VERSA

IMPLEMENTATION GUIDE

Versa SASE Gateways Integration with Azure Cloud

About This Document

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

Document Information

Title	**Versa SASE Gateways Integration with Azure Cloud**
Author	Versa Professional Services
Version	V 1.0

Disclaimer

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

1. 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

Integration Approaches for SASE Gateways with Azure

Importance of Azure Integration

Cloud workloads are rapidly increasing, making SASE gateway integration with Azure essential, as it ensures secure and direct access to cloud-hosted resources from remote users, branch offices, and mobile endpoints, enables enforcement of consistent security policies across both on-premises and cloud environments, and helps maintain uniform security policies that are critical for regulatory compliance and a strong security posture.

Type of Integration:

- Option 1: Azure VPN Integration with Versa SASE Gateway (Site-to-Site VPN Method)
- Option 2: Integration via Azure Virtual WAN
- Option 3: Integration using Virtualized Network Appliance (VOS) from Azure Marketplace

Key Components for SASE Gateway Integrations

- Resource Groups.
- Virtual Networks (VNET)
- Subnet

- Azure Virtual Machine
- Local Network Gateway
- Virtual Network Gateway
- Virtual WAN and its components
- Network Security Group

Creating Resource Groups:

Azure resource groups are logical containers that hold related resources for an Azure solution. They help you manage, monitor, and provision these resources as a single unit, simplifying organization and administration.

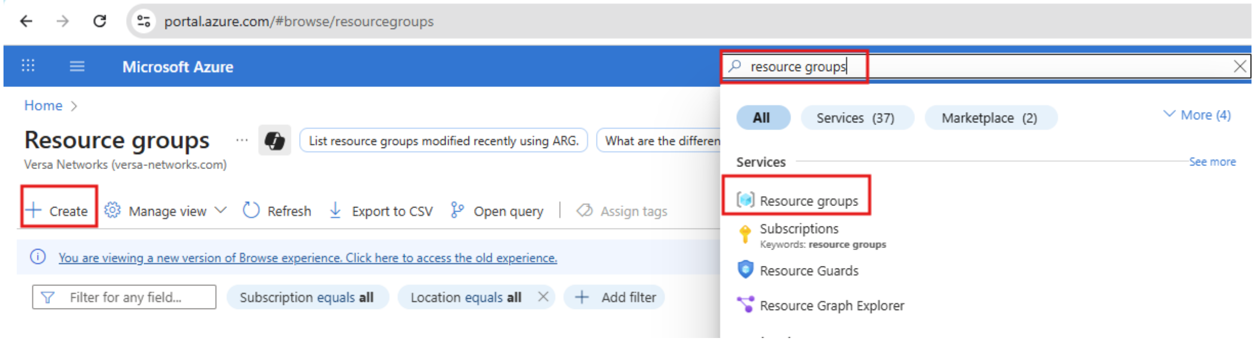
Purpose:

- Organizes network/security resources (like VNets, VPN Gateways, Firewalls, etc.) under a single group.
- Simplifies deployment and deletion — all resources in a group can be managed together.
- Enables policy enforcement and monitoring at the group level.
- Facilitates cost visibility by grouping related resources for billing.

Common Use Cases

- Networking Projects: Group VNets, VPN Gateways, Route Tables, and Firewalls into one container.
- Application Stacks: Keep app servers, DBs, storage, and network resources in one group.
- Environment Separation: Create separate groups for Dev, Test, and Prod workloads.
- Access Control: Assign specific roles to teams (e.g., Networking team only manages network resource groups).

To Create a Resource Group, Type Resource Groups in the search bar and select "Resource Groups" and click on Create.

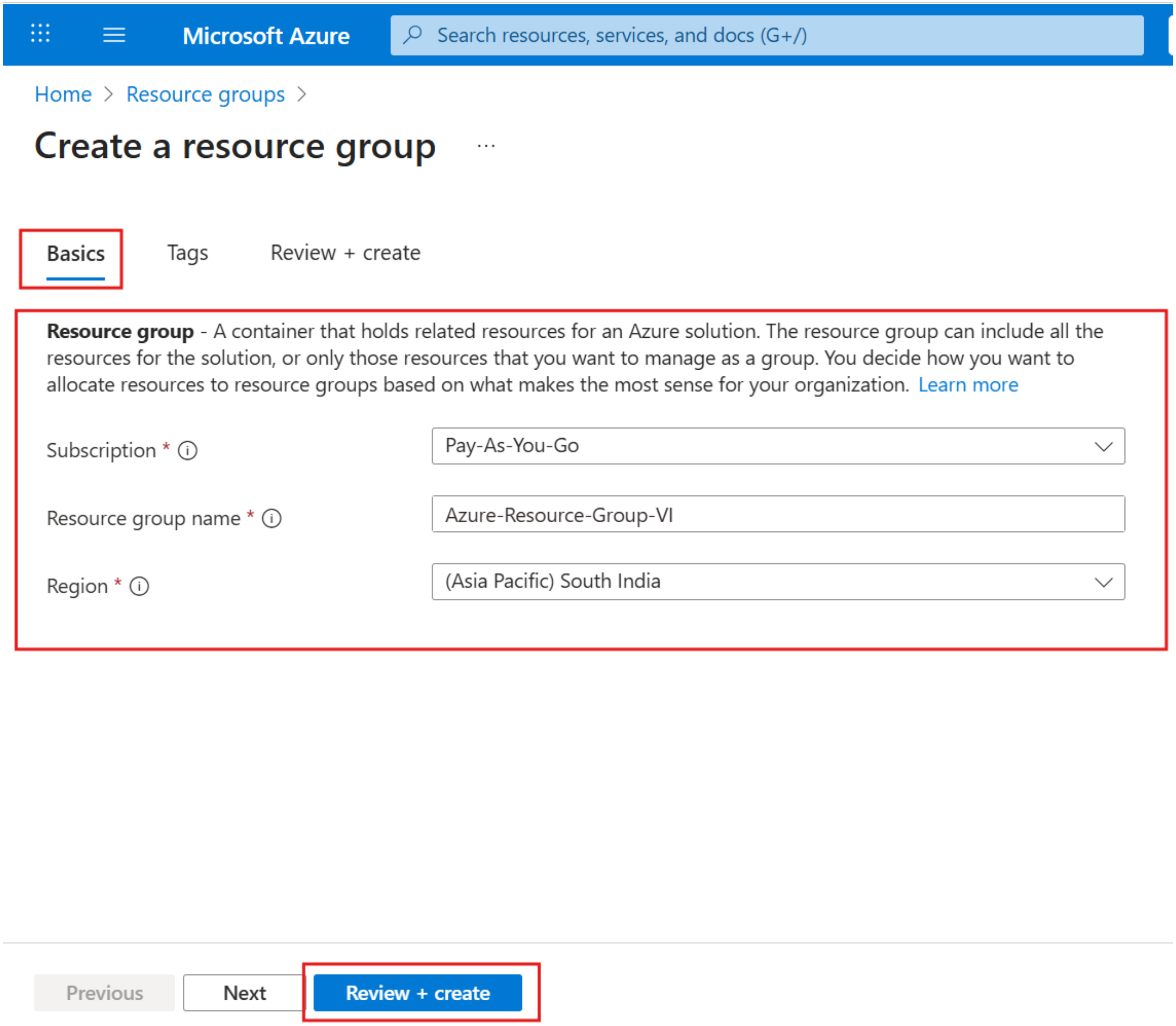


portal.azure.com/#browse/resourcegroups

resource groups

You are viewing a new version of Browse experience. Click here to access the old experience.

Under Basic tab, provide the subscription info, name of the resource group, Region and click on “Review+create”.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Resource groups >
Create a resource group ...
Basics
Tags
Review + create

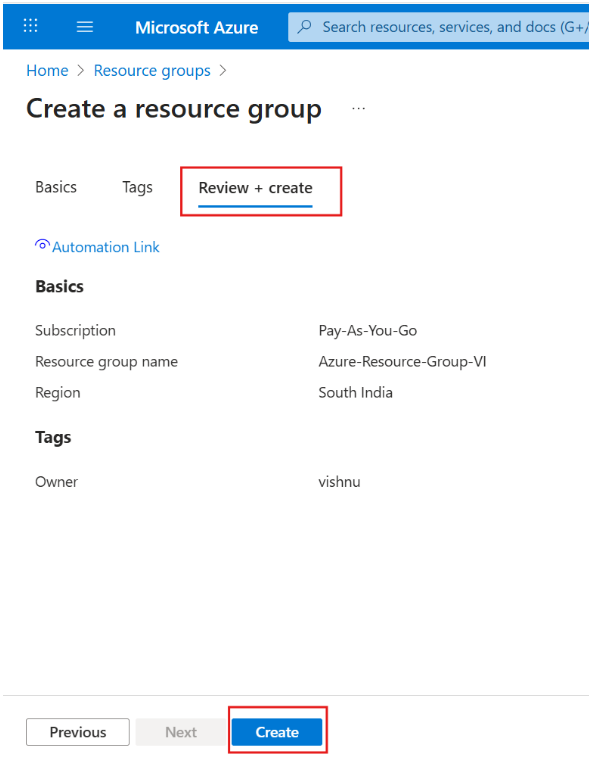
Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. Learn more

Subscription * : Pay-As-You-Go

Resource group name * : Azure-Resource-Group-VI

Region * : (Asia Pacific) South India

Under Review+create, validate the information and click on create.



Create a resource group

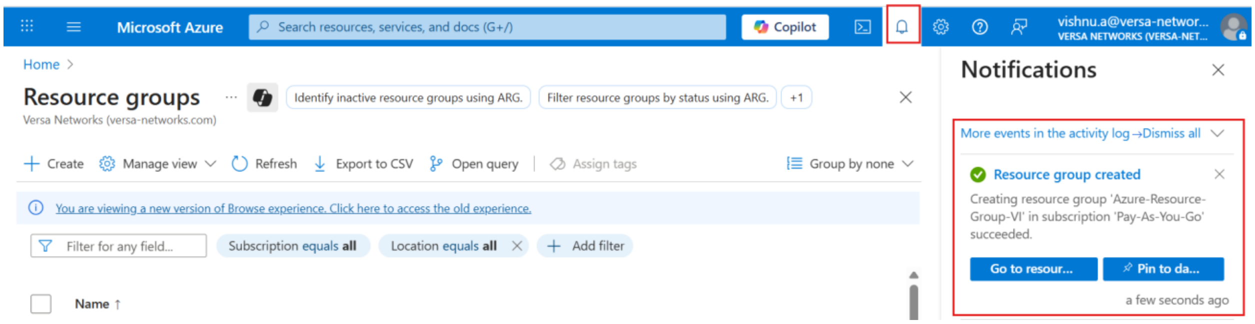
Basics

Subscription	Pay-As-You-Go
Resource group name	Azure-Resource-Group-VI
Region	South India

Tags

Owner	vishnu

You can check the status Resource group creation under Notifications.



Resource groups

You are viewing a new version of Browse experience. Click here to access the old experience.

Notifications

Resource group created

Creating resource group 'Azure-Resource-Group-VI' in subscription 'Pay-As-You-Go' succeeded.

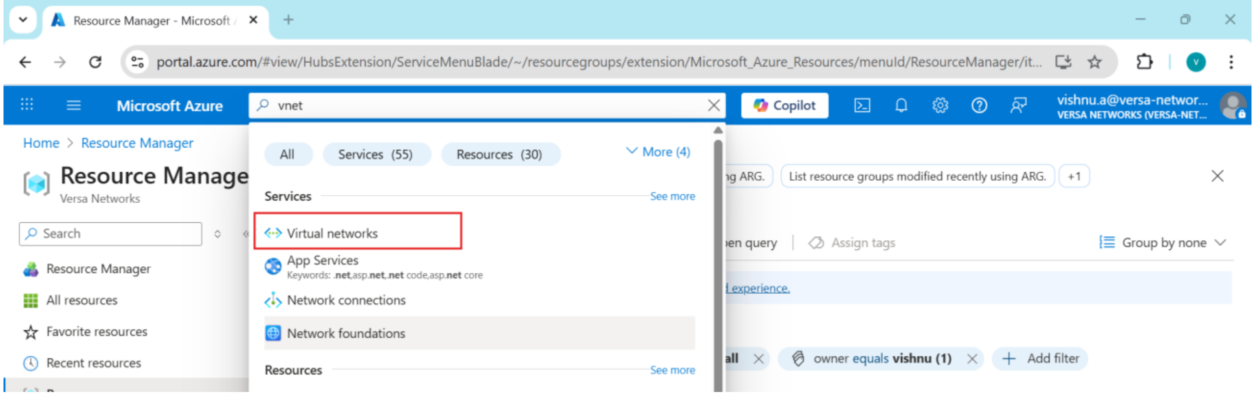
VNET:

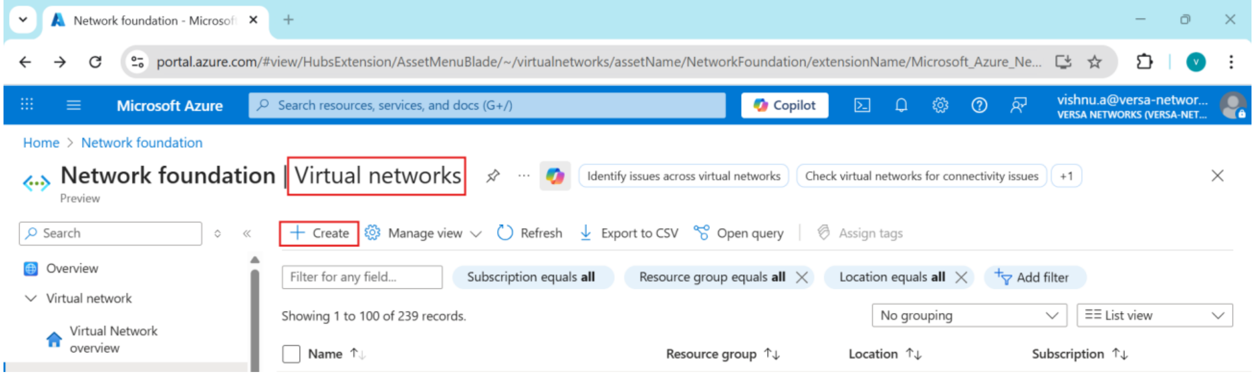
Azure Virtual Networks provide logical isolation of cloud resources, similar to a traditional on-premises network, and enable secure communication between Azure resources, on-premises environments, and the internet.

Use Cases:

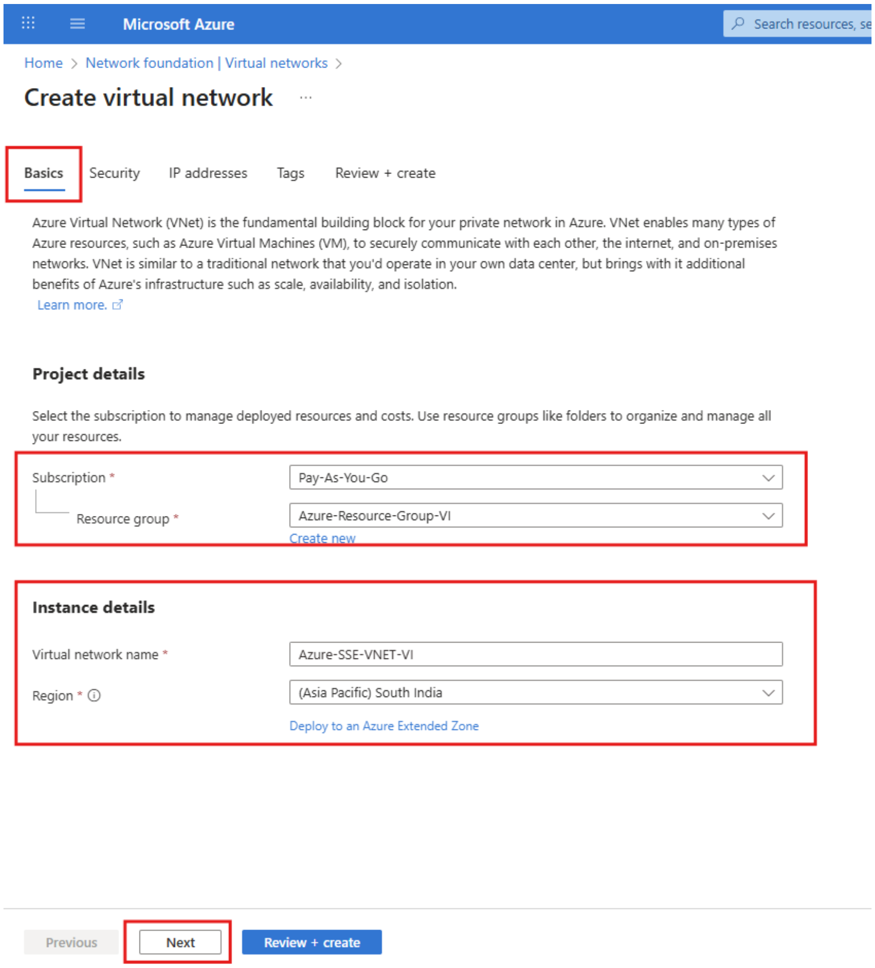
- Segmentation of workloads
- Hybrid connectivity with on-prem

To create a Virtual Network, In Azure portal, search for 'Virtual networks' and click "+Create".




Network foundation - Microsoft
portal.azure.com/#view/HubsExtension/AssetMenuBlade/~/virtualnetworks/assetName/NetworkFoundation/extensionName/Microsoft_Azure_Ne...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
vishnu.a@versa-networ...
VERSA NETWORKS (VERSA-NET...
Home > Network foundation
Network foundation | Virtual networks
Preview
Identify issues across virtual networks
Check virtual networks for connectivity issues
+1
Search
Overview
Virtual network
Virtual Network overview
Create
Manage view
Refresh
Export to CSV
Open query
Assign tags
Filter for any field...
Subscription equals all
Resource group equals all
Location equals all
Add filter
Showing 1 to 100 of 239 records.
No grouping
List view
Name
Resource group
Location
Subscription

Under “Basics” tab, specify subscription, resource group, Virtual Network name, region and then click on “Next”.



Create virtual network ...

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Pay-As-You-Go

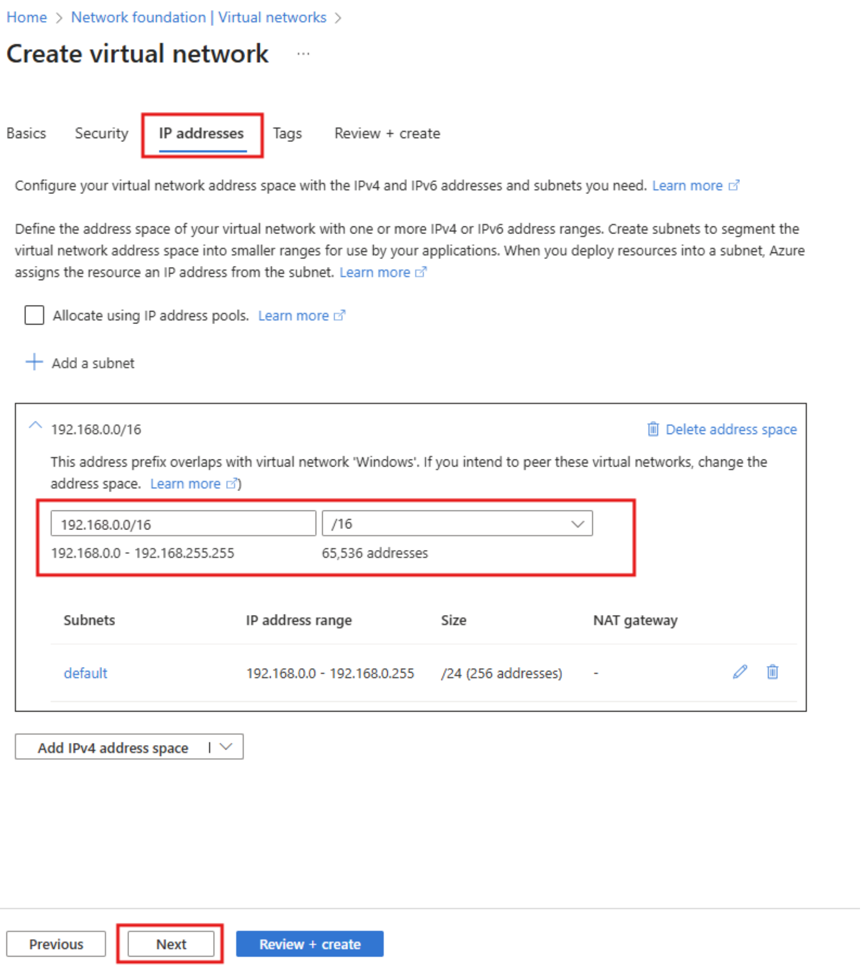
Resource group * Azure-Resource-Group-VI

Instance details

Virtual network name * Azure-SSE-VNET-VI

Region * (Asia Pacific) South India

Under “IP addresses” Define the address space of your virtual network and click on Next.



Home > Network foundation | Virtual networks >

Create virtual network ···

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. Learn more

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. Learn more

□ Allocate using IP address pools. Learn more

192.168.0.0/16

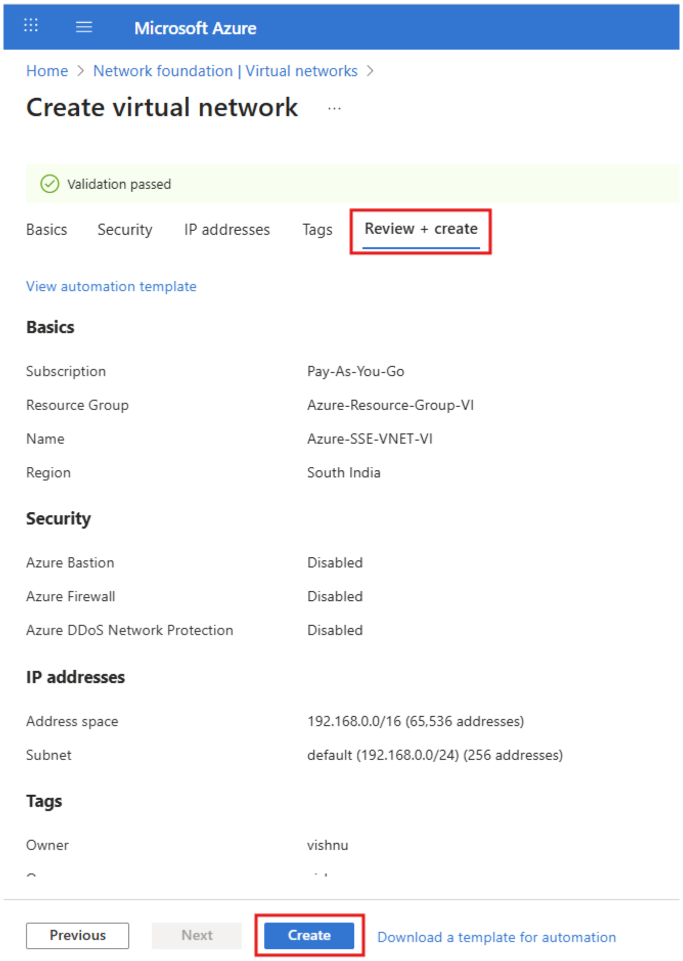
This address prefix overlaps with virtual network 'Windows'. If you intend to peer these virtual networks, change the address space. Learn more)

192.168.0.0/16 | /16

192.168.0.0 - 192.168.255.255 | 65,536 addresses

Subnets	IP address range	Size	NAT gateway
default	192.168.0.0 - 192.168.0.255	/24 (256 addresses)	-

Under “Review+create” make sure the information is correct and click on “Create”.



Create virtual network

Validation passed

Basics

Subscription	Pay-As-You-Go
Resource Group	Azure-Resource-Group-VI
Name	Azure-SSE-VNET-VI
Region	South India

Security

Azure Bastion	Disabled
Azure Firewall	Disabled
Azure DDoS Network Protection	Disabled

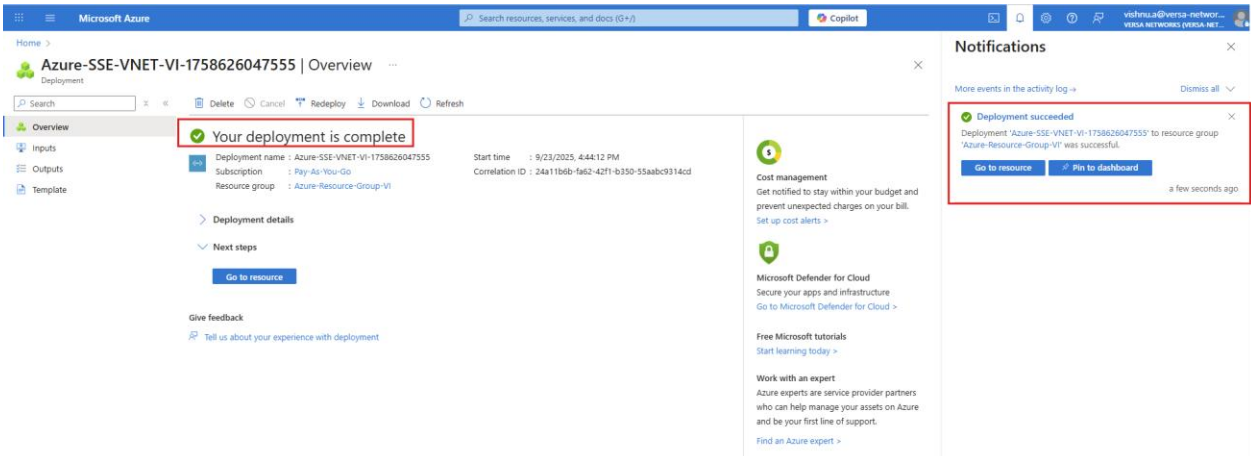
IP addresses

Address space	192.168.0.0/16 (65,536 addresses)
Subnet	default (192.168.0.0/24) (256 addresses)

Tags

Owner	vishnu

Make sure the department is complete.



Azure-SSE-VNET-VI-1758626047555 | Overview

Deployment

Your deployment is complete

Deployment name	Azure-SSE-VNET-VI-1758626047555
Subscription	Pay-As-You-Go
Resource group	Azure-Resource-Group-VI
Start time	9/23/2025, 4:44:12 PM
Correlation ID	24a11b6b-fa62-42f1-b350-55aabc9314cd

Give feedback

Tell us about your experience with deployment

Cost management

Get notified to stay within your budget and prevent unexpected charges on your bill.

Microsoft Defender for Cloud

Secure your apps and infrastructure

Free Microsoft tutorials

Work with an expert

Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.

Notifications

Deployment succeeded

Deployment 'Azure-SSE-VNET-VI-1758626047555' to resource group 'Azure-Resource-Group-VI' was successful.

a few seconds ago

SUBNET:

A subnet is a range of IP addresses within a Virtual Network (VNet) in Azure that segments the VNet into smaller, manageable sections to organize and secure resources.

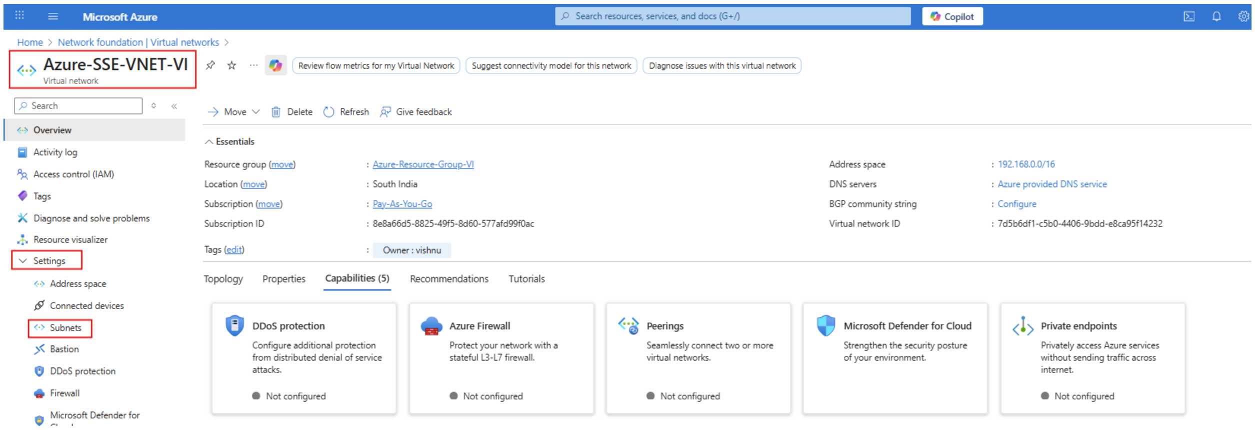
Types of Subnets:

Default Subnet: Created automatically when a VNet is created (optional).

Gateway Subnet: Dedicated subnet for VPN Gateway or ExpressRoute Gateway.

Creating subnets:

To Create subnets, go to respective Azure Vnet and under settings click on Subnets.



Essentials

Resource group (move)	: Azure-Resource-Group-VI	Address space	: 192.168.0.0/16
Location (move)	: South India	DNS servers	: Azure provided DNS service
Subscription (move)	: Pay-As-You-Go	BGP community string	: Configure
Subscription ID	: 8e8a66d5-8825-49f5-8d60-577afd99f0ac	Virtual network ID	: 7d5b6df1-c5b0-4406-9bdd-e8ca95f14232
Tags (edit)	: Owner : vishnu		

DDoS protection: Configure additional protection from distributed denial of service attacks. ● Not configured

Azure Firewall: Protect your network with a stateful L3-L7 firewall. ● Not configured

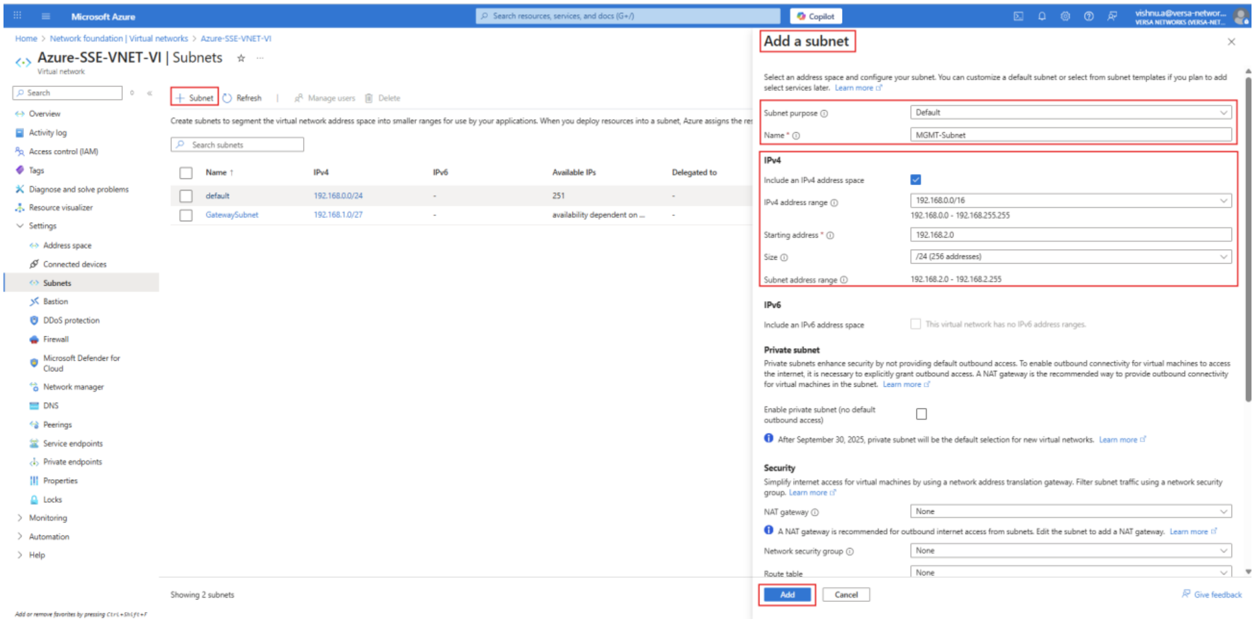
Peerings: Seamlessly connect two or more virtual networks. ● Not configured

Microsoft Defender for Cloud: Strengthen the security posture of your environment.

Private endpoints: Privately access Azure services without sending traffic across internet. ● Not configured

Create 3 different Subnets for LAN WAN and MGMT.

To create a MGMT subnet click on Subnet → under "Add a Subnet" provide the purpose , Name, IPv4 address range, Starting address, size and click on "Add".



Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the re

Name ↑	IPv4	IPv6	Available IPs	Delegated to
default	192.168.0.0/24	-	251	-
GatewaySubnet	192.168.1.0/27	-	availability dependent on ...	-

Add a subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. Learn more

Subnet purpose: Default

Name *: MGMT-Subnet

IPv4

Include an IPv4 address space ☑

IPv4 address range: 192.168.0.0/16
192.168.0.0 - 192.168.255.255

Starting address *: 192.168.2.0

Size: /24 (256 addresses)

Subnet address range: 192.168.2.0 - 192.168.2.255

IPv6

Include an IPv6 address space □ This virtual network has no IPv6 address ranges.

Private subnet

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. Learn more

Enable private subnet (no default outbound access) □

After September 30, 2025, private subnet will be the default selection for new virtual networks. Learn more

Security

Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. Learn more

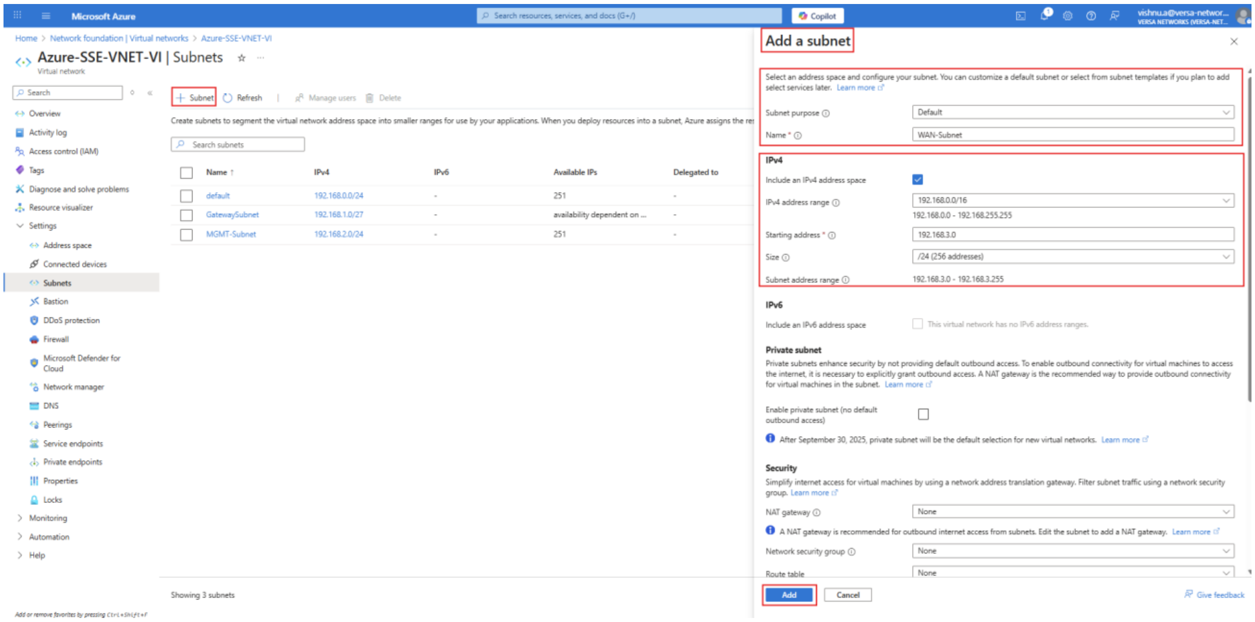
NAT gateway: None

A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway. Learn more

Network security group: None

Route table: None

Similarly create Subnet for WAN and LAN.



Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the re

Name ↑	IPv4	IPv6	Available IPs	Delegated to
default	192.168.0.0/24	-	251	-
GatewaySubnet	192.168.1.0/27	-	availability dependent on ...	-
MGMT-Subnet	192.168.2.0/24	-	251	-

Add a subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. Learn more

Subnet purpose: Default

Name *: WAN-Subnet

IPv4

Include an IPv4 address space: ☑

IPv4 address range: 192.168.0.0/16
192.168.0.0 - 192.168.255.255

Starting address *: 192.168.3.0

Size: /24 (256 addresses)

Subnet address range: 192.168.3.0 - 192.168.3.255

IPv6

Include an IPv6 address space: □ This virtual network has no IPv6 address ranges.

Private subnet

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. Learn more

Enable private subnet (no default outbound access): □

After September 30, 2025, private subnet will be the default selection for new virtual networks. Learn more

Security

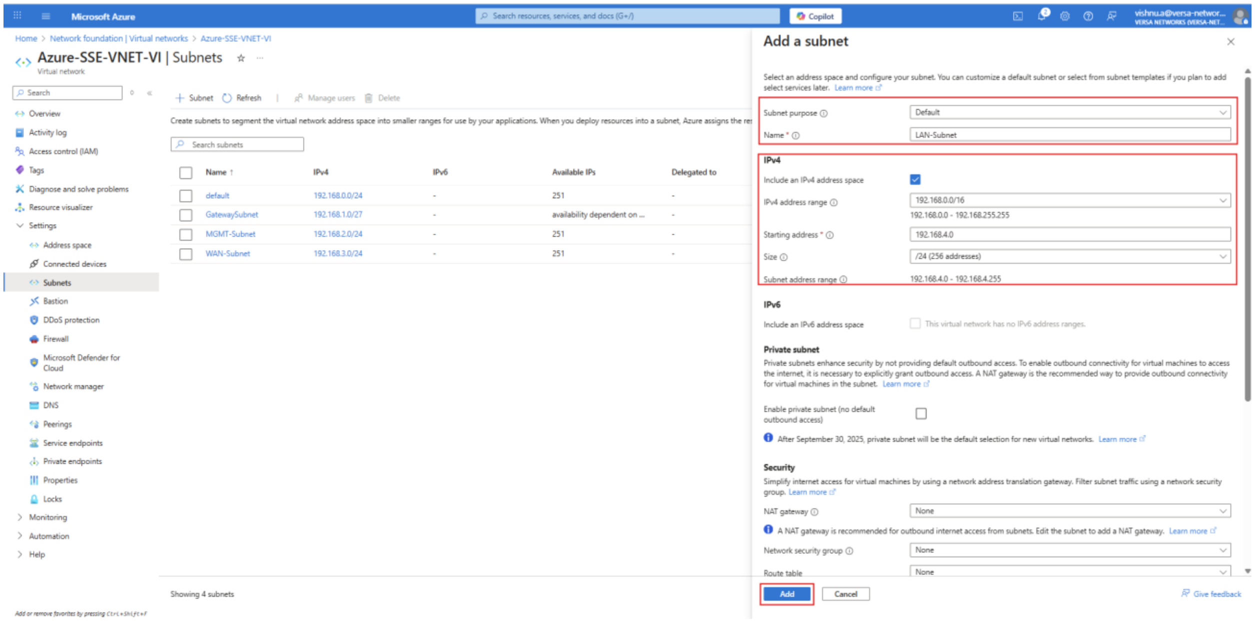
Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. Learn more

NAT gateway: None

A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway. Learn more

Network security group: None

Route table: None



Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the re

Name ↑	IPv4	IPv6	Available IPs	Delegated to
default	192.168.0.0/24	-	251	-
GatewaySubnet	192.168.1.0/27	-	availability dependent on ...	-
MGMT-Subnet	192.168.2.0/24	-	251	-
WAN-Subnet	192.168.3.0/24	-	251	-

Add a subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. Learn more

Subnet purpose: Default

Name *: LAN-Subnet

IPv4

Include an IPv4 address space: ☑

IPv4 address range: 192.168.0.0/16
192.168.0.0 - 192.168.255.255

Starting address *: 192.168.4.0

Size: /24 (256 addresses)

Subnet address range: 192.168.4.0 - 192.168.4.255

IPv6

Include an IPv6 address space: □ This virtual network has no IPv6 address ranges.

Private subnet

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. Learn more

Enable private subnet (no default outbound access): □

After September 30, 2025, private subnet will be the default selection for new virtual networks. Learn more

Security

Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. Learn more

NAT gateway: None

A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway. Learn more

Network security group: None

Route table: None

MGMT	192.168.2.0/24
WAN	192.168.3.0/24
LAN	192.168.4.0/24

Azure Virtual Machine:

Azure virtual machines (VMs) are scalable, on-demand compute resources that let you run Windows or Linux operating systems and custom applications in the Azure cloud.

Purpose in This Use Case:

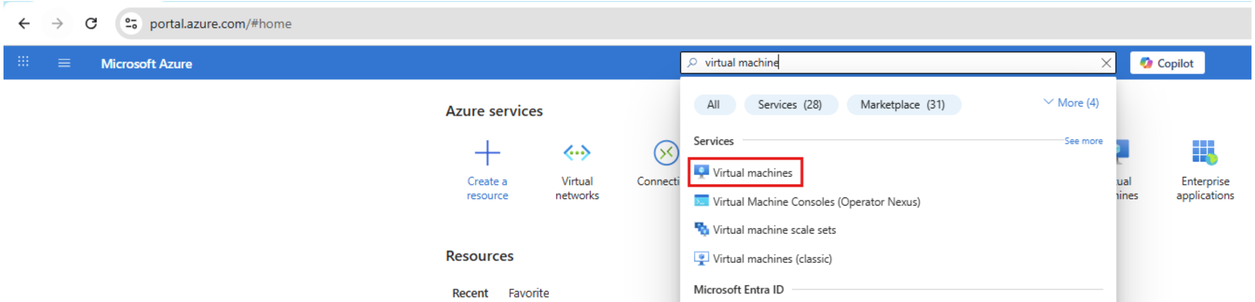
Server Hosting in Azure:
Azure VM’s host applications or services that can be communicated with on-premises environments over secure hybrid connectivity (via VGW/TGW and IPsec).

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

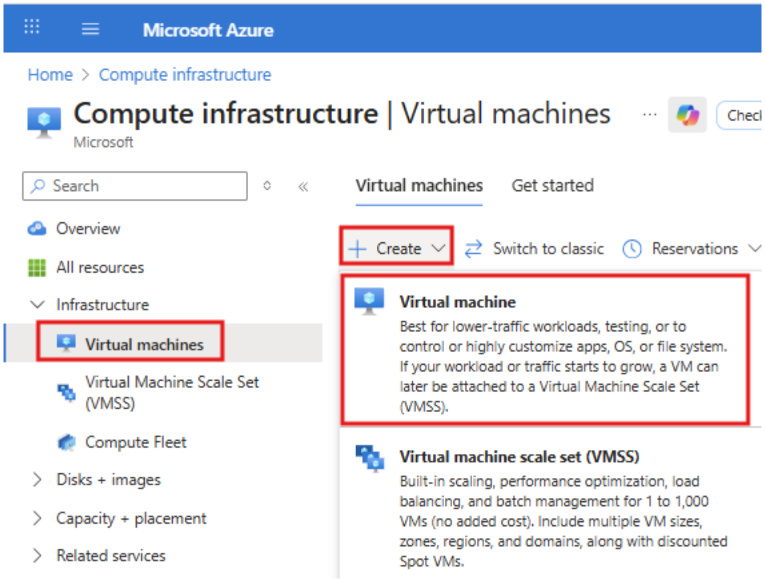
To create Azure VM instance, type Azure Virtual Machine in the search bar and select ---.

Creating Azure Virtual Machine:

To Create Azure VM, Type virtual machines in the search bar and select Virtual Machines under Services.



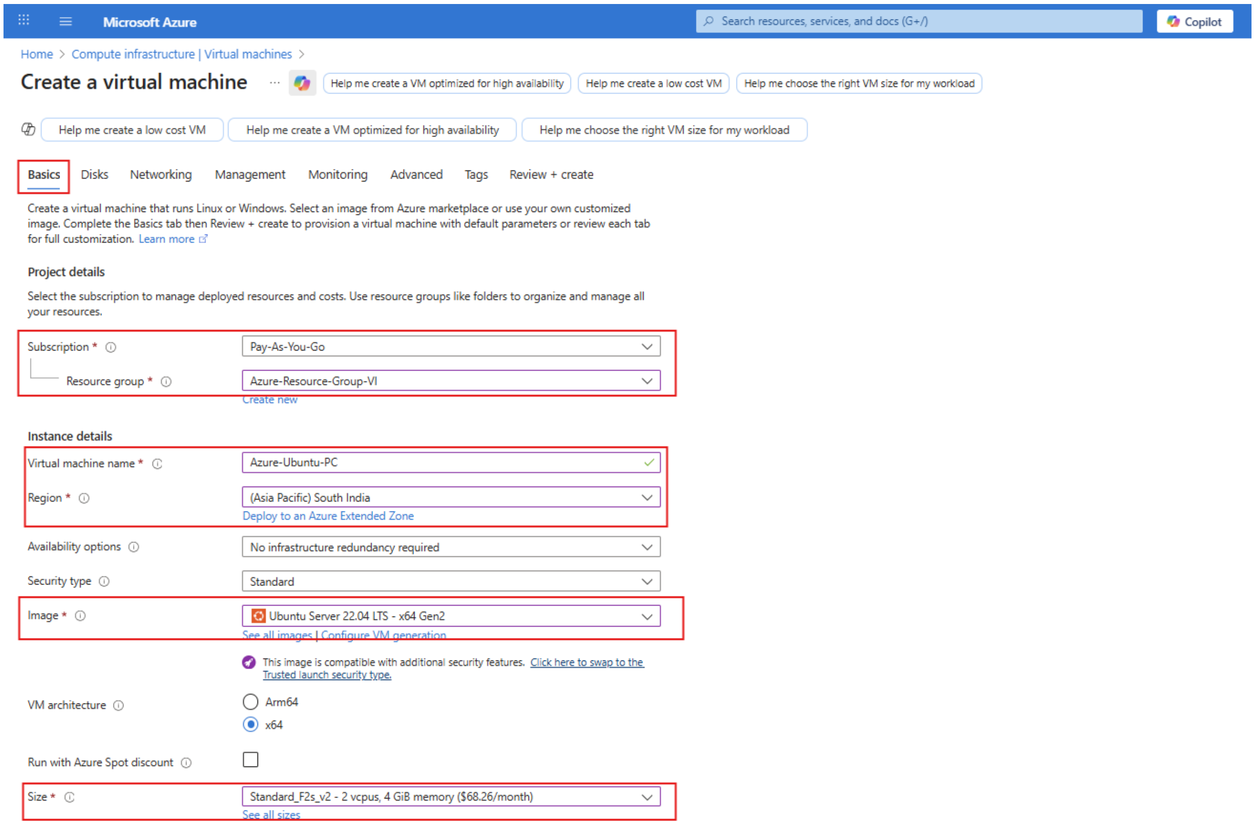
Under Virtual Machines, click on Create and select “Virtual Machine”.



Virtual machine
Best for lower-traffic workloads, testing, or to control or highly customize apps, OS, or file system. If your workload or traffic starts to grow, a VM can later be attached to a Virtual Machine Scale Set (VMSS).

Virtual machine scale set (VMSS)
Built-in scaling, performance optimization, load balancing, and batch management for 1 to 1,000 VMs (no added cost). Include multiple VM sizes, zones, regions, and domains, along with discounted Spot VMs.

In Basics tab, under Project details, make sure the correct subscription and Resource group are selected. Under Instance details, provide the name of the VM, Region and select the required image and the size as per your requirement.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Compute infrastructure | Virtual machines >
Help me create a VM optimized for high availability
Help me create a low cost VM
Help me choose the right VM size for my workload
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Basics
Disks
Networking
Management
Monitoring
Advanced
Tags
Review + create
Learn more
Create new
Deploy to an Azure Extended Zone
See all images | Configure VM generation
Click here to swap to the Trusted launch security type.
See all sizes

Create a virtual machine

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

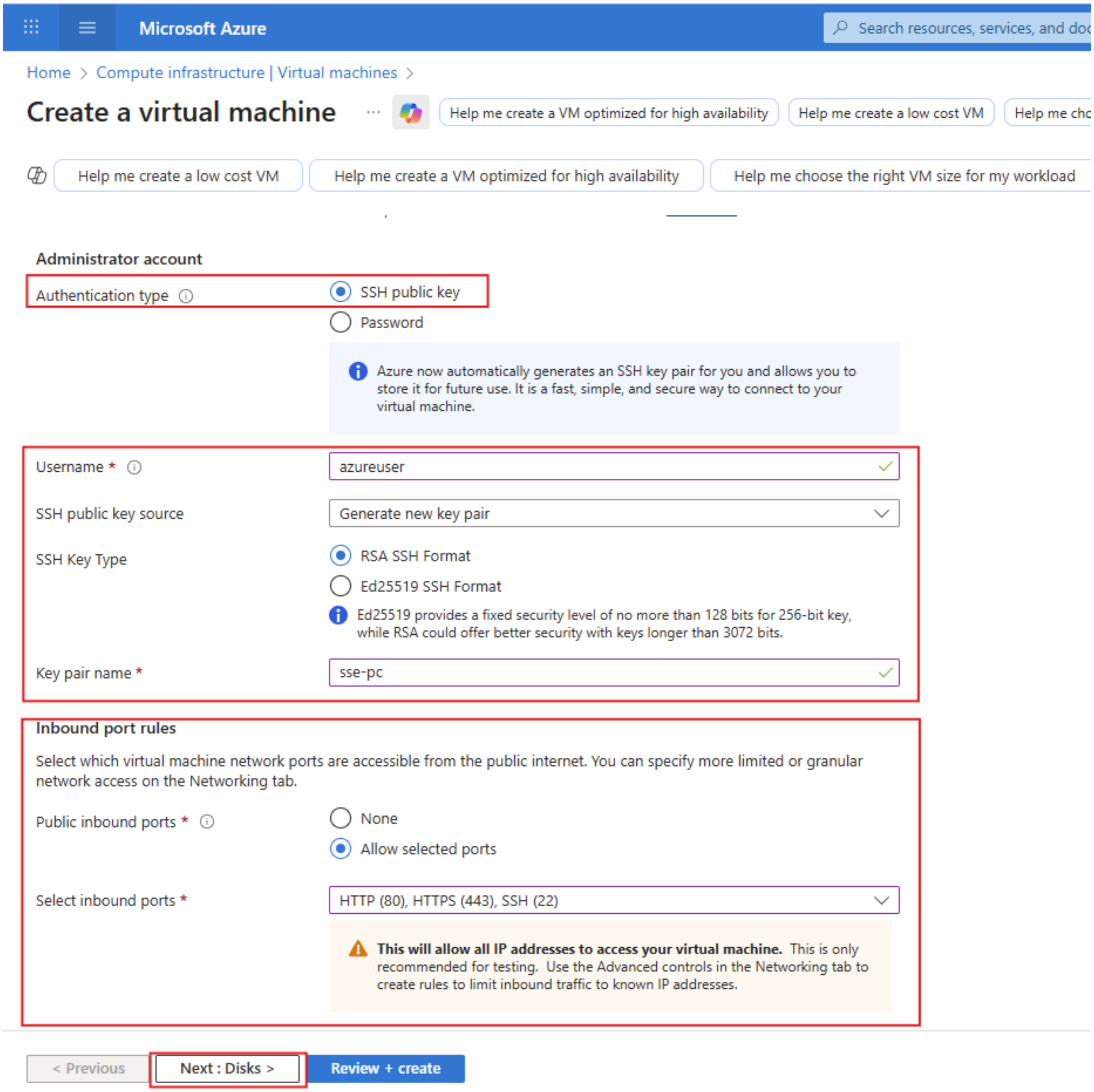
Subscription *	Pay-As-You-Go
Resource group *	Azure-Resource-Group-VI

Instance details

Virtual machine name *	Azure-Ubuntu-PC ✓
Region *	(Asia Pacific) South India
Availability options	No infrastructure redundancy required
Security type	Standard
Image *	Ubuntu Server 22.04 LTS - x64 Gen2
	This image is compatible with additional security features. Click here to swap to the Trusted launch security type.
VM architecture	○ Arm64 ● x64
Run with Azure Spot discount	□
Size *	Standard_F2s_v2 - 2 vcpus, 4 GiB memory ($68.26/month)

Under Administrator account, provide the authentication type as “SSH public key” and provide the “Username”, and select “Generate new key pair” for SSH public key source and SSH Key Type as “RSA SSH Format”.

Under Inbound port rules > Public inbound ports, choose Allow selected ports and then select required ports(ssh, http, https) from the drop-down and click on “Next: Disks>”


Microsoft Azure
Search resources, services, and doc
Home > Compute infrastructure | Virtual machines >
Help me create a VM optimized for high availability
Help me create a low cost VM
Help me cho
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
< Previous
Next : Disks >
Review + create

Create a virtual machine

Administrator account

Authentication type: ● SSH public key ○ Password

Azure now automatically generates an SSH key pair for you and allows you to store it for future use. It is a fast, simple, and secure way to connect to your virtual machine.

Username *: azureuser

SSH public key source: Generate new key pair

SSH Key Type: ● RSA SSH Format ○ Ed25519 SSH Format

Ed25519 provides a fixed security level of no more than 128 bits for 256-bit key, while RSA could offer better security with keys longer than 3072 bits.

Key pair name *: sse-pc

Inbound port rules

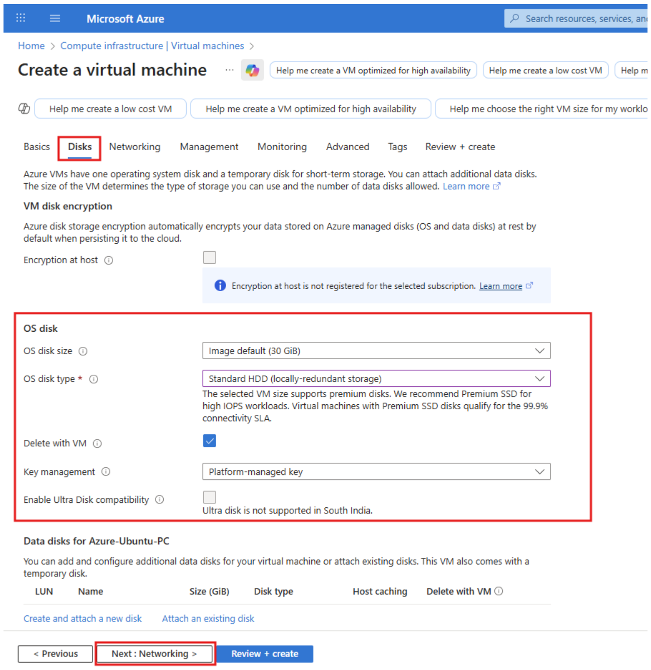
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports *: ○ None ● Allow selected ports

Select inbound ports *: HTTP (80), HTTPS (443), SSH (22)

This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

In Disks tab, select the OS disk as per the requirement and click on Next: Networking>.


Microsoft Azure
Search resources, services, and
Home > Compute infrastructure | Virtual machines >
Help me create a VM optimized for high availability
Help me create a low cost VM
Help m
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my worklo
Basics
Disks
Networking
Management
Monitoring
Advanced
Tags
Review + create
< Previous
Next : Networking >
Review + create

Create a virtual machine

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. Learn more

VM disk encryption

Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.

Encryption at host ☐

Encryption at host is not registered for the selected subscription. Learn more

OS disk

OS disk size: Image default (30 GiB)

OS disk type *: Standard HDD (locally-redundant storage)
The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

Delete with VM ☑

Key management: Platform-managed key

Enable Ultra Disk compatibility ☐
Ultra disk is not supported in South India.

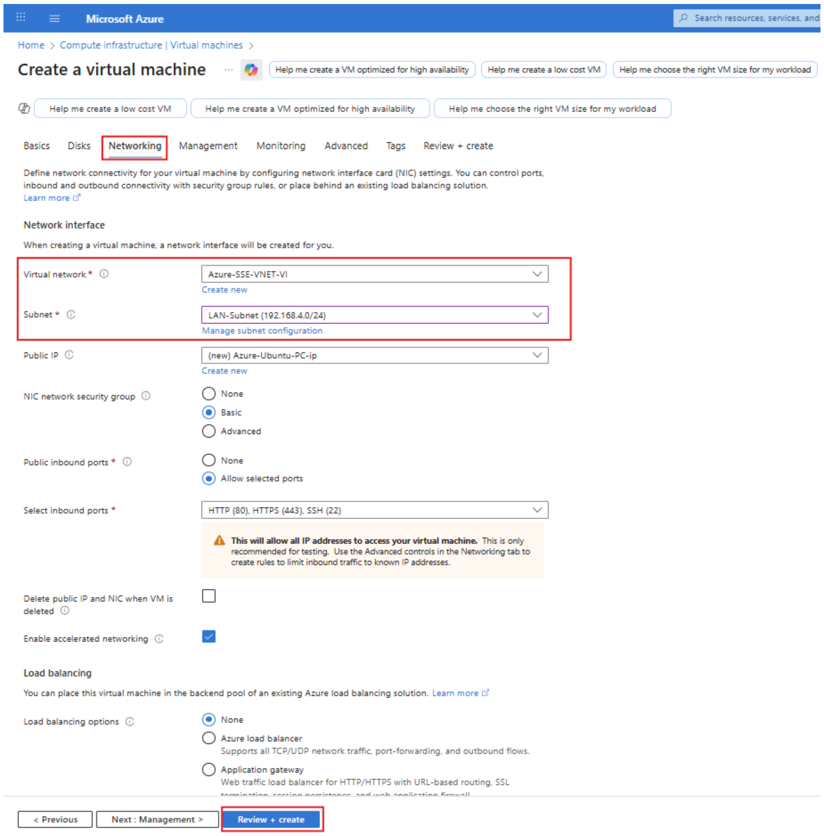
Data disks for Azure-Ubuntu-PC

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching	Delete with VM

Create and attach a new disk   Attach an existing disk

In Networking Tab, provide the Virtual Network, Subnet and leave the rest to default and click on "Review+create".


Microsoft Azure
Search resources, services, and
Home > Compute infrastructure | Virtual machines >
Help me create a VM optimized for high availability
Help me create a low cost VM
Help me choose the right VM size for my workload
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Basics
Disks
Networking
Management
Monitoring
Advanced
Tags
Review + create
< Previous
Next : Management >
Review + create

Create a virtual machine

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.
Learn more

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network *: Azure-SSE-VNET-VI
Create new

Subnet *: LAN-Subnet (192.168.4.0/24)
Manage subnet configuration

Public IP: (new) Azure-Ubuntu-PC-ip
Create new

NIC network security group: ○ None ● Basic ○ Advanced

Public inbound ports *: ○ None ● Allow selected ports

Select inbound ports *: HTTP (80), HTTPS (443), SSH (22)

This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Delete public IP and NIC when VM is deleted ☐

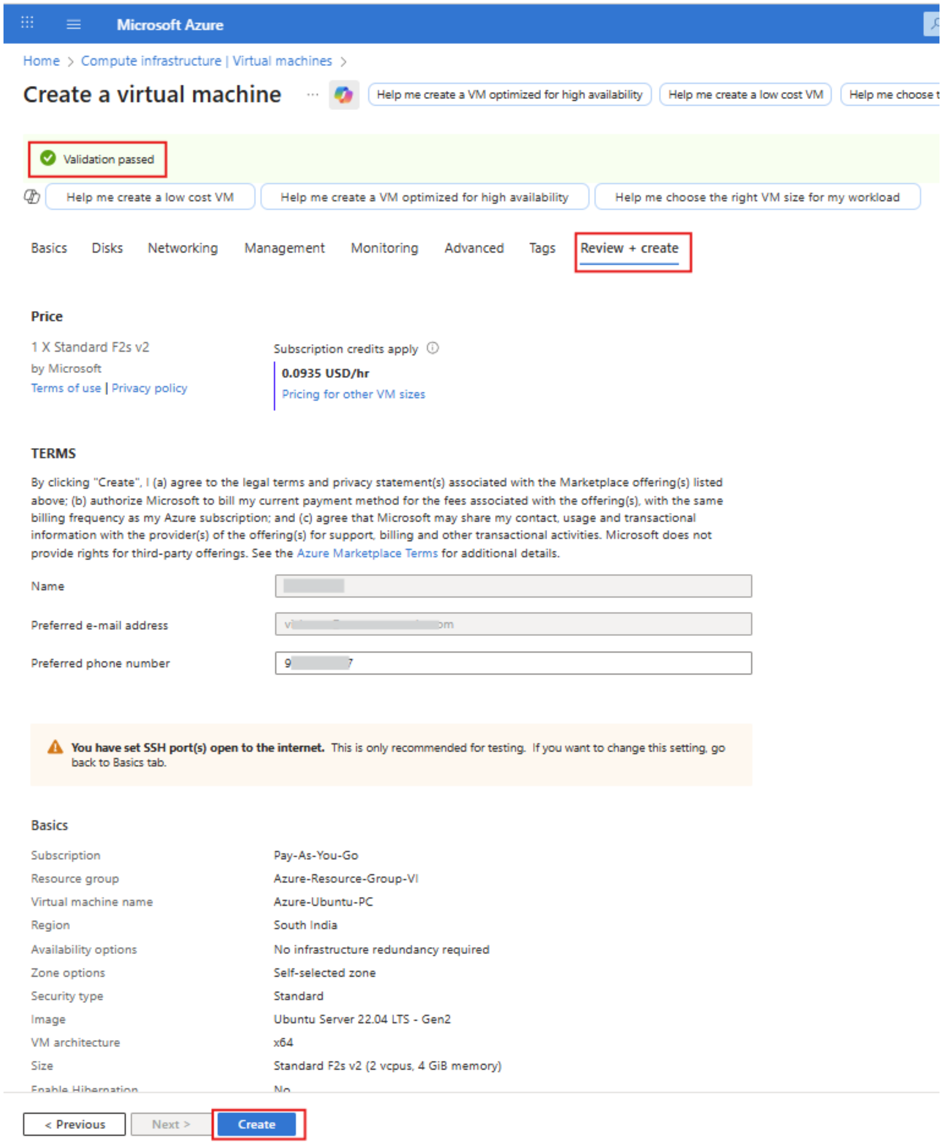
Enable accelerated networking ☑

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more

Load balancing options:
● None
○ Azure load balancer
Supports all TCP/UDP network traffic, port-forwarding, and outbound flows.
○ Application gateway
Web traffic load balancer for HTTP/HTTPS with URL-based routing, SSL termination, session persistence, and web application firewall

In "Review + create" tab click on "Create" once the validation is passed.



Home > Compute infrastructure | Virtual machines >

Create a virtual machine

Help me create a VM optimized for high availability
Help me create a low cost VM
Help me choose t

Validation passed

Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload

Basics
Disks
Networking
Management
Monitoring
Advanced
Tags
Review + create

Price

1 X Standard F2s v2
by Microsoft
Terms of use | Privacy policy

Subscription credits apply
0.0935 USD/hr
Pricing for other VM sizes

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.

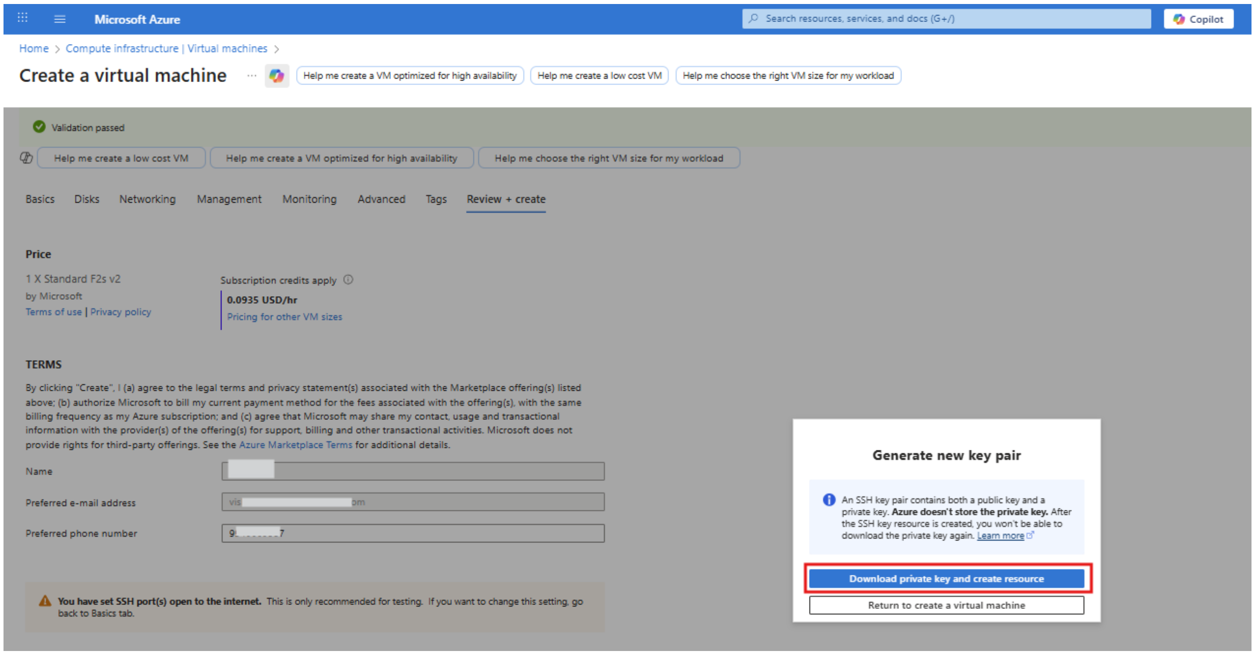
Name	[redacted]
Preferred e-mail address	vi[redacted]om
Preferred phone number	9[redacted]7

You have set SSH port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.

Basics

Subscription	Pay-As-You-Go
Resource group	Azure-Resource-Group-VI
Virtual machine name	Azure-Ubuntu-PC
Region	South India
Availability options	No infrastructure redundancy required
Zone options	Self-selected zone
Security type	Standard
Image	Ubuntu Server 22.04 LTS - Gen2
VM architecture	x64
Size	Standard F2s v2 (2 vcpus, 4 GiB memory)
Enable Hibernation	No

Clicking On create will give a “Generate new key pair” popup. Click on “Download private key and create resource”. This will download a .pem file to your PC.



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Compute infrastructure | Virtual machines >

Create a virtual machine

Help me create a VM optimized for high availability
Help me create a low cost VM
Help me choose the right VM size for my workload

Validation passed

Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Basics
Disks
Networking
Management
Monitoring
Advanced
Tags
Review + create

Price

1 X Standard F2s v2
by Microsoft
Terms of use | Privacy policy

Subscription credits apply
0.0935 USD/hr
Pricing for other VM sizes

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.

Name: [redacted]
Preferred e-mail address: [redacted]
Preferred phone number: [redacted]

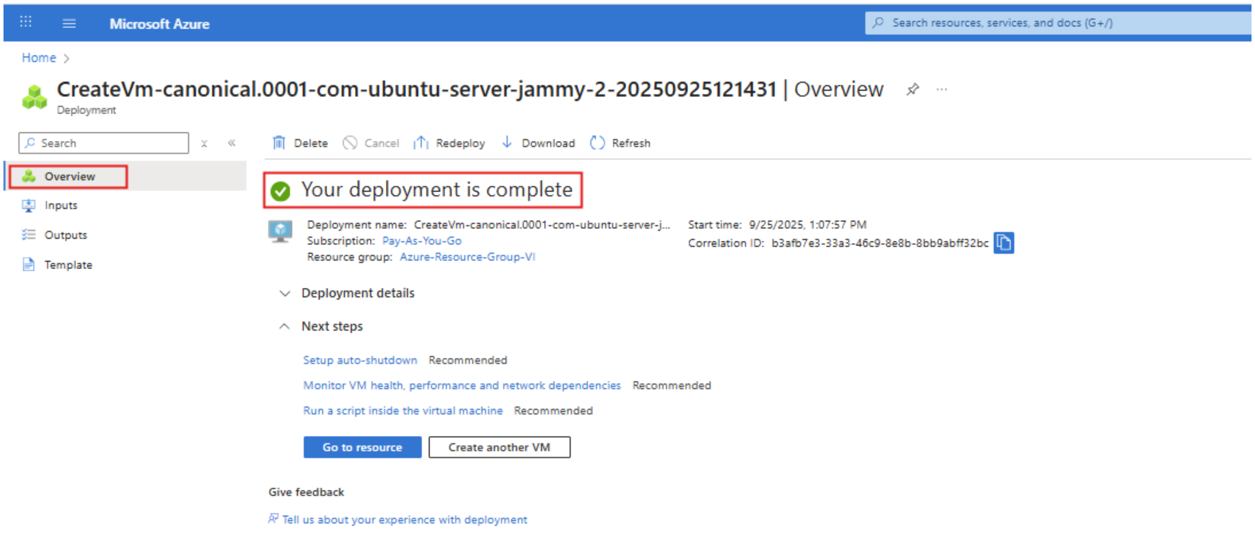
You have set SSH port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.

Generate new key pair

An SSH key pair contains both a public key and a private key. **Azure doesn't store the private key.** After the SSH key resource is created, you won't be able to download the private key again. Learn more

Download private key and create resource
Return to create a virtual machine

You can check the deployment status from Overview tab. Once the Deployment is complete click on “Go to Resource”.



CreateVm-canonical.0001-com-ubuntu-server-jammy-2-20250925121431 | Overview
Deployment

Your deployment is complete

Deployment name: CreateVm-canonical.0001-com-ubuntu-server-j...
Subscription: Pay-As-You-Go
Resource group: Azure-Resource-Group-VI
Start time: 9/25/2025, 1:07:57 PM
Correlation ID: b3afb7e3-33a3-46c9-8e8b-8bb9abff32bc

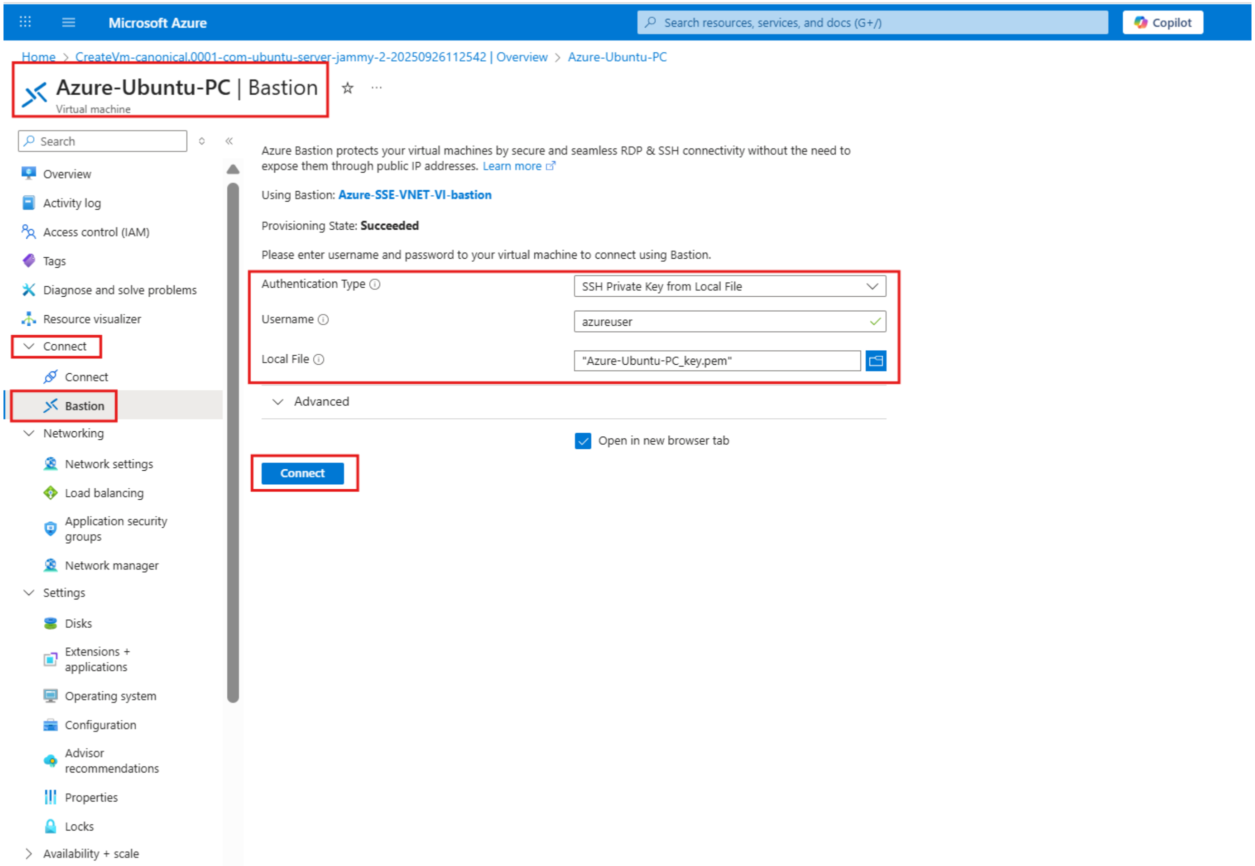
Deployment details

Next steps

Setup auto-shutdown Recommended
Monitor VM health, performance and network dependencies Recommended
Run a script inside the virtual machine Recommended

Give feedback
Tell us about your experience with deployment

To Access the Virtual Machine, under “Connect” go to “Bastion” and provide the Authentication Type as “SSH Private key from local file”, provide the username of the VM and select the .pem file which was downloaded while creating the virtual machine and click on “Connect”.



Home > CreateVm-canonical.0001-com-ubuntu-server-jammy-2-20250926112542 | Overview > Azure-Ubuntu-PC

Azure-Ubuntu-PC | Bastion
Virtual machine

Azure Bastion protects your virtual machines by secure and seamless RDP & SSH connectivity without the need to expose them through public IP addresses. Learn more

Using Bastion: **Azure-SSE-VNET-VI-bastion**

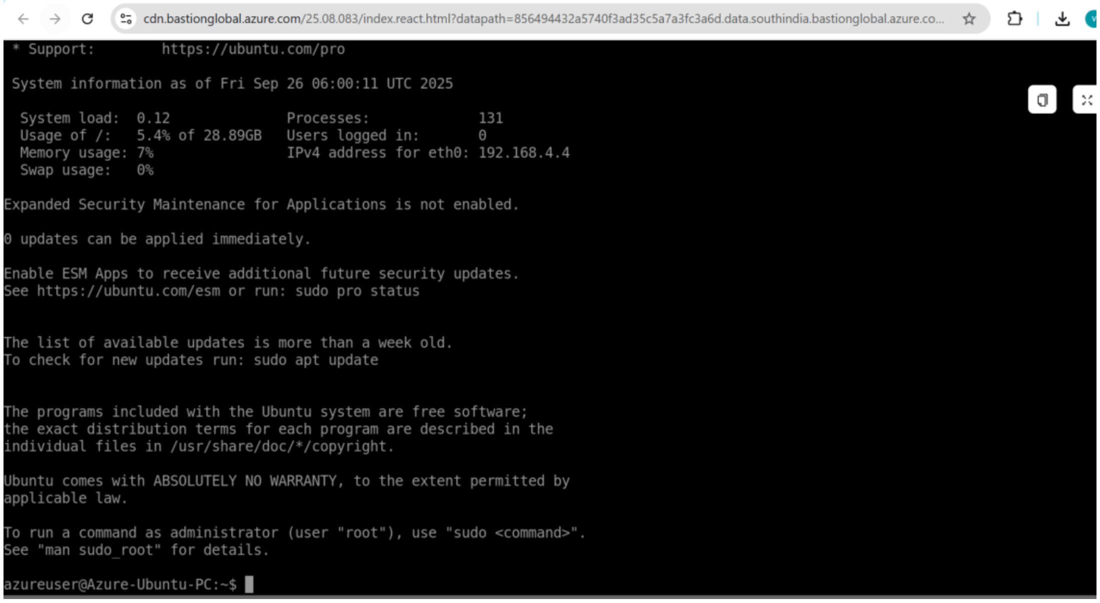
Provisioning State: **Succeeded**

Please enter username and password to your virtual machine to connect using Bastion.

Authentication Type: SSH Private Key from Local File
Username: azureuser
Local File: "Azure-Ubuntu-PC_key.pem"

☑ Open in new browser tab

This will open the VM console in the new tab.



cdn.bastionglobal.azure.com/25.08.083/index.react.html?datapath=856494432a5740f3ad35c5a7a3fc3a6d.data.southindia.bastionglobal.azure.co...

```
 * Support:        https://ubuntu.com/pro

 System information as of Fri Sep 26 06:00:11 UTC 2025

  System load:  0.12               Processes:             131
  Usage of /:   5.4% of 28.89GB    Users logged in:       0
  Memory usage: 7%                 IPv4 address for eth0: 192.168.4.4
  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


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

azureuser@Azure-Ubuntu-PC:~$
```

Local Network Gateway:

A Local Network Gateway in Azure represents your on-premises (or SASE) VPN device and is used in Site-to-Site (S2S) VPN configurations.

Use Case:

Required to create a connection between Azure's VPN Gateway and your on-prem/SASE device

Virtual Network Gateway

A Virtual Network Gateway in Azure serves as the VPN or ExpressRoute endpoint, connecting the Virtual Network Gateway to on-premises networks, other VNets, or ExpressRoute circuits.

Virtual WAN

Azure Virtual WAN is a networking service provided by Microsoft Azure that simplifies large-scale branch connectivity, hybrid networks, and remote user access through unified, global architecture. It is ideal for enterprises looking to modernize their network and security infrastructure in the cloud.

Key Components:

Virtual WAN Hub:

- A Microsoft-managed virtual network.
- Acts as the central point for connectivity.
- Supports high-scale branch, site, and user connections.

VPN Gateway:

- Supports IPsec Site-to-Site VPN.
- Scalable, with active-active high availability.

Use Cases:

- Global branch connectivity via IPsec or SD-WAN.
- Secure remote user access with integrated policies.

Network Security Group (NSG)

A Network Security Group (NSG) in Azure acts as a virtual firewall to control inbound and outbound traffic, filtering based on IP address, port number, and protocol; it can be associated with subnets or network interfaces (NICs), includes default security rules with support for custom rule creation, enables segmentation and access control within a Virtual Network, and helps enforce least privilege while improving the overall network security posture.

Option 1: SASE Gateway (Site-to-Site VPN Method)

Concept: Secure IPsec VPN tunnel between Azure VPN Gateway and Versa SASE gateway.

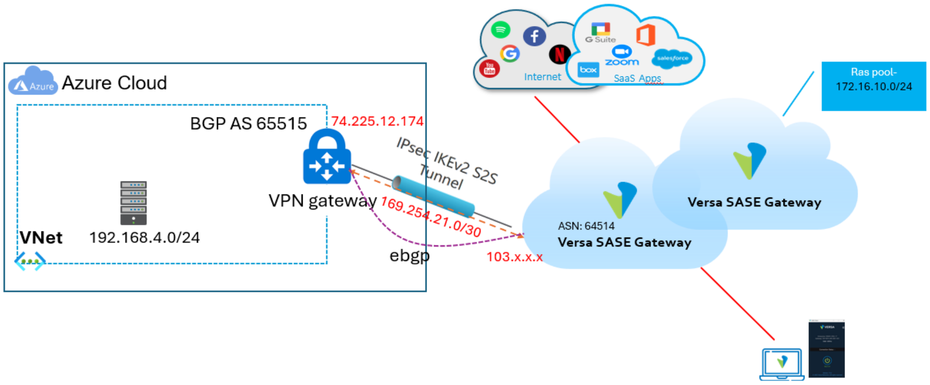
A site-to-site IPsec VPN is established between the SASE Gateway and the Azure VPN Gateway. The tunnels are configured for high availability, and dynamic route exchange is performed over the IPsec connection using eBGP between the VPN Gateway and the SASE Gateway.

This option is used when you have a single VNet and requires a simple, direct, and cost-effective

IPsec tunnel to connect the SASE Gateway with Azure.

Use Cases: Connect a specific Azure VNet to Versa SASE, extend on-prem networks.

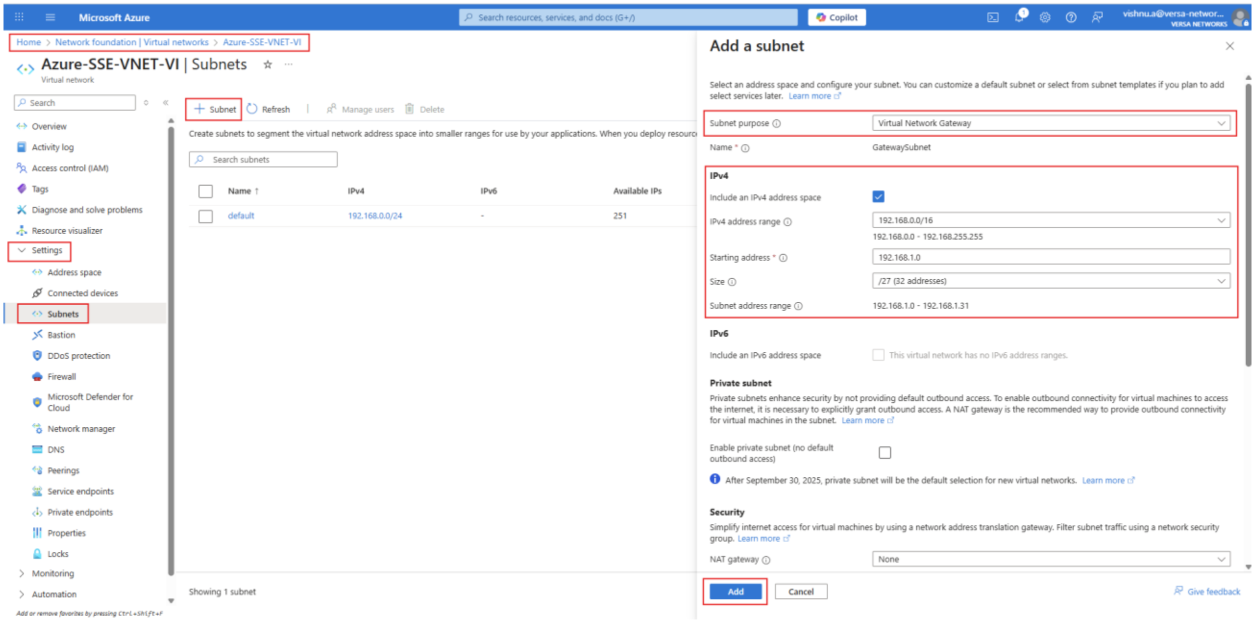
Key Components: Azure VNet, VPN Gateway, Local Network Gateway, VPN Connection, Versa SASE Gateway



Azure Configuration

Creating a Virtual network Gateway (VPN Gateway)

To create a VPN Gateway, first we need Gateway subnet to be created.



Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resourc

	Name ↑	IPv4	IPv6	Available IPs
□	default	192.168.0.0/24	-	251

Showing 1 subnet

Add a subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. Learn more

Subnet purpose: Virtual Network Gateway

Name *: GatewaySubnet

IPv4

Include an IPv4 address space: ☑

IPv4 address range: 192.168.0.0/16
192.168.0.0 - 192.168.255.255

Starting address *: 192.168.1.0

Size: /27 (32 addresses)

Subnet address range: 192.168.1.0 - 192.168.1.31

IPv6

Include an IPv6 address space: □ This virtual network has no IPv6 address ranges.

Private subnet

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. Learn more

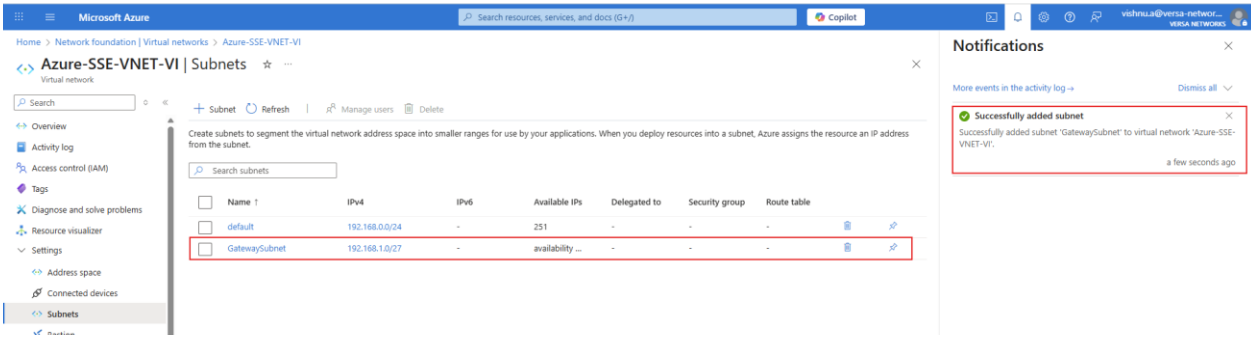
Enable private subnet (no default outbound access): □

After September 30, 2025, private subnet will be the default selection for new virtual networks. Learn more

Security

Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. Learn more

NAT gateway: None



Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet.

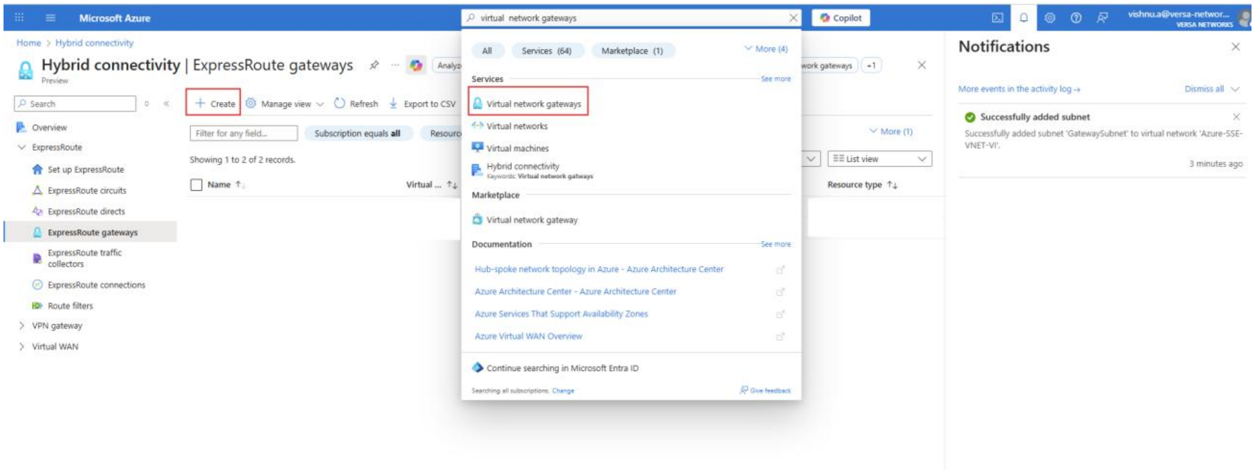
Name ↑	IPv4	IPv6	Available IPs	Delegated to	Security group	Route table
default	192.168.0.0/24	-	251	-	-	-
GatewaySubnet	192.168.1.0/27	-	availability ...	-	-	-

Successfully added subnet

Successfully added subnet 'GatewaySubnet' to virtual network 'Azure-SSE-VNET-VI'.

a few seconds ago

Once the GatewaySubnet is created search Virtual network gateways in the search bar and select Virtual network gateways and click on “+create” to create a new VPN Gateway.

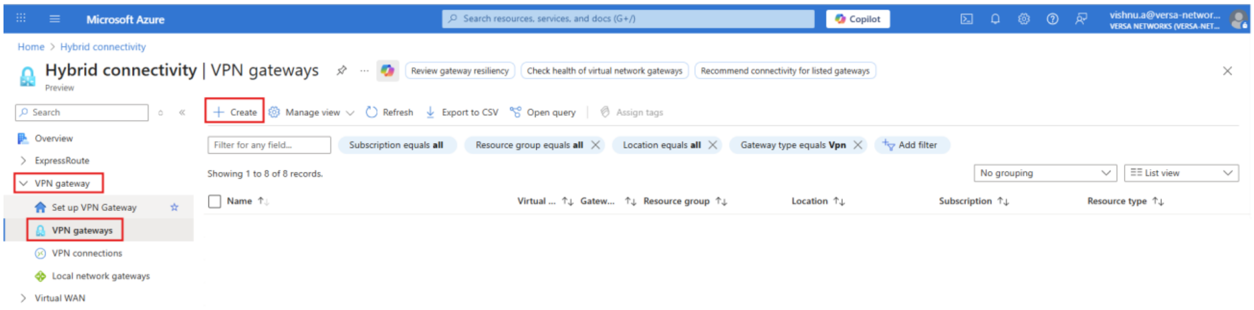


Successfully added subnet

Successfully added subnet 'GatewaySubnet' to virtual network 'Azure-SSE-VNET-VI'.

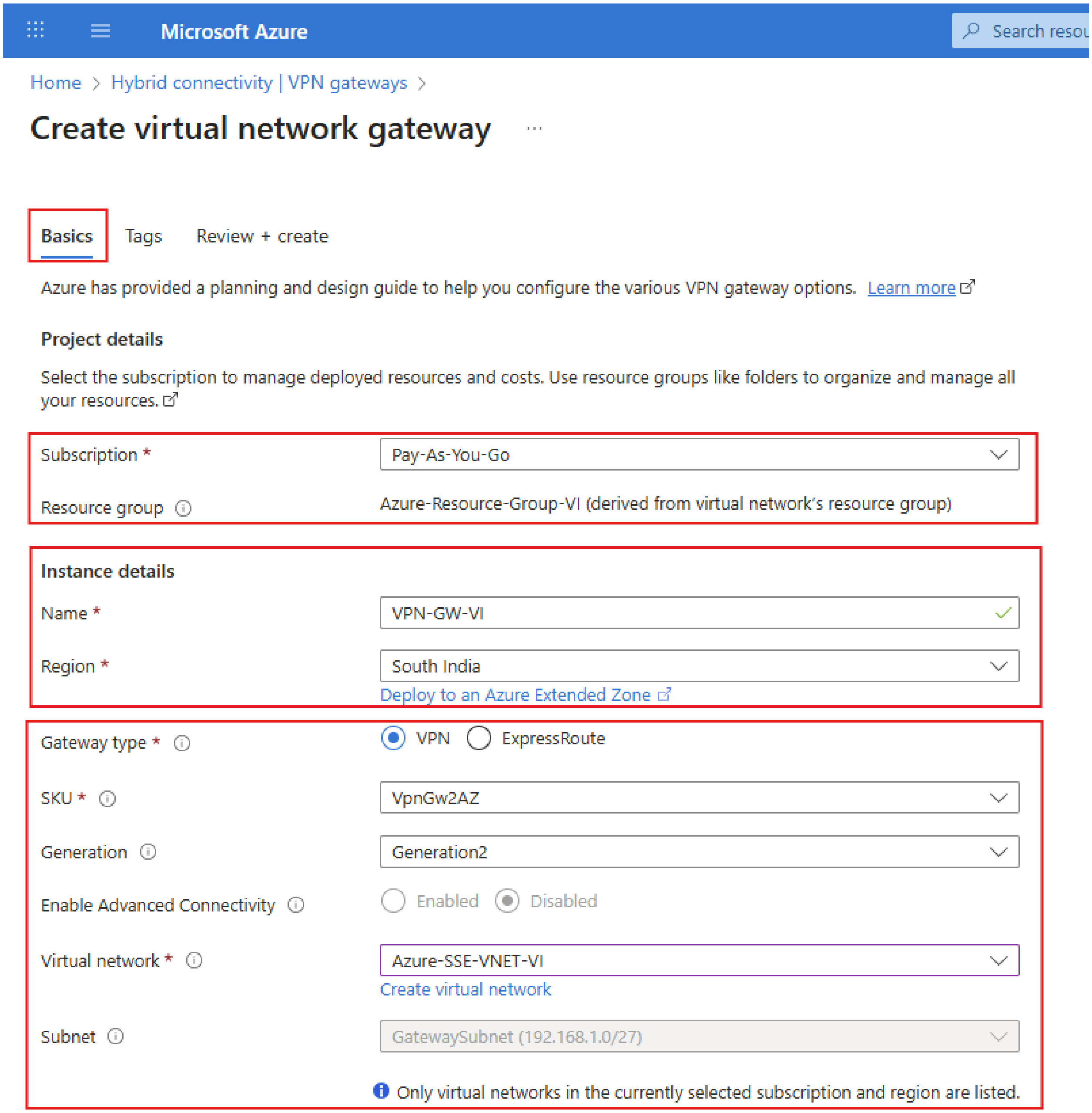
3 minutes ago

Under VPN gateway, go to VPN gateways and click on “+Create”.



Showing 1 to 8 of 8 records.

Under “Basics” tab when creating an Azure VPN Gateway, choose the subscription, region (matching the VNet), gateway type **VPN**, an appropriate AZ-enabled SKU, and generation as Generation2, then select the virtual network and **GatewaySubnet** address range is automatically populated.



Create virtual network gateway ...

Basics Tags Review + create

Azure has provided a planning and design guide to help you configure the various VPN gateway options. Learn more

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	Pay-As-You-Go
Resource group	Azure-Resource-Group-VI (derived from virtual network's resource group)

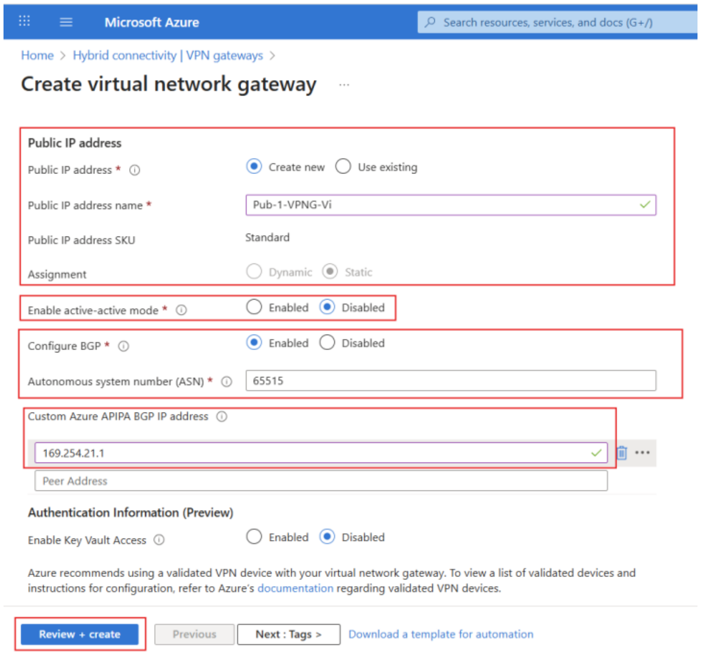
Instance details

Name *	VPN-GW-VI
Region *	South India Deploy to an Azure Extended Zone
Gateway type *	● VPN ○ ExpressRoute
SKU *	VpnGw2AZ
Generation	Generation2
Enable Advanced Connectivity	○ Enabled ● Disabled
Virtual network *	Azure-SSE-VNET-VI Create virtual network
Subnet	GatewaySubnet (192.168.1.0/27)

Only virtual networks in the currently selected subscription and region are listed.

Under "Public IP address" select "Create new" and provide the name of the Public-IP . These settings specify the public IP address objects that will be associated to the VPN gateway.

Once the IP Address information is given, enable BGP and leave the ASN to default and provide the Custom Azure BGP IP and click on "Review+create".



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Hybrid connectivity | VPN gateways >

Create virtual network gateway ...

Public IP address

Public IP address * ⓘ	● Create new ○ Use existing
Public IP address name *	Pub-1-VPNG-Vi
Public IP address SKU	Standard
Assignment	○ Dynamic ● Static
Enable active-active mode * ⓘ	○ Enabled ● Disabled
Configure BGP * ⓘ	● Enabled ○ Disabled
Autonomous system number (ASN) * ⓘ	65515

Custom Azure APIPA BGP IP address ⓘ

169.254.21.1

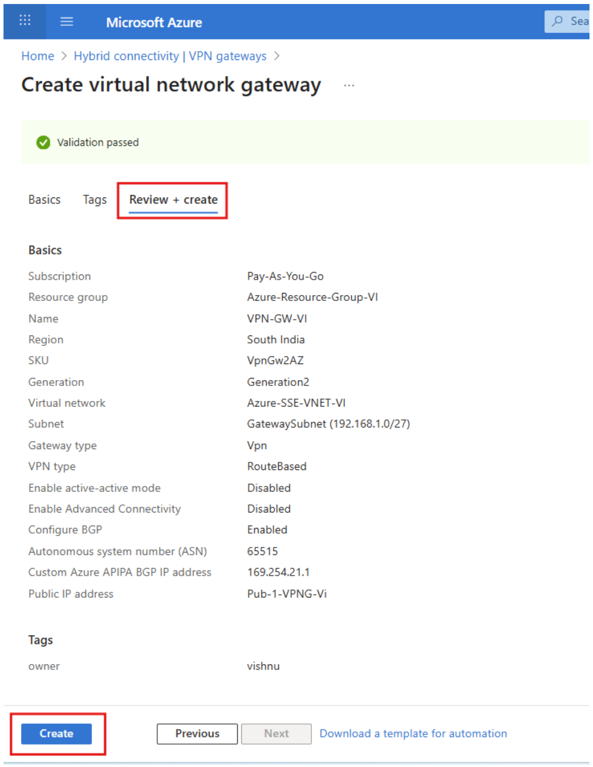
Peer Address

Authentication Information (Preview)

Enable Key Vault Access ⓘ	○ Enabled ● Disabled

Azure recommends using a validated VPN device with your virtual network gateway. To view a list of validated devices and instructions for configuration, refer to Azure's documentation regarding validated VPN devices.

Under “Review + create” tab review the configuration and click on “Create”.



Create virtual network gateway ...

Validation passed

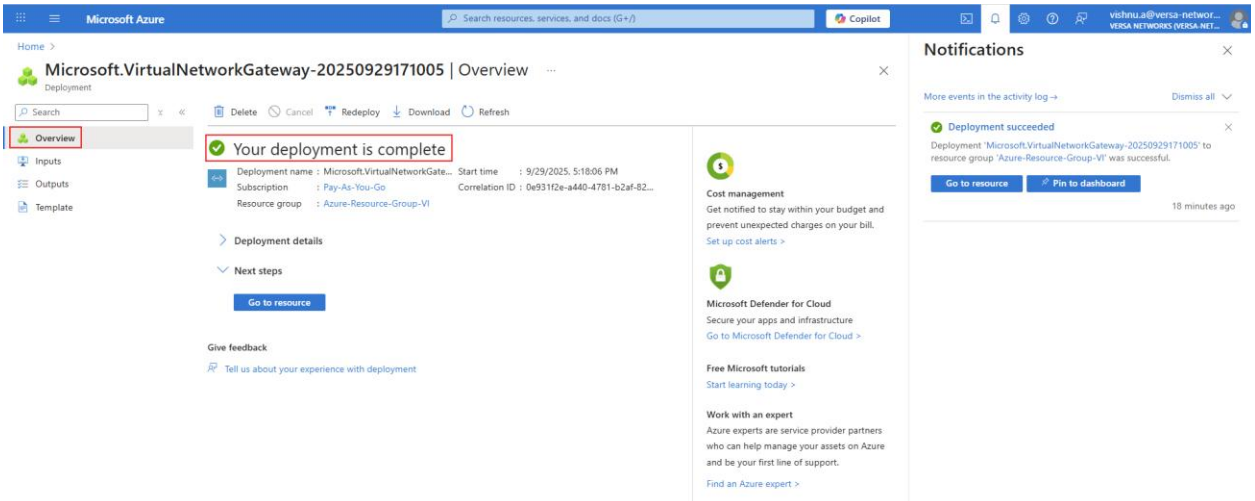
Basics

Subscription	Pay-As-You-Go
Resource group	Azure-Resource-Group-VI
Name	VPN-GW-VI
Region	South India
SKU	VpnGw2AZ
Generation	Generation2
Virtual network	Azure-SSE-VNET-VI
Subnet	GatewaySubnet (192.168.1.0/27)
Gateway type	Vpn
VPN type	RouteBased
Enable active-active mode	Disabled
Enable Advanced Connectivity	Disabled
Configure BGP	Enabled
Autonomous system number (ASN)	65515
Custom Azure APIPA BGP IP address	169.254.21.1
Public IP address	Pub-1-VPNG-Vi

Tags

owner	vishnu

VPN gateway can take 45 minutes or more to fully create and deploy. You can see the deployment status on the “Overview” page for your gateway. Once the deployment is complete, click on “Go to Resource”.



Microsoft.VirtualNetworkGateway-20250929171005 | Overview

Deployment

Your deployment is complete

Deployment name : Microsoft.VirtualNetworkGate...
Subscription : Pay-As-You-Go
Resource group : Azure-Resource-Group-VI
Start time : 9/29/2025, 5:18:06 PM
Correlation ID : 0e931f2e-a440-4781-b2af-82...

Give feedback

Tell us about your experience with deployment

Cost management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >

Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >

Free Microsoft tutorials
Start learning today >

Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
Find an Azure expert >

Notifications

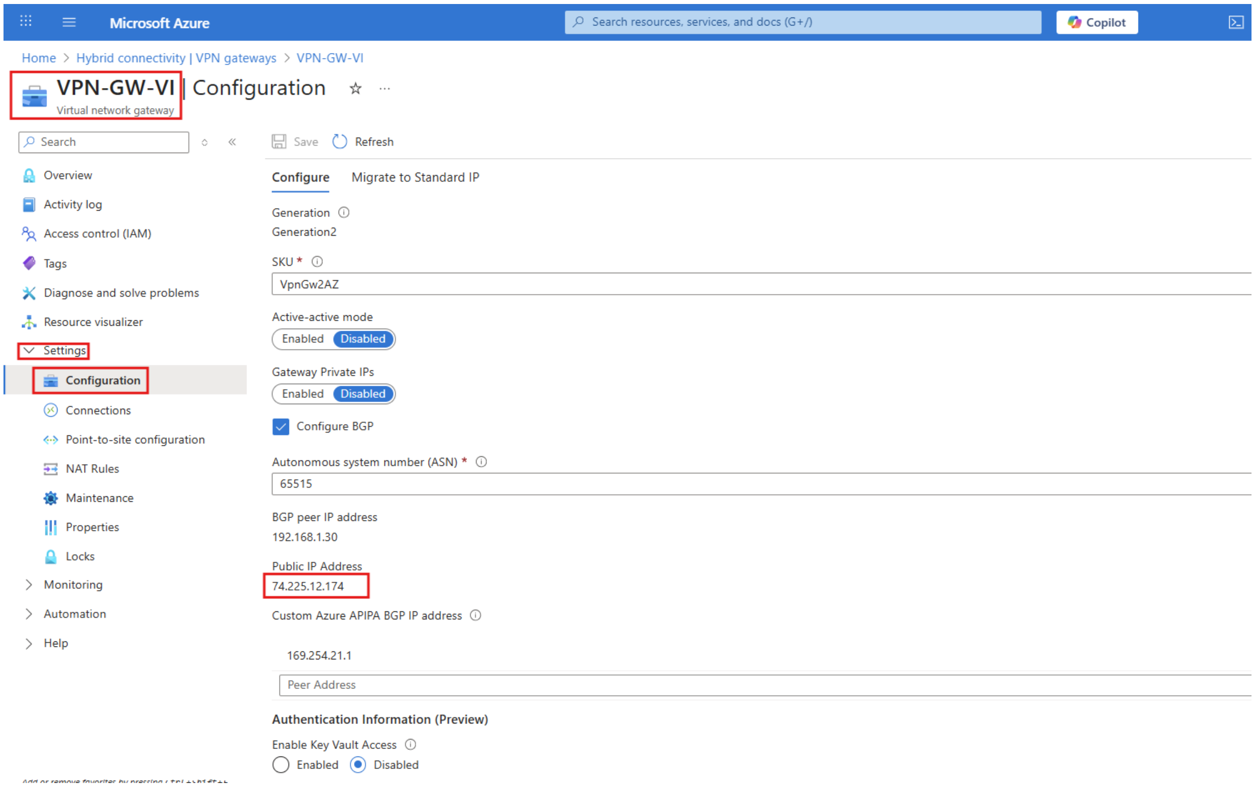
More events in the activity log → Dismiss all

Deployment succeeded
Deployment 'Microsoft.VirtualNetworkGateway-20250929171005' to resource group 'Azure-Resource-Group-VI' was successful.

Go to resource | Pin to dashboard

18 minutes ago

In the Virtual network gateway you created, under settings go to Configuration and note down the Public IP of the VPN Gateway, this IP is used to configure IPsec tunnels from SASE Gateway.



VPN-GW-VI | Configuration

Virtual network gateway

Generation: Generation2

SKU *: VpnGw2AZ

Active-active mode: Enabled [✓ Disabled]

Gateway Private IPs: Enabled [✓ Disabled]

☑ Configure BGP

Autonomous system number (ASN) *: 65515

BGP peer IP address: 192.168.1.30

Public IP Address: 74.225.12.174

Custom Azure APIPA BGP IP address

169.254.21.1

Peer Address

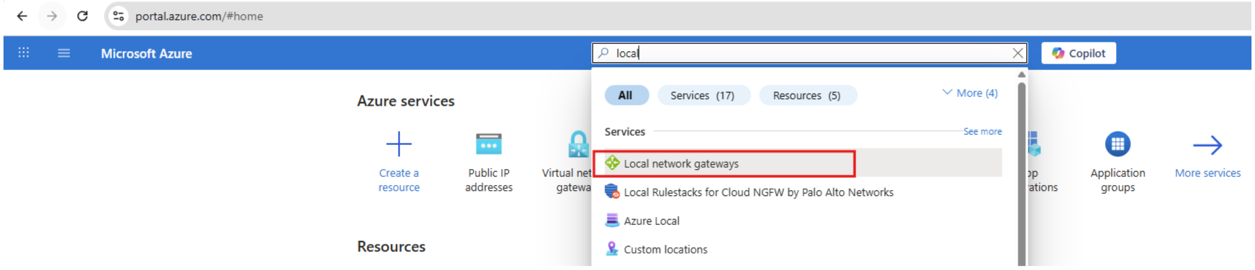
Authentication Information (Preview)

Enable Key Vault Access: ○ Enabled ● Disabled

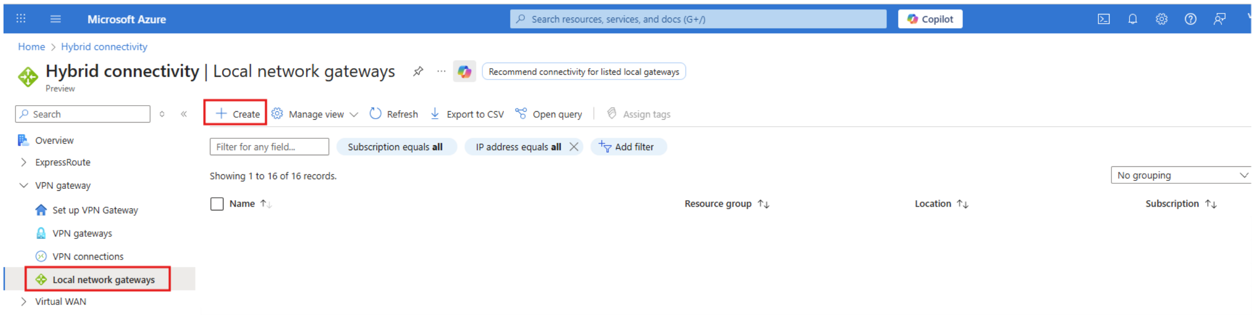
Creating Local Network Gateway

A local network gateway in Azure represents your on-premises site for routing, storing the VPN device's public IP and the on-premises address prefixes to be routed through the VPN gateway.
You can update these details if the device IP or network prefixes change, and you must create a separate local network gateway for each VPN device used in a high-availability design.

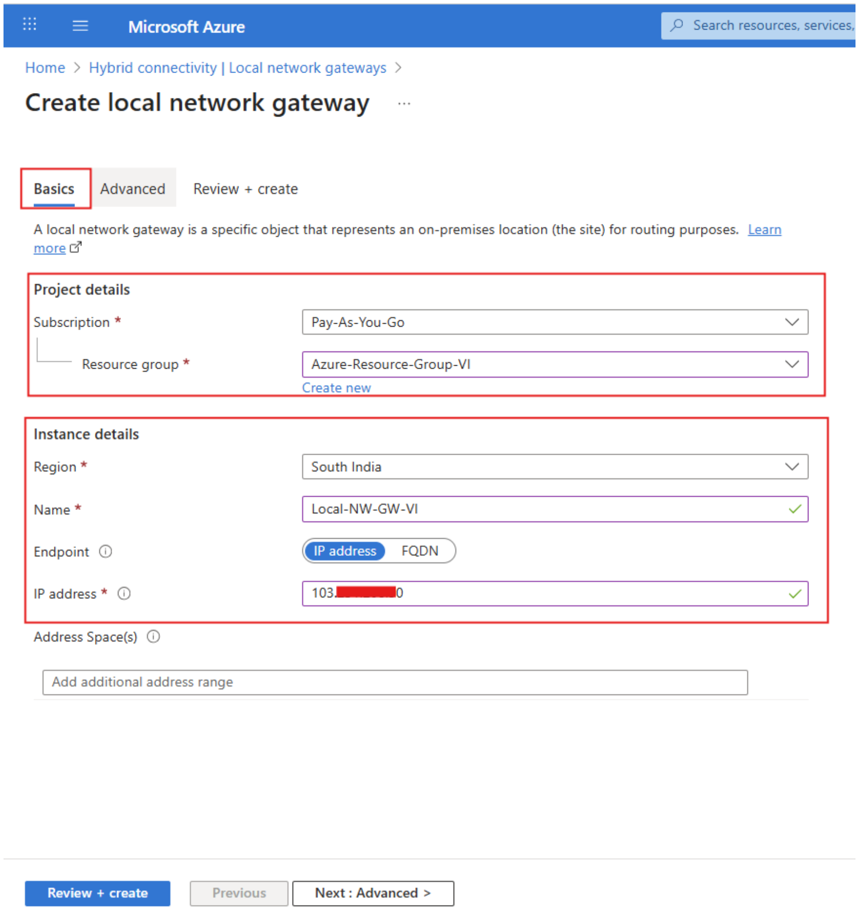
To create a Local network gateway, search 'Local network gateways' and click on it under Services.



Under VPN gateway select “Local network gateways” and click on “+Create”.



Under Basics tab Provide the Resource group, and the Instance details and click on Next.


Microsoft Azure
Search resources, services,
Home > Hybrid connectivity | Local network gateways >

Create local network gateway

Basics | Advanced | Review + create

A local network gateway is a specific object that represents an on-premises location (the site) for routing purposes. Learn more

Project details

Subscription * Pay-As-You-Go

Resource group * Azure-Resource-Group-VI

Create new

Instance details

Region * South India

Name * Local-NW-GW-VI

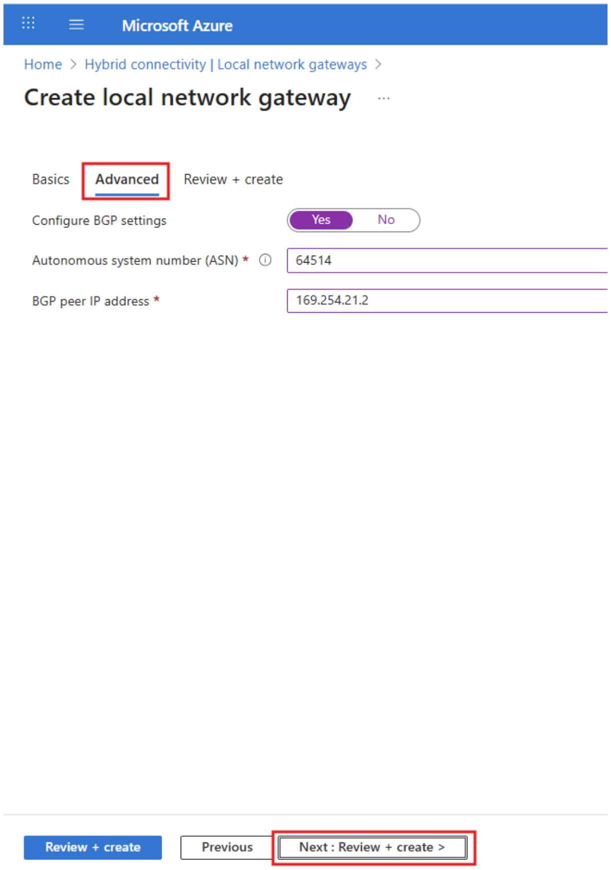
Endpoint ● IP address ○ FQDN

IP address * 103.[redacted]0

Address Space(s)

Add additional address range

Under Advance Tab, configure BGP ASN and the BGP peer IP(SASE Gateway IP).



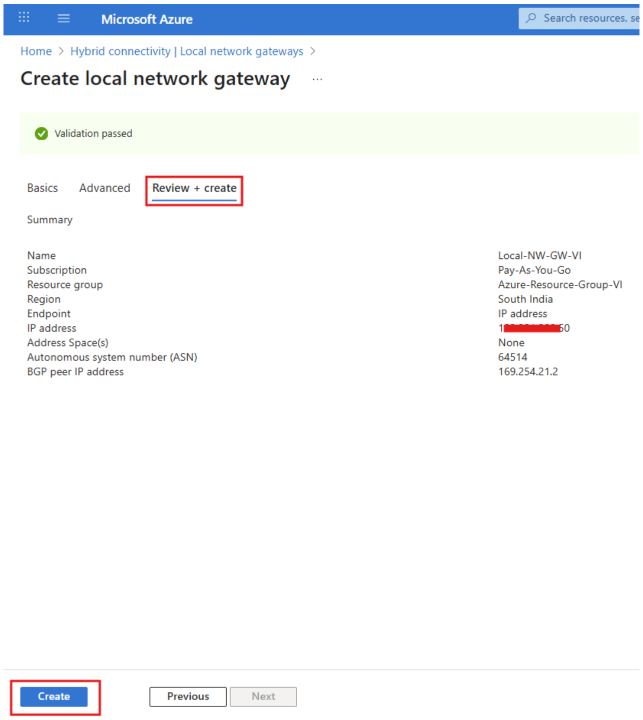
Create local network gateway ...

Configure BGP settings: Yes (selected) / No

Autonomous system number (ASN) *: 64514

BGP peer IP address *: 169.254.21.2

Under “Review+ create”, once the validation is passed click on Create.



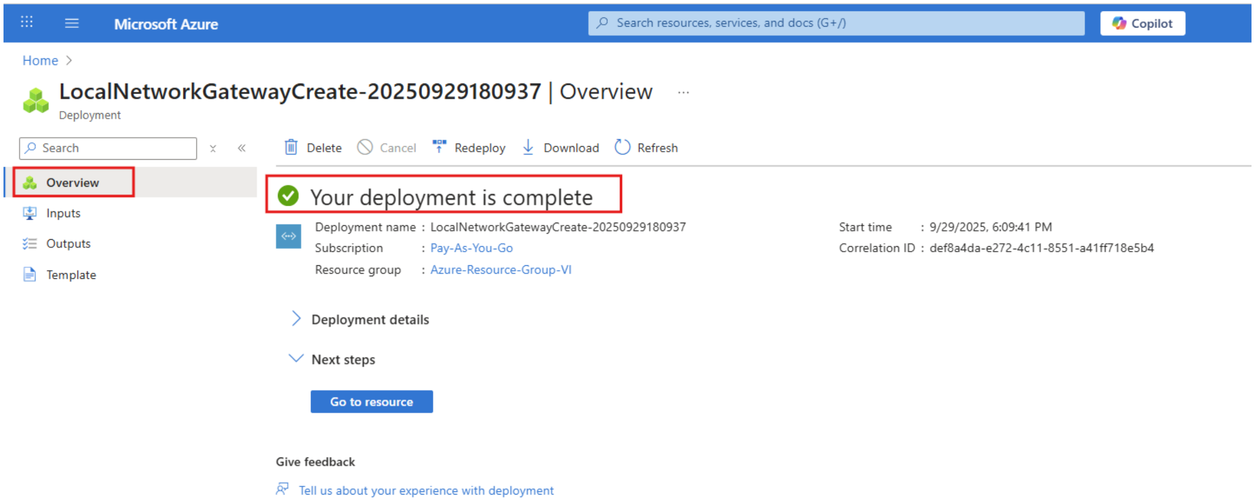
Create local network gateway ...

✓ Validation passed

Summary

Name	Local-NW-GW-VI
Subscription	Pay-As-You-Go
Resource group	Azure-Resource-Group-VI
Region	South India
Endpoint	IP address
IP address	1[redacted]50
Address Space(s)	None
Autonomous system number (ASN)	64514
BGP peer IP address	169.254.21.2

Deployment status can be viewed from “Overview” tab.



Microsoft Azure

Search resources, services, and docs (G+/)

Copilot

Home >

LocalNetworkGatewayCreate-20250929180937 | Overview ...

Deployment

Search

Delete | Cancel | Redeploy | Download | Refresh

Overview

Inputs

Outputs

Template

Your deployment is complete

Deployment name : LocalNetworkGatewayCreate-20250929180937

Subscription : Pay-As-You-Go

Resource group : Azure-Resource-Group-VI

Start time : 9/29/2025, 6:09:41 PM

Correlation ID : def8a4da-e272-4c11-8551-a41ff718e5b4

Deployment details

Next steps

Go to resource

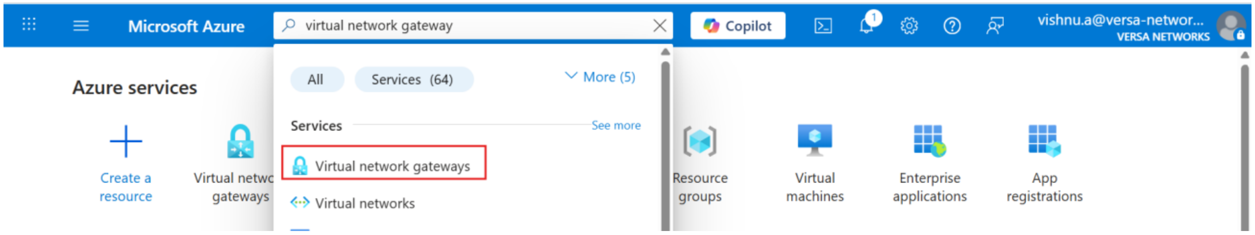
Give feedback

Tell us about your experience with deployment

Creating VPN Connection

Create a site-to-site VPN connection between your virtual network gateway and your on-premises VPN device.

To Create a VPN Connection, Go to Virtual Network gateways.



Microsoft Azure

virtual network gateway

Copilot

vishnu.a@versa-networ...
VERSA NETWORKS

Azure services

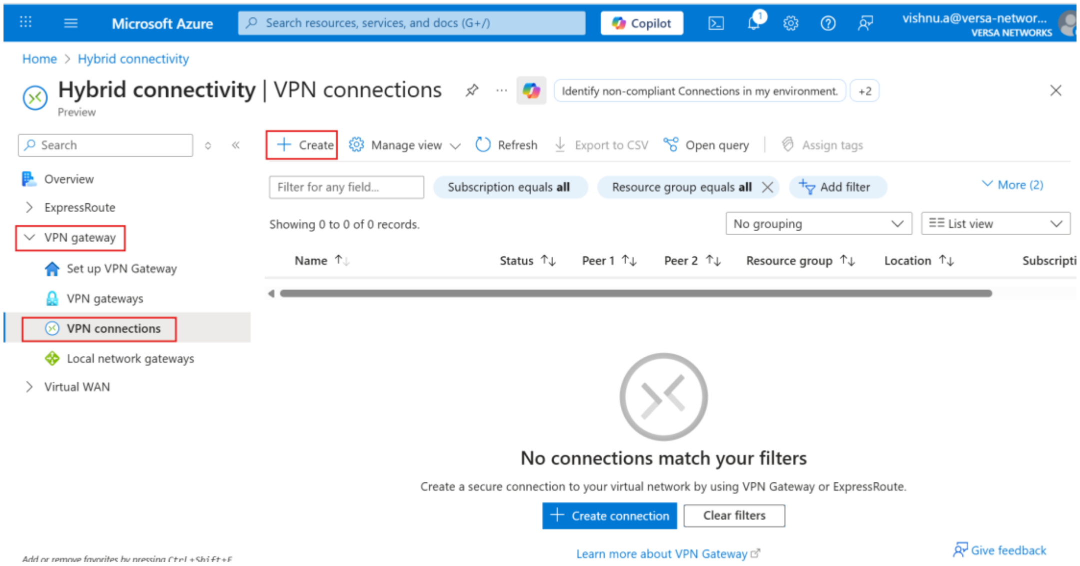
All | Services (64) | More (5)

Services | See more

Virtual network gateways

Virtual networks

Under “VPN gateway” go to “VPN connections” and click on “+Create”.



Microsoft Azure

Search resources, services, and docs (G+/)

Copilot

vishnu.a@versa-networ...
VERSA NETWORKS

Home > Hybrid connectivity

Hybrid connectivity | VPN connections

Preview

Identify non-compliant Connections in my environment. +2

Search

+ Create | Manage view | Refresh | Export to CSV | Open query | Assign tags

Overview

ExpressRoute

VPN gateway

Set up VPN Gateway

VPN gateways

VPN connections

Local network gateways

Virtual WAN

Filter for any field... | Subscription equals **all** | Resource group equals **all** | Add filter | More (2)

Showing 0 to 0 of 0 records.

No grouping | List view

Name ↑↓ | Status ↑↓ | Peer 1 ↑↓ | Peer 2 ↑↓ | Resource group ↑↓ | Location ↑↓ | Subscripti

No connections match your filters

Create a secure connection to your virtual network by using VPN Gateway or ExpressRoute.

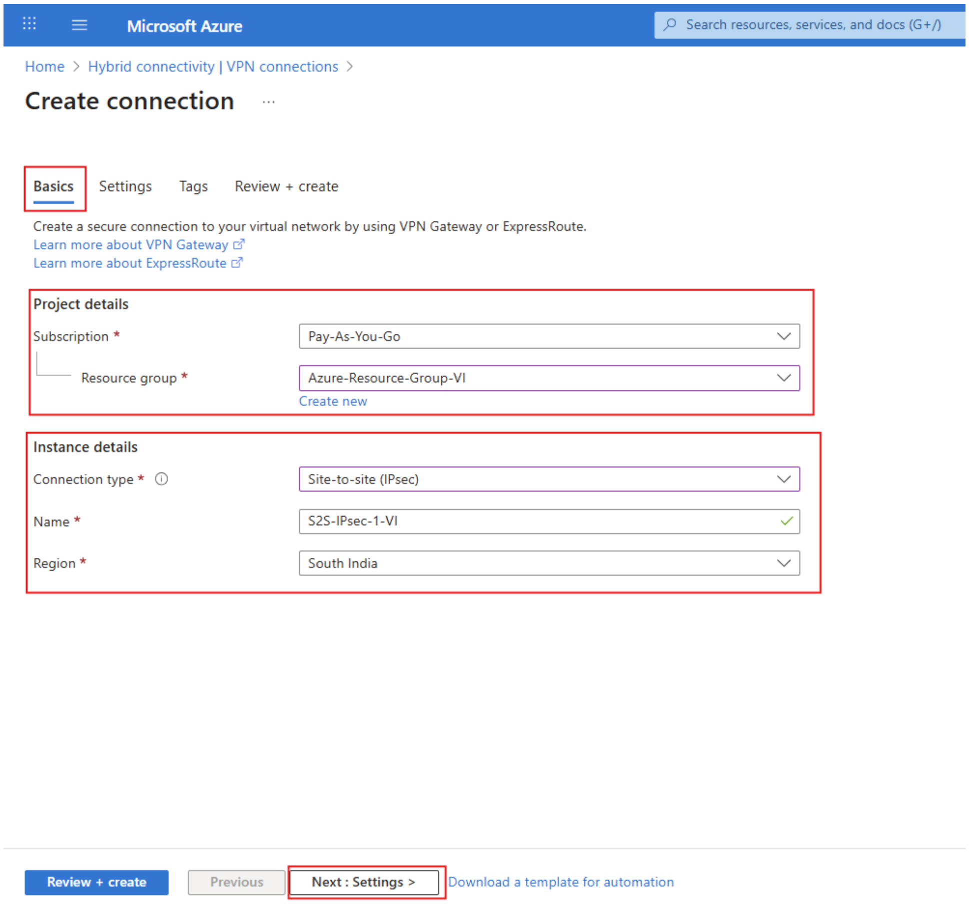
Create connection | Clear filters

Learn more about VPN Gateway

Give feedback

Add or remove favorites by pressing Ctrl+Shift+F

Under Basic tab, provide the Resource group, Connection type as "Site-to-site(IPsec), provide the name of the connection, select the Region and click on Next.



Microsoft Azure

Home > Hybrid connectivity | VPN connections >

Create connection

Create a secure connection to your virtual network by using VPN Gateway or ExpressRoute.
Learn more about VPN Gateway
Learn more about ExpressRoute

Project details

Subscription * Pay-As-You-Go

Resource group * Azure-Resource-Group-VI

Create new

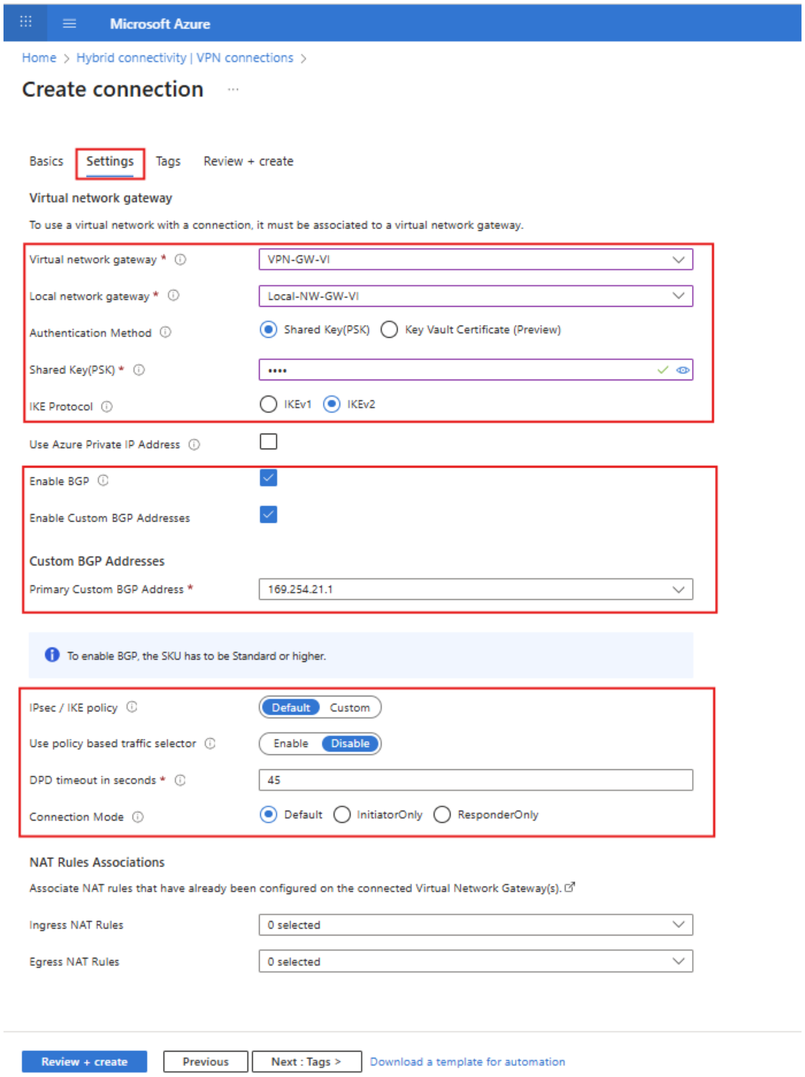
Instance details

Connection type * Site-to-site (IPsec)

Name * S2S-IPsec-1-VI

Region * South India

Under Settings, Provide the VNET Gateway, Local network Gateway, Authentication method, PSK, IKE protocol info and enable BGP with custom BGP Address and leave the rest to default.



Create connection

Virtual network gateway

To use a virtual network with a connection, it must be associated to a virtual network gateway.

Virtual network gateway * : VPN-GW-VI

Local network gateway * : Local-NW-GW-VI

Authentication Method: ● Shared Key(PSK) ○ Key Vault Certificate (Preview)

Shared Key(PSK) * : ••••

IKE Protocol: ○ IKEv1 ● IKEv2

Use Azure Private IP Address: □

Enable BGP: ☑

Enable Custom BGP Addresses: ☑

Custom BGP Addresses

Primary Custom BGP Address * : 169.254.21.1

To enable BGP, the SKU has to be Standard or higher.

IPsec / IKE policy: [✓ Default] Custom

Use policy based traffic selector: Enable [✓ Disable]

DPD timeout in seconds * : 45

Connection Mode: ● Default ○ InitiatorOnly ○ ResponderOnly

NAT Rules Associations

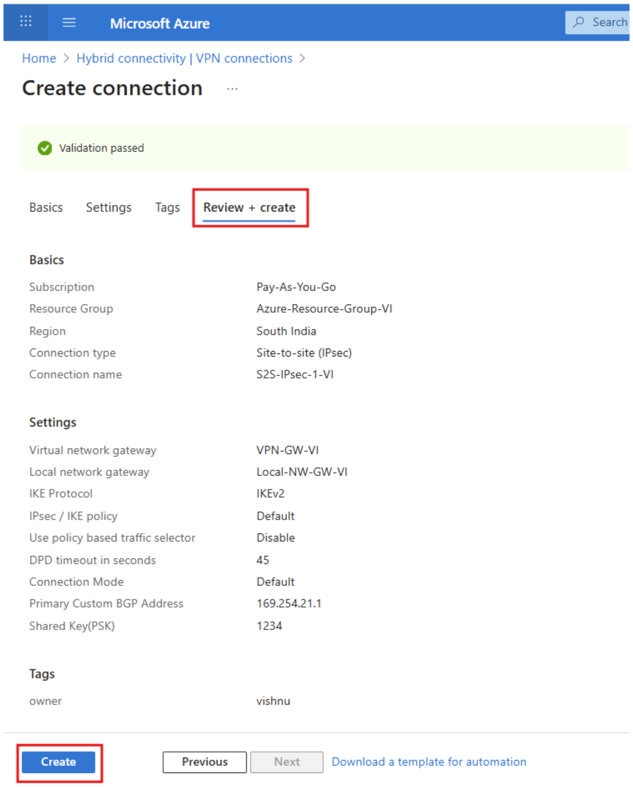
Associate NAT rules that have already been configured on the connected Virtual Network Gateway(s).

Ingress NAT Rules: 0 selected

Egress NAT Rules: 0 selected

Under Tags provide necessary information and click on “Next: Review + create >”.

Under “Review + create” tab validate the information and click on “Create”.


Microsoft Azure
Search
Home > Hybrid connectivity | VPN connections >
Basics
Settings
Tags
Review + create
Create
Previous
Next
Download a template for automation

Create connection ...

Validation passed

Basics

Subscription	Pay-As-You-Go
Resource Group	Azure-Resource-Group-VI
Region	South India
Connection type	Site-to-site (IPsec)
Connection name	S2S-IPsec-1-VI

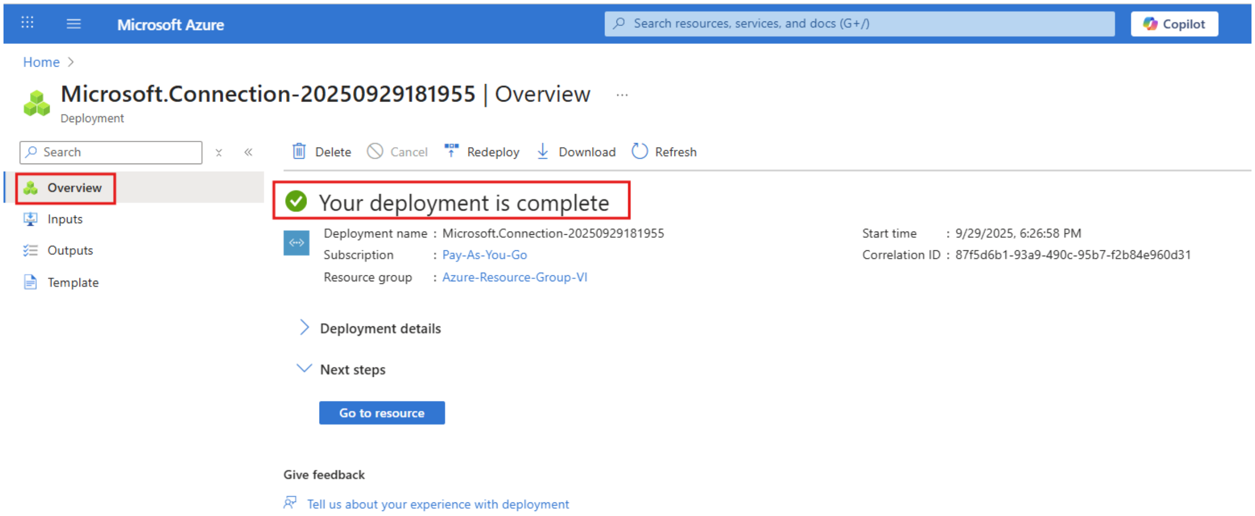
Settings

Virtual network gateway	VPN-GW-VI
Local network gateway	Local-NW-GW-VI
IKE Protocol	IKEv2
IPsec / IKE policy	Default
Use policy based traffic selector	Disable
DPD timeout in seconds	45
Connection Mode	Default
Primary Custom BGP Address	169.254.21.1
Shared Key(PSK)	1234

Tags

owner	vishnu

Deployment status can be viewed under “Overview” tab.



Microsoft.Connection-20250929181955 | Overview ...

Deployment

Your deployment is complete

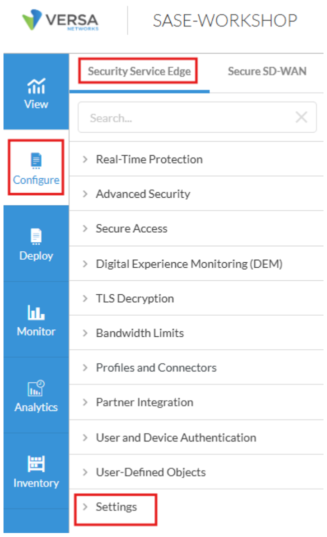
Deployment name : Microsoft.Connection-20250929181955
Subscription : Pay-As-You-Go
Resource group : Azure-Resource-Group-VI

Start time : 9/29/2025, 6:26:58 PM
Correlation ID : 87f5d6b1-93a9-490c-95b7-f2b84e960d31

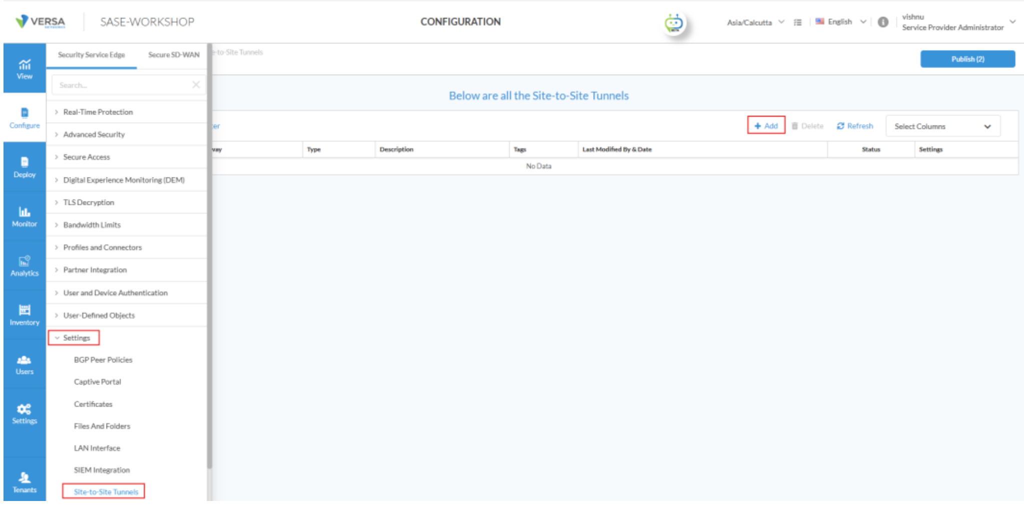
Versa SASE Gateway Configuration

Configure Site to Site Tunnels:

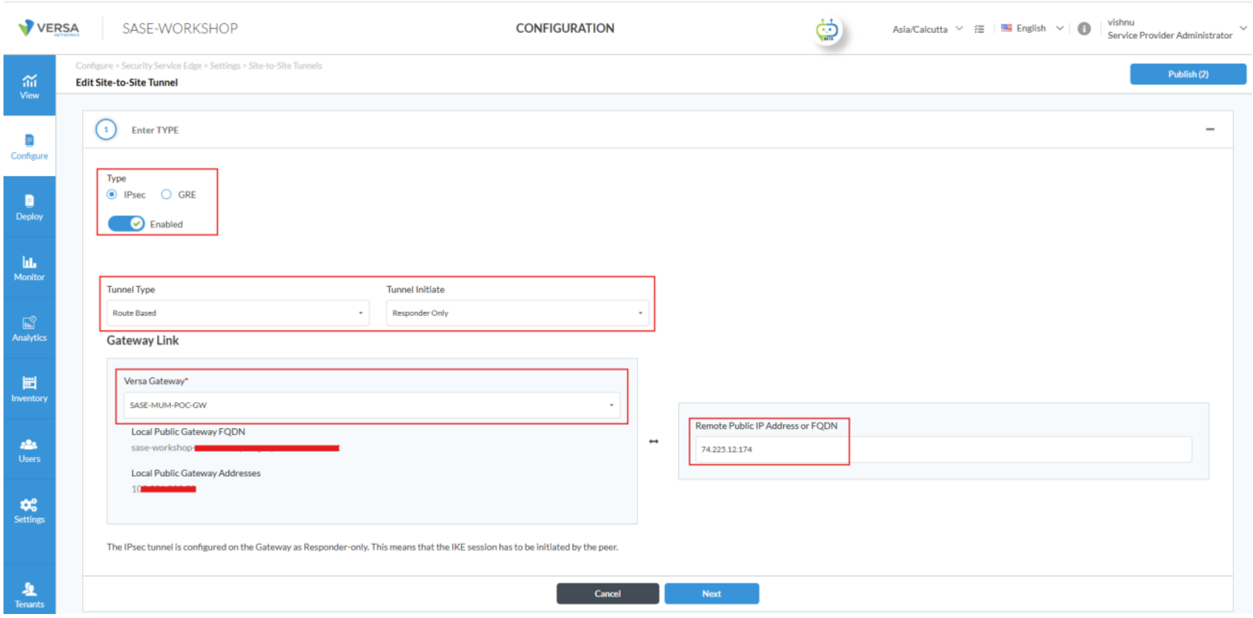
To Configure Site-to-Site Tunnels, Go to Configure →Secure Service Edge → Settings.



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 103.x.x.x, provide the Remote Public IP address.



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

Edit Site-to-Site Tunnel

1 Enter TYPE

Type
● IPsec ○ GRE
Enabled

Tunnel Type: Route Based
Tunnel Initiate: Responder Only

Gateway Link

Versa Gateway*: SASE-MUM-POC-GW

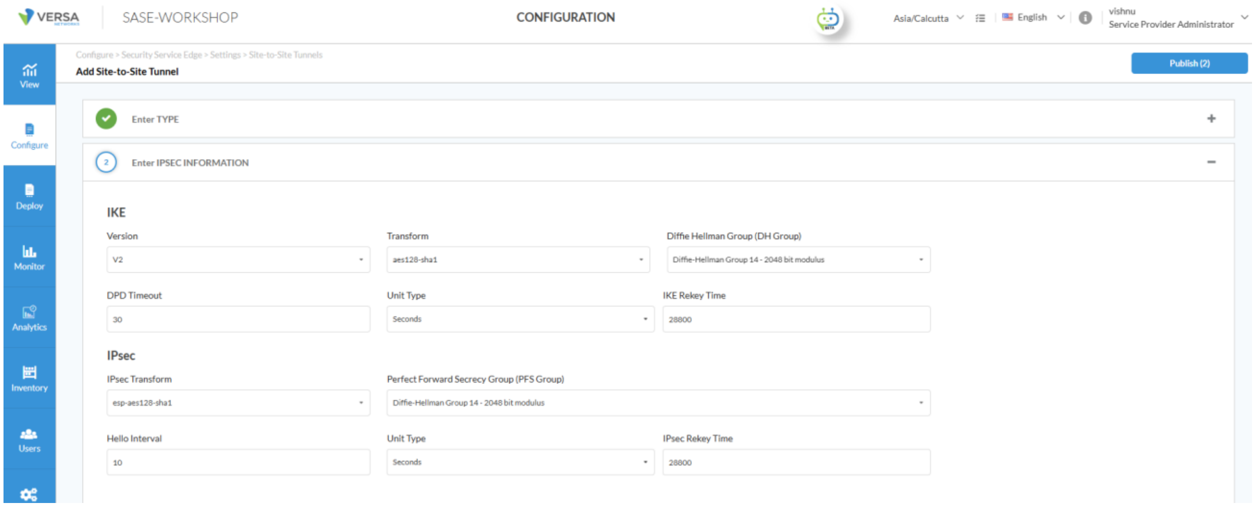
Local Public Gateway FQDN
sase-workshop[redacted]

Local Public Gateway Addresses
10[redacted]

Remote Public IP Address or FQDN: 74.225.12.174

The IPsec tunnel is configured on the Gateway as Responder-only. This means that the IKE session has to be initiated by the peer.

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

✓ Enter TYPE

2 Enter IPSEC INFORMATION

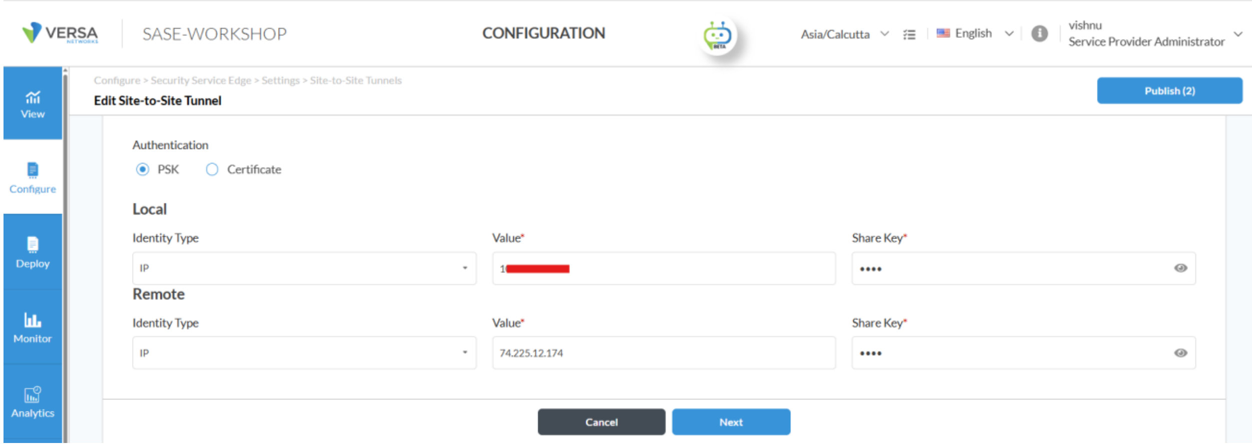
IKE

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

Edit Site-to-Site Tunnel

Authentication

● PSK ○ Certificate

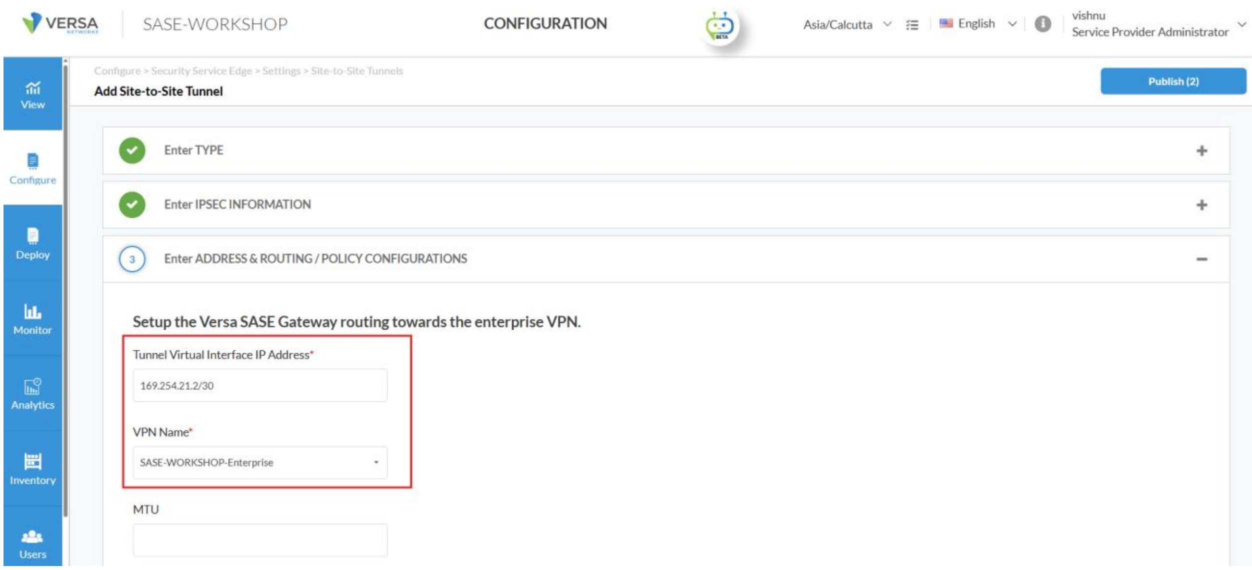
Local

Identity Type	Value*	Share Key*
IP	1[redacted]	••••

Remote

Identity Type	Value*	Share Key*
IP	74.225.12.174	••••

Under "Tunnel Virtual interface IP Address" provide the IP's generated by Azure 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

Enter TYPE

Enter IPSEC INFORMATION

3 Enter ADDRESS & ROUTING / POLICY CONFIGURATIONS

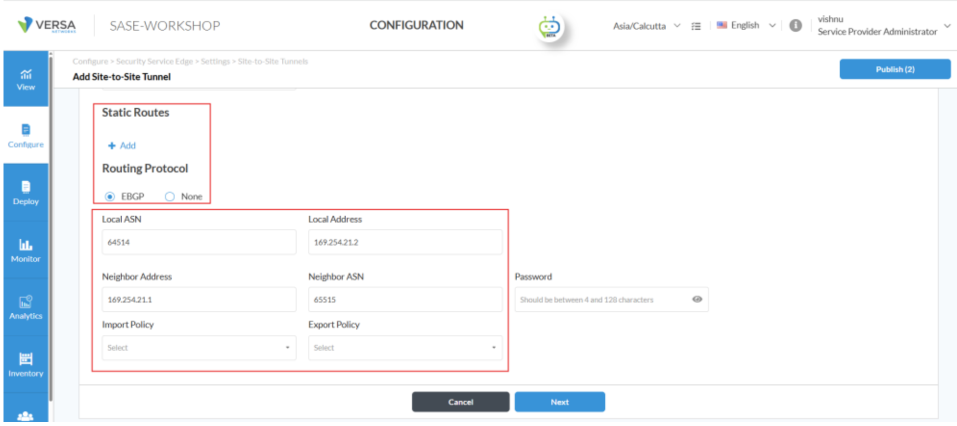
Setup the Versa SASE Gateway routing towards the enterprise VPN.

Tunnel Virtual Interface IP Address*: 169.254.21.2/30

VPN Name*: SASE-WORKSHOP-Enterprise

MTU

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



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

Add Site-to-Site Tunnel

Static Routes

+ Add

Routing Protocol

● EBGP ○ None

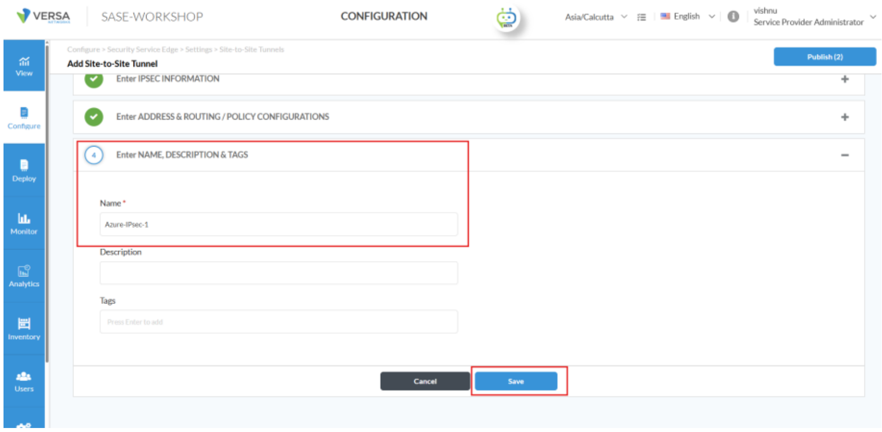
Local ASN	Local Address	
64514	169.254.21.2	
Neighbor Address	**Neighbor ASN**	**Password**
169.254.21.1	65515	Should be between 4 and 128 characters
Import Policy	**Export Policy**	
Select	Select	

Local ASN	64514

Local Address	169.254.21.2
Remote ASN	65515
Neighbor Address	169.254.21.1

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

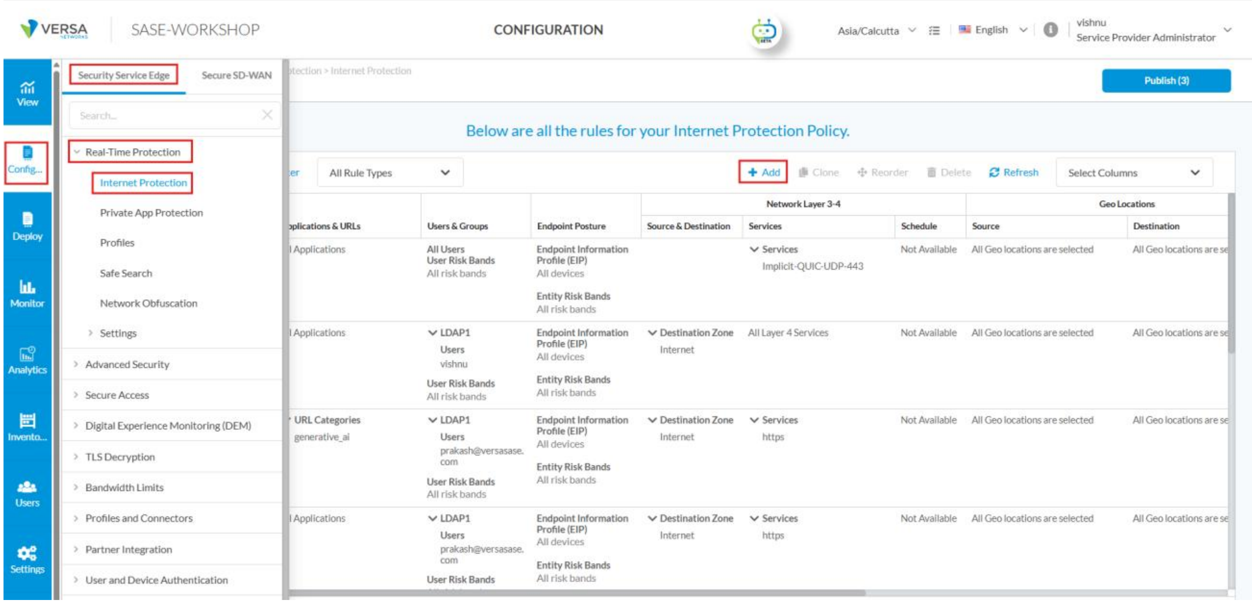
Under “Enter NAME, DESCRIPTION & TAGS” provide the Name to the IPSec tunnel and Save the configuration.



Name * Azure-IPsec-1

Configuring Secure Access Rule:

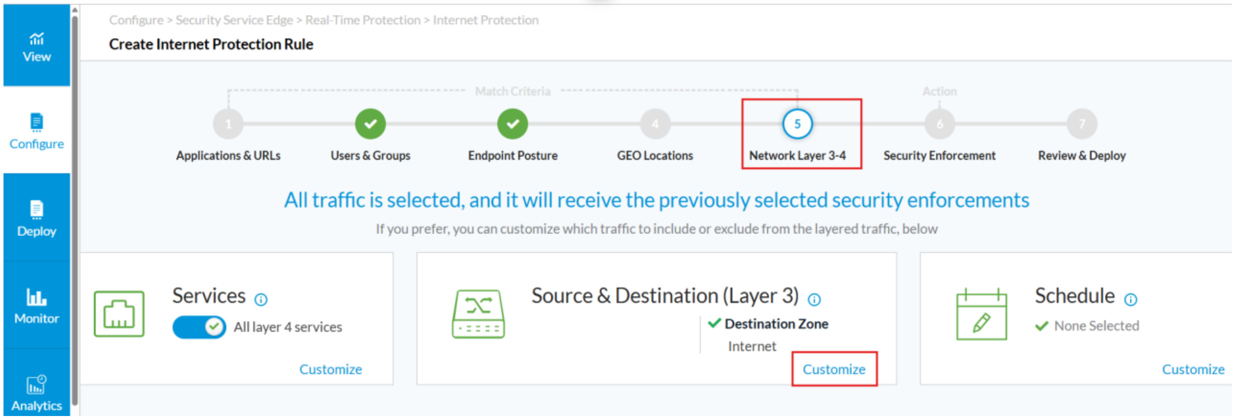
To Create a secure access rule for allowing traffic from SASE clients to AWS EC2 through IPSec tunnels, Go to Configure → Secure Service Edge → Real-Time Protection → Internet Protection and click on “Add”.



Below are all the rules for your Internet Protection Policy.

			Network Layer 3-4			Geo Locations	
plications & URLs	Users & Groups	Endpoint Posture	Source & Destination	Services	Schedule	Source	Destination
l Applications	All Users User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands		Services Implicit-QUIC-UDP-443	Not Available	All Geo locations are selected	All Geo locations are se
l Applications	LDAP1 Users vishnu User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Destination Zone Internet	All Layer 4 Services	Not Available	All Geo locations are selected	All Geo locations are se
URL Categories generative_ai	LDAP1 Users prakash@versasase.com User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Destination Zone Internet	Services https	Not Available	All Geo locations are selected	All Geo locations are se
l Applications	LDAP1 Users prakash@versasase.com User Risk Bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Destination Zone Internet	Services https	Not Available	All Geo locations are selected	All Geo locations are se

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



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

Create Internet Protection Rule

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

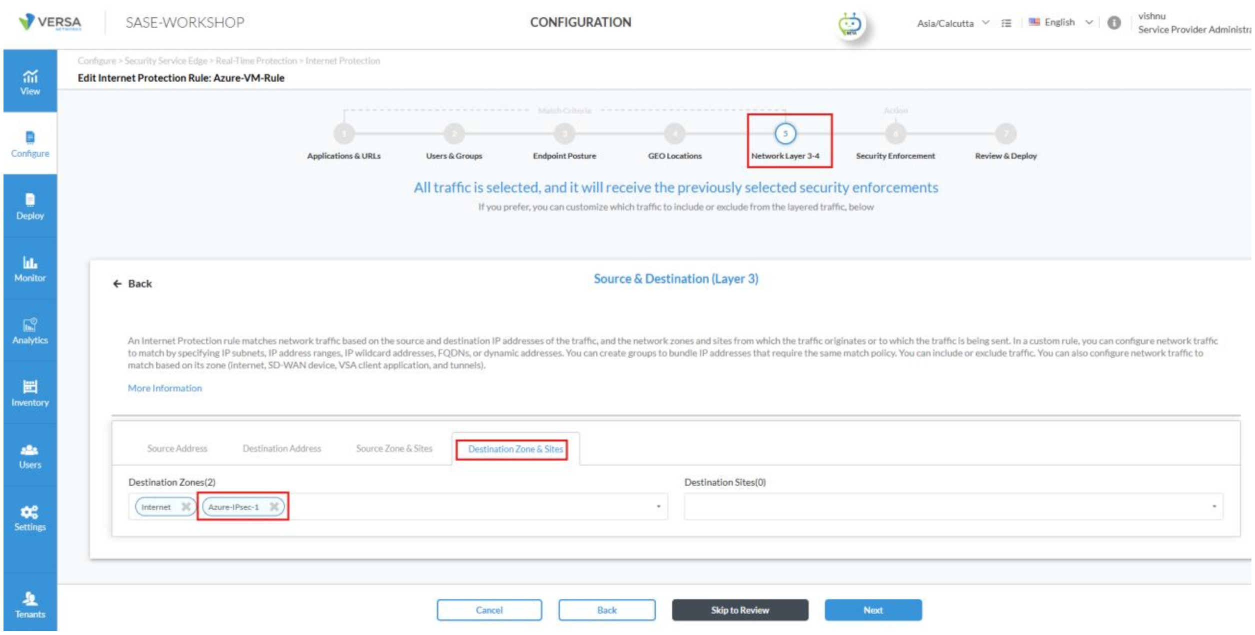
If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

Services: All layer 4 services — Customize

Source & Destination (Layer 3): ✓ Destination Zone Internet — Customize

Schedule: ✓ None Selected — Customize

Under “Destination Zone & Sites” configure “Azure-IPsec-1”.



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

Edit Internet Protection Rule: Azure-VM-Rule

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

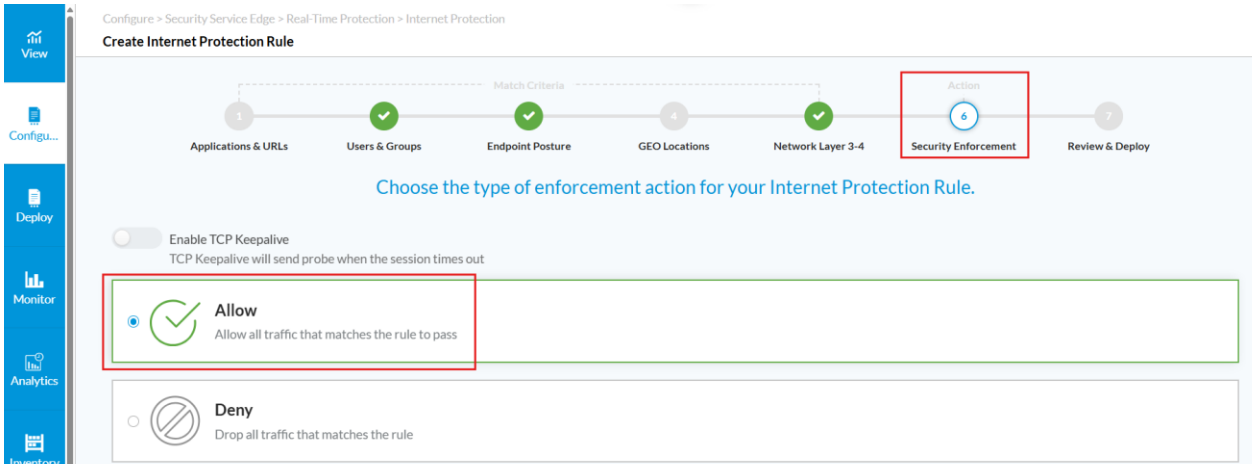
Source & Destination (Layer 3)

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(2): Internet, Azure-IPsec-1

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

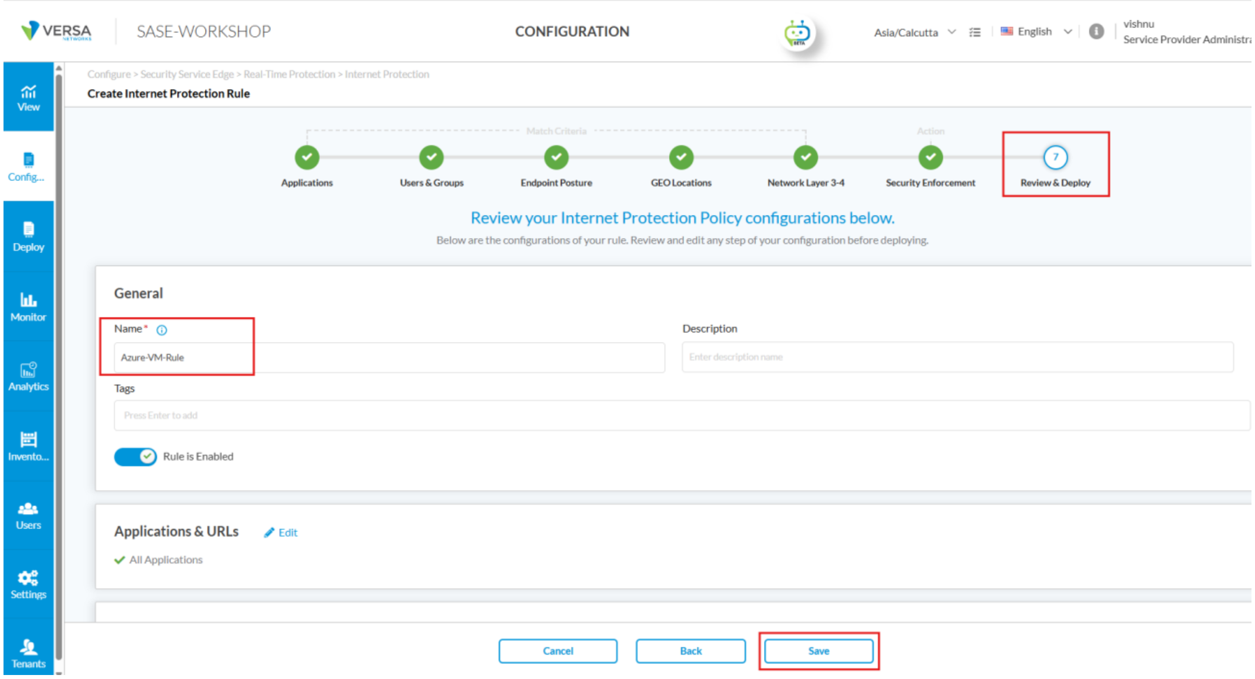
Allow all traffic that matches the rule to pass

○ 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.



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*: Azure-VM-Rule

Description: Enter description name

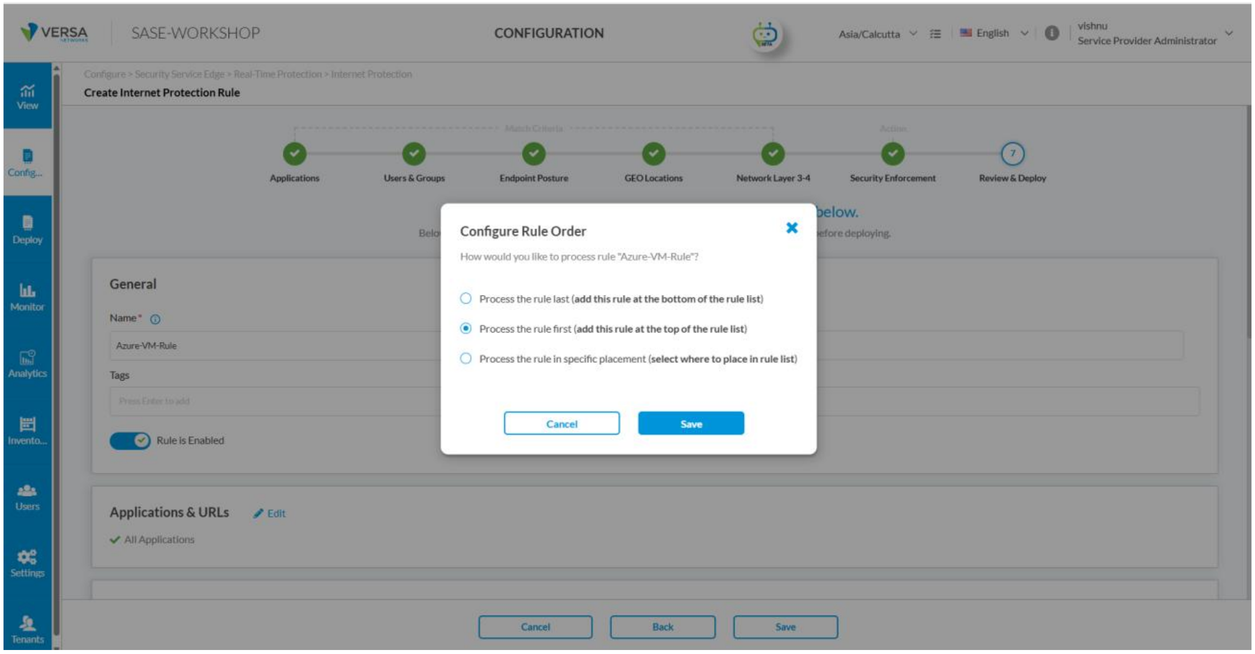
Tags: Press Enter to add

Rule is Enabled

Applications & URLs

✓ All Applications

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



Configure Rule Order

How would you like to process rule "Azure-VM-Rule"?

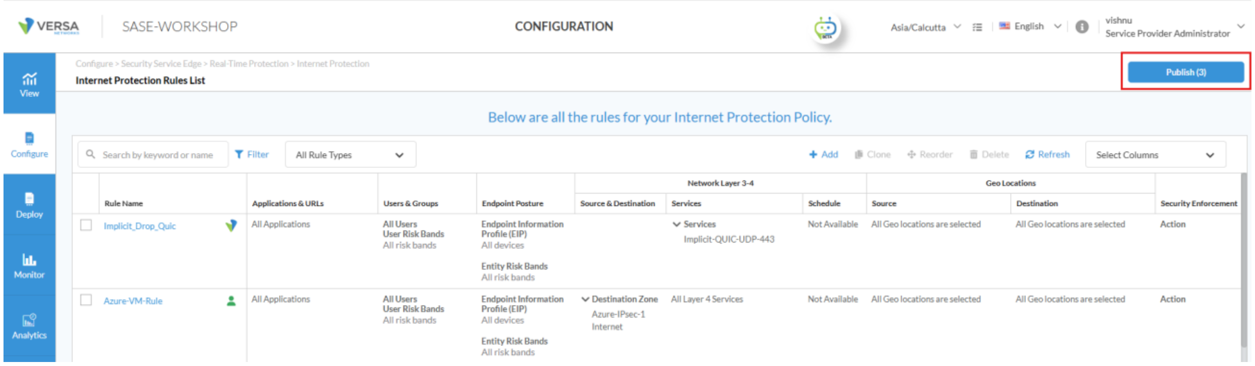
○ Process the rule last (**add this rule at the bottom of the rule list**)

● 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.



Internet Protection Rules List

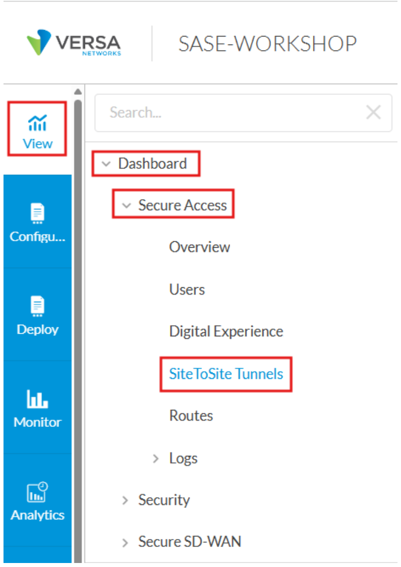
Below are all the rules for your Internet Protection Policy.

				Network Layer 3-4			Geo Locations		
Rule Name	Applications & URLs	Users & Groups	Endpoint Posture	Source & Destination	Services	Schedule	Source	Destination	Security Enforcement
Implicit_Drop_Quic	All Applications	All Users User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands		Services Implicit-QUIC-UDP-443	Not Available	All Geo locations are selected	All Geo locations are selected	Action
Azure-VM-Rule	All Applications	All Users User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Destination Zone Azure-IPsec-1 Internet	All Layer 4 Services	Not Available	All Geo locations are selected	All Geo locations are selected	Action

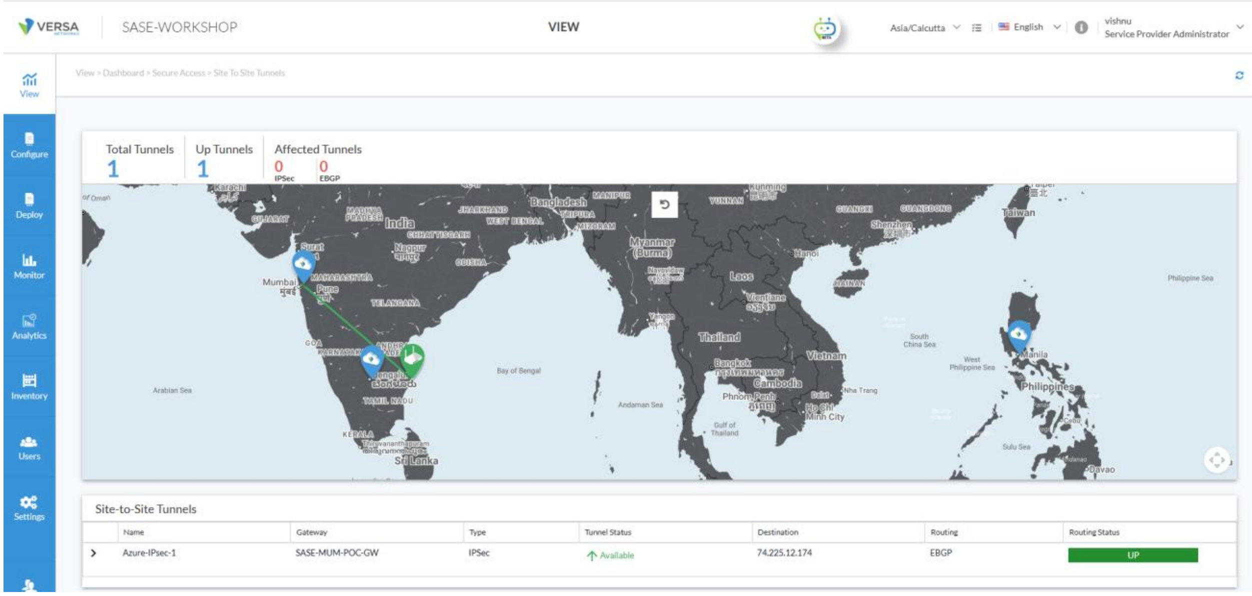
Verification

Verifying BGP and IPsec on SASE GW:

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



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



VERSA | SASE-WORKSHOP | VIEW | Asia/Calcutta | English | vishnu Service Provider Administrator

View > Dashboard > Secure Access > Site To Site Tunnels

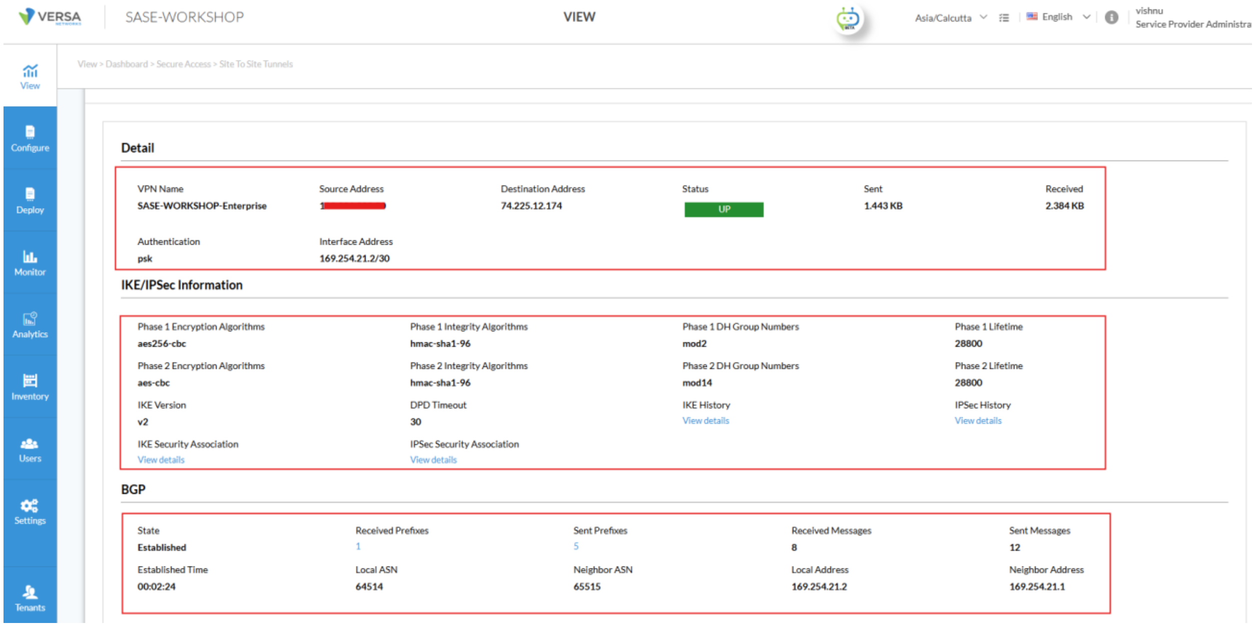
Total Tunnels	Up Tunnels	Affected Tunnels	
1	1	0 IPSec	0 EBGP

Site-to-Site Tunnels

	Name	Gateway	Type	Tunnel Status	Destination	Routing	Routing Status
>	Azure-IPsec-1	SASE-MUM-POC-GW	IPSec	↑ Available	74.225.12.174	EBGP	UP

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

Azure-IPsec-1:



VERSA | SASE-WORKSHOP | VIEW | Asia/Calcutta | English | vishnu Service Provider Administra

View > Dashboard > Secure Access > Site To Site Tunnels

Detail

VPN Name	Source Address	Destination Address	Status	Sent	Received
SASE-WORKSHOP-Enterprise	[redacted]	74.225.12.174	UP	1.443 KB	2.384 KB
Authentication	Interface Address				
psk	169.254.21.2/30				

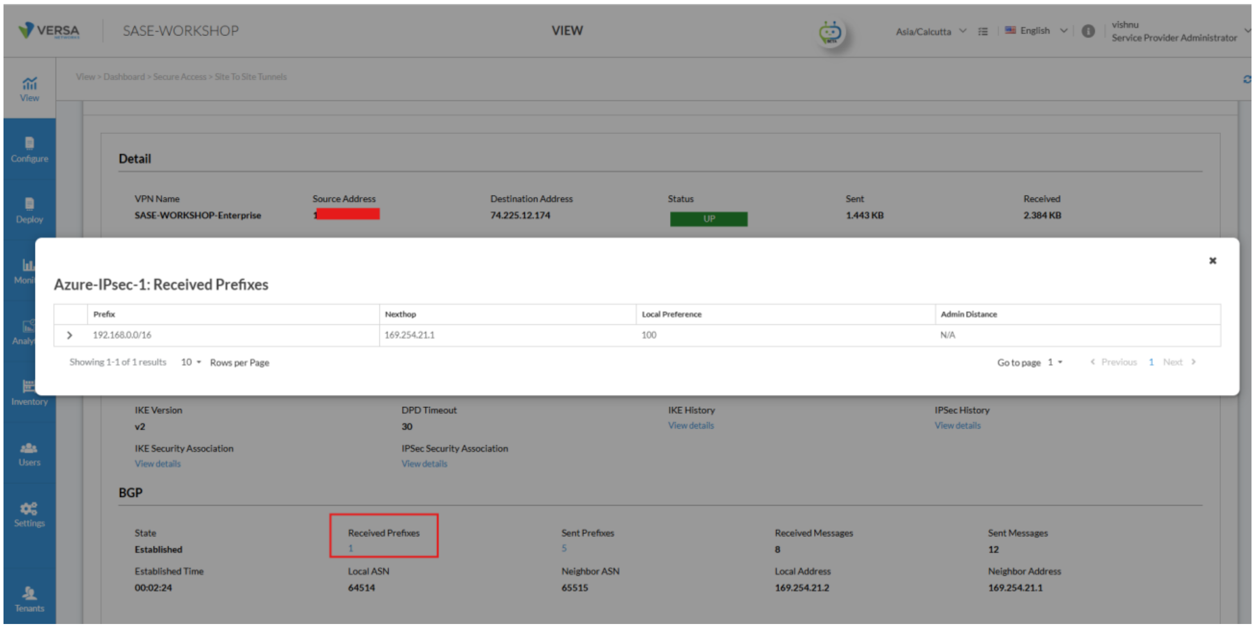
IKE/IPSec Information

Phase 1 Encryption Algorithms	Phase 1 Integrity Algorithms	Phase 1 DH Group Numbers	Phase 1 Lifetime
aes256-cbc	hmac-sha1-96	mod2	28800
Phase 2 Encryption Algorithms	Phase 2 Integrity Algorithms	Phase 2 DH Group Numbers	Phase 2 Lifetime
aes-cbc	hmac-sha1-96	mod14	28800
IKE Version	DPD Timeout	IKE History	IPSec History
v2	30	View details	View details
IKE Security Association	IPSec Security Association		
View details	View details		

BGP

State	Received Prefixes	Sent Prefixes	Received Messages	Sent Messages
Established	1	5	8	12
Established Time	Local ASN	Neighbor ASN	Local Address	Neighbor Address
00:02:24	64514	65515	169.254.21.2	169.254.21.1

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



Detail

VPN Name	Source Address	Destination Address	Status	Sent	Received
SASE-WORKSHOP-Enterprise	[redacted]	74.225.12.174	UP	1.443 KB	2.384 KB

Azure-IPsec-1: Received Prefixes

	Prefix	Nexthop	Local Preference	Admin Distance
>	192.168.0.0/16	169.254.21.1	100	N/A

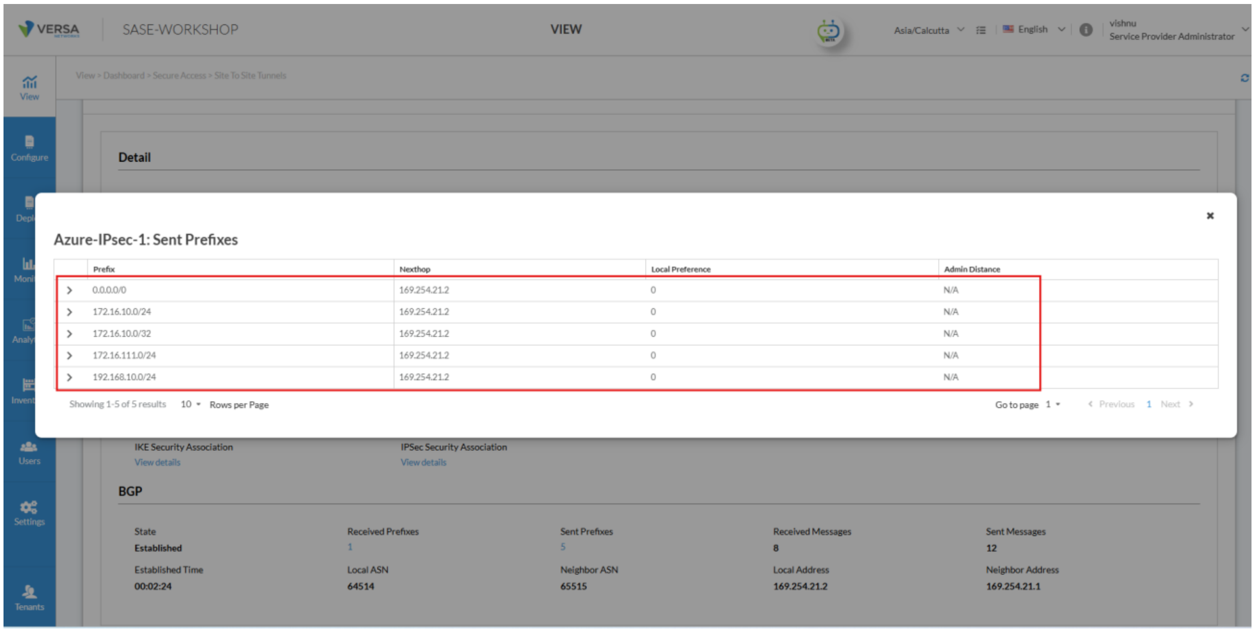
Showing 1-1 of 1 results 10 ▾ Rows per Page Go to page 1 ▾ ‹ Previous 1 Next ›

IKE Version	DPD Timeout	IKE History	IPSec History
v2	30	View details	View details

IKE Security Association	IPSec Security Association
View details	View details

BGP

State	Received Prefixes	Sent Prefixes	Received Messages	Sent Messages
Established	1	5	8	12
Established Time	**Local ASN**	**Neighbor ASN**	**Local Address**	**Neighbor Address**
00:02:24	64514	65515	169.254.21.2	169.254.21.1



Detail

Azure-IPsec-1: Sent Prefixes

	Prefix	Nexthop	Local Preference	Admin Distance
>	0.0.0.0/0	169.254.21.2	0	N/A
>	172.16.10.0/24	169.254.21.2	0	N/A
>	172.16.10.0/32	169.254.21.2	0	N/A
>	172.16.111.0/24	169.254.21.2	0	N/A
>	192.168.10.0/24	169.254.21.2	0	N/A

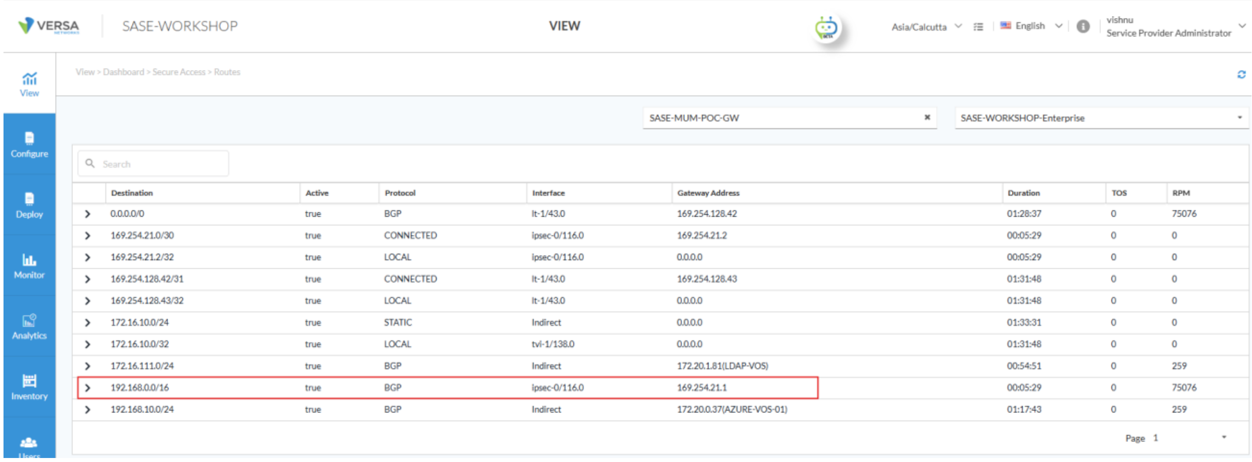
Showing 1-5 of 5 results 10 ▾ Rows per Page Go to page 1 ▾ ‹ Previous 1 Next ›

IKE Security Association	IPSec Security Association
View details	View details

BGP

State	Received Prefixes	Sent Prefixes	Received Messages	Sent Messages
Established	1	5	8	12
Established Time	**Local ASN**	**Neighbor ASN**	**Local Address**	**Neighbor Address**
00:02:24	64514	65515	169.254.21.2	169.254.21.1

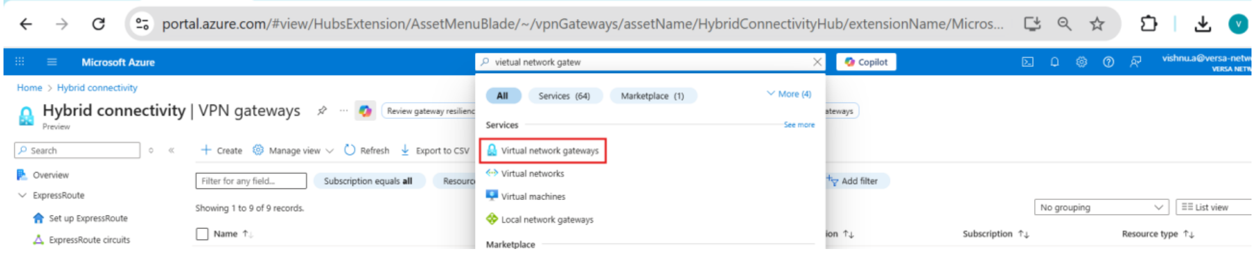
Routing Table on SASE-GW can be viewed from “View” → Dashboard → Secure Access → Routes.



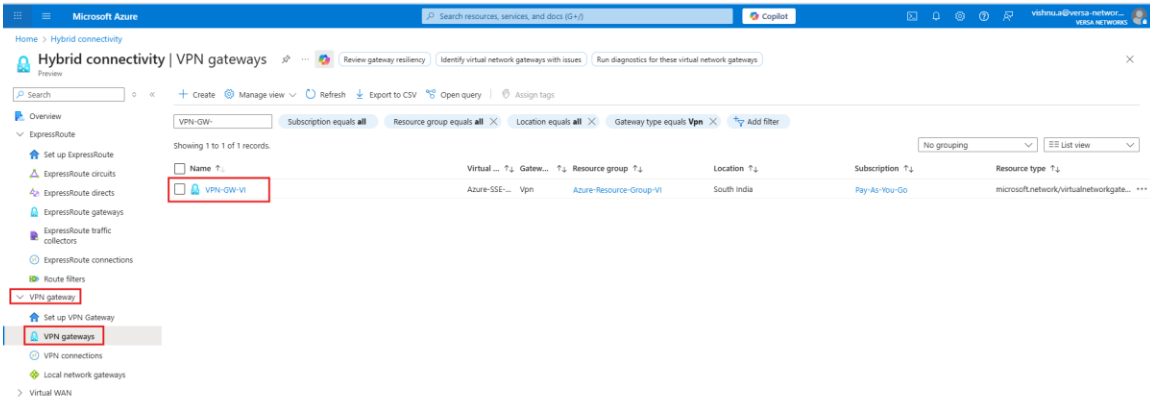
Destination	Active	Protocol	Interface	Gateway Address	Duration	TOS	RPM
0.0.0.0/0	true	BGP	lt-1/43.0	169.254.128.42	01:28:37	0	75076
169.254.21.0/30	true	CONNECTED	ipsec-0/116.0	169.254.21.2	00:05:29	0	0
169.254.21.2/32	true	LOCAL	ipsec-0/116.0	0.0.0.0	00:05:29	0	0
169.254.128.42/31	true	CONNECTED	lt-1/43.0	169.254.128.43	01:31:48	0	0
169.254.128.43/32	true	LOCAL	lt-1/43.0	0.0.0.0	01:31:48	0	0
172.16.10.0/24	true	STATIC	Indirect	0.0.0.0	01:33:31	0	0
172.16.10.0/32	true	LOCAL	tvi-1/138.0	0.0.0.0	01:31:48	0	0
172.16.111.0/24	true	BGP	Indirect	172.20.1.81(LDAP-VOS)	00:54:51	0	259
192.168.0.0/16	true	BGP	ipsec-0/116.0	169.254.21.1	00:05:29	0	75076
192.168.10.0/24	true	BGP	Indirect	172.20.0.37(AZURE-VOS-01)	01:17:43	0	259

Verify the BGP status on Azure:

To verify the BGP status and the IPsec Connections on Azure, in the search bar type Virtual network gateways and select Virtual network gateways under Services.

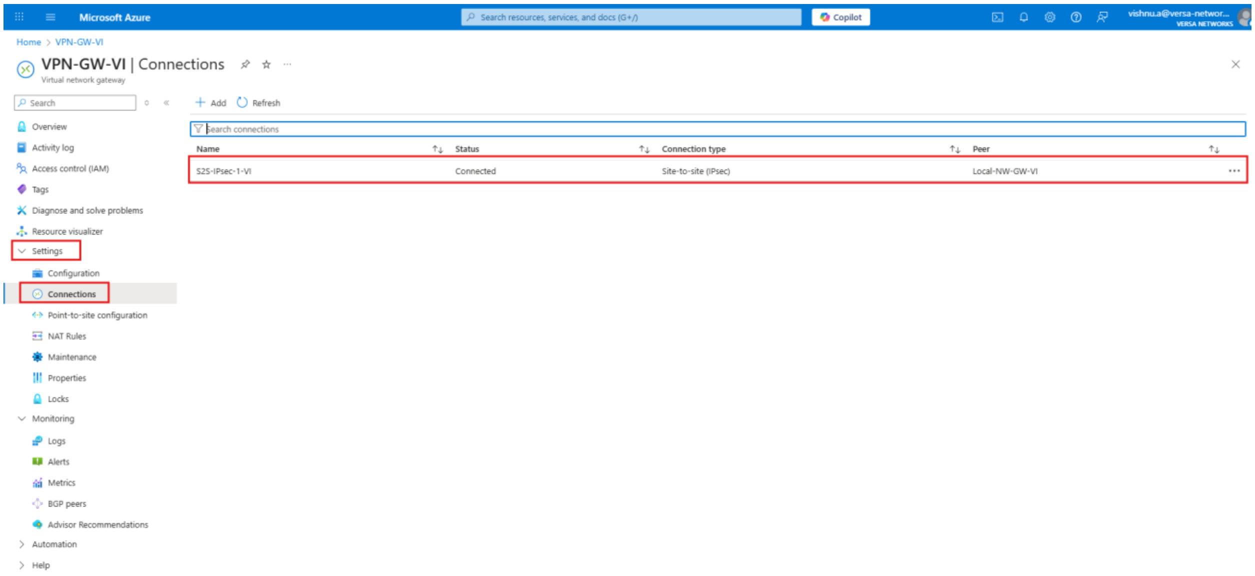


Under VPN gateway go to VPN gateways and select your VPN Gateway.



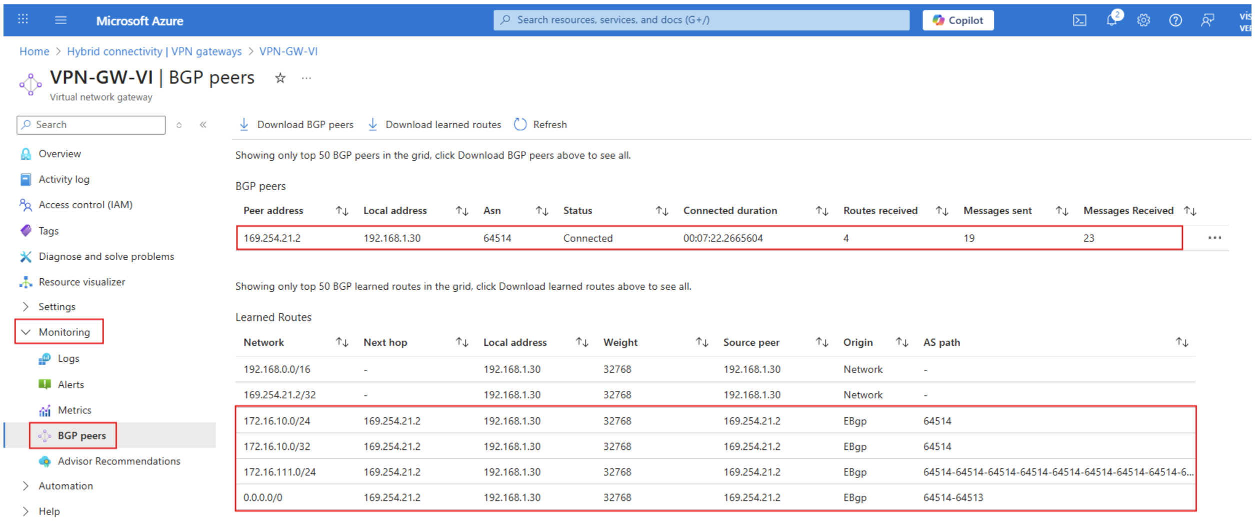
Name	Virtual ...	Gatew...	Resource group	Location	Subscription	Resource type
VPN-GW-VI	Azure-SSE-...	Vpn	Azure-Resource-Group-VI	South India	Pay-As-You-Go	microsoft.network/virtualnetworkgate...

To Verify IPsec connection, Under VPN gateway → Settings → Connections, you should see the Status as Connected.



Name	Status	Connection type	Peer
S2S-IPsec-1-VI	Connected	Site-to-site (IPsec)	Local-NW-GW-VI

To Verify BGP Under VPN gateway → Monitoring →BGP peers, you should be able to see the BGP peers and the Routes learned.



Showing only top 50 BGP peers in the grid, click Download BGP peers above to see all.

BGP peers

Peer address	Local address	Asn	Status	Connected duration	Routes received	Messages sent	Messages Received
169.254.21.2	192.168.1.30	64514	Connected	00:07:22.2665604	4	19	23

Showing only top 50 BGP learned routes in the grid, click Download learned routes above to see all.

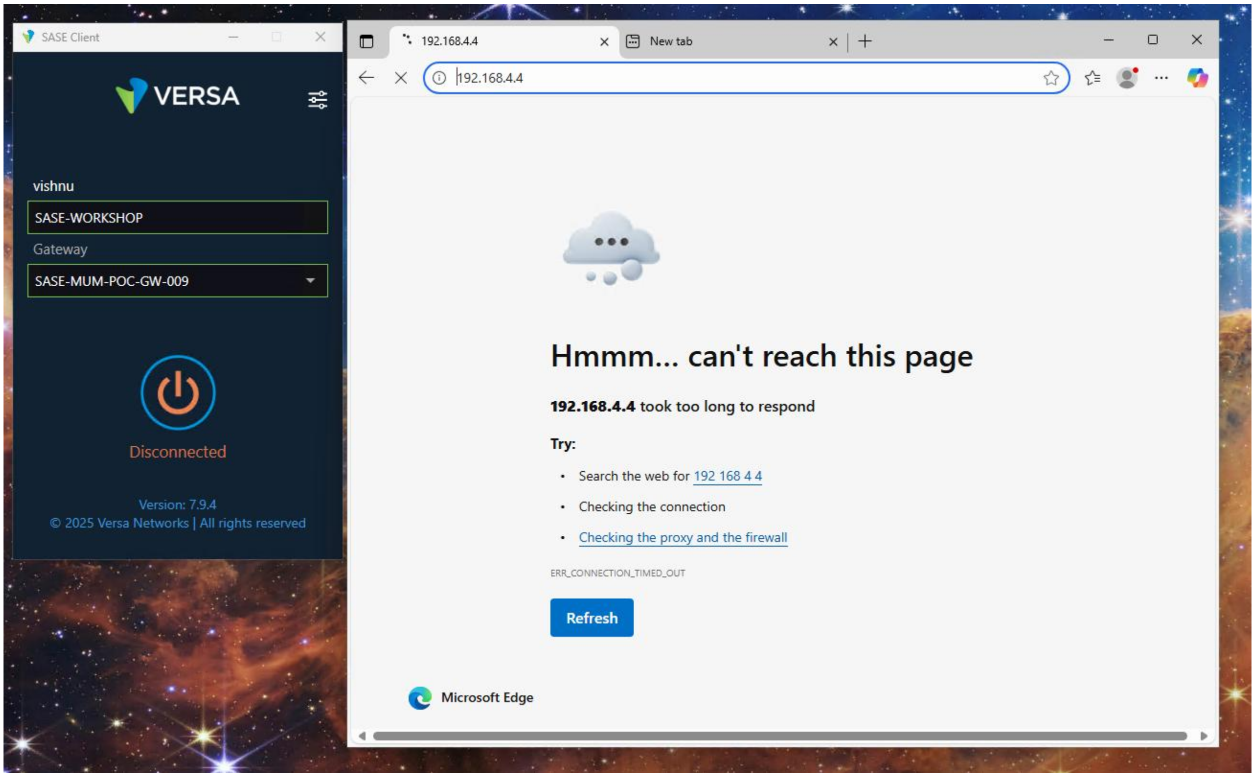
Learned Routes

Network	Next hop	Local address	Weight	Source peer	Origin	AS path
192.168.0.0/16	-	192.168.1.30	32768	192.168.1.30	Network	-
169.254.21.2/32	-	192.168.1.30	32768	192.168.1.30	Network	-
172.16.10.0/24	169.254.21.2	192.168.1.30	32768	169.254.21.2	EBgp	64514
172.16.10.0/32	169.254.21.2	192.168.1.30	32768	169.254.21.2	EBgp	64514
172.16.111.0/24	169.254.21.2	192.168.1.30	32768	169.254.21.2	EBgp	64514-64514-64514-64514-64514-64514-64514-64514-6...
0.0.0.0/0	169.254.21.2	192.168.1.30	32768	169.254.21.2	EBgp	64514-64513

Verifying connectivity:

Accessing Azure Virtual Machine instance with IP: 192.168.4.4 from Remote PC.

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



vishnu

SASE-WORKSHOP

Gateway

SASE-MUM-POC-GW-009

Disconnected

Version: 7.9.4

© 2025 Versa Networks | All rights reserved

Hmmm… can't reach this page

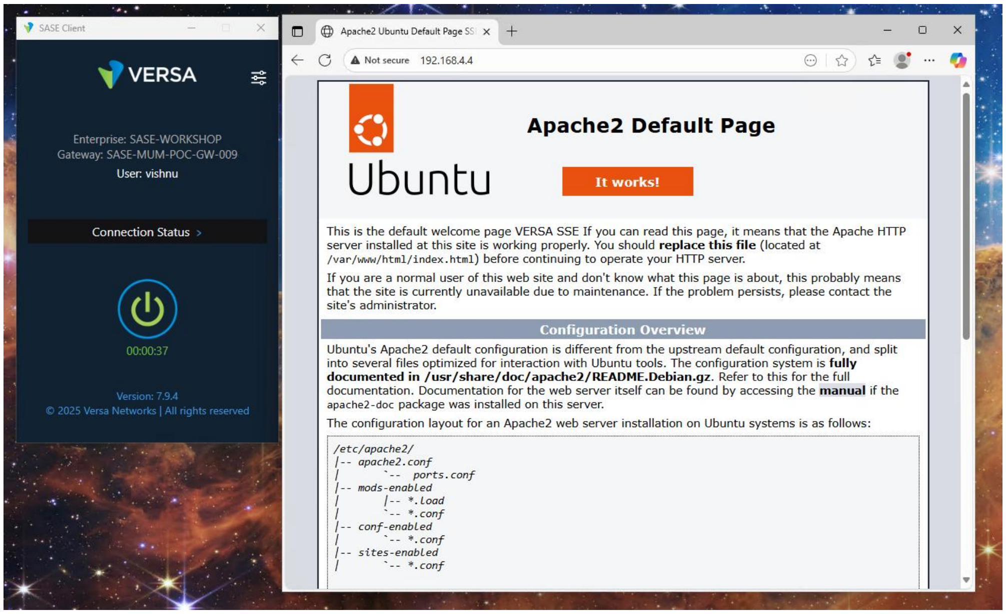
192.168.4.4 took too long to respond

Try:

- Search the web for 192 168 4 4
- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_TIMED_OUT

When the SASE Client is connected to the Gateway we were able to reach the Azure VM instance over Private IP.



Enterprise: SASE-WORKSHOP
Gateway: SASE-MUM-POC-GW-009
User: vishnu

00:00:37

Version: 7.9.4

© 2025 Versa Networks | All rights reserved

Apache2 Default Page

This is the default welcome page VERSA SSE If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) 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 means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

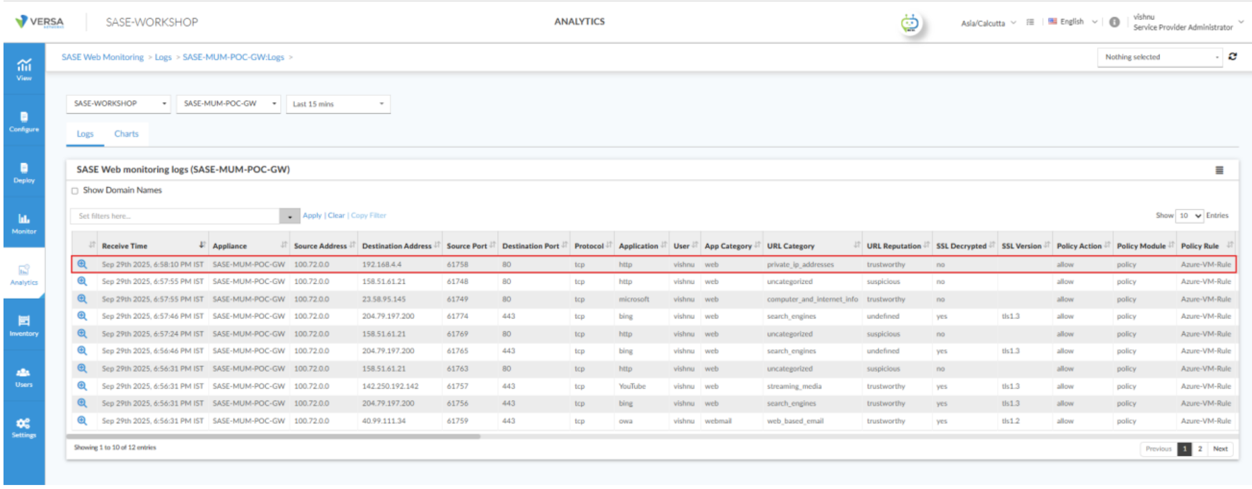
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

SASE-WEB LOGS on Analytics:

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



SASE-WORKSHOP ANALYTICS

Asia/Calcutta | English | vishnu Service Provider Administrator

SASE Web Monitoring > Logs > SASE-MUM-POC-GW:Logs >

Nothing selected

SASE-WORKSHOP | SASE-MUM-POC-GW | Last 15 mins

Logs | Charts

SASE Web monitoring logs (SASE-MUM-POC-GW)

□ Show Domain Names

Set filters here... Apply | Clear | Copy Filter

Show 10 Entries

	Receive Time	Appliance	Source Address	Destination Address	Source Port	Destination Port	Protocol	Application	User	App Category	URL Category	URL Reputation	SSL Decrypted	SSL Version	Policy Action	Policy Module	Policy Rule
	Sep 29th 2025, 6:58:10 PM IST	SASE-MUM-POC-GW	100.72.0.0	192.168.4.4	61758	80	tcp	http	vishnu	web	private_ip_addresses	trustworthy	no		allow	policy	Azure-VM-Rule
	Sep 29th 2025, 6:57:55 PM IST	SASE-MUM-POC-GW	100.72.0.0	158.51.61.21	61748	80	tcp	http	vishnu	web	uncategorized	suspicious	no		allow	policy	Azure-VM-Rule
	Sep 29th 2025, 6:57:55 PM IST	SASE-MUM-POC-GW	100.72.0.0	23.58.95.145	61749	80	tcp	microsoft	vishnu	web	computer_and_internet_info	trustworthy	no		allow	policy	Azure-VM-Rule
	Sep 29th 2025, 6:57:46 PM IST	SASE-MUM-POC-GW	100.72.0.0	204.79.197.200	61774	443	tcp	bing	vishnu	web	search_engines	undefined	yes	tls1.3	allow	policy	Azure-VM-Rule
	Sep 29th 2025, 6:57:24 PM IST	SASE-MUM-POC-GW	100.72.0.0	158.51.61.21	61769	80	tcp	http	vishnu	web	uncategorized	suspicious	no		allow	policy	Azure-VM-Rule
	Sep 29th 2025, 6:56:46 PM IST	SASE-MUM-POC-GW	100.72.0.0	204.79.197.200	61765	443	tcp	bing	vishnu	web	search_engines	undefined	yes	tls1.3	allow	policy	Azure-VM-Rule
	Sep 29th 2025, 6:56:31 PM IST	SASE-MUM-POC-GW	100.72.0.0	158.51.61.21	61763	80	tcp	http	vishnu	web	uncategorized	suspicious	no		allow	policy	Azure-VM-Rule
	Sep 29th 2025, 6:56:31 PM IST	SASE-MUM-POC-GW	100.72.0.0	142.250.192.142	61757	443	tcp	YouTube	vishnu	web	streaming_media	trustworthy	yes	tls1.3	allow	policy	Azure-VM-Rule
	Sep 29th 2025, 6:56:31 PM IST	SASE-MUM-POC-GW	100.72.0.0	204.79.197.200	61756	443	tcp	bing	vishnu	web	search_engines	trustworthy	yes	tls1.3	allow	policy	Azure-VM-Rule
	Sep 29th 2025, 6:56:31 PM IST	SASE-MUM-POC-GW	100.72.0.0	40.99.111.34	61759	443	tcp	owa	vishnu	webmail	web_based_email	trustworthy	yes	tls1.2	allow	policy	Azure-VM-Rule

Showing 1 to 10 of 12 entries

Previous 1 2 Next

Option 2: Azure VPN Integration with Versa SASE Gateway using Virtual WAN

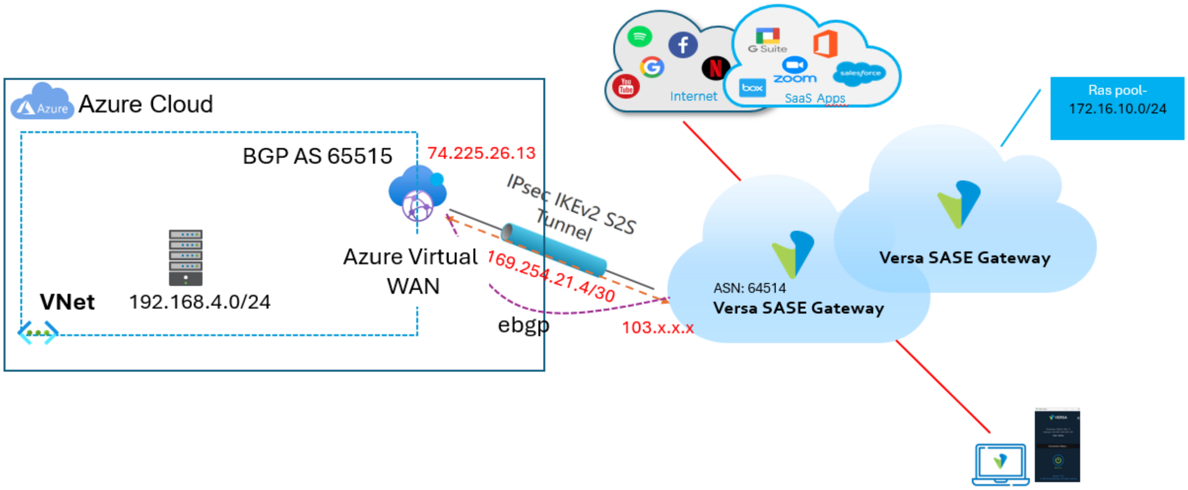
Concept: Establish IPsec between Azure vWAN hub and SASE Gateway.

In this scenario, a site-to-site IPsec VPN is established between the SASE Gateway and Azure Virtual WAN (vWAN). The VNets are connected to the vWAN through Virtual WAN hubs, and dynamic route exchange is performed over the IPsec connection using eBGP between the SASE Gateway and the Azure vWAN hub.

This option is used when you need to connect the SASE Gateway to multiple VNets or regions with centralized routing and a scalable network architecture.

Use Cases: SD-WAN, branch connectivity, centralized management.

Key Components: Azure Virtual WAN, Azure Virtual Hub, Azure VPN site, SASE gateway.



Prerequisites:

- Azure Subscription: Active subscription
- Resource Group: For VPN components.
- Versa SASE Gateway IP: Public IP address.
- On-Premises Network Details: Address spaces behind Versa SASE.

High Level Steps:

Step 1: Create a Virtual WAN.
Step 2: Create a Virtual Hub within Virtual WAN.
Step 3: Create a VPN site within Virtual WAN.
Step 4: Connect the VPN site.
Step 5: Versa Configuration.
Step 6: Validation of the IPsec tunnel and BGP status.

Azure Configuration:

Creating Virtal WAN:

Azure Virtual WAN is Microsoft's managed global transit network service that provides large-scale branch, site-to-site, and remote-user connectivity through a unified architecture. It simplifies deployment of secure, high-performance connections between on-premises locations, Azure regions, and remote users by centralizing routing, encryption, and policy control in Microsoft's backbone.

Purpose of vWAN in This Scenario

In the Versa SASE integration, Azure vWAN acts as the central connectivity hub between the Versa SASE Gateway and multiple Azure Virtual Networks (VNets).

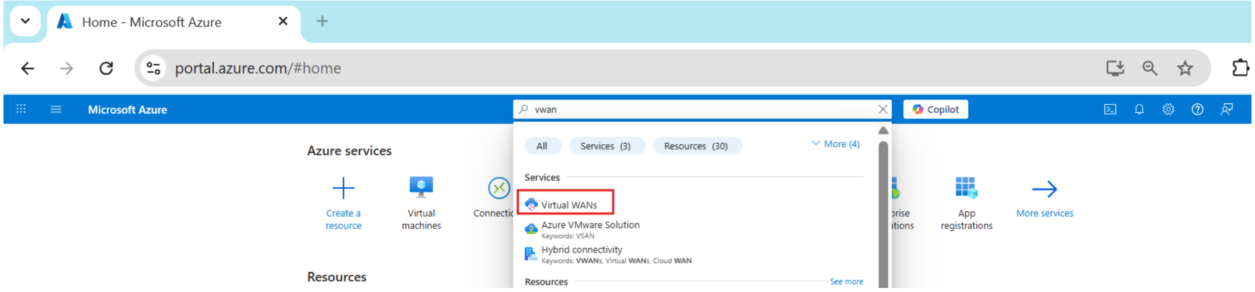
- The Versa SASE Gateway establishes a **site-to-site IPsec tunnel** to the vWAN hub.
- Dynamic routing is enabled through **eBGP** so that routes between the SASE fabric and all attached VNets are automatically exchanged.
- This eliminates the need to create individual VPN gateways for each VNet and provides a scalable, cloud-native backbone for branch-to-cloud traffic.

Key Use Cases for Azure vWAN

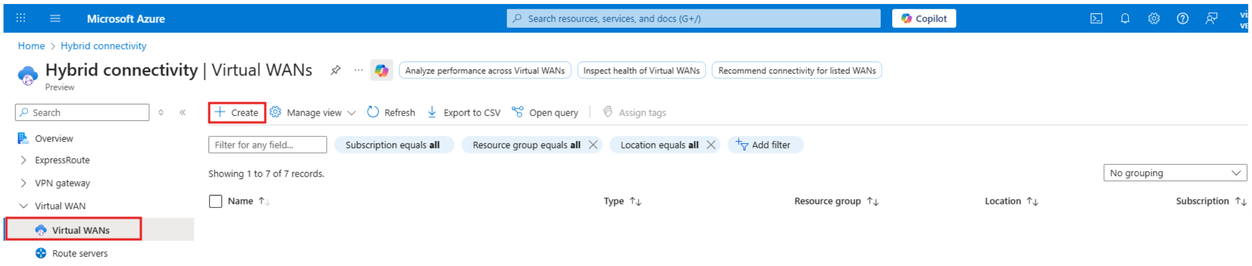
- **Global branch connectivity:** Seamlessly connect many branch offices or SD-WAN sites to Azure through a single, centrally managed hub.
- **SASE/SSE integration:** Provide a high-availability, low-latency connection point for third-party security clouds such as Versa SASE.
- **Hub-and-spoke multi-region design:** Centralize routing and security policies across multiple VNets and regions without complex peering.

- **Hybrid cloud and remote user access:** Support IPsec VPN, Point-to-Site, and ExpressRoute for flexible enterprise connectivity.

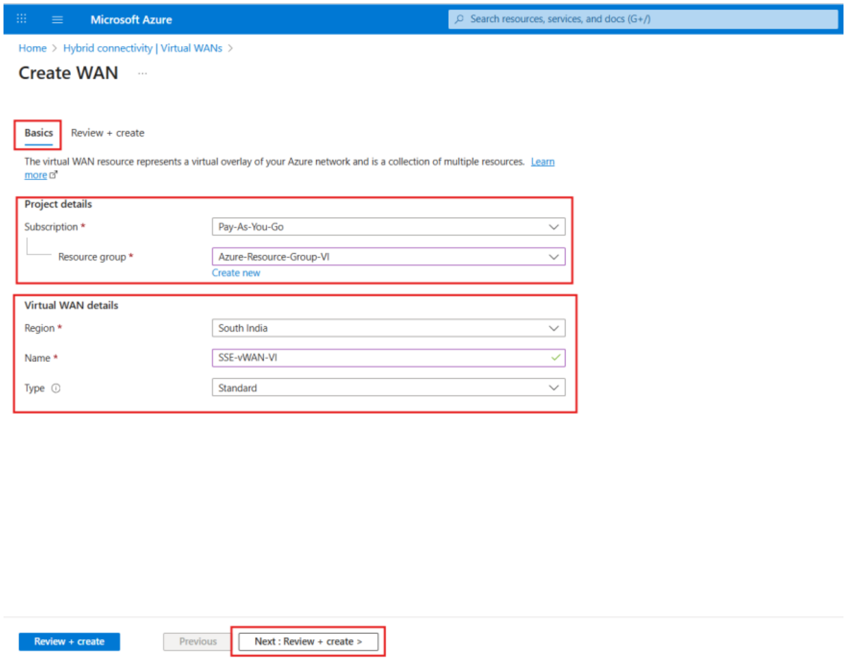
To create a Virtual WAN, search 'vWAN' → and select Virtual WANs under Services.



To create a new Virtual WAN click on "+Create".



When creating an Azure Virtual WAN, choose the subscription and an existing resource group, then select a resource location (for management only, as vWAN is global), provide a name, and set the type to Standard—required for advanced features beyond basic site-to-site connections(Can be configured as per the requirement) and click on "Next: Review+create>".



The virtual WAN resource represents a virtual overlay of your Azure network and is a collection of multiple resources. Learn more

Project details

Subscription * Pay-As-You-Go

Resource group * Azure-Resource-Group-VI

Create new

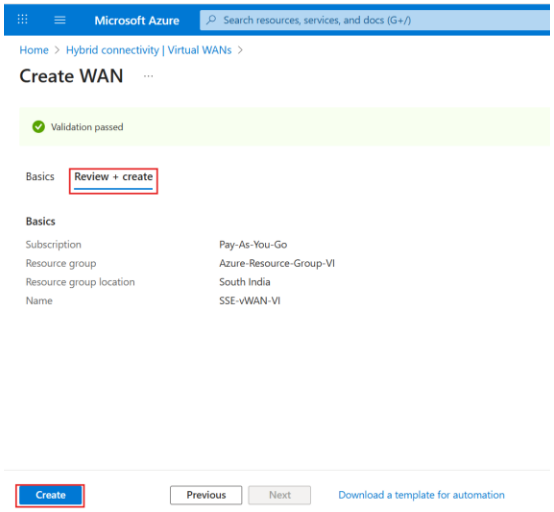
Virtual WAN details

Region * South India

Name * SSE-vWAN-VI

Type Standard

Under "Review+ create" tab click on Create.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Hybrid connectivity | Virtual WANs >
Basics
Review + create
Create
Previous
Next
Download a template for automation

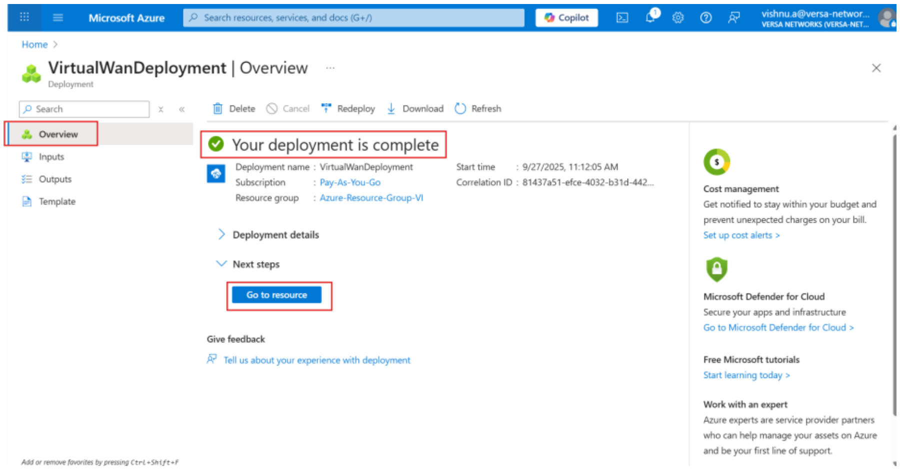
Create WAN

Validation passed

Basics

Subscription	Pay-As-You-Go
Resource group	Azure-Resource-Group-VI
Resource group location	South India
Name	SSE-vWAN-VI

Under Overview tab, you can view the status of the deployment. Once the deployment is complete click on “Go to resource”.



VirtualWanDeployment | Overview

Deployment

Your deployment is complete

Deployment name	: VirtualWanDeployment	Start time	: 9/27/2025, 11:12:05 AM
Subscription	: Pay-As-You-Go	Correlation ID	: 81437a51-efce-4032-b31d-442...
Resource group	: Azure-Resource-Group-VI		

Give feedback

Cost management
Get notified to stay within your budget and prevent unexpected charges on your bill.

Microsoft Defender for Cloud
Secure your apps and infrastructure

Free Microsoft tutorials

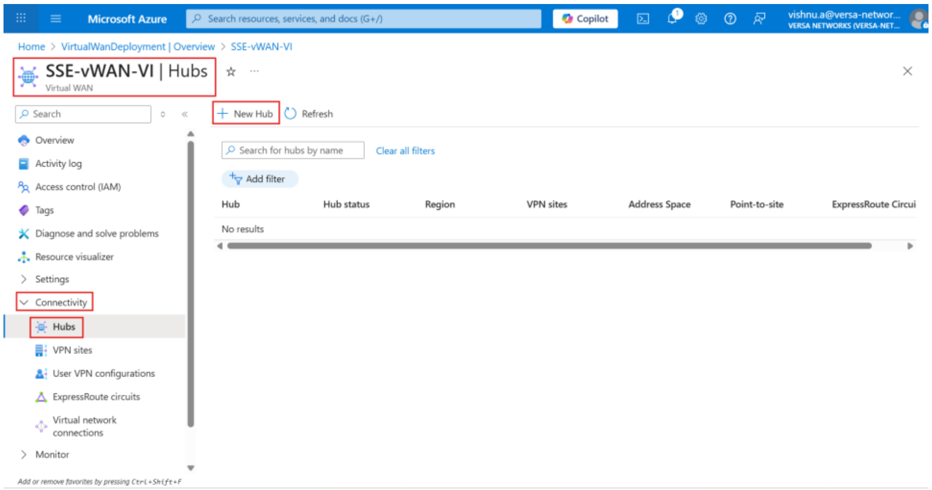
Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.

Creating Virtual Hub within vWAN

A virtual hub is a Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity from your on-premises network (vpnsite).

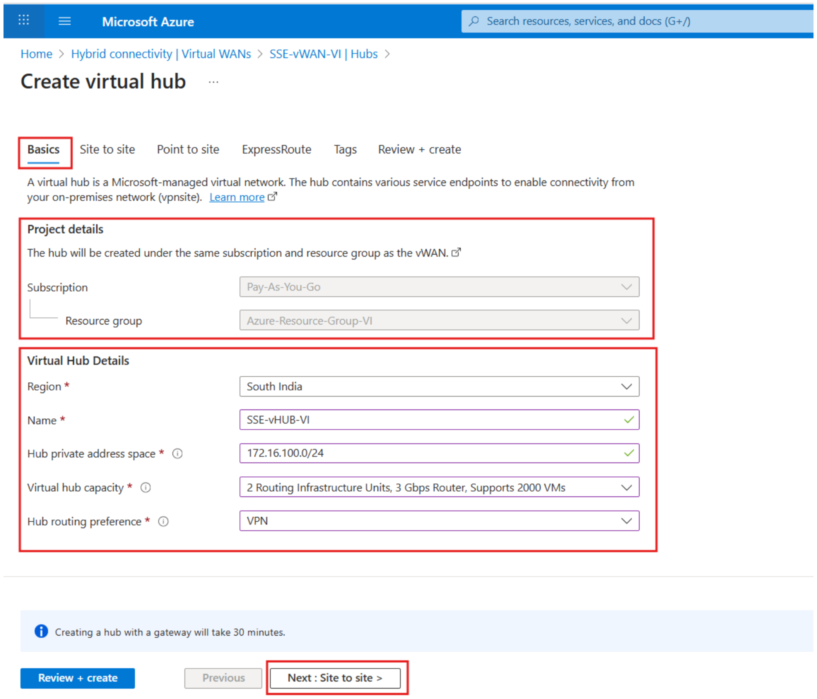
A Virtual WAN virtual hub connects to virtual networks (VNets) and on-premises using connectivity gateways, such as site-to-site (S2S) VPN gateway, ExpressRoute (ER) gateway, point-to-site (P2S) gateway, and SD-WAN Network Virtual Appliance (NVA).

To create a Virtual Hub within vWAN, Navigate to Connectivity → Hubs and click on “+New Hub”.



Hub	Hub status	Region	VPN sites	Address Space	Point-to-site	ExpressRoute Circui
No results						

When creating a Virtual Hub, select the deployment region and provide a name, specify a hub private address space (minimum /24), choose the hub capacity, and select the routing Preference as per your need.



Create virtual hub

A virtual hub is a Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity from your on-premises network (vpnsite). Learn more

Project details

The hub will be created under the same subscription and resource group as the vWAN.

Subscription	Pay-As-You-Go
Resource group	Azure-Resource-Group-VI

Virtual Hub Details

Region *	South India
Name *	SSE-vHUB-VI
Hub private address space *	172.16.100.0/24
Virtual hub capacity *	2 Routing Infrastructure Units, 3 Gbps Router, Supports 2000 VMs
Hub routing preference *	VPN

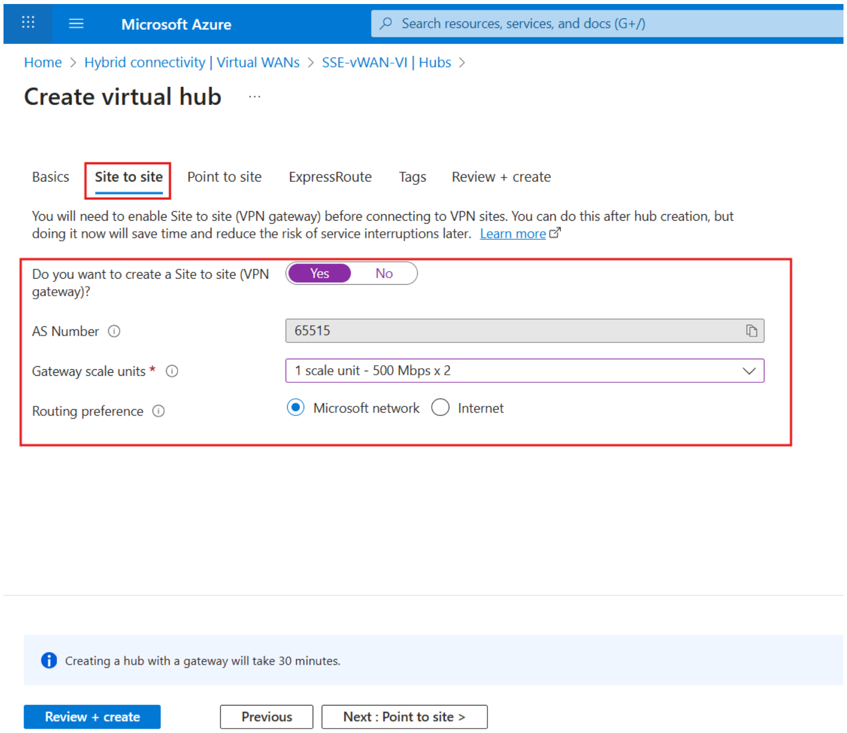
Creating a hub with a gateway will take 30 minutes.

Note:

The virtual hub router takes routing decisions using built-in route selection algorithm. To influence routing decisions in virtual hub router towards on-premises, we now have a new Virtual WAN hub feature called Hub routing preference (HRP). When a virtual hub router learns multiple routes across S2S VPN, ER and SD-WAN NVA connections for a destination route-prefix in on-premises, the virtual hub router's route selection algorithm adapts based on the hub routing preference configuration and selects the best routes.

Refer https://learn.microsoft.com/en-us/azure/virtual-wan/about-virtual-hub-routing-preference for more information.

Enable site to site and select the gateway scale units as customer preference, Routing preference and click Review+Create.



Create virtual hub

You will need to enable Site to site (VPN gateway) before connecting to VPN sites. You can do this after hub creation, but doing it now will save time and reduce the risk of service interruptions later. Learn more

Do you want to create a Site to site (VPN gateway)? [✓ Yes] No

AS Number: 65515

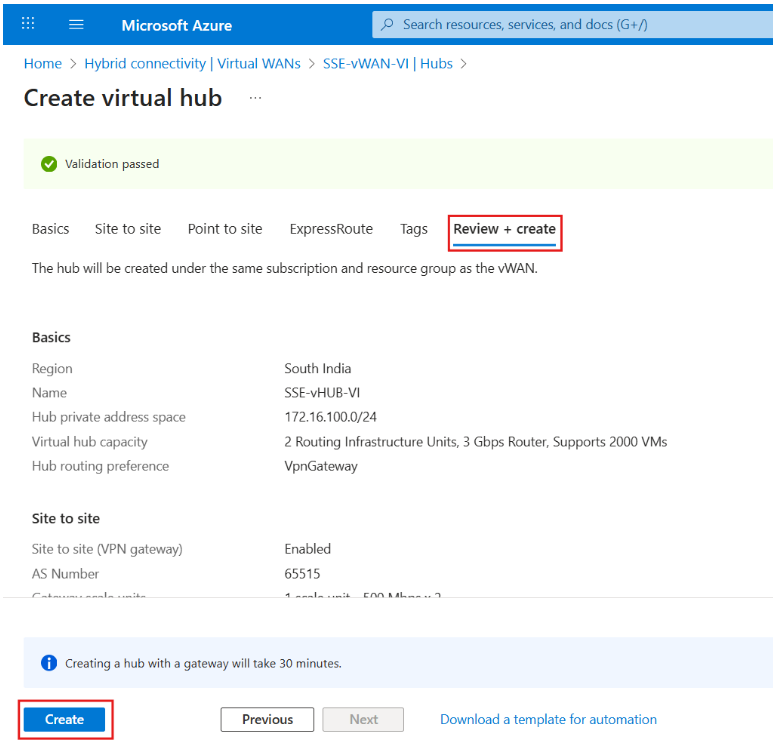
Gateway scale units *: 1 scale unit - 500 Mbps x 2

Routing preference: ● Microsoft network ○ Internet

Creating a hub with a gateway will take 30 minutes.

Note: Azure routing preference enables you to choose how your traffic routes between Azure and the Internet. You can choose to route traffic either via the Microsoft network, or, via the ISP network (public internet). These options are also referred to as cold potato routing and hot potato routing respectively. Egress data transfer price varies based on the routing selection. The public IP address in Virtual WAN is assigned by the service based on the routing option selected. For more information about routing preference via Microsoft network or ISP, please see https://docs.microsoft.com/azure/virtual-network/routing-preference-overview

Once the validation passed, click create.



Home > Hybrid connectivity | Virtual WANs > SSE-vWAN-VI | Hubs >

Create virtual hub

Validation passed

The hub will be created under the same subscription and resource group as the vWAN.

Basics

Region	South India
Name	SSE-vHUB-VI
Hub private address space	172.16.100.0/24
Virtual hub capacity	2 Routing Infrastructure Units, 3 Gbps Router, Supports 2000 VMs
Hub routing preference	VpnGateway

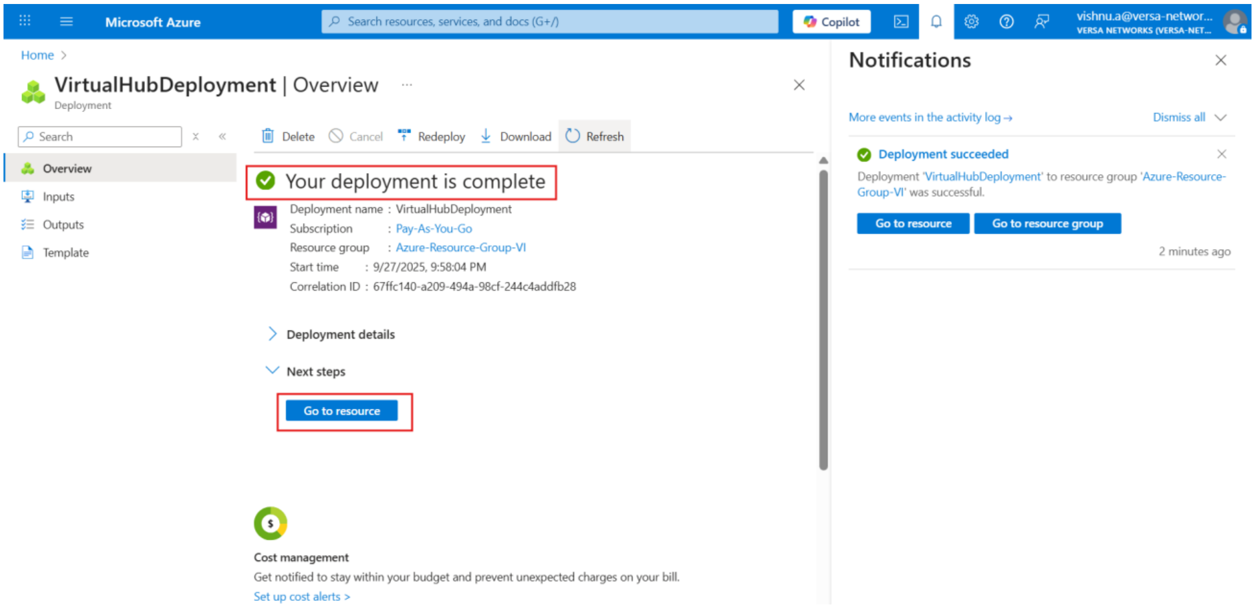
Site to site

Site to site (VPN gateway)	Enabled
AS Number	65515
Gateway scale units	1 scale unit - 500 Mbps x 2

Creating a hub with a gateway will take 30 minutes.

Note: Creating an Azure virtual hub without a gateway takes approximately 5 to 7 minutes, while creating one with a gateway (such as a site-to-site VPN or ExpressRoute gateway) can take up to 30 minutes.

Once the deployment is complete click on "Go to resource".



Home >

VirtualHubDeployment | Overview

Deployment

Your deployment is complete

Deployment name : VirtualHubDeployment
Subscription : Pay-As-You-Go
Resource group : Azure-Resource-Group-VI
Start time : 9/27/2025, 9:58:04 PM
Correlation ID : 67ffc140-a209-494a-98cf-244c4addfb28

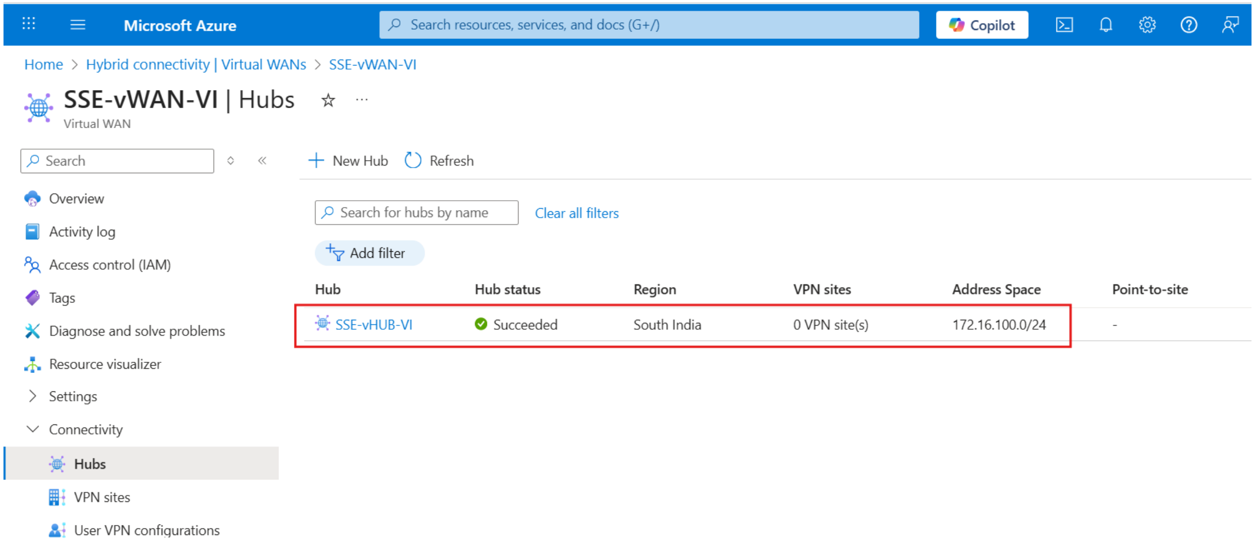
Cost management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >

Notifications

Deployment succeeded
Deployment 'VirtualHubDeployment' to resource group 'Azure-Resource-Group-VI' was successful.

2 minutes ago

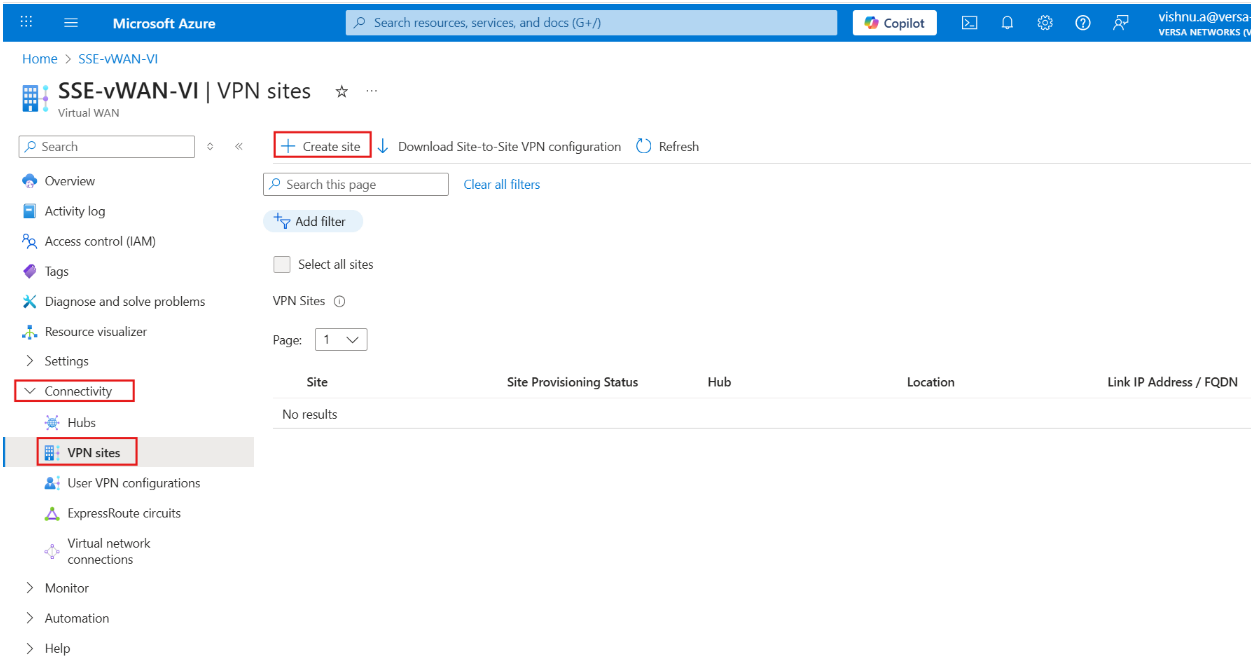
After deployment, under Connectivity → Hubs, we can see Hub status as succeeded.



Hub	Hub status	Region	VPN sites	Address Space	Point-to-site
SSE-vHUB-VI	Succeeded	South India	0 VPN site(s)	172.16.100.0/24	-

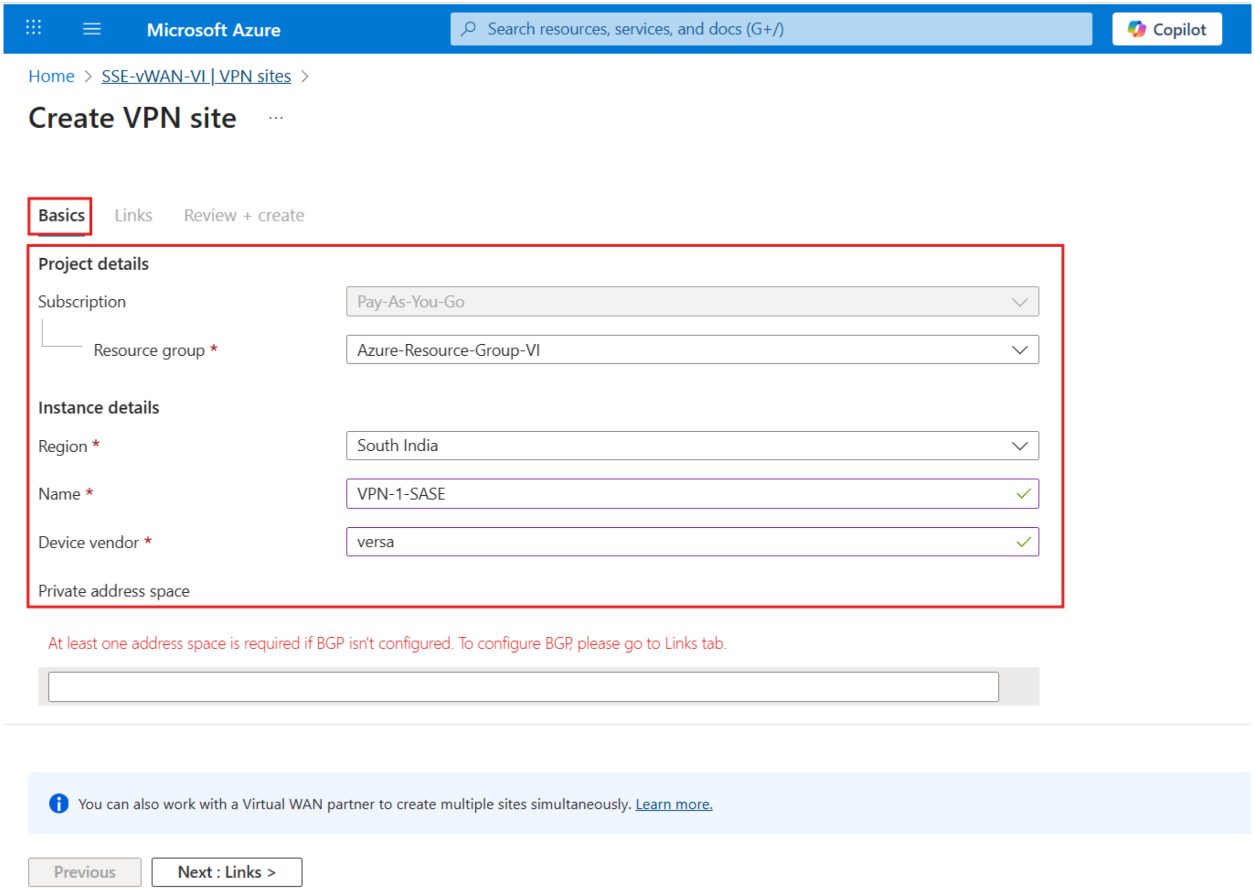
Creating a VPN site

To Create a VPN site within Virtual WAN. Navigate to Virtual WAN→ Connectivity →VPN Sites and click on “Create site”.



Site	Site Provisioning Status	Hub	Location	Link IP Address / FQDN
No results				

Fill in the details of Region, Name of the VPN and Device vendor and then click next.



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > SSE-vWAN-VI | VPN sites >

Create VPN site

Basics | Links | Review + create

Project details

Subscription	Pay-As-You-Go
Resource group *	Azure-Resource-Group-VI

Instance details

Region *	South India
Name *	VPN-1-SASE
Device vendor *	versa

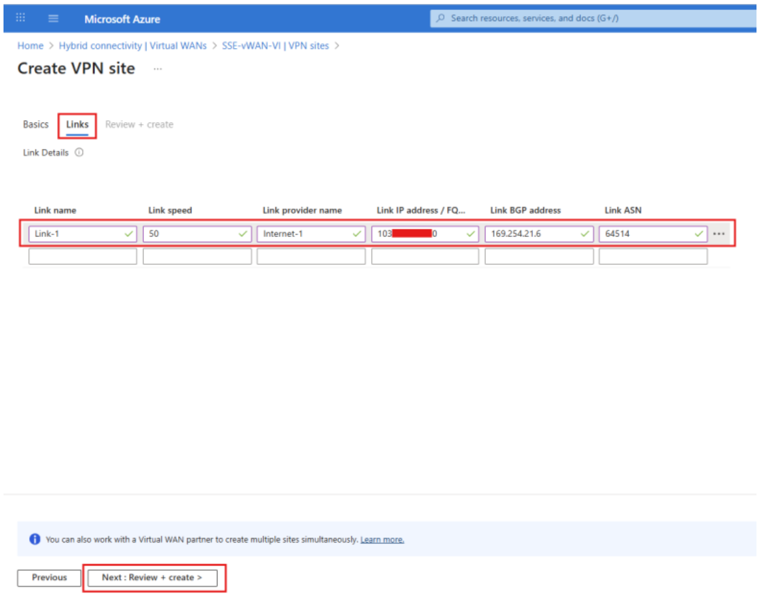
Private address space

At least one address space is required if BGP isn't configured. To configure BGP, please go to Links tab.

You can also work with a Virtual WAN partner to create multiple sites simultaneously. Learn more.

Provide a Link Name, its speed in Mbps, and the provider name (e.g., ATT or Verizon) for the branch VPN site, then specify the public IP or FQDN of the on-premises VPN device (IP takes precedence if both are given) under “Link IP address/FQDN”.

Under Link BGP Address provide a BGP IP of your VPN device and it should be different from public IP you specified and not part of site’s VNet address space—typically a loopback interface address. Under link ASN provide the AS Number of SASE GW.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Hybrid connectivity | Virtual WANs > SSE-vWAN-VI | VPN sites >
Basics
Links
Review + create
Previous
Next : Review + create >

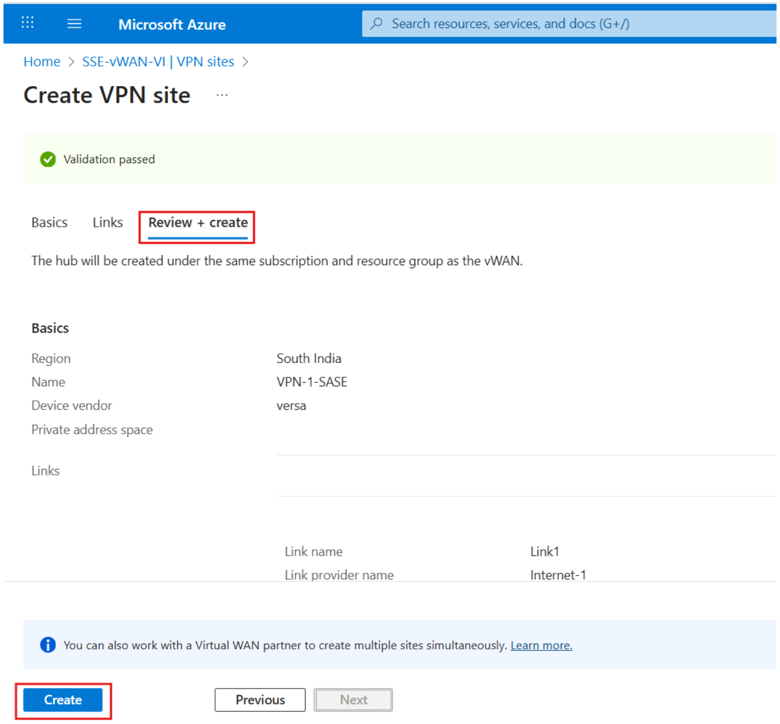
Create VPN site

Link Details

Link name	Link speed	Link provider name	Link IP address / FQ...	Link BGP address	Link ASN
Link-1	50	Internet-1	103[redacted]0	169.254.21.6	64514

You can also work with a Virtual WAN partner to create multiple sites simultaneously. Learn more.

Under “Review + create” click on Create once the validation is passed.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > SSE-vWAN-VI | VPN sites >
Basics
Links
Review + create
Create
Previous
Next

Create VPN site

Validation passed

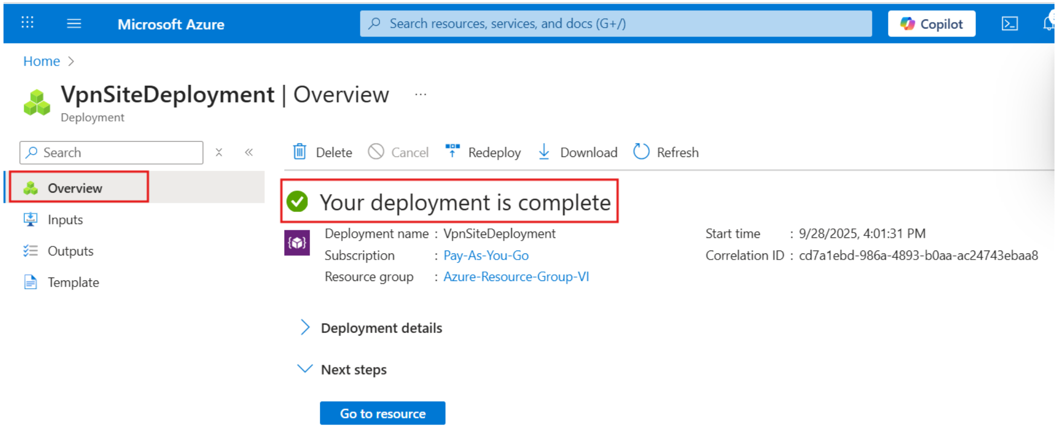
The hub will be created under the same subscription and resource group as the vWAN.

Basics

Region	South India
Name	VPN-1-SASE
Device vendor	versa
Private address space	
Links	
Link name	Link1
Link provider name	Internet-1

You can also work with a Virtual WAN partner to create multiple sites simultaneously. Learn more.

Deployment status can be viewed under Overview tab.



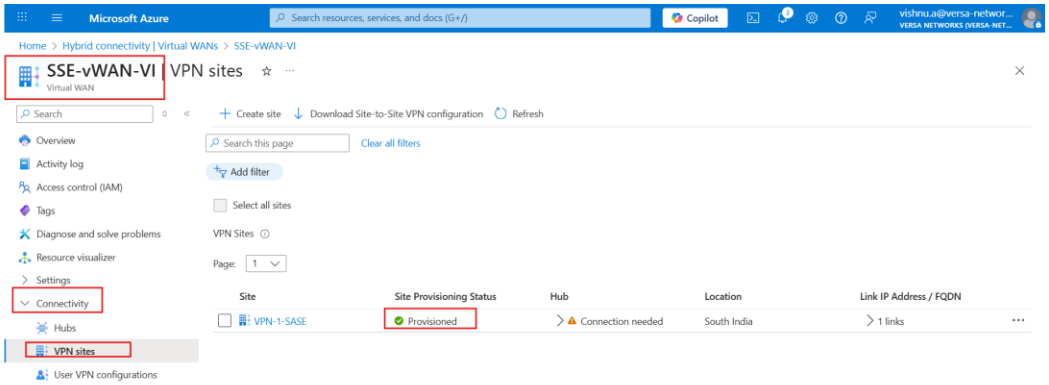
VpnSiteDeployment | Overview

Your deployment is complete

Deployment name : VpnSiteDeployment
Subscription : Pay-As-You-Go
Resource group : Azure-Resource-Group-VI

Start time : 9/28/2025, 4:01:31 PM
Correlation ID : cd7a1ebd-986a-4893-b0aa-ac24743ebaa8

On your Virtual WAN, go to Connectivity → VPN sites, make sure the Status is shown Provisioned.

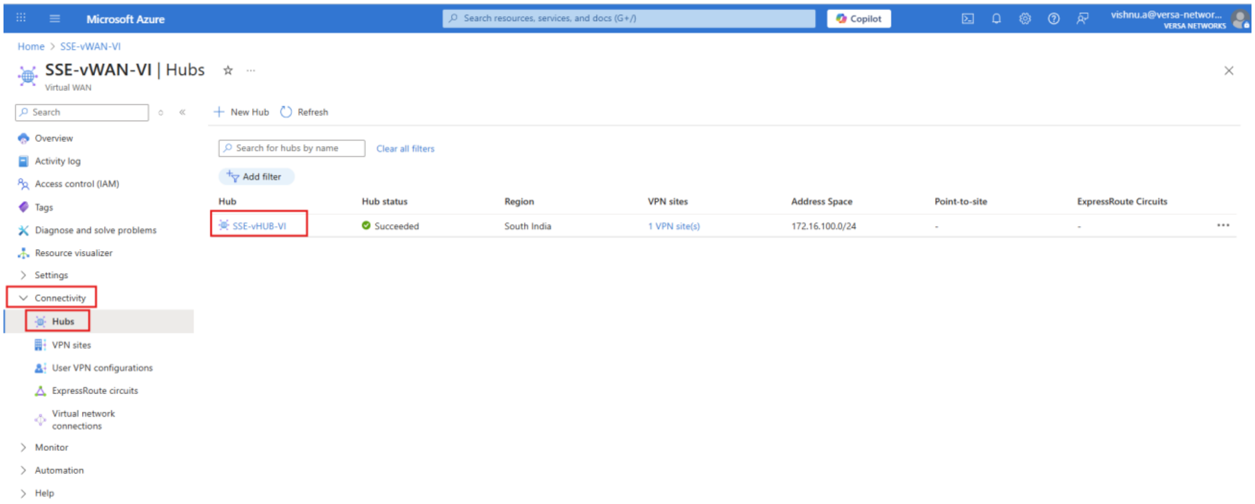


SSE-vWAN-VI | VPN sites

Site	Site Provisioning Status	Hub	Location	Link IP Address / FQDN
VPN-1-SASE	Provisioned	> Connection needed	South India	> 1 links

Connecting the VPN sites

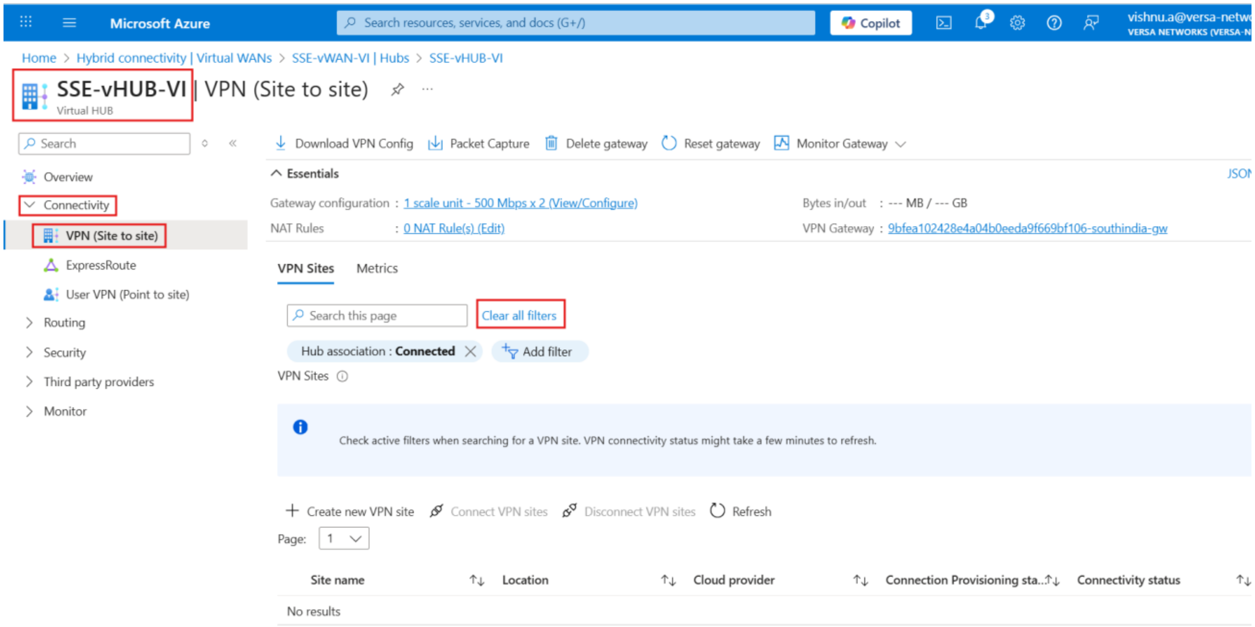
To Connect to VPN Sites, on your Virtual WAN, go to Connectivity → Hubs and click on the hub that you created.



SSE-vWAN-VI | Hubs

Hub	Hub status	Region	VPN sites	Address Space	Point-to-site	ExpressRoute Circuits
SSE-vHUB-VI	Succeeded	South India	1 VPN site(s)	172.16.100.0/24	-	-

On the page for the hub that you created, under "Connectivity", click VPN (Site to site) and click on "Clear all filters".



Gateway configuration : 1 scale unit - 500 Mbps x 2 (View/Configure)

NAT Rules : 0 NAT Rule(s) (Edit)

Bytes in/out : --- MB / --- GB

VPN Gateway : 9bfea102428e4a04b0eeda9f669bf106-southindia-gw

Hub association : Connected

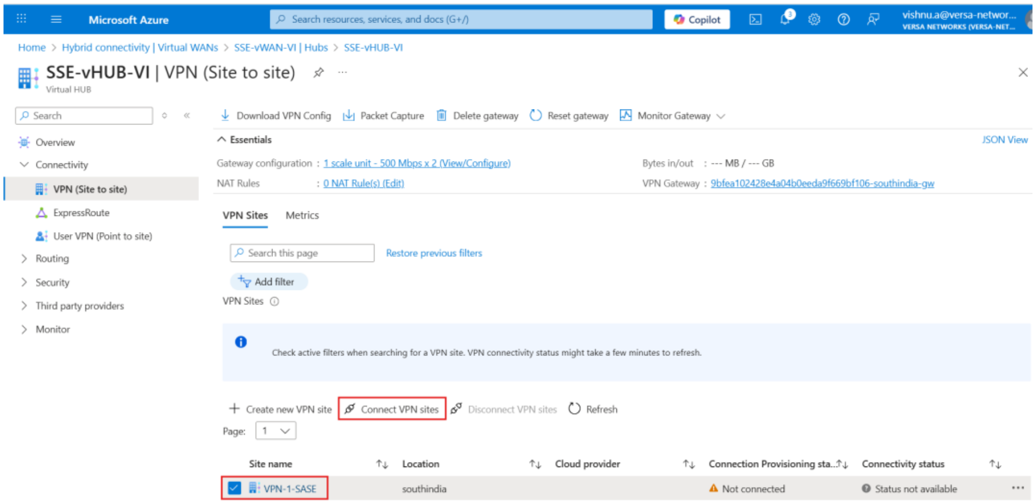
VPN Sites

Check active filters when searching for a VPN site. VPN connectivity status might take a few minutes to refresh.

Page: 1

Site name	Location	Cloud provider	Connection Provisioning sta...	Connectivity status
No results				

Next, select the VPN site and click on Connect VPN sites.



Gateway configuration : 1 scale unit - 500 Mbps x 2 (View/Configure)

NAT Rules : 0 NAT Rule(s) (Edit)

Bytes in/out : --- MB / --- GB

VPN Gateway : 9bfea102428e4a04b0eeda9f669bf106-southindia-gw

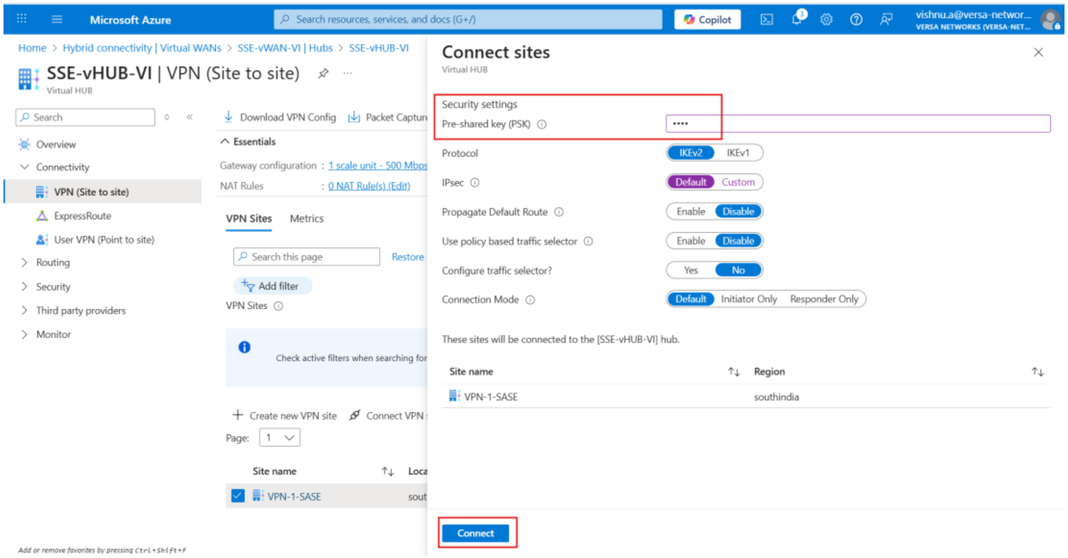
VPN Sites

Check active filters when searching for a VPN site. VPN connectivity status might take a few minutes to refresh.

Page: 1

Site name	Location	Cloud provider	Connection Provisioning sta...	Connectivity status
☑ VPN-1-SASE	southindia		Not connected	Status not available

Enter the PSK details and click on “Connect”.



Gateway configuration : 1 scale unit - 500 Mbps
NAT Rules : 0 NAT Rule(s) (Edit)
VPN Sites
Check active filters when searching for

Site name	Loca
☑ VPN-1-SASE	sout

Connect sites
Virtual HUB

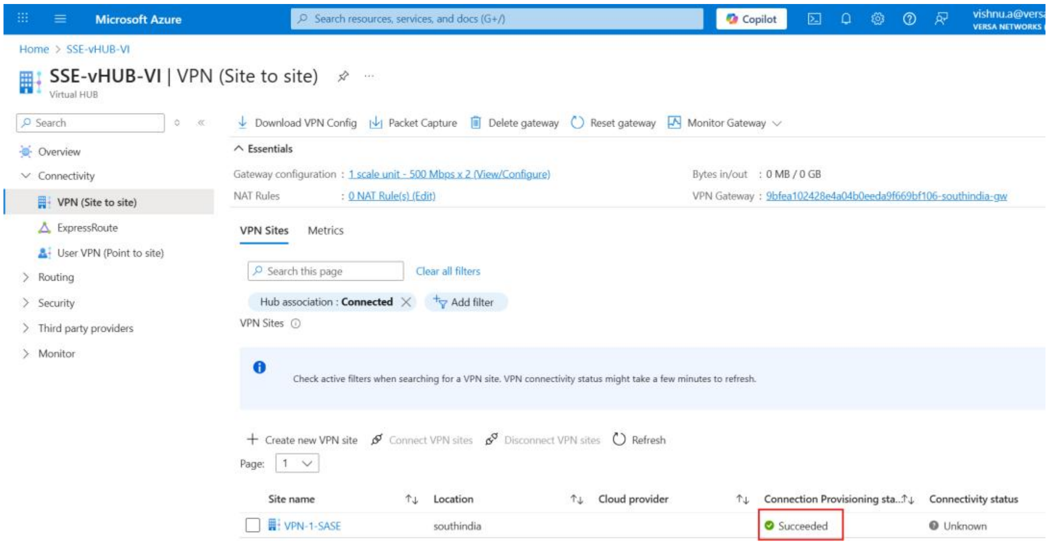
Security settings

Pre-shared key (PSK)	••••
Protocol	[✓ IKEv2] IKEv1
IPsec	[✓ Default] Custom
Propagate Default Route	Enable [✓ Disable]
Use policy based traffic selector	Enable [✓ Disable]
Configure traffic selector?	Yes [✓ No]
Connection Mode	[✓ Default] Initiator Only Responder Only

These sites will be connected to the [SSE-vHUB-VI] hub.

Site name	Region
VPN-1-SASE	southindia

Once it created, the Connection Provisioning status shows “Succeeded”.



Gateway configuration : 1 scale unit - 500 Mbps x 2 (View/Configure)
NAT Rules : 0 NAT Rule(s) (Edit)
Bytes in/out : 0 MB / 0 GB
VPN Gateway : 9bfea102428e4a04b0eeda9f669bf106-southindia-gw

Hub association : Connected

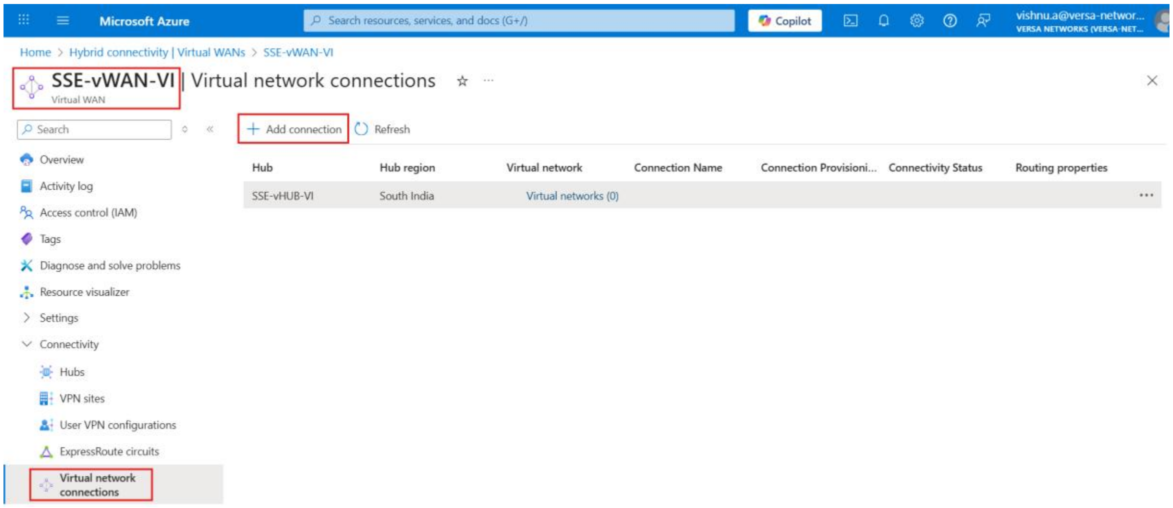
VPN Sites

Check active filters when searching for a VPN site. VPN connectivity status might take a few minutes to refresh.

Site name	Location	Cloud provider	Connection Provisioning sta...	Connectivity status
□ VPN-1-SASE	southindia		✓ Succeeded	● Unknown

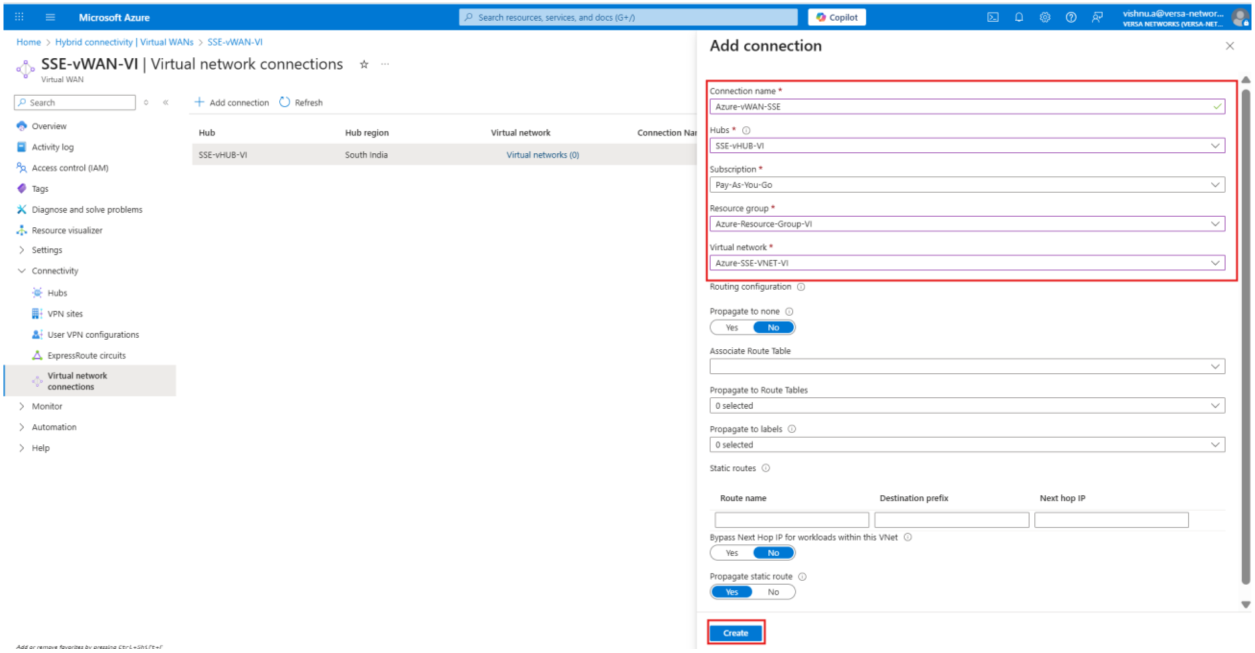
Connecting a VNet to the virtual hub:

In the Azure portal, go to your Virtual WAN, under Connectivity click on Virtual network connections and select “+ Add connection”.



Hub	Hub region	Virtual network	Connection Name	Connection Provisioni...	Connectivity Status	Routing properties
SSE-vHUB-VI	South India	Virtual networks (0)				

Give the connection a name, choose the Virtual WAN hub to associate it with, confirm the subscription and resource group, and select the virtual network to connect—making sure that VNet does not already have a virtual network gateway and click on Create.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
vishnu.a@versa-networ...
VERSA NETWORKS (VERSA-NET...
Home > Hybrid connectivity | Virtual WANs > SSE-vWAN-VI
SSE-vWAN-VI | Virtual network connections
Virtual WAN
Search
+ Add connection
Refresh
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Connectivity
Hubs
VPN sites
User VPN configurations
ExpressRoute circuits
Virtual network connections
Monitor
Automation
Help
Add or remove favorites by pressing Ctrl+Shift+F

Hub	Hub region	Virtual network	Connection Nar
SSE-vHUB-VI	South India	Virtual networks (0)	

Add connection

Connection name *: Azure-vWAN-SSE

Hubs *: SSE-vHUB-VI

Subscription *: Pay-As-You-Go

Resource group *: Azure-Resource-Group-VI

Virtual network *: Azure-SSE-VNET-VI

Routing configuration

Propagate to none: Yes [✓ No]

Associate Route Table:

Propagate to Route Tables: 0 selected

Propagate to labels: 0 selected

Static routes

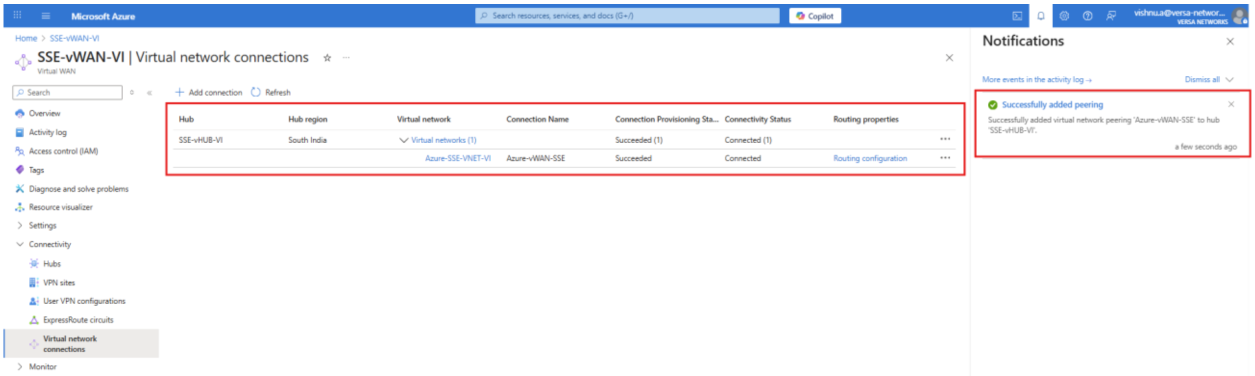
Route name	Destination prefix	Next hop IP

Bypass Next Hop IP for workloads within this VNet: Yes [✓ No]

Propagate static route: [✓ Yes] No

Create

Verify the Virtual network connections from the notifications.



Hub	Hub region	Virtual network	Connection Name	Connection Provisioning Sta...	Connectivity Status	Routing properties
SSE-vHUB-VI	South India	Virtual networks (1)		Succeeded (1)	Connected (1)	
		Azure-SSE-VNET-VI	Azure-vWAN-SSE	Succeeded	Connected	Routing configuration

Notifications

More events in the activity log → Dismiss all

Successfully added peering

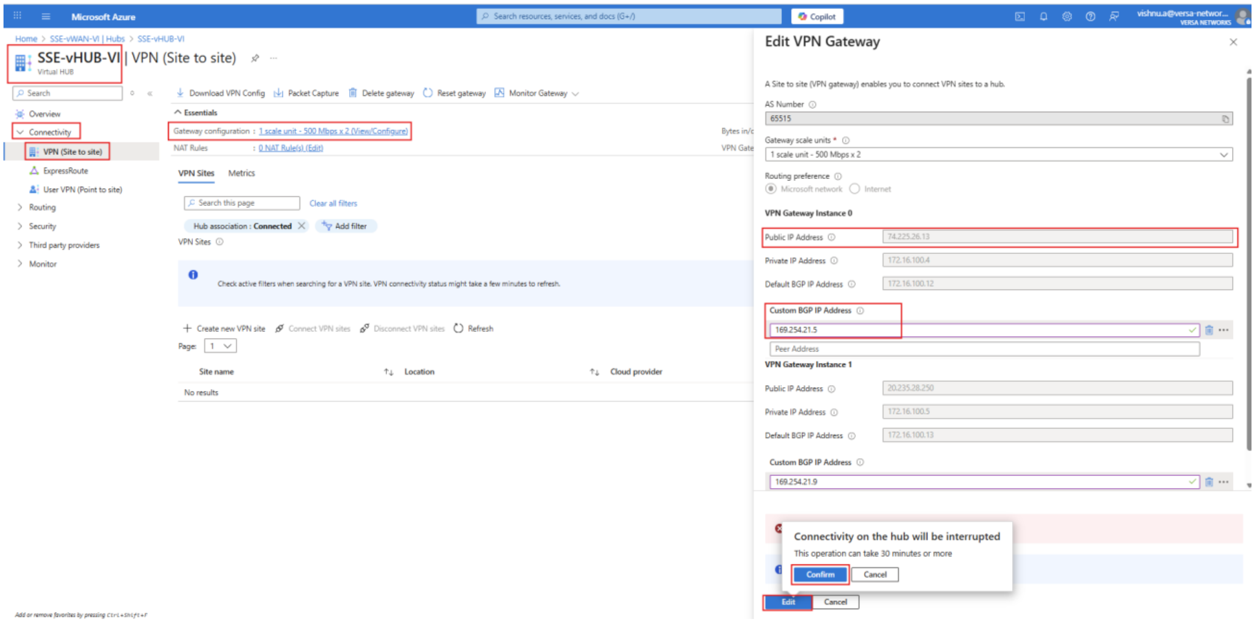
Successfully added virtual network peering 'Azure-vWAN-SSE' to hub 'SSE-vHUB-VI'.

a few seconds ago

View or edit gateway settings

To view and edit your VPN gateway settings. Go to your **Virtual HUB -> VPN (Site to site)** and click on the **Gateway configuration**.

Under Edit VPN Gateway, make note of the Public IP, add the “Custom BGP IP Address” and click **Edit → Confirm**.



SSE-vHUB-VI | VPN (Site to site)
Virtual HUB

Gateway configuration : 1 scale unit - 500 Mbps x 2 (View/Configure)
NAT Rules : 0 NAT Rule(s) (Edit)

Hub association : Connected

VPN Sites

Check active filters when searching for a VPN site. VPN connectivity status might take a few minutes to refresh.

Page: 1

No results

Edit VPN Gateway

A Site to site (VPN gateway) enables you to connect VPN sites to a hub.

AS Number: 65515
Gateway scale units *: 1 scale unit - 500 Mbps x 2
Routing preference: ● Microsoft network ○ Internet

VPN Gateway Instance 0
Public IP Address: 74.225.26.13
Private IP Address: 172.16.100.4
Default BGP IP Address: 172.16.100.12
Custom BGP IP Address: 169.254.21.5
Peer Address

VPN Gateway Instance 1
Public IP Address: 20.235.28.250
Private IP Address: 172.16.100.5
Default BGP IP Address: 172.16.100.13
Custom BGP IP Address: 169.254.21.9

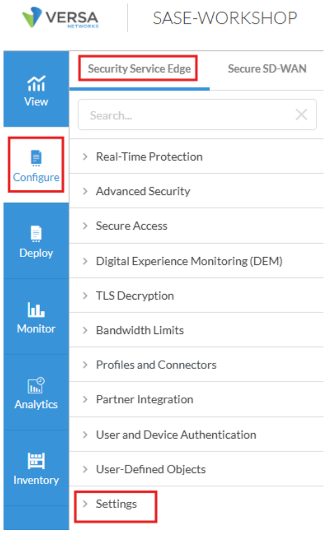
Connectivity on the hub will be interrupted
This operation can take 30 minutes or more

Note: Modifying the Hub will take minimum 30 Minutes.

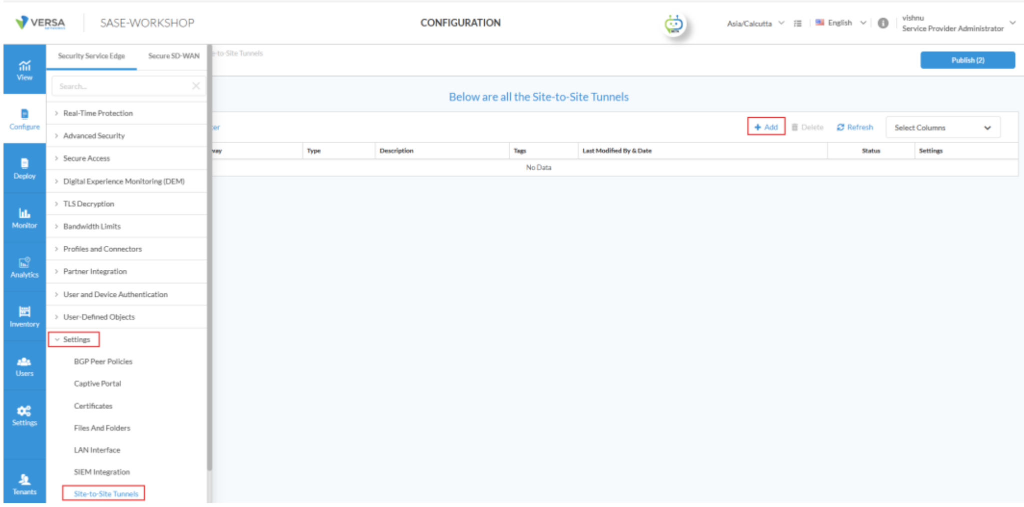
Versa SASE Gateway Configuration

Configure Site to Site Tunnels:

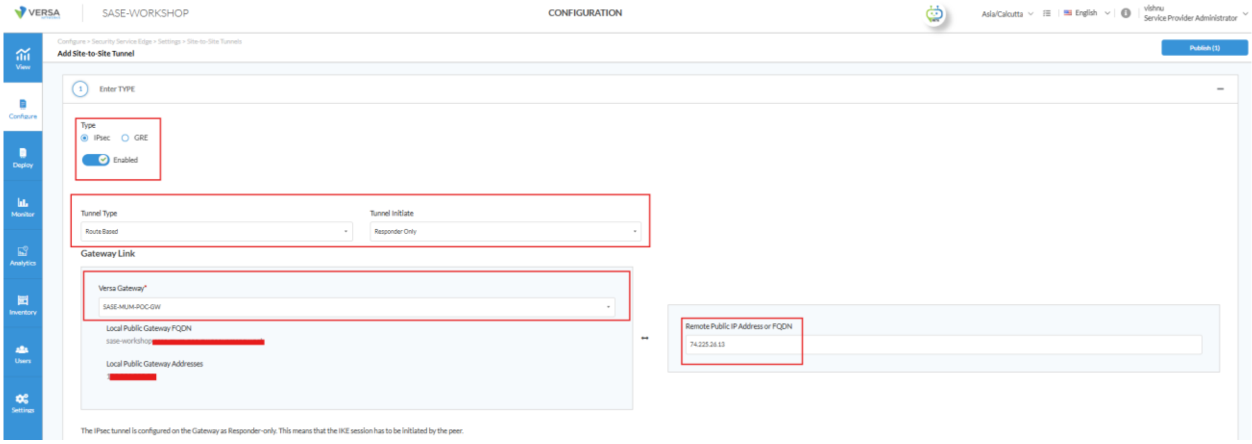
To Configure Site-to-Site Tunnels, Go to Configure →Secure Service Edge → Settings.



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 103.x.x.x, provide the Remote Public IP address.



Add Site-to-Site Tunnel

Type
● IPsec ○ GRE
Enabled

Tunnel Type: Route Based

Tunnel Initiate: Responder Only

Gateway Link

Versa Gateway*: SASE-MUM-POC-GW

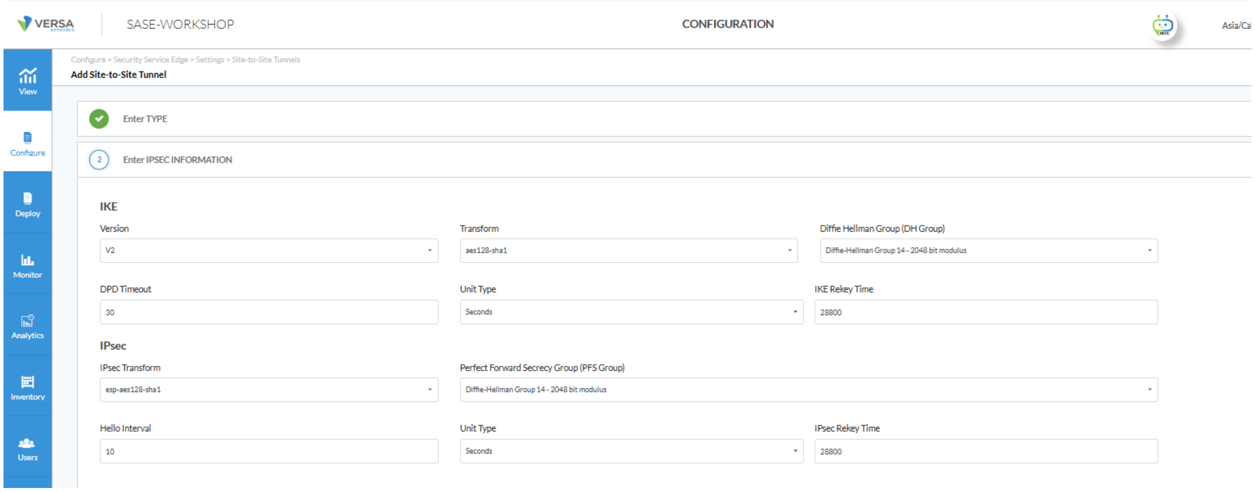
Local Public Gateway FQDN
sase-workshop[redacted]

Local Public Gateway Addresses
[redacted]

Remote Public IP Address or FQDN: 74.225.26.13

The IPsec tunnel is configured on the Gateway as Responder-only. This means that the IKE session has to be initiated by the peer.

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

Enter TYPE

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

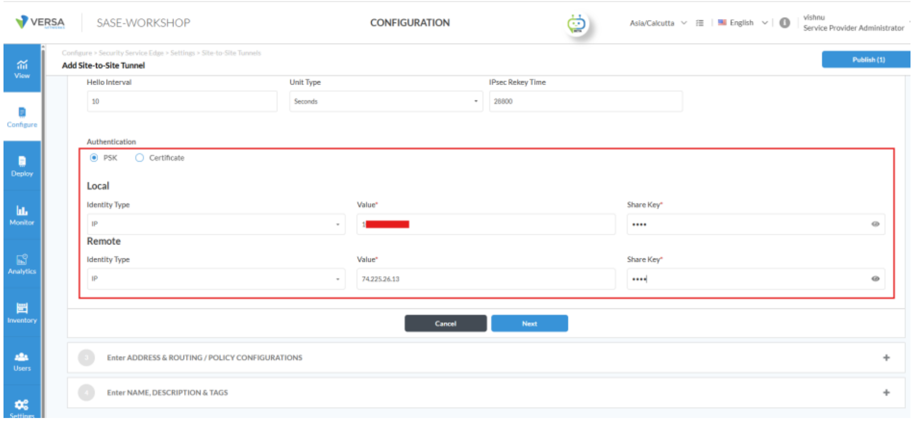
Perfect Forward Secrecy Group (PFS Group): Diffie-Hellman Group 14 - 2048 bit modulus

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

Hello Interval: 10

Unit Type: Seconds

IPsec Rekey Time: 28800

Authentication

● PSK ○ Certificate

Local

Identity Type: IP

Value*: [redacted]

Share Key*: ••••

Remote

Identity Type: IP

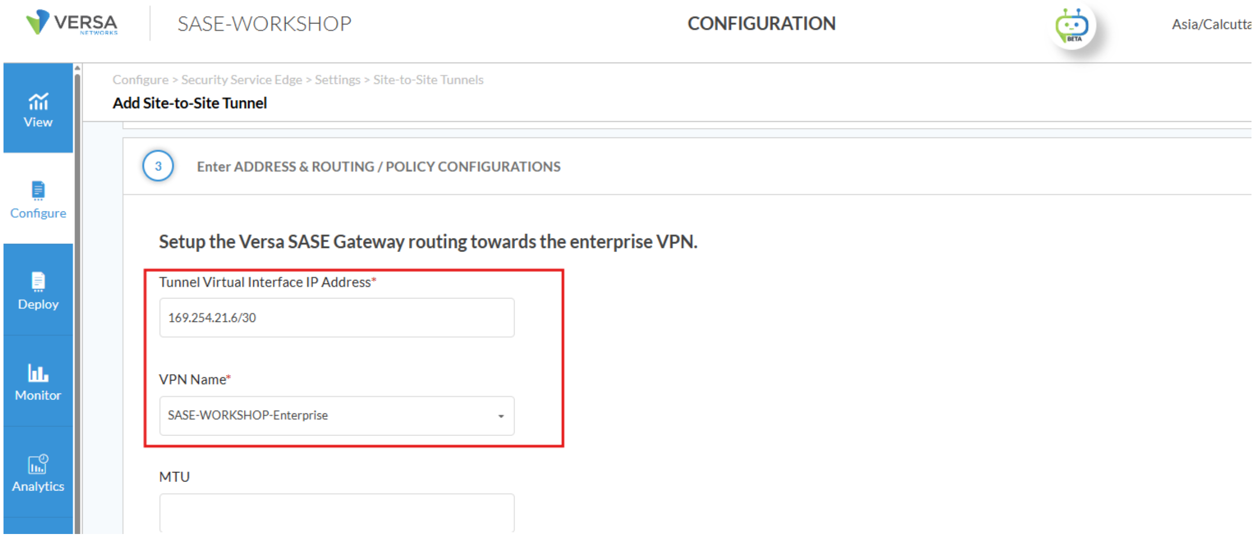
Value*: 74.225.26.13

Share Key*: ••••

3 Enter ADDRESS & ROUTING / POLICY CONFIGURATIONS +

4 Enter NAME, DESCRIPTION & TAGS +

Under “Tunnel Virtual interface IP Address” provide the IP’s generated by Azure 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

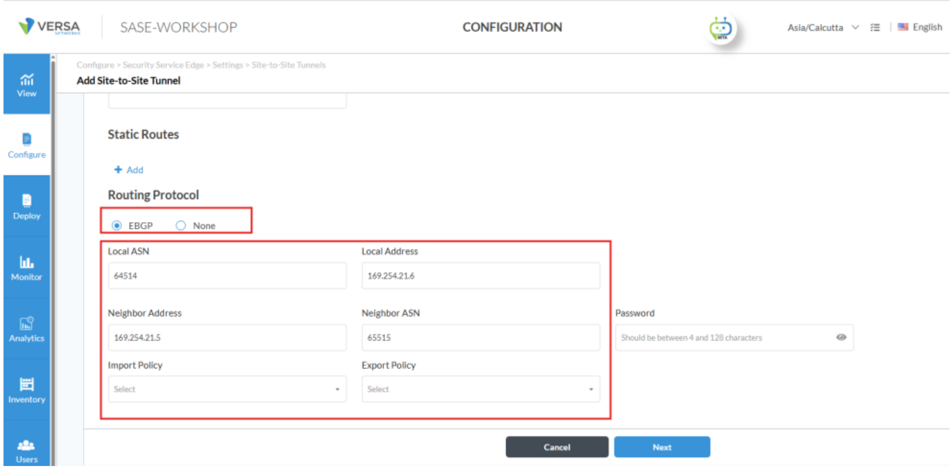
Setup the Versa SASE Gateway routing towards the enterprise VPN.

Tunnel Virtual Interface IP Address*: 169.254.21.6/30

VPN Name*: SASE-WORKSHOP-Enterprise

MTU

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



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

Add Site-to-Site Tunnel

Static Routes

Routing Protocol

● EBGP ○ None

Local ASN: 64514

Local Address: 169.254.21.6

Neighbor Address: 169.254.21.5

Neighbor ASN: 65515

Password: Should be between 4 and 128 characters

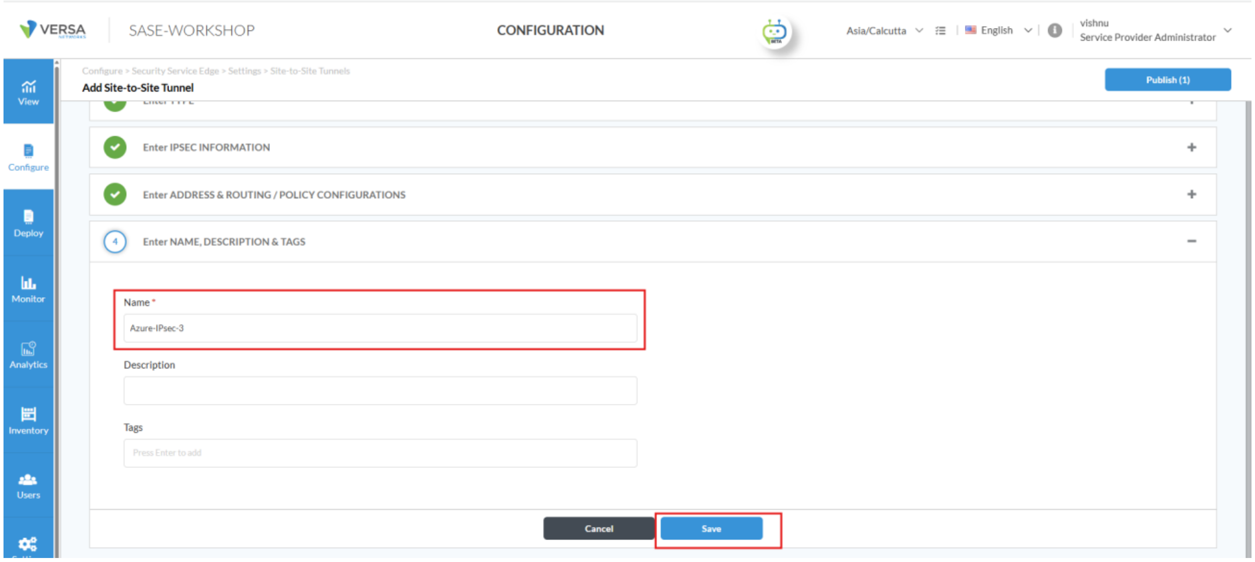
Import Policy: Select

Export Policy: Select

Local ASN	64514
Local Address	169.254.21.6
Remote ASN	65515
Neighbor Address	169.254.21.5

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

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



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

Add Site-to-Site Tunnel

Enter IPSEC INFORMATION

Enter ADDRESS & ROUTING / POLICY CONFIGURATIONS

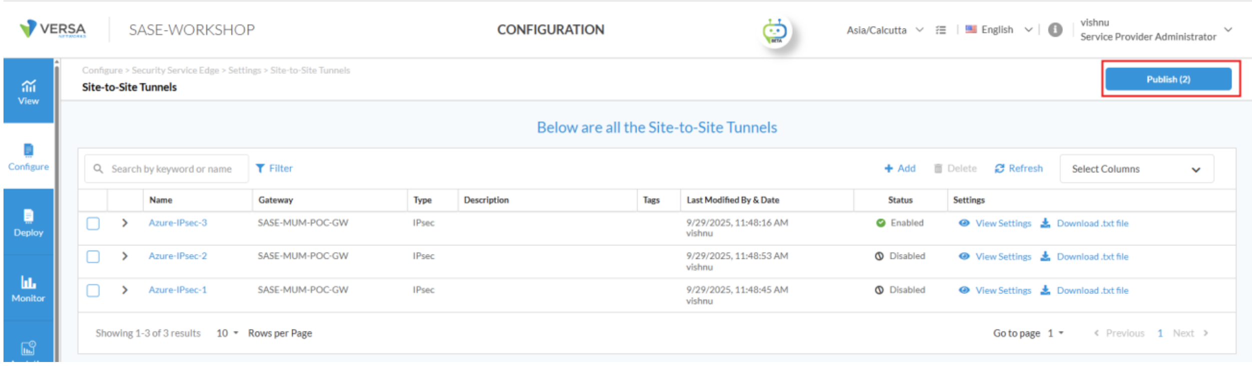
4 Enter NAME, DESCRIPTION & TAGS

Name * Azure-IPsec-3

Description

Tags: Press Enter to add

After saving the configuration, Publish the Config to respective SASE Gateways.



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

Site-to-Site Tunnels

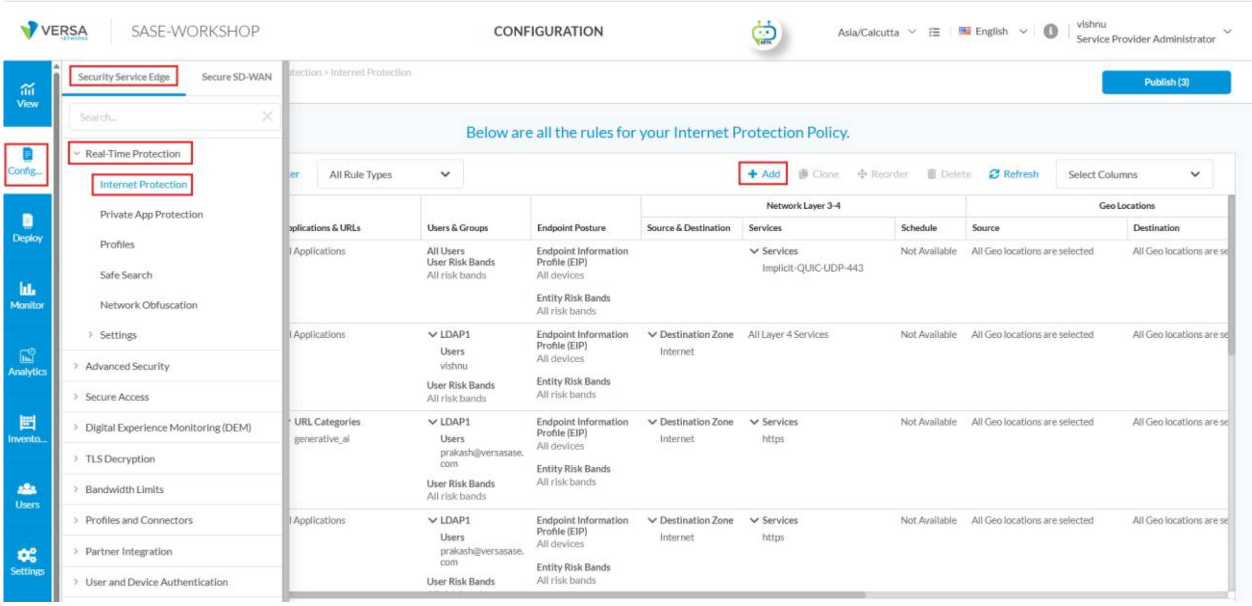
Below are all the Site-to-Site Tunnels

Name	Gateway	Type	Description	Tags	Last Modified By & Date	Status	Settings
Azure-IPsec-3	SASE-MUM-POC-GW	IPsec			9/29/2025, 11:48:16 AM vishnu	Enabled	View Settings Download .txt file
Azure-IPsec-2	SASE-MUM-POC-GW	IPsec			9/29/2025, 11:48:53 AM vishnu	Disabled	View Settings Download .txt file
Azure-IPsec-1	SASE-MUM-POC-GW	IPsec			9/29/2025, 11:48:45 AM vishnu	Disabled	View Settings Download .txt file

Showing 1-3 of 3 results 10 Rows per Page Go to page 1 Previous 1 Next

Configuring Secure Access Rule:

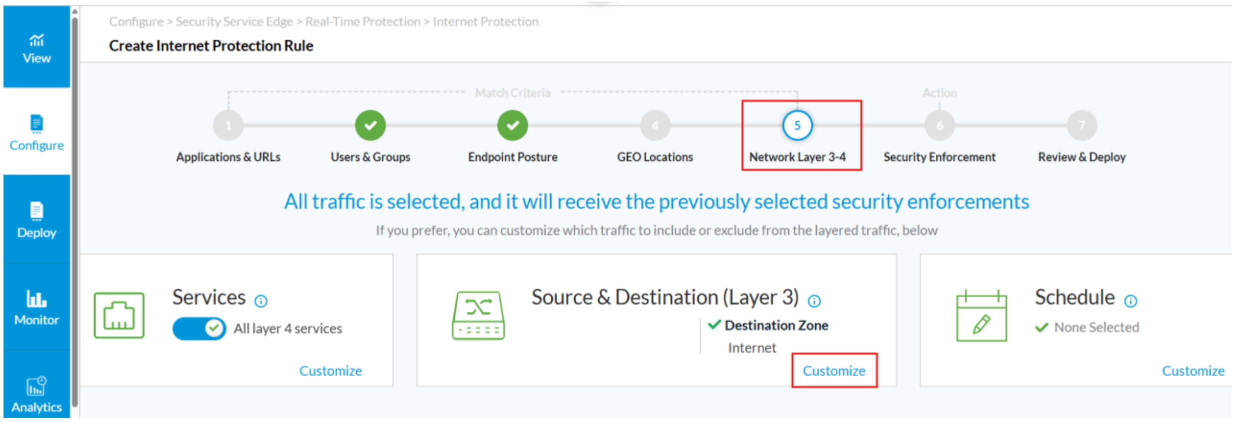
To Create a secure access rule for allowing traffic from SASE clients to AWS EC2 through IPSec tunnels, Go to Configure → Secure Service Edge → Real-Time Protection → Internet Protection and click on "Add".



Below are all the rules for your Internet Protection Policy.

			Network Layer 3-4			Geo Locations	
plications & URLs	Users & Groups	Endpoint Posture	Source & Destination	Services	Schedule	Source	Destination
l Applications	All Users User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands		Services Implicit-QUIC-UDP-443	Not Available	All Geo locations are selected	All Geo locations are se
l Applications	LDAP1 Users vishnu User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Destination Zone Internet	All Layer 4 Services	Not Available	All Geo locations are selected	All Geo locations are se
URL Categories generative_ai	LDAP1 Users prakash@versasase.com User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Destination Zone Internet	Services https	Not Available	All Geo locations are selected	All Geo locations are se
l Applications	LDAP1 Users prakash@versasase.com User Risk Bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Destination Zone Internet	Services https	Not Available	All Geo locations are selected	All Geo locations are se

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

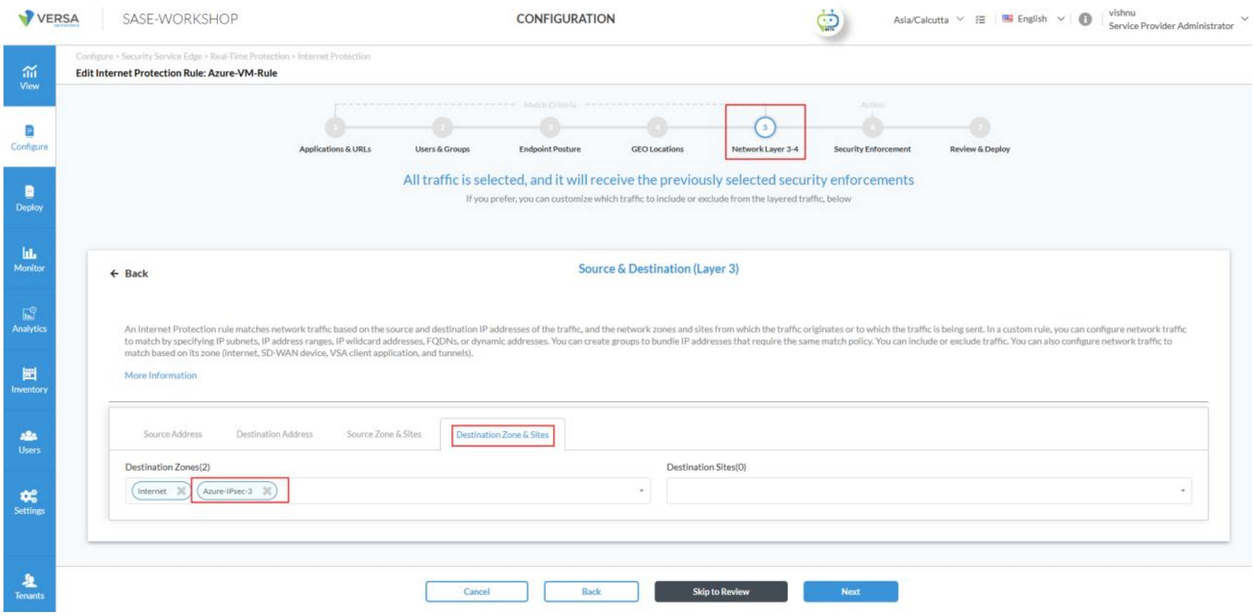
If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

Services
All layer 4 services
Customize

Source & Destination (Layer 3)
✓ Destination Zone
Internet
Customize

Schedule
✓ None Selected
Customize

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



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

Edit Internet Protection Rule: Azure-VM-Rule

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

← Back

Source & Destination (Layer 3)

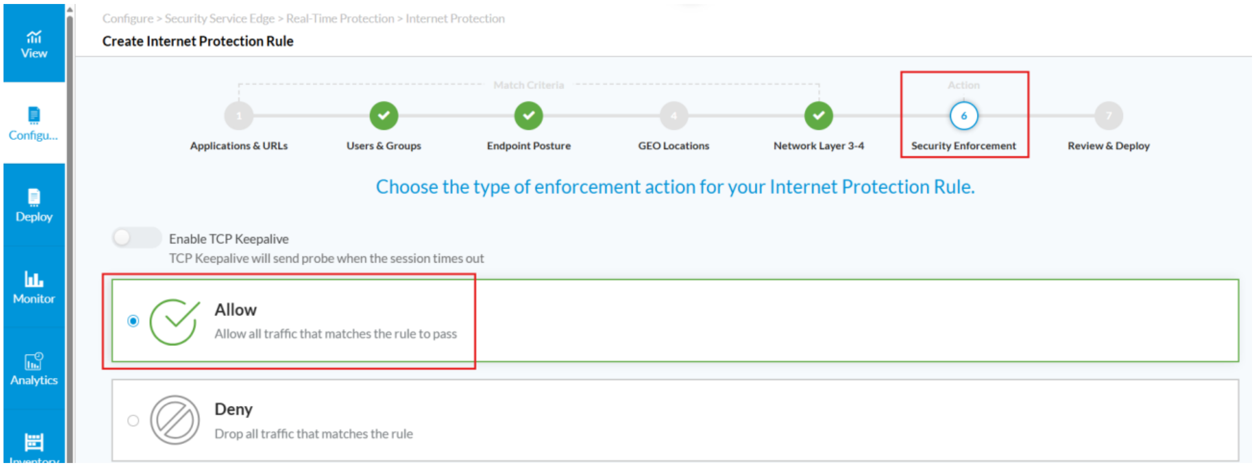
An Internet Protection rule matches network traffic based on the source and destination IP addresses of the traffic, and the network zones and sites from which the traffic originates or to which the traffic is being sent. In a custom rule, you can configure network traffic to match by specifying IP subnets, 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).

More Information

Destination Zones(2): Internet, Azure-IPsec-3

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

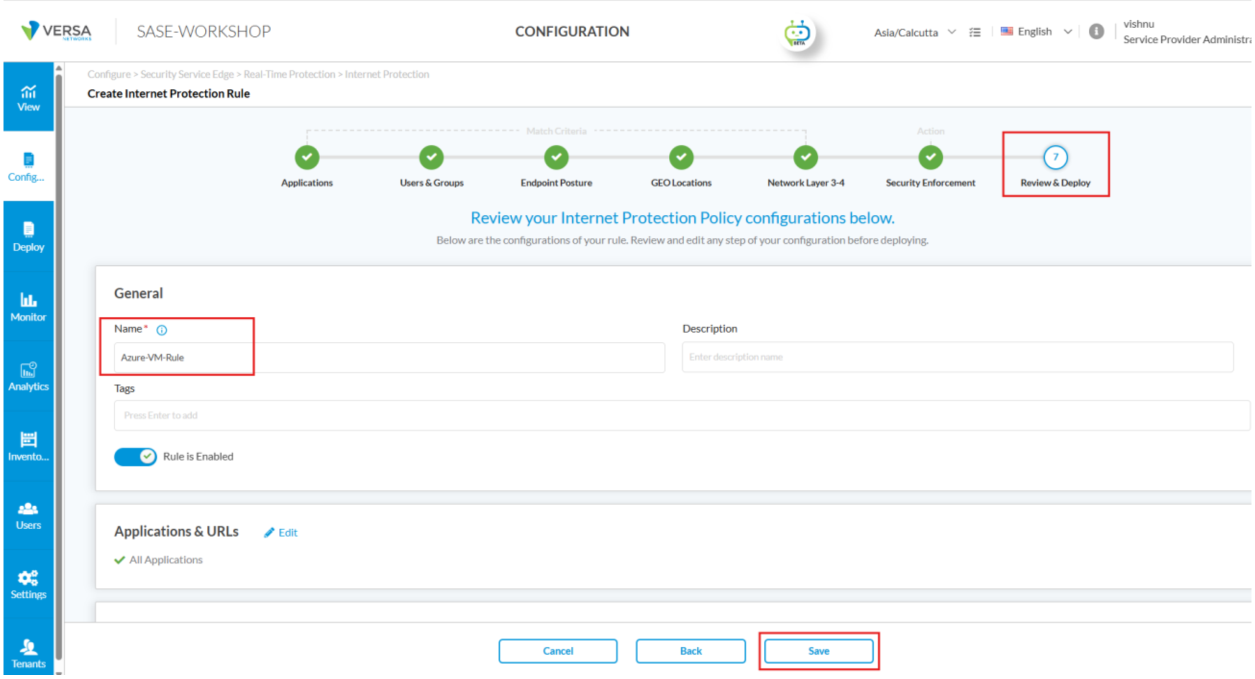
Allow all traffic that matches the rule to pass

○ 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*: Azure-VM-Rule

Description: Enter description name

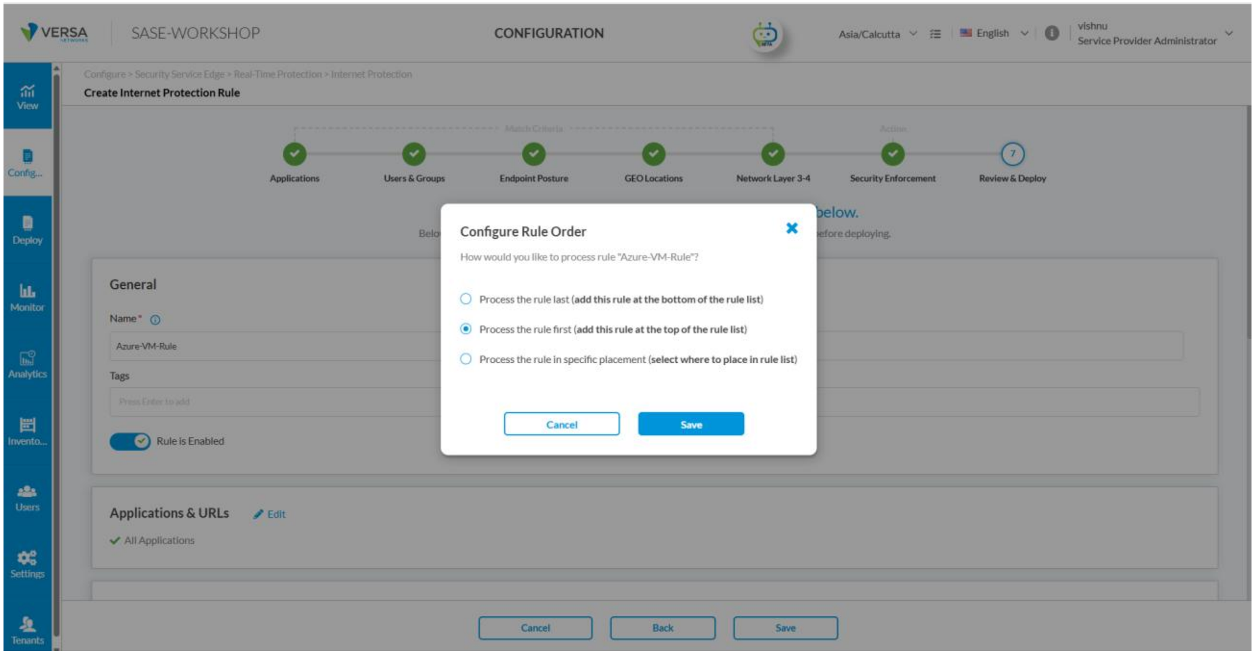
Tags: Press Enter to add

Rule is Enabled

Applications & URLs

✓ All Applications

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 "Azure-VM-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

General

Name*: Azure-VM-Rule

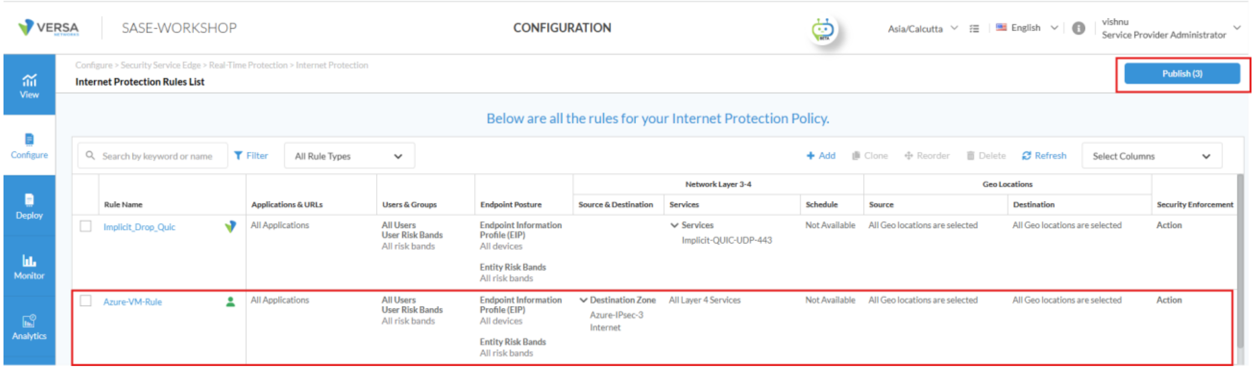
Tags: Press Enter to add

Rule is Enabled

Applications & URLs

✓ All Applications

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



Internet Protection Rules List

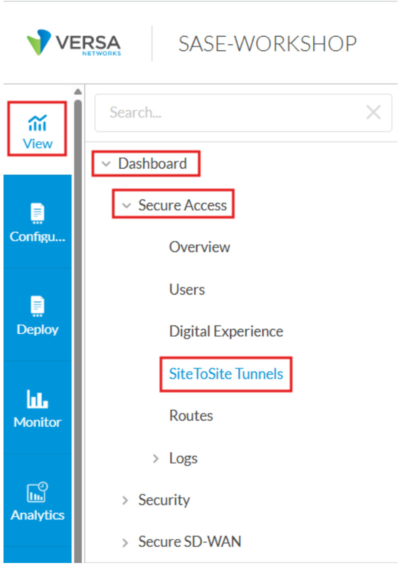
Below are all the rules for your Internet Protection Policy.

Rule Name	Applications & URLs	Users & Groups	Endpoint Posture	Network Layer 3-4			Geo Locations		
				Source & Destination	Services	Schedule	Source	Destination	Security Enforcement
Implicit_Drop_Quic	All Applications	All Users User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands		Services Implicit-QUIC-UDP-443	Not Available	All Geo locations are selected	All Geo locations are selected	Action
Azure-VM-Rule	All Applications	All Users User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Destination Zone Azure-IPsec-3 Internet	All Layer 4 Services	Not Available	All Geo locations are selected	All Geo locations are selected	Action

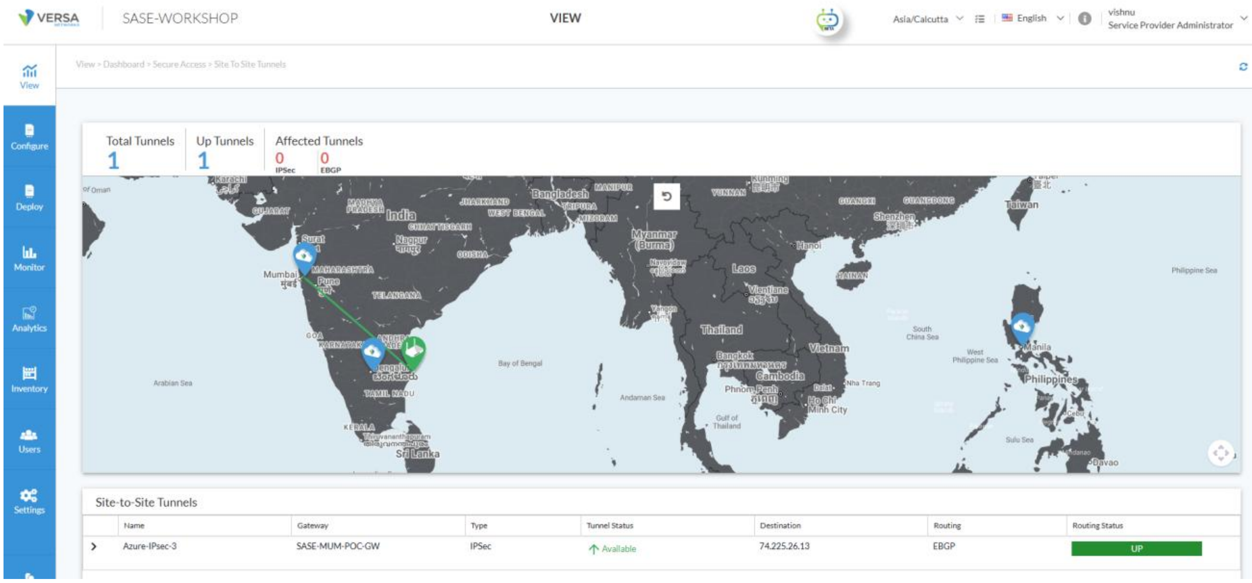
Verification

Verifying BGP and IPsec on SASE GW:

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



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

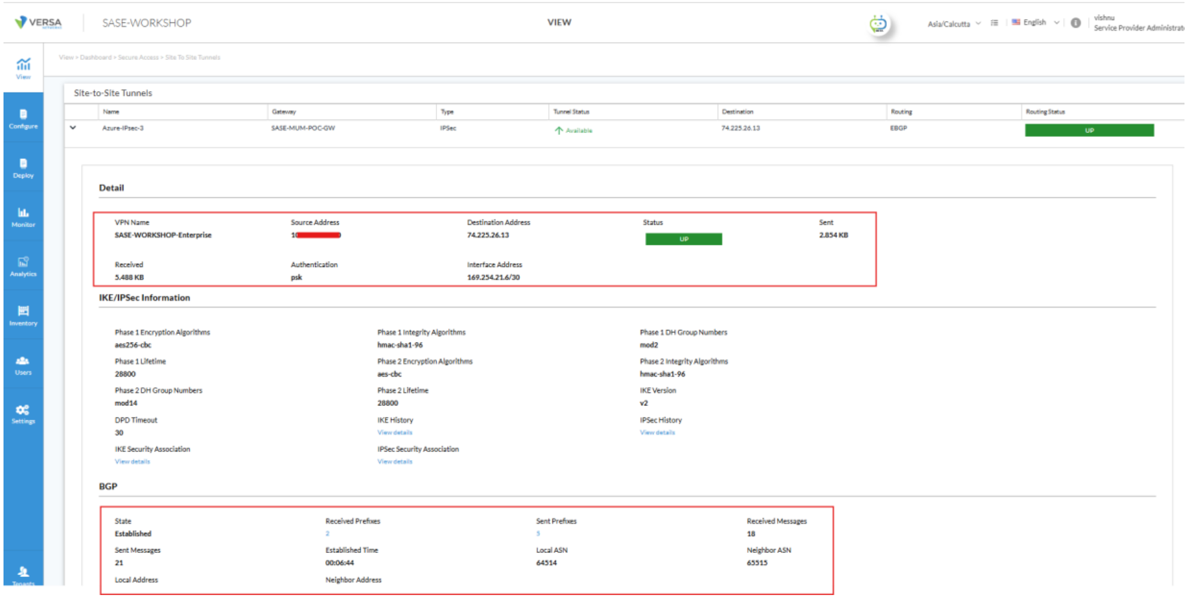


Total Tunnels 1 | Up Tunnels 1 | Affected Tunnels 0 IPSec 0 EBGP

Site-to-Site Tunnels

	Name	Gateway	Type	Tunnel Status	Destination	Routing	Routing Status
>	Azure-IPsec-3	SASE-MUM-POC-GW	IPSec	↑ Available	74.225.26.13	EBGP	UP

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



Site-to-Site Tunnels

	Name	Gateway	Type	Tunnel Status	Destination	Routing	Routing Status
⌄	Azure-IPsec-3	SASE-MUM-POC-GW	IPSec	↑ Available	74.225.26.13	EBGP	UP

Detail

VPN Name: SASE-WORKSHOP-Enterprise
Source Address: 1[redacted]
Destination Address: 74.225.26.13
Status: UP
Sent: 2.854 KB
Received: 5.488 KB
Authentication: psk
Interface Address: 169.254.21.6/30

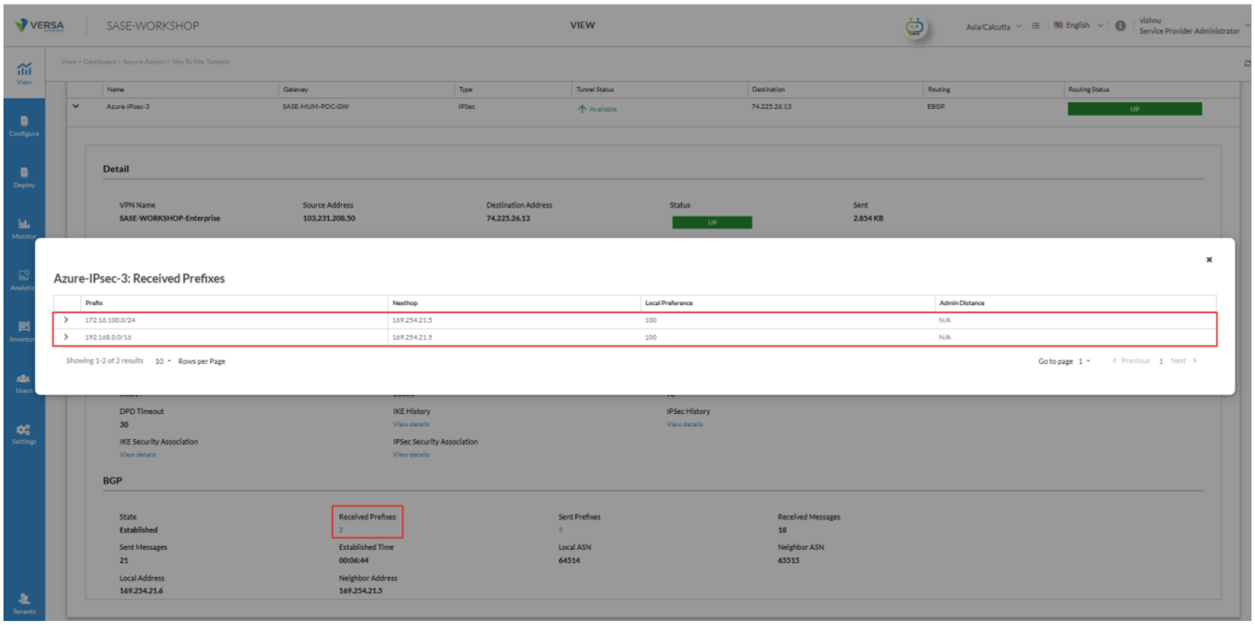
IKE/IPSec Information

Phase 1 Encryption Algorithms: aes256-cbc
Phase 1 Integrity Algorithms: hmac-sha1-96
Phase 1 DH Group Numbers: mod2
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: 2
Sent Prefixes: 5
Received Messages: 18
Sent Messages: 21
Established Time: 00:06:44
Local ASN: 64514
Neighbor ASN: 65515
Local Address
Neighbor Address

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



Name	Gateway	Type	Tunnel Status	Destination	Routing	Routing Status
Azure-IPsec-3	SASE-MUM-POC-GW	IPSec	Available	74.225.26.13	EBGP	UP

Detail

VPN Name: SASE-WORKSHOP-Enterprise
Source Address: 103.231.208.50
Destination Address: 74.225.26.13
Status: UP
Sent: 2.854 KB

Azure-IPsec-3: Received Prefixes

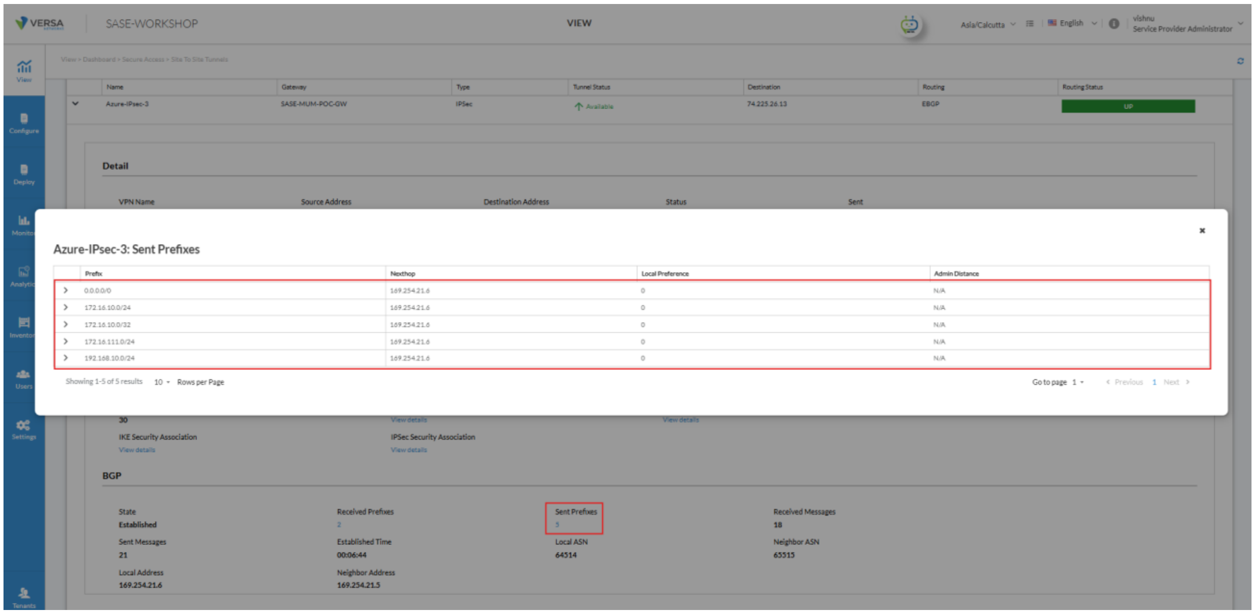
Prefix	Nexthop	Local Preference	Admin Distance
172.16.100.0/24	169.254.21.5	100	N/A
192.168.0.0/16	169.254.21.5	100	N/A

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

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: 2
Sent Prefixes: 5
Received Messages: 18
Sent Messages: 21
Established Time: 00:06:44
Local ASN: 64514
Neighbor ASN: 65515
Local Address: 169.254.21.6
Neighbor Address: 169.254.21.5



Name	Gateway	Type	Tunnel Status	Destination	Routing	Routing Status
Azure-IPsec-3	SASE-MUM-POC-GW	IPSec	Available	74.225.26.13	EBGP	UP

Detail

VPN Name Source Address Destination Address Status Sent

Azure-IPsec-3: Sent Prefixes

Prefix	Nexthop	Local Preference	Admin Distance
0.0.0.0/0	169.254.21.6	0	N/A
172.16.10.0/24	169.254.21.6	0	N/A
172.16.10.0/32	169.254.21.6	0	N/A
172.16.111.0/24	169.254.21.6	0	N/A
192.168.10.0/24	169.254.21.6	0	N/A

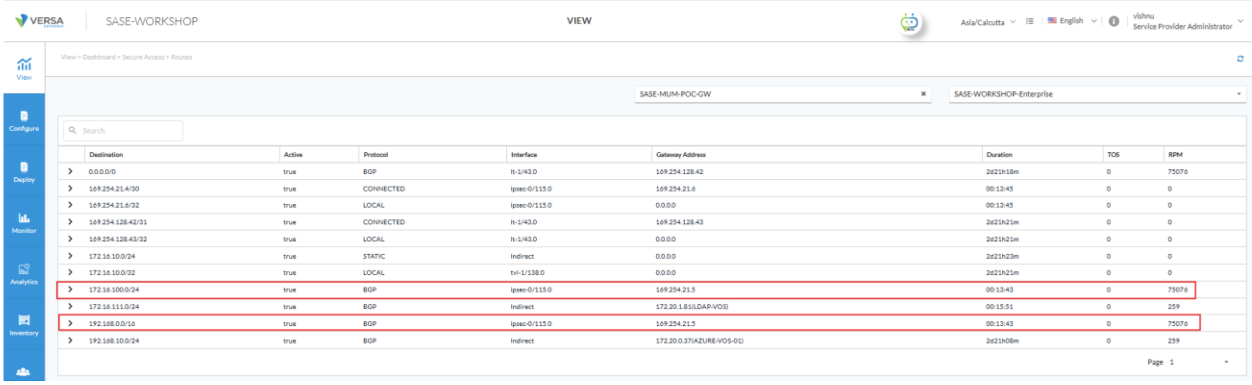
Showing 1-5 of 5 results 10 Rows per Page Go to page 1 Previous 1 Next

30
IKE Security Association: View details
IPSec Security Association: View details

BGP

State: Established
Received Prefixes: 2
Sent Prefixes: 5
Received Messages: 18
Sent Messages: 21
Established Time: 00:06:44
Local ASN: 64514
Neighbor ASN: 65515
Local Address: 169.254.21.6
Neighbor Address: 169.254.21.5

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



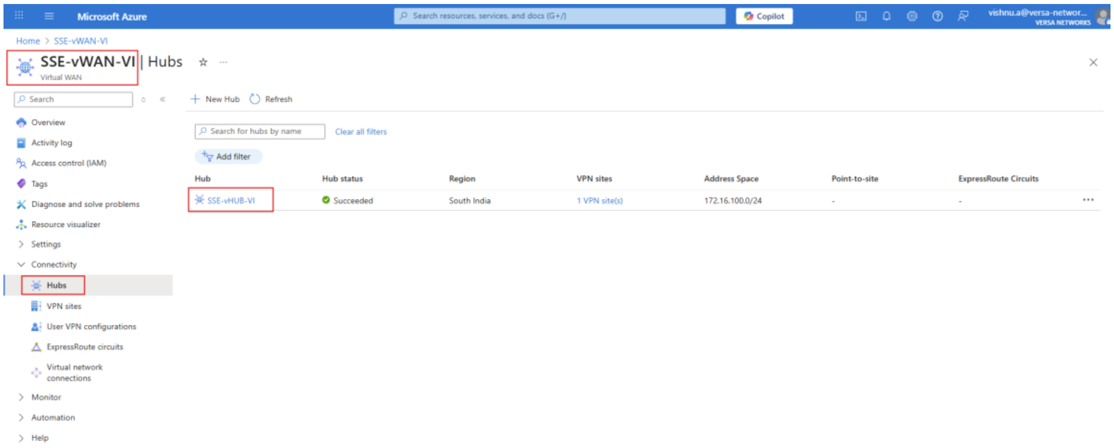
SASE-MUM-POC-GW SASE-WORKSHOP-Enterprise

Destination	Active	Protocol	Interface	Gateway Address	Duration	TOS	RPM
0.0.0.0/0	true	BGP	lt-1/43.0	169.254.128.42	2d21h18m	0	75076
169.254.21.4/30	true	CONNECTED	ipsec-0/115.0	169.254.21.6	00:13:45	0	0
169.254.21.6/32	true	LOCAL	ipsec-0/115.0	0.0.0.0	00:13:45	0	0
169.254.128.42/31	true	CONNECTED	lt-1/43.0	169.254.128.43	2d21h21m	0	0
169.254.128.43/32	true	LOCAL	lt-1/43.0	0.0.0.0	2d21h21m	0	0
172.16.10.0/24	true	STATIC	Indirect	0.0.0.0	2d21h23m	0	0
172.16.10.0/32	true	LOCAL	tvi-1/138.0	0.0.0.0	2d21h21m	0	0
172.16.100.0/24	true	BGP	ipsec-0/115.0	169.254.21.5	00:13:43	0	75076
172.16.111.0/24	true	BGP	Indirect	172.20.1.81(LDAP-VOS)	00:15:51	0	259
192.168.0.0/16	true	BGP	ipsec-0/115.0	169.254.21.5	00:13:43	0	75076
192.168.10.0/24	true	BGP	Indirect	172.20.0.37(AZURE-VOS-01)	2d21h08m	0	259

Page 1

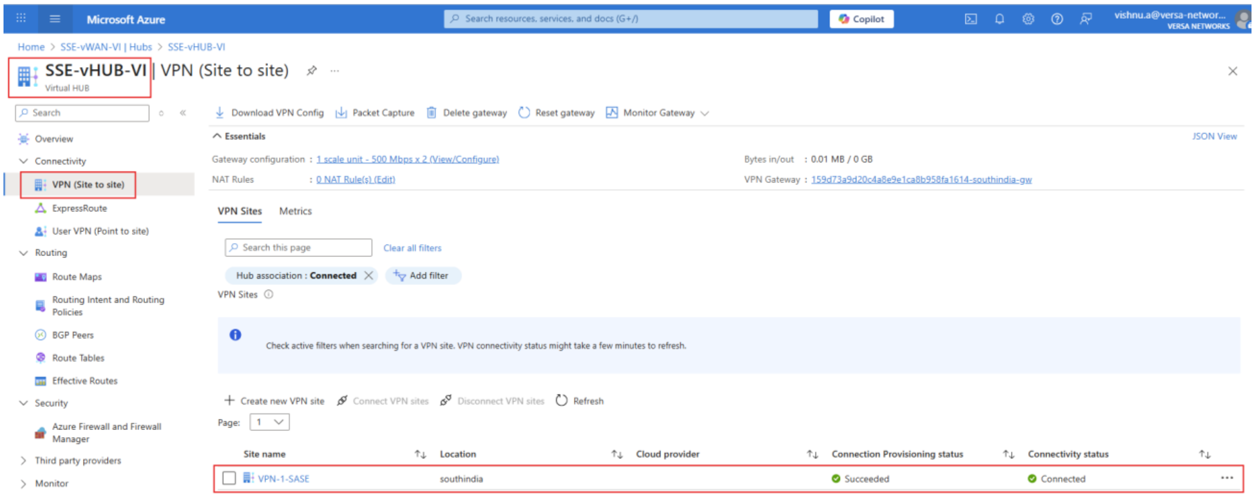
Verifying BGP and IPsec on Azure:

To verify IPsec in Azure portal, Go to the Azure Virtual Hub that you created under Virtual WAN.



Hub	Hub status	Region	VPN sites	Address Space	Point-to-site	ExpressRoute Circuits
SSE-vHUB-VI	Succeeded	South India	1 VPN site(s)	172.16.100.0/24	-	-

Under Virtual Hub, go to Connectivity →VPN (site to site) and you should see the Connectivity status as “Connected”.



Gateway configuration : 1 scale unit - 500 Mbps x 2 (View/Configure)
NAT Rules : 0 NAT Rule(s) (Edit)
Bytes in/out : 0.01 MB / 0 GB
VPN Gateway : 159d73a9d20c4a8e9e1ca8b958fa1614-southindia-gw

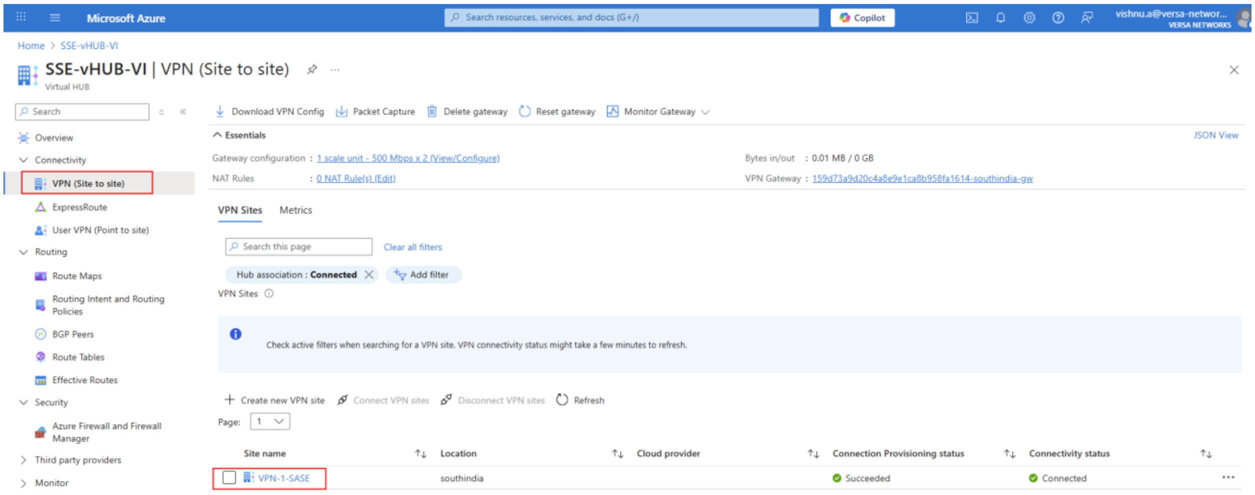
VPN Sites

Check active filters when searching for a VPN site. VPN connectivity status might take a few minutes to refresh.

Site name	Location	Cloud provider	Connection Provisioning status	Connectivity status
VPN-1-SASE	southindia		Succeeded	Connected

Verify the BGP status and Routes Learnt on Azure:

To Verify the BGP status, Go to “VPN(Site to Site)” under Connectivity → click on VPN Connection (VPN-1-SASE).



Gateway configuration : 1 scale unit - 500 Mbps x 2 (View/Configure)

NAT Rules : 0 NAT Rule(s) (Edit)

Bytes in/out : 0.01 MB / 0 GB

VPN Gateway : 159d73a9d20c4a8e9e1ca8b958fa1614-southindia-gw

Hub association : **Connected**

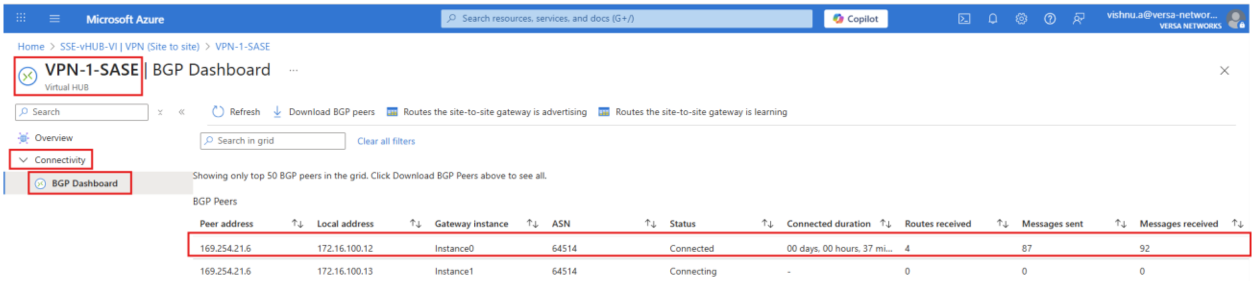
VPN Sites

Check active filters when searching for a VPN site. VPN connectivity status might take a few minutes to refresh.

Page: 1

Site name	Location	Cloud provider	Connection Provisioning status	Connectivity status
□ VPN-1-SASE	southindia		Succeeded	Connected

Under the Virtual HUB, go to Connectivity → BGP Dashboard, you should see the Connectivity status as Connected along with Routes received, Messages sent and received.

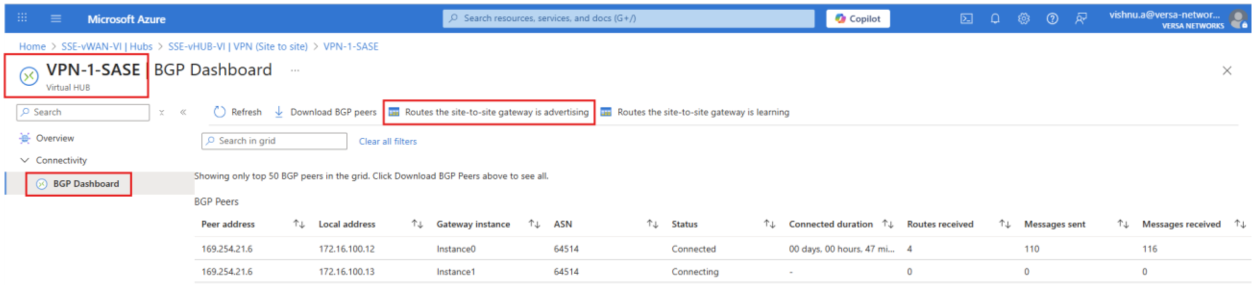

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
vishnu.a@versa-networ...
VERSA NETWORKS
Home > SSE-vHUB-VI | VPN (Site to site) > VPN-1-SASE
VPN-1-SASE | BGP Dashboard
Virtual HUB
Search
Overview
Connectivity
BGP Dashboard
Refresh
Download BGP peers
Routes the site-to-site gateway is advertising
Routes the site-to-site gateway is learning
Search in grid
Clear all filters

Showing only top 50 BGP peers in the grid. Click Download BGP Peers above to see all.

BGP Peers

Peer address	Local address	Gateway instance	ASN	Status	Connected duration	Routes received	Messages sent	Messages received
169.254.21.6	172.16.100.12	Instance0	64514	Connected	00 days, 00 hours, 37 mi...	4	87	92
169.254.21.6	172.16.100.13	Instance1	64514	Connecting	-	0	0	0

To view the advertised routes from the HUB, click on “Routes the site-to-site gateways is advertising” tab.

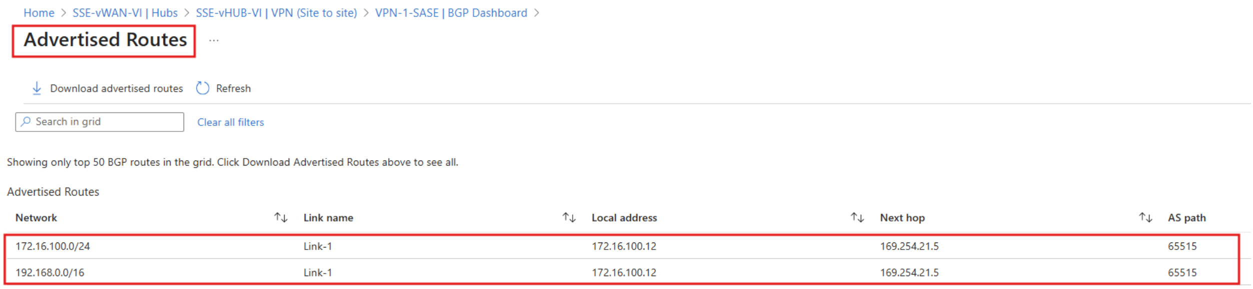

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
vishnu.a@versa-networ...
VERSA NETWORKS
Home > SSE-vWAN-VI | Hubs > SSE-vHUB-VI | VPN (Site to site) > VPN-1-SASE
VPN-1-SASE | BGP Dashboard
Virtual HUB
Search
Overview
Connectivity
BGP Dashboard
Refresh
Download BGP peers
Routes the site-to-site gateway is advertising
Routes the site-to-site gateway is learning
Search in grid
Clear all filters

Showing only top 50 BGP peers in the grid. Click Download BGP Peers above to see all.

BGP Peers

Peer address	Local address	Gateway instance	ASN	Status	Connected duration	Routes received	Messages sent	Messages received
169.254.21.6	172.16.100.12	Instance0	64514	Connected	00 days, 00 hours, 47 mi...	4	110	116
169.254.21.6	172.16.100.13	Instance1	64514	Connecting	-	0	0	0

Under Advertised Routes, you should see the routes that are advertised over BGP.



Home > SSE-vWAN-VI | Hubs > SSE-vHUB-VI | VPN (Site to site) > VPN-1-SASE | BGP Dashboard >

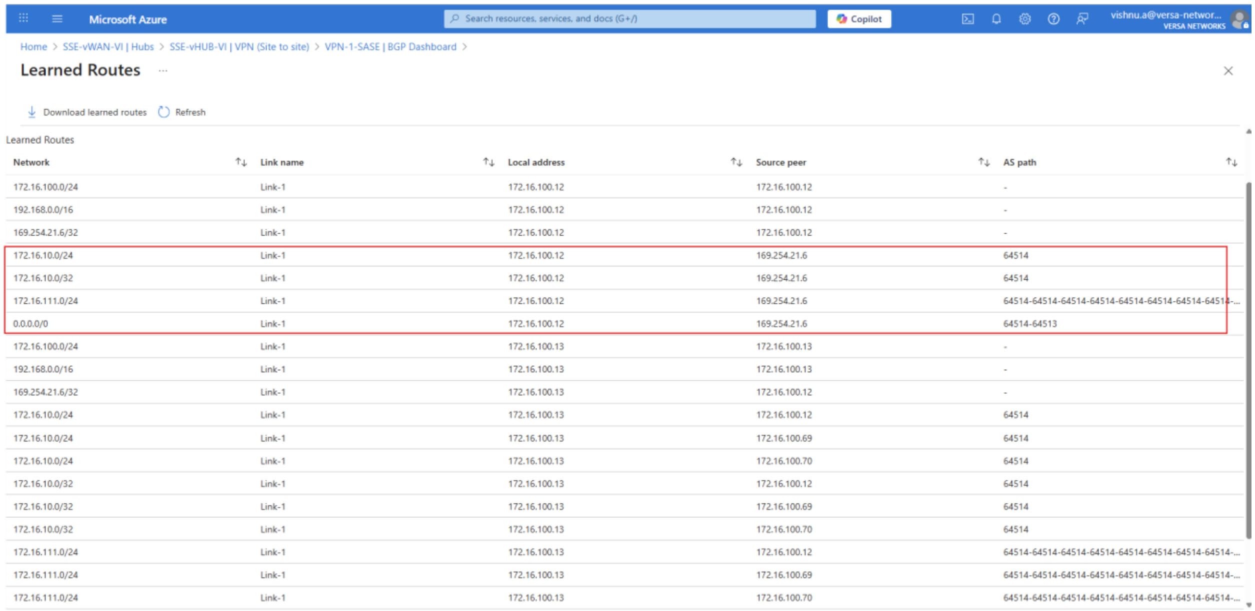
Advertised Routes ···

Showing only top 50 BGP routes in the grid. Click Download Advertised Routes above to see all.

Advertised Routes

Network	Link name	Local address	Next hop	AS path
172.16.100.0/24	Link-1	172.16.100.12	169.254.21.5	65515
192.168.0.0/16	Link-1	172.16.100.12	169.254.21.5	65515

To view the learned routes from the SASE Gateway, click on “Routes the site-to-site gateway is learning” tab.



Home > SSE-vWAN-VI | Hubs > SSE-vHUB-VI | VPN (Site to site) > VPN-1-SASE | BGP Dashboard >

Learned Routes ···

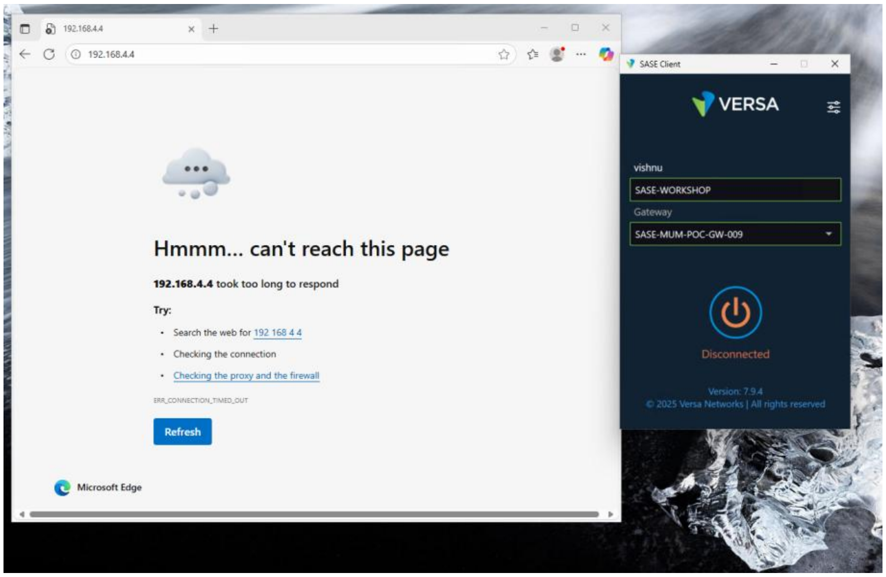
Learned Routes

Network	Link name	Local address	Source peer	AS path
172.16.100.0/24	Link-1	172.16.100.12	172.16.100.12	-
192.168.0.0/16	Link-1	172.16.100.12	172.16.100.12	-
169.254.21.6/32	Link-1	172.16.100.12	172.16.100.12	-
172.16.10.0/24	Link-1	172.16.100.12	169.254.21.6	64514
172.16.10.0/32	Link-1	172.16.100.12	169.254.21.6	64514
172.16.111.0/24	Link-1	172.16.100.12	169.254.21.6	64514-64514-64514-64514-64514-64514-64514-64514-...
0.0.0.0/0	Link-1	172.16.100.12	169.254.21.6	64514-64513
172.16.100.0/24	Link-1	172.16.100.13	172.16.100.13	-
192.168.0.0/16	Link-1	172.16.100.13	172.16.100.13	-
169.254.21.6/32	Link-1	172.16.100.13	172.16.100.12	-
172.16.10.0/24	Link-1	172.16.100.13	172.16.100.12	64514
172.16.10.0/24	Link-1	172.16.100.13	172.16.100.69	64514
172.16.10.0/24	Link-1	172.16.100.13	172.16.100.70	64514
172.16.10.0/32	Link-1	172.16.100.13	172.16.100.12	64514
172.16.10.0/32	Link-1	172.16.100.13	172.16.100.69	64514
172.16.10.0/32	Link-1	172.16.100.13	172.16.100.70	64514
172.16.111.0/24	Link-1	172.16.100.13	172.16.100.12	64514-64514-64514-64514-64514-64514-64514-64514-...
172.16.111.0/24	Link-1	172.16.100.13	172.16.100.69	64514-64514-64514-64514-64514-64514-64514-64514-...
172.16.111.0/24	Link-1	172.16.100.13	172.16.100.70	64514-64514-64514-64514-64514-64514-64514-64514-...

Verifying connectivity:

Accessing Azure Virtual Machine instance with IP: 192.168.4.4 from Remote PC.

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



vishnu

SASE-WORKSHOP

Gateway

SASE-MUM-POC-GW-009

Disconnected

Version: 7.9.4
© 2025 Versa Networks | All rights reserved

Hmmm... can't reach this page

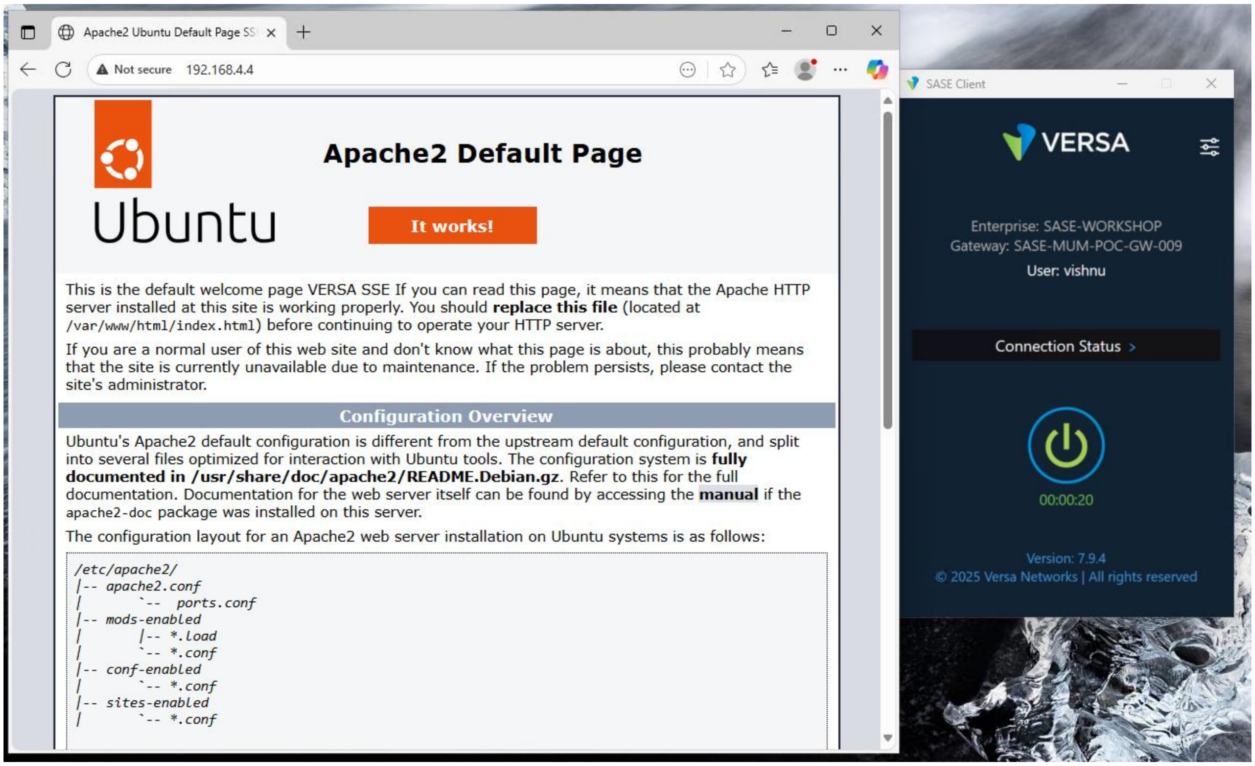
192.168.4.4 took too long to respond

Try:

- Search the web for 192 168 4 4
- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_TIMED_OUT

When the SASE Client is connected to the Gateway we were able to reach the Azure VM instance over Private IP.



Enterprise: SASE-WORKSHOP
Gateway: SASE-MUM-POC-GW-009
User: vishnu

Connection Status >

00:00:20

Version: 7.9.4
© 2025 Versa Networks | All rights reserved

Apache2 Default Page

It works!

This is the default welcome page VERSA SSE If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) 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 means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

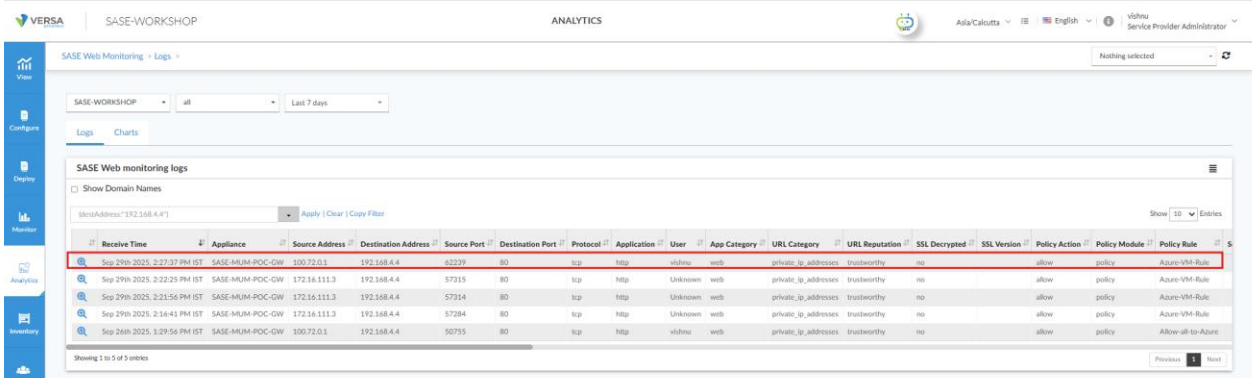
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

SASE-WEB LOGS on Analytics:

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



VERSA | SASE-WORKSHOP | ANALYTICS | Asia/Calcutta | English | vishnu Service Provider Administrator

SASE Web Monitoring > Logs >

Nothing selected

SASE-WORKSHOP | all | Last 7 days

Logs | Charts

SASE Web monitoring logs

□ Show Domain Names

{destAddress:"192.168.4.4"} Apply | Clear | Copy Filter

Show 10 Entries

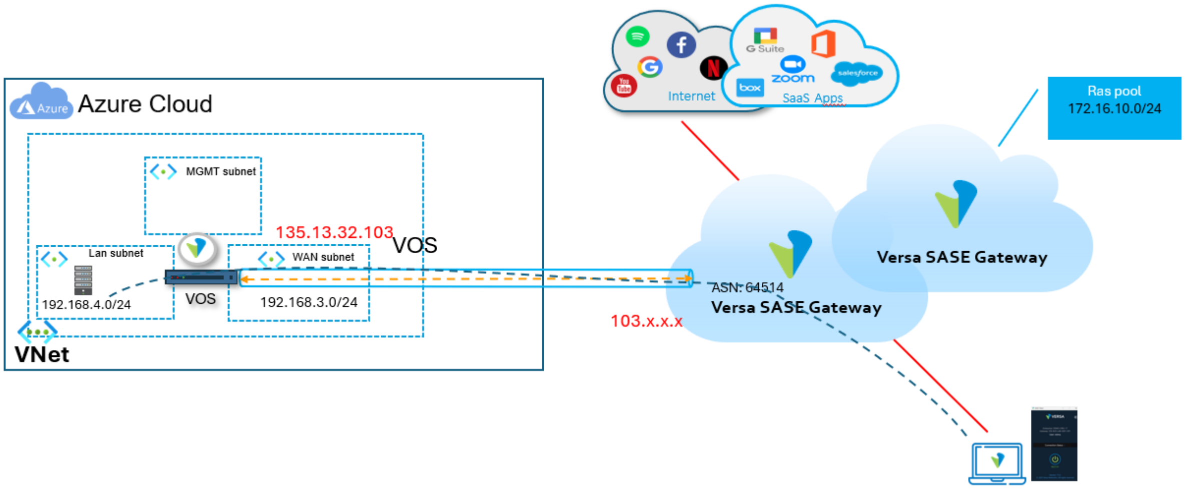
Receive Time	Appliance	Source Address	Destination Address	Source Port	Destination Port	Protocol	Application	User	App Category	URL Category	URL Reputation	SSL Decrypted	SSL Version	Policy Action	Policy Module	Policy Rule
Sep 29th 2025, 2:27:37 PM IST	SASE-MUM-POC-GW	100.72.0.1	192.168.4.4	62239	80	tcp	http	vishnu	web	private_ip_addresses	trustworthy	no		allow	policy	Azure-VM-Rule
Sep 29th 2025, 2:22:25 PM IST	SASE-MUM-POC-GW	172.16.111.3	192.168.4.4	57315	80	tcp	http	Unknown	web	private_ip_addresses	trustworthy	no		allow	policy	Azure-VM-Rule
Sep 29th 2025, 2:21:56 PM IST	SASE-MUM-POC-GW	172.16.111.3	192.168.4.4	57314	80	tcp	http	Unknown	web	private_ip_addresses	trustworthy	no		allow	policy	Azure-VM-Rule
Sep 29th 2025, 2:16:41 PM IST	SASE-MUM-POC-GW	172.16.111.3	192.168.4.4	57284	80	tcp	http	Unknown	web	private_ip_addresses	trustworthy	no		allow	policy	Azure-VM-Rule
Sep 26th 2025, 1:29:56 PM IST	SASE-MUM-POC-GW	100.72.0.1	192.168.4.4	50755	80	tcp	http	vishnu	web	private_ip_addresses	trustworthy	no		allow	policy	Allow-all-to-Azure

Showing 1 to 5 of 5 entries

Option 3: SASE Gateway Integration with Azure Virtualized Network Appliance (VOS).

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

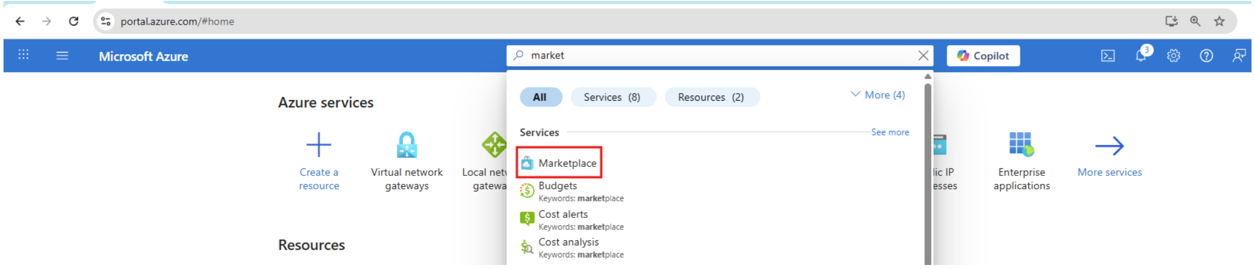
This option can be used when you already have an SD-WAN fabric, and you want to leverage SD-WAN capabilities.



Azure Configuration

Creating an Azure instance

To create a VOS NVA in Azure, search for Marketplace in the search bar and click on “Marketplace” under services.



portal.azure.com/#home

Microsoft Azure

market

Copilot

Azure services

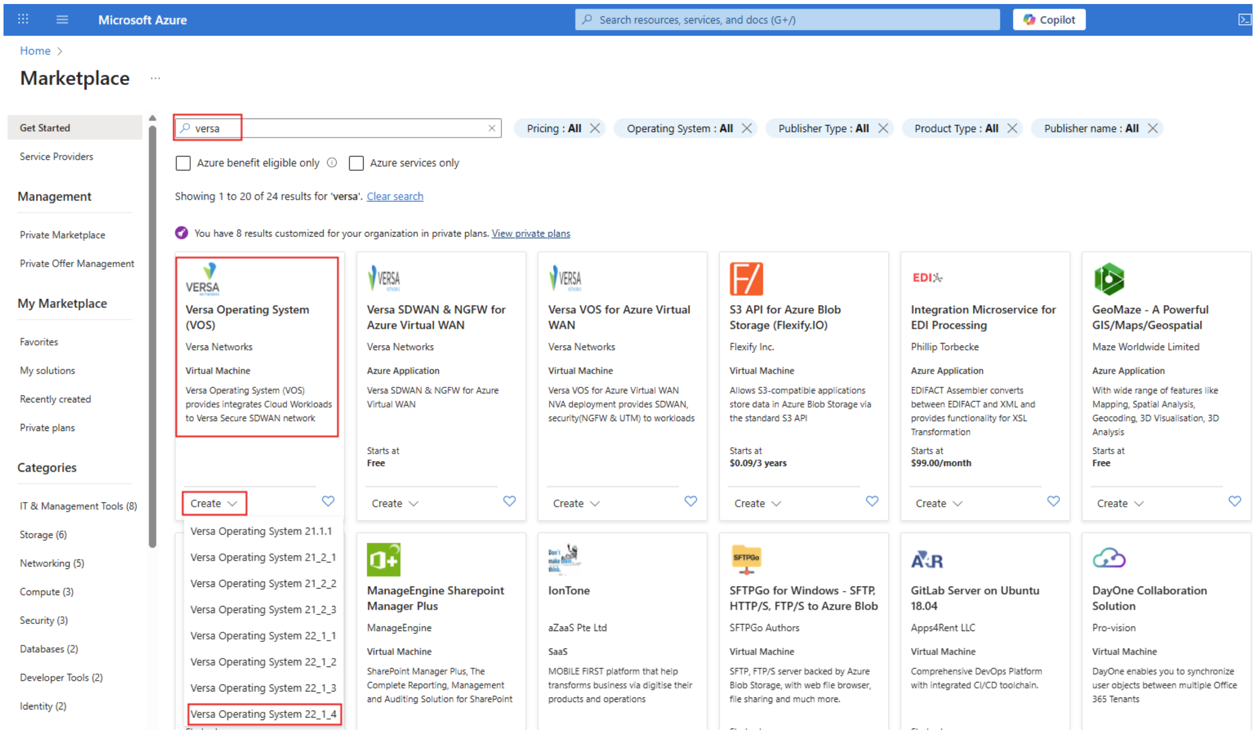
All | Services (8) | Resources (2) | More (4)

Services — See more

- Marketplace
- Budgets
  Keywords: **market**place
- Cost alerts
  Keywords: **market**place
- Cost analysis
  Keywords: **market**place

Resources

In the Market Place search for Versa and choose the VOS version under Create dropdown.



Microsoft Azure

Search resources, services, and docs (G+/)

Copilot

Home >

Marketplace ···

Get Started
Service Providers

Management
Private Marketplace
Private Offer Management

My Marketplace
Favorites
My solutions
Recently created
Private plans

Categories
IT & Management Tools (8)
Storage (6)
Networking (5)
Compute (3)
Security (3)
Databases (2)
Developer Tools (2)
Identity (2)

versa

Pricing : **All** | Operating System : **All** | Publisher Type : **All** | Product Type : **All** | Publisher name : **All**

□ Azure benefit eligible only □ Azure services only

Showing 1 to 20 of 24 results for 'versa'. Clear search

You have 8 results customized for your organization in private plans. View private plans

Versa Operating System (VOS)
Versa Networks
Virtual Machine
Versa Operating System (VOS) provides integrates Cloud Workloads to Versa Secure SDWAN network
Create

- Versa Operating System 21.1.1
- Versa Operating System 21_2_1
- Versa Operating System 21_2_2
- Versa Operating System 21_2_3
- Versa Operating System 22_1_1
- Versa Operating System 22_1_2
- Versa Operating System 22_1_3
- Versa Operating System 22_1_4

Versa SDWAN & NGFW for Azure Virtual WAN
Versa Networks
Azure Application
Versa SDWAN & NGFW for Azure Virtual WAN
Starts at
Free
Create

Versa VOS for Azure Virtual WAN
Versa Networks
Virtual Machine
Versa VOS for Azure Virtual WAN NVA deployment provides SDWAN, security(NGFW & UTM) to workloads
Create

S3 API for Azure Blob Storage (Flexify.IO)
Flexify Inc.
Virtual Machine
Allows S3-compatible applications store data in Azure Blob Storage via the standard S3 API
Starts at
$0.09/3 years
Create

Integration Microservice for EDI Processing
Phillip Torbecke
Azure Application
EDIFACT Assembler converts between EDIFACT and XML and provides functionality for XSL Transformation
Starts at
$99.00/month
Create

GeoMaze - A Powerful GIS/Maps/Geospatial
Maze Worldwide Limited
Azure Application
With wide range of features like Mapping, Spatial Analysis, Geocoding, 3D Visualisation, 3D Analysis
Starts at
Free
Create

ManageEngine Sharepoint Manager Plus
ManageEngine
Virtual Machine
SharePoint Manager Plus, The Complete Reporting, Management and Auditing Solution for SharePoint

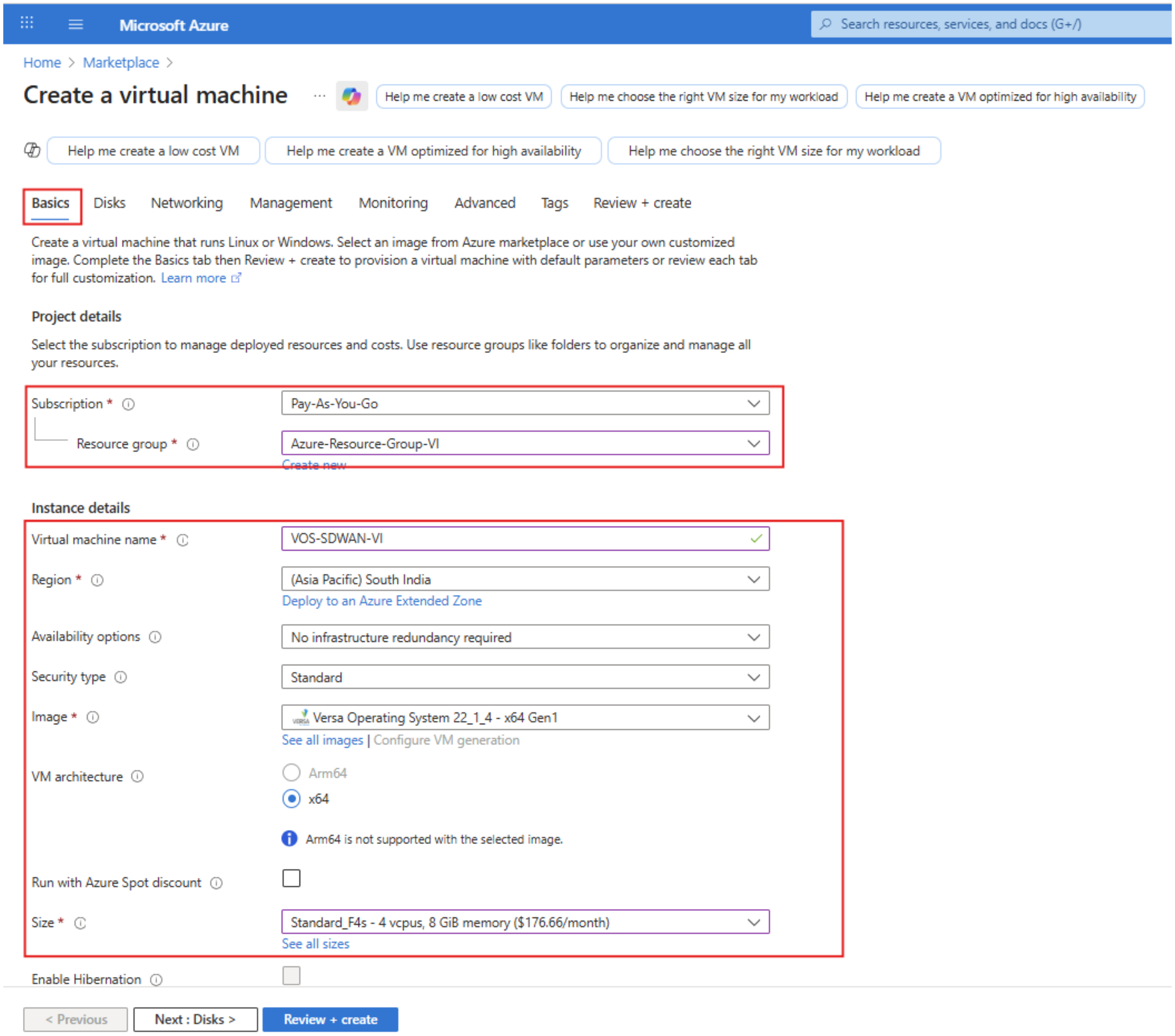
IonTone
aZaaS Pte Ltd
SaaS
MOBILE FIRST platform that help transforms business via digitise their products and operations

SFTPGo for Windows - SFTP, HTTP/S, FTP/S to Azure Blob
SFTPGo Authors
Virtual Machine
SFTP, FTP/S server backed by Azure Blob Storage, with web file browser, file sharing and much more.

GitLab Server on Ubuntu 18.04
Apps4Rent LLC
Virtual Machine
Comprehensive DevOps Platform with integrated CI/CD toolchain.

DayOne Collaboration Solution
Pro-vision
Virtual Machine
DayOne enables you to synchronize user objects between multiple Office 365 Tenants

Under Basic Tab, Provide the resource group, VM name, region and size as per the requirement.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Marketplace >

Create a virtual machine

Help me create a low cost VM
Help me choose the right VM size for my workload
Help me create a VM optimized for high availability
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Basics
Disks
Networking
Management
Monitoring
Advanced
Tags
Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Pay-As-You-Go

Resource group * : Azure-Resource-Group-VI

Create new

Instance details

Virtual machine name * : VOS-SDWAN-VI

Region * : (Asia Pacific) South India

Deploy to an Azure Extended Zone

Availability options : No infrastructure redundancy required

Security type : Standard

Image * : Versa Operating System 22_1_4 - x64 Gen1

See all images | Configure VM generation

VM architecture : ○ Arm64 ● x64

Arm64 is not supported with the selected image.

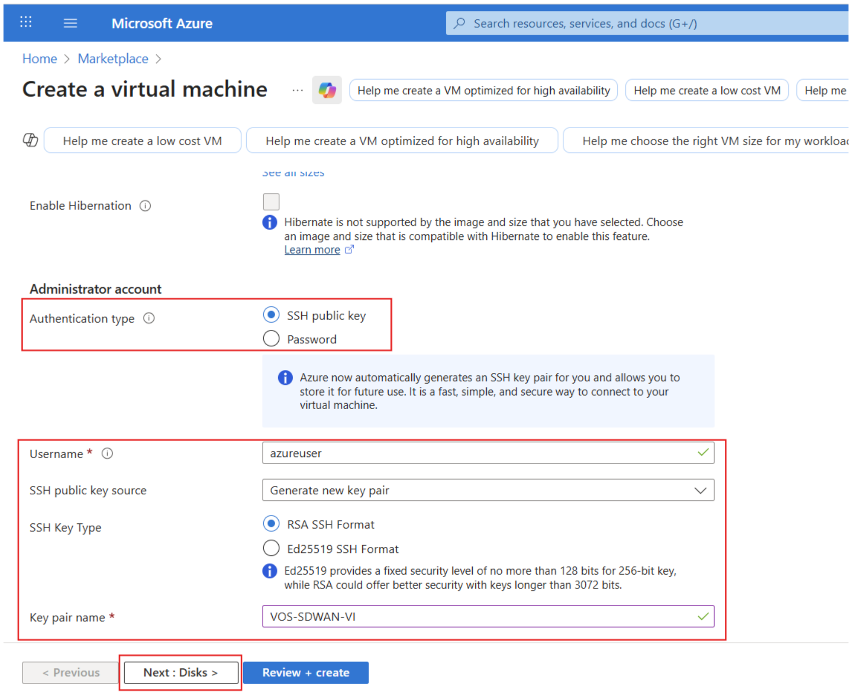
Run with Azure Spot discount : □

Size * : Standard_F4s - 4 vcpus, 8 GiB memory ($176.66/month)

See all sizes

Enable Hibernation : □

Under Administrator account, provide the Authentication type as “SSH public key”, username, SSH public key source as “Generate new key pair” , SSH key Type as “RSA SSH Format” , the key pair name and click on “Next: Disks>”.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Marketplace >
Create a virtual machine
Help me create a VM optimized for high availability
Help me create a low cost VM
Help me
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
See all sizes

Enable Hibernation ⓘ □

Hibernate is not supported by the image and size that you have selected. Choose an image and size that is compatible with Hibernate to enable this feature. Learn more

Administrator account

Authentication type ⓘ ● SSH public key ○ Password

Azure now automatically generates an SSH key pair for you and allows you to store it for future use. It is a fast, simple, and secure way to connect to your virtual machine.

Username * ⓘ azureuser

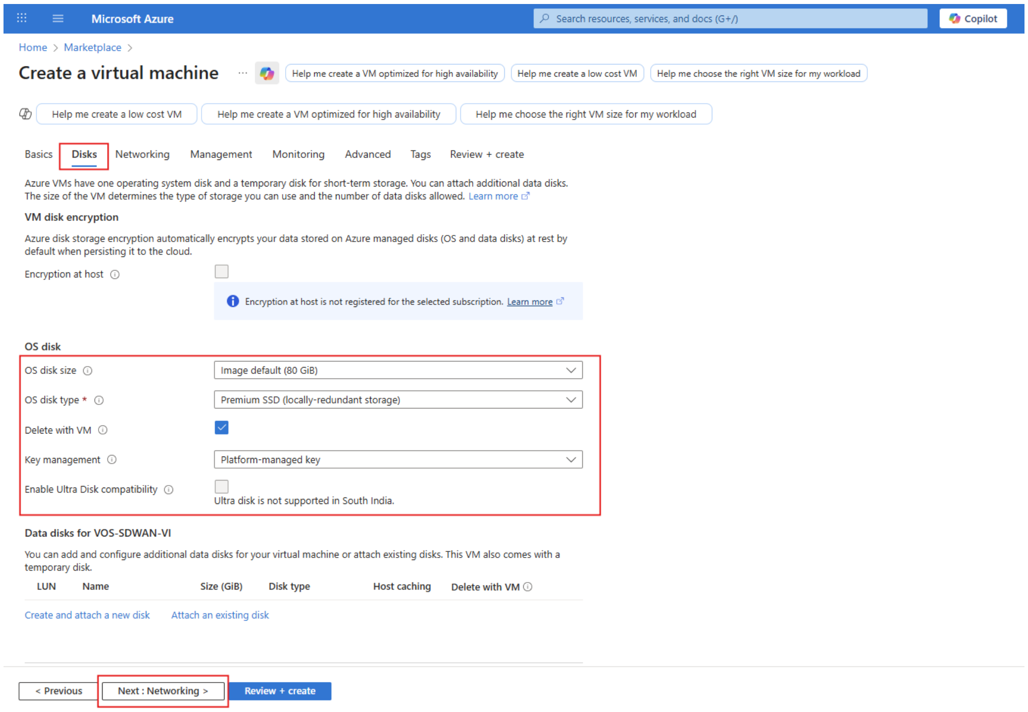
SSH public key source: Generate new key pair

SSH Key Type: ● RSA SSH Format ○ Ed25519 SSH Format

Ed25519 provides a fixed security level of no more than 128 bits for 256-bit key, while RSA could offer better security with keys longer than 3072 bits.

Key pair name * VOS-SDWAN-VI

Under “Disks” configure the OS disk size, type as per the requirement and click “Next: Networking >.



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Marketplace >
Create a virtual machine
Help me create a VM optimized for high availability
Help me create a low cost VM
Help me choose the right VM size for my workload
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Basics
Disks
Networking
Management
Monitoring
Advanced
Tags
Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. Learn more

VM disk encryption

Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.

Encryption at host ⓘ □

Encryption at host is not registered for the selected subscription. Learn more

OS disk

OS disk size ⓘ Image default (80 GiB)

OS disk type * ⓘ Premium SSD (locally-redundant storage)

Delete with VM ⓘ ☑

Key management ⓘ Platform-managed key

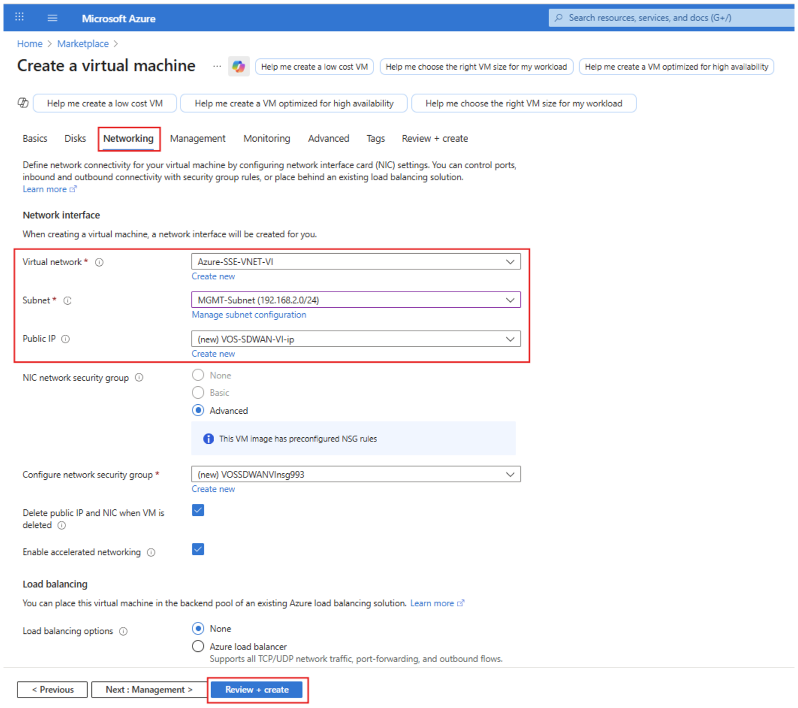
Enable Ultra Disk compatibility ⓘ □ Ultra disk is not supported in South India.

Data disks for VOS-SDWAN-VI

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching	Delete with VM ⓘ

Under “Networking” tab provide the Virtual Network, subnet and leave the rest to default. and Click review +create.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Marketplace >
Help me create a low cost VM
Help me choose the right VM size for my workload
Help me create a VM optimized for high availability
Basics
Disks
Networking
Management
Monitoring
Advanced
Tags
Review + create
< Previous
Next : Management >
Review + create

Create a virtual machine

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.
Learn more

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * : Azure-SSE-VNET-VI (Create new)

Subnet * : MGMT-Subnet (192.168.2.0/24) (Manage subnet configuration)

Public IP : (new) VOS-SDWAN-VI-ip (Create new)

NIC network security group: ○ None ○ Basic ● Advanced

This VM image has preconfigured NSG rules

Configure network security group * : (new) VOSSDWANVInsg993 (Create new)

Delete public IP and NIC when VM is deleted ☑

Enable accelerated networking ☑

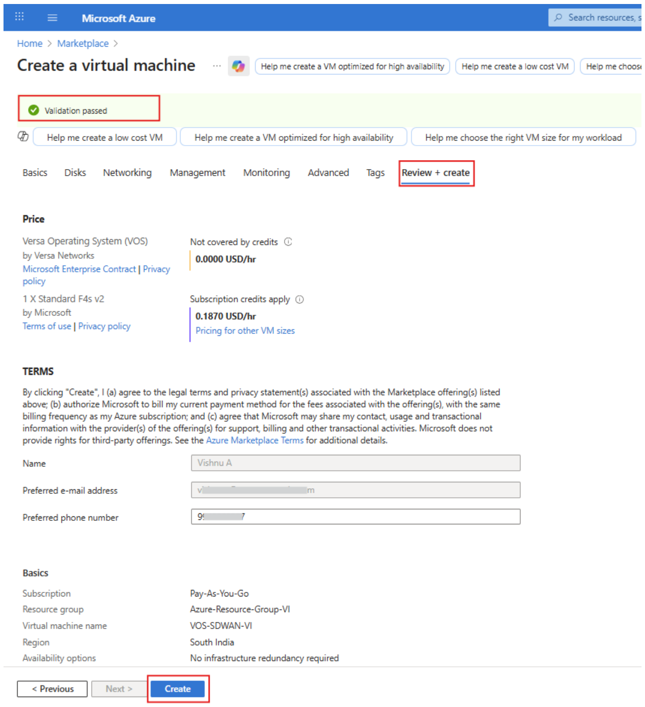
Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more

Load balancing options: ● None ○ Azure load balancer

Supports all TCP/UDP network traffic, port-forwarding, and outbound flows.

Once the validation is passed, click on “Create”.


Microsoft Azure
Search resources, s
Home > Marketplace >
Help me create a VM optimized for high availability
Help me create a low cost VM
Help me choose
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Basics
Disks
Networking
Management
Monitoring
Advanced
Tags
Review + create
< Previous
Next >
Create

Create a virtual machine

Validation passed

Price

Versa Operating System (VOS)
by Versa Networks
Microsoft Enterprise Contract | Privacy policy

Not covered by credits
0.0000 USD/hr

1 X Standard F4s v2
by Microsoft
Terms of use | Privacy policy

Subscription credits apply
0.1870 USD/hr
Pricing for other VM sizes

TERMS

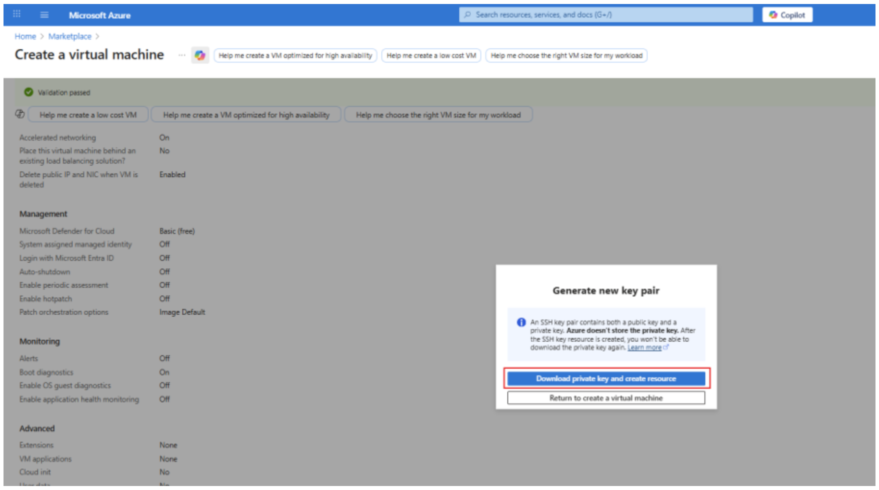
By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.

Name	Vishnu A
Preferred e-mail address	[redacted]
Preferred phone number	[redacted]

Basics

Subscription	Pay-As-You-Go
Resource group	Azure-Resource-Group-VI
Virtual machine name	VOS-SDWAN-VI
Region	South India
Availability options	No infrastructure redundancy required

In “Generate new key pair” click on “Download private key and create resource”.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Marketplace >
Help me create a VM optimized for high availability
Help me create a low cost VM
Help me choose the right VM size for my workload
Download private key and create resource
Return to create a virtual machine

Create a virtual machine

Validation passed

Accelerated networking On
Place this virtual machine behind an existing load balancing solution? No
Delete public IP and NIC when VM is deleted Enabled

Management
Microsoft Defender for Cloud Basic (free)
System assigned managed identity Off
Login with Microsoft Entra ID Off
Auto-shutdown Off
Enable periodic assessment Off
Enable hotpatch Off
Patch orchestration options Image Default

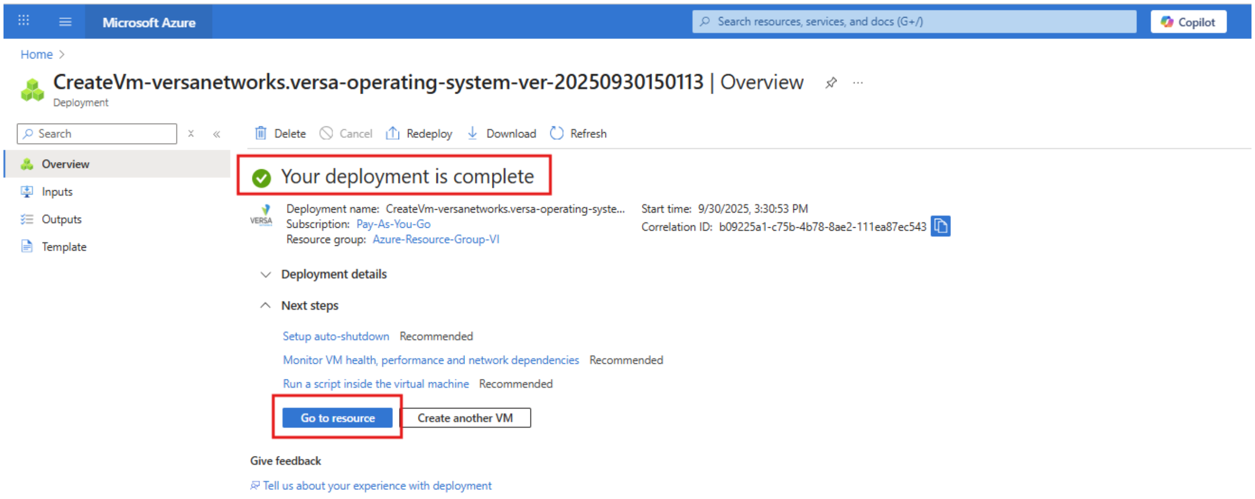
Monitoring
Alerts Off
Boot diagnostics On
Enable OS guest diagnostics Off
Enable application health monitoring Off

Advanced
Extensions None
VM applications None
Cloud init No

Generate new key pair

An SSH key pair contains both a public key and a private key. **Azure doesn't store the private key.** After the SSH key resource is created, you won't be able to download the private key again. Learn more

Deployment status can be viewed under Overview tab. Once it is complete click on “Go to resource”.



CreateVm-versanetworks.versa-operating-system-ver-20250930150113 | Overview
Deployment

Your deployment is complete

Deployment name: CreateVm-versanetworks.versa-operating-syste...
Subscription: Pay-As-You-Go
Resource group: Azure-Resource-Group-VI
Start time: 9/30/2025, 3:30:53 PM
Correlation ID: b09225a1-c75b-4b78-8ae2-111ea87ec543

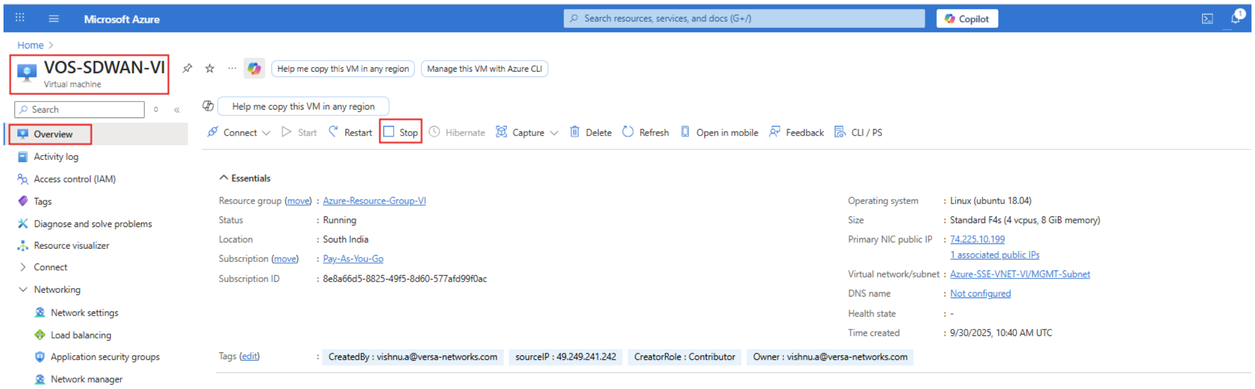
Deployment details

Next steps

Setup auto-shutdown Recommended
Monitor VM health, performance and network dependencies Recommended
Run a script inside the virtual machine Recommended

Give feedback
Tell us about your experience with deployment

To add LAN and WAN interfaces to VOS, we must stop the VM.



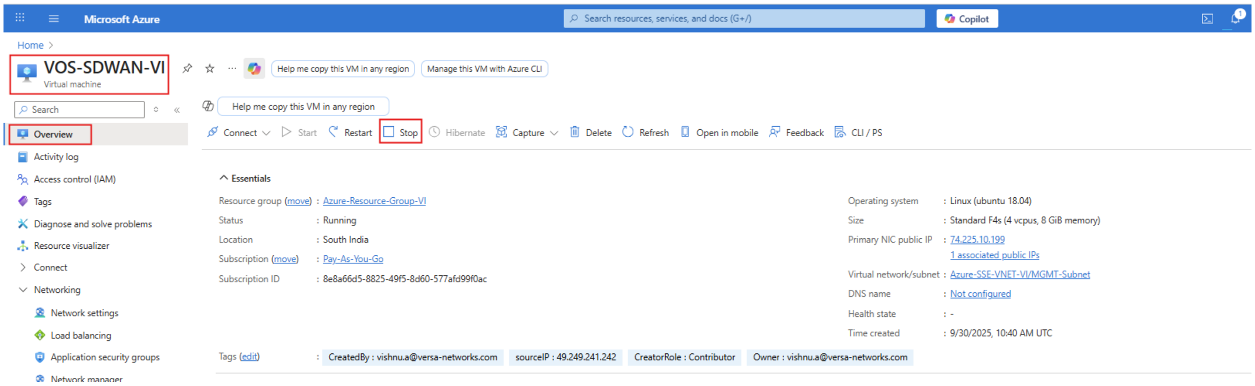
VOS-SDWAN-VI
Virtual machine

Essentials

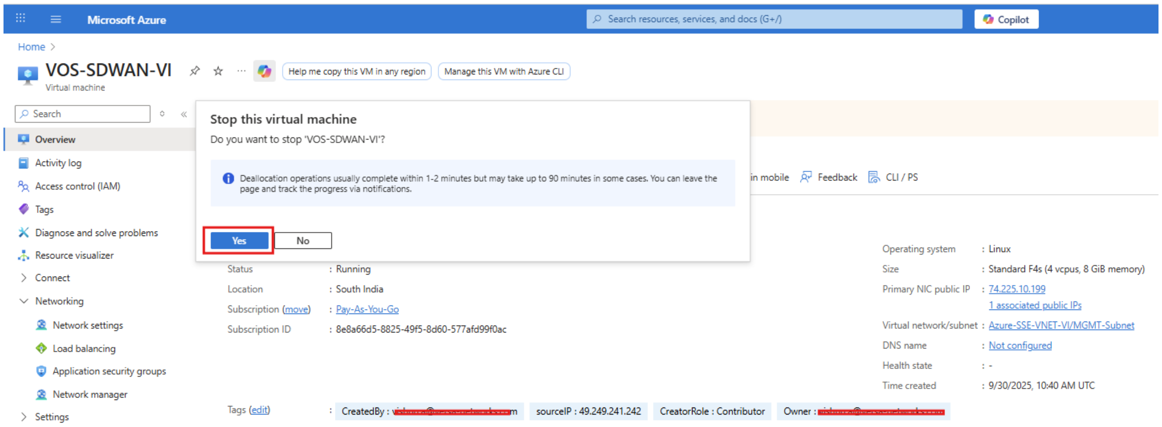
Resource group (move) : Azure-Resource-Group-VI
Status : Running
Location : South India
Subscription (move) : Pay-As-You-Go
Subscription ID : 8e8a66d5-8825-49f5-8d60-577afd99f0ac

Operating system : Linux (ubuntu 18.04)
Size : Standard F4s (4 vcpus, 8 GiB memory)
Primary NIC public IP : 74.225.10.199
1 associated public IPs
Virtual network/subnet : Azure-SSE-VNET-VI/MGMT-Subnet
DNS name : Not configured
Health state : -
Time created : 9/30/2025, 10:40 AM UTC

Tags (edit) : CreatedBy : vishnu.a@versa-networks.com sourceIP : 49.249.241.242 CreatorRole : Contributor Owner : vishnu.a@versa-networks.com



Resource group (move) : Azure-Resource-Group-VI
Status : Running
Location : South India
Subscription (move) : Pay-As-You-Go
Subscription ID : 8e8a66d5-8825-49f5-8d60-577afd99f0ac
Operating system : Linux (ubuntu 18.04)
Size : Standard F4s (4 vcpus, 8 GiB memory)
Primary NIC public IP : 74.225.10.199
1 associated public IPs
Virtual network/subnet : Azure-SSE-VNET-VI/MGMT-Subnet
DNS name : Not configured
Health state : -
Time created : 9/30/2025, 10:40 AM UTC
Tags (edit) : CreatedBy : vishnu.a@versa-networks.com | sourceIP : 49.249.241.242 | CreatorRole : Contributor | Owner : vishnu.a@versa-networks.com



Stop this virtual machine

Do you want to stop 'VOS-SDWAN-VI'?

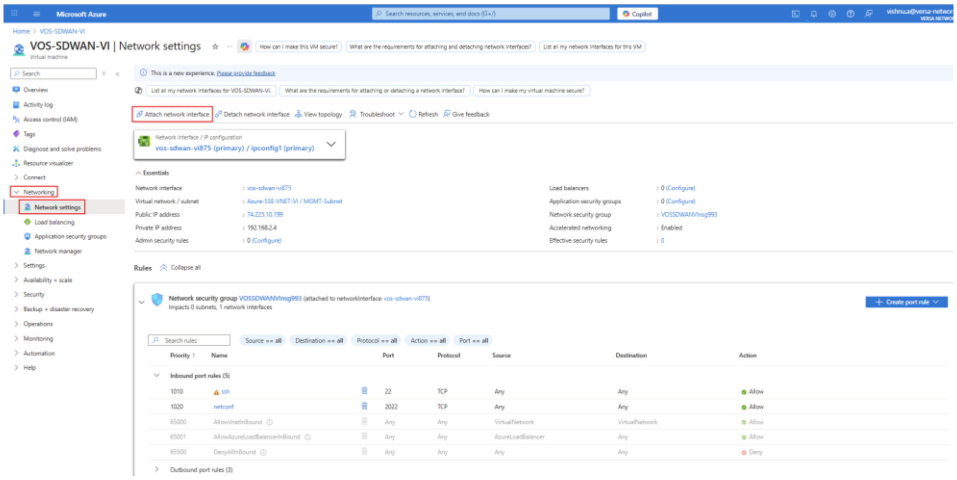
Deallocation operations usually complete within 1-2 minutes but may take up to 90 minutes in some cases. You can leave the page and track the progress via notifications.

Yes | No

Status : Running
Location : South India
Subscription (move) : Pay-As-You-Go
Subscription ID : 8e8a66d5-8825-49f5-8d60-577afd99f0ac
Operating system : Linux
Size : Standard F4s (4 vcpus, 8 GiB memory)
Primary NIC public IP : 74.225.10.199
1 associated public IPs
Virtual network/subnet : Azure-SSE-VNET-VI/MGMT-Subnet
DNS name : Not configured
Health state : -
Time created : 9/30/2025, 10:40 AM UTC
Tags (edit) : CreatedBy : [redacted] | sourceIP : 49.249.241.242 | CreatorRole : Contributor | Owner : [redacted]

Adding WAN and LAN interfaces:

To add WAN network interfaces, under Networking click on “Network settings” → “Attach network interface”.

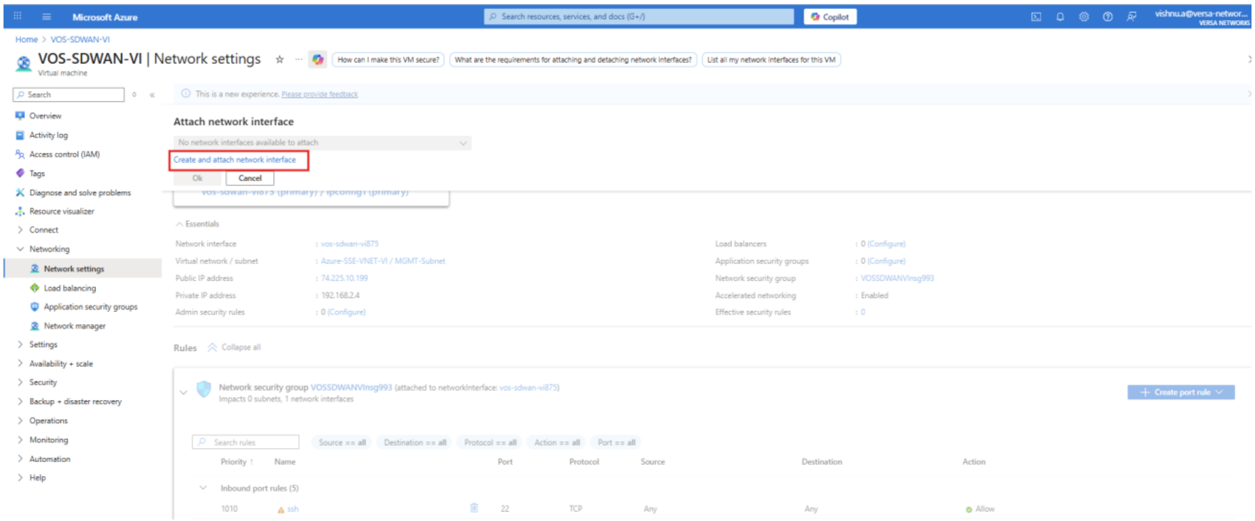

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
vishnu.a@versa-networ
VERSA NETWOR
Home > VOS-SDWAN-VI
VOS-SDWAN-VI | Network settings
Virtual machine
How can I make this VM secure?
What are the requirements for attaching and detaching network interfaces?
List all my network interfaces for this VM
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Networking
Network settings
Load balancing
Application security groups
Network manager
Settings
Availability + scale
Security
Backup + disaster recovery
Operations
Monitoring
Automation
Help
This is a new experience. Please provide feedback
List all my network interfaces for VOS-SDWAN-VI.
What are the requirements for attaching or detaching a network interface?
How can I make my virtual machine secure?
Attach network interface
Detach network interface
View topology
Troubleshoot
Refresh
Give feedback
Network interface / IP configuration
vos-sdwan-vi875 (primary) / ipconfig1 (primary)
Essentials
Rules
Collapse all
Create port rule
Search rules
Source == all
Destination == all
Protocol == all
Action == all
Port == all

Network interface : vos-sdwan-vi875
Virtual network / subnet : Azure-SSE-VNET-VI / MGMT-Subnet
Public IP address : 74.225.10.199
Private IP address : 192.168.2.4
Admin security rules : 0 (Configure)
Load balancers : 0 (Configure)
Application security groups : 0 (Configure)
Network security group : VOSSDWANVInsg993
Accelerated networking : Enabled
Effective security rules : 0

Network security group VOSSDWANVInsg993 (attached to networkInterface: vos-sdwan-vi875)
Impacts 0 subnets, 1 network interfaces

Priority ↑	Name	Port	Protocol	Source	Destination	Action
Inbound port rules (5)						
1010	ssh	22	TCP	Any	Any	Allow
1020	netconf	2022	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound port rules (3)						

Click on “Create and attach network interface” .



VOS-SDWAN-VI | Network settings
Virtual machine

Attach network interface

No network interfaces available to attach

Create and attach network interface

Ok   Cancel

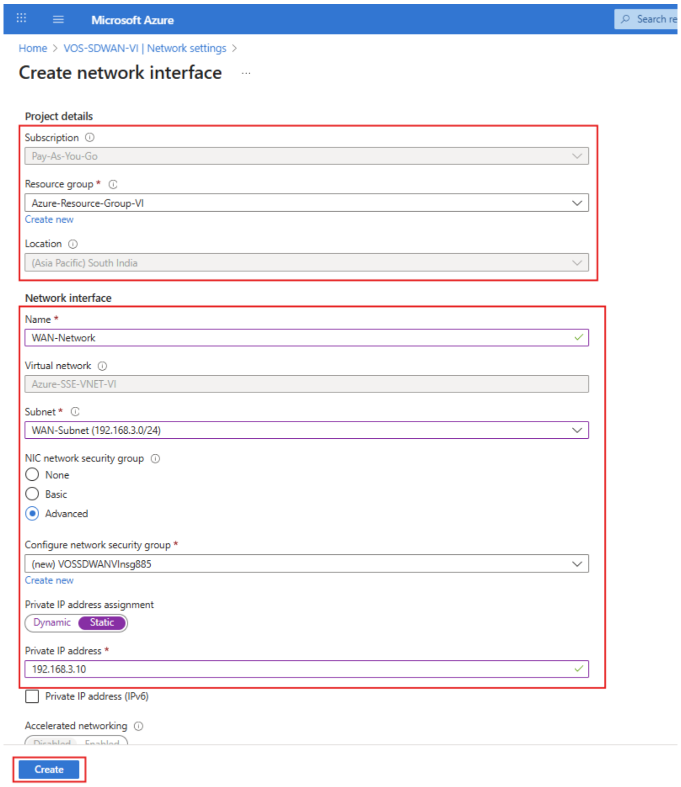
Essentials

Network interface	: vos-sdwan-vi875	Load balancers	: 0 (Configure)
Virtual network / subnet	: Azure-SSE-VNET-VI / MGMT-Subnet	Application security groups	: 0 (Configure)
Public IP address	: 74.225.10.199	Network security group	: VOSSDWANVInsg993
Private IP address	: 192.168.2.4	Accelerated networking	: Enabled
Admin security rules	: 0 (Configure)	Effective security rules	: 0

Network security group VOSSDWANVInsg993 (attached to networkInterface: vos-sdwan-vi875)
Impacts 0 subnets, 1 network interfaces

Priority ↑	Name	Port	Protocol	Source	Destination	Action
Inbound port rules (5)						
1010	ssh	22	TCP	Any	Any	Allow

Under “Create Network interface” , provide the Resource group, Name of the network interface, select WAN-subnet from the Subnet dropdown, NSG, under Private IP address select “Static” and give the IP from WAN Subnet and click on “Create”.



Create network interface

Project details

Subscription: Pay-As-You-Go

Resource group *: Azure-Resource-Group-VI
Create new

Location: (Asia Pacific) South India

Network interface

Name *: WAN-Network

Virtual network: Azure-SSE-VNET-VI

Subnet *: WAN-Subnet (192.168.3.0/24)

NIC network security group
○ None
○ Basic
● Advanced

Configure network security group *: (new) VOSSDWANVInsg885
Create new

Private IP address assignment: Dynamic [✓ Static]

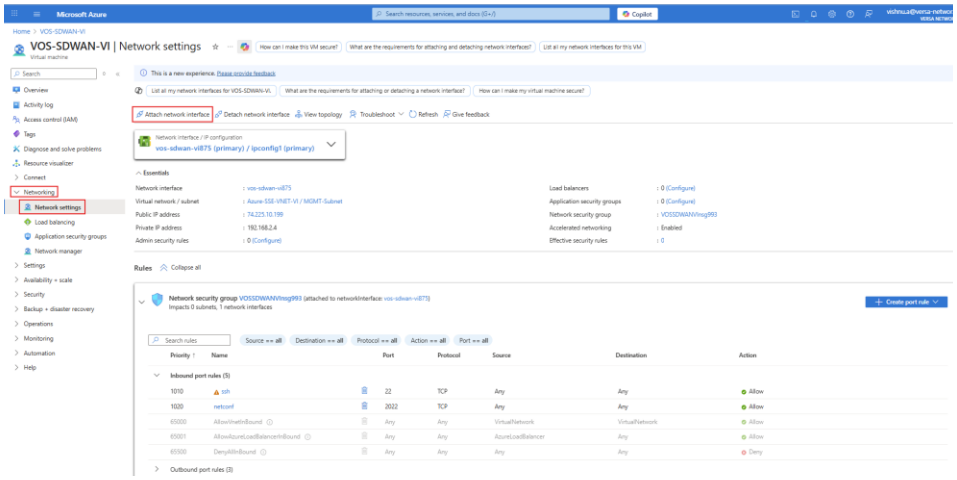
Private IP address *: 192.168.3.10

□ Private IP address (IPv6)

Accelerated networking: Disabled Enabled

Create

To add LAN network interfaces, under Networking click on “Network settings” → “Attach network interface”.



Network interface / IP configuration: vos-sdwan-vi875 (primary) / ipconfig1 (primary)

Essentials

Network interface	: vos-sdwan-vi875	Load balancers	: 0 (Configure)
Virtual network / subnet	: Azure-SSE-VNET-VI / MGMT-Subnet	Application security groups	: 0 (Configure)
Public IP address	: 74.225.10.199	Network security group	: VOSSDWANVInsg993
Private IP address	: 192.168.2.4	Accelerated networking	: Enabled
Admin security rules	: 0 (Configure)	Effective security rules	: 0

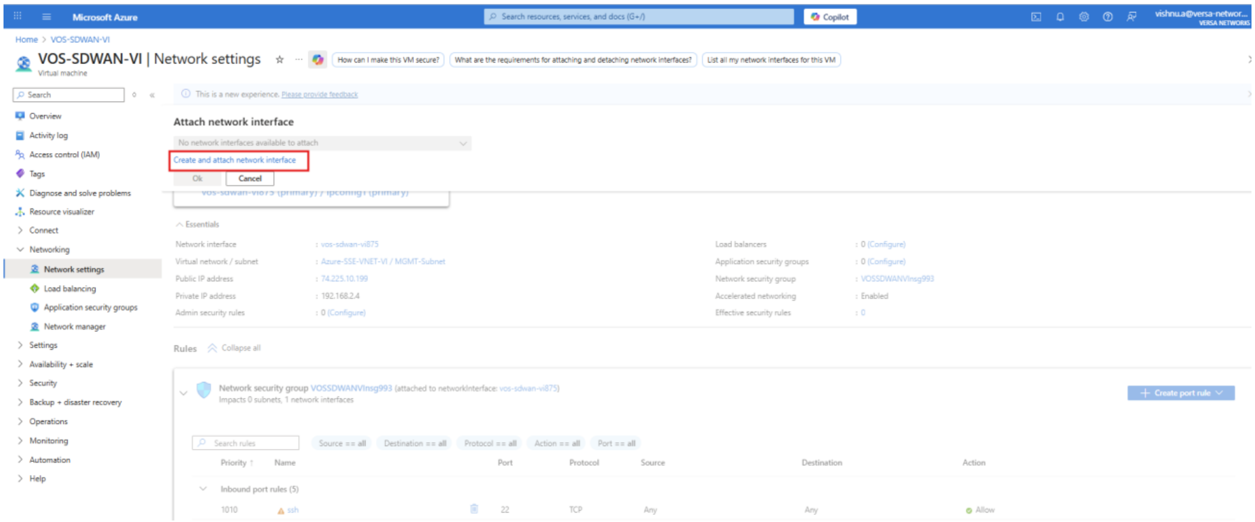
Rules

Network security group VOSSDWANVInsg993 (attached to networkInterface: vos-sdwan-vi875)
Impacts 0 subnets, 1 network interfaces

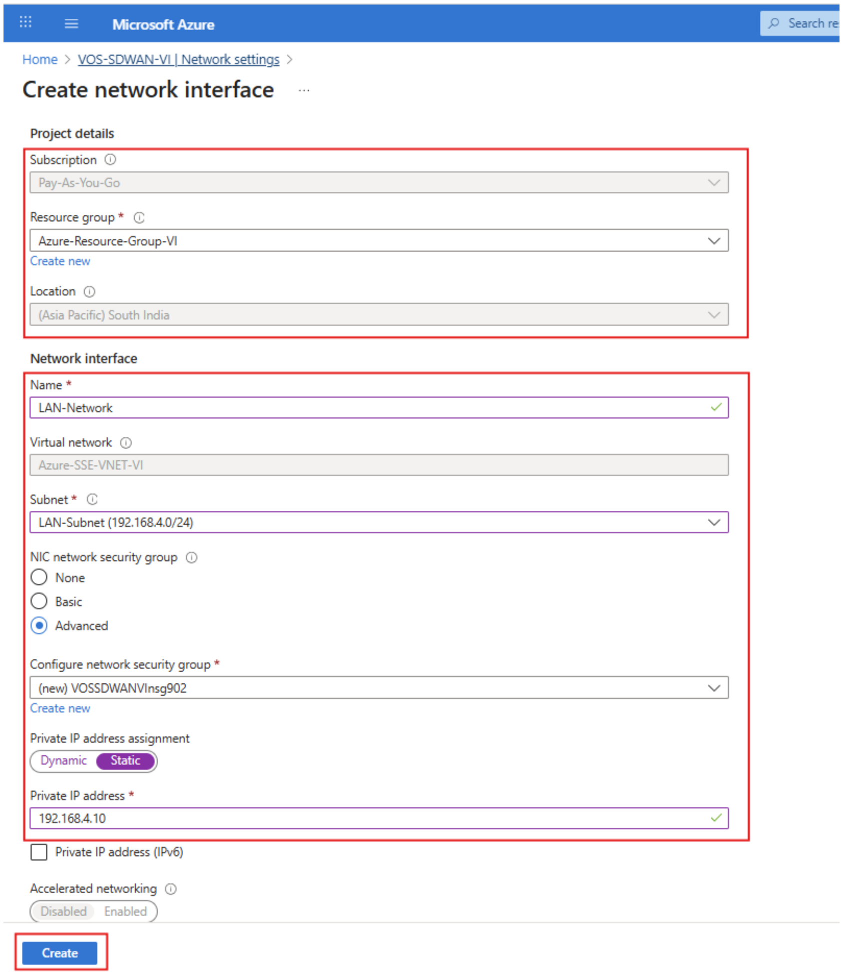
Source == all · Destination == all · Protocol == all · Action == all · Port == all

Priority ↑	Name	Port	Protocol	Source	Destination	Action
Inbound port rules (5)						
1010	ssh	22	TCP	Any	Any	Allow
1020	netconf	2022	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound port rules (3)						

Click on “Create and attach network interface” .


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
vishnu.a@versa-networ...
VERSA NETWORKS
Home > VOS-SDWAN-VI
VOS-SDWAN-VI | Network settings
Virtual machine
How can I make this VM secure?
What are the requirements for attaching and detaching network interfaces?
List all my network interfaces for this VM
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Networking
Network settings
Load balancing
Application security groups
Network manager
Settings
Availability + scale
Security
Backup + disaster recovery
Operations
Monitoring
Automation
Help
This is a new experience. Please provide feedback
Attach network interface
No network interfaces available to attach
Create and attach network interface
Ok
Cancel
Create port rule

Under “Create Network interface” , provide the Resource group, Name of the network interface, select WAN-subnet from the Subnet dropdown, NSG under Private IP address select “Static” and give the IP from LAN Subnet and click on “Create”.



Home > VOS-SDWAN-VI | Network settings >

Create network interface

Project details

Subscription: Pay-As-You-Go

Resource group *: Azure-Resource-Group-VI

Create new

Location: (Asia Pacific) South India

Network interface

Name *: LAN-Network

Virtual network: Azure-SSE-VNET-VI

Subnet *: LAN-Subnet (192.168.4.0/24)

NIC network security group

○ None
○ Basic
● Advanced

Configure network security group *: (new) VOSSDWANVInsg902

Create new

Private IP address assignment: Dynamic [✓ Static]

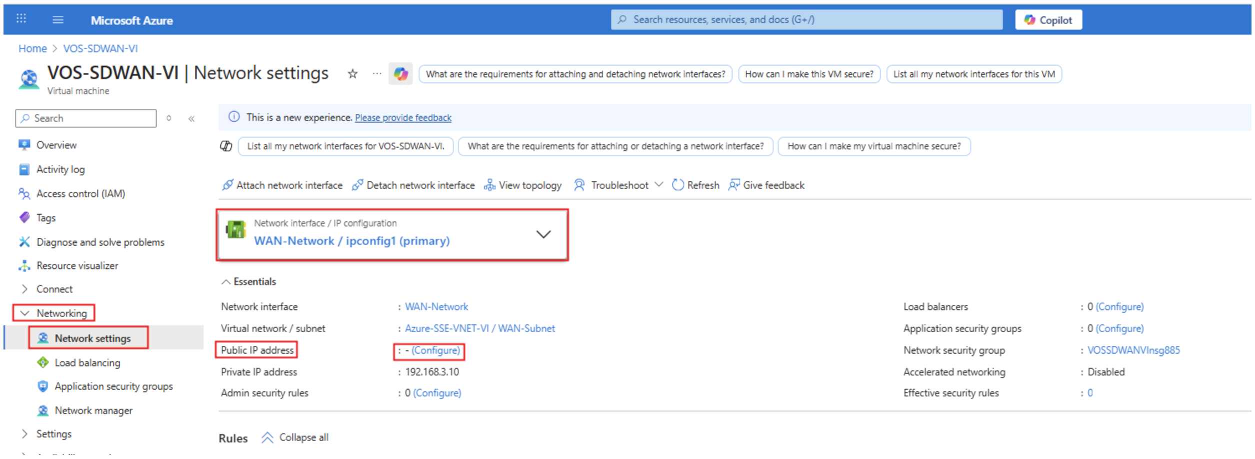
Private IP address *: 192.168.4.10

□ Private IP address (IPv6)

Accelerated networking: Disabled Enabled

Configure the Public IP address for WAN interface:

To Configure Public IP on the WAN interface, Navigate to Virtual Machine → Networking → Network settings → WAN interface and click on "Configure" under Public IP address.



Home > VOS-SDWAN-VI

VOS-SDWAN-VI | Network settings

Virtual machine

This is a new experience. Please provide feedback

Network interface / IP configuration: WAN-Network / ipconfig1 (primary)

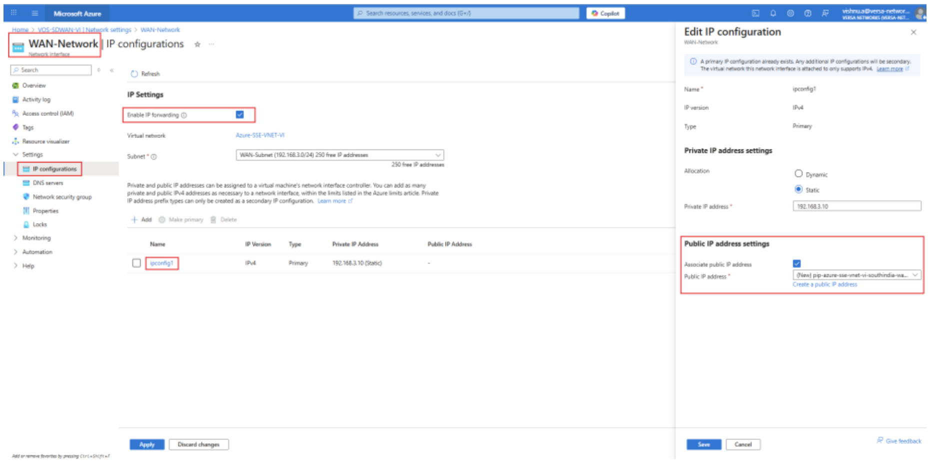
Essentials

Network interface	: WAN-Network	Load balancers	: 0 (Configure)
Virtual network / subnet	: Azure-SSE-VNET-VI / WAN-Subnet	Application security groups	: 0 (Configure)
Public IP address	: - (Configure)	Network security group	: VOSSDWANVInsg885
Private IP address	: 192.168.3.10	Accelerated networking	: Disabled
Admin security rules	: 0 (Configure)	Effective security rules	: 0

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
What are the requirements for attaching and detaching network interfaces?
How can I make this VM secure?
List all my network interfaces for this VM
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Networking
Network settings
Load balancing
Application security groups
Network manager
Settings
List all my network interfaces for VOS-SDWAN-VI.
What are the requirements for attaching or detaching a network interface?
How can I make my virtual machine secure?
Attach network interface
Detach network interface
View topology
Troubleshoot
Refresh
Give feedback
Rules
Collapse all

Under "Settings" → IP configuration → IP settings, enable IP Forwarding, select ipconfig1, this will open "Edit IP configuration" window. Select the "Associate public IP addresses" check box and click on "save".

Note: Enabling IP forwarding allows the virtual machine on this network interface to act as a router and receive traffic addressed to other destinations.



IP Settings

Enable IP forwarding ⓘ ☑

Virtual network: Azure-SSE-VNET-VI

Subnet * ⓘ: WAN-Subnet (192.168.3.0/24) 250 free IP addresses — 250 free IP addresses

Private and public IP addresses can be assigned to a virtual machine's network interface controller. You can add as many private and public IPv4 addresses as necessary to a network interface, within the limits listed in the Azure limits article. Private IP address prefix types can only be created as a secondary IP configuration. Learn more

	Name	IP Version	Type	Private IP Address	Public IP Address
□	ipconfig1	IPv4	Primary	192.168.3.10 (Static)	-

Edit IP configuration
WAN-Network

ⓘ A primary IP configuration already exists. Any additional IP configurations will be secondary. The virtual network this network interface is attached to only supports IPv4. Learn more

Name *: ipconfig1
IP version: IPv4
Type: Primary

Private IP address settings

Allocation: ○ Dynamic ● Static

Private IP address *: 192.168.3.10

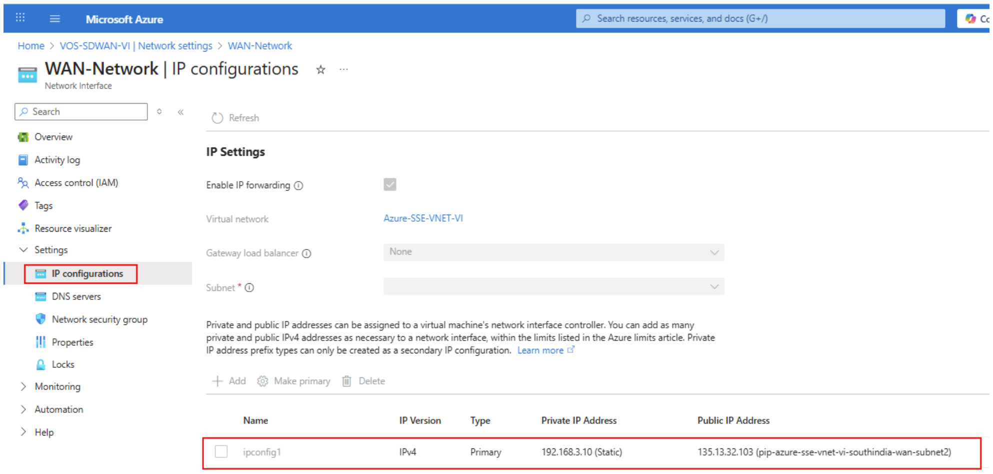
Public IP address settings

Associate public IP address ☑

Public IP address *: (New) pip-azure-sse-vnet-vi-southindia-wa...

Create a public IP address

After saving, we can see the public IP address assigned to the WAN Interface.



IP Settings

Enable IP forwarding ⓘ ☑

Virtual network: Azure-SSE-VNET-VI

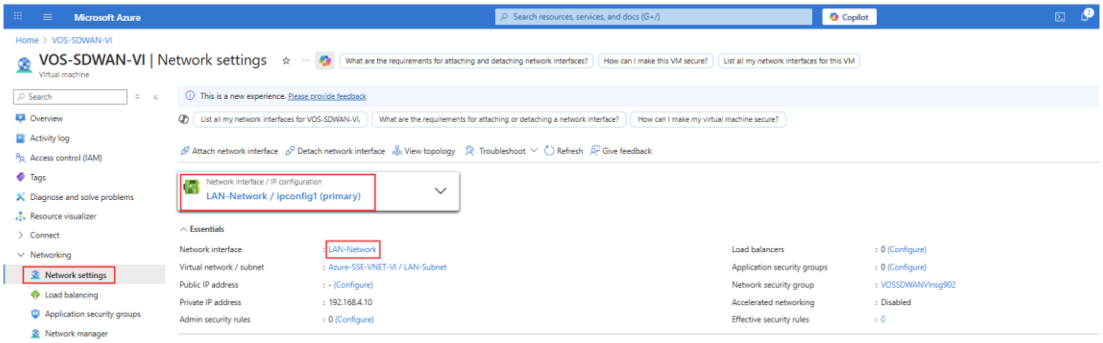
Gateway load balancer ⓘ: None

Subnet * ⓘ:

Private and public IP addresses can be assigned to a virtual machine's network interface controller. You can add as many private and public IPv4 addresses as necessary to a network interface, within the limits listed in the Azure limits article. Private IP address prefix types can only be created as a secondary IP configuration. Learn more

	Name	IP Version	Type	Private IP Address	Public IP Address
□	ipconfig1	IPv4	Primary	192.168.3.10 (Static)	135.13.32.103 (pip-azure-sse-vnet-vi-southindia-wan-subnet2)

Similarly, Enable the IP forwarding in the LAN interface by Navigating to Virtual Machine → Networking → Network settings → LAN interface and click on Network interface.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > VOS-SDWAN-VI
VOS-SDWAN-VI | Network settings
Virtual machine
What are the requirements for attaching and detaching network interfaces?
How can I make this VM secure?
List all my network interfaces for this VM
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Networking
Network settings
Load balancing
Application security groups
Network manager
List all my network interfaces for VOS-SDWAN-VI.
What are the requirements for attaching or detaching a network interface?
How can I make my virtual machine secure?
Attach network interface
Detach network interface
View topology
Troubleshoot
Refresh
Give feedback

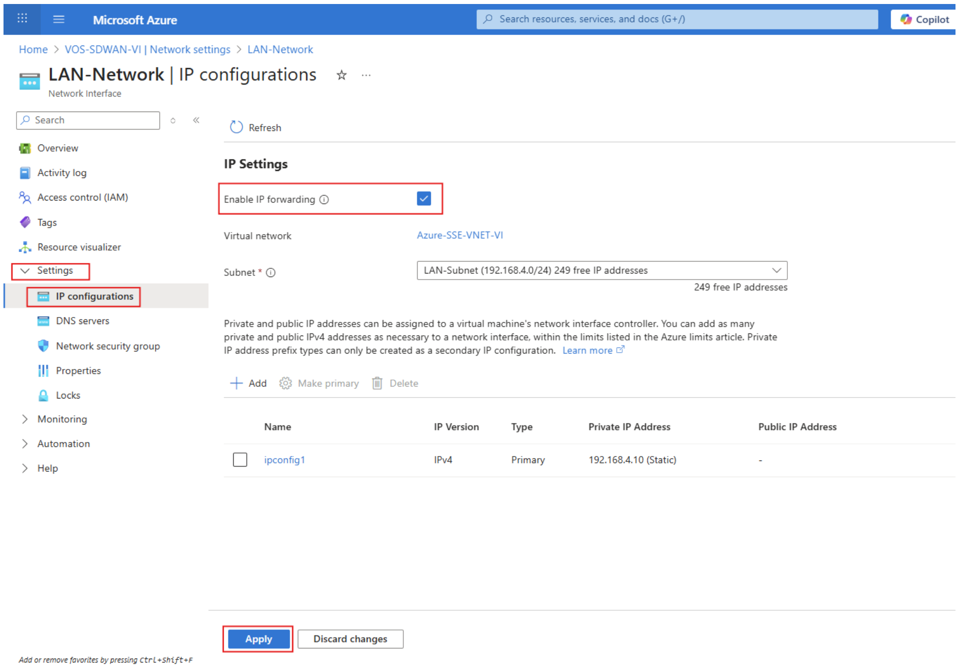
ⓘ This is a new experience. Please provide feedback

Network interface / IP configuration
LAN-Network / ipconfig1 (primary)

Essentials

Network interface	: LAN-Network	Load balancers	: 0 (Configure)
Virtual network / subnet	: Azure-SSE-VNET-VI / LAN-Subnet	Application security groups	: 0 (Configure)
Public IP address	: - (Configure)	Network security group	: VOSSDWANVInsg902
Private IP address	: 192.168.4.10	Accelerated networking	: Disabled
Admin security rules	: 0 (Configure)	Effective security rules	: 0

Under “Settings” → IP configuration → IP settings, enable IP Forwarding and click on “Apply”.



Home > VOS-SDWAN-VI | Network settings > LAN-Network

LAN-Network | IP configurations

Network Interface

IP Settings

Enable IP forwarding ☑

Virtual network: Azure-SSE-VNET-VI

Subnet *: LAN-Subnet (192.168.4.0/24) 249 free IP addresses

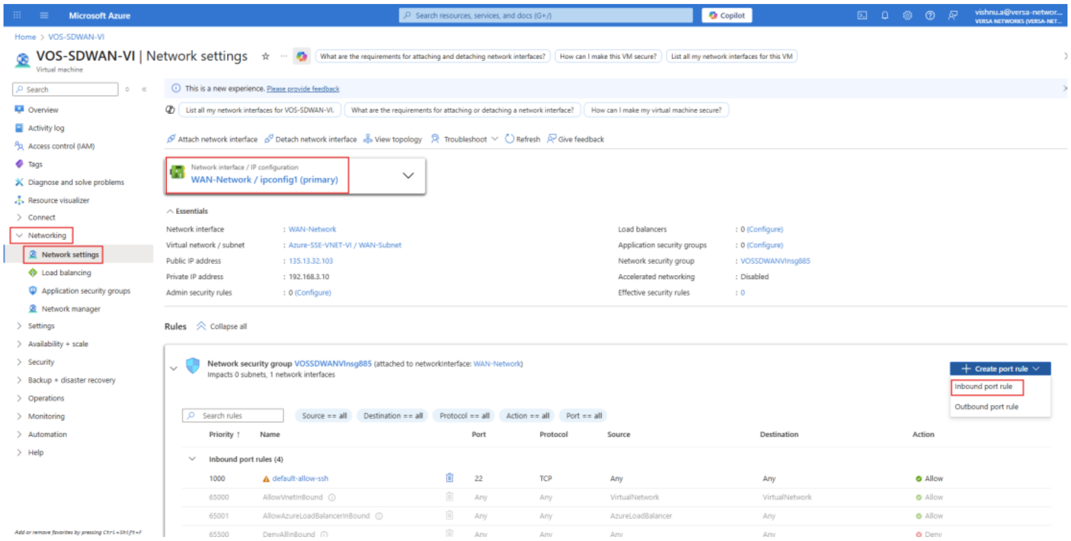
249 free IP addresses

Private and public IP addresses can be assigned to a virtual machine's network interface controller. You can add as many private and public IPv4 addresses as necessary to a network interface, within the limits listed in the Azure limits article. Private IP address prefix types can only be created as a secondary IP configuration. Learn more

	Name	IP Version	Type	Private IP Address	Public IP Address
□	ipconfig1	IPv4	Primary	192.168.4.10 (Static)	-

Edit the NSG for WAN interface.

To allow Netconf session and 8443 from VD to VOS, add a new rule inbound on WAN interface to allow 2022.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
vishnu.a@versa-networ...
VERSA NETWORKS (VERSA-NET...
What are the requirements for attaching and detaching network interfaces?
How can I make this VM secure?
List all my network interfaces for this VM
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Networking
Network settings
Load balancing
Application security groups
Network manager
Settings
Availability + scale
Security
Backup + disaster recovery
Operations
Monitoring
Automation
Help
This is a new experience. Please provide feedback
List all my network interfaces for VOS-SDWAN-VI.
What are the requirements for attaching or detaching a network interface?
How can I make my virtual machine secure?
Attach network interface
Detach network interface
View topology
Troubleshoot
Refresh
Give feedback
Rules
Collapse all
Create port rule
Inbound port rule
Outbound port rule
Search rules
Source == all
Destination == all
Protocol == all
Action == all
Port == all
Add or remove favorites by pressing Ctrl+Shift+F

Home > VOS-SDWAN-VI

VOS-SDWAN-VI | Network settings

Virtual machine

Network interface / IP configuration: WAN-Network / ipconfig1 (primary)

Essentials

Network interface : WAN-Network

Virtual network / subnet : Azure-SSE-VNET-VI / WAN-Subnet

Public IP address : 135.13.32.103

Private IP address : 192.168.3.10

Admin security rules : 0 (Configure)

Load balancers : 0 (Configure)

Application security groups : 0 (Configure)

Network security group : VOSSDWANVInsg885

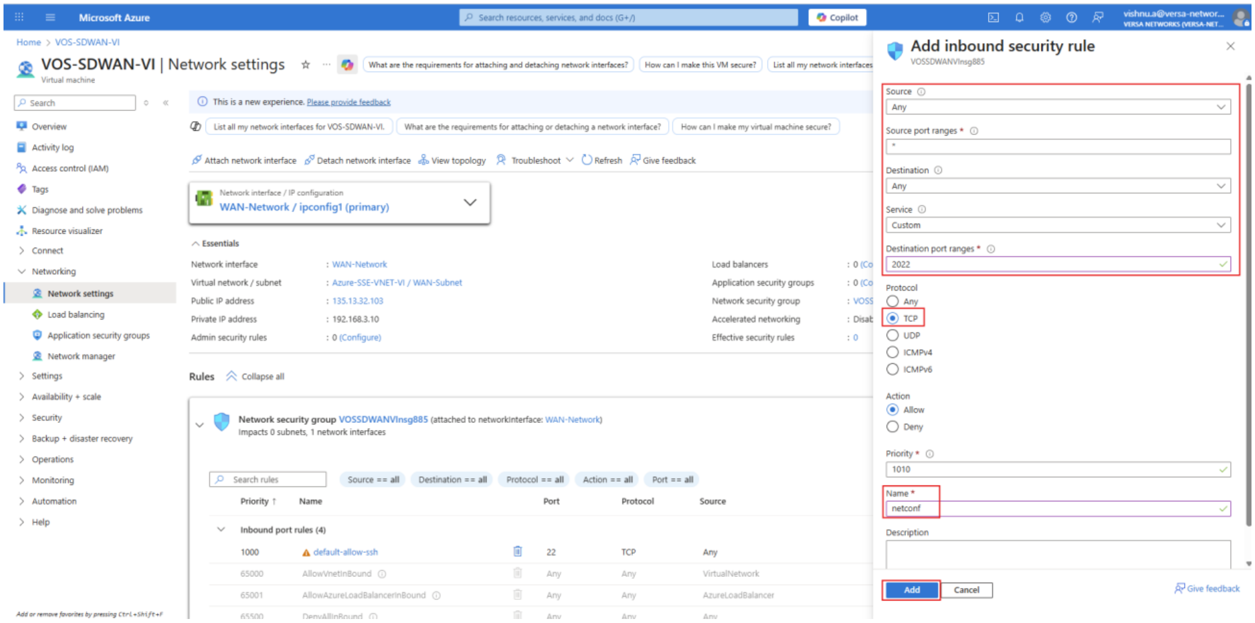
Accelerated networking : Disabled

Effective security rules : 0

Network security group VOSSDWANVInsg885 (attached to networkinterface: WAN-Network)
Impacts 0 subnets, 1 network interfaces

Inbound port rules (4)

Priority ↑	Name	Port	Protocol	Source	Destination	Action
1000	default-allow-ssh	22	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
vishnu.a@versa-networ...
VERSA NETWORKS (VERSA-NET...
Home > VOS-SDWAN-VI
What are the requirements for attaching and detaching network interfaces?
How can I make this VM secure?
List all my network interfaces
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Networking
Network settings
Load balancing
Application security groups
Network manager
Settings
Availability + scale
Security
Backup + disaster recovery
Operations
Monitoring
Automation
Help
Add or remove favorites by pressing Ctrl+Shift+F
This is a new experience. Please provide feedback
List all my network interfaces for VOS-SDWAN-VI.
What are the requirements for attaching or detaching a network interface?
How can I make my virtual machine secure?
Attach network interface
Detach network interface
View topology
Troubleshoot
Refresh
Give feedback
Search rules
Source == all
Destination == all
Protocol == all
Action == all
Port == all
Collapse all
Add
Cancel
Give feedback

VOS-SDWAN-VI | Network settings

Virtual machine

Network interface / IP configuration
WAN-Network / ipconfig1 (primary)

Essentials

Network interface	: WAN-Network	Load balancers	: 0 (Co
Virtual network / subnet	: Azure-SSE-VNET-VI / WAN-Subnet	Application security groups	: 0 (Co
Public IP address	: 135.13.32.103	Network security group	: VOSS
Private IP address	: 192.168.3.10	Accelerated networking	: Disab
Admin security rules	: 0 (Configure)	Effective security rules	: 0

Rules

Network security group VOSSDWANVInsg885 (attached to networkInterface: WAN-Network)
Impacts 0 subnets, 1 network interfaces

Priority ↑	Name	Port	Protocol	Source
Inbound port rules (4)				
1000	default-allow-ssh	22	TCP	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer
65500	DenyAllInBound	Any	Any	Any

Add inbound security rule

VOSSDWANVInsg885

Source: Any

Source port ranges *: *

Destination: Any

Service: Custom

Destination port ranges *: 2022

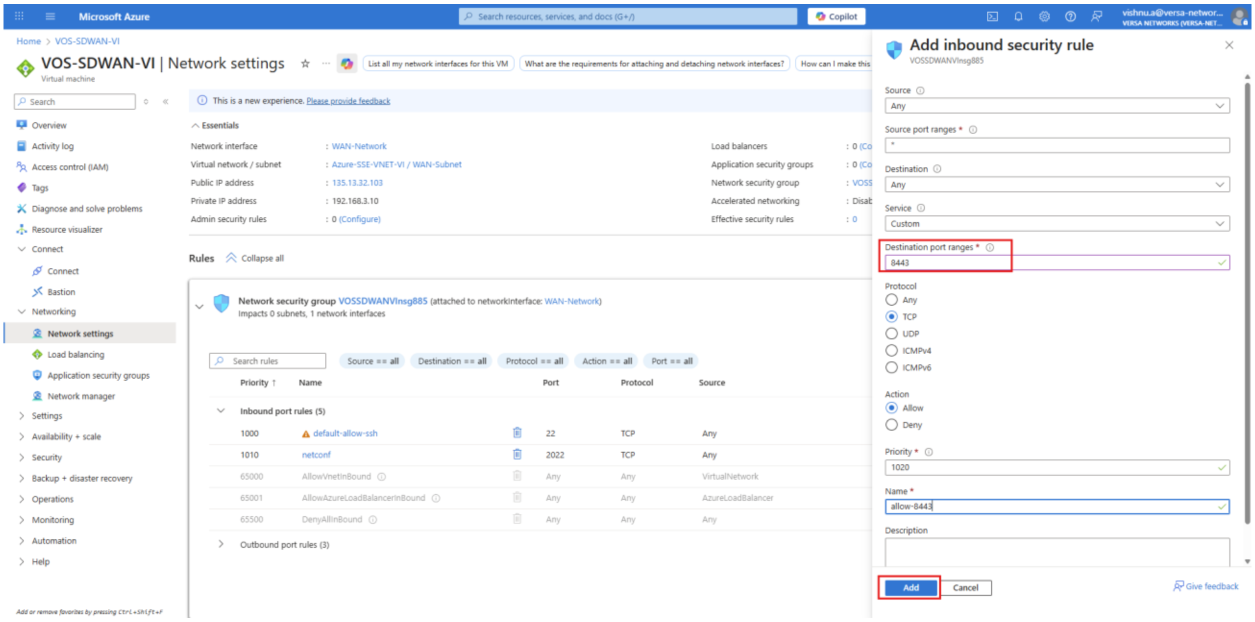
Protocol: ○ Any ● TCP ○ UDP ○ ICMPv4 ○ ICMPv6

Action: ● Allow ○ Deny

Priority *: 1010

Name *: netconf

Description:



VOS-SDWAN-VI | Network settings

Virtual machine

Essentials

Network interface	: WAN-Network	Load balancers	: 0 (Co
Virtual network / subnet	: Azure-SSE-VNET-VI / WAN-Subnet	Application security groups	: 0 (Co
Public IP address	: 135.13.32.103	Network security group	: VOSS
Private IP address	: 192.168.3.10	Accelerated networking	: Disab
Admin security rules	: 0 (Configure)	Effective security rules	: 0

Rules

Network security group VOSSDWANVInsg885 (attached to networkInterface: WAN-Network)
Impacts 0 subnets, 1 network interfaces

Priority ↑	Name	Port	Protocol	Source
Inbound port rules (5)				
1000	default-allow-ssh	22	TCP	Any
1010	netconf	2022	TCP	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer
65500	DenyAllInBound	Any	Any	Any
Outbound port rules (3)				

Add inbound security rule

VOSSDWANVInsg885

Source: Any

Source port ranges *: *

Destination: Any

Service: Custom

Destination port ranges *: 8443

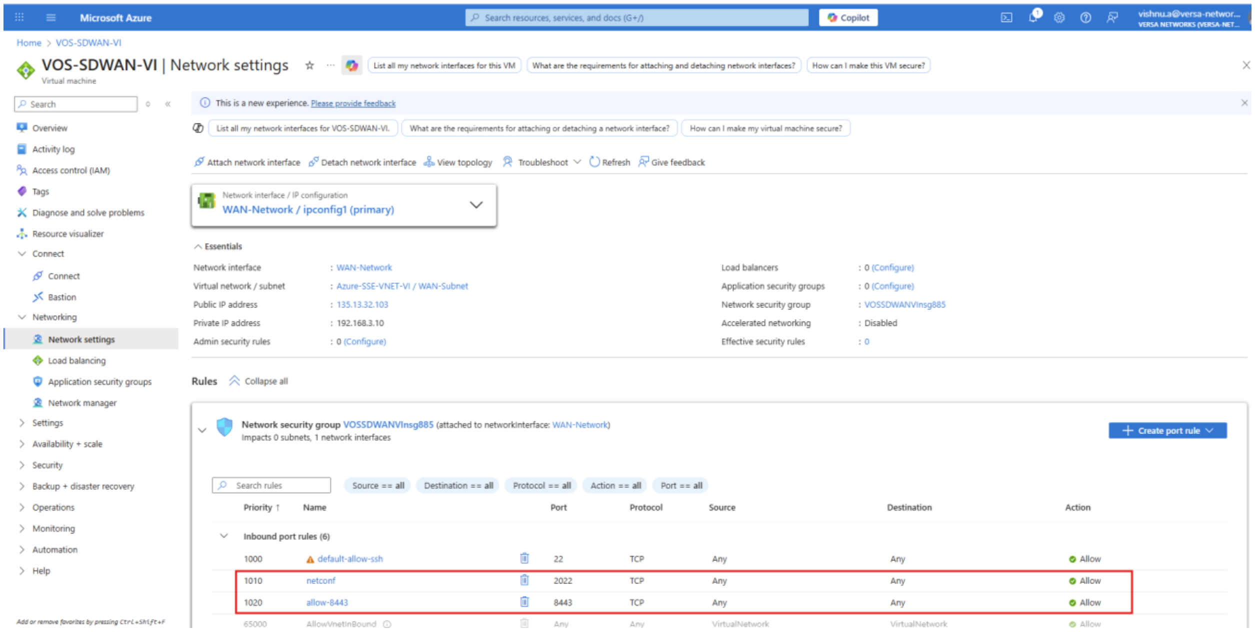
Protocol: ○ Any ● TCP ○ UDP ○ ICMPv4 ○ ICMPv6

Action: ● Allow ○ Deny

Priority *: 1020

Name *: allow-8443

Description:



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
vishnu.a@versa-networ...
VERSA NETWORKS (VERSA-NET...
Home > VOS-SDWAN-VI

VOS-SDWAN-VI | Network settings

Virtual machine

List all my network interfaces for this VM
What are the requirements for attaching and detaching network interfaces?
How can I make this VM secure?
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Connect
Bastion
Networking
Network settings
Load balancing
Application security groups
Network manager
Settings
Availability + scale
Security
Backup + disaster recovery
Operations
Monitoring
Automation
Help
Add or remove favorites by pressing Ctrl+Shift+F
This is a new experience. Please provide feedback
List all my network interfaces for VOS-SDWAN-VI.
What are the requirements for attaching or detaching a network interface?
How can I make my virtual machine secure?
Attach network interface
Detach network interface
View topology
Troubleshoot
Refresh
Give feedback

Network interface / IP configuration
WAN-Network / ipconfig1 (primary)

Essentials

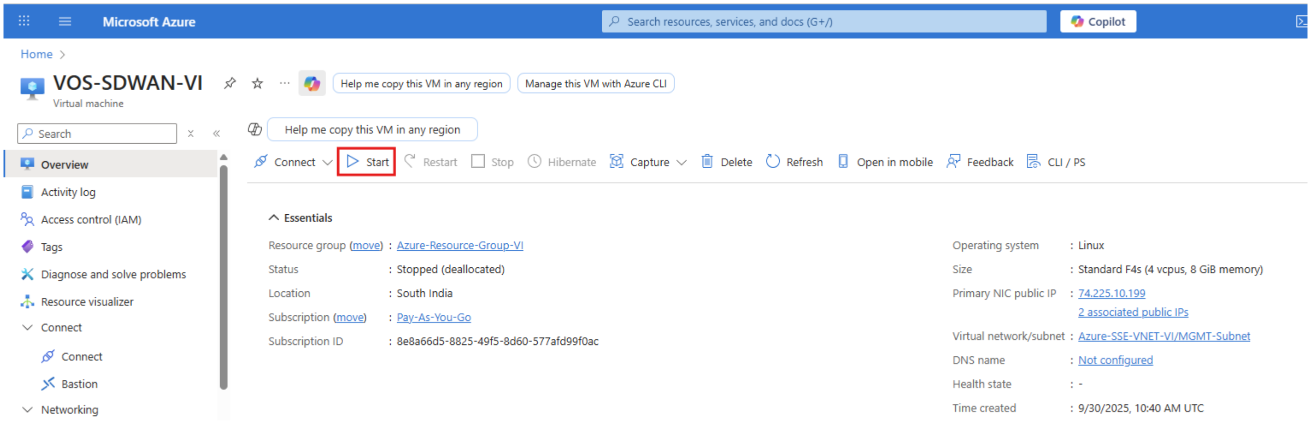
Network interface : WAN-Network
Virtual network / subnet : Azure-SSE-VNET-VI / WAN-Subnet
Public IP address : 135.13.32.103
Private IP address : 192.168.3.10
Admin security rules : 0 (Configure)
Load balancers : 0 (Configure)
Application security groups : 0 (Configure)
Network security group : VOSSDWANVInsg885
Accelerated networking : Disabled
Effective security rules : 0

Rules

Network security group VOSSDWANVInsg885 (attached to networkInterface: WAN-Network)
Impacts 0 subnets, 1 network interfaces

Priority ↑	Name	Port	Protocol	Source	Destination	Action
Inbound port rules (6)						
1000	default-allow-ssh	22	TCP	Any	Any	Allow
1010	netconf	2022	TCP	Any	Any	Allow
1020	allow-8443	8443	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow

Once all the above configuration is done, start VOS Virtual machine.



VOS-SDWAN-VI

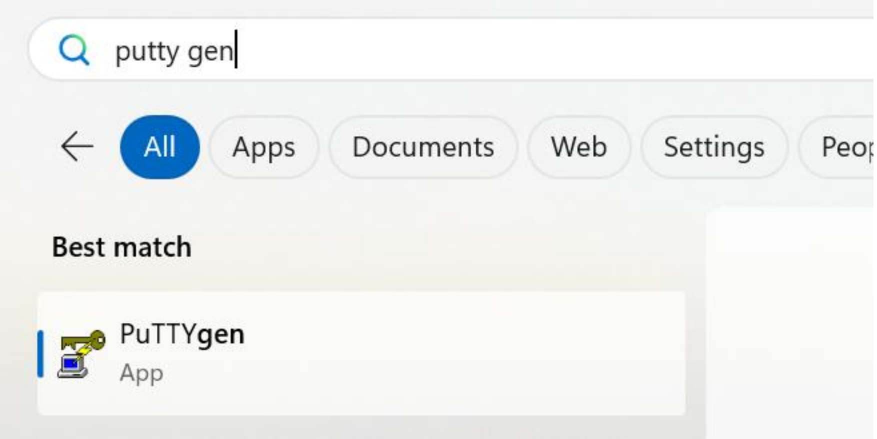
Virtual machine

Essentials

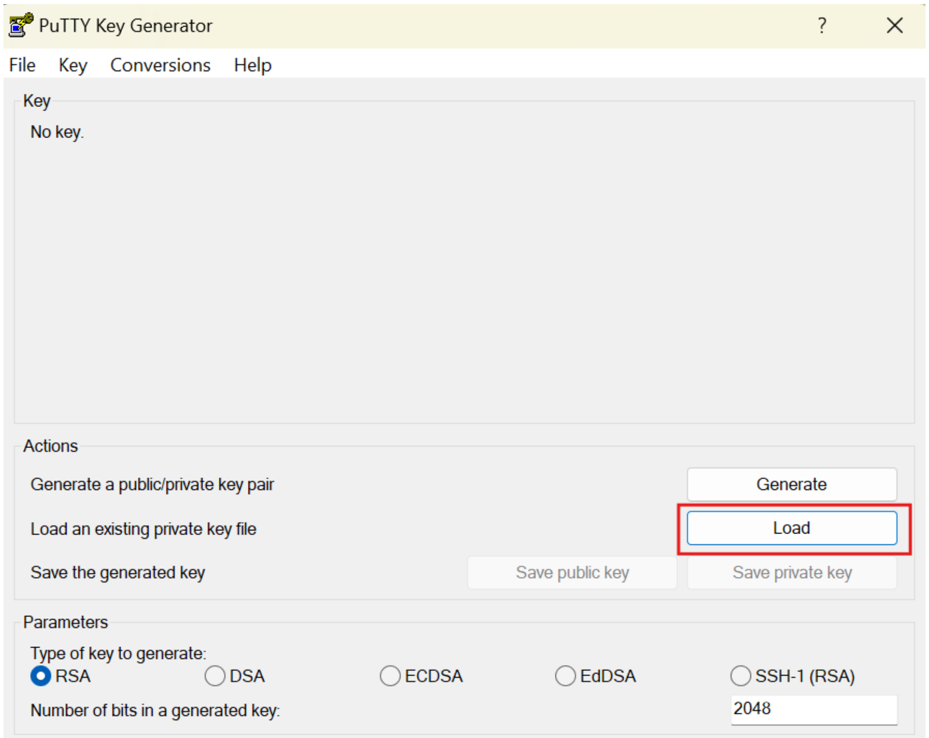
Resource group (move) : Azure-Resource-Group-VI
Status : Stopped (deallocated)
Location : South India
Subscription (move) : Pay-As-You-Go
Subscription ID : 8e8a66d5-8825-49f5-8d60-577afd99f0ac
Operating system : Linux
Size : Standard F4s (4 vcpus, 8 GiB memory)
Primary NIC public IP : 74.225.10.199
2 associated public IPs
Virtual network/subnet : Azure-SSE-VNET-VI/MGMT-Subnet
DNS name : Not configured
Health state : -
Time created : 9/30/2025, 10:40 AM UTC

To take access to the device,

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 VOS instance.



Key

No key.

Generate a public/private key pair

Load an existing private key file

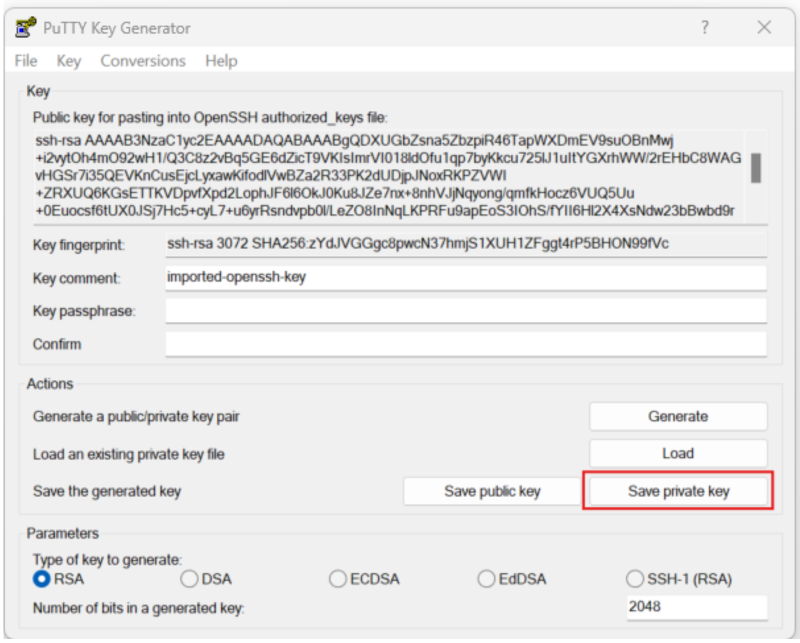
Save the generated key

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 AAAAB3NzaC1yc2EAAAADAQABAAABgQDXUGbZsna5ZbzpiR46TapWXDmEV9suOBnMwj
+i2vytOh4mO92wH1/Q3C8z2vBq5GE6dZicT9VKIsImrVI018ldOfu1qp7byKkcu725lJ1uItYGXrhWW/2rEHbC8WAG
vHGSr7i35QEVKnCusEjcLyxawKifodlVwBZa2R33PK2dUDjpJNoxRKPZVWI
+ZRXUQ6KGsETTKVDpvfXpd2LophJF6l6OkJ0Ku8JZe7nx+8nhVJjNqyong/qmfkHocz6VUQ5Uu
+0Euocsf6tUX0JSj7Hc5+cyL7+u6yrRsndvpb0l/LeZO8InNqLKPRFu9apEoS3IOhS/fYII6Hl2X4XsNdw23bBwbd9r
```

Key fingerprint: ssh-rsa 3072 SHA256:zYdJVGGgc8pwcN37hmjS1XUH1ZFggt4rP5BHON99fVc

Key comment: imported-openssh-key

Key passphrase:

Confirm

Generate a public/private key pair

Load an existing private key file

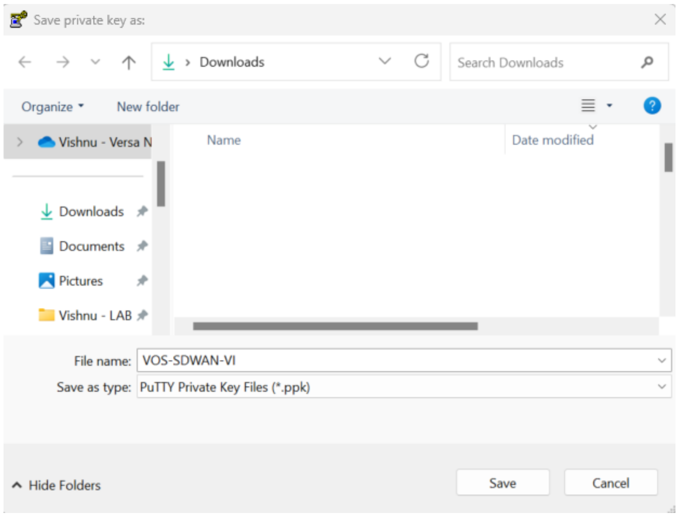
Save the generated key

Type of key to generate:

● RSA ○ DSA ○ ECDSA ○ EdDSA ○ SSH-1 (RSA)

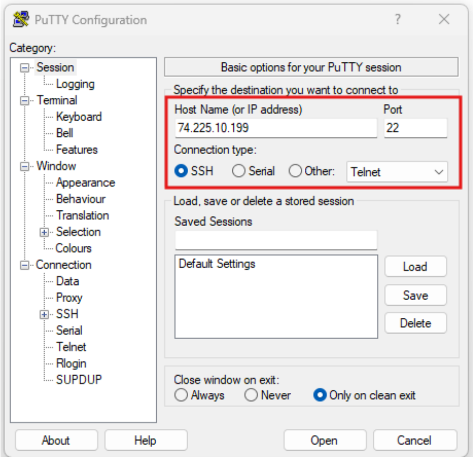
Number of bits in a generated key: 2048

Save the key to your PC.

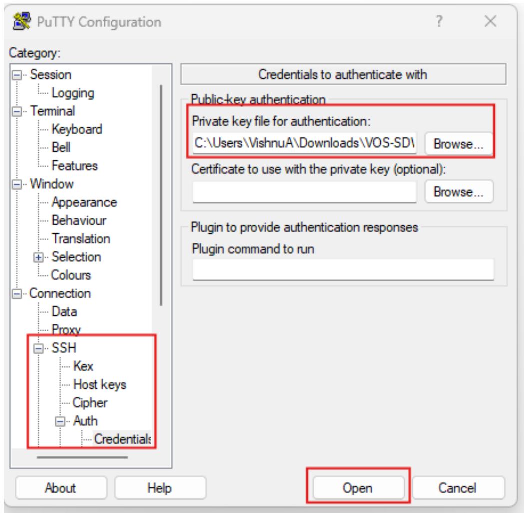


File name: VOS-SDWAN-VI
Save as type: PuTTY Private Key Files (*.ppk)

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

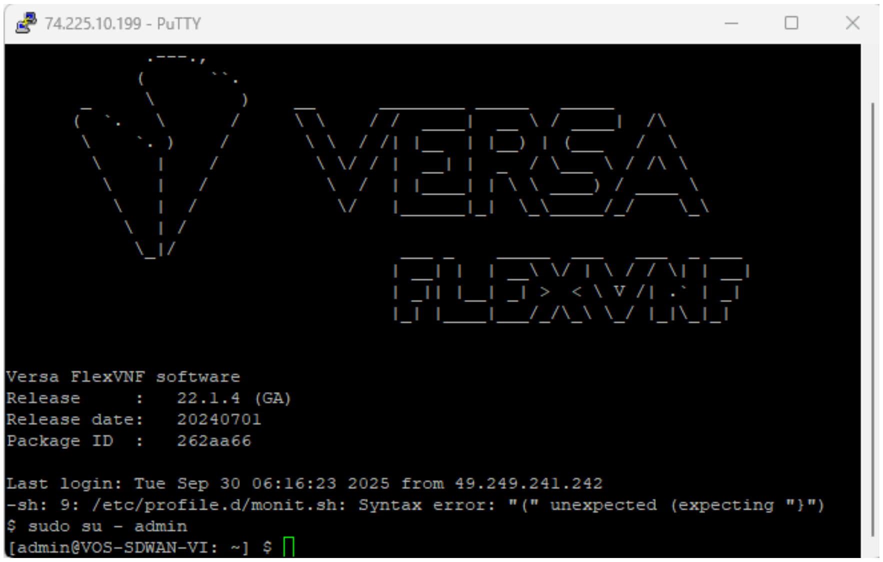


Specify the destination you want to connect to
Host Name (or IP address): 74.225.10.199
Port: 22
Connection type: ● SSH ○ Serial ○ Other: Telnet
Close window on exit: ○ Always ○ Never ● Only on clean exit



Private key file for authentication: C:\Users\VishnuA\Downloads\VOS-SD\
Certificate to use with the private key (optional):

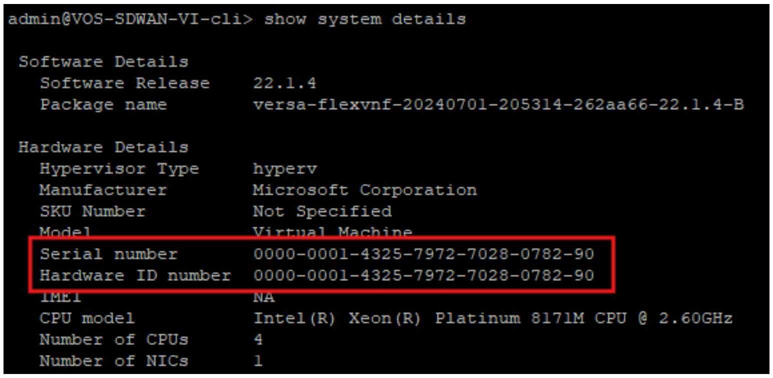
Login with username azureuser and type "sudo su -admin".



```
Versa FlexVNF software
Release     :   22.1.4 (GA)
Release date:   20240701
Package ID  :   262aa66

Last login: Tue Sep 30 06:16:23 2025 from 49.249.241.242
-sh: 9: /etc/profile.d/monit.sh: Syntax error: "(" unexpected (expecting "}")
$ sudo su - admin
[admin@VOS-SDWAN-VI: ~] $
```

Note down the serial number of the device for the device onboarding.



```
admin@VOS-SDWAN-VI-cli> show system details

 Software Details
   Software Release    22.1.4
   Package name        versa-flexvnf-20240701-205314-262aa66-22.1.4-B

 Hardware Details
   Hypervisor Type     hyperv
   Manufacturer        Microsoft Corporation
   SKU Number          Not Specified
   Model               Virtual Machine
   Serial number       0000-0001-4325-7972-7028-0782-90
   Hardware ID number  0000-0001-4325-7972-7028-0782-90
   IMEI                NA
   CPU model           Intel(R) Xeon(R) Platinum 8171M CPU @ 2.60GHz
   Number of CPUs      4
   Number of NICs      1
```

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.

sudo chown admin:versa authorized_keys

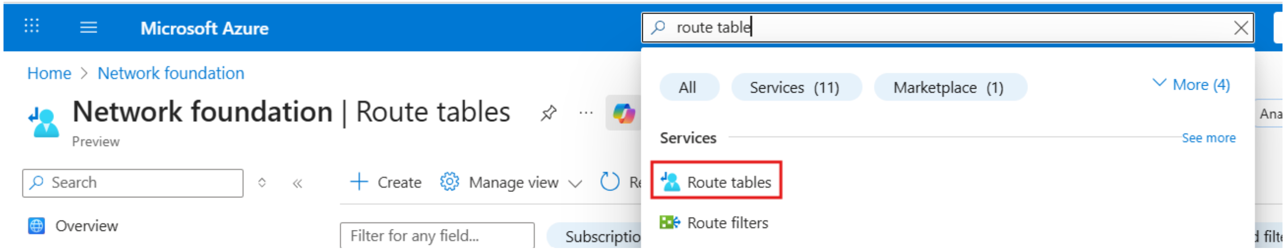
To add the id_dsa.pub.it to authorized_keys in the appliance edit the file using "sudo nano .ssh/authorized_keys" add the copied id_dsa.pub.
NOTE: File permission should be 600. To change the file permission run -

chmod 600 authorized_keys.

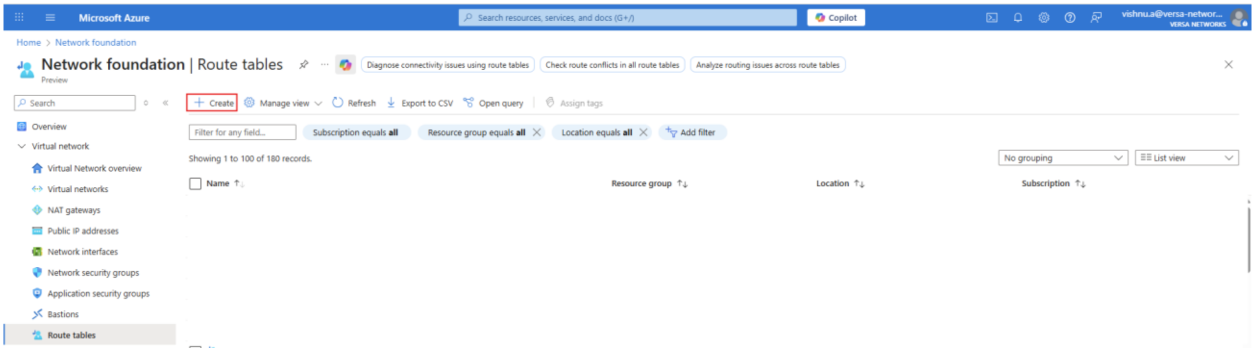
Routing in Azure:

Create a Route table for LAN to forward the traffic from the WEB server towards the SDWAN Device.

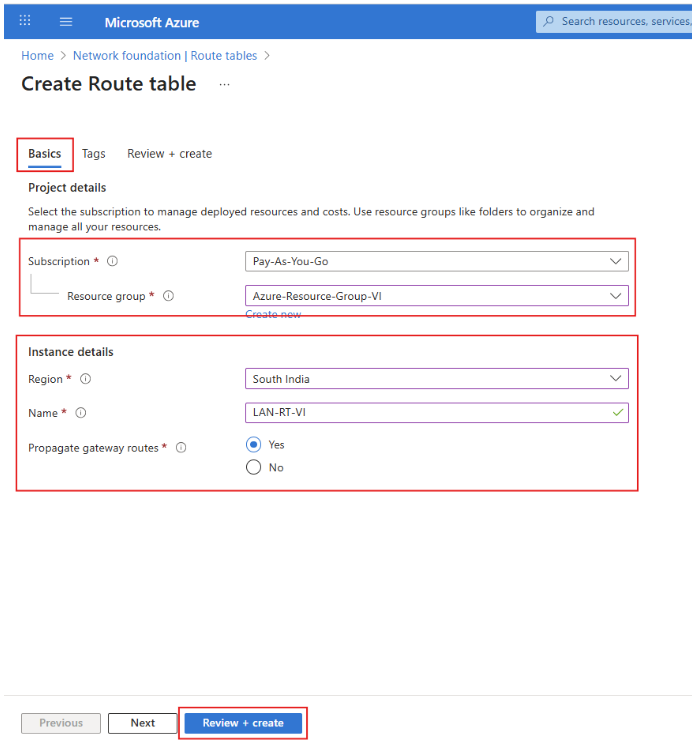
To create a route table search for "route tables" and select "Route tables" from Services.



Under route tables click on “Create”.



Under Basics, tab provide information regarding subscription, Resource group, Region and the Name for Route Table and click on Next.


Microsoft Azure
Search resources, services,
Home > Network foundation | Route tables >
Create Route table
Basics
Tags
Review + create

Project details

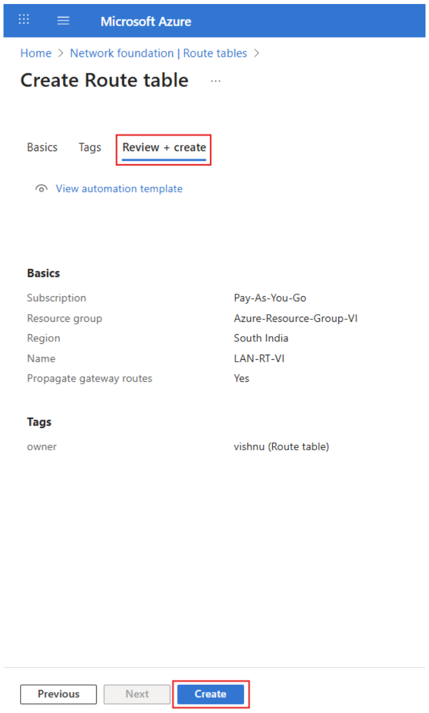
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	Pay-As-You-Go
Resource group *	Azure-Resource-Group-VI

Instance details

Region *	South India
Name *	LAN-RT-VI
Propagate gateway routes *	● Yes ○ No

Under Review+ Create tab, click on Create.



Create Route table ...

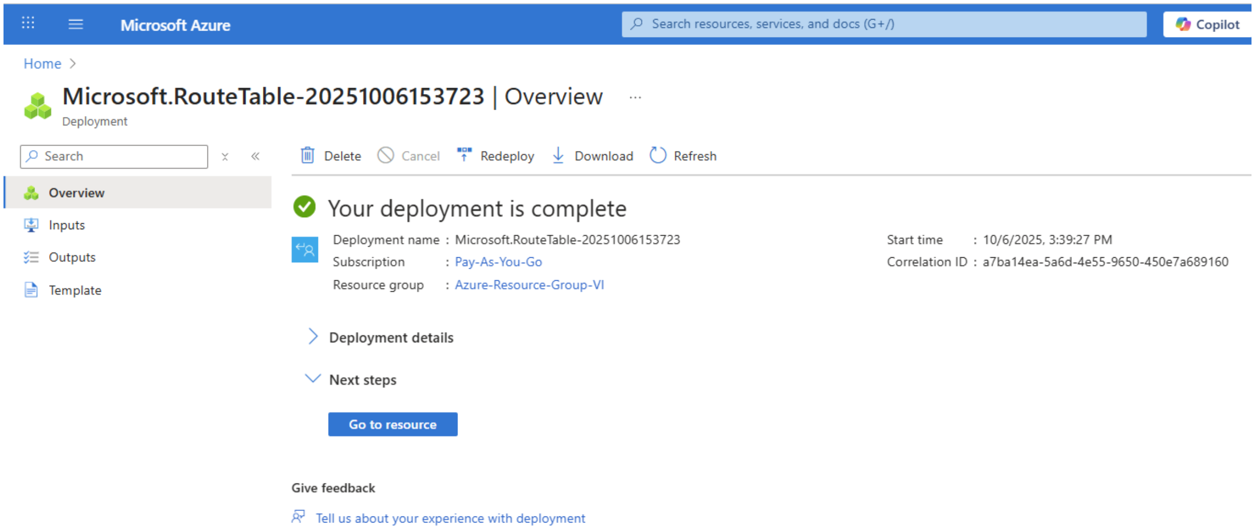
Basics

Subscription	Pay-As-You-Go
Resource group	Azure-Resource-Group-VI
Region	South India
Name	LAN-RT-VI
Propagate gateway routes	Yes

Tags

owner	vishnu (Route table)

The deployment status can be viewed under Overview.



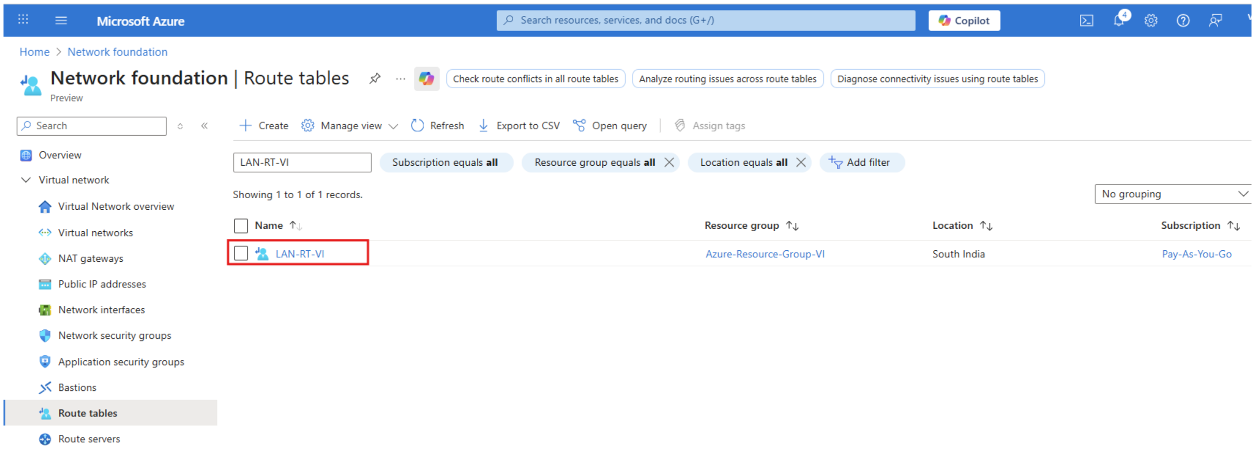
Microsoft.RouteTable-20251006153723 | Overview ...

Deployment

Your deployment is complete

Deployment name	: Microsoft.RouteTable-20251006153723	Start time	: 10/6/2025, 3:39:27 PM
Subscription	: Pay-As-You-Go	Correlation ID	: a7ba14ea-5a6d-4e55-9650-450e7a689160
Resource group	: Azure-Resource-Group-VI		

Once the deployment is complete go to the Route table you created.

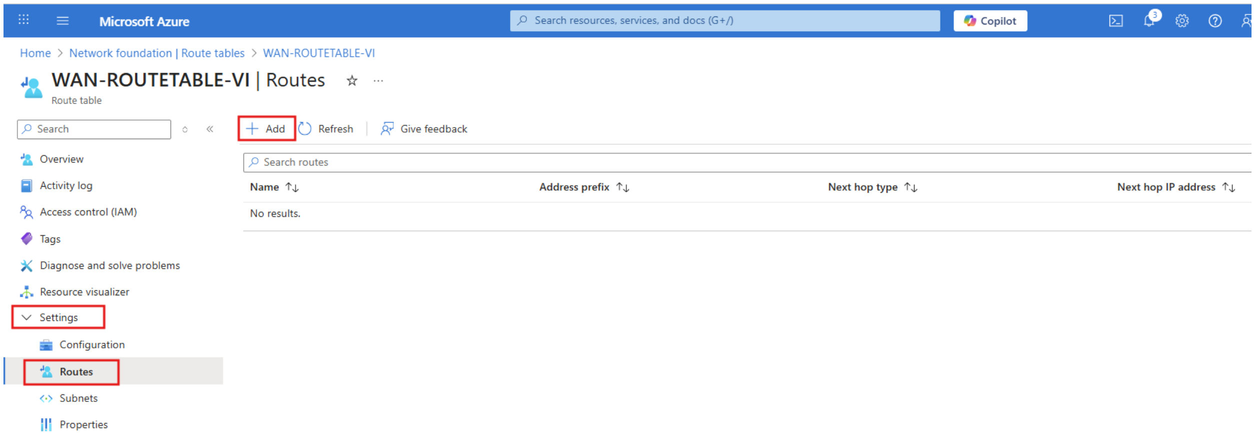


Network foundation | Route tables

Showing 1 to 1 of 1 records.

Name	Resource group	Location	Subscription
LAN-RT-VI	Azure-Resource-Group-VI	South India	Pay-As-You-Go

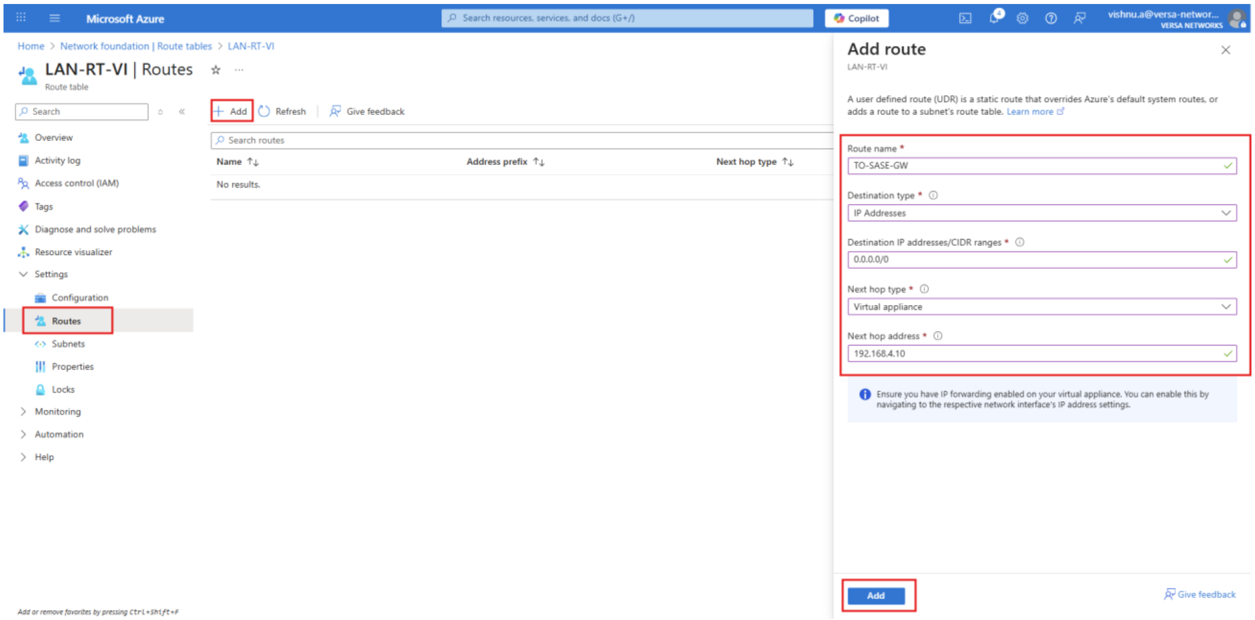
To add new Route, under Settings → Routes click on +Add.



WAN-ROUTETABLE-VI | Routes

Name	Address prefix	Next hop type	Next hop IP address
No results.			

Under “Add route” provide a Name, Destination Type, Destination IP and the Next hop and click on Add.



Add route

LAN-RT-VI

A user defined route (UDR) is a static route that overrides Azure's default system routes, or adds a route to a subnet's route table. Learn more

Route name * TO-SASE-GW

Destination type * IP Addresses

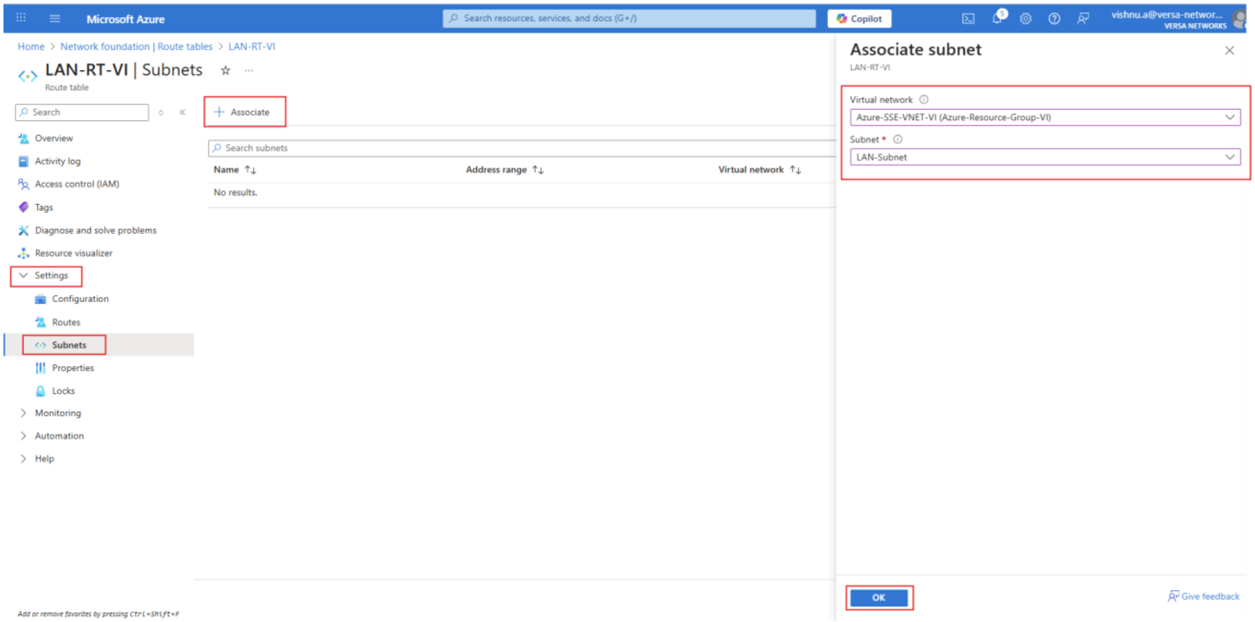
Destination IP addresses/CIDR ranges * 0.0.0.0/0

Next hop type * Virtual appliance

Next hop address * 192.168.4.10

Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.

Under Subnets, Click in Associate and Associate LAN-Subnet to the route table and click on “Ok”.



Name ↑↓	Address range ↑↓	Virtual network ↑↓
No results.		

Associate subnet

LAN-RT-VI

Virtual network: Azure-SSE-VNET-VI (Azure-Resource-Group-VI)

Subnet *: LAN-Subnet

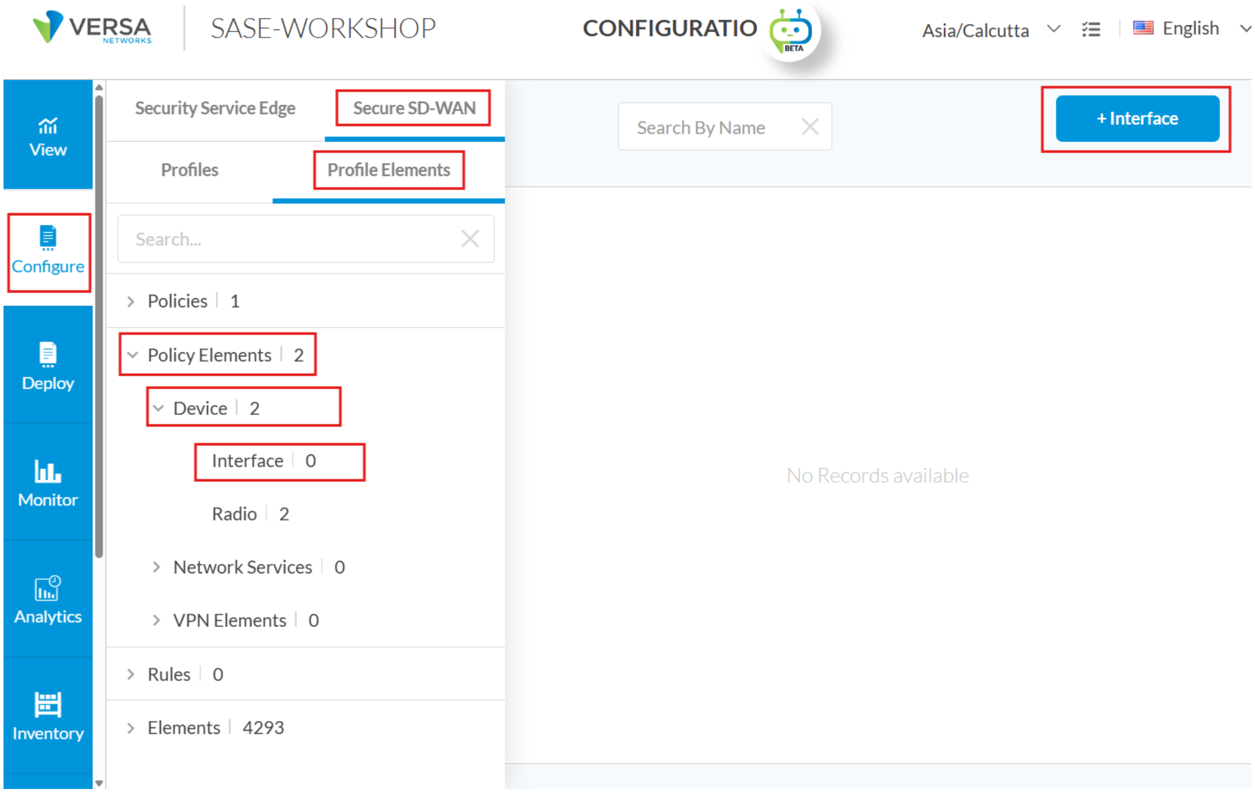
Concerto Configuration:

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

Creating Master profile in Concerto:

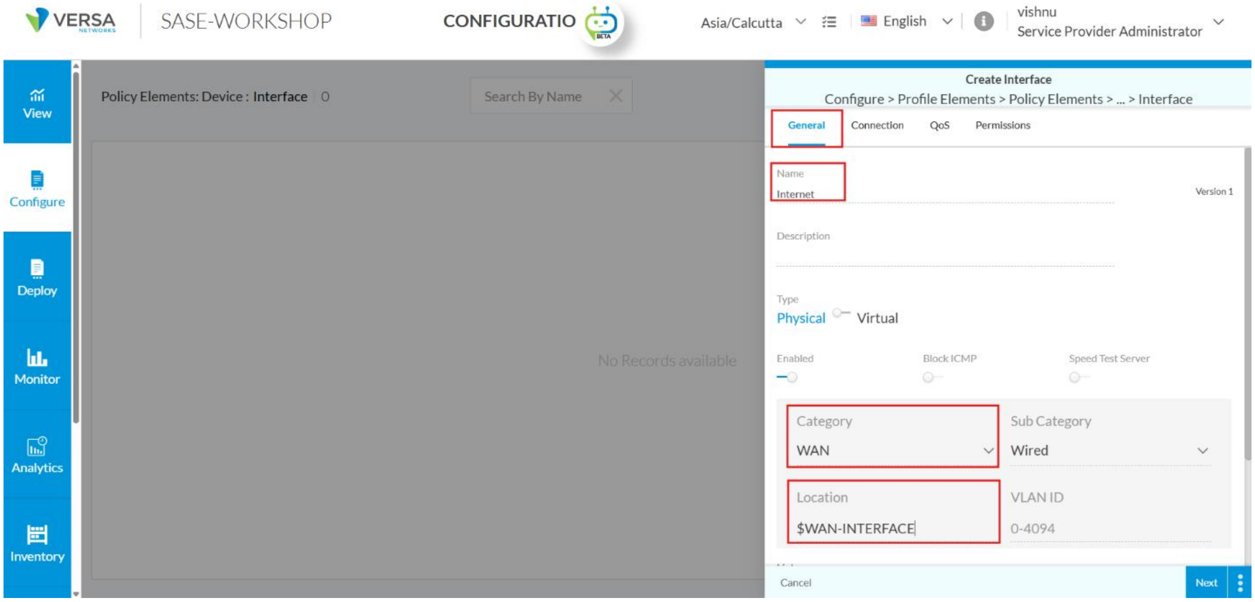
Creating Interface:

Go to respective Tenant and click on Configure → Secure SD-WAN → Profile Elements → 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

Description:

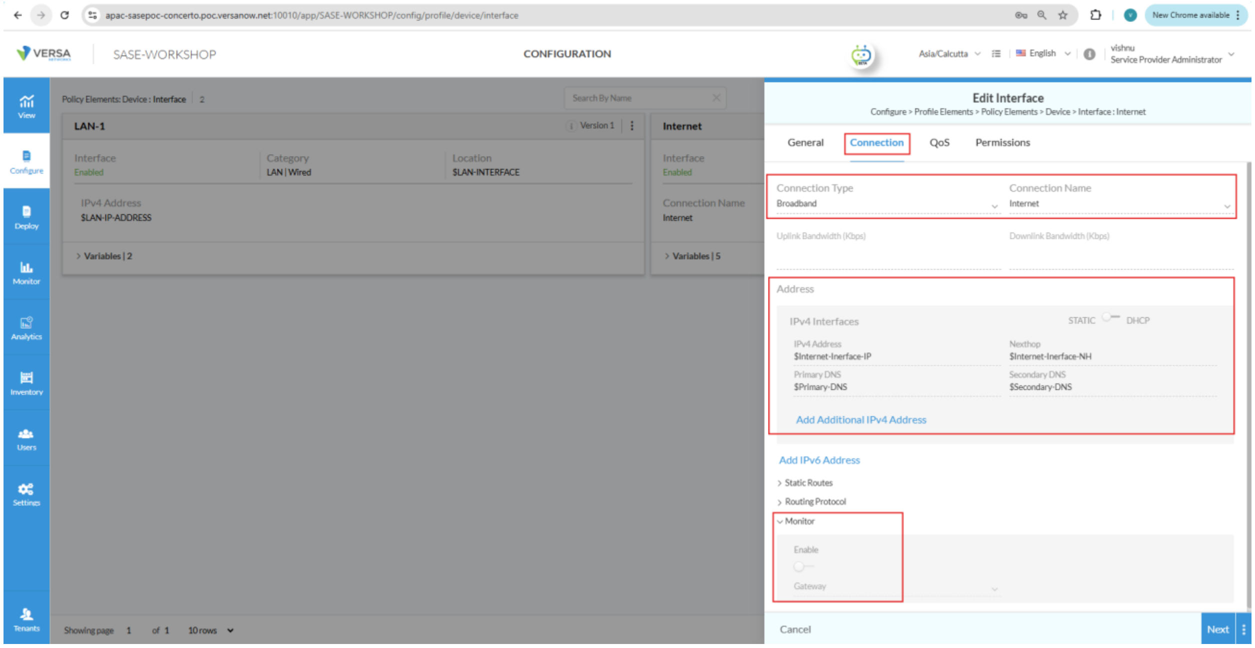
Category: WAN

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 ,DNS information, Disable Monitor and save.



Edit Interface

Configure > Profile Elements > Policy Elements > Device > Interface : Internet

General | Connection | QoS | Permissions

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

Add Additional IPv4 Address

Add IPv6 Address

> Static Routes

> Routing Protocol

Monitor

Enable

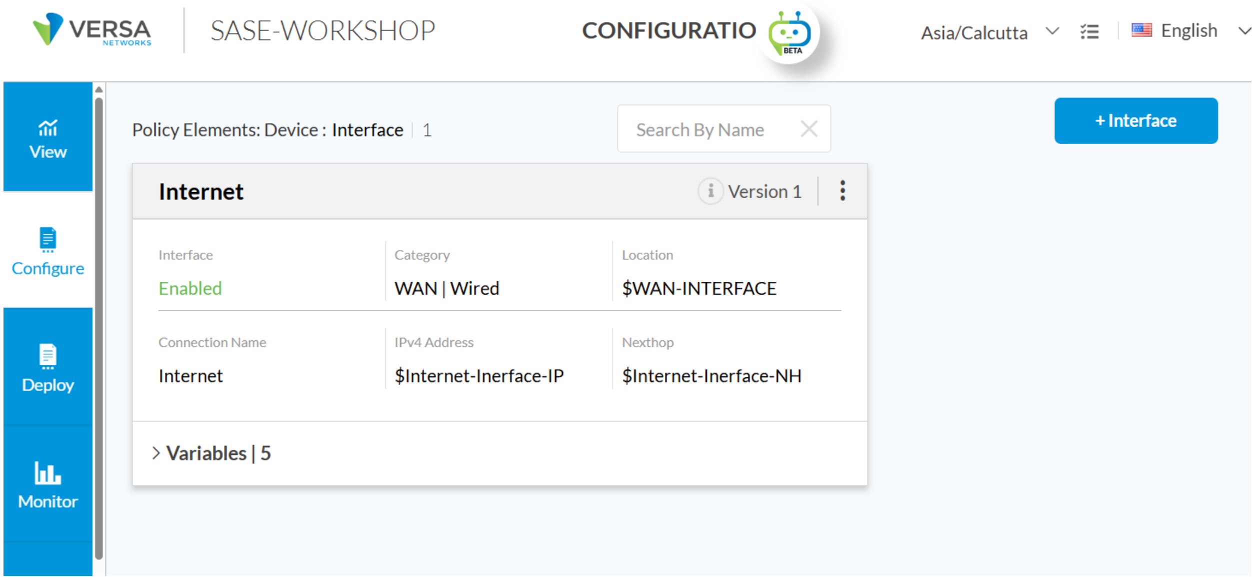
Gateway

Cancel | Next

Note:

- By default, it is DHCP you can disable the knob to configure it as STATIC.
- Disable Monitor – if you don't disable this, a static route to Gateway of WAN subnet will be created along with with ICMP monitor, since the subnet gateway IP is pingable on Azure, static route on Internet Transport VR is not installed in the routing table, making the device unreachable to the Headend.

This will create a WAN interface.



Policy Elements: Device : Interface | 1

+ Interface

Internet — Version 1

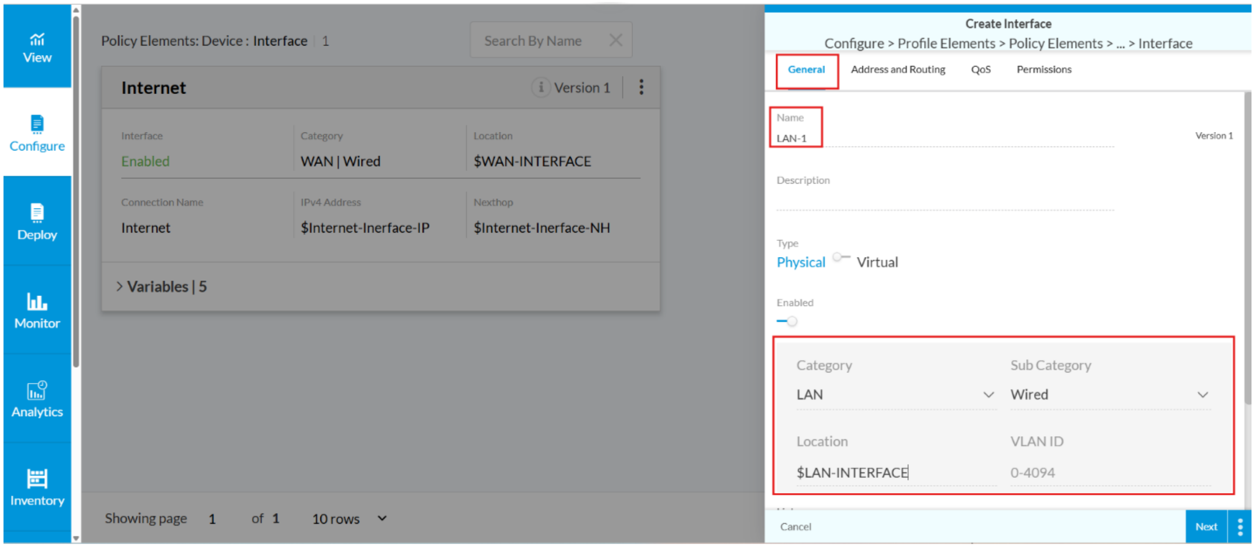
Interface	Category	Location
Enabled	WAN | Wired	$WAN-INTERFACE

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

> Variables | 5

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

Create Interface

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

Name: LAN-1

Version 1

Description

Type: Physical ○ Virtual

Enabled

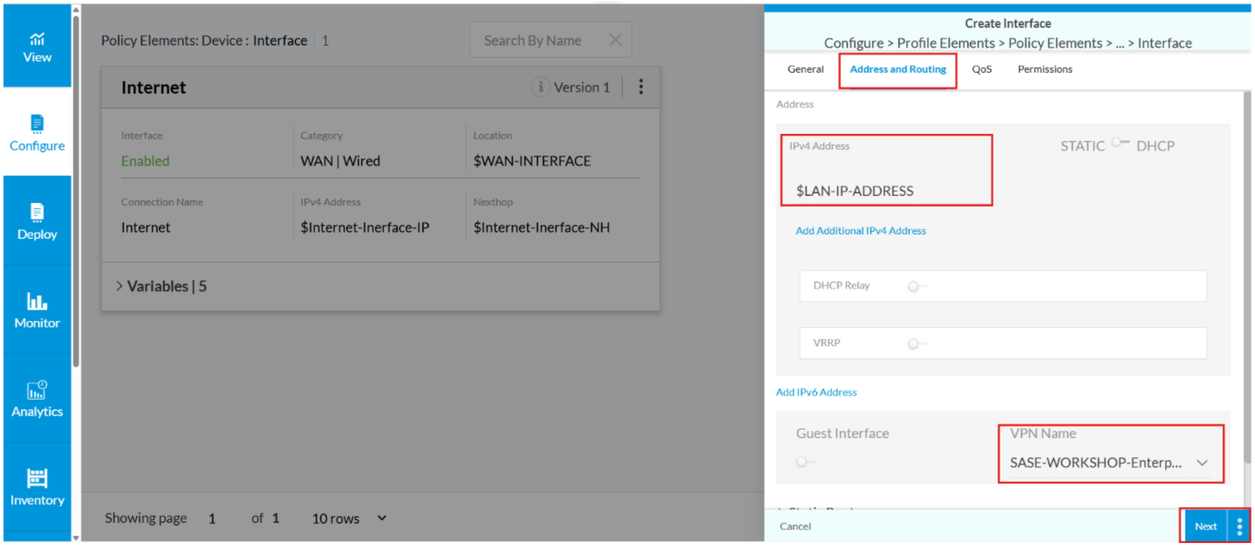
Category: LAN

Sub Category: Wired

Location: $LAN-INTERFACE

VLAN ID: 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

Create Interface

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

Address

IPv4 Address: $LAN-IP-ADDRESS

STATIC ○ DHCP

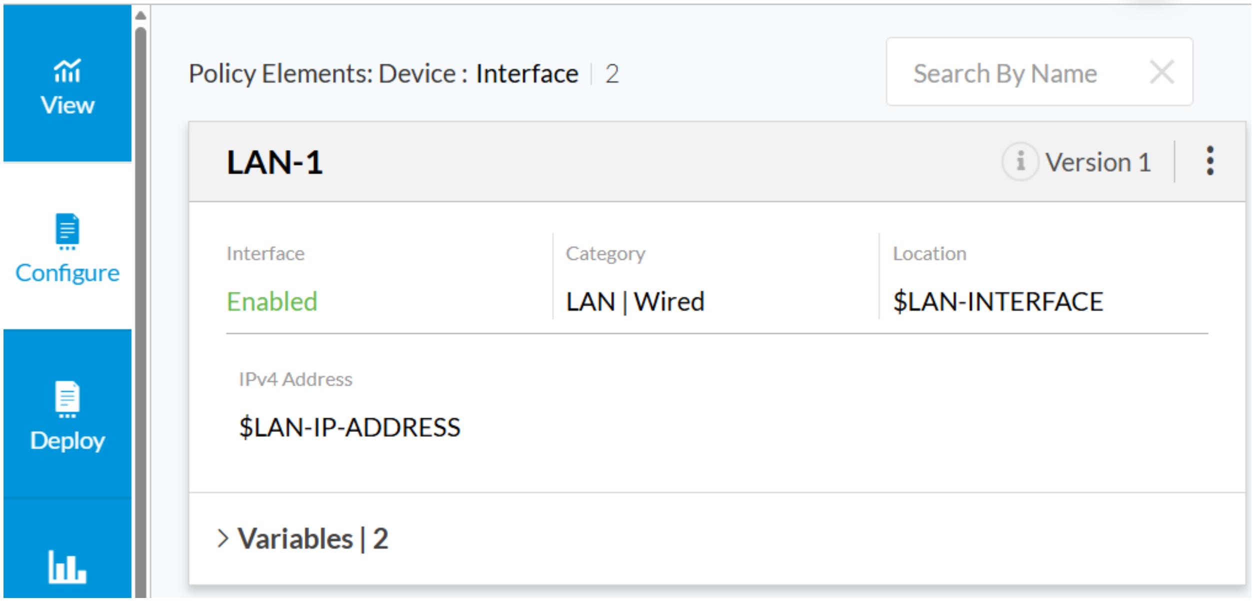
DHCP Relay

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

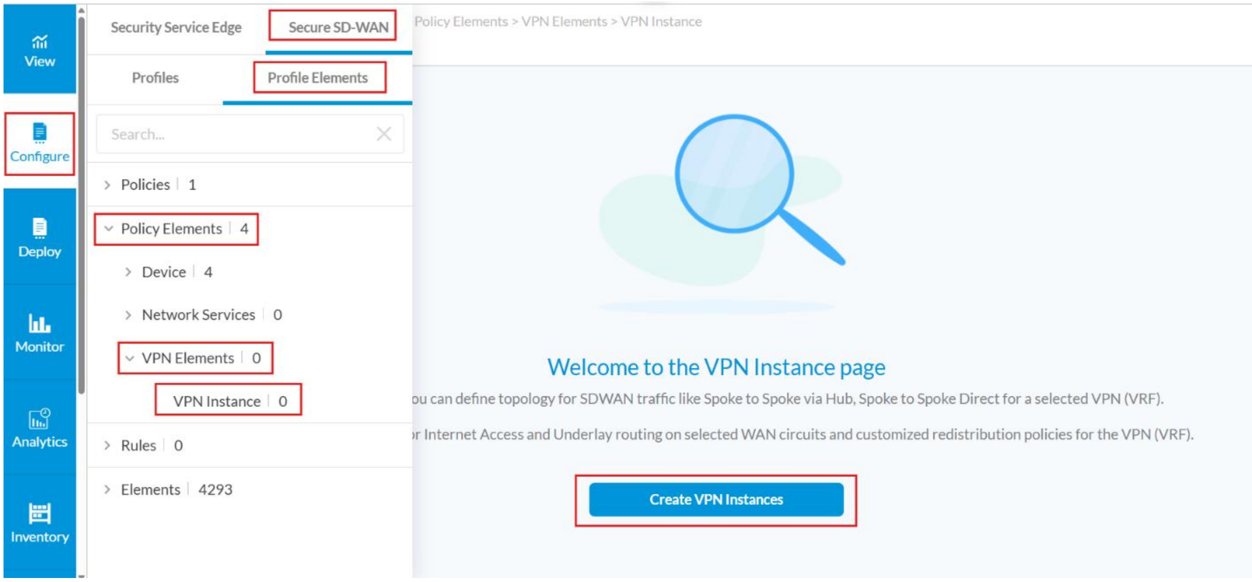
$LAN-IP-ADDRESS

Variables | 2

Creating 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

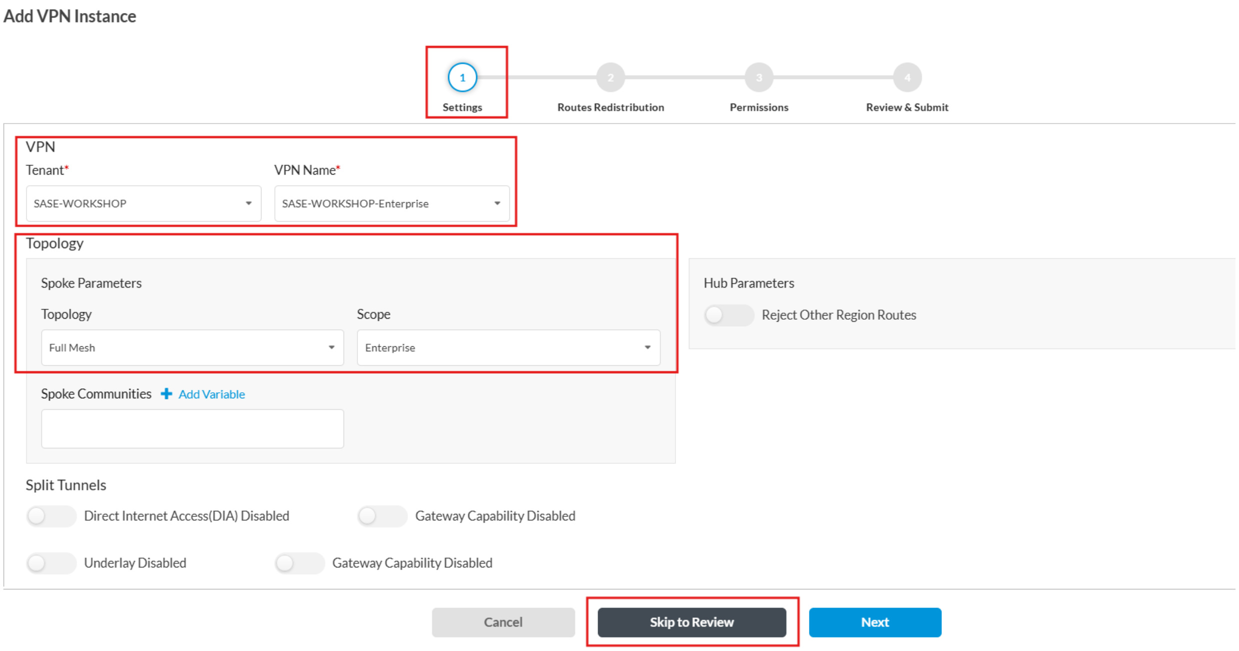
ou can define topology for SDWAN traffic like Spoke to Spoke via Hub, Spoke to Spoke Direct for a selected VPN (VRF).

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 + Add Variable

Hub Parameters

Reject Other Region Routes

Split Tunnels

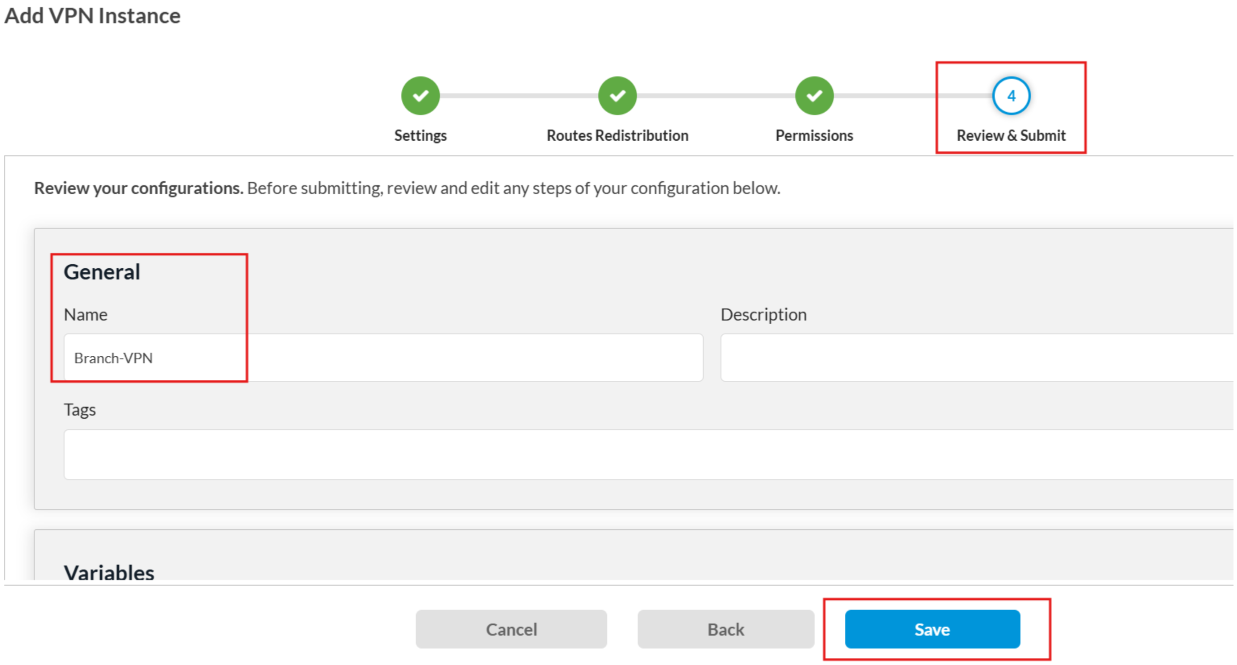
Direct Internet Access(DIA) Disabled

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

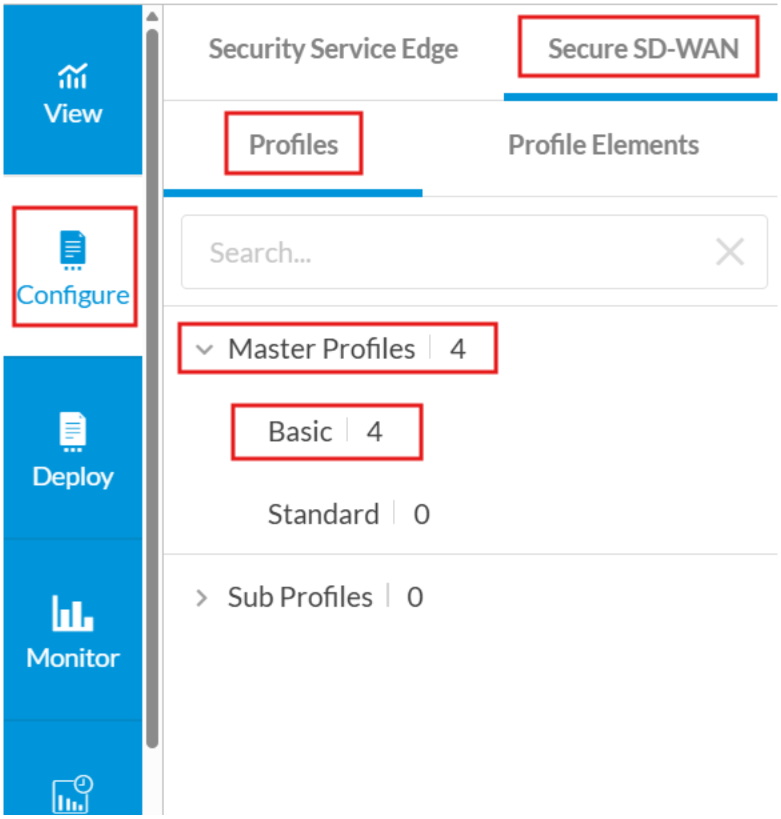
Variables

Master Profile:

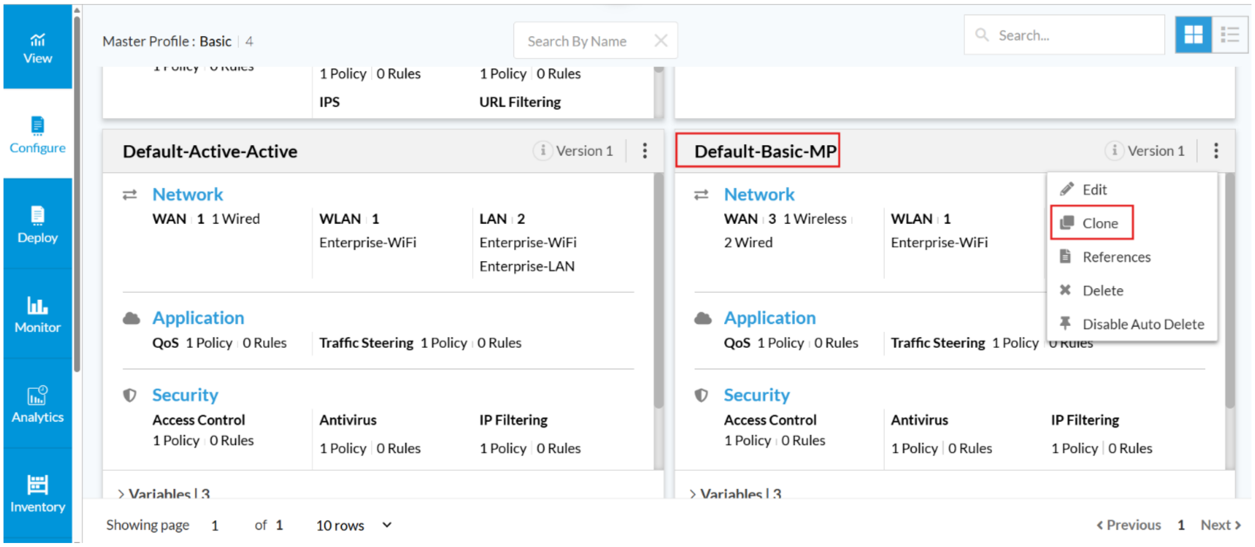
A master profile is a collection of one or more sub-profiles. A single master profile can be applied to one or more devices.

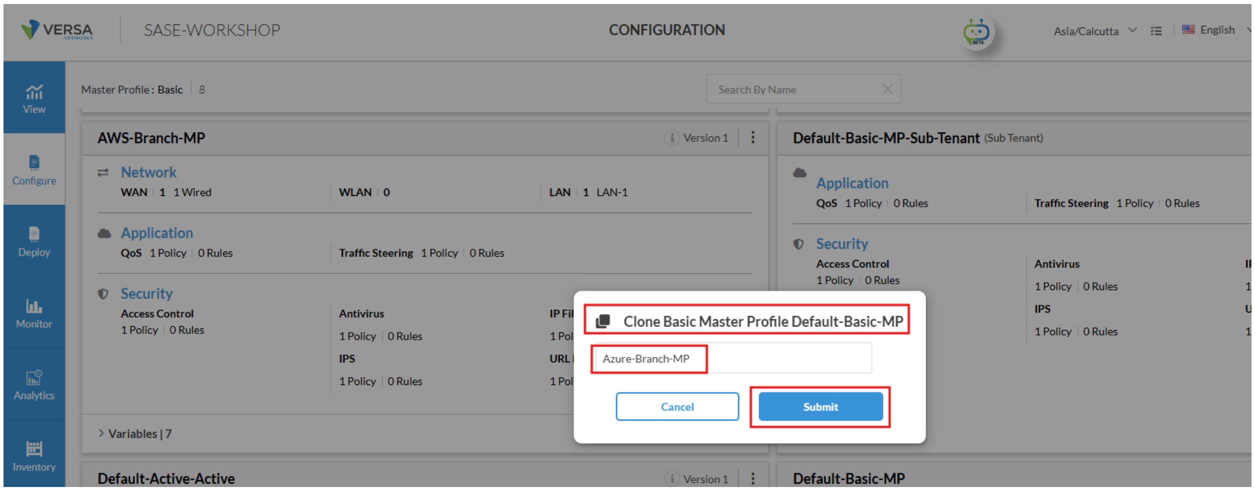
Creating a Basic Master Profile:

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



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

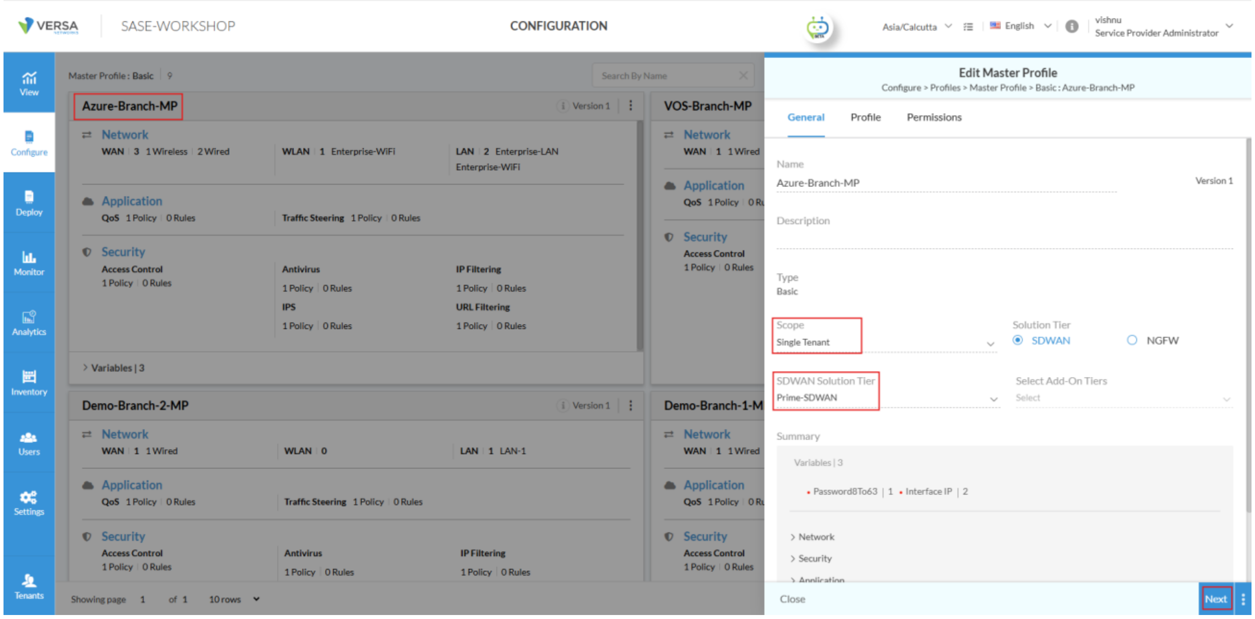




Clone Basic Master Profile Default-Basic-MP

Azure-Branch-MP

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 : Azure-Branch-MP

Name: Azure-Branch-MP — Version 1

Type: Basic

Scope: Single Tenant

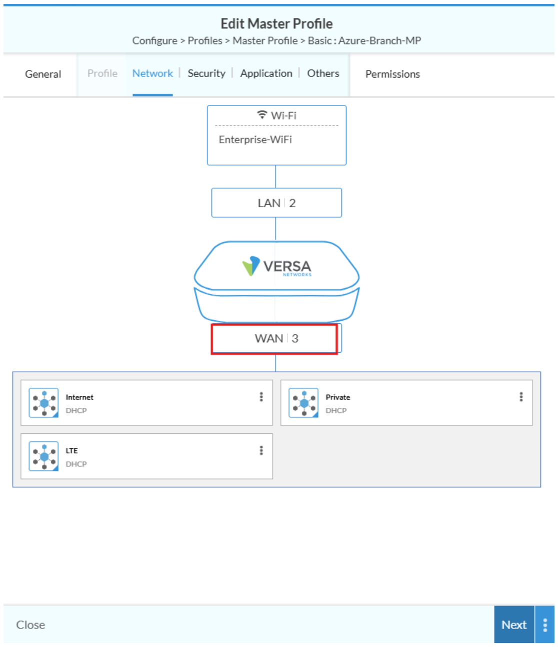
Solution Tier: ● SDWAN ○ NGFW

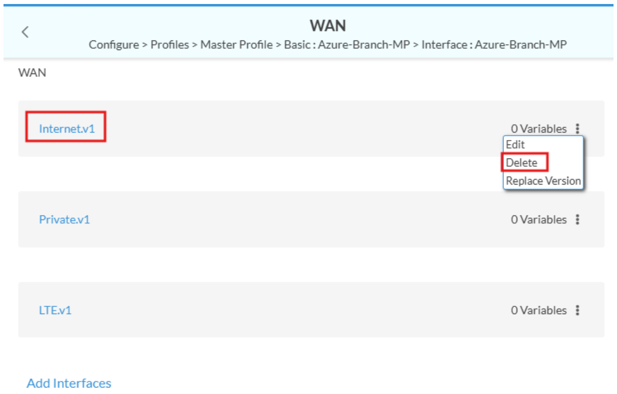
SDWAN Solution Tier: Prime-SDWAN

Select Add-On Tiers: Select

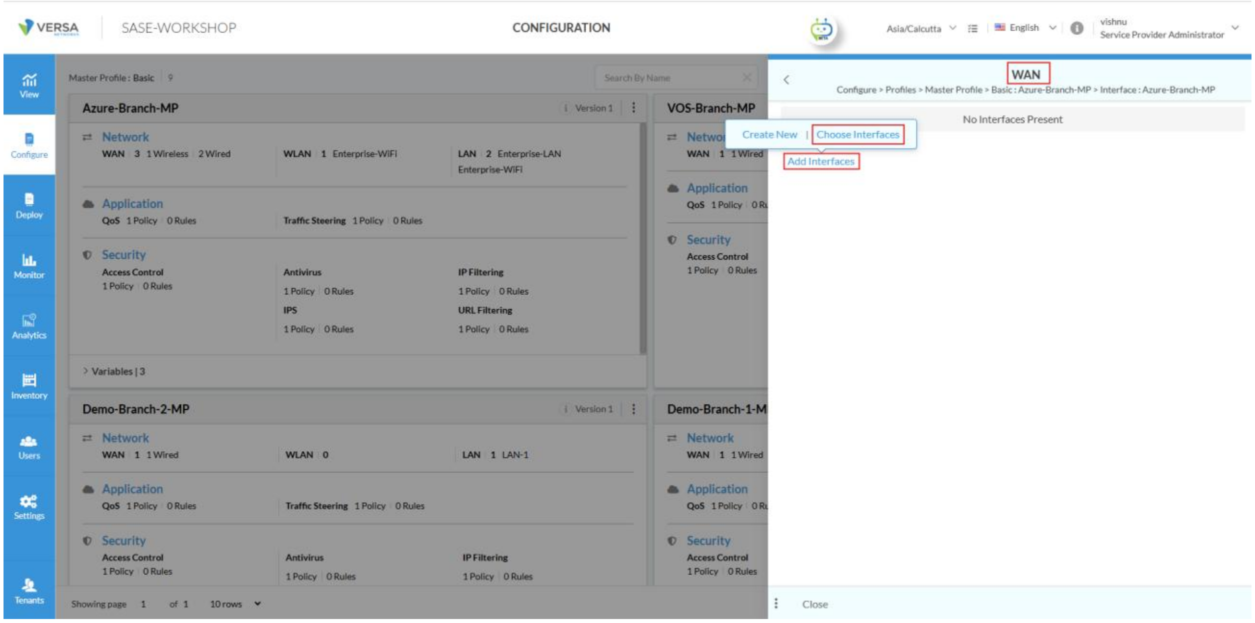
Summary: Variables | 3 — Password8To63 | 1 • Interface IP | 2

Click on WAN and remove all the interfaces.

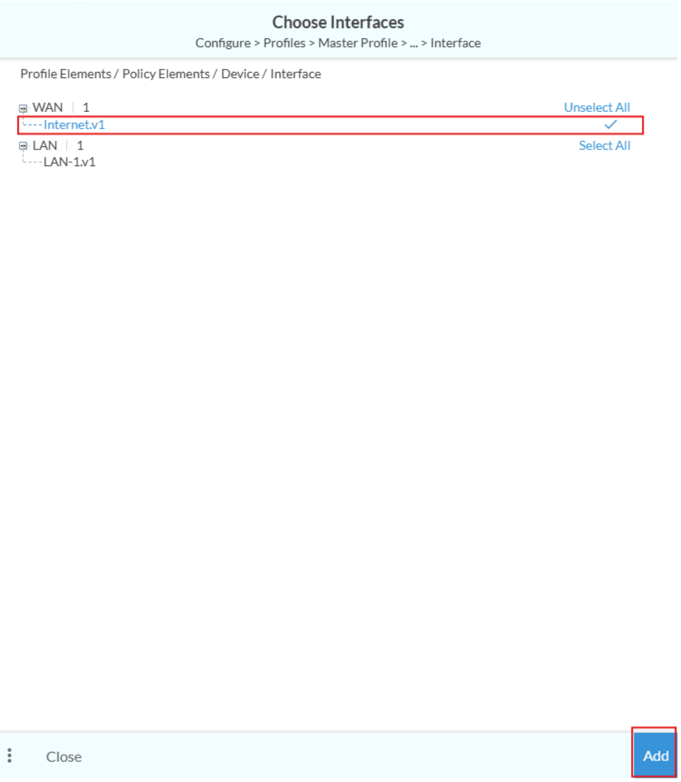




One all the interfaces are removed under WAN, click on “Add Interfaces” and select “Choose Interfaces”.



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 ✓

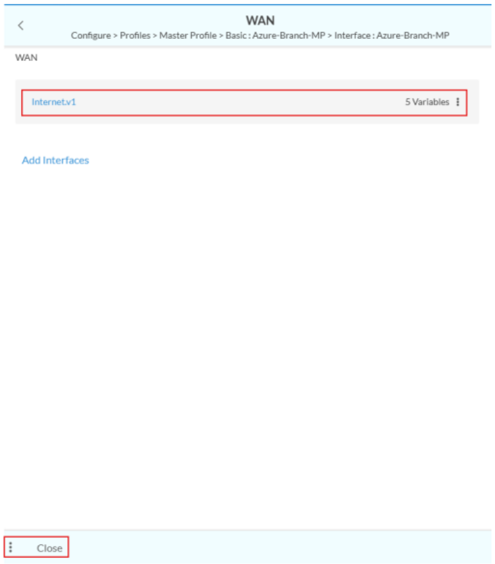
⊟ LAN | 1 Select All

LAN-1.v1

Close

Add

Once added click on Close.



WAN

Configure > Profiles > Master Profile > Basic : Azure-Branch-MP > Interface : Azure-Branch-MP

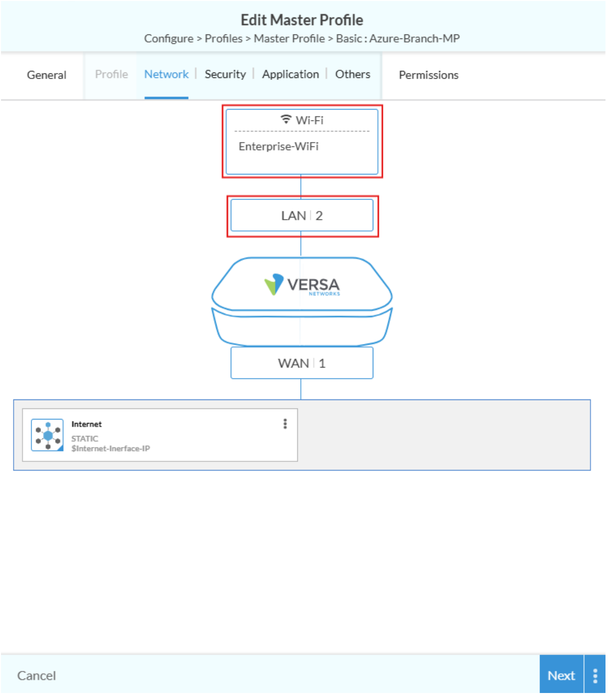
WAN

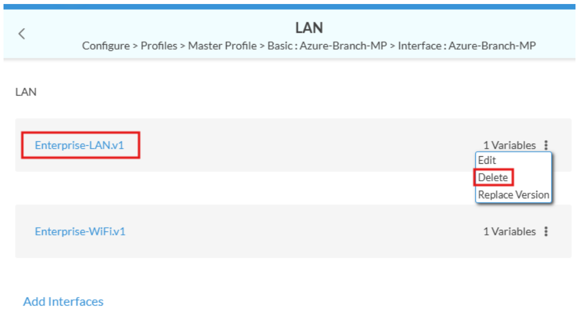
Internet.v1 5 Variables

Add Interfaces

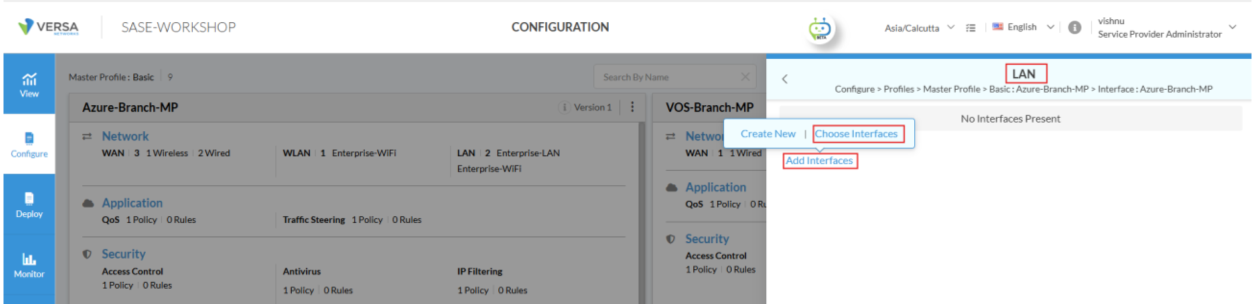
Close

Repeat the same for LAN interfaces

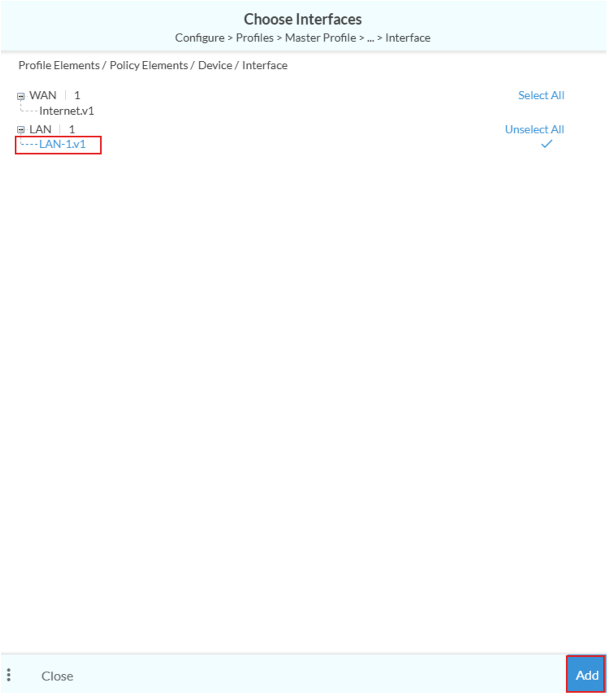




One all the interfaces are removed under LAN, click on "Add Interfaces" and select "Choose Interfaces".



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

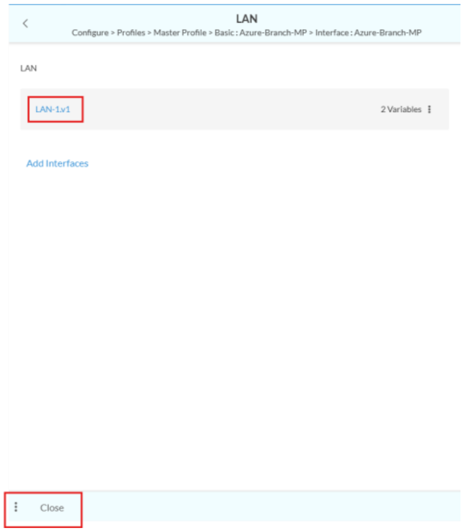


Choose Interfaces

Configure > Profiles > Master Profile > ... > Interface

Profile Elements / Policy Elements / Device / Interface

Once added click on Close.

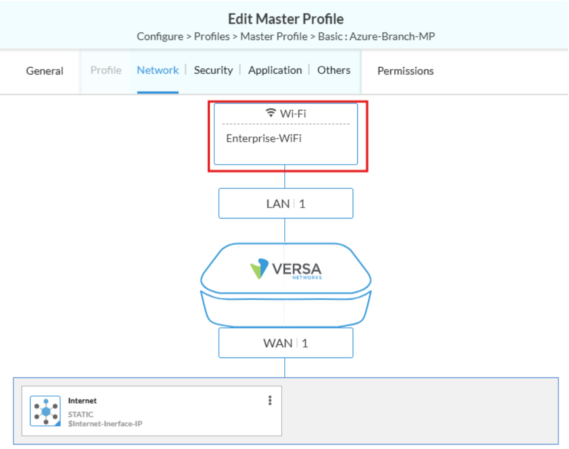


LAN

Configure > Profiles > Master Profile > Basic : Azure-Branch-MP > Interface : Azure-Branch-MP

LAN

Click on “Enterprise WiFi”, select 3 dots and then delete.



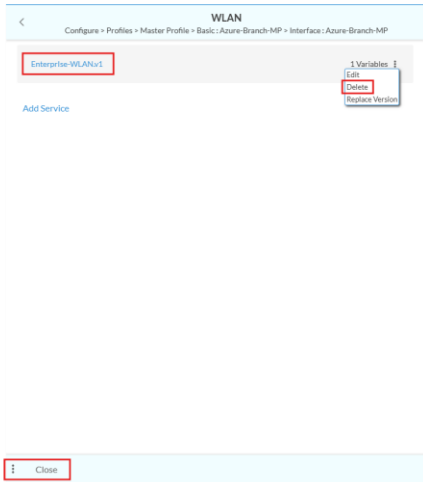
Edit Master Profile

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

Internet

STATIC

$Internet-Inerface-IP



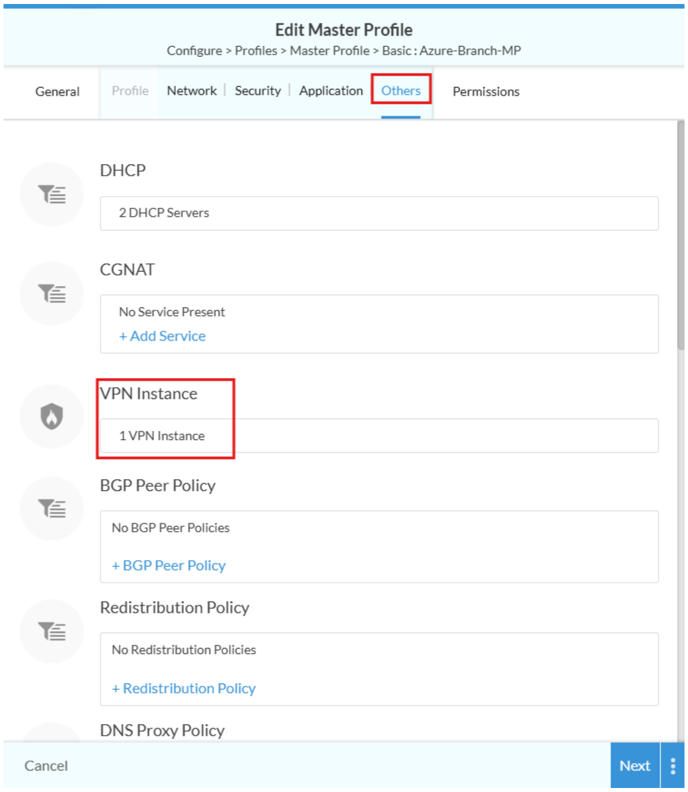
WLAN

Configure > Profiles > Master Profile > Basic : Azure-Branch-MP > Interface : Azure-Branch-MP

Enterprise-WLAN.v1

1 Variables

Once the configuration is complete, move to Others tab and select VPN Instance.



Edit Master Profile

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

DHCP

2 DHCP Servers

CGNAT

No Service Present

VPN Instance

1 VPN Instance

BGP Peer Policy

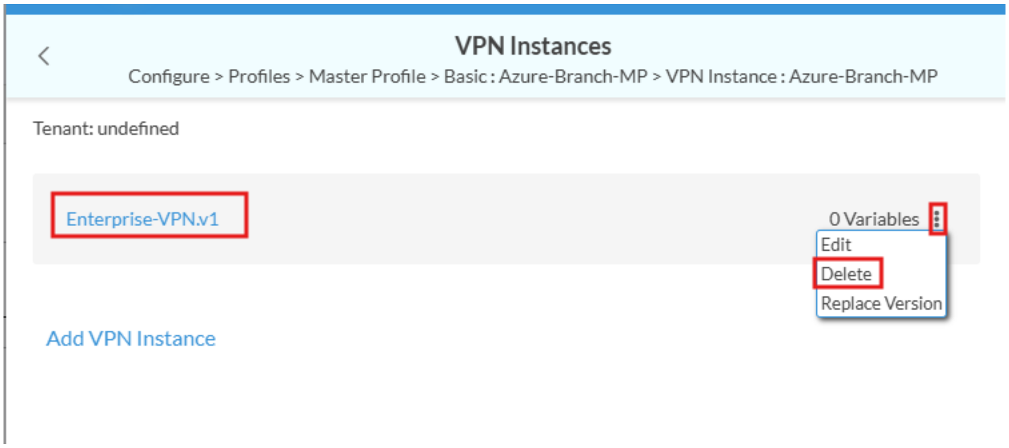
No BGP Peer Policies

Redistribution Policy

No Redistribution Policies

DNS Proxy Policy

Delete the existing VPN instance and add the one which we have created.



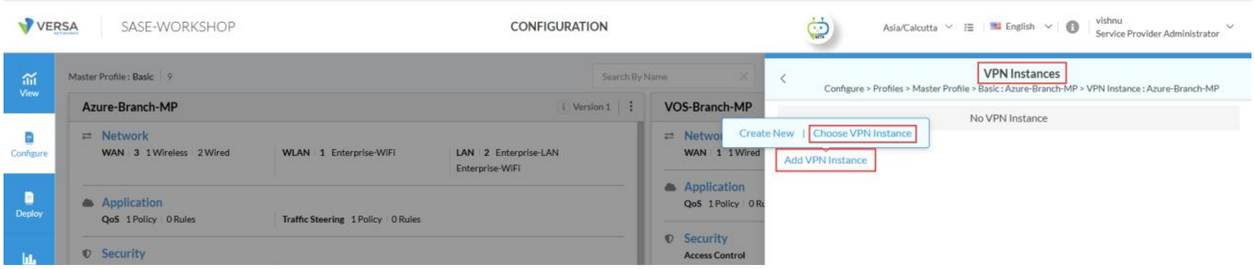
VPN Instances

Configure > Profiles > Master Profile > Basic : Azure-Branch-MP > VPN Instance : Azure-Branch-MP

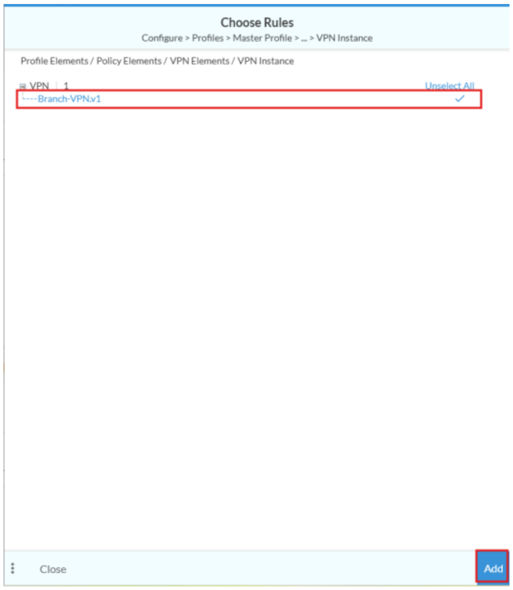
Tenant: undefined

Enterprise-VPN.v1 — 0 Variables

Under VPN Instances, click on “Add VPN Instance” and click on “Choose VPN Instance”.



Select the VPN instance and click on Add.



Choose Rules

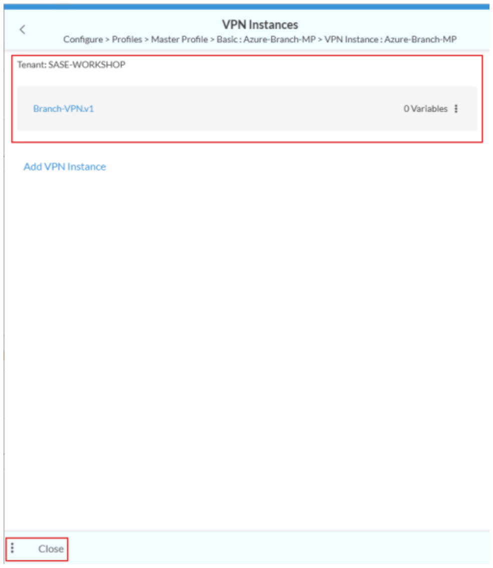
Configure > Profiles > Master Profile > ... > VPN Instance

Profile Elements / Policy Elements / VPN Elements / VPN Instance

VPN 1

Branch-VPN.v1 ✓

Once added, click on “Close” and save the Master profile.

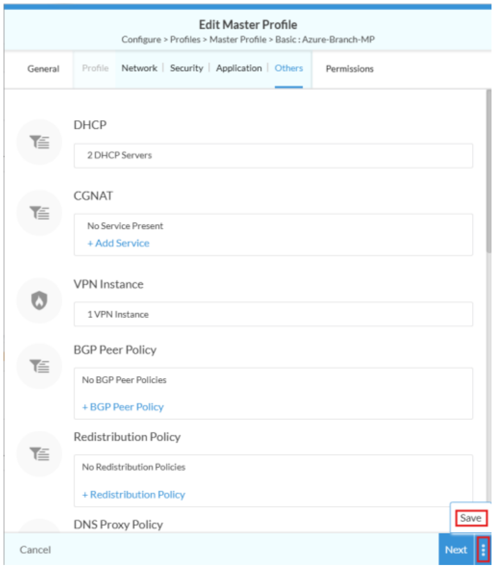


VPN Instances

Configure > Profiles > Master Profile > Basic : Azure-Branch-MP > VPN Instance : Azure-Branch-MP

Tenant: SASE-WORKSHOP

Branch-VPN.v1 0 Variables



Edit Master Profile

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

DHCP: 2 DHCP Servers

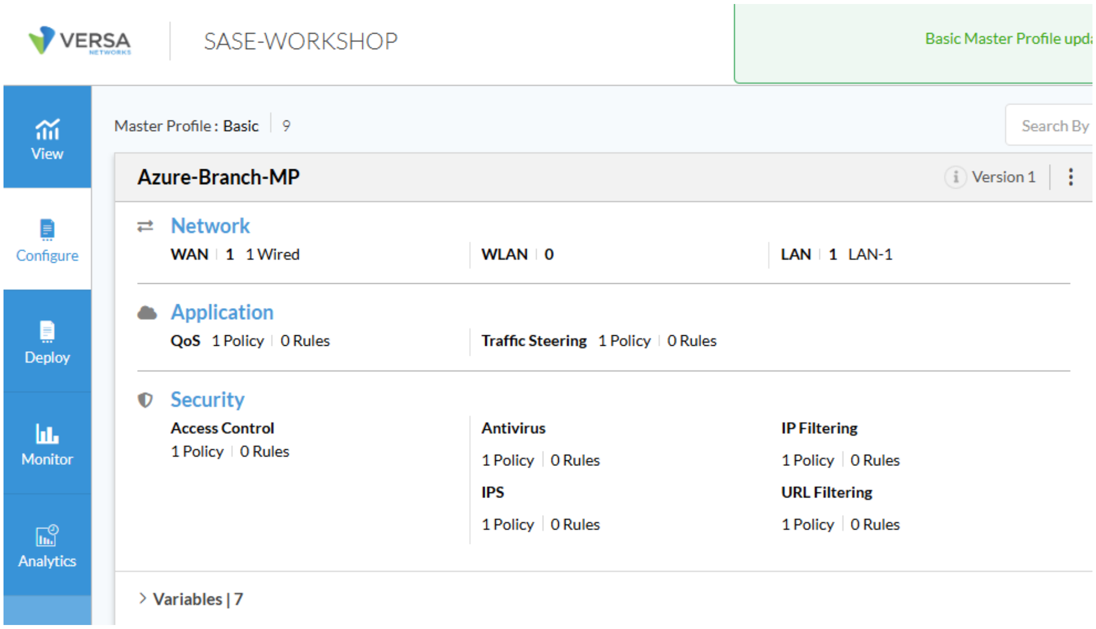
CGNAT: No Service Present

VPN Instance: 1 VPN Instance

BGP Peer Policy: No BGP Peer Policies

Redistribution Policy: No Redistribution Policies

DNS Proxy Policy



SASE-WORKSHOP

Basic Master Profile upd

Master Profile : Basic | 9

Azure-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 1 Policy | 0 Rules

Antivirus 1 Policy | 0 Rules

IP Filtering 1 Policy | 0 Rules

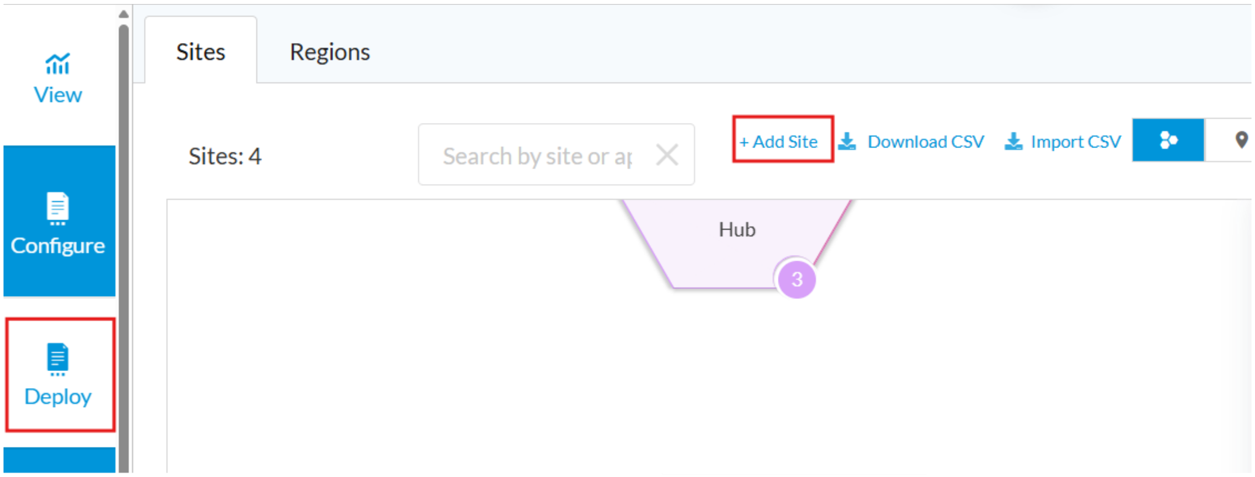
IPS 1 Policy | 0 Rules

URL Filtering 1 Policy | 0 Rules

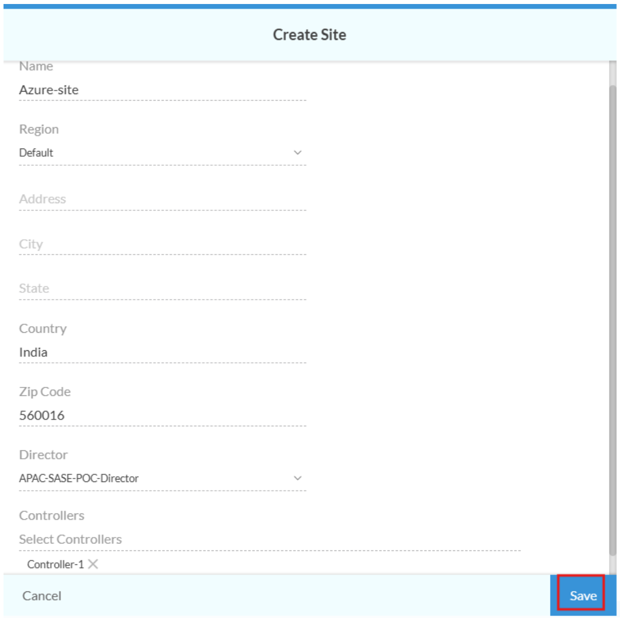
> Variables | 7

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
Azure-site

Region
Default

Address

City

State

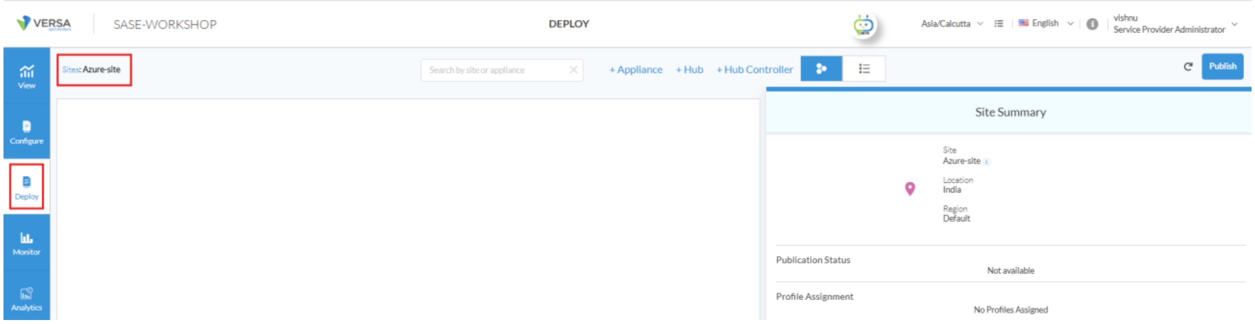
Country
India

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: Azure-site

Site Summary

Site
Azure-site

Location
India

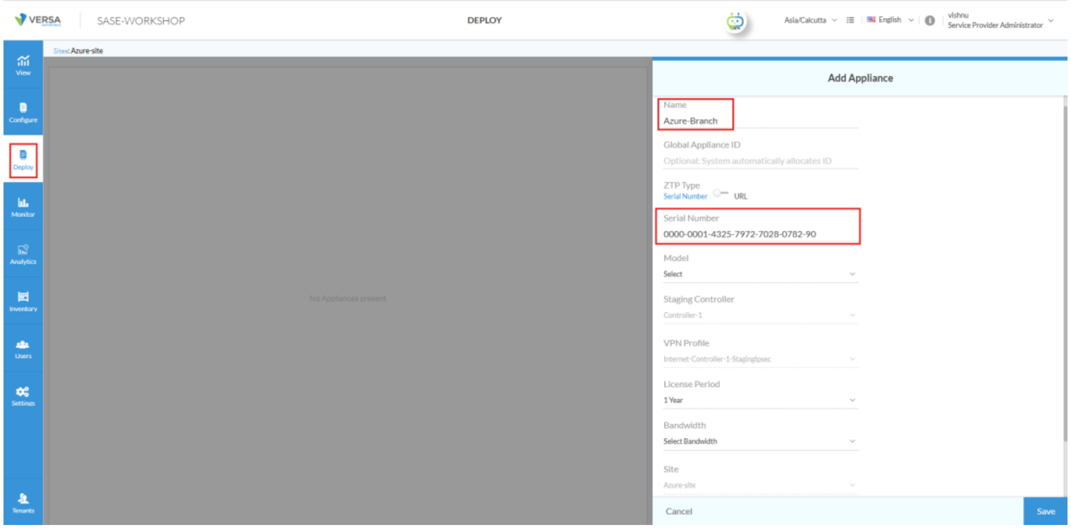
Region
Default

Publication Status
Not available

Profile Assignment
No Profiles Assigned

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.



Add Appliance

Name
Azure-Branch

Global Appliance ID
Optional: System automatically allocates ID

ZTP Type
Serial Number ○— URL

Serial Number
0000-0001-4325-7972-7028-0782-90

Model
Select

Staging Controller
Controller-1

VPN Profile
Internet-Controller-1-StagingIpsec

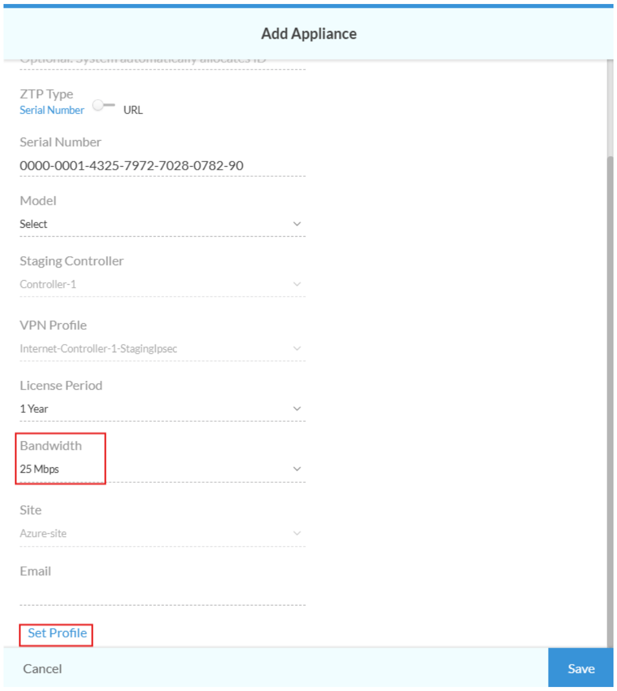
License Period
1 Year

Bandwidth
Select Bandwidth

Site
Azure-site

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.


Add Appliance

Optional: System automatically allocates ID

ZTP Type
Serial Number ○— URL

Serial Number
0000-0001-4325-7972-7028-0782-90

Model
Select

Staging Controller
Controller-1

VPN Profile
Internet-Controller-1-StagingIpsec

License Period
1 Year

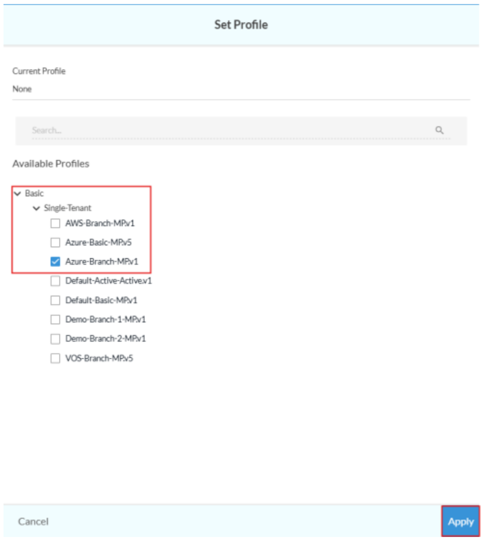
Bandwidth
25 Mbps

Site
Azure-site

Email

Set Profile

Cancel | Save


Set Profile

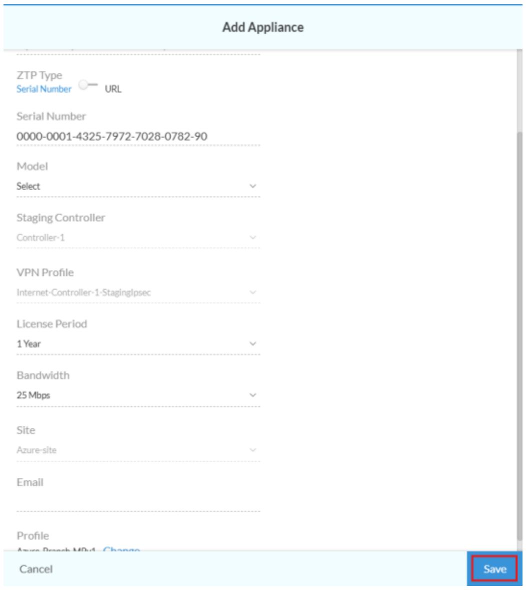
Current Profile
None

Search...

Available Profiles

- Basic
  - Single-Tenant
    - ☐ AWS-Branch-MP.v1
    - ☐ Azure-Basic-MP.v5
    - ☑ Azure-Branch-MP.v1
    - ☐ Default-Active-Active.v1
    - ☐ Default-Basic-MP.v1
    - ☐ Demo-Branch-1-MP.v1
    - ☐ Demo-Branch-2-MP.v1
    - ☐ VOS-Branch-MP.v5

Cancel | Apply



Add Appliance

ZTP Type
Serial Number URL

Serial Number
0000-0001-4325-7972-7028-0782-90

Model
Select

Staging Controller
Controller-1

VPN Profile
Internet-Controller-1-StagingIpsec

License Period
1 Year

Bandwidth
25 Mbps

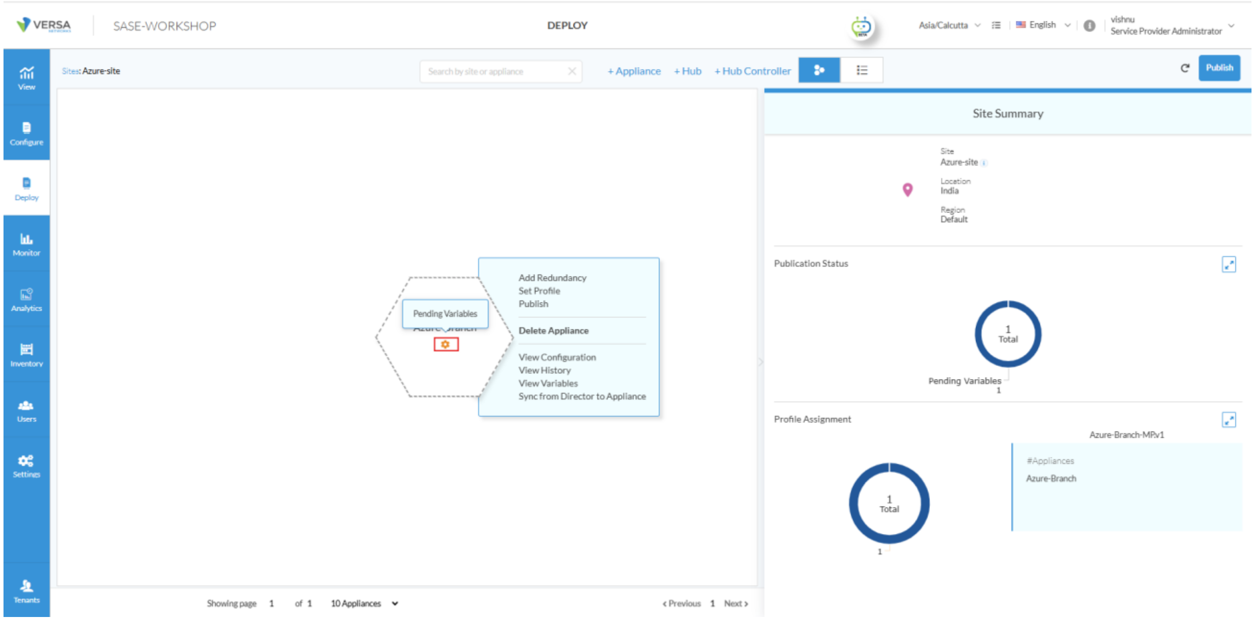
Site
Azure-site

Email

Profile
Azure-Branch-MP-v1 Change

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.



Sites: Azure-site

Site Summary

Site
Azure-site

Location
India

Region
Default

Publication Status

1 Total

Pending Variables
1

Profile Assignment

Azure-Branch-MP.v1

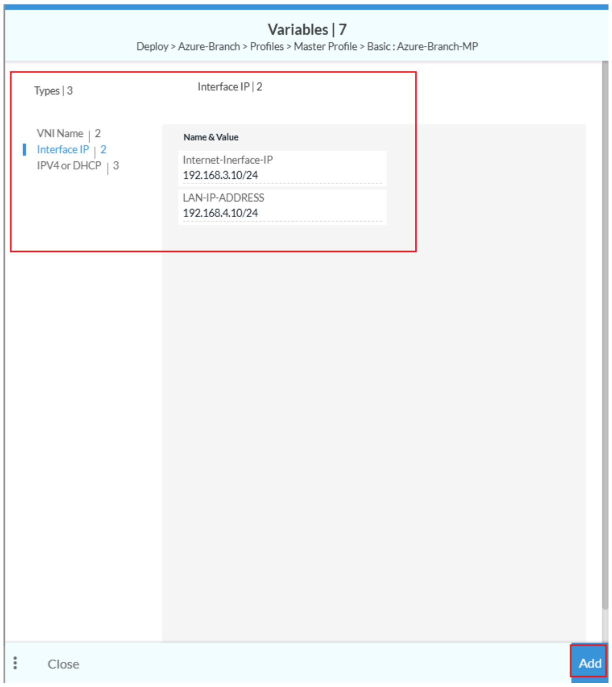
1 Total

1

#Appliances
Azure-Branch

Add the pending variables and click on Add.

Review the configuration of the appliance and click on Save.



Variables | 7

Deploy > Azure-Branch > Profiles > Master Profile > Basic : Azure-Branch-MP

Types | 3

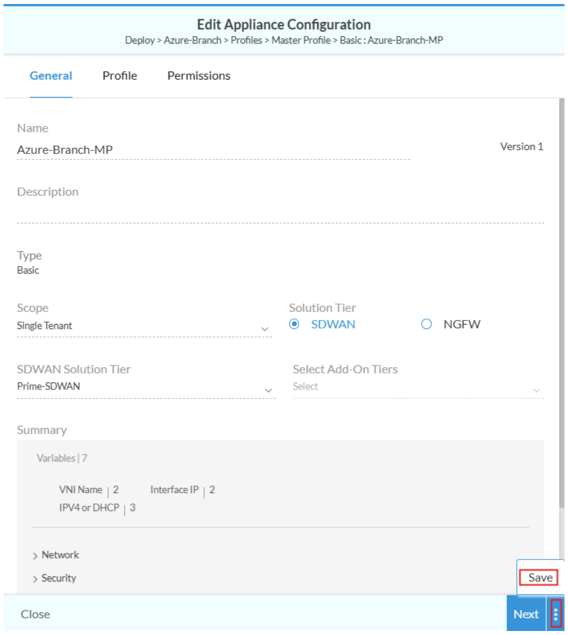
VNI Name | 2
Interface IP | 2
IPV4 or DHCP | 3

Interface IP | 2

Name & Value

Internet-Inerface-IP
192.168.3.10/24

LAN-IP-ADDRESS
192.168.4.10/24



Edit Appliance Configuration

Deploy > Azure-Branch > Profiles > Master Profile > Basic : Azure-Branch-MP

Name: Azure-Branch-MP

Version 1

Description

Type: Basic

Scope: Single Tenant

Solution Tier: ● SDWAN ○ NGFW

SDWAN Solution Tier: Prime-SDWAN

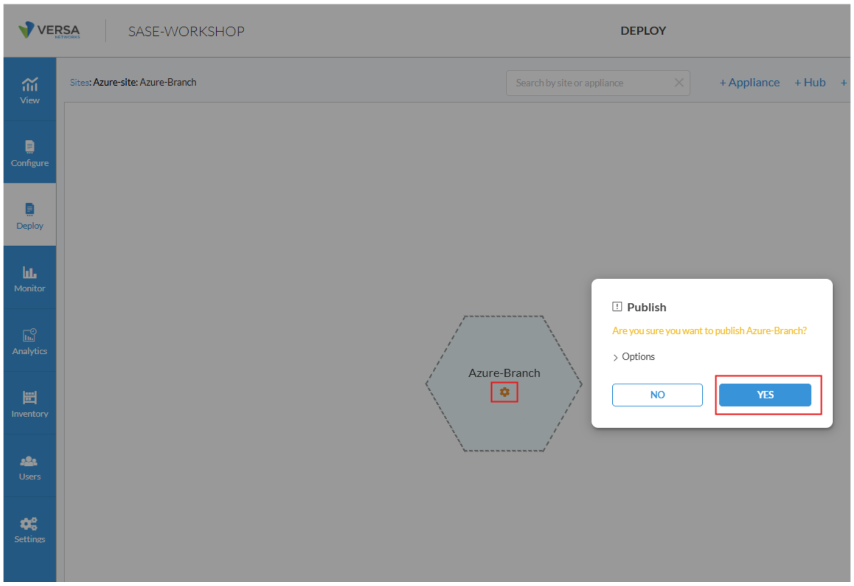
Select Add-On Tiers: Select

Summary

Variables | 7

VNI Name | 2
Interface IP | 2
IPV4 or DHCP | 3

To Publish the configuration on to the Director, click on Publish.

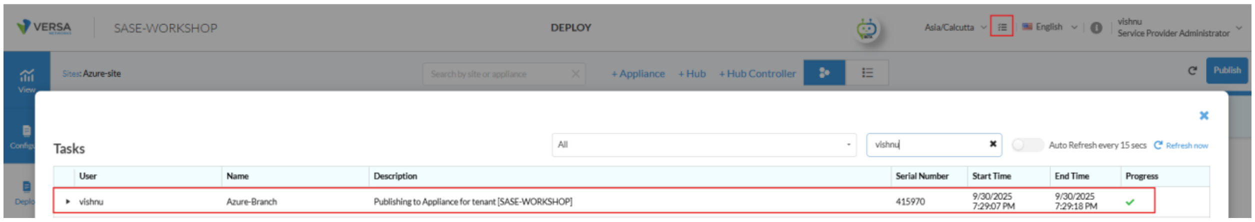


Publish

Are you sure you want to publish Azure-Branch?

> Options

Once the device is published, we can check the status in the tasks.



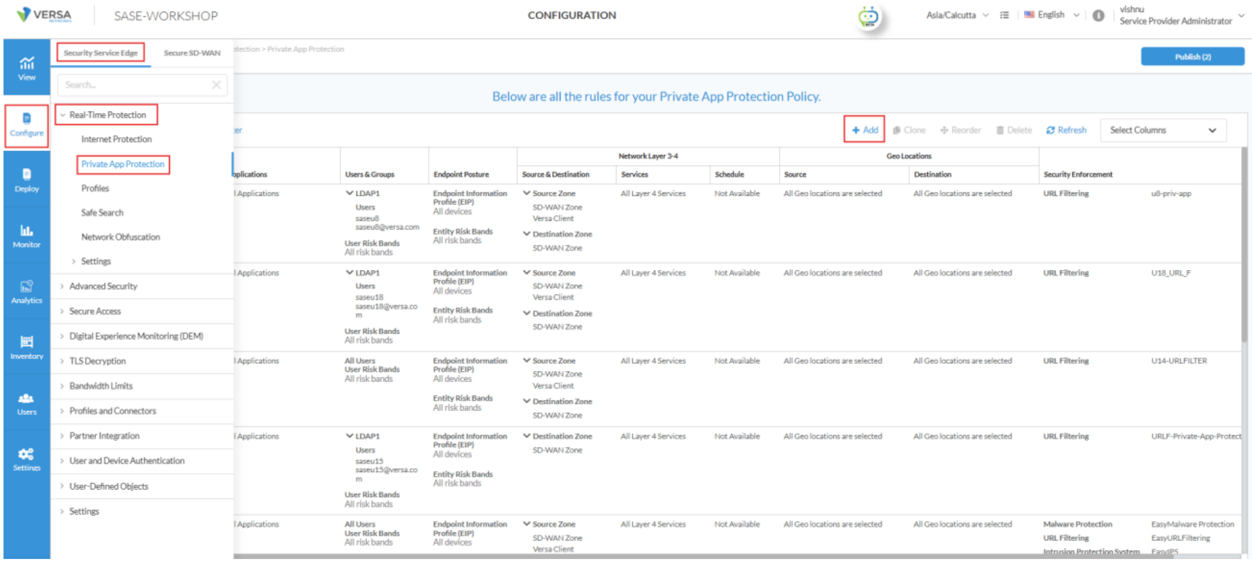
Tasks

All | vishnu | Auto Refresh every 15 secs | Refresh now

User	Name	Description	Serial Number	Start Time	End Time	Progress
▸ vishnu	Azure-Branch	Publishing to Appliance for tenant [SASE-WORKSHOP]	415970	9/30/2025 7:29:07 PM	9/30/2025 7:29:18 PM	✓

Configuring Private app Protection Rule:

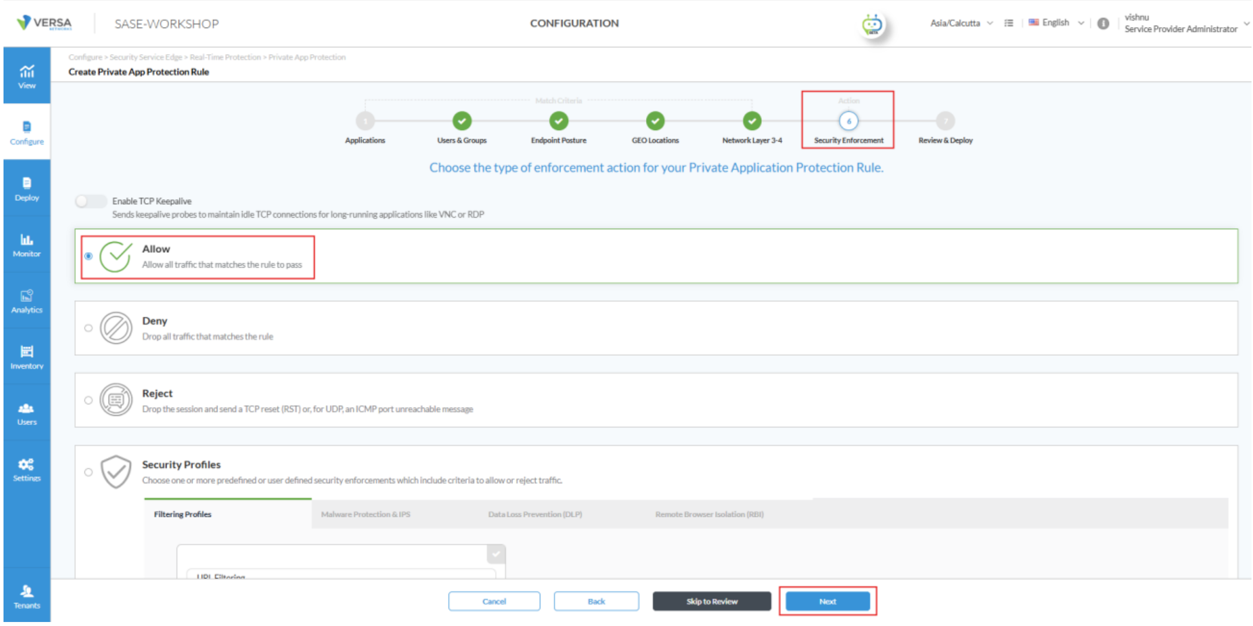
To Create a secure access rule for allowing traffic from SASE clients to Azure VM through overlay tunnels, Go to Configure → Secure Service Edge → Real-Time Protection → Private App Protection and click on “Add”.



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 Users saseu8 saseu8@versa.com User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Source Zone SD-WAN Zone Versa Client Destination Zone 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 Users saseu18 saseu18@versa.com User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Source Zone SD-WAN Zone Versa Client Destination Zone 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 User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Source Zone SD-WAN Zone Versa Client Destination Zone 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 Users saseu15 saseu15@versa.com User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Destination Zone 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 User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices	Source Zone SD-WAN Zone Versa Client	All Layer 4 Services	Not Available	All Geo locations are selected	All Geo locations are selected	Malware Protection URL Filtering Intrusion Protection System	EasyMalware Protection EasyURLFiltering EasyIPS

Leave everything to default and Under “Security Enforcement” Configure the action as “Allow”.



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

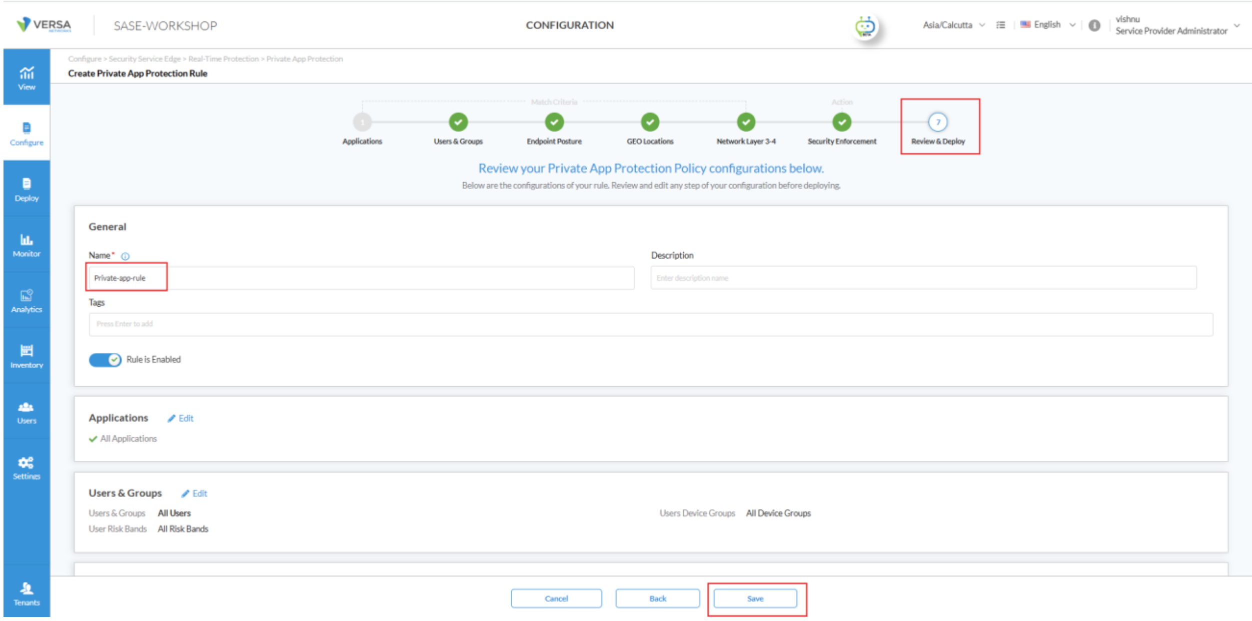
○ Deny
Drop all traffic that matches the rule

○ 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

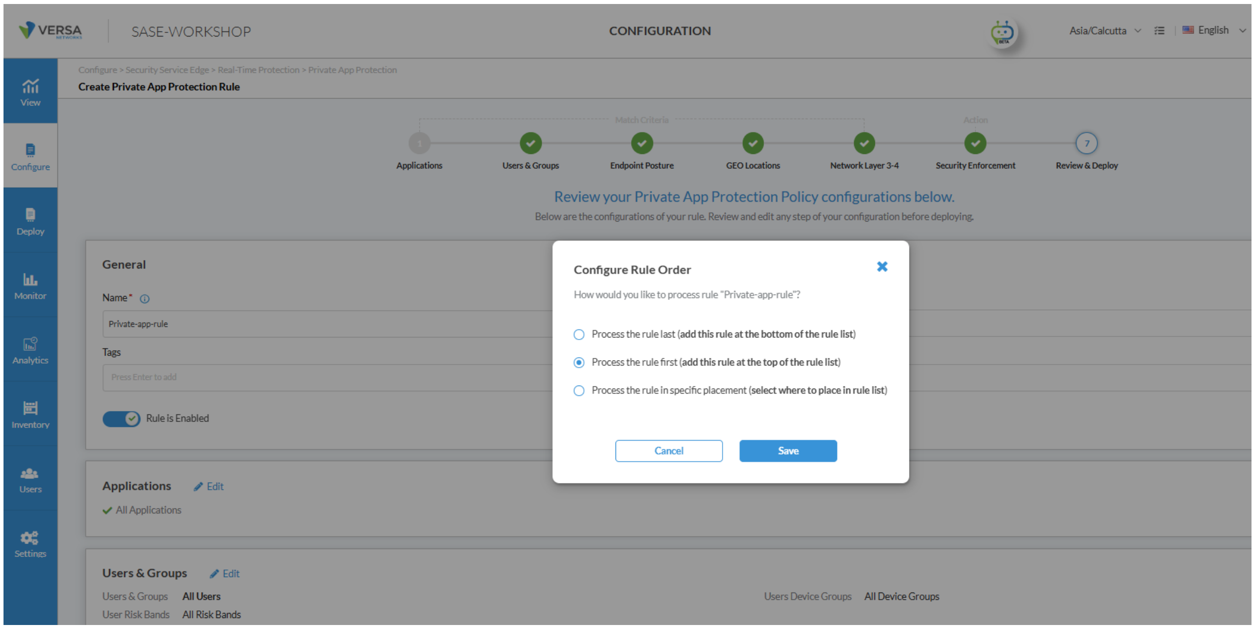
Users & Groups Edit

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 Rule Order

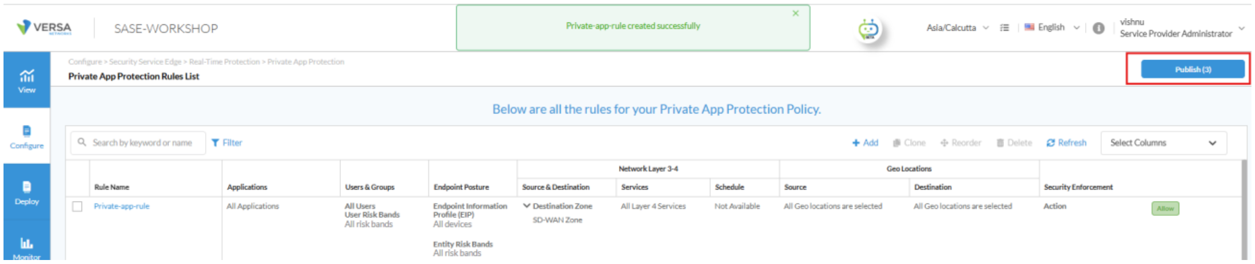
How would you like to process rule "Private-app-rule"?

○ 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)

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

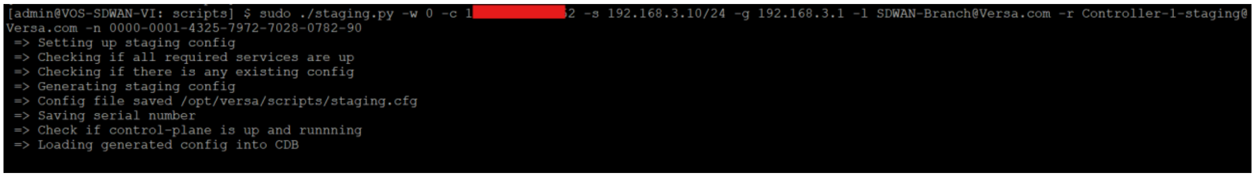
Private App Protection Rules List

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 User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Destination Zone SD-WAN Zone	All Layer 4 Services	Not Available	All Geo locations are selected	All Geo locations are selected	Action Allow

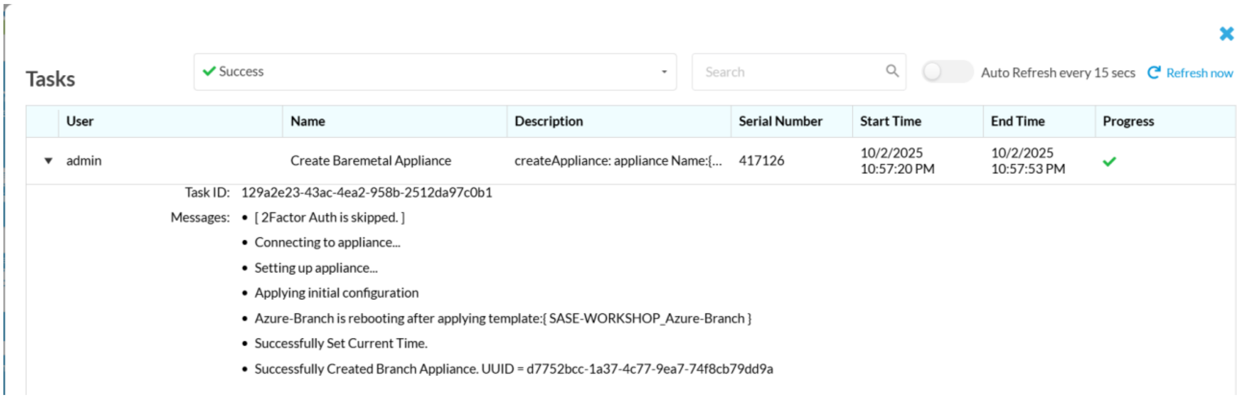
Onboarding VOS:

To perform ZTP, run the staging.py script



```
[admin@VOS-SDWAN-VI: scripts] $ sudo ./staging.py -w 0 -c 1[redacted]2 -s 192.168.3.10/24 -g 192.168.3.1 -l SDWAN-Branch@Versa.com -r Controller-1-staging@
Versa.com -n 0000-0001-4325-7972-7028-0782-90
 => 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.



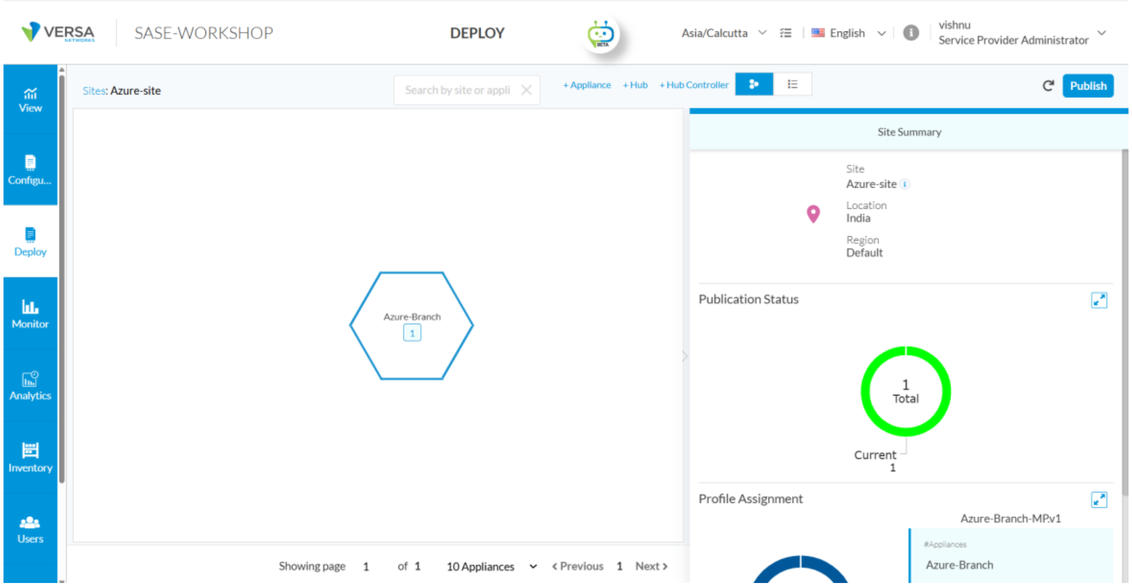
	User	Name	Description	Serial Number	Start Time	End Time	Progress
▾	admin	Create Baremetal Appliance	createAppliance: appliance Name:{...	417126	10/2/2025 10:57:20 PM	10/2/2025 10:57:53 PM	✓

Task ID: 129a2e23-43ac-4ea2-958b-2512da97c0b1

Messages:

- [2Factor Auth is skipped.]
- Connecting to appliance...
- Setting up appliance...
- Applying initial configuration
- Azure-Branch is rebooting after applying template:{ SASE-WORKSHOP_Azure-Branch }
- Successfully Set Current Time.
- Successfully Created Branch Appliance. UUID = d7752bcc-1a37-4c77-9ea7-74f8cb79dd9a

Once the device is onboarded it will show up in Concerto.

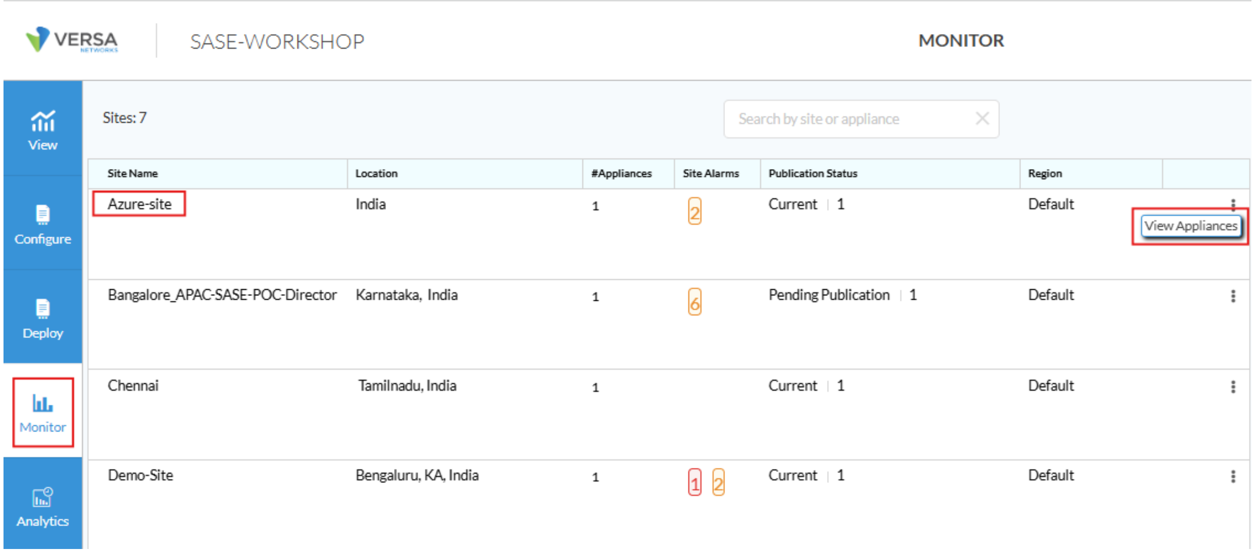


Verification

Verifying Routing on VOS Azure-Branch:

Dynamic tunnels between VOS AWS-Branch and SASE Gateway should be up.

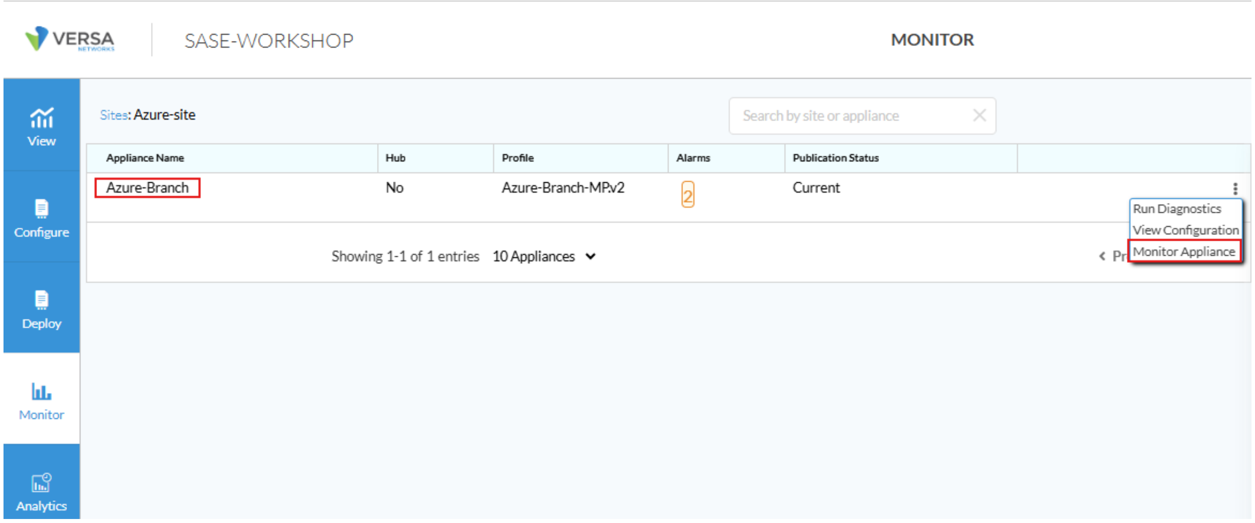
To view the tunnel status, click on “Monitor”, go to respective Site and click on “View Appliance”.



Sites: 7

Site Name	Location	#Appliances	Site Alarms	Publication Status	Region	
Azure-site	India	1	2	Current | 1	Default	View Appliances
Bangalore_APAC-SASE-POC-Director	Karnataka, India	1	6	Pending Publication | 1	Default	
Chennai	Tamilnadu, India	1		Current | 1	Default	
Demo-Site	Bengaluru, KA, India	1	1 2	Current | 1	Default	

Click on “Monitor Appliance” under respective appliance.

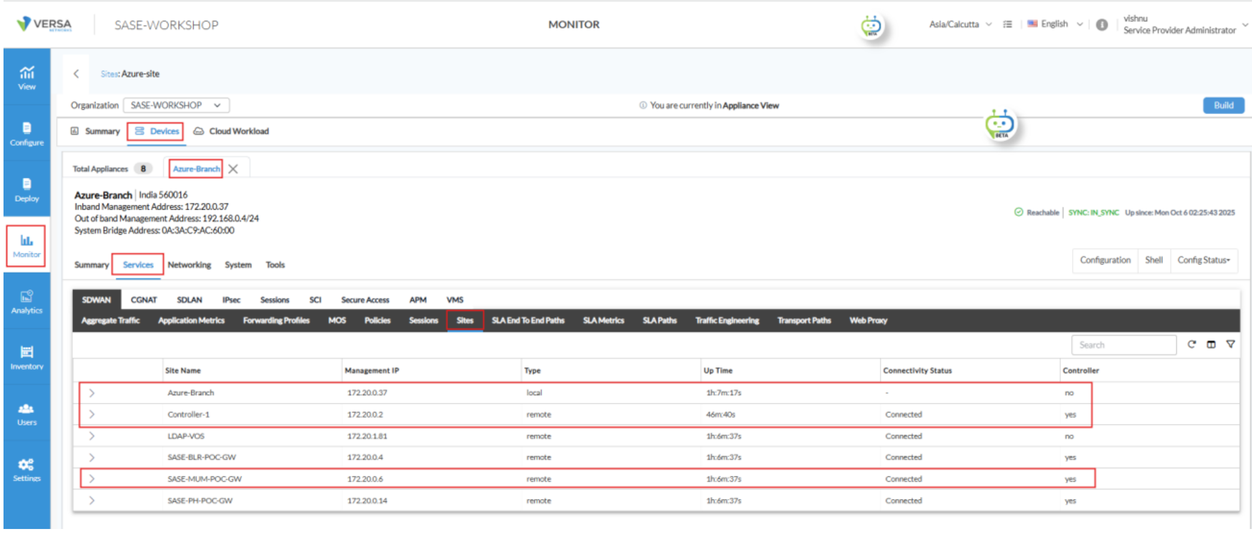


Sites: Azure-site

Appliance Name	Hub	Profile	Alarms	Publication Status	
Azure-Branch	No	Azure-Branch-MP.v2	2	Current	

Showing 1-1 of 1 entries 10 Appliances

Under Monitor → Devices → <Branch Name> → Services → SDWAN → Sites. Make sure all the devices are connected.



Sites: Azure-site

Organization: SASE-WORKSHOP

You are currently in Appliance View

Total Appliances 8 | Azure-Branch

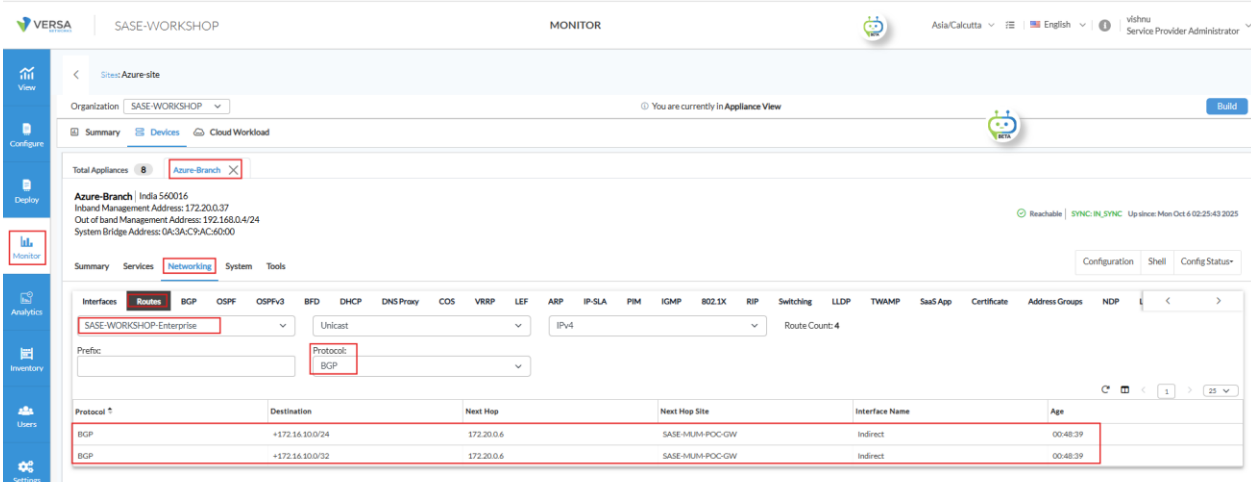
Azure-Branch | India 560016
Inband Management Address: 172.20.0.37
Out of band Management Address: 192.168.0.4/24
System Bridge Address: 0A:3A:C9:AC:60:00

Reachable | SYNC: IN_SYNC Up since: Mon Oct 6 02:25:43 2025

Summary | Services | Networking | System | Tools

Site Name	Management IP	Type	Up Time	Connectivity Status	Controller
Azure-Branch	172.20.0.37	local	1h:7m:17s	-	no
Controller-1	172.20.0.2	remote	46m:40s	Connected	yes
LDAP-VOS	172.20.1.81	remote	1h:6m:37s	Connected	no
SASE-BLR-POC-GW	172.20.0.4	remote	1h:6m:37s	Connected	yes
SASE-MUM-POC-GW	172.20.0.6	remote	1h:6m:37s	Connected	yes
SASE-PH-POC-GW	172.20.0.14	remote	1h:6m:37s	Connected	yes

To view the SASE Client routes received, Go to Networking and check the Routes under the Enterprise LAN VR.



Sites: Azure-site

Organization: SASE-WORKSHOP

You are currently in Appliance View

Total Appliances 8 | Azure-Branch

Azure-Branch | India 560016
Inband Management Address: 172.20.0.37
Out of band Management Address: 192.168.0.4/24
System Bridge Address: 0A:3A:C9:AC:60:00

Reachable | SYNC: IN_SYNC Up since: Mon Oct 6 02:25:43 2025

Summary | Services | Networking | System | Tools

SASE-WORKSHOP-Enterprise | Unicast | IPv4 | Route Count: 4

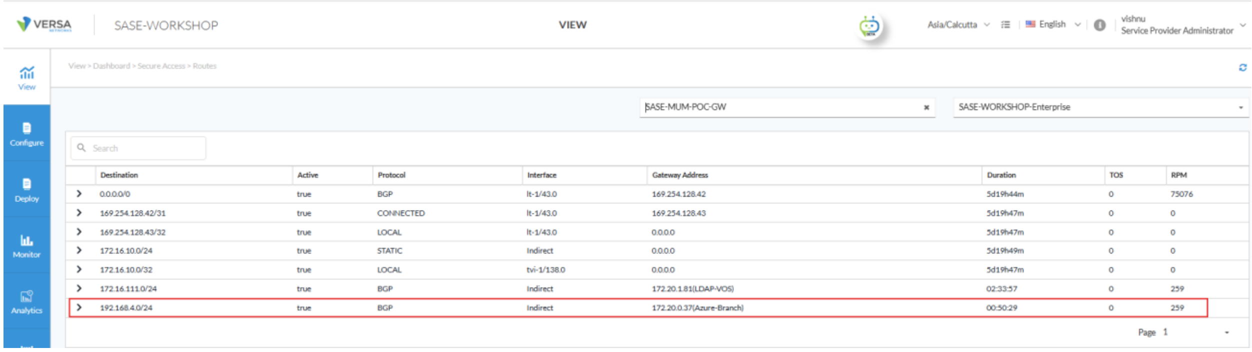
Prefix:

Protocol: BGP

Protocol	Destination	Next Hop	Next Hop Site	Interface Name	Age
BGP	+172.16.10.0/24	172.20.0.6	SASE-MUM-POC-GW	Indirect	00:48:39
BGP	+172.16.10.0/32	172.20.0.6	SASE-MUM-POC-GW	Indirect	00:48:39

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-MUM-POC-GW | SASE-WORKSHOP-Enterprise

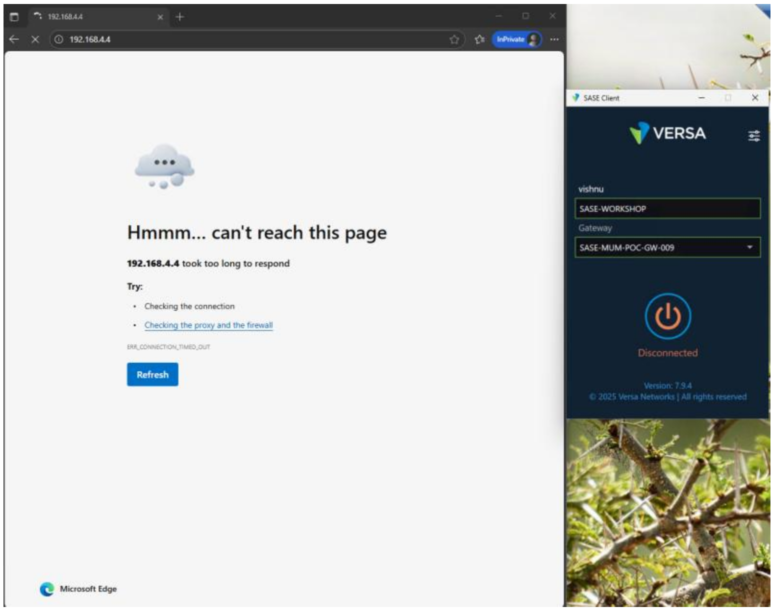
Destination	Active	Protocol	Interface	Gateway Address	Duration	TOS	RPM
0.0.0.0/0	true	BGP	lt-1/43.0	169.254.128.42	5d19h44m	0	75076
169.254.128.42/31	true	CONNECTED	lt-1/43.0	169.254.128.43	5d19h47m	0	0
169.254.128.43/32	true	LOCAL	lt-1/43.0	0.0.0.0	5d19h47m	0	0
172.16.10.0/24	true	STATIC	Indirect	0.0.0.0	5d19h49m	0	0
172.16.10.0/32	true	LOCAL	tvi-1/138.0	0.0.0.0	5d19h47m	0	0
172.16.111.0/24	true	BGP	Indirect	172.20.1.81(LDAP-VOS)	02:33:57	0	259
192.168.4.0/24	true	BGP	Indirect	172.20.0.37(Azure-Branch)	00:50:29	0	259

Page 1

Verifying Connectivity:

Accessing Azure VM instance with IP: 192.168.4.4 from PC connected to SASE Client.

When the SASE Client is not connected to Gateway, we were unable to reach the Azure VM instance over Private IP.



Hmmm... can't reach this page

192.168.4.4 took too long to respond

Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_TIMED_OUT

vishnu

SASE-WORKSHOP

Gateway

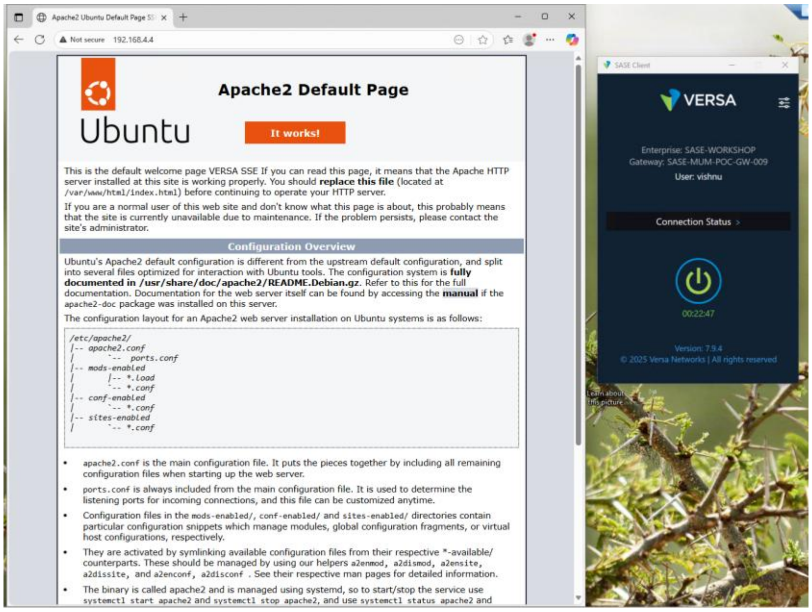
SASE-MUM-POC-GW-009

Disconnected

Version: 7.9.4

© 2025 Versa Networks | All rights reserved

When the SASE Client is connected to the Gateway, we were able to reach the Azure VM instance over Private IP.



Apache2 Default Page

It works!

This is the default welcome page VERSA SSE If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) 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 means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers a2enmod, a2dismod, a2ensite, a2dissite, and a2enconf, a2disconf . See their respective man pages for detailed information.
- The binary is called apache2 and is managed using systemd, so to start/stop the service use systemctl start apache2 and systemctl stop apache2, and use systemctl status apache2 and

Enterprise: SASE-WORKSHOP

Gateway: SASE-MUM-POC-GW-009

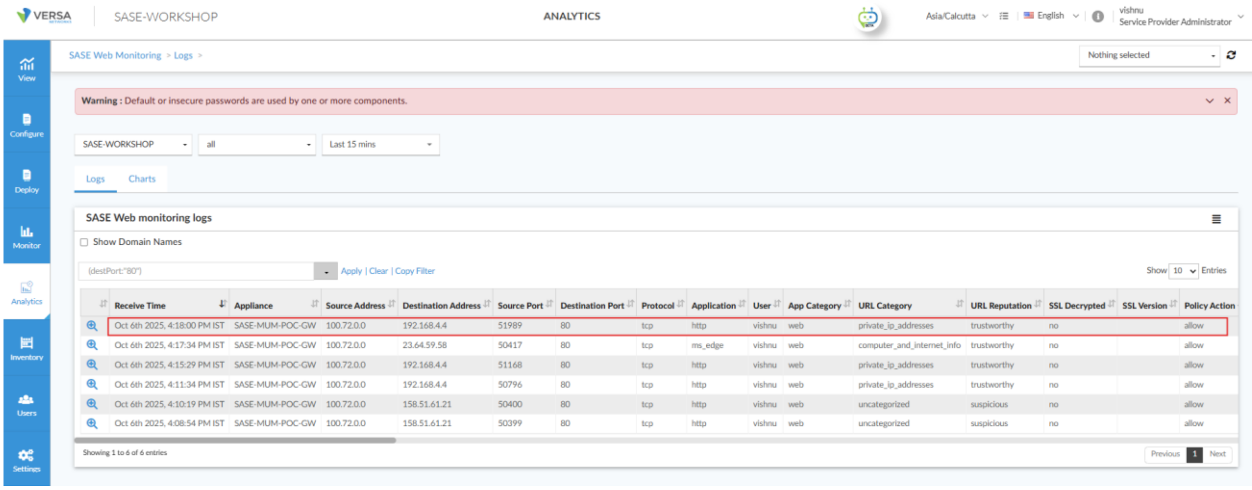
User: vishnu

00:22:47

Version: 7.9.4

© 2025 Versa Networks | All rights reserved

SASE-WEB LOGS on Analytics:



Warning : Default or insecure passwords are used by one or more components.

SASE Web monitoring logs

□ Show Domain Names

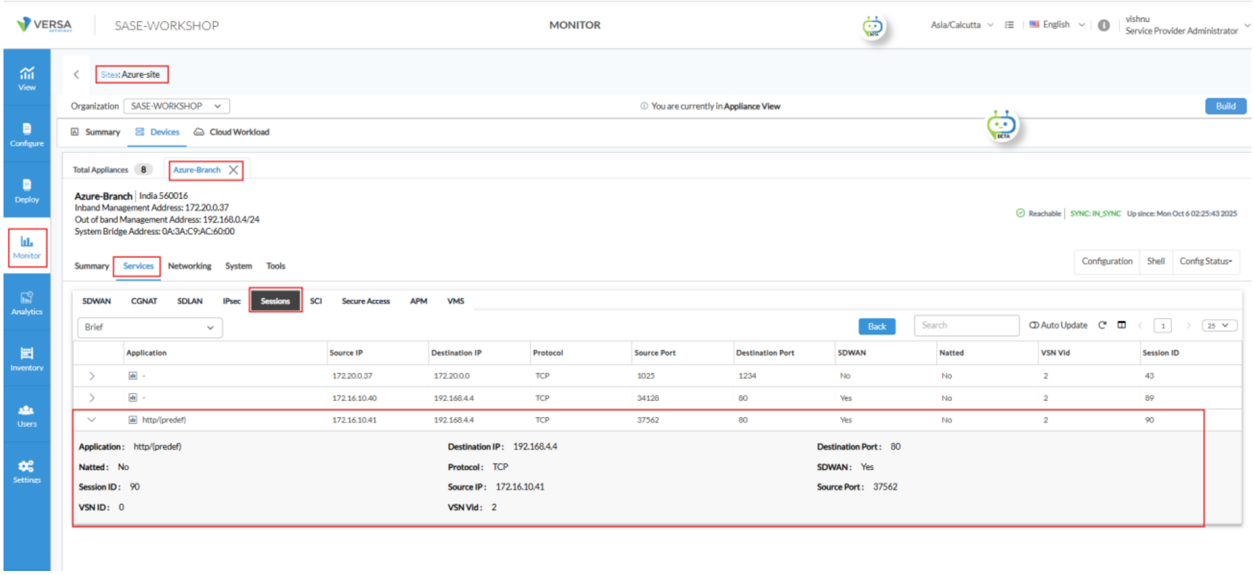
(destPort:"80")

Receive Time	Appliance	Source Address	Destination Address	Source Port	Destination Port	Protocol	Application	User	App Category	URL Category	URL Reputation	SSL Decrypted	SSL Version	Policy Action
Oct 6th 2025, 4:18:00 PM IST	SASE-MUM-POC-GW	100.72.0.0	192.168.4.4	51989	80	tcp	http	vishnu	web	private_ip_addresses	trustworthy	no		allow
Oct 6th 2025, 4:17:34 PM IST	SASE-MUM-POC-GW	100.72.0.0	23.64.59.58	50417	80	tcp	ms_edge	vishnu	web	computer_and_internet_info	trustworthy	no		allow
Oct 6th 2025, 4:15:29 PM IST	SASE-MUM-POC-GW	100.72.0.0	192.168.4.4	51168	80	tcp	http	vishnu	web	private_ip_addresses	trustworthy	no		allow
Oct 6th 2025, 4:11:34 PM IST	SASE-MUM-POC-GW	100.72.0.0	192.168.4.4	50796	80	tcp	http	vishnu	web	private_ip_addresses	trustworthy	no		allow
Oct 6th 2025, 4:10:19 PM IST	SASE-MUM-POC-GW	100.72.0.0	158.51.61.21	50400	80	tcp	http	vishnu	web	uncategorized	suspicious	no		allow
Oct 6th 2025, 4:08:54 PM IST	SASE-MUM-POC-GW	100.72.0.0	158.51.61.21	50399	80	tcp	http	vishnu	web	uncategorized	suspicious	no		allow

Showing 1 to 6 of 6 entries

Session Table on Azure Branch:

You should be able to View the session information Under Monitor → Devices → <Branch Name> → Services → Sessions.



You are currently in **Appliance View**

Azure-Branch | India 560016
Inband Management Address: 172.20.0.37
Out of band Management Address: 192.168.0.4/24
System Bridge Address: 0A:3A:C9:AC:60:00

Reachable | SYNC: IN_SYNC Up since: Mon Oct 6 02:25:43 2025

Application	Source IP	Destination IP	Protocol	Source Port	Destination Port	SDWAN	Natted	VSN Vid	Session ID
-	172.20.0.37	172.20.0.0	TCP	1025	1234	No	No	2	43
-	172.16.10.40	192.168.4.4	TCP	34128	80	Yes	No	2	89
http/(predef)	172.16.10.41	192.168.4.4	TCP	37562	80	Yes	No	2	90

Application : http/(predef)
Natted : No
Session ID : 90
VSN ID : 0
Destination IP : 192.168.4.4
Protocol : TCP
Source IP : 172.16.10.41
VSN Vid : 2
Destination Port : 80
SDWAN : Yes
Source Port : 37562

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.