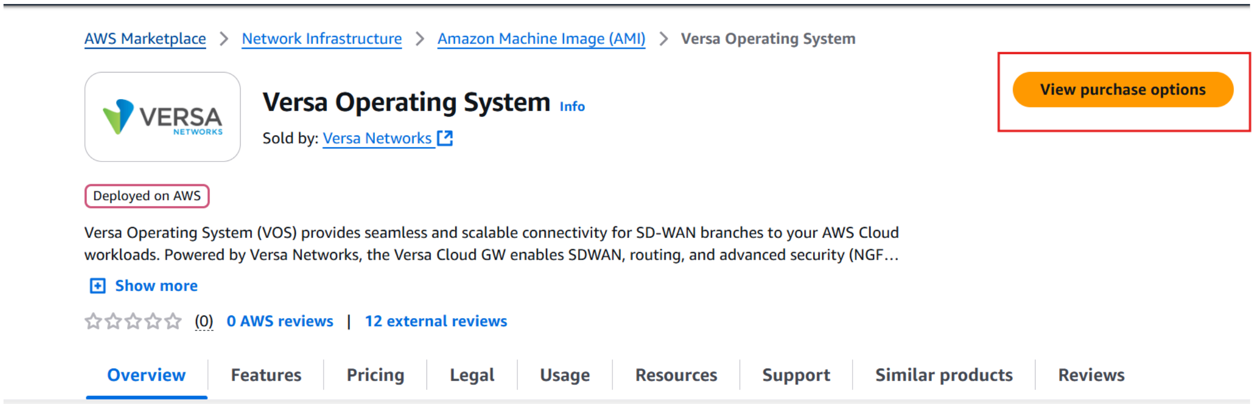
Versa Operating System

By Versa Networks | Ver 22.1.3-b

12 external reviews

Versa Operating System (VOS) is a cloud-native, multi-tenant, and multi-service software platform with a full set of networking capabilities, including SD-WAN, with a wide range of security functions; making it possible to seamlessly design rich managed services and software-defined enterprise...

To Proceed further with click on “View Purchase options”.



AWS Marketplace > Network Infrastructure > Amazon Machine Image (AMI) > Versa Operating System

**Versa Operating System** Info

Sold by: Versa Networks

View purchase options

Deployed on AWS

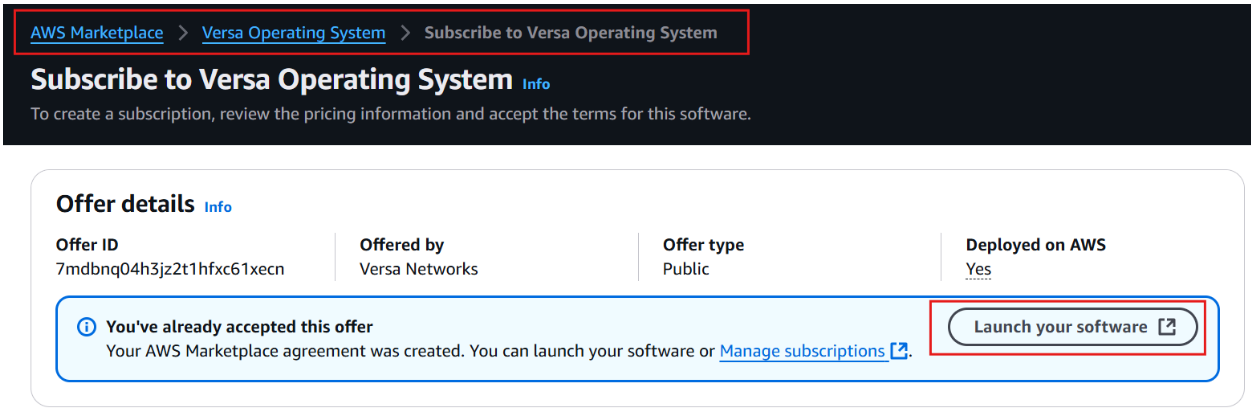
Versa Operating System (VOS) provides seamless and scalable connectivity for SD-WAN branches to your AWS Cloud workloads. Powered by Versa Networks, the Versa Cloud GW enables SDWAN, routing, and advanced security (NGF…

Show more

☆☆☆☆☆ (0) 0 AWS reviews | 12 external reviews

Overview | Features | Pricing | Legal | Usage | Resources | Support | Similar products | Reviews

Under Offer details click on “Launch your software”.



AWS Marketplace > Versa Operating System > Subscribe to Versa Operating System

**Subscribe to Versa Operating System** Info

To create a subscription, review the pricing information and accept the terms for this software.

**Offer details** Info

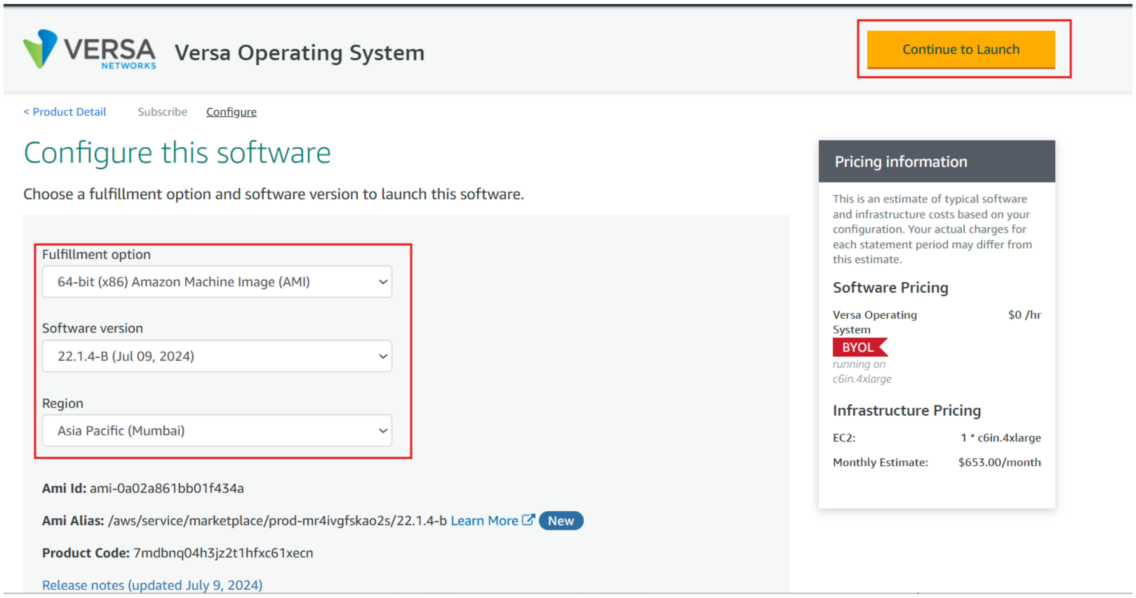
| Offer ID | Offered by | Offer type | Deployed on AWS |
|---|---|---|---|
| 7mdbnq04h3jz2t1hfxc61xecn | Versa Networks | Public | Yes |

**You've already accepted this offer**

Your AWS Marketplace agreement was created. You can launch your software or Manage subscriptions.

Launch your software

Under “Configure this Software”, select the required Software version and Region, then click on “Continue to Launch”.



## Configure this software

Choose a fulfillment option and software version to launch this software.

Fulfillment option: 64-bit (x86) Amazon Machine Image (AMI)

Software version: 22.1.4-B (Jul 09, 2024)

Region: Asia Pacific (Mumbai)

**Ami Id:** ami-0a02a861bb01f434a

**Ami Alias:** /aws/service/marketplace/prod-mr4ivgfskao2s/22.1.4-b Learn More

**Product Code:** 7mdbnq04h3jz2t1hfxc61xecn

Release notes (updated July 9, 2024)

This is an estimate of typical software and infrastructure costs based on your configuration. Your actual charges for each statement period may differ from this estimate.

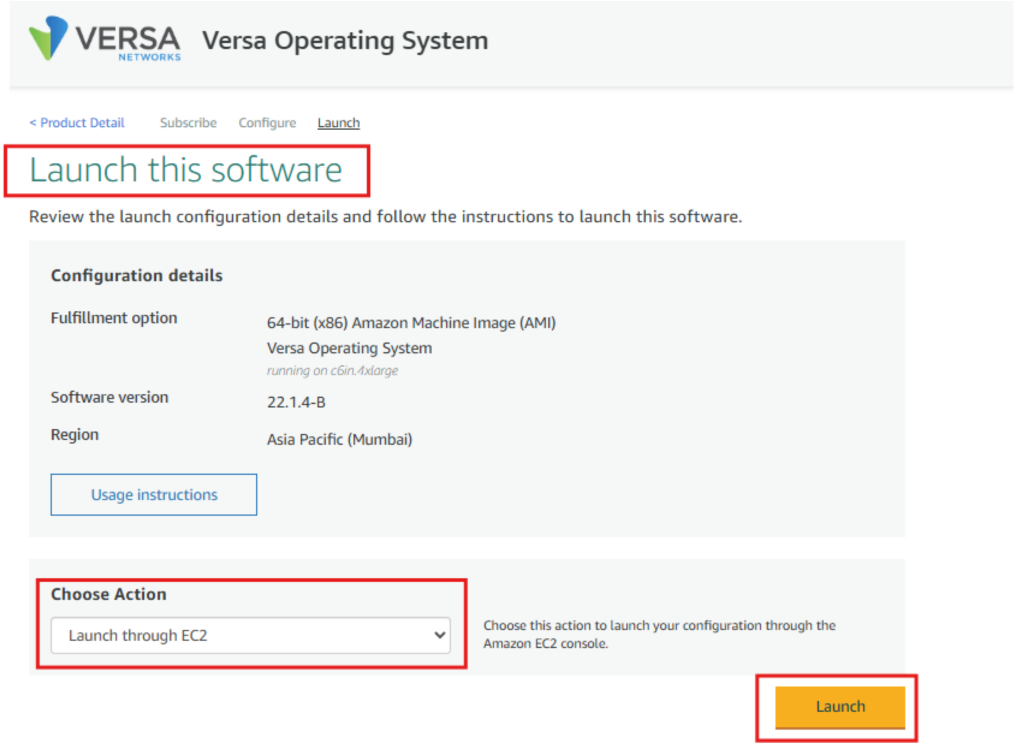
Software Pricing

| | |
|---|---|
| Versa Operating System BYOL *running on c6in.4xlarge* | $0 /hr |

Infrastructure Pricing

| | |
|---|---|
| EC2: | 1 * c6in.4xlarge |
| Monthly Estimate: | $653.00/month |

Under “Launch this software” Choose Action as “Launch through EC2” and click on Launch.



VERSA NETWORKS Versa Operating System

< Product Detail Subscribe Configure Launch

Launch this software

Review the launch configuration details and follow the instructions to launch this software.

**Configuration details**

Fulfillment option: 64-bit (x86) Amazon Machine Image (AMI)
Versa Operating System
*running on c6in.4xlarge*

Software version: 22.1.4-B

Region: Asia Pacific (Mumbai)

Usage instructions

**Choose Action**

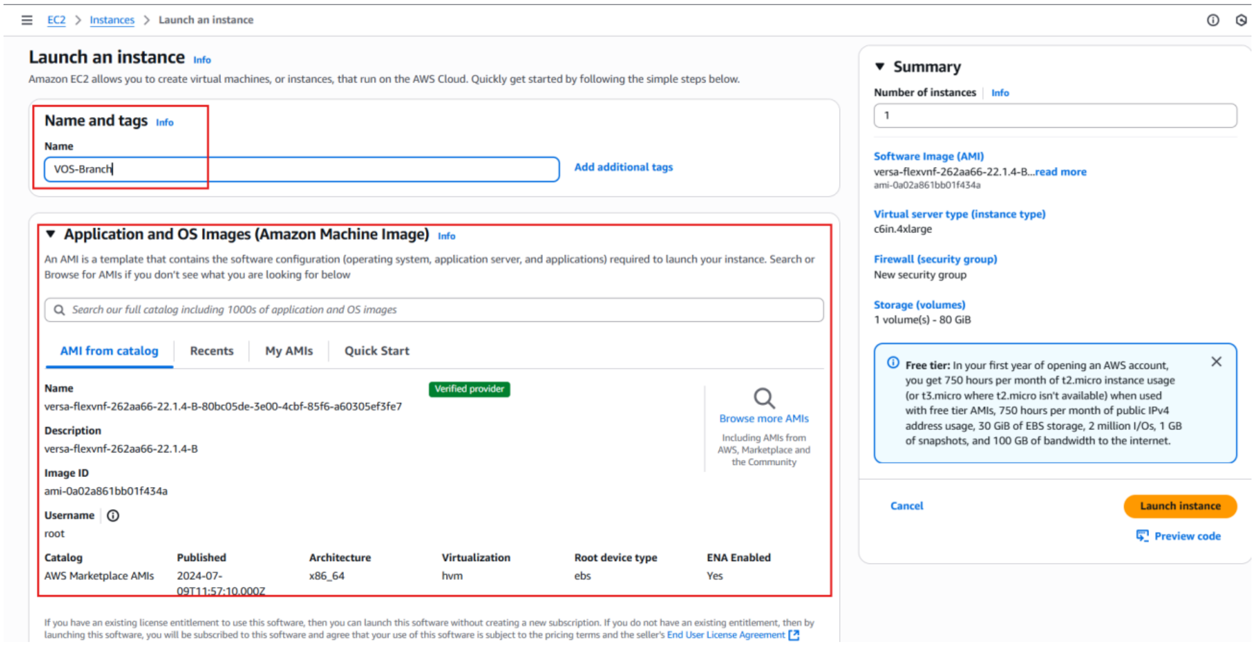
Launch through EC2

Choose this action to launch your configuration through the Amazon EC2 console.

Launch

This will open up EC2 instance dashboard.

Under “Name and tags” provide name for the VOS device and very if AMI information is correct.



EC2 > Instances > Launch an instance

**Launch an instance** Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

**Name and tags** Info

Name: VOS-Branch

Add additional tags

**Application and OS Images (Amazon Machine Image)** Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

*Search our full catalog including 1000s of application and OS images*

AMI from catalog | Recents | My AMIs | Quick Start

Name: versa-flexvnf-262aa66-22.1.4-B-80bc05de-3e00-4cbf-85f6-a60305ef3fe7 Verified provider

Description: versa-flexvnf-262aa66-22.1.4-B

Image ID: ami-0a02a861bb01f434a

Username: root

| Catalog | Published | Architecture | Virtualization | Root device type | ENA Enabled |
|---|---|---|---|---|---|
| AWS Marketplace AMIs | 2024-07-09T11:57:10.000Z | x86_64 | hvm | ebs | Yes |

Browse more AMIs
Including AMIs from AWS, Marketplace and the Community

If you have an existing license entitlement to use this software, then you can launch this software without creating a new subscription. If you do not have an existing entitlement, then by launching this software, you will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's End User License Agreement

**Summary**

Number of instances: 1

Software Image (AMI): versa-flexvnf-262aa66-22.1.4-B...read more
ami-0a02a861bb01f434a

Virtual server type (instance type): c6in.4xlarge

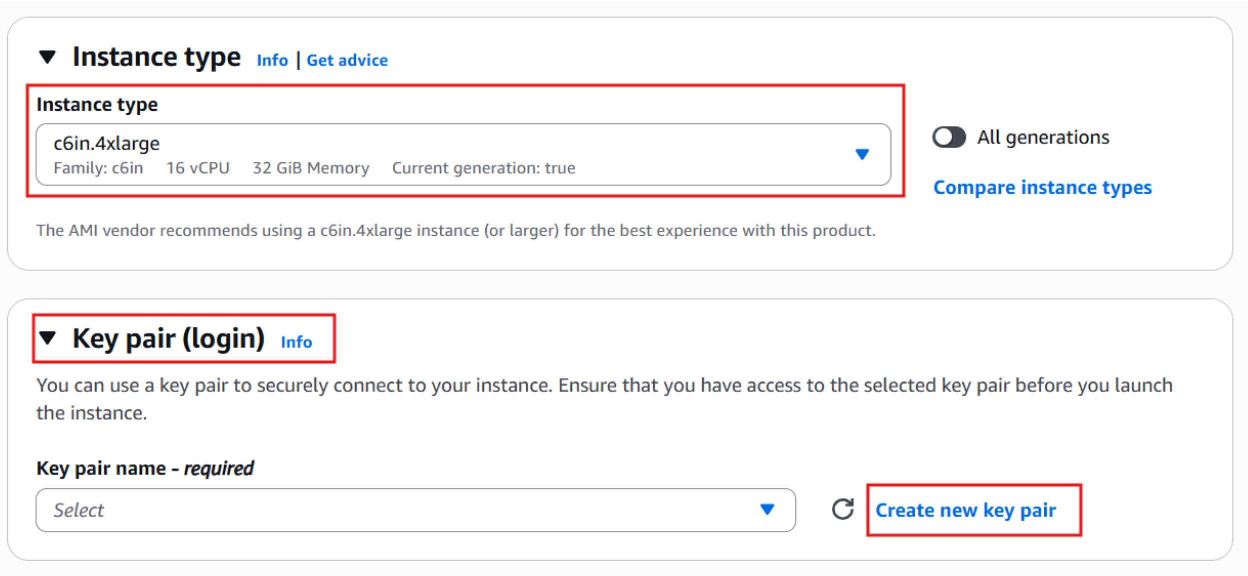
Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 80 GiB

**Free tier:** In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel | Launch instance | Preview code

“Instance type” is selected by default and under Key pair select “Create new key pair”.



Instance type Info | Get advice

Instance type

c6in.4xlarge
Family: c6in 16 vCPU 32 GiB Memory Current generation: true

All generations

Compare instance types

The AMI vendor recommends using a c6in.4xlarge instance (or larger) for the best experience with this product.

Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

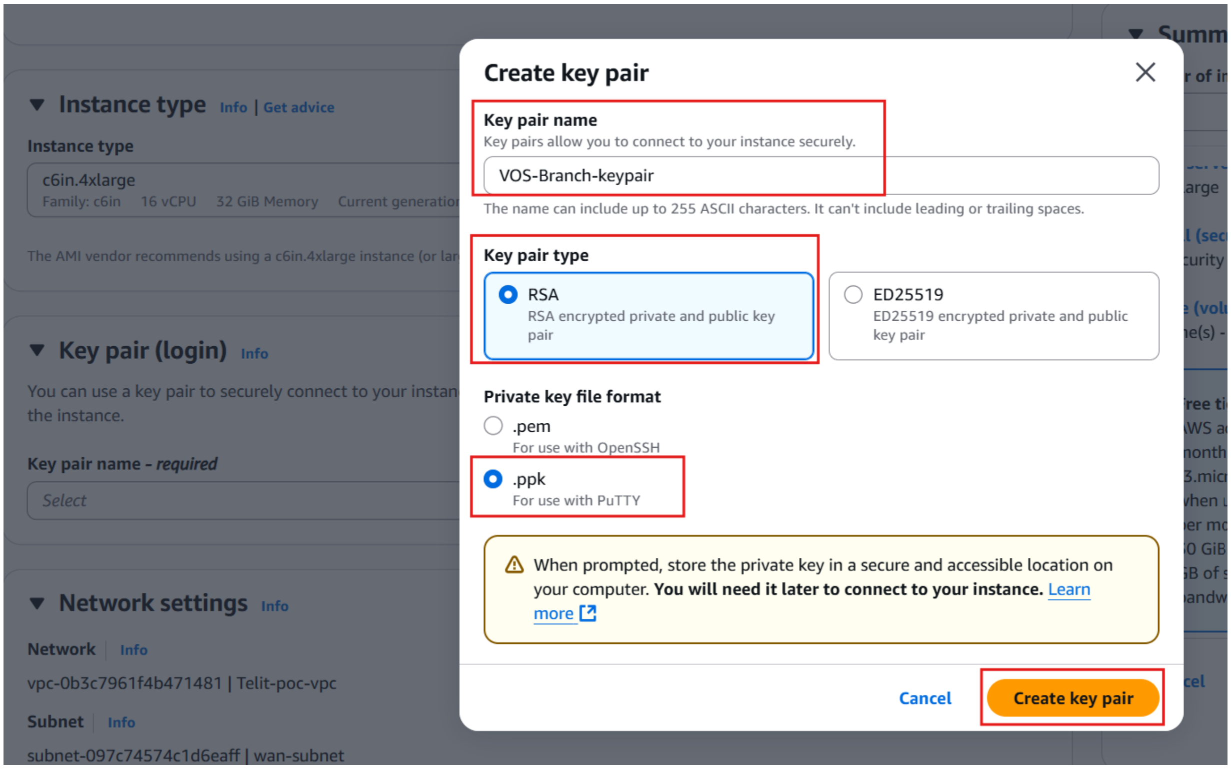
Key pair name - *required*

*Select*

Create new key pair

**Note:** Refer the link for Qualified AWS Instances and select the instance type as per the requirement. https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Deployment_Basics/Qualified_AWS%2C_Azure%2C_and_Google_Cloud_Instances

Under “Create key pair”, provide a name, select key pair



Create key pair

Key pair name
Key pairs allow you to connect to your instance securely.

VOS-Branch-keypair

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

● RSA
RSA encrypted private and public key pair

○ ED25519
ED25519 encrypted private and public key pair

Private key file format

○ .pem
For use with OpenSSH

● .ppk
For use with PuTTY

When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** Learn more

Cancel

Create key pair

Network settings Info

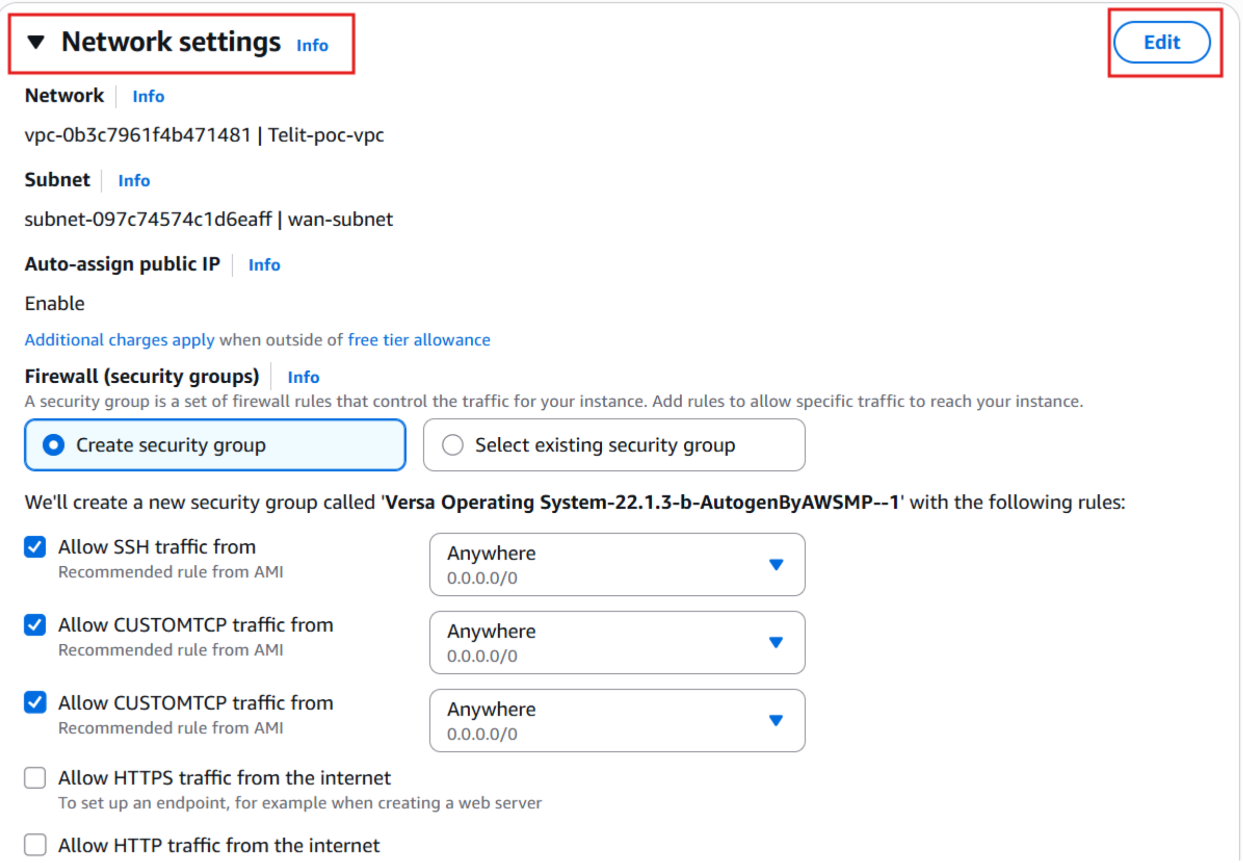
Network Info

vpc-0b3c7961f4b471481 | Telit-poc-vpc

Subnet Info

subnet-097c74574c1d6eaff | wan-subnet

Under “Network settings” click on Edit.



▼ **Network settings** Info

Edit

**Network** | Info

vpc-0b3c7961f4b471481 | Telit-poc-vpc

**Subnet** | Info

subnet-097c74574c1d6eaff | wan-subnet

**Auto-assign public IP** | Info

Enable

Additional charges apply when outside of free tier allowance

**Firewall (security groups)** | Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

We'll create a new security group called '**Versa Operating System-22.1.3-b-AutogenByAWSMP--1**' with the following rules:

☑ Allow SSH traffic from — Anywhere 0.0.0.0/0
Recommended rule from AMI

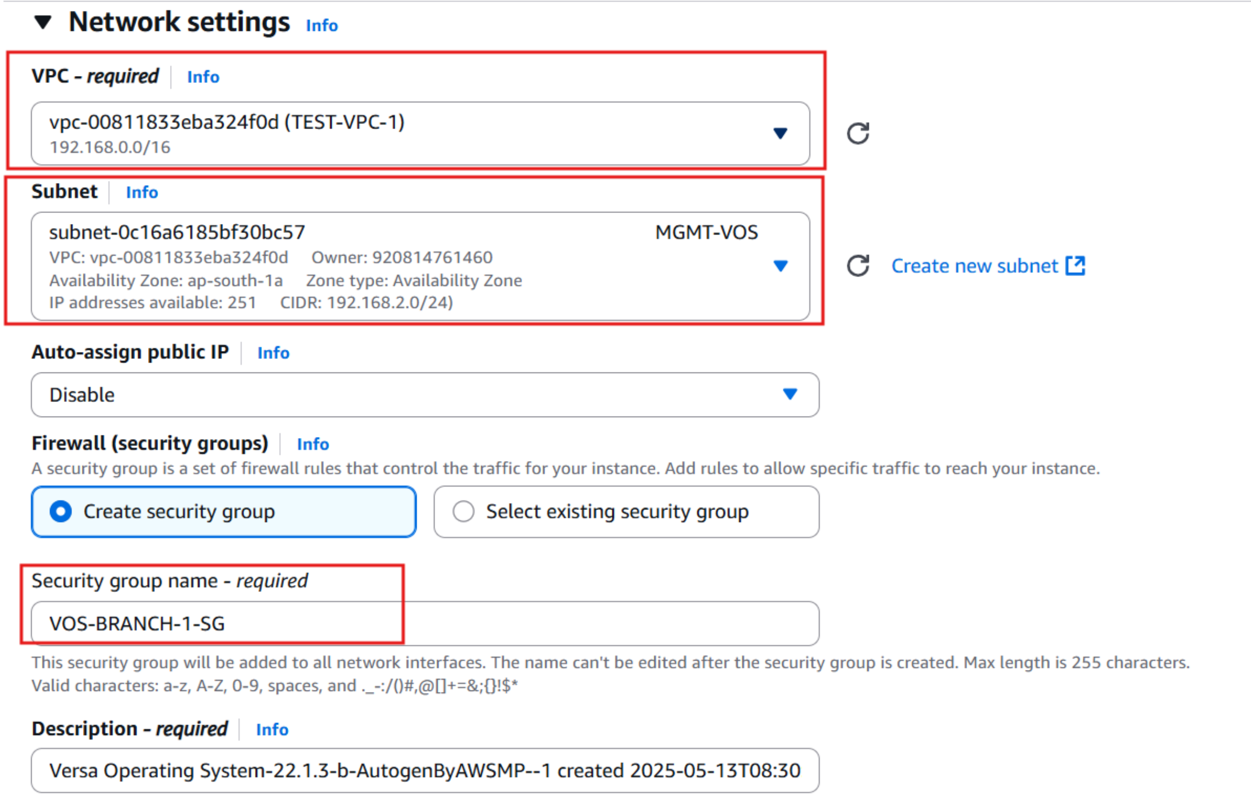
☑ Allow CUSTOMTCP traffic from — Anywhere 0.0.0.0/0
Recommended rule from AMI

☑ Allow CUSTOMTCP traffic from — Anywhere 0.0.0.0/0
Recommended rule from AMI

□ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

□ Allow HTTP traffic from the internet

Under VPC, select the VPC which you have created, select the required subnet and modify the security group name.



▼ **Network settings** Info

**VPC - *required*** | Info

vpc-00811833eba324f0d (TEST-VPC-1)
192.168.0.0/16

**Subnet** | Info

subnet-0c16a6185bf30bc57 MGMT-VOS
VPC: vpc-00811833eba324f0d Owner: 920814761460
Availability Zone: ap-south-1a Zone type: Availability Zone
IP addresses available: 251 CIDR: 192.168.2.0/24)

Create new subnet

**Auto-assign public IP** | Info

Disable

**Firewall (security groups)** | Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

Security group name - *required*

VOS-BRANCH-1-SG

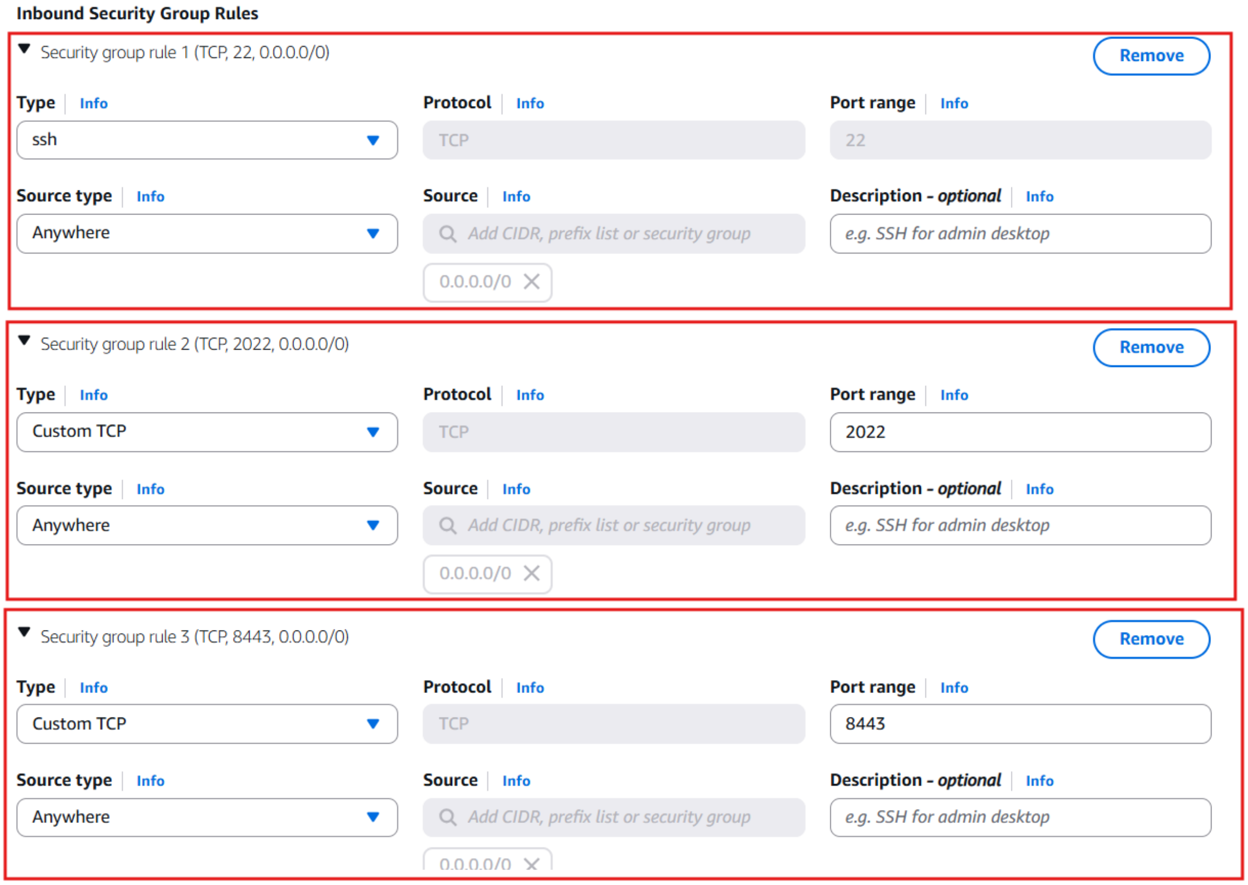
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters.
Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

**Description - *required*** | Info

Versa Operating System-22.1.3-b-AutogenByAWSMP--1 created 2025-05-13T08:30

Security Groups act as virtual firewalls, controlling the flow of network traffic to and from EC2 instances within a VPC. They are a key part of AWS's security, helping to ensure only authorized traffic can reach your instances. Security Groups work by defining rules that specify which types of traffic (TCP, UDP, ICMP) and on which ports are allowed to pass through.

Ensure that all required ports are permitted under the 'Inbound Security Group Rules'. By default, all outbound traffic from VOS is allowed. When VOS is launched from the Marketplace, it comes with a set of predefined inbound rules



**Inbound Security Group Rules**

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)

Type: ssh
Protocol: TCP
Port range: 22
Source type: Anywhere
Source: Add CIDR, prefix list or security group — 0.0.0.0/0
Description - *optional*: *e.g. SSH for admin desktop*

▼ Security group rule 2 (TCP, 2022, 0.0.0.0/0)

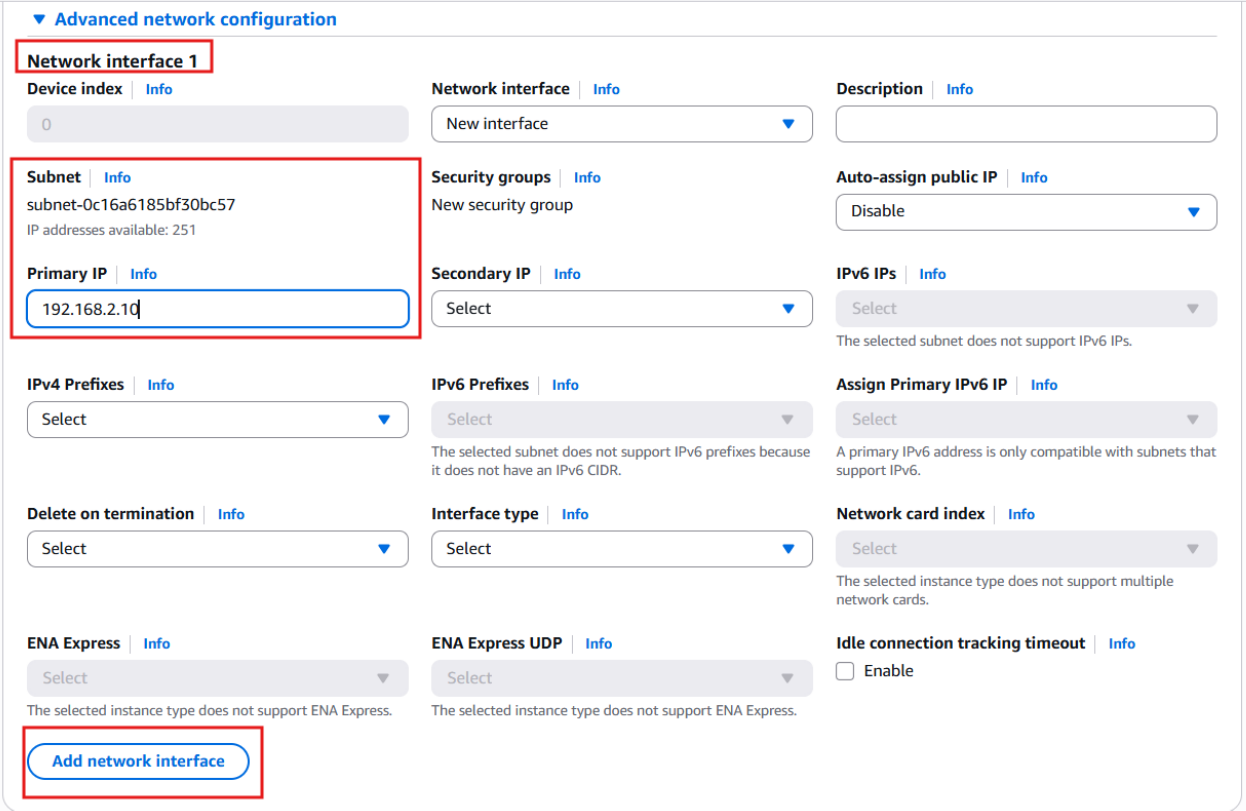
Type: Custom TCP
Protocol: TCP
Port range: 2022
Source type: Anywhere
Source: Add CIDR, prefix list or security group — 0.0.0.0/0
Description - *optional*: *e.g. SSH for admin desktop*

▼ Security group rule 3 (TCP, 8443, 0.0.0.0/0)

Type: Custom TCP
Protocol: TCP
Port range: 8443
Source type: Anywhere
Source: Add CIDR, prefix list or security group — 0.0.0.0/0
Description - *optional*: *e.g. SSH for admin desktop*

**Note:** Refer to the provided link for the list of firewall ports that need to be allowed in AWS Security Groups to ensure VOS is reachable from the Headend https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Deployment_Basics/Firewall_Requirements#VOS_Device_Firewall_Requirements

Click Advanced Network configuration. For the first network interface, select the management subnet that you created earlier, and then click Add Network Interface.



▼ Advanced network configuration

Network interface 1

Device index | Info
0

Network interface | Info
New interface ▼

Description | Info

Subnet | Info
subnet-0c16a6185bf30bc57
IP addresses available: 251

Security groups | Info
New security group

Auto-assign public IP | Info
Disable ▼

Primary IP | Info
192.168.2.10

Secondary IP | Info
Select ▼

IPv6 IPs | Info
Select ▼
The selected subnet does not support IPv6 IPs.

IPv4 Prefixes | Info
Select ▼

IPv6 Prefixes | Info
Select ▼
The selected subnet does not support IPv6 prefixes because it does not have an IPv6 CIDR.

Assign Primary IPv6 IP | Info
Select ▼
A primary IPv6 address is only compatible with subnets that support IPv6.

Delete on termination | Info
Select ▼

Interface type | Info
Select ▼

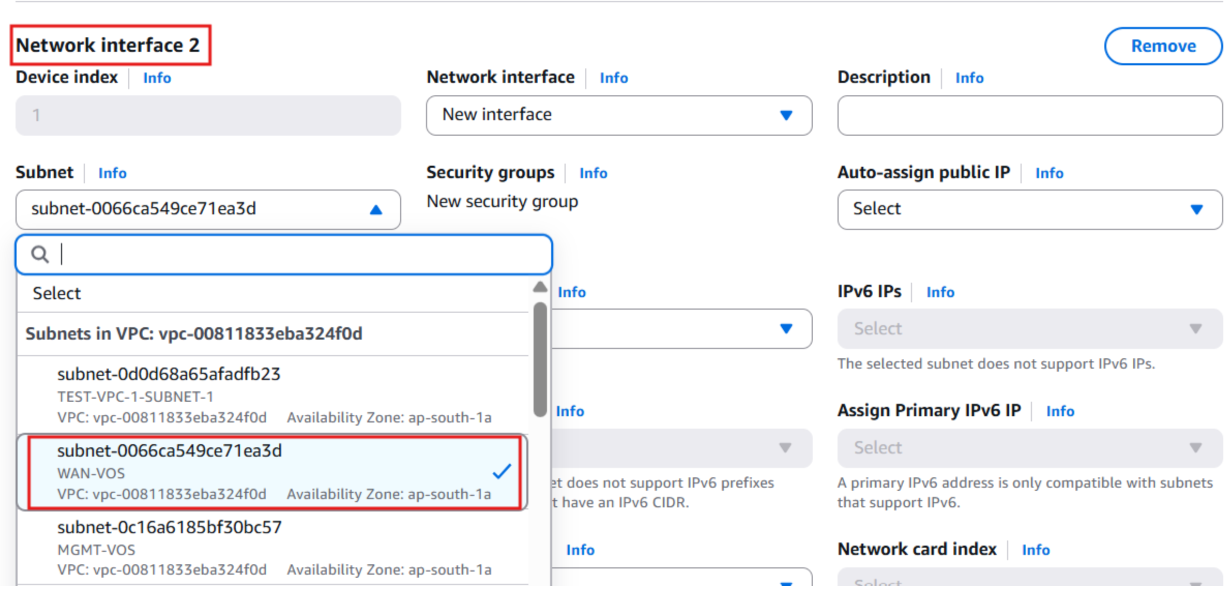
Network card index | Info
Select ▼
The selected instance type does not support multiple network cards.

ENA Express | Info
Select ▼
The selected instance type does not support ENA Express.

ENA Express UDP | Info
Select ▼
The selected instance type does not support ENA Express.

Idle connection tracking timeout | Info
□ Enable

Under Network Interface 2, select the WAN subnet and provide an IP address and click on “Add network interface”.



Network interface 2

Remove

Device index | Info
1

Network interface | Info
New interface ▼

Description | Info

Subnet | Info
subnet-0066ca549ce71ea3d ▲

Select

Subnets in VPC: vpc-00811833eba324f0d

subnet-0d0d68a65afadfb23
TEST-VPC-1-SUBNET-1
VPC: vpc-00811833eba324f0d Availability Zone: ap-south-1a

subnet-0066ca549ce71ea3d ✓
WAN-VOS
VPC: vpc-00811833eba324f0d Availability Zone: ap-south-1a

subnet-0c16a6185bf30bc57
MGMT-VOS
VPC: vpc-00811833eba324f0d Availability Zone: ap-south-1a

Security groups | Info
New security group

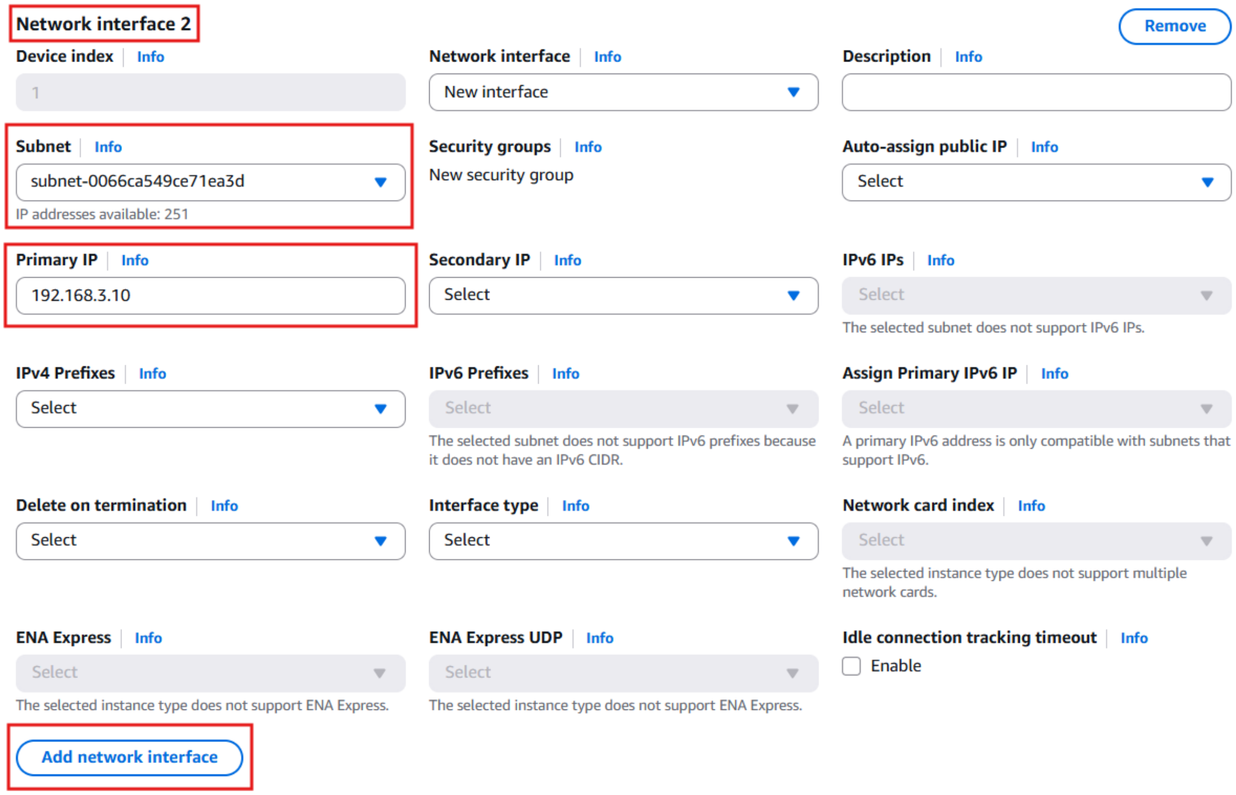
Auto-assign public IP | Info
Select ▼

IPv6 IPs | Info
Select ▼
The selected subnet does not support IPv6 IPs.

Assign Primary IPv6 IP | Info
Select ▼
A primary IPv6 address is only compatible with subnets that support IPv6.

et does not support IPv6 prefixes
t have an IPv6 CIDR.

Network card index | Info



Network interface 2

Remove

Device index | Info
1

Network interface | Info
New interface ▼

Description | Info

Subnet | Info
subnet-0066ca549ce71ea3d ▼
IP addresses available: 251

Security groups | Info
New security group

Auto-assign public IP | Info
Select ▼

Primary IP | Info
192.168.3.10

Secondary IP | Info
Select ▼

IPv6 IPs | Info
Select ▼
The selected subnet does not support IPv6 IPs.

IPv4 Prefixes | Info
Select ▼

IPv6 Prefixes | Info
Select ▼
The selected subnet does not support IPv6 prefixes because it does not have an IPv6 CIDR.

Assign Primary IPv6 IP | Info
Select ▼
A primary IPv6 address is only compatible with subnets that support IPv6.

Delete on termination | Info
Select ▼

Interface type | Info
Select ▼

Network card index | Info
Select ▼
The selected instance type does not support multiple network cards.

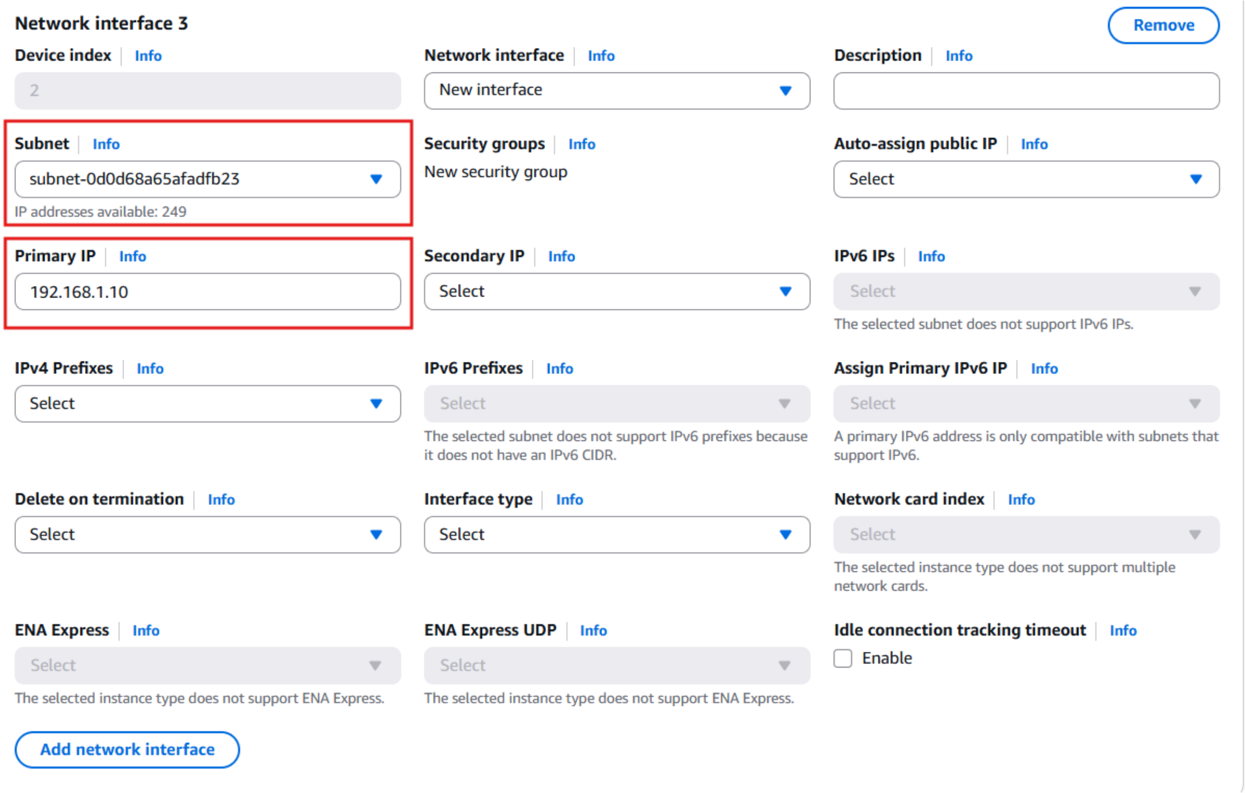
ENA Express | Info
Select ▼
The selected instance type does not support ENA Express.

ENA Express UDP | Info
Select ▼
The selected instance type does not support ENA Express.

Idle connection tracking timeout | Info
□ Enable

Add network interface

Under Network Interface 3, select the LAN subnet which we have created and provide an IP address.



Network interface 3

Device index: 2

Network interface: New interface

Description:

Subnet: subnet-0d0d68a65afadfb23

IP addresses available: 249

Security groups: New security group

Auto-assign public IP: Select

Primary IP: 192.168.1.10

Secondary IP: Select

IPv6 IPs: Select

The selected subnet does not support IPv6 IPs.

IPv4 Prefixes: Select

IPv6 Prefixes: Select

The selected subnet does not support IPv6 prefixes because it does not have an IPv6 CIDR.

Assign Primary IPv6 IP: Select

A primary IPv6 address is only compatible with subnets that support IPv6.

Delete on termination: Select

Interface type: Select

Network card index: Select

The selected instance type does not support multiple network cards.

ENA Express: Select

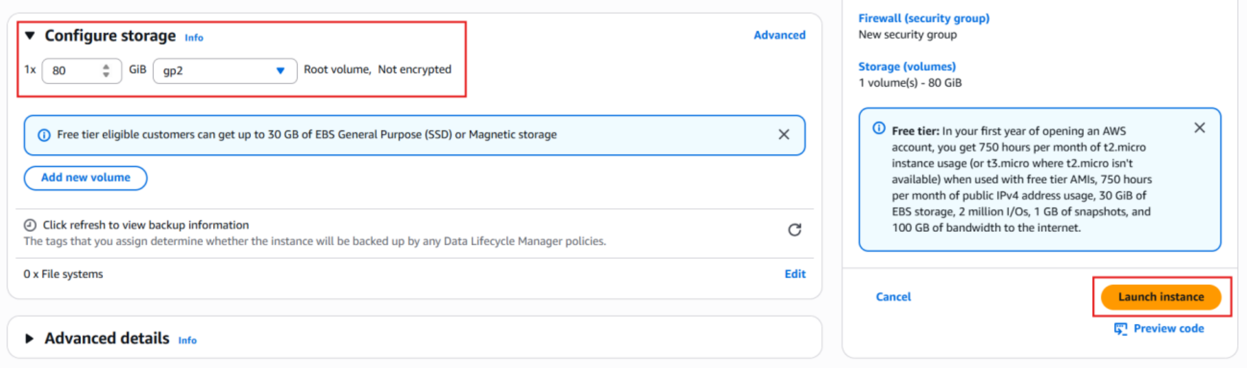
The selected instance type does not support ENA Express.

ENA Express UDP: Select

The selected instance type does not support ENA Express.

Idle connection tracking timeout: □ Enable

In the Configure Storage section, the 80-GiB root volume is selected by default.



Configure storage

1x 80 GiB gp2 Root volume, Not encrypted

ⓘ Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Click refresh to view backup information

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems

Advanced details

Firewall (security group)

New security group

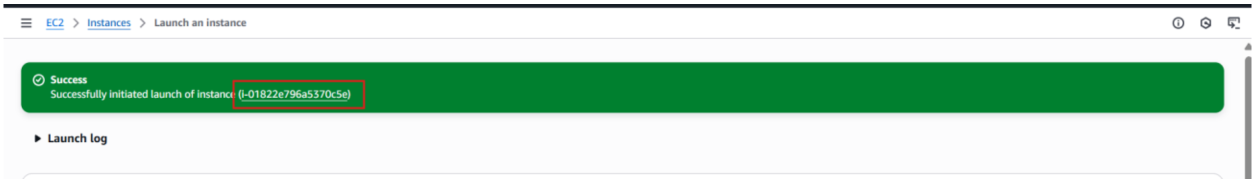
Storage (volumes)

1 volume(s) - 80 GiB

ⓘ **Free tier:** In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Once all the configuration is complete, click on Launch instance.

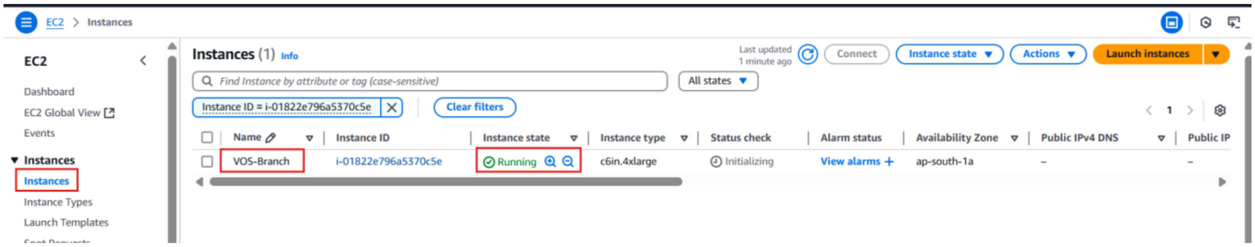
Once the instance is created click on the instance ID to view the EC2 instance created.



EC2 > Instances > Launch an instance

Success

Successfully initiated launch of instance (i-01822e796a5370c5e)



| □ | Name | Instance ID | Instance state | Instance type | Status check | Alarm status | Availability Zone | Public IPv4 DNS | Public IP |
|---|---|---|---|---|---|---|---|---|---|
| □ | VOS-Branch | i-01822e796a5370c5e | Running | c6in.4xlarge | Initializing | View alarms + | ap-south-1a | – | – |

## Associating Elastic IP Address with an Interface:

### Elastic IP Address:

An Elastic IP address in AWS is a static, public IPv4 address that you can associate with any instance or network interface within your Virtual Private Cloud (VPC). It's designed for dynamic cloud environments where EC2 instances might be stopped, started, or even terminated, ensuring that the public IP remains consistent.

### Purpose in This Use Case:

- Elastic IPs are assigned to the SD-WAN device’s management interface to enable SSH access for onboarding and remote administration.
- Used on WAN interfaces of SD-WAN device to establish Connectivity to Headend components and the SASE Gateway.

### Note:

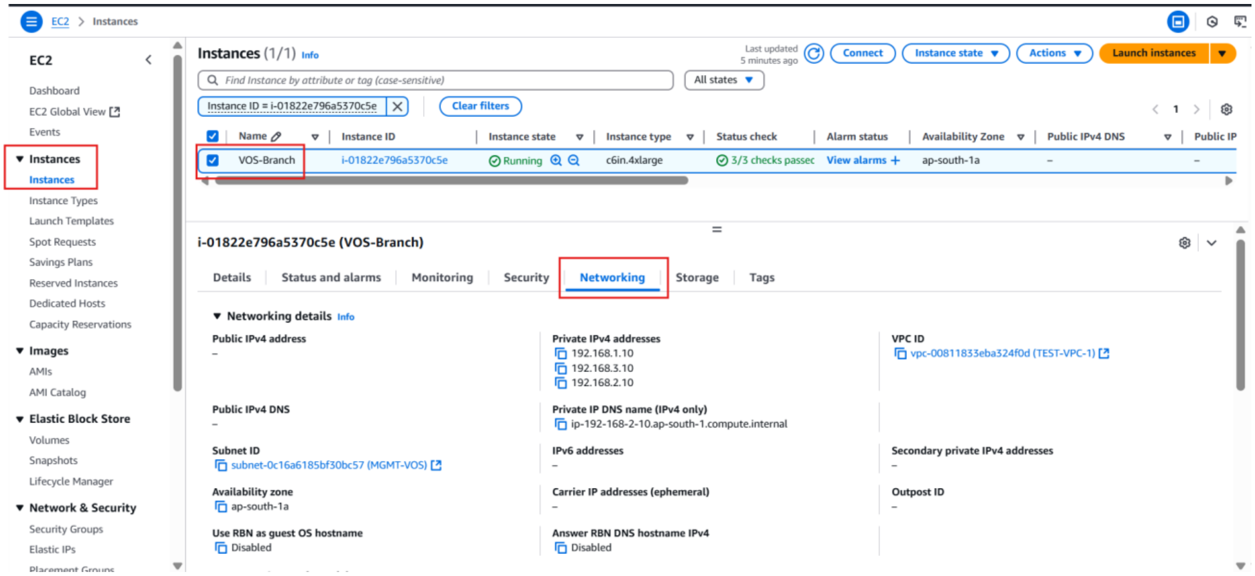
- There is a charge for all Elastic IP addresses whether they are in use (allocated to a resource, like an EC2 instance) or idle (created in your account but unallocated).
- If you created the VM using an AWS marketplace AMI image, issue the ”sudo passwd admin” command to change the default password of the admin account.

### Associating Elastic IP Address with an Interface:

After the VOS EC2 instance is up and running, you associate an elastic IP address with an interface. To do this, you must determine the interface ID from the EC2 instance that you created. If the controller is reachable from the branch using a public IP address, you associate the elastic IP address on the WAN and management interfaces.

To associate an elastic IP address with an interface:

Navigate to EC2 → Instances, and then select the VOS EC2 instance and select the Networking tab.



Instances (1/1) Info

Find Instance by attribute or tag (case-sensitive)

Instance ID = i-01822e796a5370c5e

| | Name | Instance ID | Instance state | Instance type | Status check | Alarm status | Availability Zone | Public IPv4 DNS | Public IP |
|---|---|---|---|---|---|---|---|---|---|
| ☑ | VOS-Branch | i-01822e796a5370c5e | Running | c6in.4xlarge | 3/3 checks passec | View alarms + | ap-south-1a | – | – |

i-01822e796a5370c5e (VOS-Branch)

Networking details Info

Public IPv4 address
–

Private IPv4 addresses
192.168.1.10
192.168.3.10
192.168.2.10

VPC ID
vpc-00811833eba324f0d (TEST-VPC-1)

Public IPv4 DNS
–

Private IP DNS name (IPv4 only)
ip-192-168-2-10.ap-south-1.compute.internal

Subnet ID
subnet-0c16a6185bf30bc57 (MGMT-VOS)

IPv6 addresses
–

Secondary private IPv4 addresses
–

Availability zone
ap-south-1a

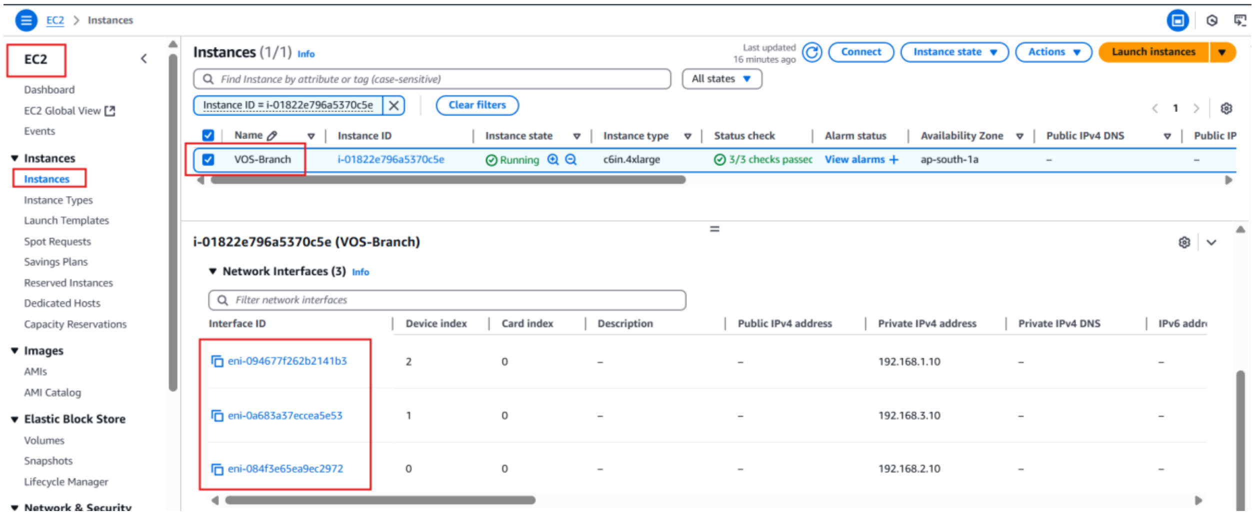
Carrier IP addresses (ephemeral)
–

Outpost ID
–

Use RBN as guest OS hostname
Disabled

Answer RBN DNS hostname IPv4
Disabled

Scroll down until you see the network interface IDs for the NICs attached to the management and WAN subnets and make a note of these IDs.



Instances (1/1) Info

Find Instance by attribute or tag (case-sensitive)

Instance ID = i-01822e796a5370c5e

| | Name | Instance ID | Instance state | Instance type | Status check | Alarm status | Availability Zone | Public IPv4 DNS | Public IP |
|---|---|---|---|---|---|---|---|---|---|
| ☑ | VOS-Branch | i-01822e796a5370c5e | Running | c6in.4xlarge | 3/3 checks passec | View alarms + | ap-south-1a | – | – |

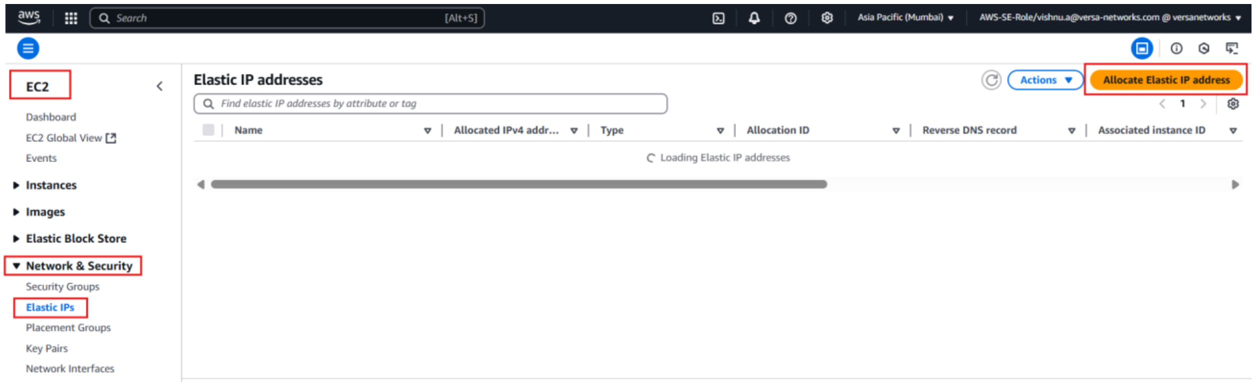
i-01822e796a5370c5e (VOS-Branch)

Network Interfaces (3) Info

Filter network interfaces

| Interface ID | Device index | Card index | Description | Public IPv4 address | Private IPv4 address | Private IPv4 DNS | IPv6 addr |
|---|---|---|---|---|---|---|---|
| eni-094677f262b2141b3 | 2 | 0 | – | – | 192.168.1.10 | – | – |
| eni-0a683a37eccea5e53 | 1 | 0 | – | – | 192.168.3.10 | – | – |
| eni-084f3e65ea9ec2972 | 0 | 0 | – | – | 192.168.2.10 | – | – |

To Allocate Elastic IP Addresses, under EC2 dashboard go to “Network & Security” → Elastic IPs and click on “Allocate Elastic IP address”.



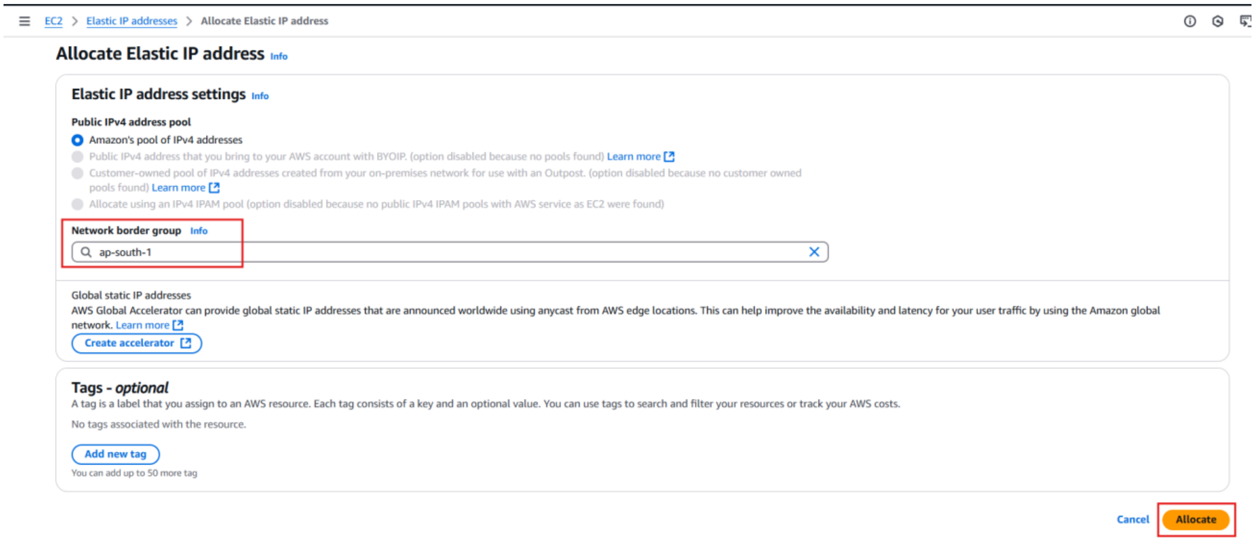
Elastic IP addresses

Find elastic IP addresses by attribute or tag

| | Name | Allocated IPv4 addr... | Type | Allocation ID | Reverse DNS record | Associated instance ID |
|---|---|---|---|---|---|---|

Loading Elastic IP addresses

Leave the Elastic IP address settings to default and click on “Allocate”.



EC2 > Elastic IP addresses > Allocate Elastic IP address

Allocate Elastic IP address Info

Elastic IP address settings Info

Public IPv4 address pool

● Amazon's pool of IPv4 addresses

○ Public IPv4 address that you bring to your AWS account with BYOIP. (option disabled because no pools found) Learn more

○ Customer-owned pool of IPv4 addresses created from your on-premises network for use with an Outpost. (option disabled because no customer owned pools found) Learn more

○ Allocate using an IPv4 IPAM pool (option disabled because no public IPv4 IPAM pools with AWS service as EC2 were found)

Network border group Info

ap-south-1

Global static IP addresses

AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. Learn more

Create accelerator

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.

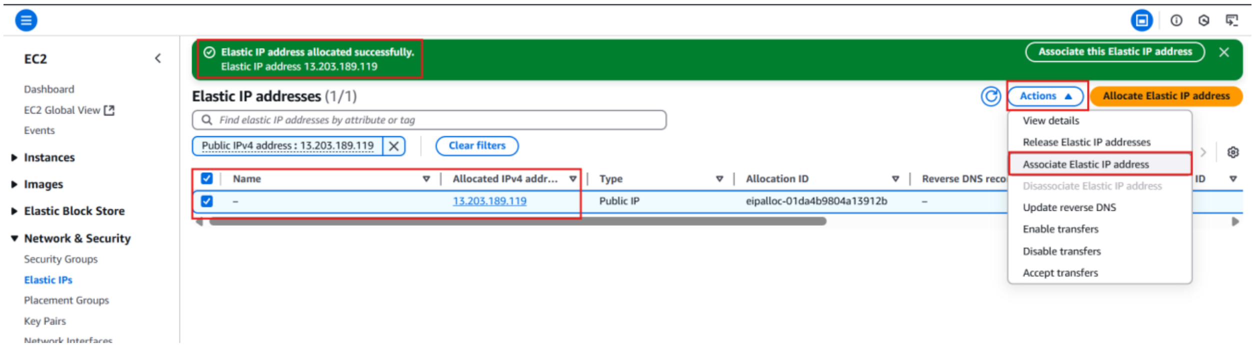
No tags associated with the resource.

Add new tag

You can add up to 50 more tag

Cancel Allocate

Once it is created, Select the Elastic IP address → Actions → Associate the Elastic IP address.



Elastic IP address allocated successfully.
Elastic IP address 13.203.189.119

Associate this Elastic IP address

Elastic IP addresses (1/1)

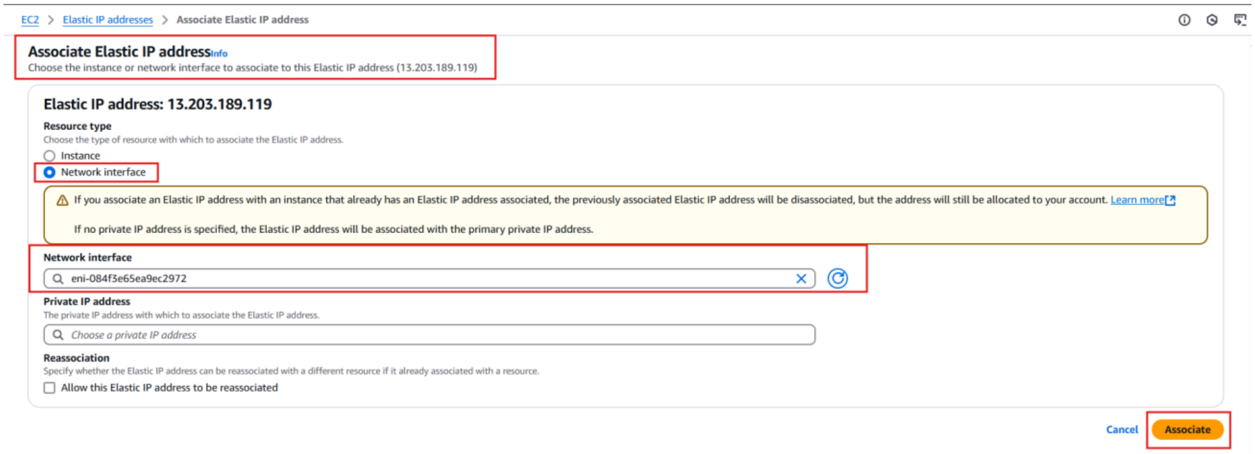
Find elastic IP addresses by attribute or tag

Public IPv4 address : 13.203.189.119 ✕ Clear filters

| ☑ | Name | Allocated IPv4 addr... | Type | Allocation ID | Reverse DNS reco... |
|---|---|---|---|---|---|
| ☑ | – | 13.203.189.119 | Public IP | eipalloc-01da4b9804a13912b | – |

Actions ▲
Allocate Elastic IP address
View details
Release Elastic IP addresses
Associate Elastic IP address
Disassociate Elastic IP address
Update reverse DNS
Enable transfers
Disable transfers
Accept transfers

Under "Associate the Elastic IP address" select the resource type as "Network interface" and provide the interface ID of MGMT interface and click on "Associate".



EC2 > Elastic IP addresses > Associate Elastic IP address

Associate Elastic IP addressInfo

Choose the instance or network interface to associate to this Elastic IP address (13.203.189.119)

Elastic IP address: 13.203.189.119

Resource type

Choose the type of resource with which to associate the Elastic IP address.

○ Instance

● Network interface

⚠ If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account. Learn more

If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address.

Network interface

eni-084f3e65ea9ec2972

Private IP address

The private IP address with which to associate the Elastic IP address.

*Choose a private IP address*

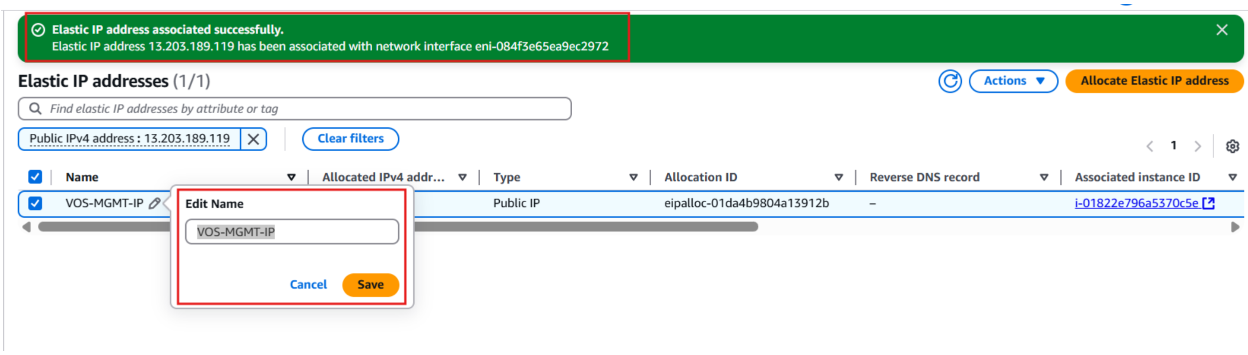
Reassociation

Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.

□ Allow this Elastic IP address to be reassociated

Cancel Associate

Make sure the association is successful and provide a name to the Elastic IP. This will be used to take management access of VOS.



Elastic IP address associated successfully.
Elastic IP address 13.203.189.119 has been associated with network interface eni-084f3e65ea9ec2972

Elastic IP addresses (1/1)

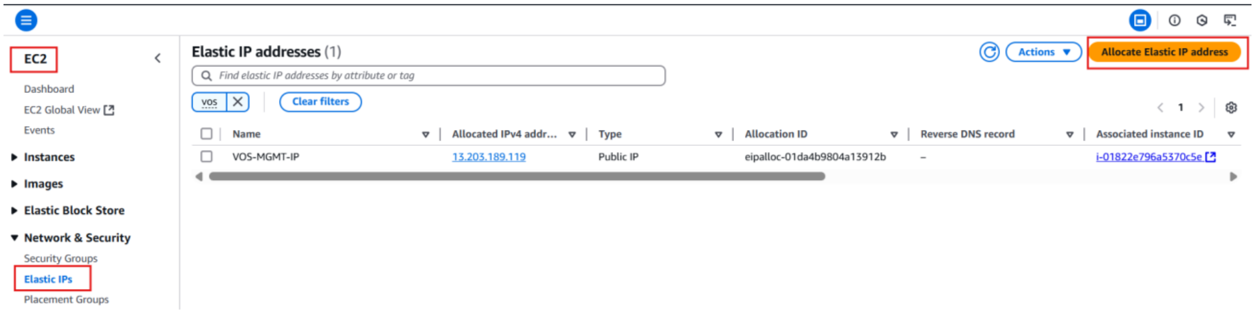
Actions ▼
Allocate Elastic IP address
Find elastic IP addresses by attribute or tag
Public IPv4 address : 13.203.189.119
Clear filters

| ☑ Name | Allocated IPv4 addr... | Type | Allocation ID | Reverse DNS record | Associated instance ID |
|---|---|---|---|---|---|
| ☑ VOS-MGMT-IP |  | Public IP | eipalloc-01da4b9804a13912b | – | i-01822e796a5370c5e |

Edit Name: VOS-MGMT-IP

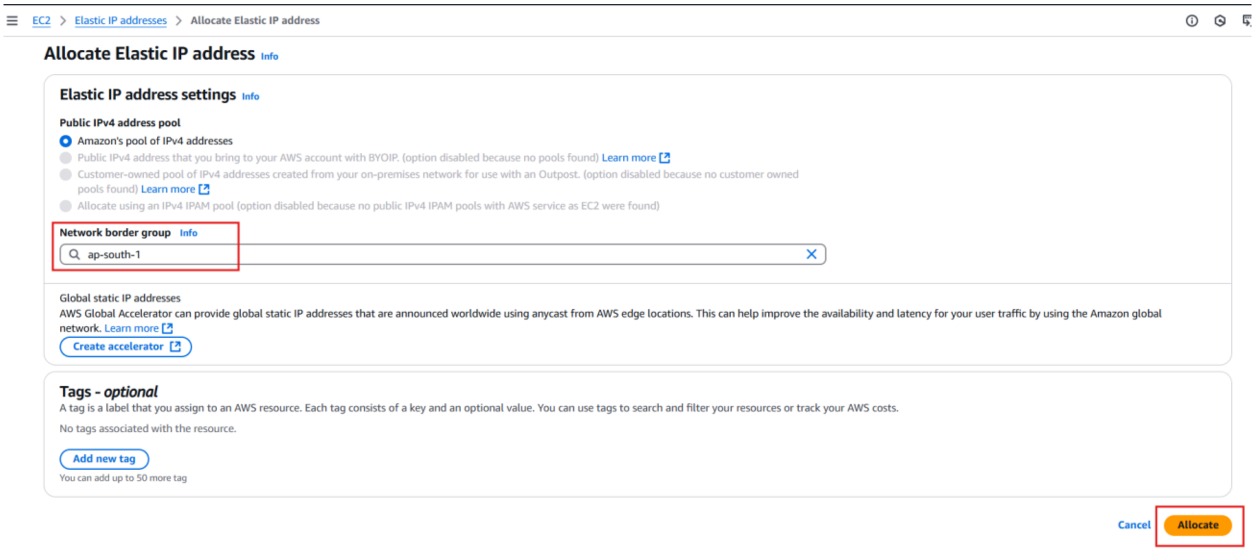
Repeat the above process for WAN interface.

Under EC2 dashboard go to “Network & Security” → “Elastic IPs” and click on “Allocate Elastic IP address”.



| Name | Allocated IPv4 addr... | Type | Allocation ID | Reverse DNS record | Associated instance ID |
|---|---|---|---|---|---|
| VOS-MGMT-IP | 13.203.189.119 | Public IP | eipalloc-01da4b9804a13912b | – | i-01822e796a5370c5e |

Leave the Elastic IP address settings to default and click on “Allocate”.



Allocate Elastic IP address Info

Elastic IP address settings Info

Public IPv4 address pool

● Amazon's pool of IPv4 addresses
○ Public IPv4 address that you bring to your AWS account with BYOIP. (option disabled because no pools found) Learn more
○ Customer-owned pool of IPv4 addresses created from your on-premises network for use with an Outpost. (option disabled because no customer owned pools found) Learn more
○ Allocate using an IPv4 IPAM pool (option disabled because no public IPv4 IPAM pools with AWS service as EC2 were found)

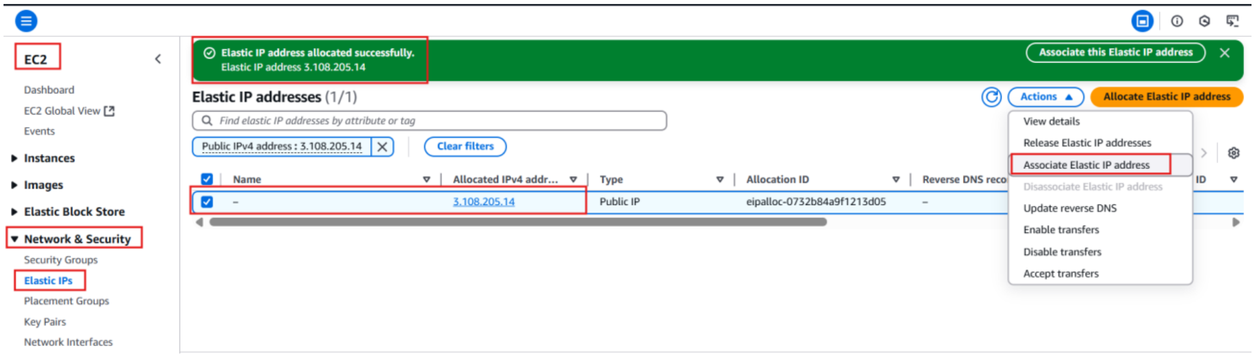
Network border group Info: ap-south-1

Global static IP addresses
AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. Learn more

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.
No tags associated with the resource.

You can add up to 50 more tag

Once it is created, Select the Elastic IP address → Actions → Associate the Elastic IP address.

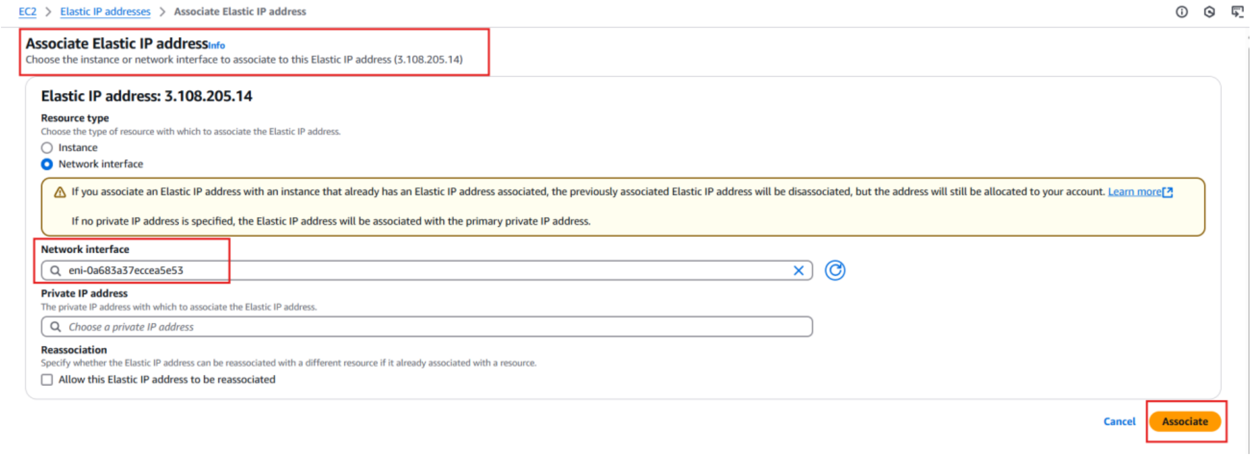


Elastic IP address allocated successfully.
Elastic IP address 3.108.205.14

Elastic IP addresses (1/1)

| Name | Allocated IPv4 addr... | Type | Allocation ID | Reverse DNS reco |
|---|---|---|---|---|
| – | 3.108.205.14 | Public IP | eipalloc-0732b84a9f1213d05 | – |

Under “Associate the Elastic IP address” select the resource type as “Network interface” and provide the interface ID of WAN interface and click on “Associate”.



EC2 > Elastic IP addresses > Associate Elastic IP address

Associate Elastic IP address Info
Choose the instance or network interface to associate to this Elastic IP address (3.108.205.14)

Elastic IP address: 3.108.205.14

Resource type
Choose the type of resource with which to associate the Elastic IP address.
○ Instance
● Network interface

If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account. Learn more

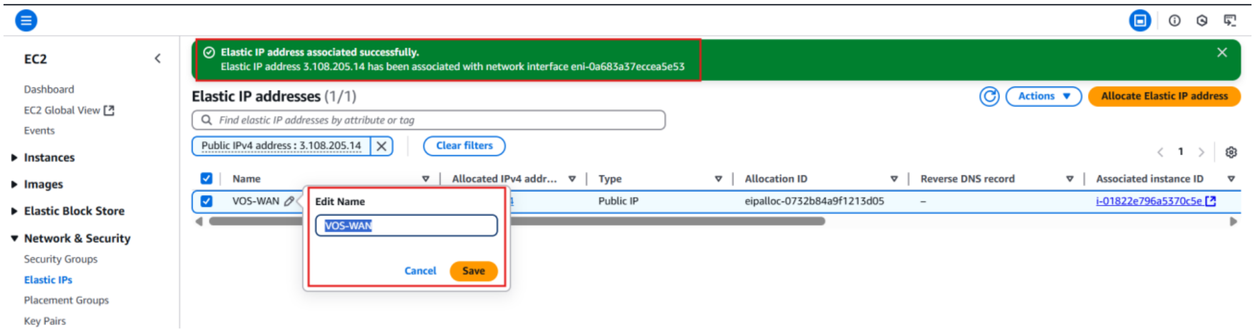
If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address.

Network interface
eni-0a683a37eccea5e53

Private IP address
The private IP address with which to associate the Elastic IP address.
Choose a private IP address

Reassociation
Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.
☐ Allow this Elastic IP address to be reassociated

Make sure the association is successful and provide a name to the Elastic IP. This will be used to access Controller.



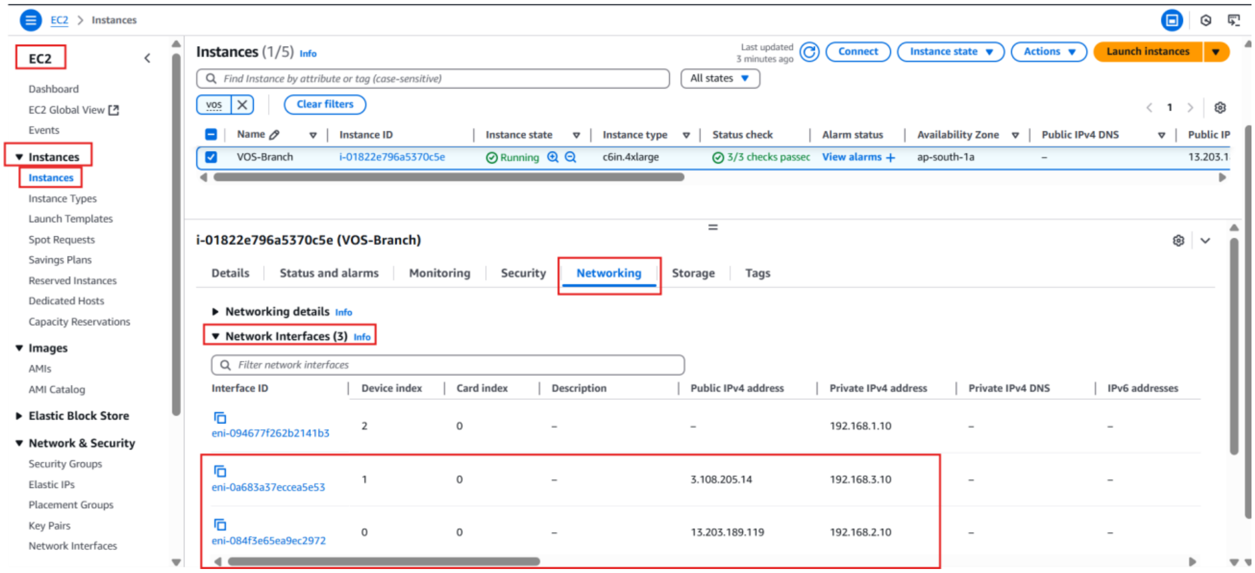
Elastic IP address associated successfully.
Elastic IP address 3.108.205.14 has been associated with network interface eni-0a683a37eccea5e53

Elastic IP addresses (1/1)

| Name | Allocated IPv4 addr... | Type | Allocation ID | Reverse DNS record | Associated instance ID |
|---|---|---|---|---|---|
| VOS-WAN | | Public IP | eipalloc-0732b84a9f1213d05 | – | i-01822e796a5370c5e |

Edit Name
VOS-WAN

Once done you can check the associations under “EC2” Dashboard → Instances, and then select the VOS EC2 instance and click on “Networking” tab.



EC2 > Instances

EC2

Dashboard
EC2 Global View
Events
▼ Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
▼ Images
AMIs
AMI Catalog
▶ Elastic Block Store
▼ Network & Security
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces

Instances (1/5) Info

Last updated 3 minutes ago | Connect | Instance state ▼ | Actions ▼ | Launch instances ▼

Find Instance by attribute or tag (case-sensitive) | All states ▼

vos ✕ | Clear filters

| | Name | Instance ID | Instance state | Instance type | Status check | Alarm status | Availability Zone | Public IPv4 DNS | Public IP |
|---|---|---|---|---|---|---|---|---|---|
| ☑ | VOS-Branch | i-01822e796a5370c5e | Running | c6in.4xlarge | 3/3 checks passec | View alarms + | ap-south-1a | – | 13.203.1 |

i-01822e796a5370c5e (VOS-Branch)

Details | Status and alarms | Monitoring | Security | Networking | Storage | Tags

▶ Networking details Info

▼ Network Interfaces (3) Info

Filter network interfaces

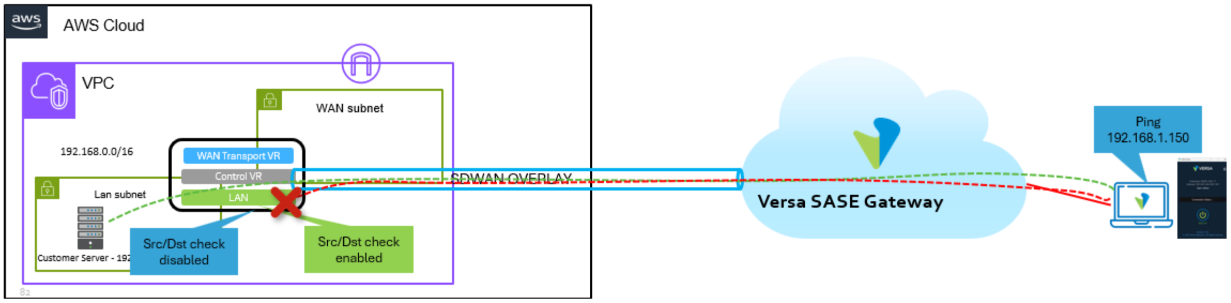
| Interface ID | Device index | Card index | Description | Public IPv4 address | Private IPv4 address | Private IPv4 DNS | IPv6 addresses |
|---|---|---|---|---|---|---|---|
| eni-094677f262b2141b3 | 2 | 0 | – | – | 192.168.1.10 | – | – |
| eni-0a683a37eccea5e53 | 1 | 0 | – | 3.108.205.14 | 192.168.3.10 | – | – |
| eni-084f3e65ea9ec2972 | 0 | 0 | – | 13.203.189.119 | 192.168.2.10 | – | – |

## Disable the Source and Destination Check on WAN and LAN Interfaces:

By default, AWS EC2 instances perform source/destination checks, meaning the instance must be either the source or destination of any traffic it handles. This ensures traffic is only allowed if it's directly related to that instance.

**In this Scenario:**

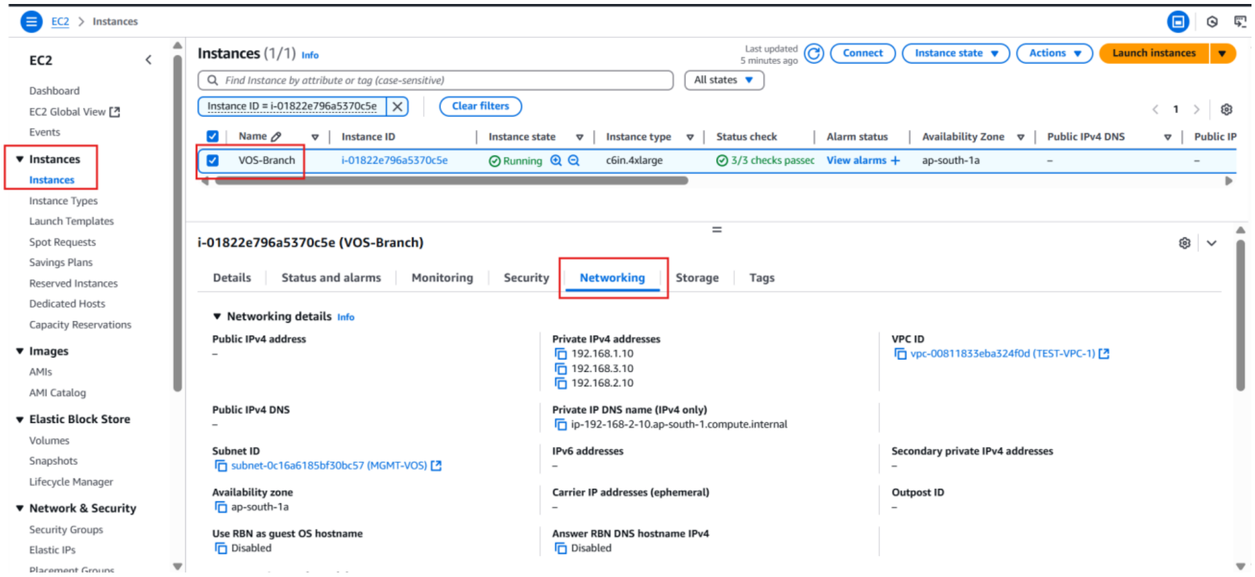
- A customer server is connected to the LAN interface of the SD-WAN instance. The SD-WAN instance forwards traffic between LAN and WAN (not the traffic originator or receiver).
- We must disable source/destination check on the LAN and WAN interface of SD-WAN instance to allow it to route or forward traffic on behalf of other devices (e.g., server behind LAN).



In the example here, we disable the source and destination check for the VOS WAN and LAN interfaces vni-0/0 and vni-0/1.

**Disable the source and destination check:**

Navigate to EC2 → Instances, and then select the VOS EC2 instance and select the Networking tab.



Instances (1/1) Info

Last updated 5 minutes ago

Instance ID = i-01822e796a5370c5e

| Name | Instance ID | Instance state | Instance type | Status check | Alarm status | Availability Zone | Public IPv4 DNS | Public IP |
|---|---|---|---|---|---|---|---|---|
| VOS-Branch | i-01822e796a5370c5e | Running | c6in.4xlarge | 3/3 checks passec | View alarms + | ap-south-1a | – | – |

i-01822e796a5370c5e (VOS-Branch)

Networking details Info

Public IPv4 address: –

Private IPv4 addresses: 192.168.1.10, 192.168.3.10, 192.168.2.10

VPC ID: vpc-00811833eba324f0d (TEST-VPC-1)

Public IPv4 DNS: –

Private IP DNS name (IPv4 only): ip-192-168-2-10.ap-south-1.compute.internal

Subnet ID: subnet-0c16a6185bf30bc57 (MGMT-VOS)

IPv6 addresses: –

Secondary private IPv4 addresses: –

Availability zone: ap-south-1a

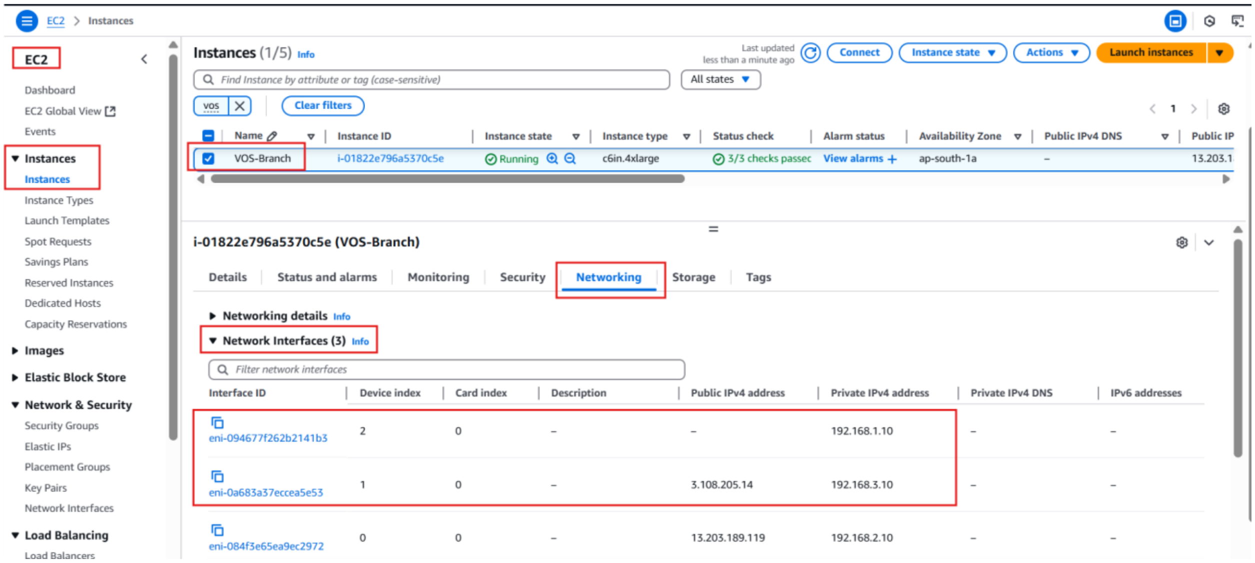
Carrier IP addresses (ephemeral): –

Outpost ID: –

Use RBN as guest OS hostname: Disabled

Answer RBN DNS hostname IPv4: Disabled

Scroll down until you see the network interface IDs, and make note of WAN and LAN interface ID's.



Instances (1/5) Info

Last updated less than a minute ago

vos

| Name | Instance ID | Instance state | Instance type | Status check | Alarm status | Availability Zone | Public IPv4 DNS | Public IP |
|---|---|---|---|---|---|---|---|---|
| VOS-Branch | i-01822e796a5370c5e | Running | c6in.4xlarge | 3/3 checks passec | View alarms + | ap-south-1a | – | 13.203.1 |

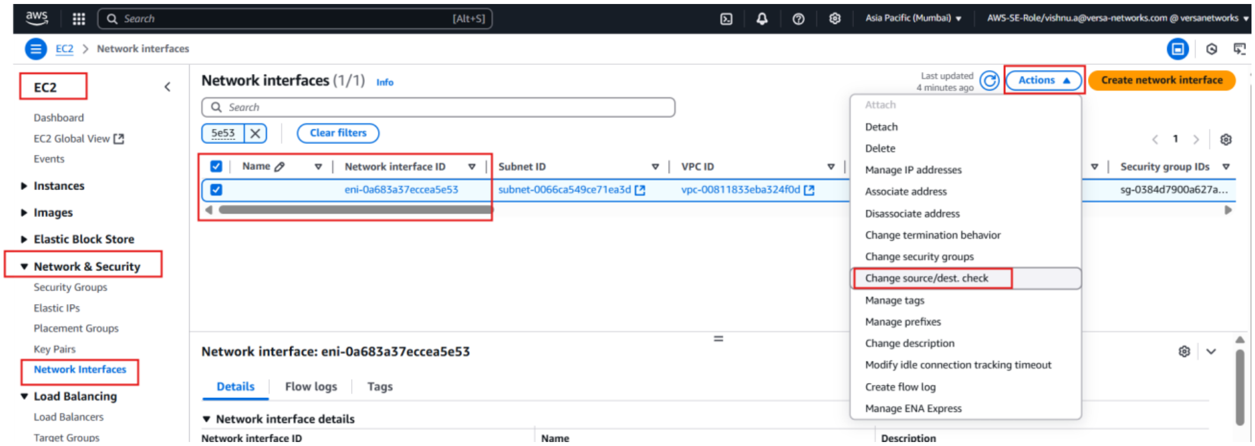
i-01822e796a5370c5e (VOS-Branch)

Networking details Info

Network Interfaces (3) Info

| Interface ID | Device index | Card index | Description | Public IPv4 address | Private IPv4 address | Private IPv4 DNS | IPv6 addresses |
|---|---|---|---|---|---|---|---|
| eni-094677f262b2141b3 | 2 | 0 | – | – | 192.168.1.10 | – | – |
| eni-0a683a37eccea5e53 | 1 | 0 | – | 3.108.205.14 | 192.168.3.10 | – | – |
| eni-084f3e65ea9ec2972 | 0 | 0 | – | 13.203.189.119 | 192.168.2.10 | – | – |

Under EC2, go to "Network & Security" → Network Interfaces → WAN network interface → Actions → Change source/dest.check.



Network interfaces (1/1) Info

Last updated 4 minutes ago

5e53

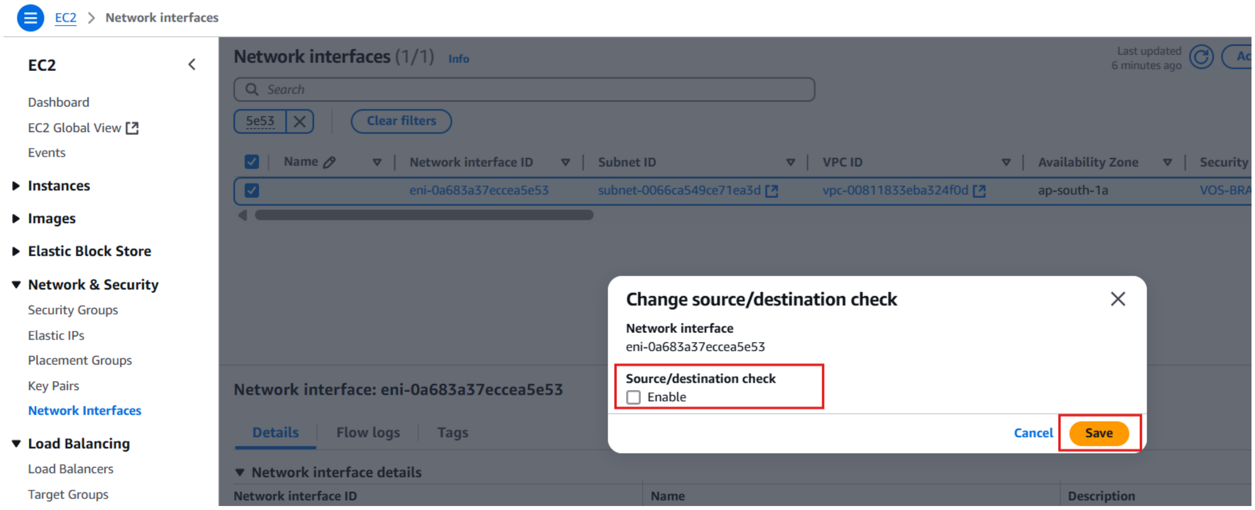
| Name | Network interface ID | Subnet ID | VPC ID | Security group IDs |
|---|---|---|---|---|
| | eni-0a683a37eccea5e53 | subnet-0066ca549ce71ea3d | vpc-00811833eba324f0d | sg-0384d7900a627a... |

Network interface: eni-0a683a37eccea5e53

Network interface details

Network interface ID | Name | Description

Disable “Source/destination check” and save it.



| Name | Network interface ID | Subnet ID | VPC ID | Availability Zone | Security |
|---|---|---|---|---|---|
| | eni-0a683a37eccea5e53 | subnet-0066ca549ce71ea3d | vpc-00811833eba324f0d | ap-south-1a | VOS-BRA |

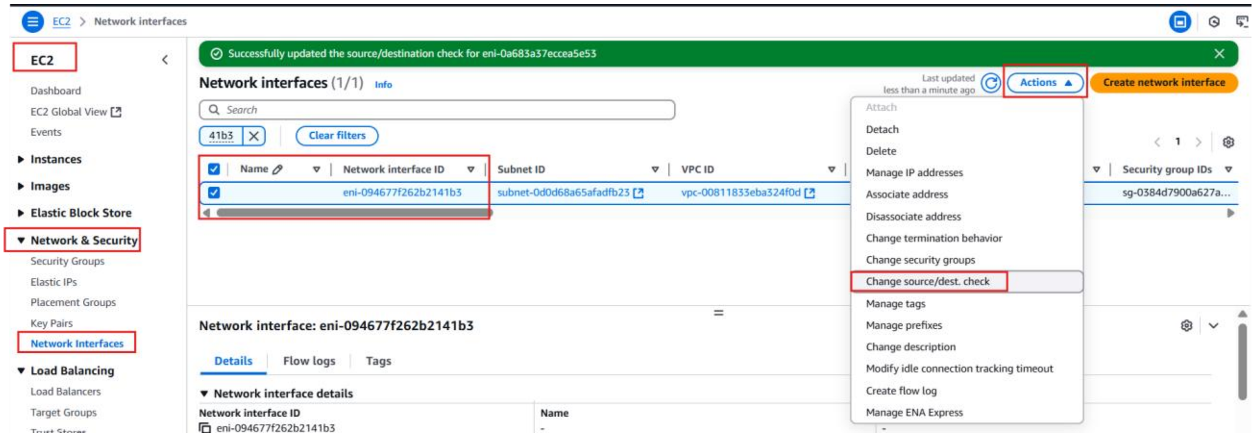
Network interface: eni-0a683a37eccea5e53

Change source/destination check

Network interface
eni-0a683a37eccea5e53

Source/destination check
☐ Enable

Repeat the same for LAN interface.

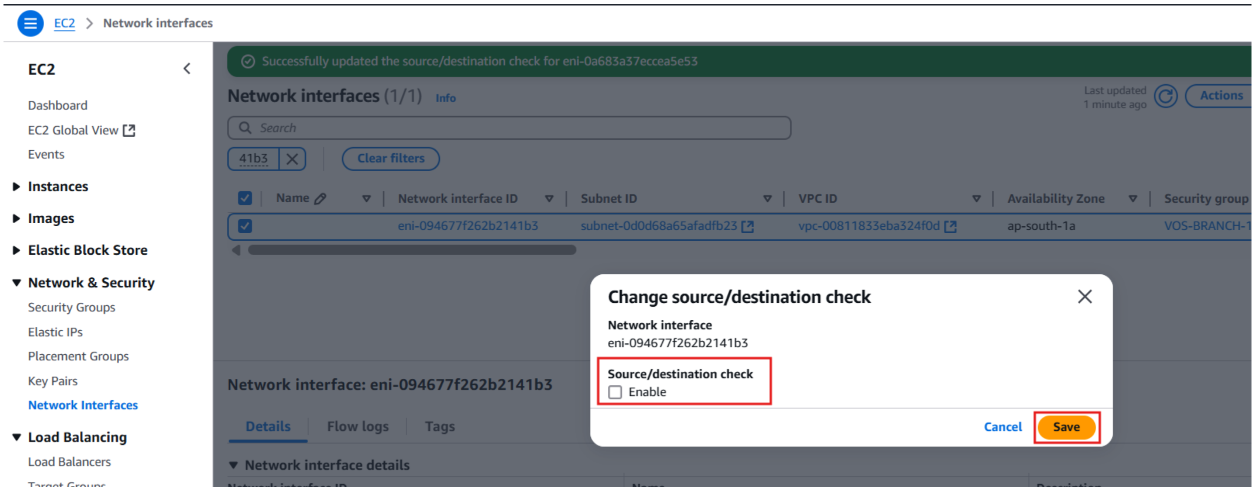


Successfully updated the source/destination check for eni-0a683a37eccea5e53

| Name | Network interface ID | Subnet ID | VPC ID | Security group IDs |
|---|---|---|---|---|
| | eni-094677f262b2141b3 | subnet-0d0d68a65afadfb23 | vpc-00811833eba324f0d | sg-0384d7900a627a... |

Network interface: eni-094677f262b2141b3

Network interface ID: eni-094677f262b2141b3
Name: -



Successfully updated the source/destination check for eni-0a683a37eccea5e53

| Name | Network interface ID | Subnet ID | VPC ID | Availability Zone | Security group |
|---|---|---|---|---|---|
| | eni-094677f262b2141b3 | subnet-0d0d68a65afadfb23 | vpc-00811833eba324f0d | ap-south-1a | VOS-BRANCH-1 |

Network interface: eni-094677f262b2141b3

Change source/destination check

Network interface
eni-094677f262b2141b3

Source/destination check
☐ Enable

### Copying Director Keys to VOS to resolve Connectivity Issues:

In bare metal appliance creation process, regardless of release, the Versa Director connects to an appliance and injects the public key into the appliance, to enable communication via key based login.

By Default, Versa Director tries to talk to an appliance with *admin/versa123* or any other custom username which is set in Versa Director CLI. But at present, all the AMI that are shared with customer are prepared with password login disabled attribute, for security purpose. Users are required to supply pem key to login into the box. Therefore, Versa Director fails to communicate with appliances, and the appliance/branch creation fails.

**To solve this issue:**

Copy the Versa Director */var/versa/vnms/ncs/homes/admin/.ssh/id_dsa.pub* contents to the below file in appliance:

```
[admin@AWS-Branch: ~] $ ls -al .ssh/authorized_keys
-rw------- 1 admin versa 1012 May 13 21:42 .ssh/authorized_keys
```

Create *authorized_keys* file if it is not present on the appliance.

To add the id_dsa.pub.it to authorized_keys in the appliance edit the file using “sudo nano  .ssh/authorized_keys” add the copied id_dsa.pub.
**NOTE**: File permission should be 600. To change the file permission run -

chmod 600 authorized_keys.

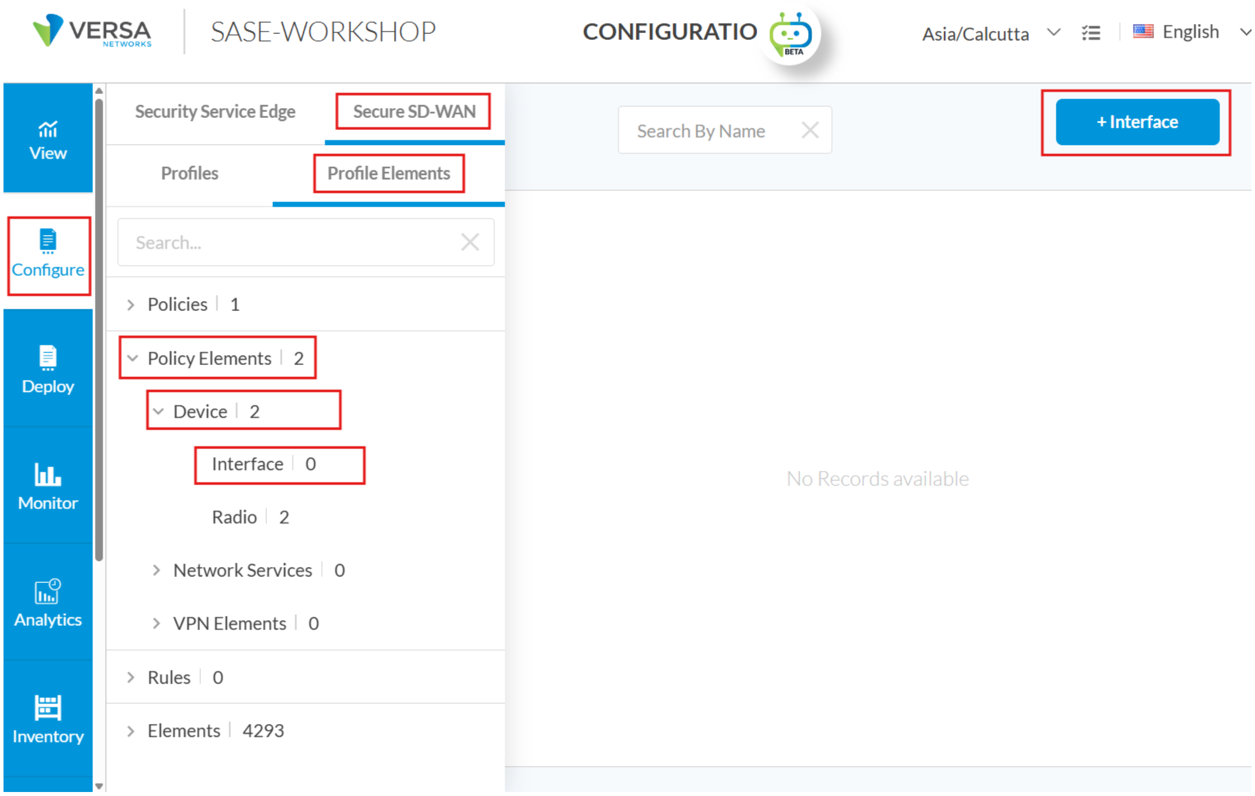
## Concerto Configuration:

To Onboard the branch to the Headend we need to create Master profile and device on Concerto.

### Creating Master profile in Concerto:

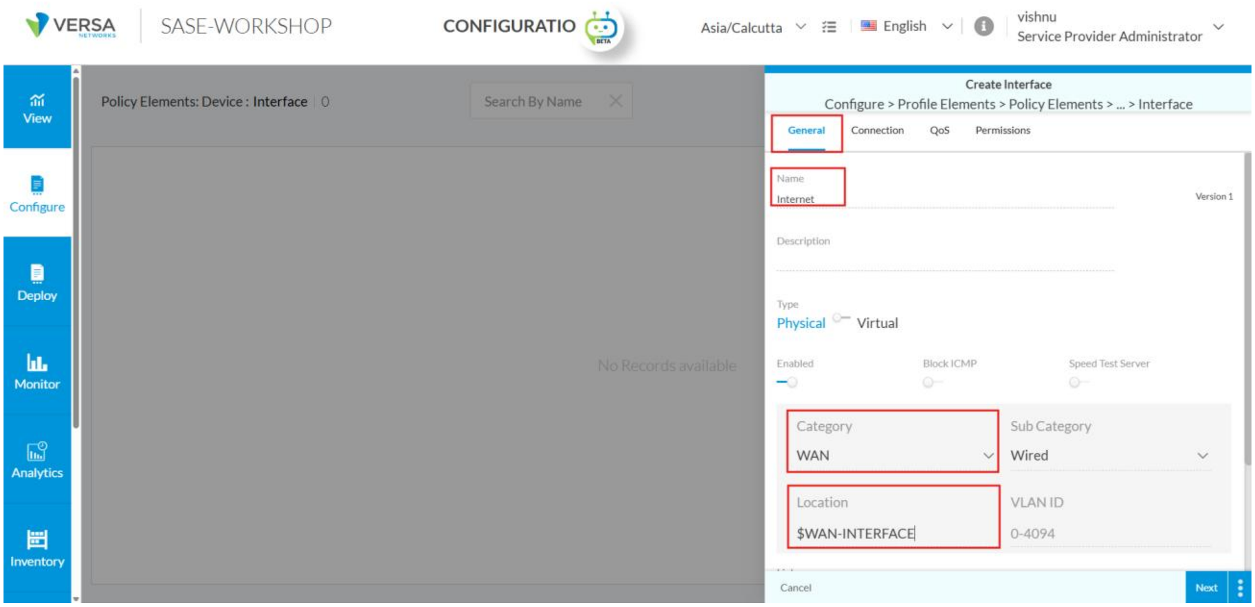
### Creating Interface:

Go to respective Tenant and click on Configure → Secure SD-WAN à Profile Elements à Policy Elements → Device → Interface → Add Interface



### WAN Interface:

Provide the name of the interface and select the category as WAN and under Location, interface can be specified or can be parameterized based on the requirement.



Name: Internet

Type: Physical / Virtual

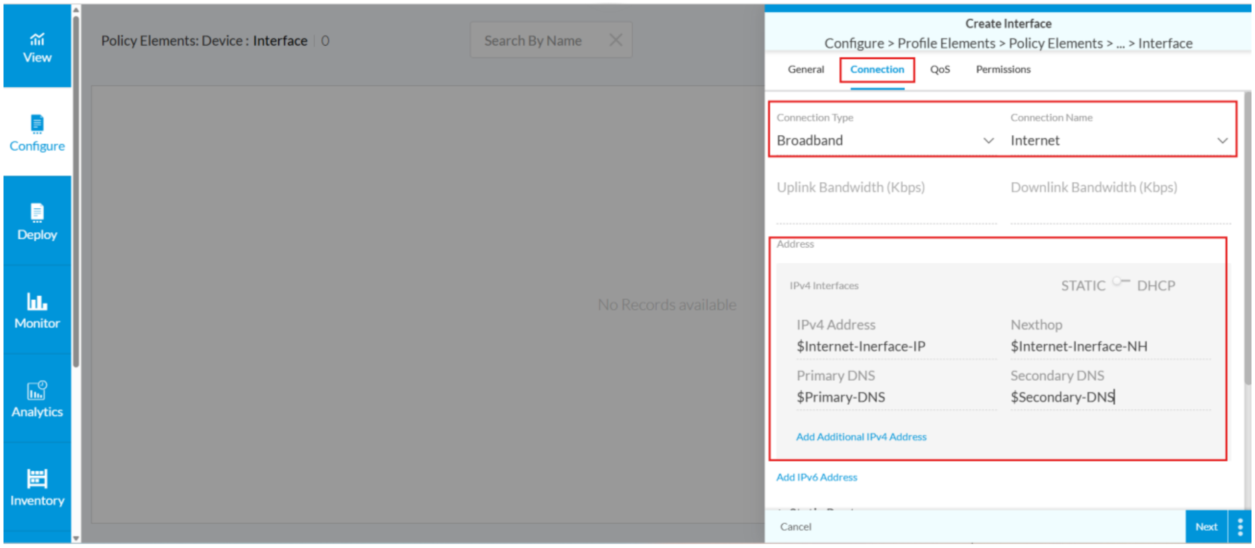
Category: WAN

Sub Category: Wired

Location: $WAN-INTERFACE

VLAN ID: 0-4094

Under Connection provide the necessary information regarding the Connection Type, Connection Name, IPv4 Address, Nexthop and DNS information and save.



Policy Elements: Device : Interface | 0

Create Interface

Configure > Profile Elements > Policy Elements > ... > Interface

Connection Type: Broadband

Connection Name: Internet

Uplink Bandwidth (Kbps)

Downlink Bandwidth (Kbps)

Address

IPv4 Interfaces — STATIC ○ DHCP

IPv4 Address: $Internet-Inerface-IP

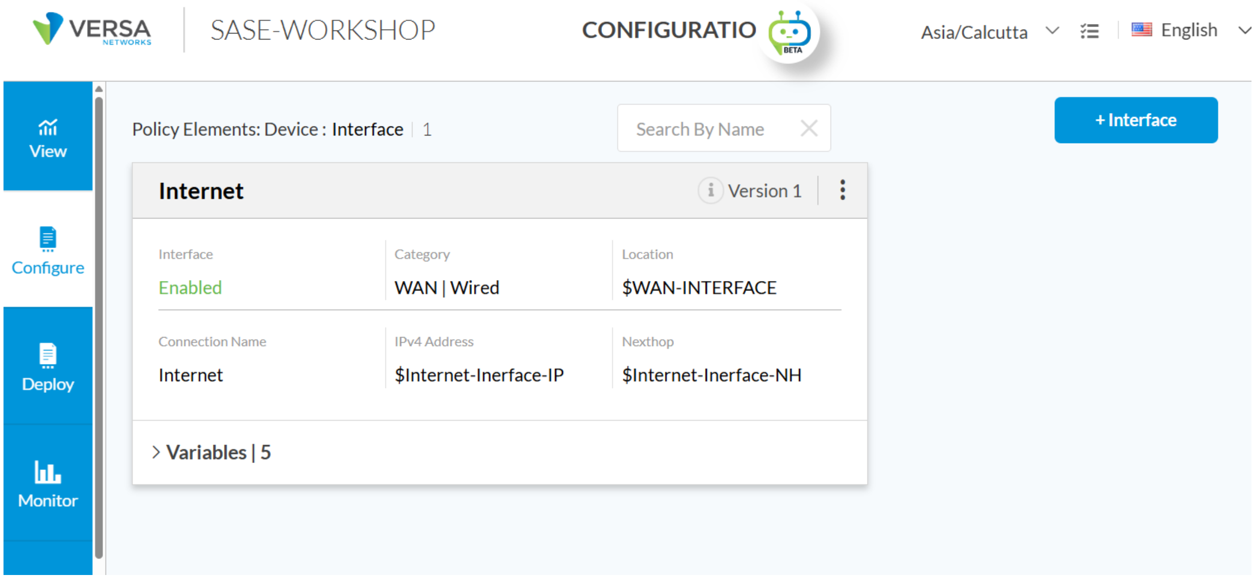
Nexthop: $Internet-Inerface-NH

Primary DNS: $Primary-DNS

Secondary DNS: $Secondary-DNS

**Note:** By default, it is DHCP you can disable the knob to configure it as STATIC.

This will create a WAN interface.



Policy Elements: Device : Interface | 1

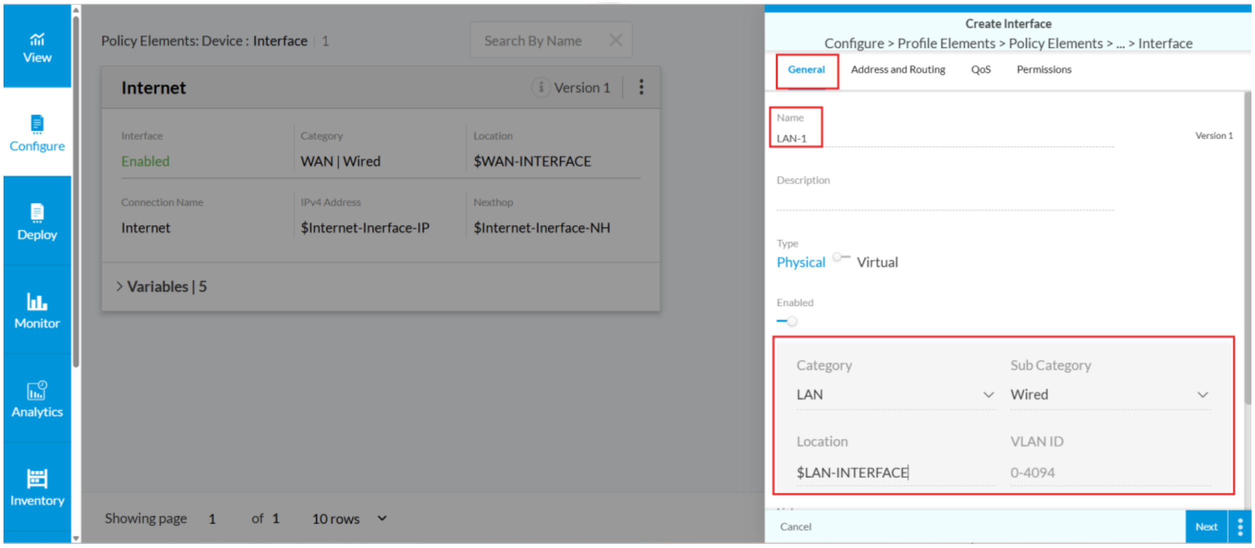
Internet

| Interface | Category | Location |
|---|---|---|
| Enabled | WAN \| Wired | $WAN-INTERFACE |

| Connection Name | IPv4 Address | Nexthop |
|---|---|---|
| Internet | $Internet-Inerface-IP | $Internet-Inerface-NH |

## LAN Interface:

To create a LAN interface, select the category as LAN and provide necessary information.



Policy Elements: Device : Interface | 1

**Internet** Version 1

| Interface | Category | Location |
|---|---|---|
| Enabled | WAN \| Wired | $WAN-INTERFACE |

| Connection Name | IPv4 Address | Nexthop |
|---|---|---|
| Internet | $Internet-Inerface-IP | $Internet-Inerface-NH |

> Variables | 5

Showing page 1 of 1 10 rows

Create Interface

Configure > Profile Elements > Policy Elements > ... > Interface

Name: LAN-1

Version 1

Description

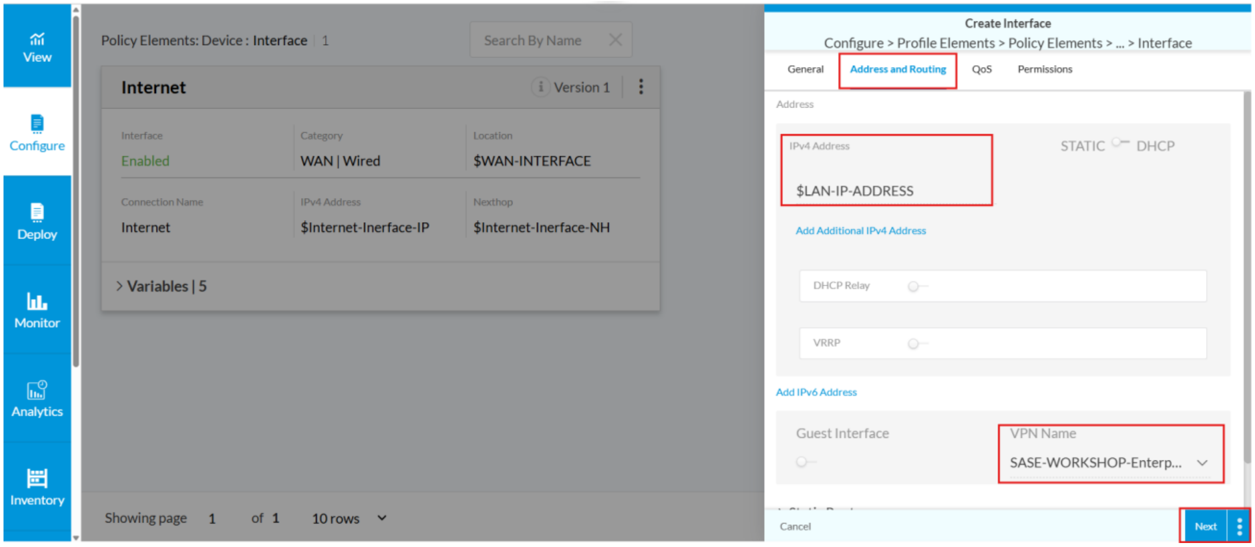
Type: Physical / Virtual

Enabled

| Category | Sub Category |
|---|---|
| LAN | Wired |

| Location | VLAN ID |
|---|---|
| $LAN-INTERFACE | 0-4094 |

Under Address and routing provide the IPv4 address as a parameter, VPN Name and save the configuration.



Policy Elements: Device : Interface | 1

**Internet** Version 1

| Interface | Category | Location |
|---|---|---|
| Enabled | WAN \| Wired | $WAN-INTERFACE |

| Connection Name | IPv4 Address | Nexthop |
|---|---|---|
| Internet | $Internet-Inerface-IP | $Internet-Inerface-NH |

> Variables | 5

Showing page 1 of 1 10 rows

Create Interface

Configure > Profile Elements > Policy Elements > ... > Interface

Address

IPv4 Address: $LAN-IP-ADDRESS

STATIC / DHCP

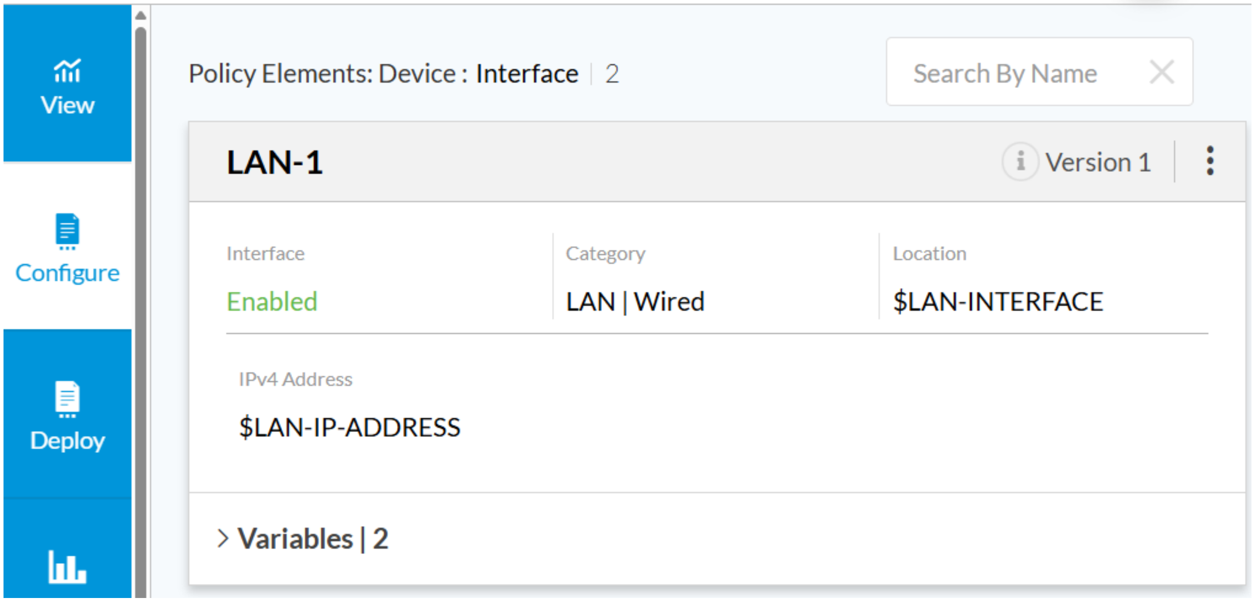
DHCP Relay

VRRP

Guest Interface

VPN Name: SASE-WORKSHOP-Enterp...

This will create a LAN interface.



Policy Elements: Device : Interface | 2

LAN-1 — Version 1

| Interface | Category | Location |
|---|---|---|
| Enabled | LAN \| Wired | $LAN-INTERFACE |

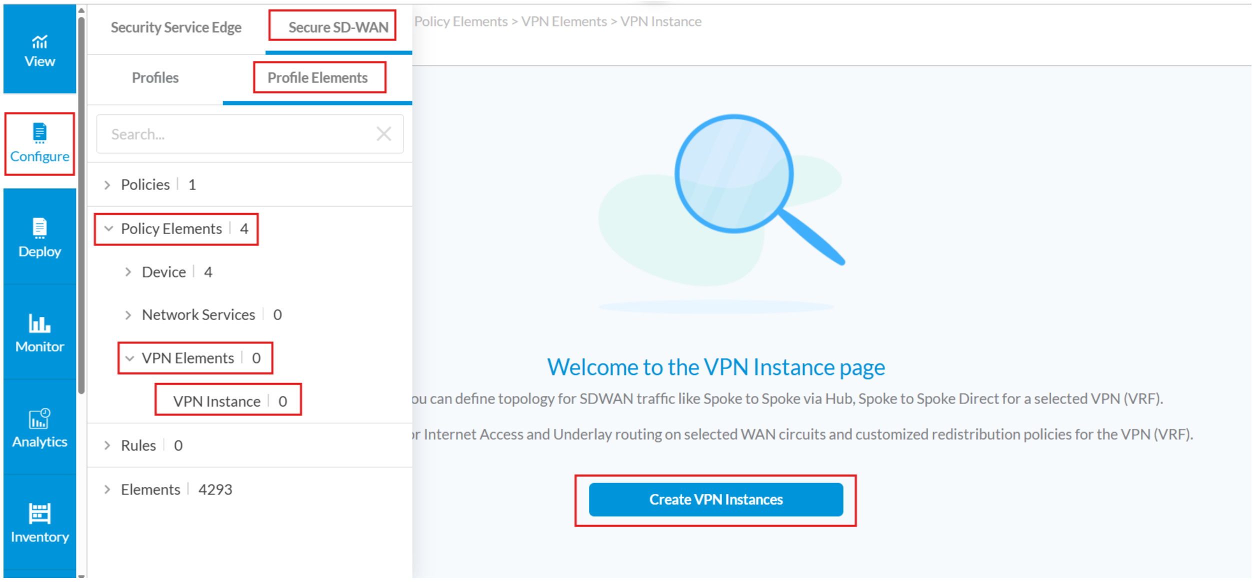
IPv4 Address: $LAN-IP-ADDRESS

Variables | 2

### VPN Instance:

To define the topology of the network we need VPN instance to be created.

Under Configure, go to “Secure SD-WAN” → Profile Elements → Policy Elements → VPN Elements → VPN Instance and click on “Create VPN Instance”.



Welcome to the VPN Instance page

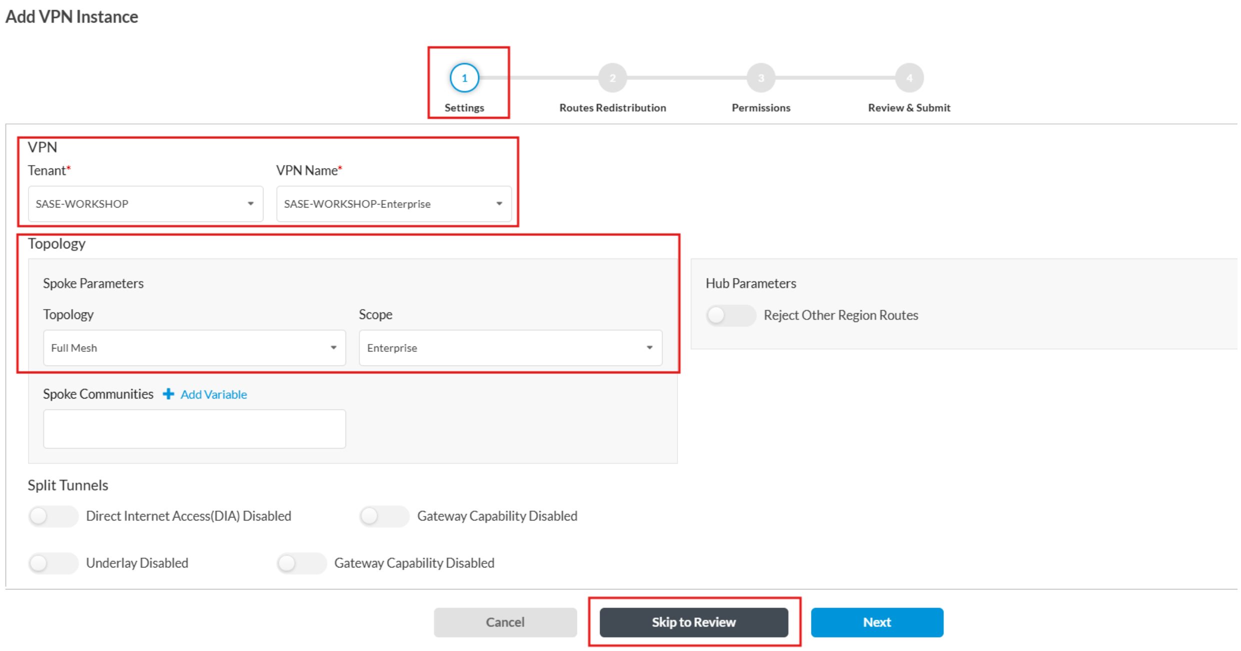
ou can define topology for SDWAN traffic like Spoke to Spoke via Hub, Spoke to Spoke Direct for a selected VPN (VRF).

r Internet Access and Underlay routing on selected WAN circuits and customized redistribution policies for the VPN (VRF).

In the Settings tab under VPN select the Tenant name and the VPN name.

Under Topology select the topology as per the need. By default, it is full mesh. DIA can be enabled under Split Tunnels if needed.

Once done click on “Skip to Review”.



Add VPN Instance

VPN

Tenant*: SASE-WORKSHOP

VPN Name*: SASE-WORKSHOP-Enterprise

Topology

Spoke Parameters

Topology: Full Mesh

Scope: Enterprise

Spoke Communities

Hub Parameters

Reject Other Region Routes

Split Tunnels

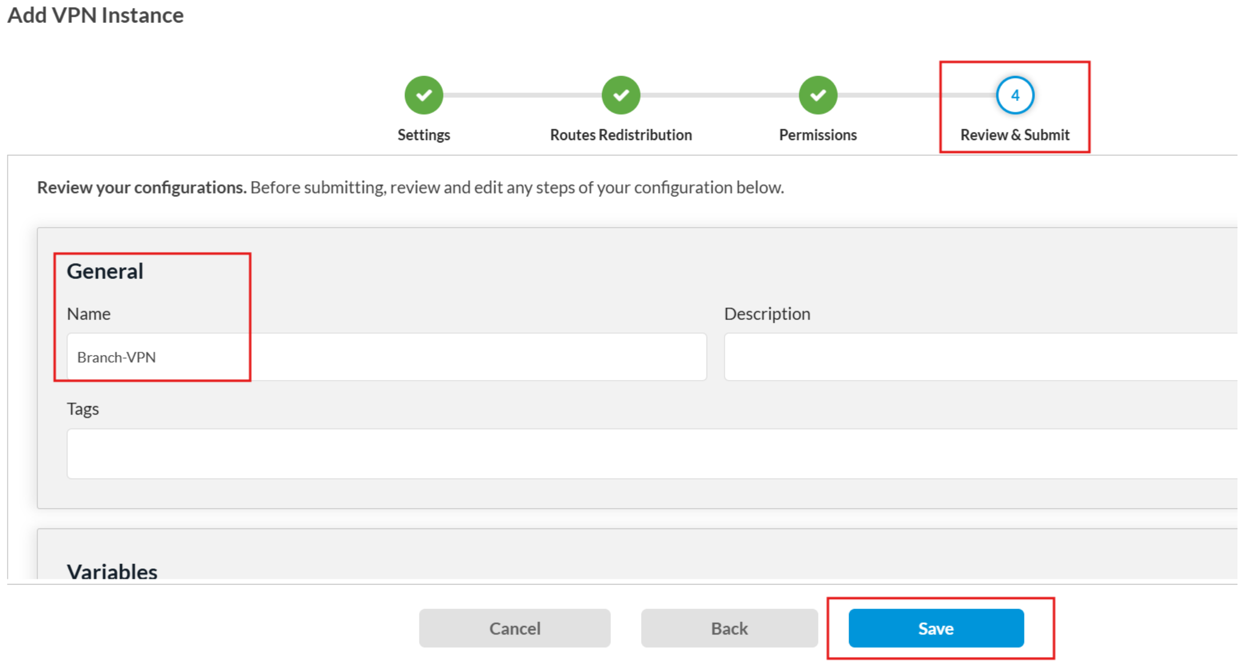
Direct Internet Access(DIA) Disabled

Gateway Capability Disabled

Underlay Disabled

Gateway Capability Disabled

Under “Review & Submit” provide a name to the VPN and Save the configuration.



Add VPN Instance

**Review your configurations.** Before submitting, review and edit any steps of your configuration below.

General

Name: Branch-VPN

Description

Tags

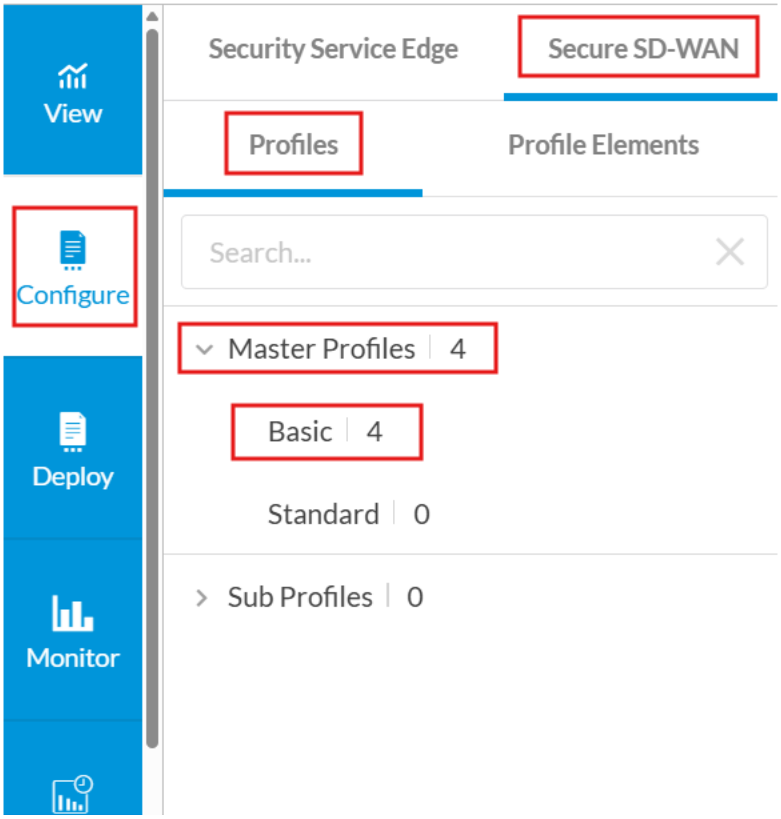
Variables

### Master Profile:

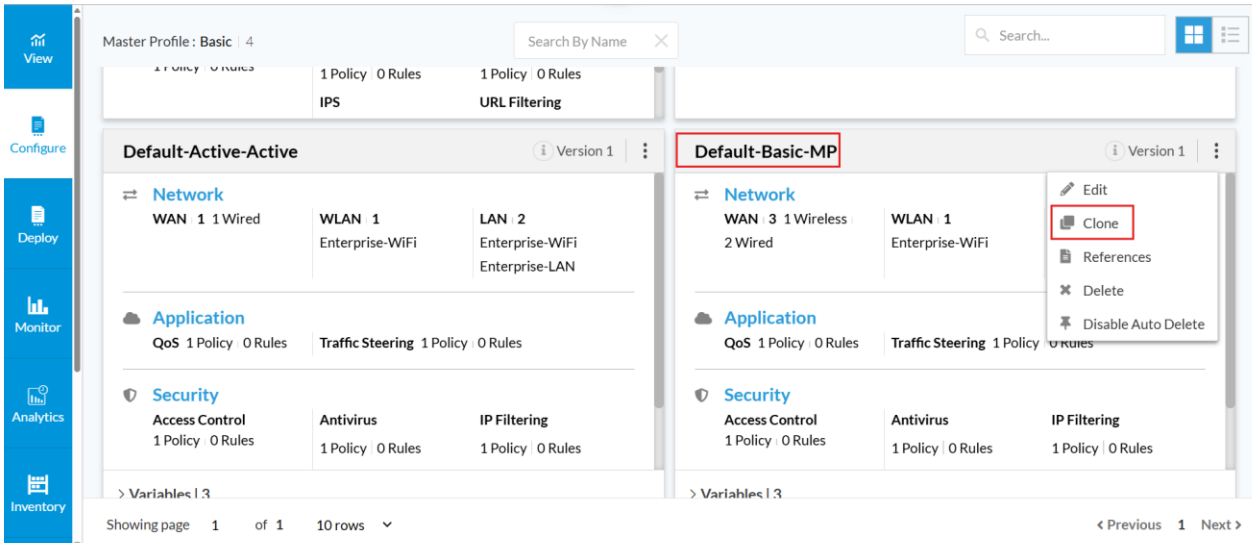
A master profile is a collection of one or more sub-profiles. A single master profile can be applied to one or more devices.

### Creating a Basic Master Profile:

Under respective Tenant go to Configure → Secure SD-WAN → Profiles → Master Profiles → Basic.



Clone the default Basic- MP and Provide a Name to it.



1 Policy | 0 Rules | 1 Policy | 0 Rules | 1 Policy | 0 Rules
IPS | URL Filtering

**Default-Active-Active** Version 1

Network
WAN | 1 | 1 Wired — WLAN | 1 | Enterprise-WiFi — LAN | 2 | Enterprise-WiFi, Enterprise-LAN

Application
QoS 1 Policy | 0 Rules — Traffic Steering 1 Policy | 0 Rules

Security
Access Control 1 Policy | 0 Rules — Antivirus 1 Policy | 0 Rules — IP Filtering 1 Policy | 0 Rules

› Variables | 3

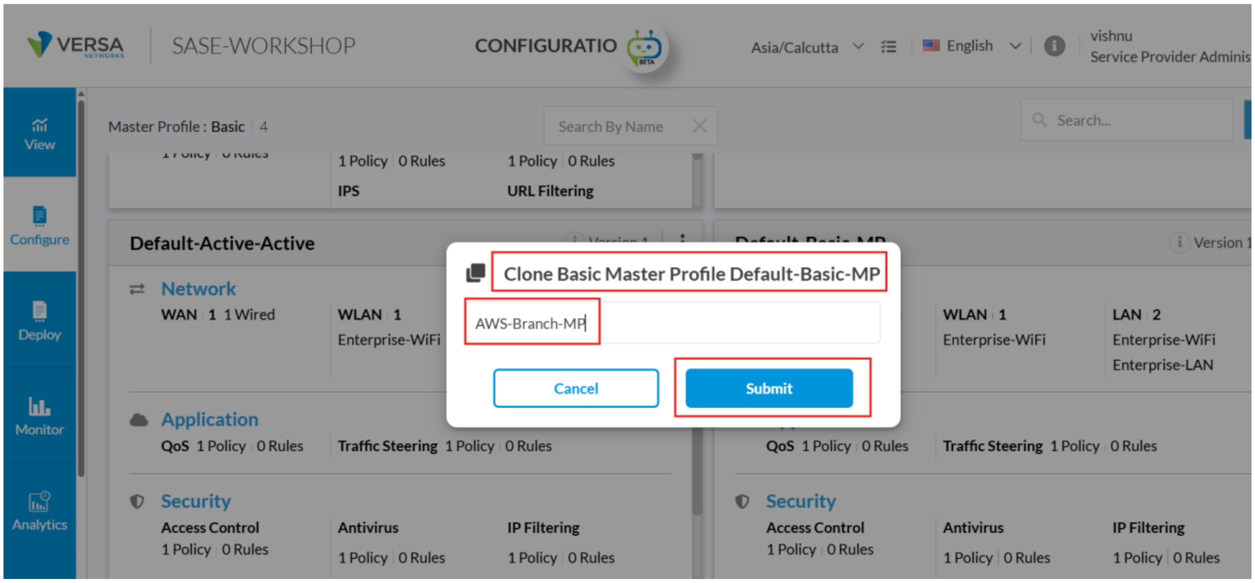
**Default-Basic-MP** Version 1

Network
WAN | 3 | 1 Wireless, 2 Wired — WLAN | 1 | Enterprise-WiFi

Application
QoS 1 Policy | 0 Rules — Traffic Steering 1 Policy | 0 Rules

Security
Access Control 1 Policy | 0 Rules — Antivirus 1 Policy | 0 Rules — IP Filtering 1 Policy | 0 Rules

› Variables | 3

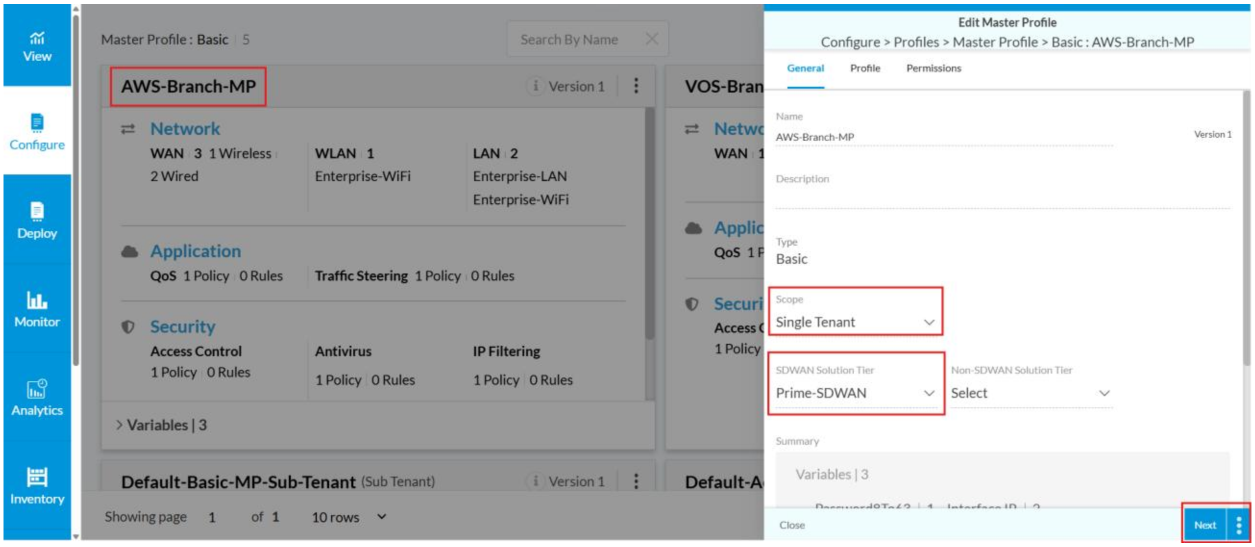


Clone Basic Master Profile Default-Basic-MP

AWS-Branch-MP

Cancel Submit

Click on Edit Master Profile, under General tab provide the “Scope”, “SDWAN Solution Tier” and click on Next.



Edit Master Profile

Configure > Profiles > Master Profile > Basic : AWS-Branch-MP

General Profile Permissions

Name: AWS-Branch-MP Version 1

Description

Type: Basic

Scope: Single Tenant

SDWAN Solution Tier: Prime-SDWAN

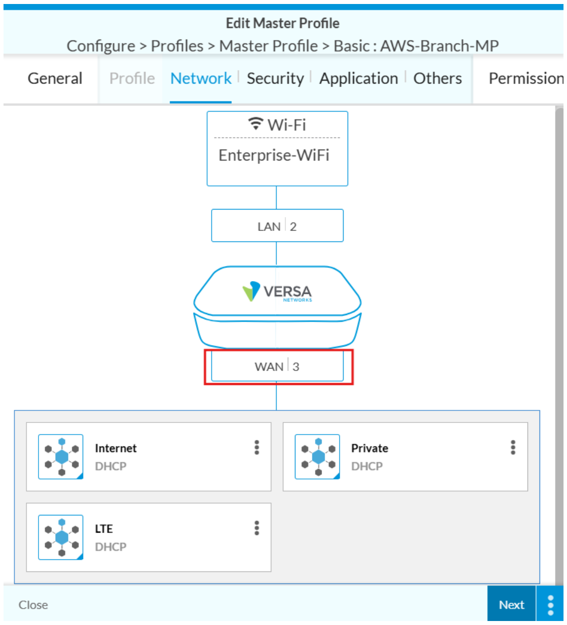
Non-SDWAN Solution Tier: Select

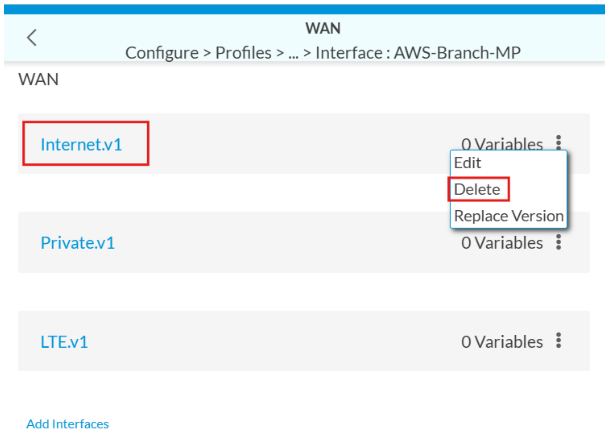
Summary

Variables | 3

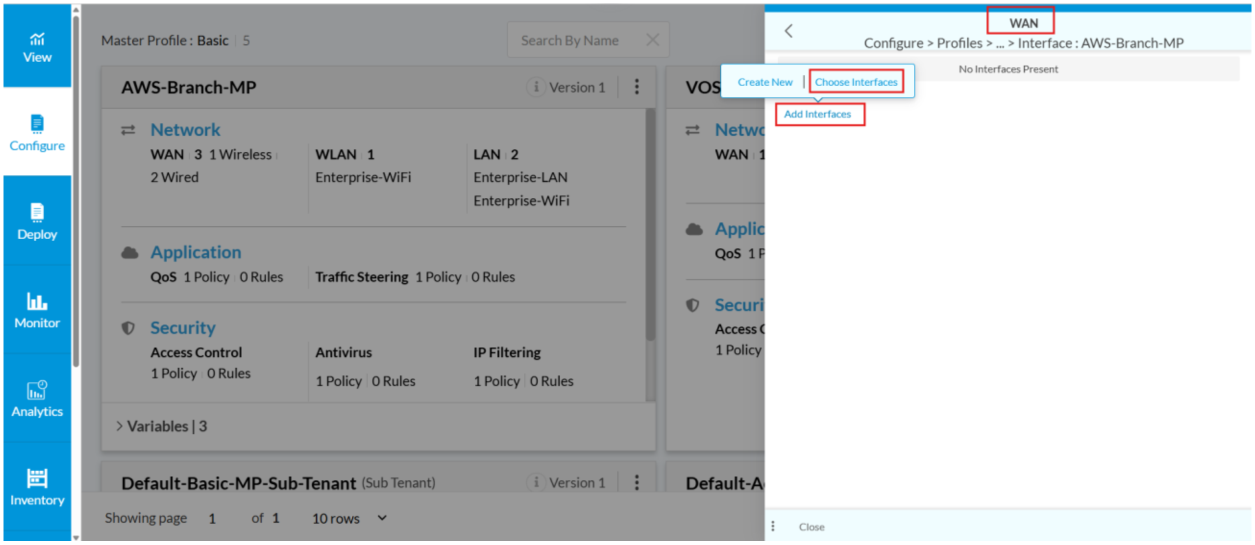
Close Next

Click on WAN and remove all the interfaces.

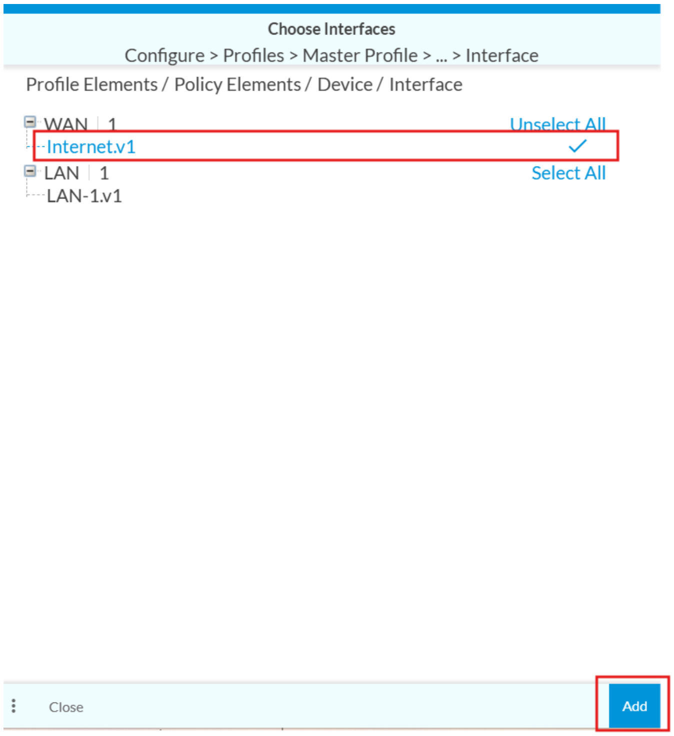




One all the interfaces are removed under WAN, click on “Add Interfaces” and select “Choose Interfaces”.



Choose the WAN interface which we have created earlier and click on Add.



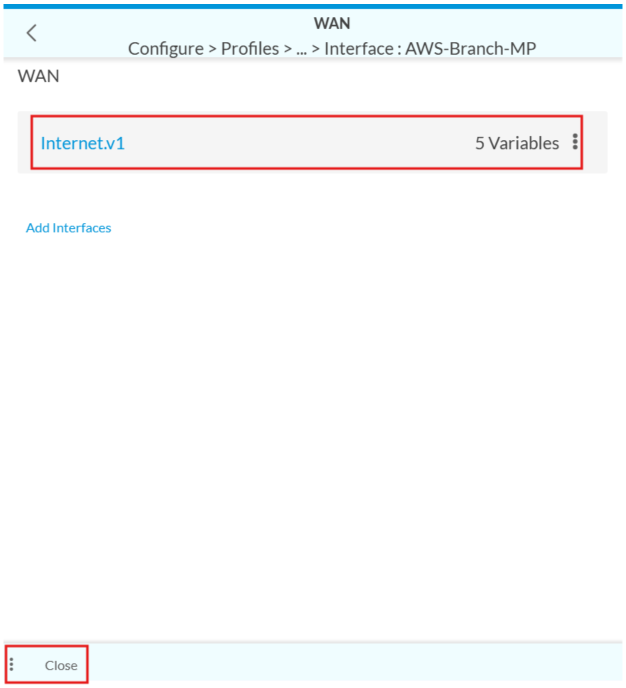
Choose Interfaces

Configure > Profiles > Master Profile > ... > Interface

Profile Elements / Policy Elements / Device / Interface

- WAN | 1 — Unselect All
  - Internet.v1 ✓
- LAN | 1 — Select All
  - LAN-1.v1

Once added click on Close.



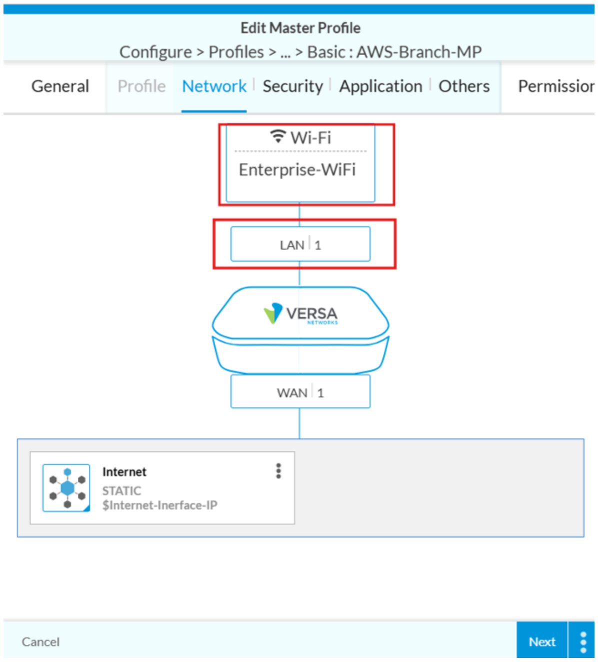
WAN

Configure > Profiles > ... > Interface : AWS-Branch-MP

WAN

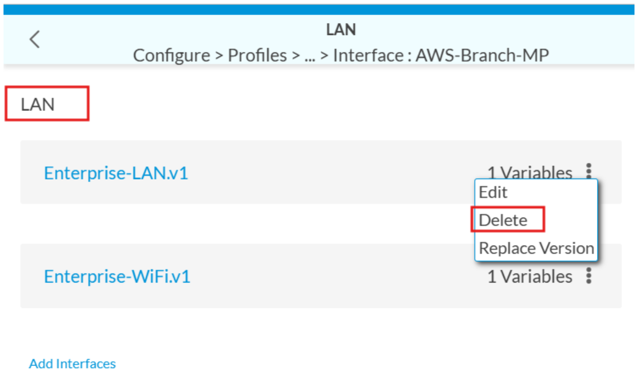
Internet.v1 — 5 Variables

Repeat the same for LAN interfaces



Edit Master Profile

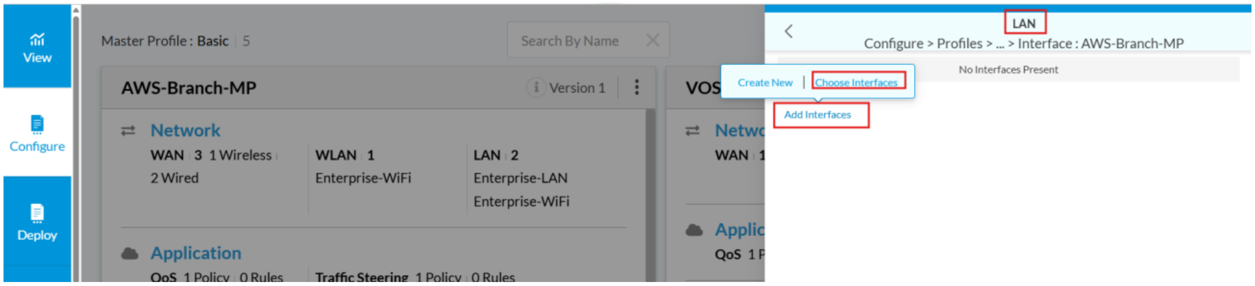
Configure > Profiles > ... > Basic : AWS-Branch-MP



LAN

Configure > Profiles > ... > Interface : AWS-Branch-MP

One all the interfaces are removed under LAN, click on “Add Interfaces” and select “Choose Interfaces”.



Master Profile : Basic | 5

AWS-Branch-MP

Network

WAN | 3 | 1 Wireless | 2 Wired

WLAN | 1 | Enterprise-WiFi

LAN | 2 | Enterprise-LAN | Enterprise-WiFi

Application

QoS | 1 Policy | 0 Rules

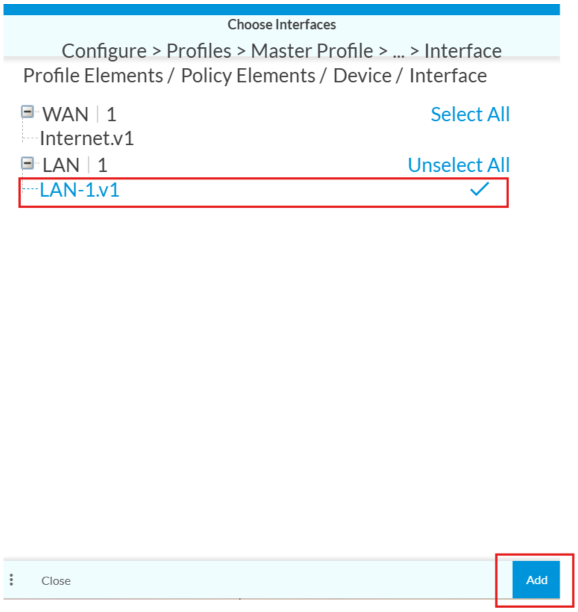
Traffic Steering | 1 Policy | 0 Rules

LAN

Configure > Profiles > ... > Interface : AWS-Branch-MP

No Interfaces Present

Choose the LAN interface which we have created earlier and click on Add.



Choose Interfaces

Configure > Profiles > Master Profile > ... > Interface

Profile Elements / Policy Elements / Device / Interface

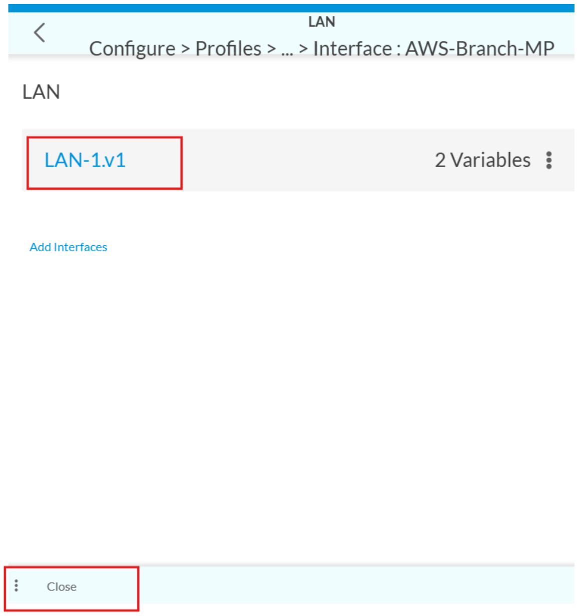
WAN | 1 — Select All

Internet.v1

LAN | 1 — Unselect All

LAN-1.v1 ✓

Once added click on Close.



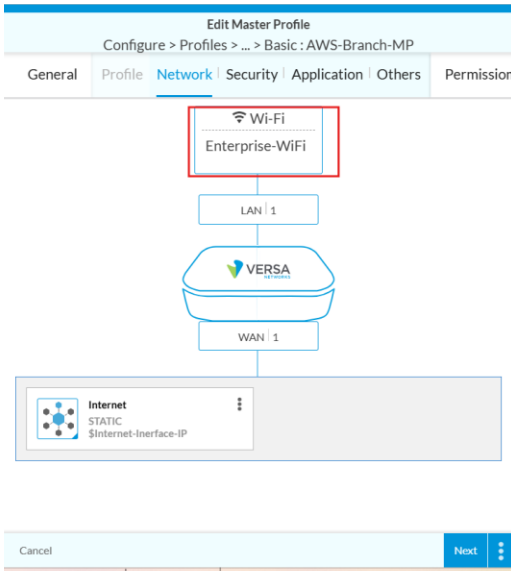
LAN

Configure > Profiles > ... > Interface : AWS-Branch-MP

LAN

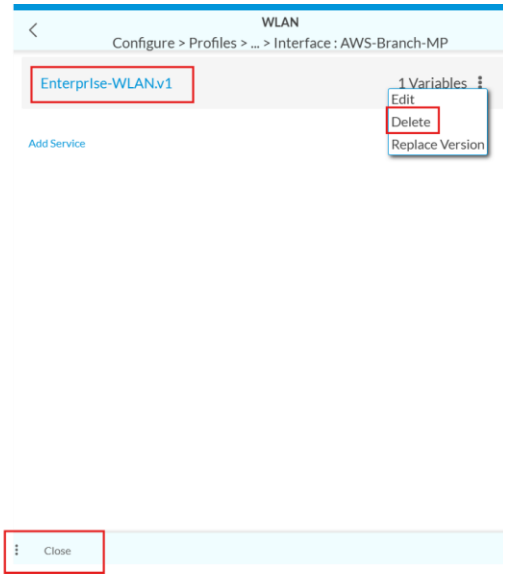
LAN-1.v1 2 Variables

Click on "Enterprise WiFi", select 3 dots and then delete.



Edit Master Profile

Configure > Profiles > ... > Basic : AWS-Branch-MP

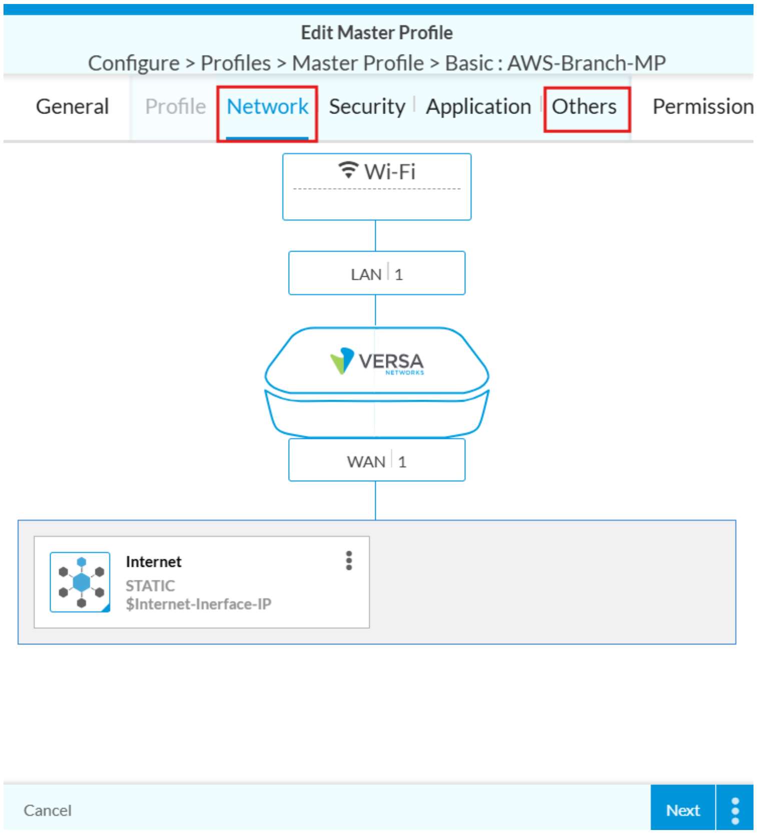


WLAN

Configure > Profiles > ... > Interface : AWS-Branch-MP

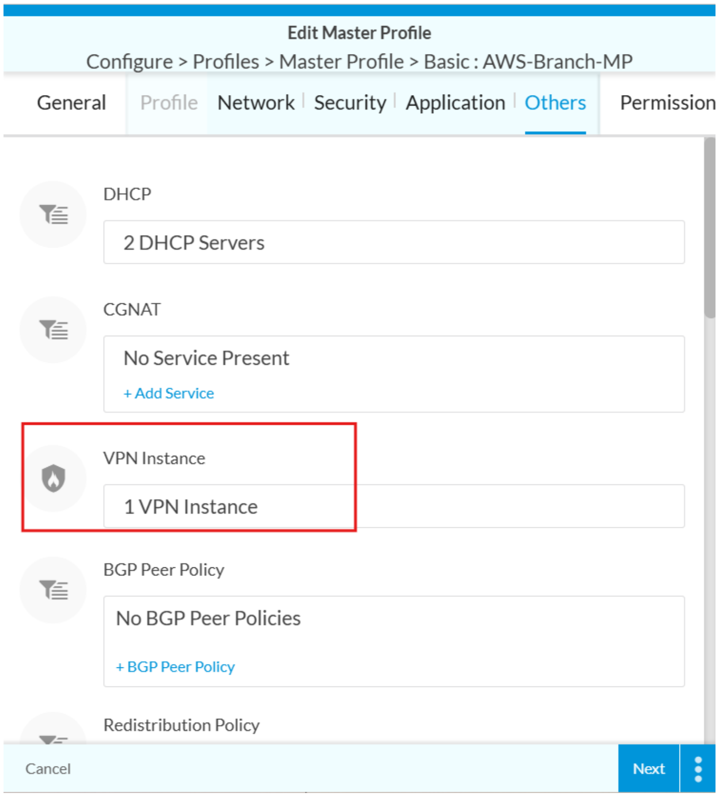
Enterprlse-WLAN.v1 1 Variables

Once the configuration is complete, move to Others tab.


Edit Master Profile

Configure > Profiles > Master Profile > Basic : AWS-Branch-MP

Under Others tab select VPN Instance.


Edit Master Profile

Configure > Profiles > Master Profile > Basic : AWS-Branch-MP

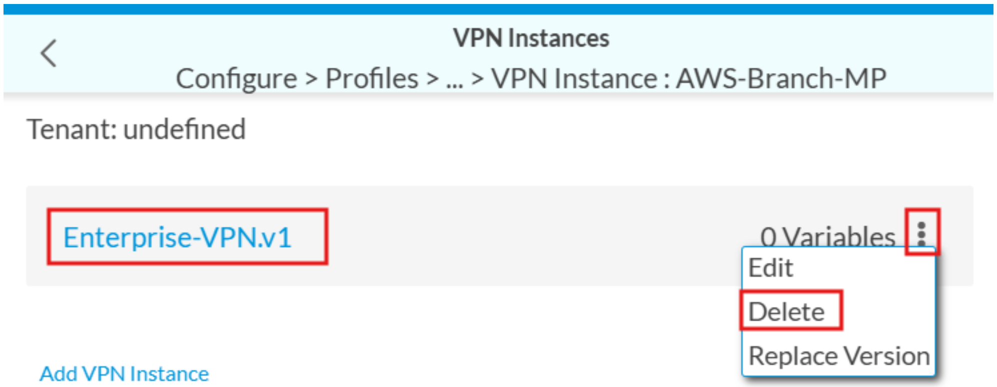
DHCP: 2 DHCP Servers

CGNAT: No Service Present

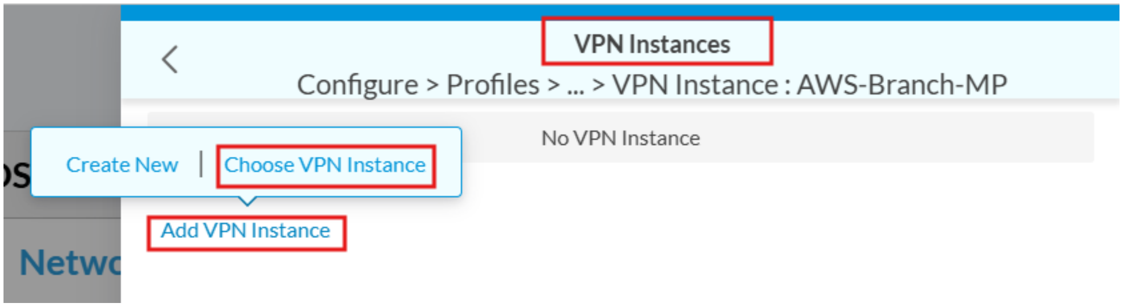
VPN Instance: 1 VPN Instance

BGP Peer Policy: No BGP Peer Policies

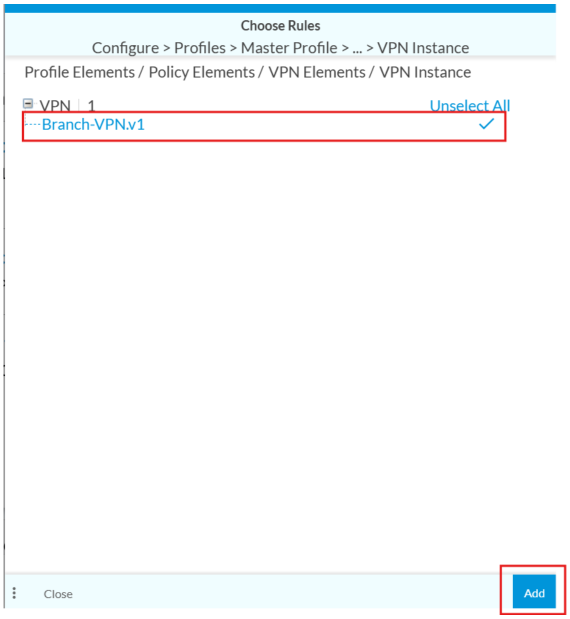
Delete the existing VPN instance and add the one which we have created.



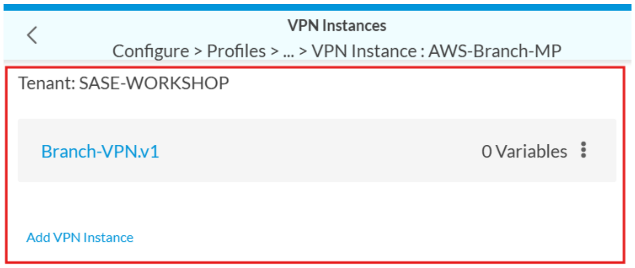
Under VPN Instances, click on “Add VPN Instance” and click on “Choose VPN Instance”.


VPN Instances
Configure > Profiles > ... > VPN Instance : AWS-Branch-MP
No VPN Instance
Create New | Choose VPN Instance
Add VPN Instance
Netwo

Select the VPN instance and click on Add.


Choose Rules
Configure > Profiles > Master Profile > ... > VPN Instance
Profile Elements / Policy Elements / VPN Elements / VPN Instance
VPN 1
Unselect All
Branch-VPN.v1 ✓
Close
Add

Once added, click on “Close” and save the Master profile.



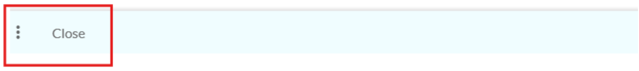
VPN Instances

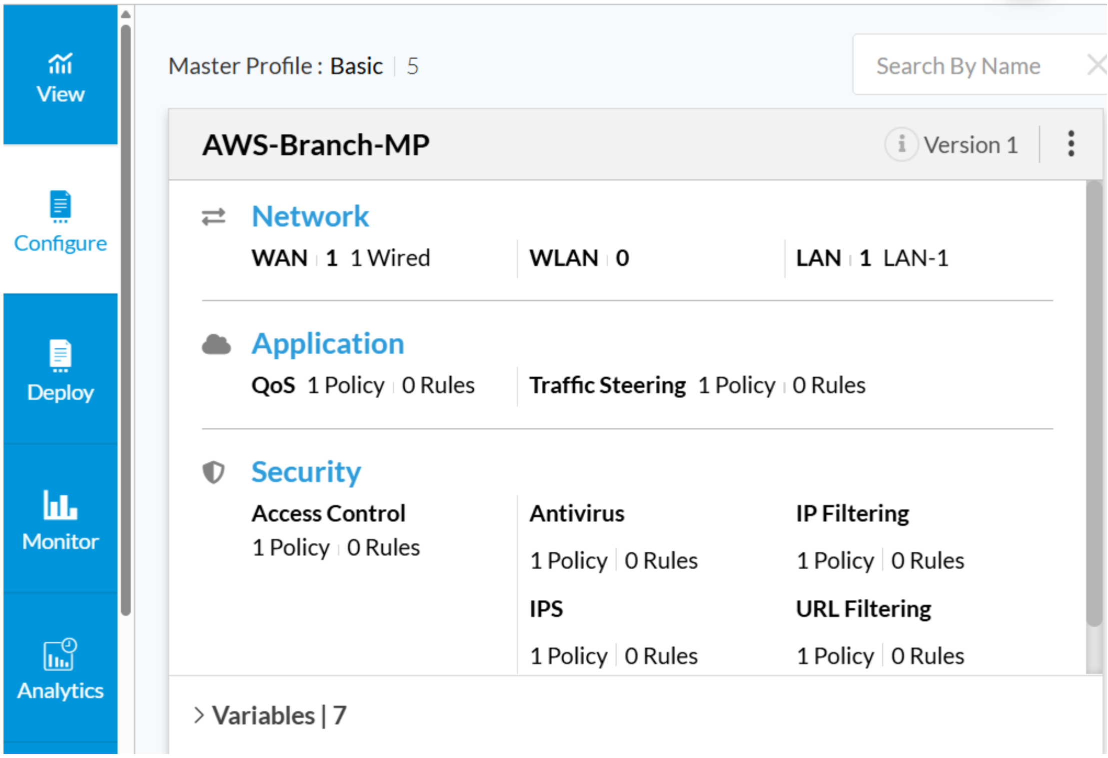
Configure > Profiles > ... > VPN Instance : AWS-Branch-MP

Tenant: SASE-WORKSHOP

Branch-VPN.v1 0 Variables

Add VPN Instance





Master Profile : Basic | 5

AWS-Branch-MP Version 1

**Network**

WAN | 1 | 1 Wired — WLAN | 0 — LAN | 1 | LAN-1

**Application**

QoS 1 Policy | 0 Rules — Traffic Steering 1 Policy | 0 Rules

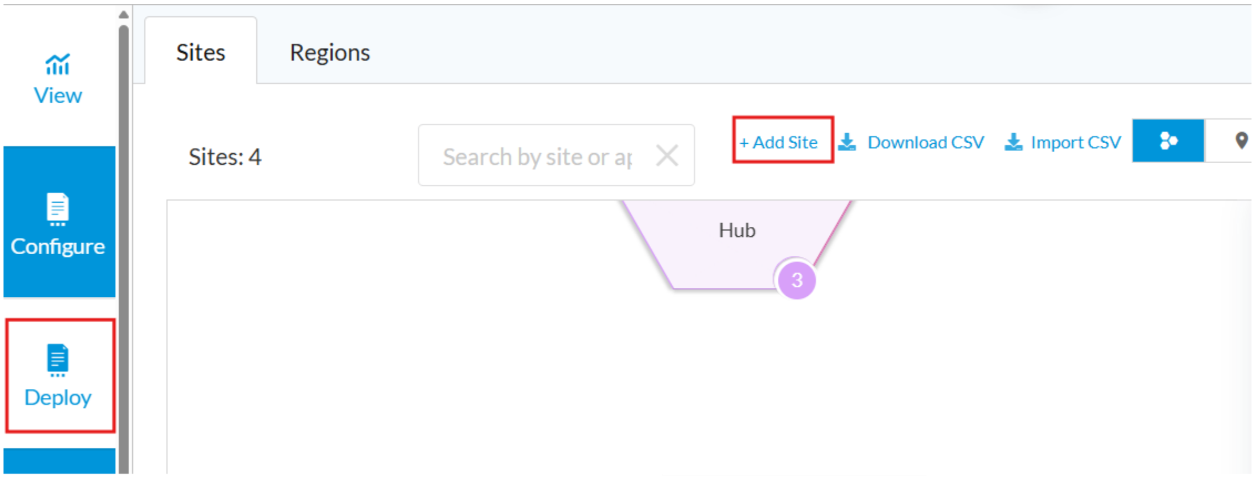
**Security**

| Access Control | Antivirus | IP Filtering |
|---|---|---|
| 1 Policy \| 0 Rules | 1 Policy \| 0 Rules | 1 Policy \| 0 Rules |
| | IPS | URL Filtering |
| | 1 Policy \| 0 Rules | 1 Policy \| 0 Rules |

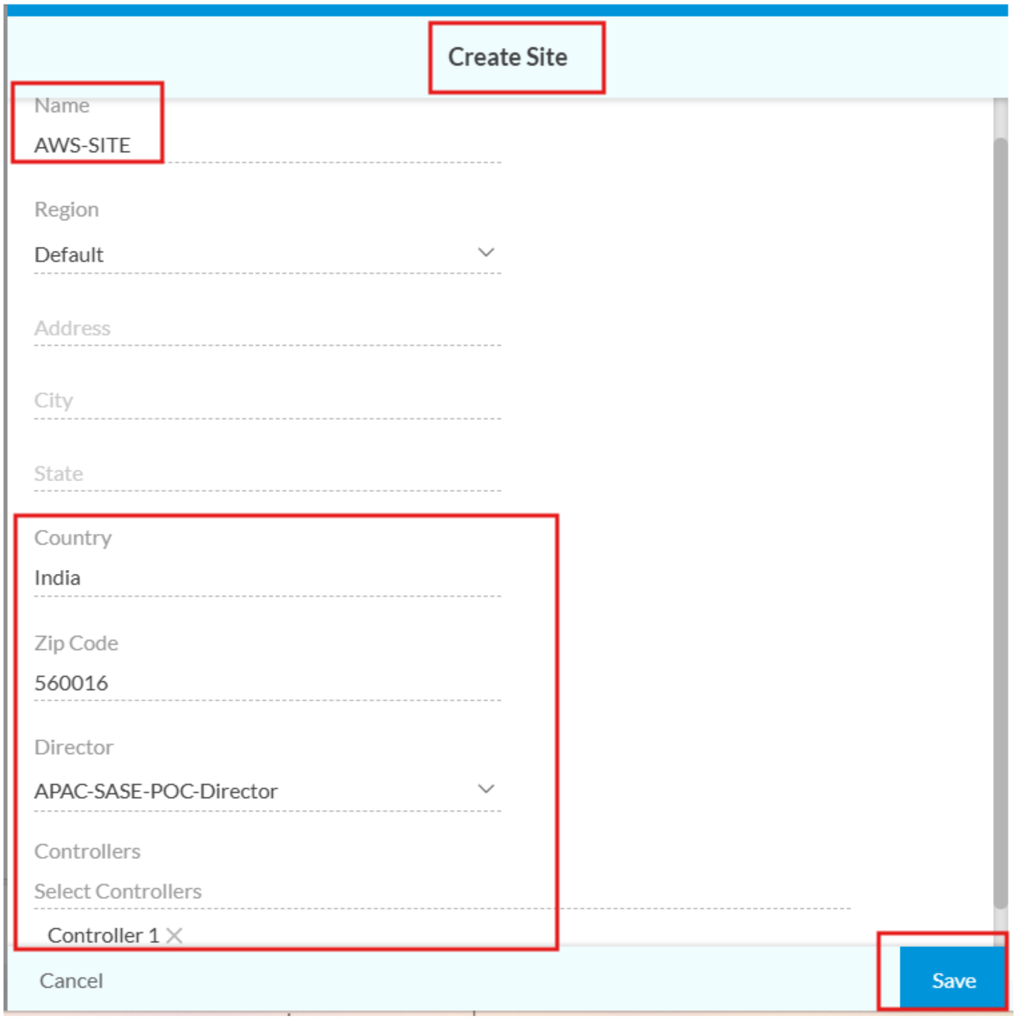
> Variables | 7

## Deploying the device:

Go to “Deploy” and click on Add Site.



Under Create Site, Provide Name, Country, Zip, Director details, controllers and click on Save.



Create Site

Name
AWS-SITE

Region
Default

Address

City

State

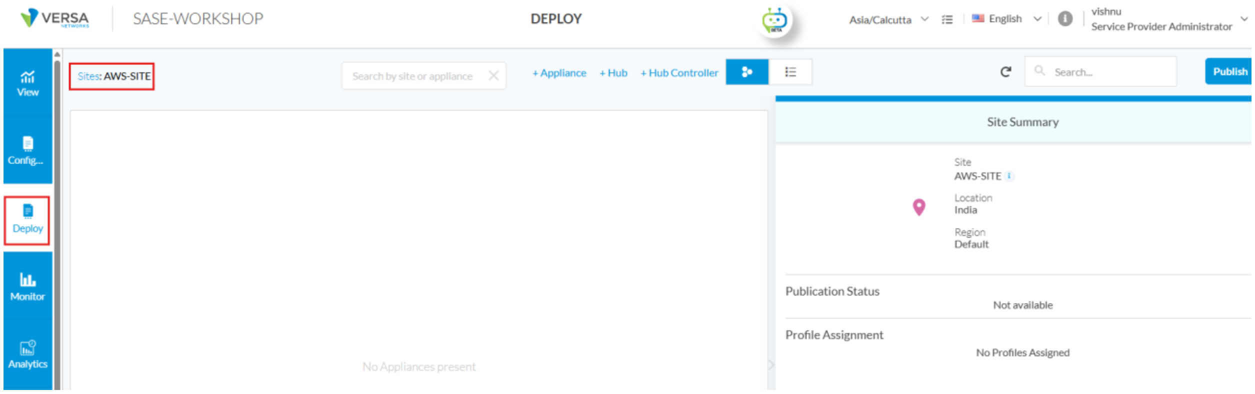
Country
India

Zip Code
560016

Director
APAC-SASE-POC-Director

Controllers
Select Controllers
Controller 1

Double click on the created site. It will take you to the below page.



Sites: AWS-SITE

Site Summary

Site: AWS-SITE
Location: India
Region: Default

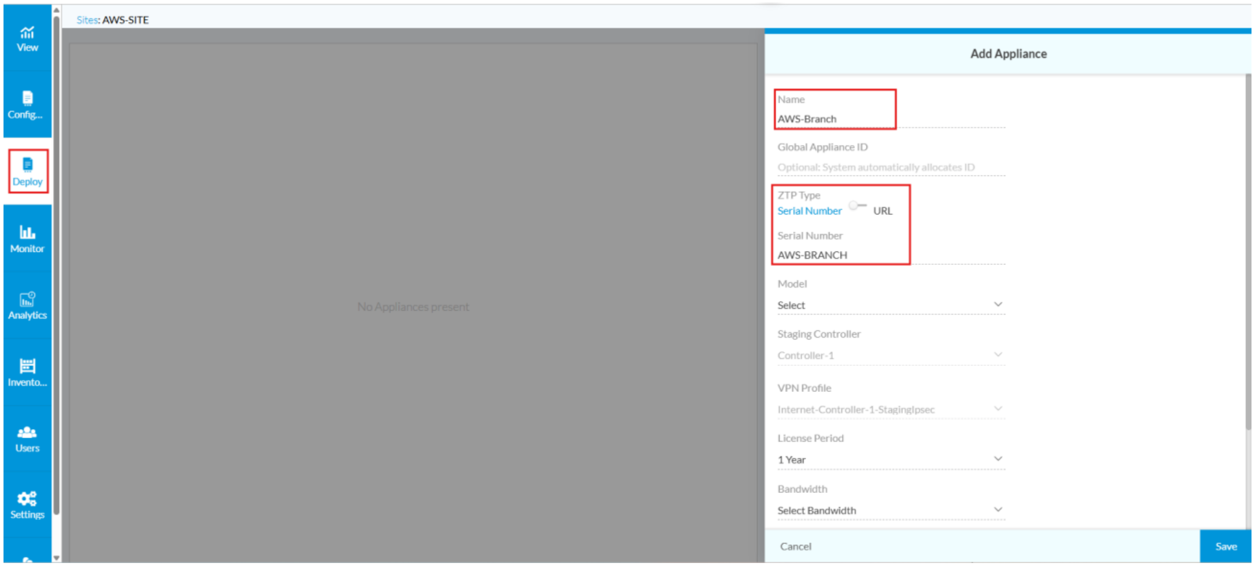
Publication Status: Not available

Profile Assignment: No Profiles Assigned

No Appliances present

Since we will be deploying a device with type as appliance, click on "+Appliance".

Under Add Appliance Provide necessary information and select the ZTP type as Serial for Script based ZTP.



Sites: AWS-SITE

No Appliances present

Add Appliance

Name: AWS-Branch

Global Appliance ID: Optional: System automatically allocates ID

ZTP Type: Serial Number ○ URL

Serial Number: AWS-BRANCH

Model: Select

Staging Controller: Controller-1

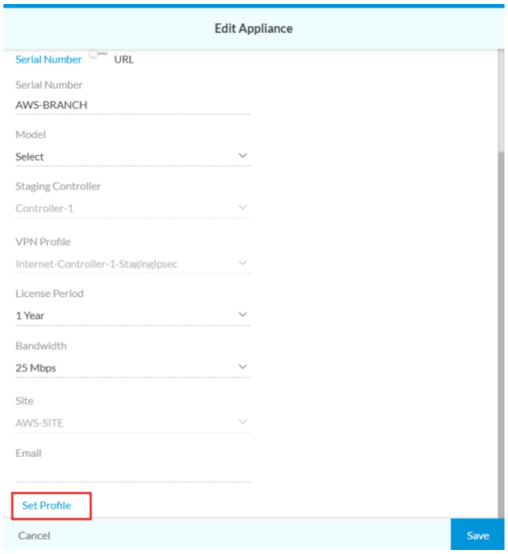
VPN Profile: Internet-Controller-1-StagingIpsec

License Period: 1 Year

Bandwidth: Select Bandwidth

Cancel
Save

Provide the Bandwidth and click on "Set Profile" to associate the master profile which we have created and click on "Apply" and save the Appliance.



Edit Appliance

Serial Number ○ URL

Serial Number: AWS-BRANCH

Model: Select

Staging Controller: Controller-1

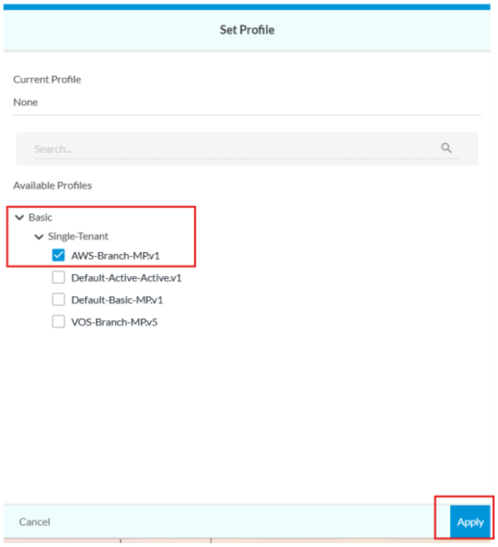
VPN Profile: Internet-Controller-1-StagingIpsec

License Period: 1 Year

Bandwidth: 25 Mbps

Site: AWS-SITE

Email:



Set Profile

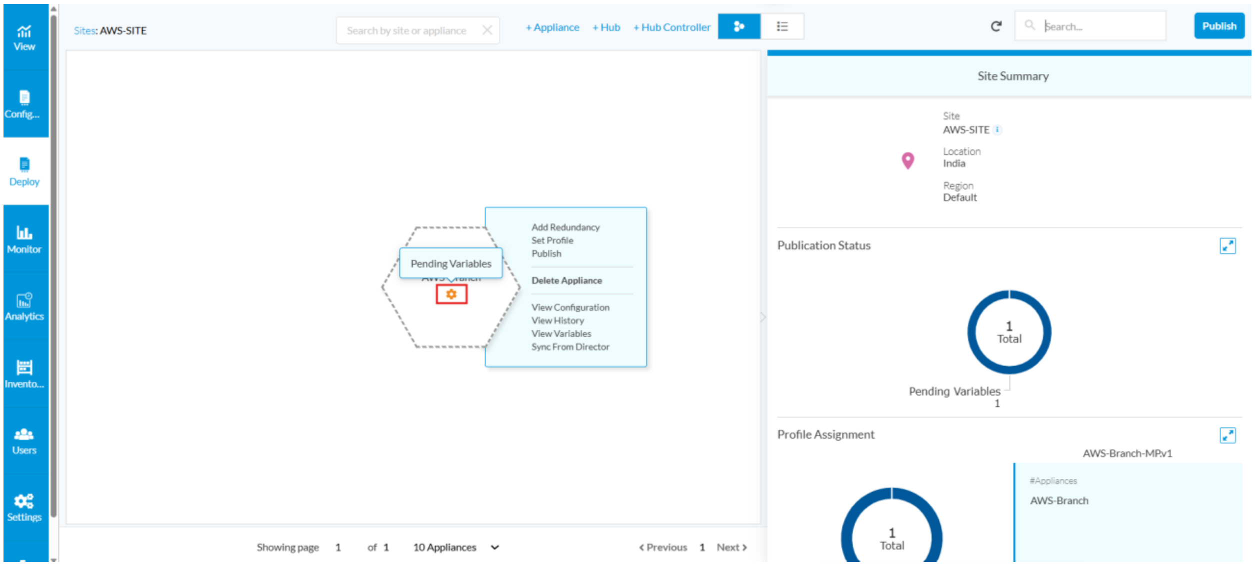
Current Profile: None

Available Profiles

- Basic
  - Single-Tenant
    - ☑ AWS-Branch-MPv1
    - □ Default-Active-Active.v1
    - □ Default-Basic-MPv1
    - □ VOS-Branch-MPv5

All the Parameters provided under Profile elements should be filled under Pending Variables in "Deploy" tab while creating the device.

When you hover onto the Gear icon, it shows pending variables, click on it to fill the variables.



Site Summary

Site: AWS-SITE

Location: India

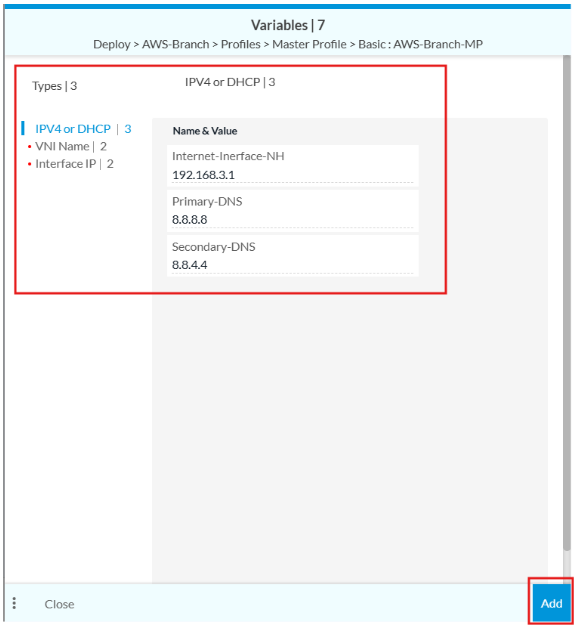
Region: Default

Publication Status

Profile Assignment

Add the pending variables and click on Add.

Review the configuration of the appliance and click on Save.



Variables | 7

Deploy > AWS-Branch > Profiles > Master Profile > Basic : AWS-Branch-MP

Types | 3

IPV4 or DHCP | 3

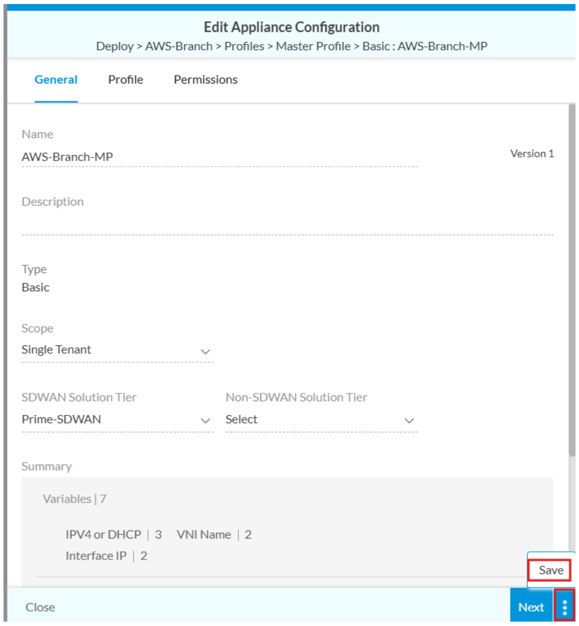
- IPV4 or DHCP | 3
- VNI Name | 2
- Interface IP | 2

Name & Value

Internet-Inerface-NH
192.168.3.1

Primary-DNS
8.8.8.8

Secondary-DNS
8.8.4.4



Edit Appliance Configuration

Deploy > AWS-Branch > Profiles > Master Profile > Basic : AWS-Branch-MP

Name: AWS-Branch-MP — Version 1

Description

Type: Basic

Scope: Single Tenant

SDWAN Solution Tier: Prime-SDWAN

Non-SDWAN Solution Tier: Select

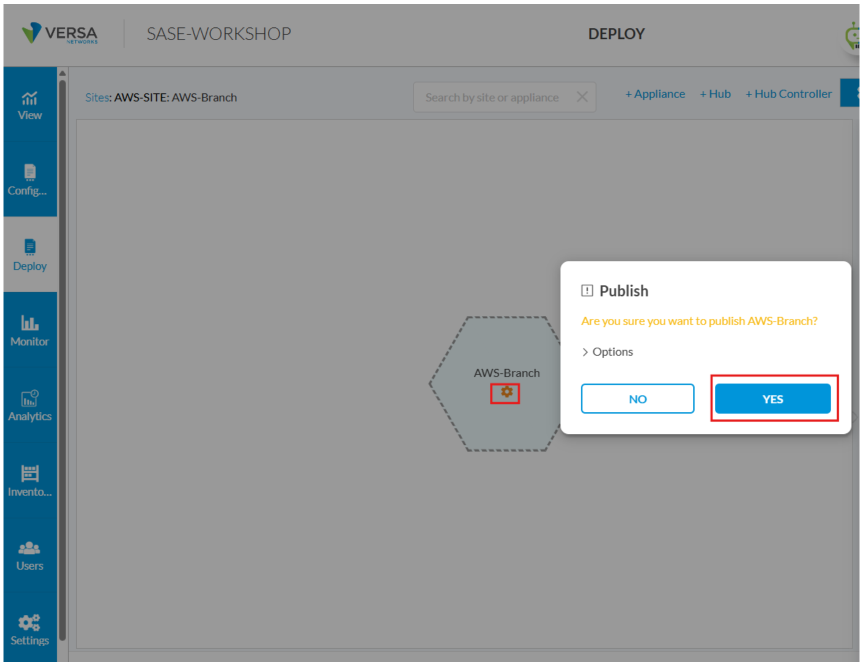
Summary

Variables | 7

IPV4 or DHCP | 3 VNI Name | 2

Interface IP | 2

To Publish the configuration on to the Director, click on Publish.



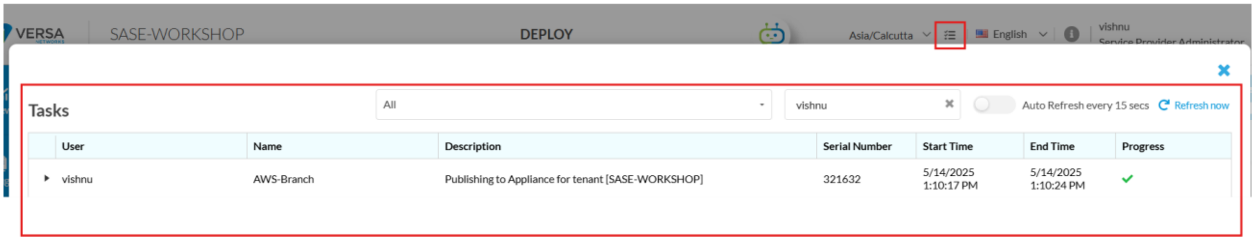
Sites: AWS-SITE: AWS-Branch

Publish

Are you sure you want to publish AWS-Branch?

> Options

Once the device is published, we can check the status in the tasks.

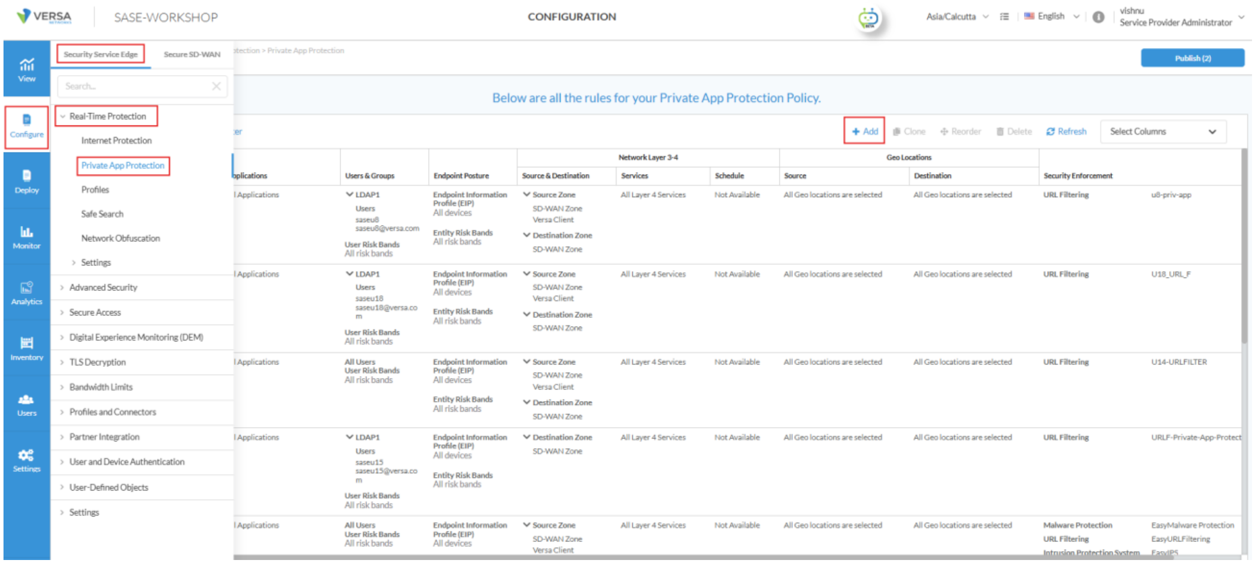


Tasks

| User | Name | Description | Serial Number | Start Time | End Time | Progress |
|---|---|---|---|---|---|---|
| vishnu | AWS-Branch | Publishing to Appliance for tenant [SASE-WORKSHOP] | 321632 | 5/14/2025 1:10:17 PM | 5/14/2025 1:10:24 PM | ✓ |

## Creating Private app Protection Rule:

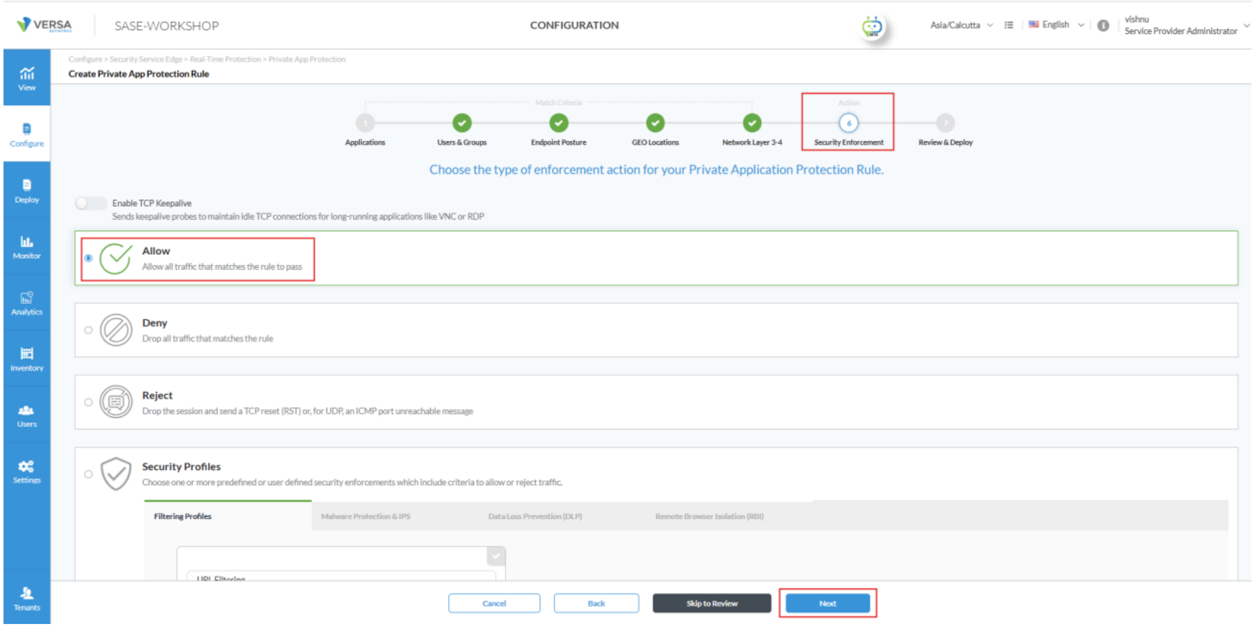
To Create a secure access rule for allowing traffic from SASE clients to Azure VM through overlay tunnels, Go to Configure → Secure Service Edge → Real-Time Protection → Private App Protection and click on “Add”.



Below are all the rules for your Private App Protection Policy.

|  |  |  | Network Layer 3-4 |  |  | Geo Locations |  |  |  |
|---|---|---|---|---|---|---|---|---|---|
| …plications | Users & Groups | Endpoint Posture | Source & Destination | Services | Schedule | Source | Destination | Security Enforcement |  |
| …l Applications | LDAP1<br>Users<br>saseu8<br>saseu8@versa.com<br>User Risk Bands<br>All risk bands | Endpoint Information Profile (EIP)<br>All devices<br>Entity Risk Bands<br>All risk bands | Source Zone<br>SD-WAN Zone<br>Versa Client<br>Destination Zone<br>SD-WAN Zone | All Layer 4 Services | Not Available | All Geo locations are selected | All Geo locations are selected | URL Filtering | u8-priv-app |
| …l Applications | LDAP1<br>Users<br>saseu18<br>saseu18@versa.co m<br>User Risk Bands<br>All risk bands | Endpoint Information Profile (EIP)<br>All devices<br>Entity Risk Bands<br>All risk bands | Source Zone<br>SD-WAN Zone<br>Versa Client<br>Destination Zone<br>SD-WAN Zone | All Layer 4 Services | Not Available | All Geo locations are selected | All Geo locations are selected | URL Filtering | U18_URL_F |
| …l Applications | All Users<br>User Risk Bands<br>All risk bands | Endpoint Information Profile (EIP)<br>All devices<br>Entity Risk Bands<br>All risk bands | Source Zone<br>SD-WAN Zone<br>Versa Client<br>Destination Zone<br>SD-WAN Zone | All Layer 4 Services | Not Available | All Geo locations are selected | All Geo locations are selected | URL Filtering | U14-URLFILTER |
| …l Applications | LDAP1<br>Users<br>saseu15<br>saseu15@versa.co m<br>User Risk Bands<br>All risk bands | Endpoint Information Profile (EIP)<br>All devices<br>Entity Risk Bands<br>All risk bands | Destination Zone<br>SD-WAN Zone | All Layer 4 Services | Not Available | All Geo locations are selected | All Geo locations are selected | URL Filtering | URLF-Private-App-Protect |
| …l Applications | All Users<br>User Risk Bands<br>All risk bands | Endpoint Information Profile (EIP)<br>All devices | Source Zone<br>SD-WAN Zone<br>Versa Client | All Layer 4 Services | Not Available | All Geo locations are selected | All Geo locations are selected | Malware Protection<br>URL Filtering<br>Intrusion Protection System | EasyMalware Protection<br>EasyURLFiltering<br>EasyIPS |

Leave everything to default and Under “Security Enforcement” Configure the action as “Allow”.



Create Private App Protection Rule

Choose the type of enforcement action for your Private Application Protection Rule.

○ Enable TCP Keepalive
Sends keepalive probes to maintain idle TCP connections for long-running applications like VNC or RDP

● Allow
Allow all traffic that matches the rule to pass

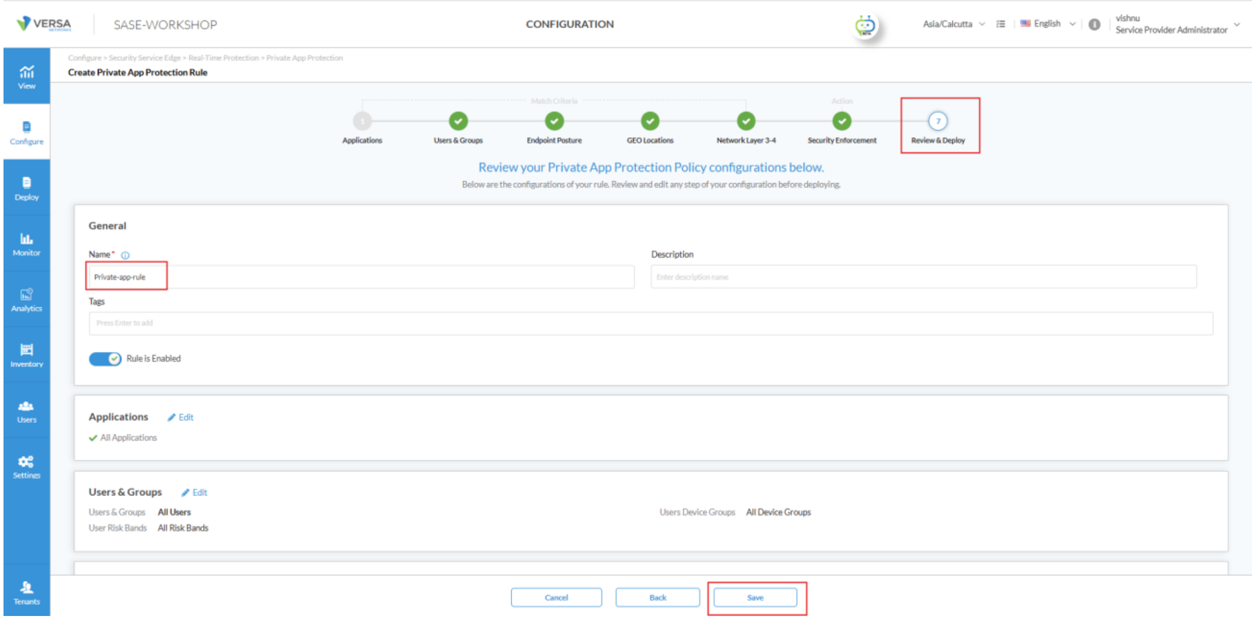
○ Deny
Drop all traffic that matches the rule

○ Reject
Drop the session and send a TCP reset (RST) or, for UDP, an ICMP port unreachable message

○ Security Profiles
Choose one or more predefined or user defined security enforcements which include criteria to allow or reject traffic.

**Note**: Security Enforcement and match criteria can be configured as per the requirement.

Under “Review and Deploy” provide the “Name” for the Private App Protection Rule and click on “Save”.



Configure > Security Service Edge > Real-Time Protection > Private App Protection

Create Private App Protection Rule

Review your Private App Protection Policy configurations below.

Below are the configurations of your rule. Review and edit any step of your configuration before deploying.

General

Name*: Private-app-rule

Description: Enter description name

Tags: Press Enter to add

Rule is Enabled

Applications ✎ Edit

✓ All Applications

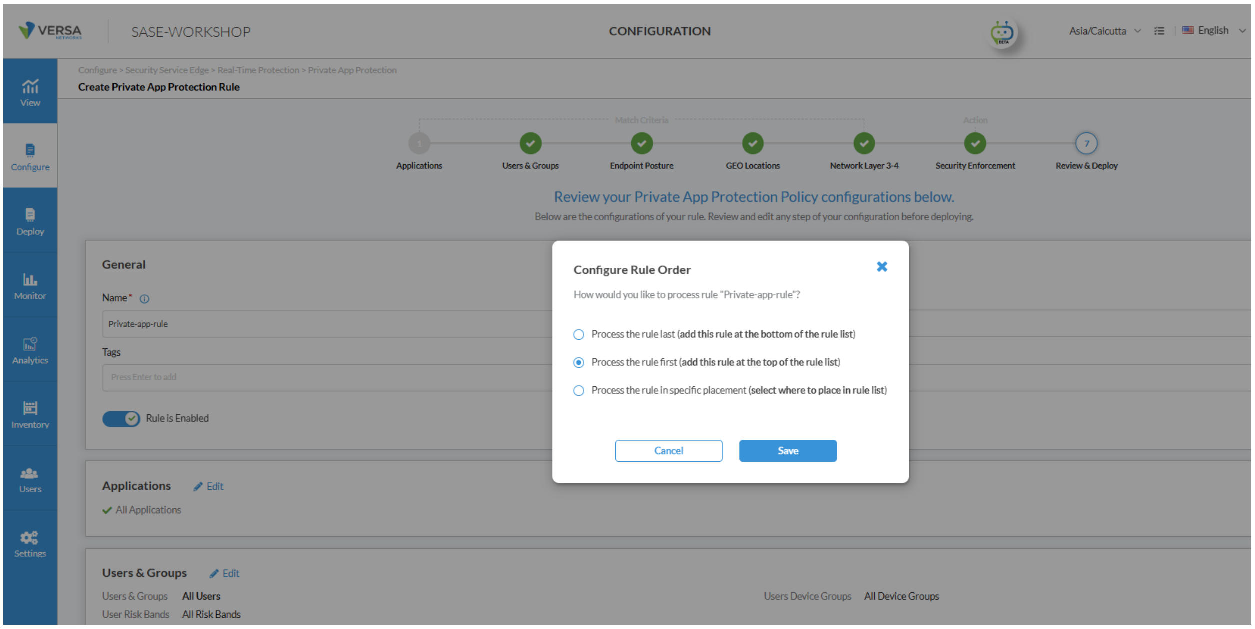
Users & Groups ✎ Edit

Users & Groups: All Users

User Risk Bands: All Risk Bands

Users Device Groups: All Device Groups

Under “Configure the Rule Order” place the rule at the top.



Configure > Security Service Edge > Real-Time Protection > Private App Protection

Create Private App Protection Rule

Review your Private App Protection Policy configurations below.

Below are the configurations of your rule. Review and edit any step of your configuration before deploying.

Configure Rule Order

How would you like to process rule "Private-app-rule"?

○ Process the rule last (add this rule at the bottom of the rule list)

● Process the rule first (add this rule at the top of the rule list)

○ Process the rule in specific placement (select where to place in rule list)

General

Name*: Private-app-rule

Tags: Press Enter to add

Rule is Enabled

Applications ✎ Edit

✓ All Applications

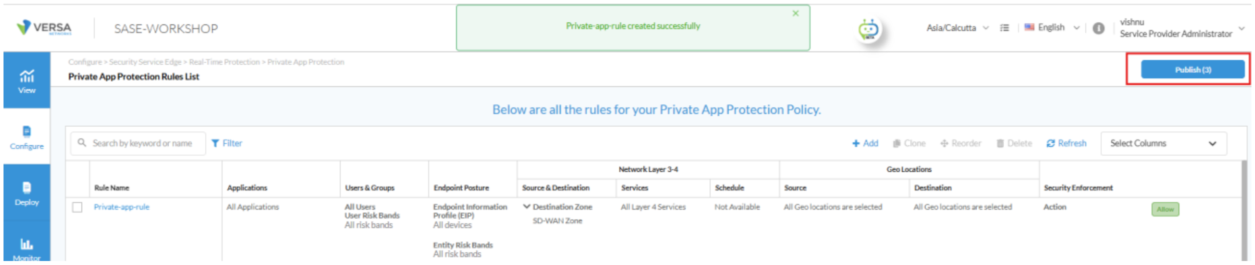
Users & Groups ✎ Edit

Users & Groups: All Users

User Risk Bands: All Risk Bands

Users Device Groups: All Device Groups

Once the configuration is complete Publish the Configuration to SASE Gateways.



Private-app-rule created successfully

Configure > Security Service Edge > Real-Time Protection > Private App Protection

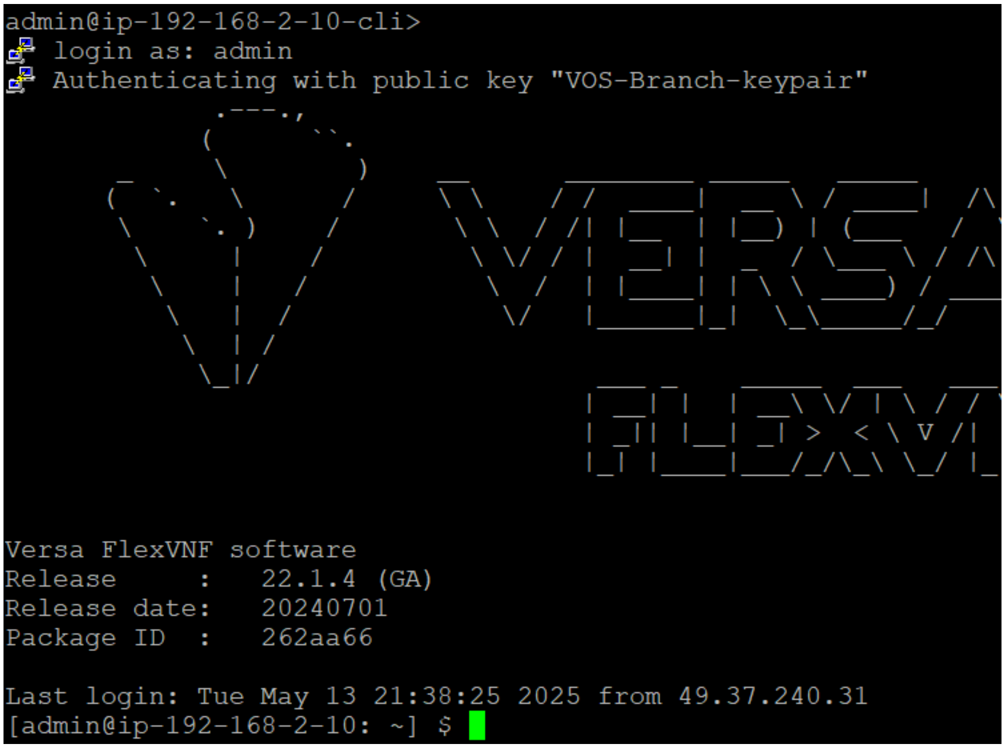
Private App Protection Rules List

Below are all the rules for your Private App Protection Policy.

| | | | | Network Layer 3-4 | | | Geo Locations | | |
|---|---|---|---|---|---|---|---|---|---|
| Rule Name | Applications | Users & Groups | Endpoint Posture | Source & Destination | Services | Schedule | Source | Destination | Security Enforcement |
| Private-app-rule | All Applications | All Users<br>User Risk Bands<br>All risk bands | Endpoint Information Profile (EIP)<br>All devices<br>Entity Risk Bands<br>All risk bands | Destination Zone<br>SD-WAN Zone | All Layer 4 Services | Not Available | All Geo locations are selected | All Geo locations are selected | Action Allow |

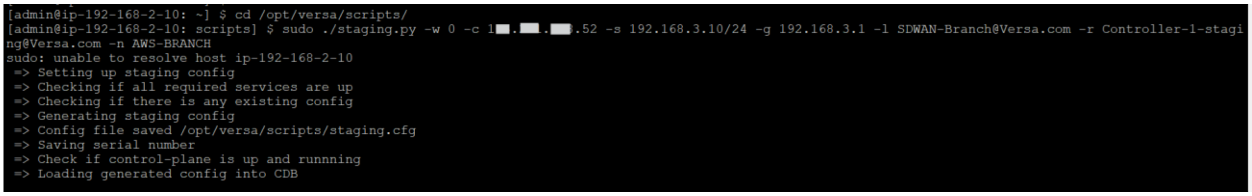
## Onboarding VOS:

SSH to the AWS VOS EC2 instance. (refer Accessing EC2 Instance) and login with username admin.



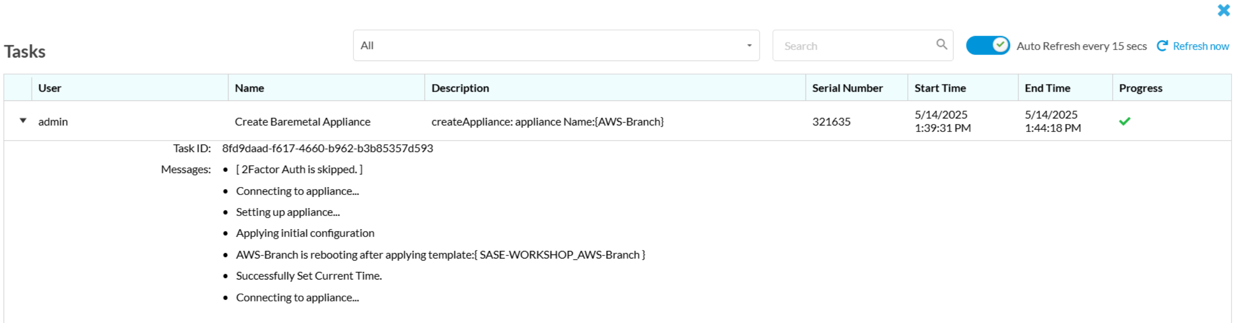
```
admin@ip-192-168-2-10-cli>
 login as: admin
 Authenticating with public key "VOS-Branch-keypair"

Versa FlexVNF software
Release      :   22.1.4 (GA)
Release date:   20240701
Package ID  :   262aa66

Last login: Tue May 13 21:38:25 2025 from 49.37.240.31
[admin@ip-192-168-2-10: ~] $
```

To perform ZTP, run the staging.py script



```
[admin@ip-192-168-2-10: ~] $ cd /opt/versa/scripts/
[admin@ip-192-168-2-10: scripts] $ sudo ./staging.py -w 0 -c 1[redacted].[redacted].[redacted].52 -s 192.168.3.10/24 -g 192.168.3.1 -l SDWAN-Branch@Versa.com -r Controller-1-stagi
ng@Versa.com -n AWS-BRANCH
sudo: unable to resolve host ip-192-168-2-10
 => Setting up staging config
 => Checking if all required services are up
 => Checking if there is any existing config
 => Generating staging config
 => Config file saved /opt/versa/scripts/staging.cfg
 => Saving serial number
 => Check if control-plane is up and runnning
 => Loading generated config into CDB
```

Check the status on the task bar.

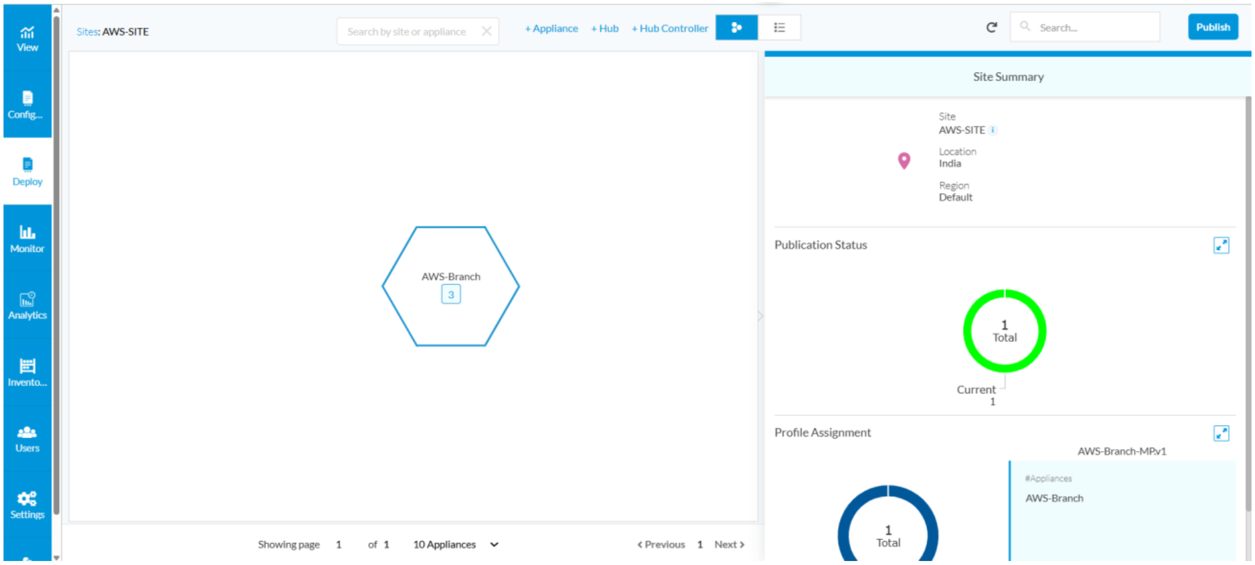


|  | User | Name | Description | Serial Number | Start Time | End Time | Progress |
|---|---|---|---|---|---|---|---|
| ▾ | admin | Create Baremetal Appliance | createAppliance: appliance Name:[AWS-Branch] | 321635 | 5/14/2025<br>1:39:31 PM | 5/14/2025<br>1:44:18 PM | ✓ |

Task ID: 8fd9daad-f617-4660-b962-b3b85357d593

Messages:
- [ 2Factor Auth is skipped. ]
- Connecting to appliance...
- Setting up appliance...
- Applying initial configuration
- AWS-Branch is rebooting after applying template:[ SASE-WORKSHOP_AWS-Branch ]
- Successfully Set Current Time.
- Connecting to appliance...

Once the device is onboarded it will show up in Concerto.



Sites: AWS-SITE

Site Summary

Site
AWS-SITE

Location
India

Region
Default

Publication Status: 1 Total, Current 1

Profile Assignment: AWS-Branch-MPv1, 1 Total

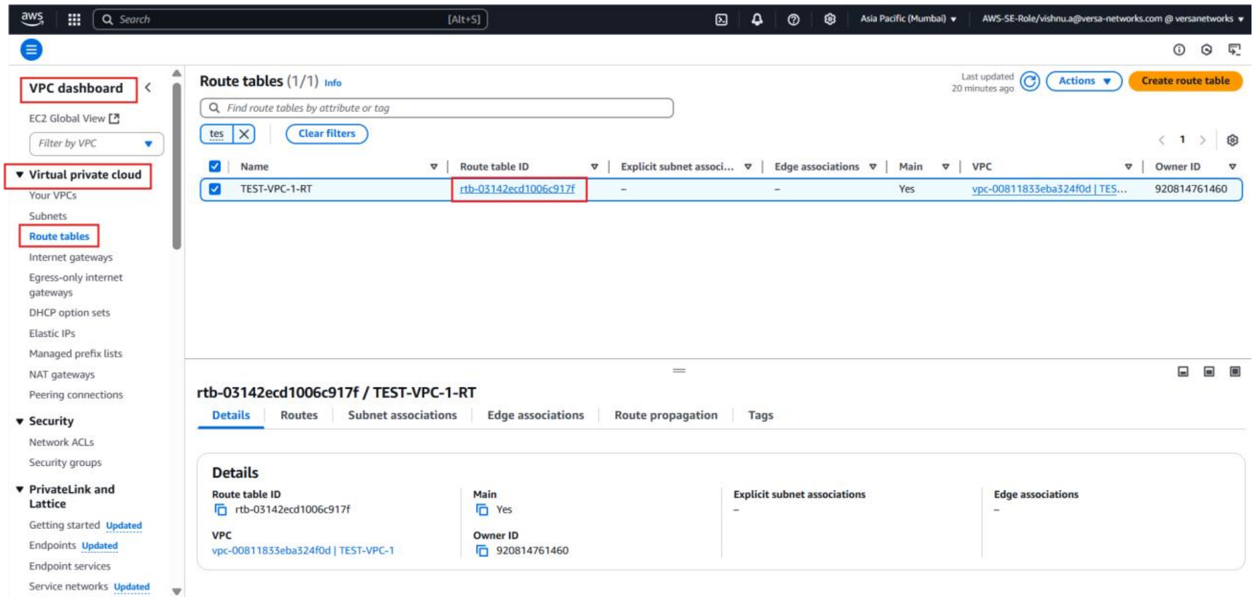
#Appliances
AWS-Branch

Showing page 1 of 1 10 Appliances

## Routing in AWS:

For an EC2 instance to reach the subnets connected to SASE GW we need to create a static route towards VOS LAN interface on the Main Routing table of VPC.

Under VPC dashboard, go to Virtual Private Cloud → Route tables and select the Main Route table of your VPC.



Route tables (1/1)

Last updated 20 minutes ago

| ☑ | Name | Route table ID | Explicit subnet associ... | Edge associations | Main | VPC | Owner ID |
|---|---|---|---|---|---|---|---|
| ☑ | TEST-VPC-1-RT | rtb-03142ecd1006c917f | – | – | Yes | vpc-00811833eba324f0d \| TES... | 920814761460 |

rtb-03142ecd1006c917f / TEST-VPC-1-RT

Details

Route table ID
rtb-03142ecd1006c917f

Main
Yes

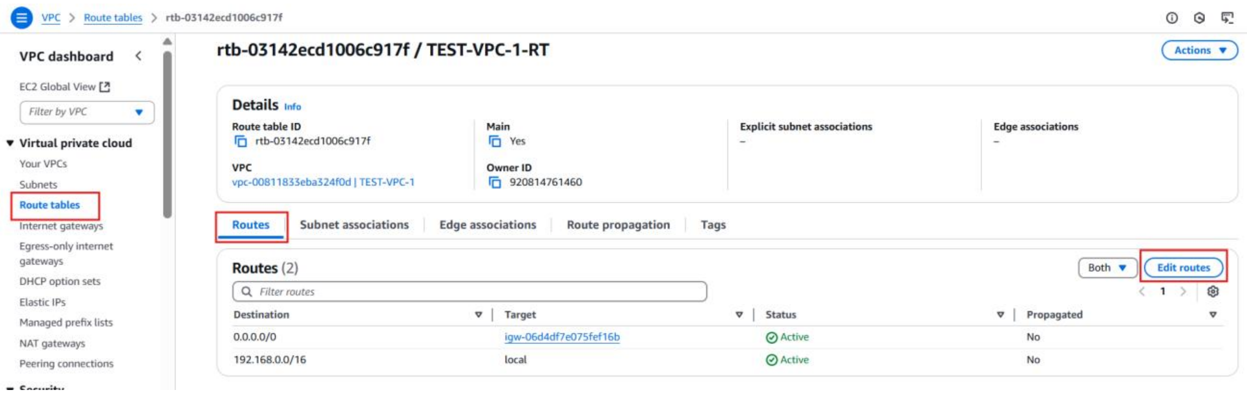
Explicit subnet associations
–

Edge associations
–

VPC
vpc-00811833eba324f0d | TEST-VPC-1

Owner ID
920814761460

Once clicking on “Route Table ID”, under Routes click on “Edit routes”.



VPC > Route tables > rtb-03142ecd1006c917f

rtb-03142ecd1006c917f / TEST-VPC-1-RT

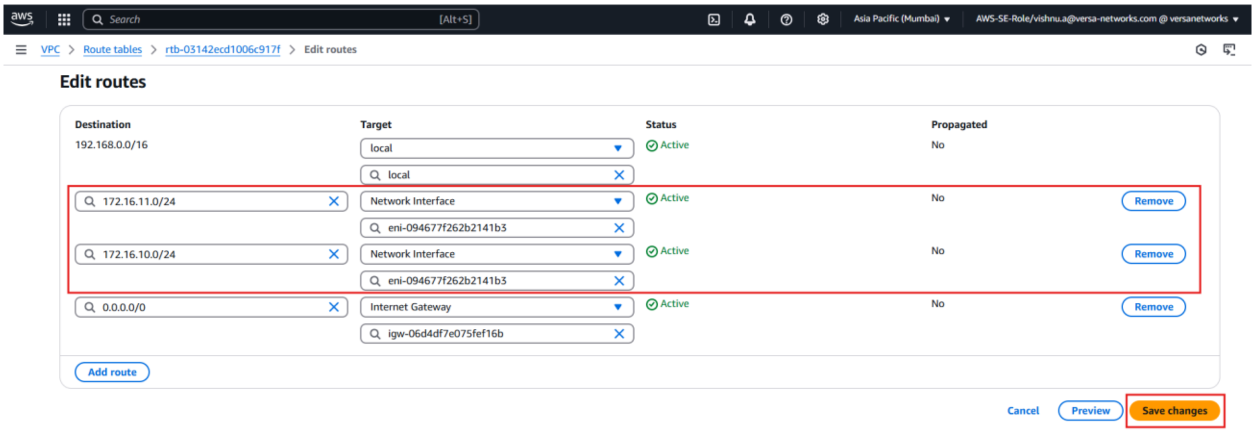
Details Info

| Route table ID | Main | Explicit subnet associations | Edge associations |
|---|---|---|---|
| rtb-03142ecd1006c917f | Yes | – | – |
| VPC<br>vpc-00811833eba324f0d \| TEST-VPC-1 | Owner ID<br>920814761460 | | |

Routes (2)

| Destination | Target | Status | Propagated |
|---|---|---|---|
| 0.0.0.0/0 | igw-06d4df7e075fef16b | Active | No |
| 192.168.0.0/16 | local | Active | No |

Under destination add the SASE Client pools with the target as VOS-Branch LAN interface and save the changes.

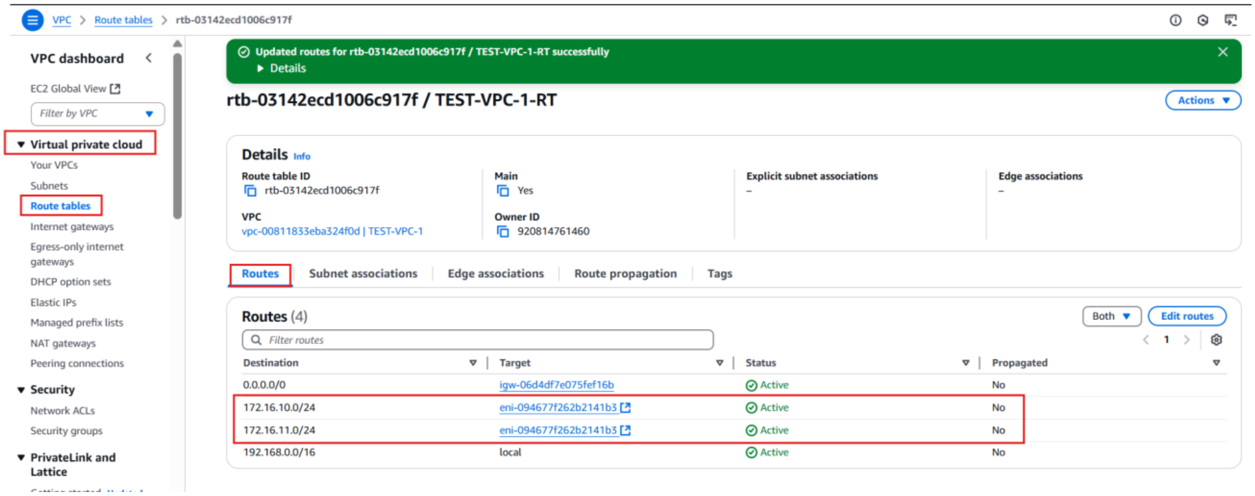


VPC > Route tables > rtb-03142ecd1006c917f > Edit routes

Edit routes

| Destination | Target | Status | Propagated |
|---|---|---|---|
| 192.168.0.0/16 | local<br>local | Active | No |
| 172.16.11.0/24 | Network Interface<br>eni-094677f262b2141b3 | Active | No |
| 172.16.10.0/24 | Network Interface<br>eni-094677f262b2141b3 | Active | No |
| 0.0.0.0/0 | Internet Gateway<br>igw-06d4df7e075fef16b | Active | No |

Once saved the routes should be visible in the Main Routing table of VPC.



VPC > Route tables > rtb-03142ecd1006c917f

Updated routes for rtb-03142ecd1006c917f / TEST-VPC-1-RT successfully

rtb-03142ecd1006c917f / TEST-VPC-1-RT

Details Info

| Route table ID | Main | Explicit subnet associations | Edge associations |
|---|---|---|---|
| rtb-03142ecd1006c917f | Yes | – | – |
| VPC<br>vpc-00811833eba324f0d \| TEST-VPC-1 | Owner ID<br>920814761460 | | |

Routes (4)

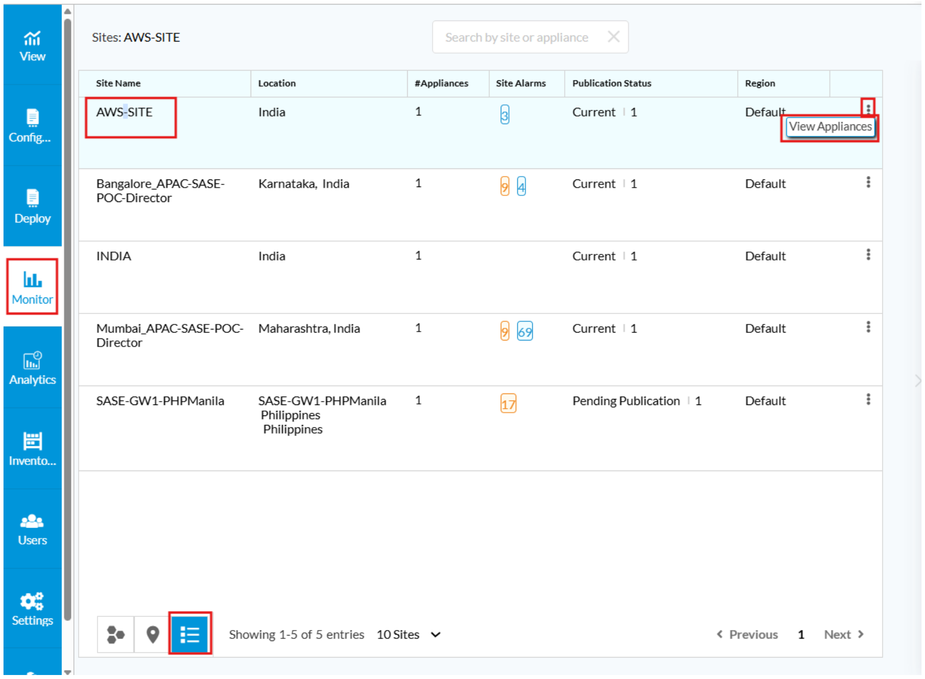
| Destination | Target | Status | Propagated |
|---|---|---|---|
| 0.0.0.0/0 | igw-06d4df7e075fef16b | Active | No |
| 172.16.10.0/24 | eni-094677f262b2141b3 | Active | No |
| 172.16.11.0/24 | eni-094677f262b2141b3 | Active | No |
| 192.168.0.0/16 | local | Active | No |

## Verifying Routes

### Verifying Routing on VOS AWS-Branch:

Dynamic tunnels between VOS AWS-Branch and SASE Gateway should be up.

To view the tunnel status, click on “Monitor”, go to respective Site and click on “View Appliance”.



Sites: AWS-SITE

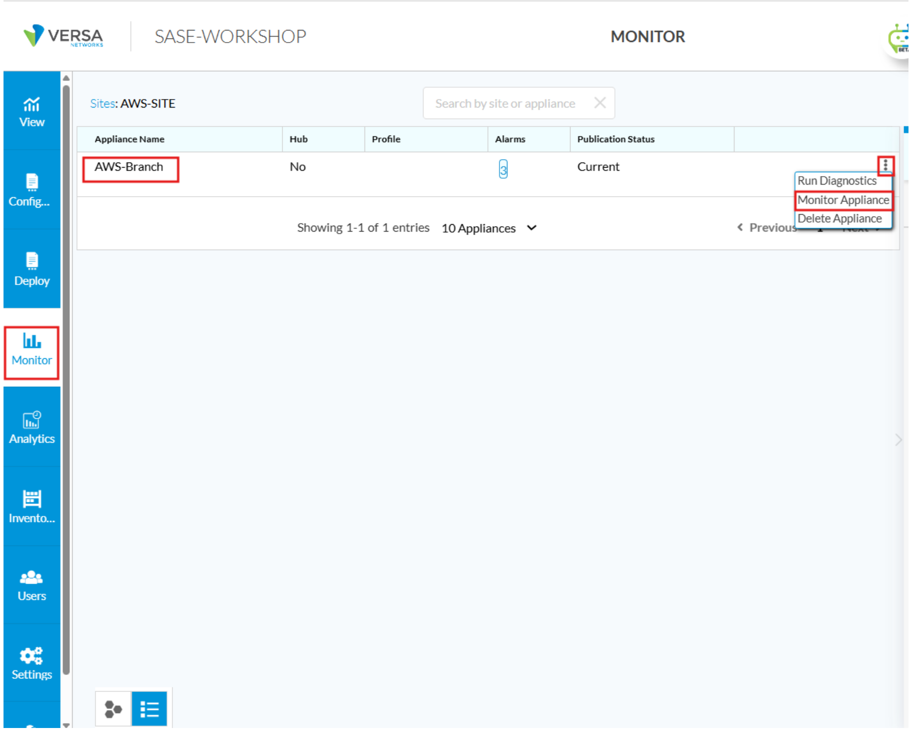
Search by site or appliance

| Site Name | Location | #Appliances | Site Alarms | Publication Status | Region |
|---|---|---|---|---|---|
| AWS-SITE | India | 1 | 3 | Current \| 1 | Default |
| Bangalore_APAC-SASE-POC-Director | Karnataka, India | 1 | 9 4 | Current \| 1 | Default |
| INDIA | India | 1 |  | Current \| 1 | Default |
| Mumbai_APAC-SASE-POC-Director | Maharashtra, India | 1 | 9 69 | Current \| 1 | Default |
| SASE-GW1-PHPManila | SASE-GW1-PHPManila Philippines Philippines | 1 | 17 | Pending Publication \| 1 | Default |

Showing 1-5 of 5 entries 10 Sites

‹ Previous 1 Next ›

Under Monitor, click on “Monitor Appliance”.



Sites: AWS-SITE

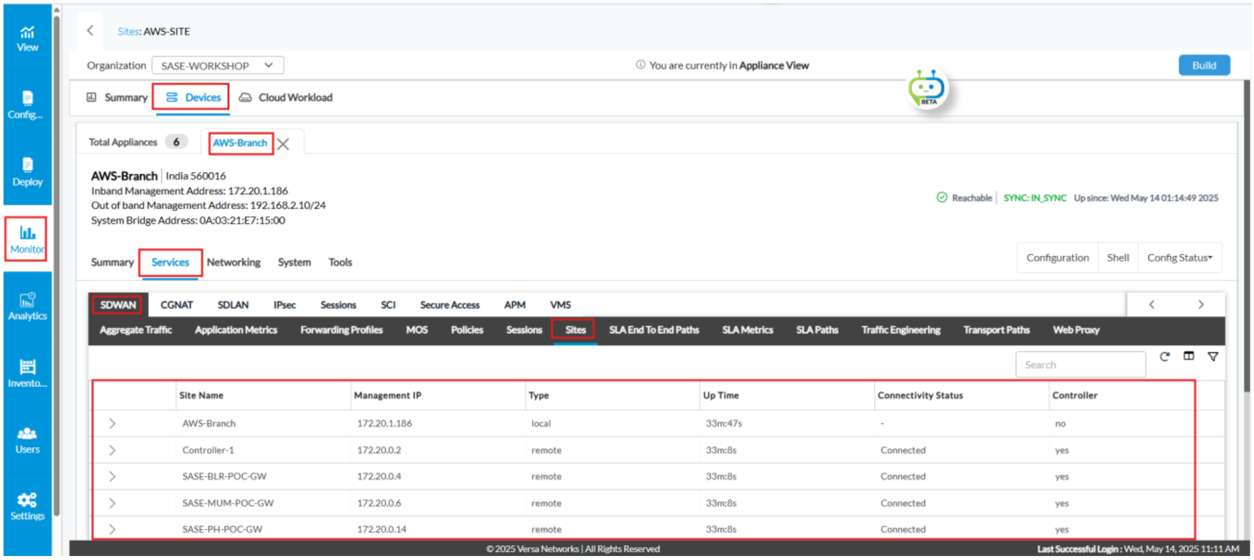
Search by site or appliance

| Appliance Name | Hub | Profile | Alarms | Publication Status |
|---|---|---|---|---|
| AWS-Branch | No |  | 3 | Current |

Showing 1-1 of 1 entries 10 Appliances

‹ Previous

Under Monitor → Devices → <Branch Name> → Services → SDWAN → Sites. Make sure all the devices are connected.



Sites: AWS-SITE

Organization: SASE-WORKSHOP

You are currently in **Appliance View**

Total Appliances 6 | AWS-Branch

**AWS-Branch** | India 560016
Inband Management Address: 172.20.1.186
Out of band Management Address: 192.168.2.10/24
System Bridge Address: 0A:03:21:E7:15:00

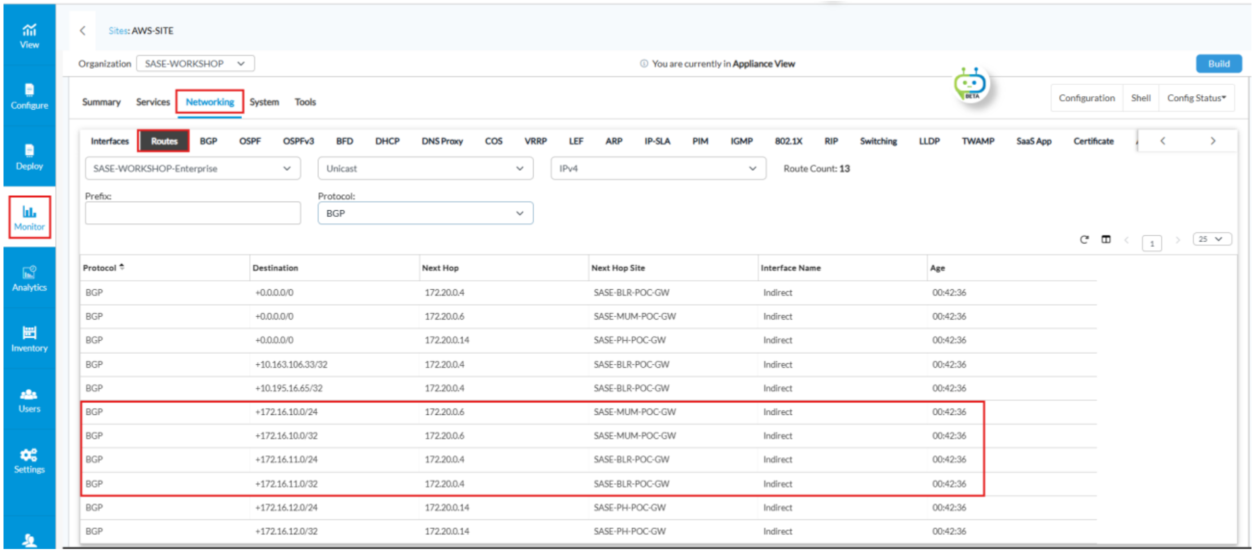
Reachable | SYNC: IN_SYNC Up since: Wed May 14 01:14:49 2025

Summary | Services | Networking | System | Tools

| Site Name | Management IP | Type | Up Time | Connectivity Status | Controller |
|---|---|---|---|---|---|
| AWS-Branch | 172.20.1.186 | local | 33m:47s | - | no |
| Controller-1 | 172.20.0.2 | remote | 33m:8s | Connected | yes |
| SASE-BLR-POC-GW | 172.20.0.4 | remote | 33m:8s | Connected | yes |
| SASE-MUM-POC-GW | 172.20.0.6 | remote | 33m:8s | Connected | yes |
| SASE-PH-POC-GW | 172.20.0.14 | remote | 33m:8s | Connected | yes |

© 2025 Versa Networks | All Rights Reserved   **Last Successful Login :** Wed, May 14, 2025 11:11 AM

To view the SASE Client routes received, Go to Networking → Routes



Sites: AWS-SITE

Organization: SASE-WORKSHOP

You are currently in **Appliance View**

SASE-WORKSHOP-Enterprise | Unicast | IPv4 | Route Count: **13**

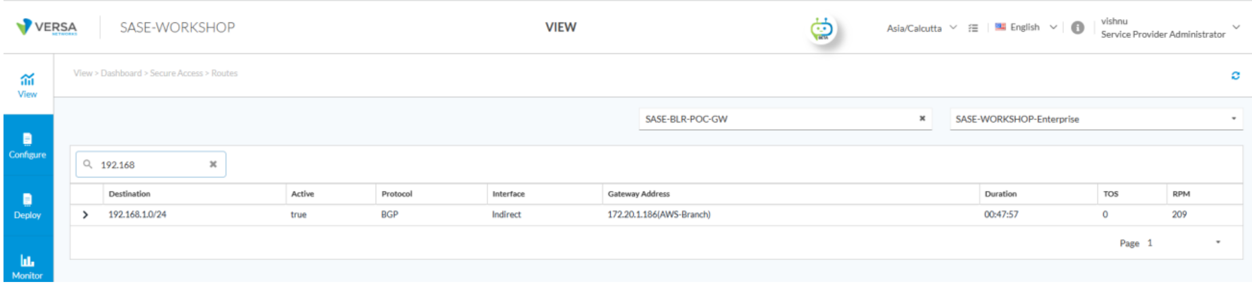
Prefix:

Protocol: BGP

| Protocol | Destination | Next Hop | Next Hop Site | Interface Name | Age |
|---|---|---|---|---|---|
| BGP | +0.0.0.0/0 | 172.20.0.4 | SASE-BLR-POC-GW | Indirect | 00:42:36 |
| BGP | +0.0.0.0/0 | 172.20.0.6 | SASE-MUM-POC-GW | Indirect | 00:42:36 |
| BGP | +0.0.0.0/0 | 172.20.0.14 | SASE-PH-POC-GW | Indirect | 00:42:36 |
| BGP | +10.163.106.33/32 | 172.20.0.4 | SASE-BLR-POC-GW | Indirect | 00:42:36 |
| BGP | +10.195.16.65/32 | 172.20.0.4 | SASE-BLR-POC-GW | Indirect | 00:42:36 |
| BGP | +172.16.10.0/24 | 172.20.0.6 | SASE-MUM-POC-GW | Indirect | 00:42:36 |
| BGP | +172.16.10.0/32 | 172.20.0.6 | SASE-MUM-POC-GW | Indirect | 00:42:36 |
| BGP | +172.16.11.0/24 | 172.20.0.4 | SASE-BLR-POC-GW | Indirect | 00:42:36 |
| BGP | +172.16.11.0/32 | 172.20.0.4 | SASE-BLR-POC-GW | Indirect | 00:42:36 |
| BGP | +172.16.12.0/24 | 172.20.0.14 | SASE-PH-POC-GW | Indirect | 00:42:36 |
| BGP | +172.16.12.0/32 | 172.20.0.14 | SASE-PH-POC-GW | Indirect | 00:42:36 |

## Verifying Routing on SASE Gateway:

Routing Table on SASE-GW can be viewed from “View” → Dashboard → Secure Access → Routes.



View > Dashboard > Secure Access > Routes

SASE-BLR-POC-GW | SASE-WORKSHOP-Enterprise

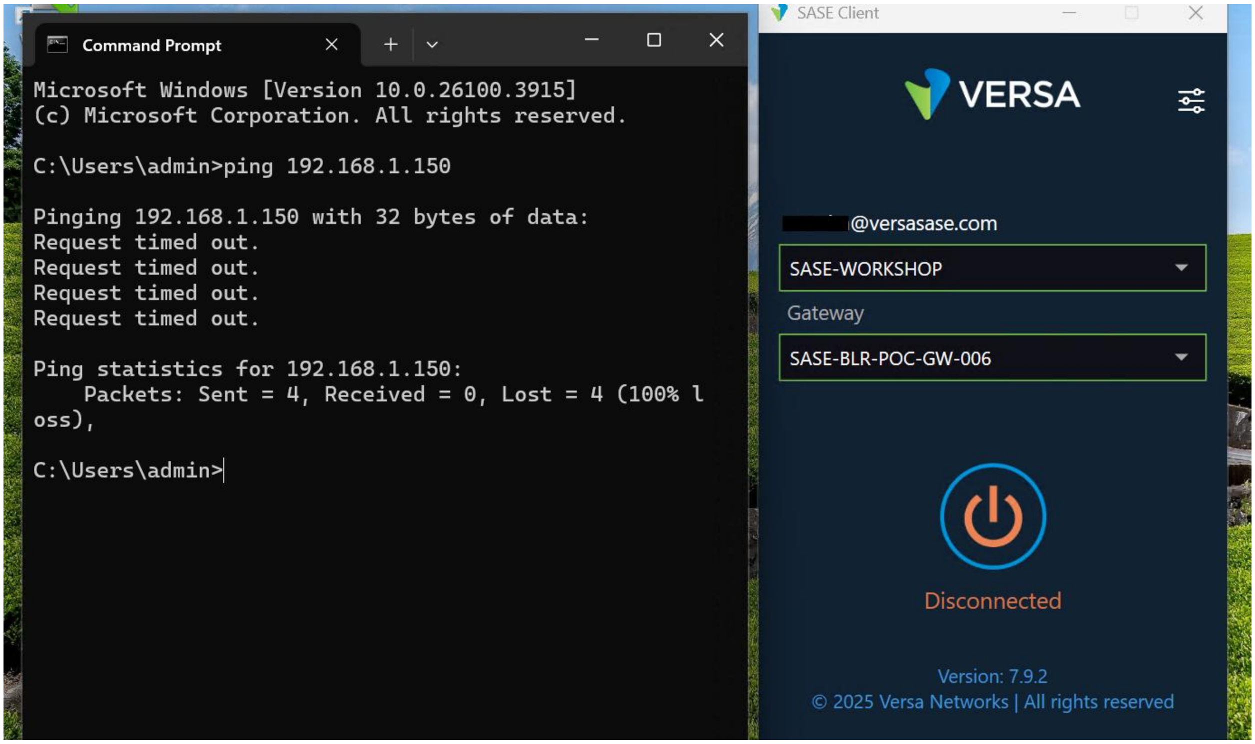
192.168

| Destination | Active | Protocol | Interface | Gateway Address | Duration | TOS | RPM |
|---|---|---|---|---|---|---|---|
| 192.168.1.0/24 | true | BGP | Indirect | 172.20.1.186(AWS-Branch) | 00:47:57 | 0 | 209 |

## Verifying Connectivity:

Accessing EC2 instance with IP: 192.168.1.150 from PC connected to SASE Client.

When the SASE Client is not connected to Gateway, we were unable to reach the EC2 instance in AWS over Private IP.



```
Microsoft Windows [Version 10.0.26100.3915]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>ping 192.168.1.150

Pinging 192.168.1.150 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.150:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% l
oss),

C:\Users\admin>
```

[redacted]@versasase.com

SASE-WORKSHOP

Gateway

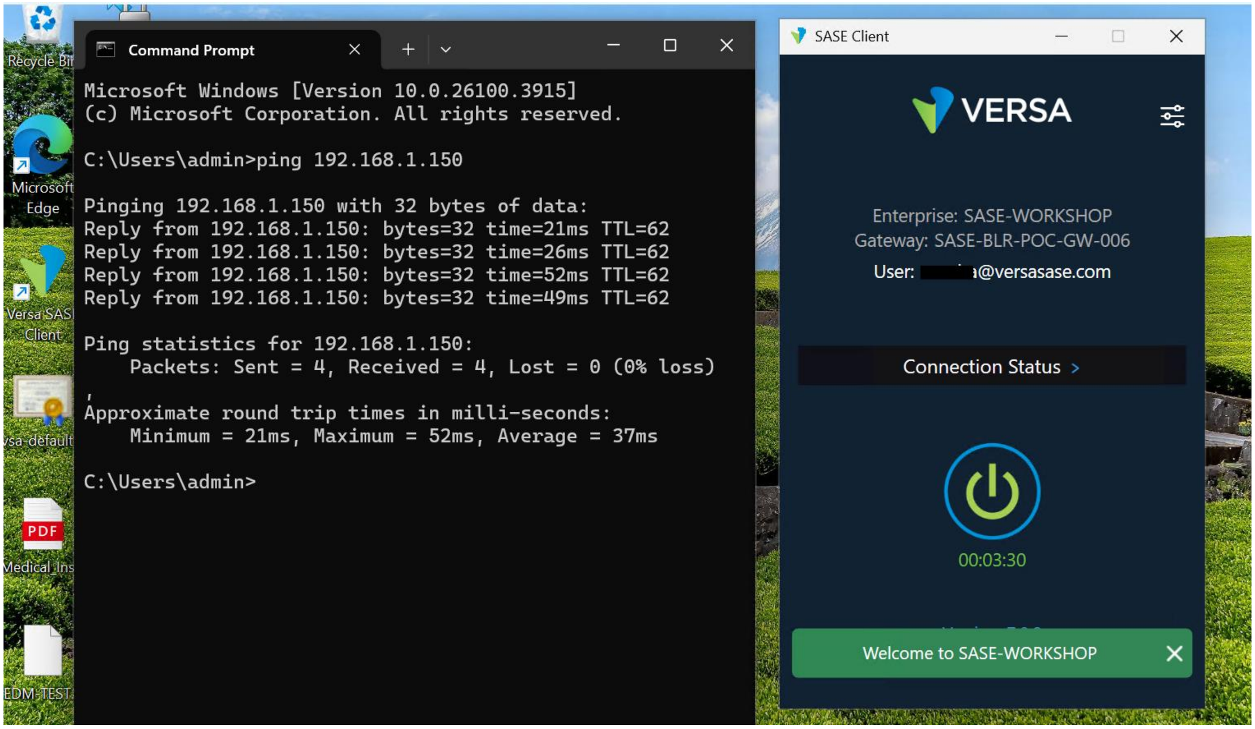
SASE-BLR-POC-GW-006

Disconnected

Version: 7.9.2

© 2025 Versa Networks | All rights reserved

When the SASE Client is connected to the Gateway, we were able to reach the EC2 instance in AWS over Private IP.



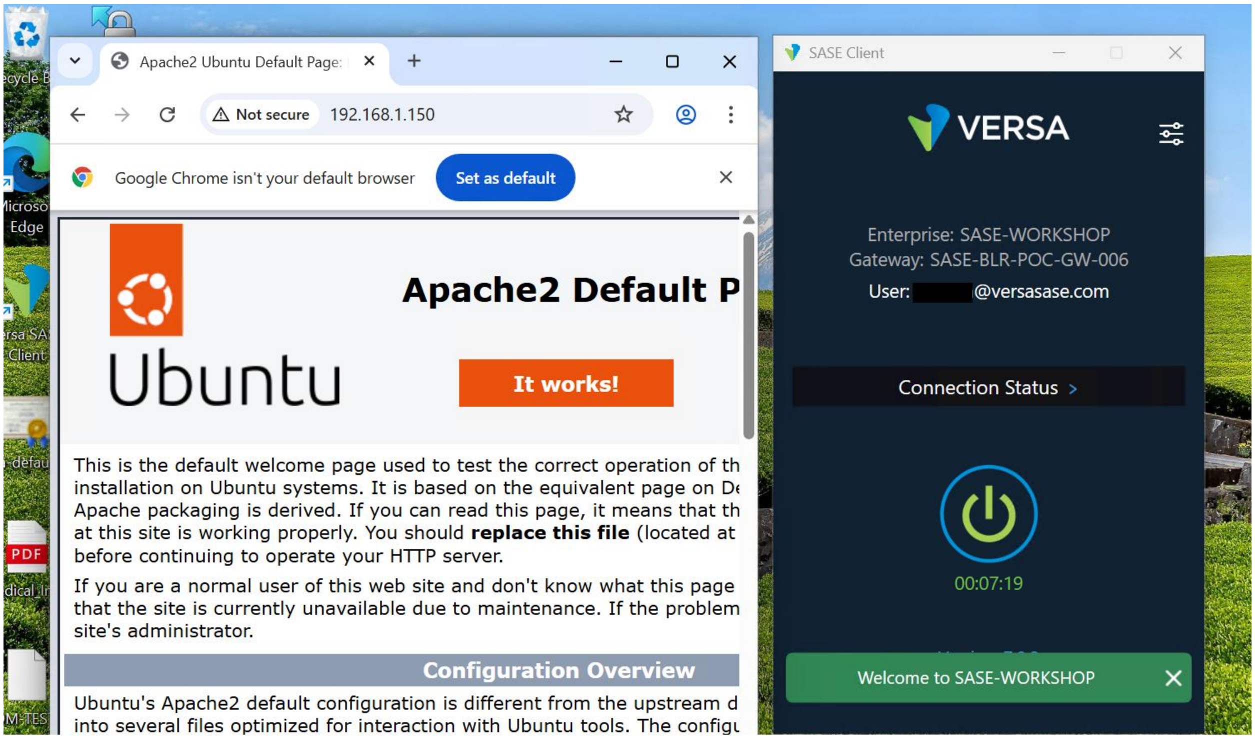
```
Microsoft Windows [Version 10.0.26100.3915]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>ping 192.168.1.150

Pinging 192.168.1.150 with 32 bytes of data:
Reply from 192.168.1.150: bytes=32 time=21ms TTL=62
Reply from 192.168.1.150: bytes=32 time=26ms TTL=62
Reply from 192.168.1.150: bytes=32 time=52ms TTL=62
Reply from 192.168.1.150: bytes=32 time=49ms TTL=62

Ping statistics for 192.168.1.150:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
,
Approximate round trip times in milli-seconds:
    Minimum = 21ms, Maximum = 52ms, Average = 37ms

C:\Users\admin>
```

Enterprise: SASE-WORKSHOP
Gateway: SASE-BLR-POC-GW-006
User: [redacted]@versasase.com

00:03:30

Welcome to SASE-WORKSHOP

If the EC2 instance is a webserver then you should be able to access the webpage over Private IP.



Apache2 Default P

It works!

This is the default welcome page used to test the correct operation of th installation on Ubuntu systems. It is based on the equivalent page on De Apache packaging is derived. If you can read this page, it means that th at this site is working properly. You should **replace this file** (located at before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page that the site is currently unavailable due to maintenance. If the problem site's administrator.

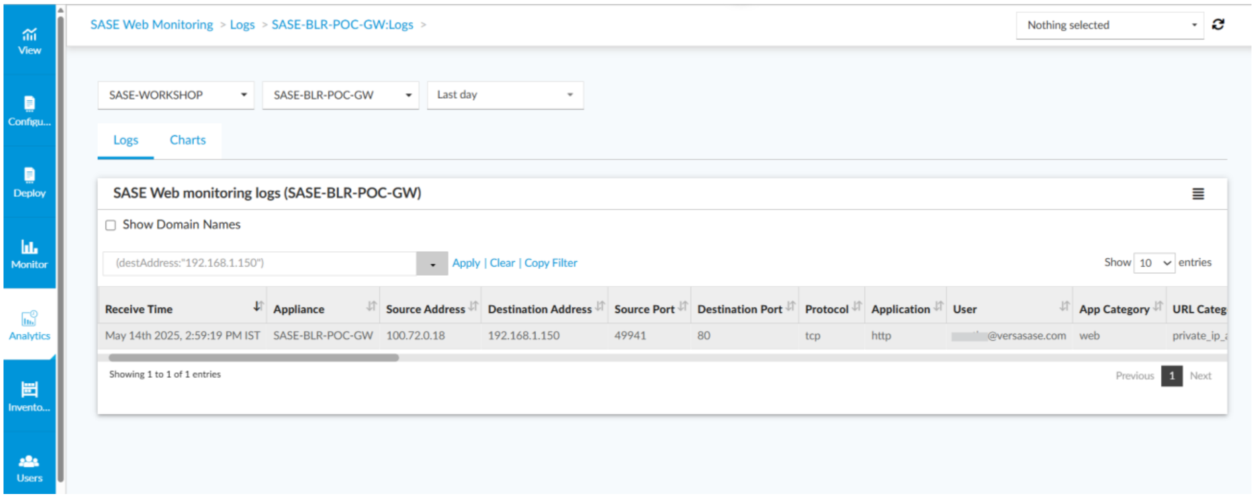
Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream d into several files optimized for interaction with Ubuntu tools. The configu

Enterprise: SASE-WORKSHOP
Gateway: SASE-BLR-POC-GW-006
User: [redacted]@versasase.com

Welcome to SASE-WORKSHOP

## SASE-WEB LOGS on Analytics:



SASE Web monitoring logs (SASE-BLR-POC-GW)

□ Show Domain Names

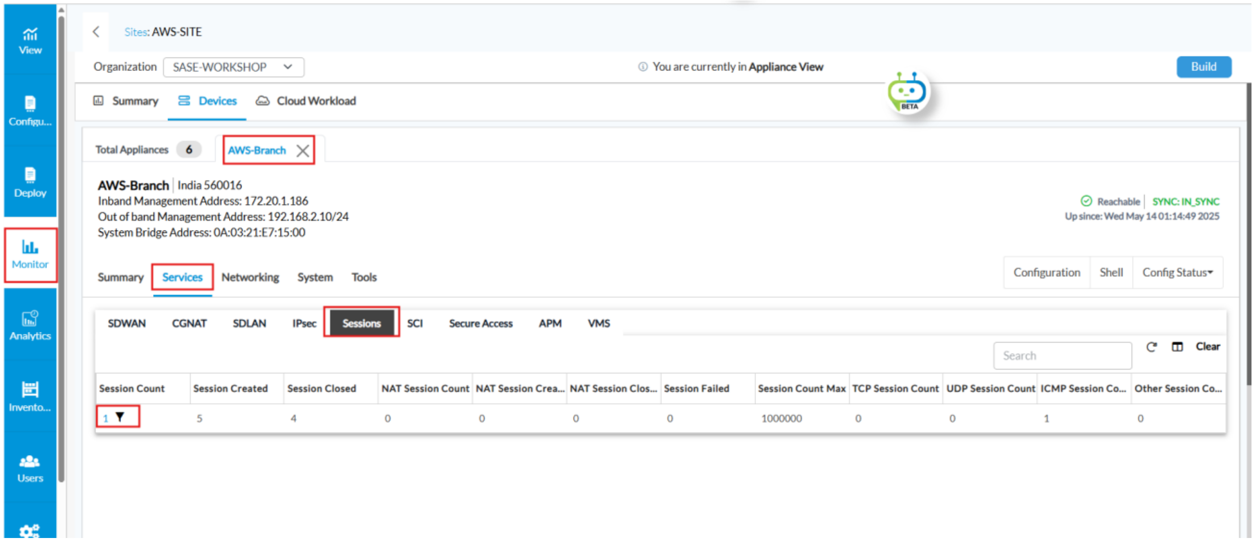
(destAddress:"192.168.1.150")

Show 10 entries

| Receive Time | Appliance | Source Address | Destination Address | Source Port | Destination Port | Protocol | Application | User | App Category | URL Categ |
|---|---|---|---|---|---|---|---|---|---|---|
| May 14th 2025, 2:59:19 PM IST | SASE-BLR-POC-GW | 100.72.0.18 | 192.168.1.150 | 49941 | 80 | tcp | http | [redacted]@versasase.com | web | private_ip_a |

Showing 1 to 1 of 1 entries

You should be able to View the session information Under Monitor → Devices → <Branch Name> → Services → Sessions.



You are currently in **Appliance View**

**AWS-Branch** | India 560016
Inband Management Address: 172.20.1.186
Out of band Management Address: 192.168.2.10/24
System Bridge Address: 0A:03:21:E7:15:00

Reachable | SYNC: IN_SYNC
Up since: Wed May 14 01:14:49 2025

| Session Count | Session Created | Session Closed | NAT Session Count | NAT Session Crea... | NAT Session Clos... | Session Failed | Session Count Max | TCP Session Count | UDP Session Count | ICMP Session Co... | Other Session Co... |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 ▼ | 5 | 4 | 0 | 0 | 0 | 0 | 1000000 | 0 | 0 | 1 | 0 |

## About Versa

Versa, the global leader in SASE, enables organizations to create self-protecting networks that radically simplify and automate their network and security infrastructure. Powered by AI, the VersaONE Universal SASE Platform delivers converged SSE, SD-WAN, and SD-LAN solutions that protect data and defend against cyberthreats while delivering a superior digital experience. Thousands of customers globally, with hundreds of thousands of sites and millions of users, trust Versa with their mission critical networks and security. Versa is privately held and funded by investors such as Sequoia Capital, Mayfield, and BlackRock. For more information, visit https://www.versa-networks.com and follow Versa on LinkedIn and X (Twitter) @versanetworks.