Configure a Public Cloud Device To Be a Virtual CPE Router or an SD-WAN Gateway

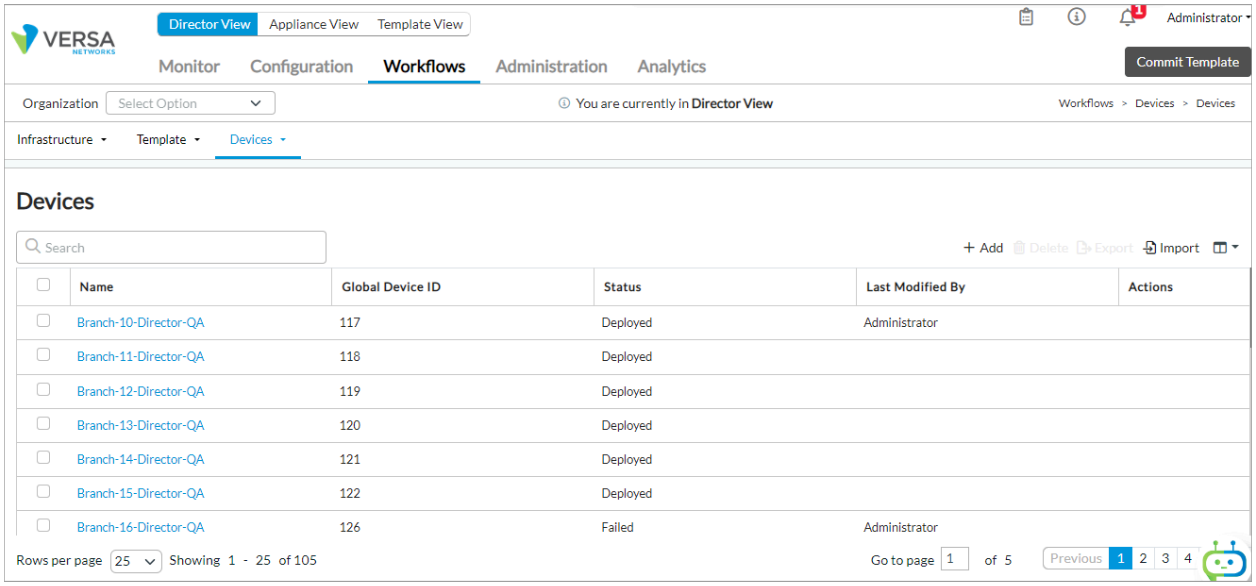
For supported software information, click here.

Normally, the Versa Operating System[TM] (VOS[TM]) devices that you receive are preconfigured as either a virtual CPE router or an SD-WAN device. If your devices are preconfigured, you can skip this article. If they are not, follow the procedures in this article to configure an AWS or Azure virtual machine (VM) to be either a virtual CPE or an SD-WAN gateway.

Configure a VOS Device as a Secure SD-WAN or SD-Security Device

To configure a branch VOS device on AWS or Azure to be an SD-WAN gateway device:

1. In Director view, select the Workflows tab in the top menu bar.
2. Select Devices > Devices in the left menu bar. The table in the main pane displays the devices that are already configured.



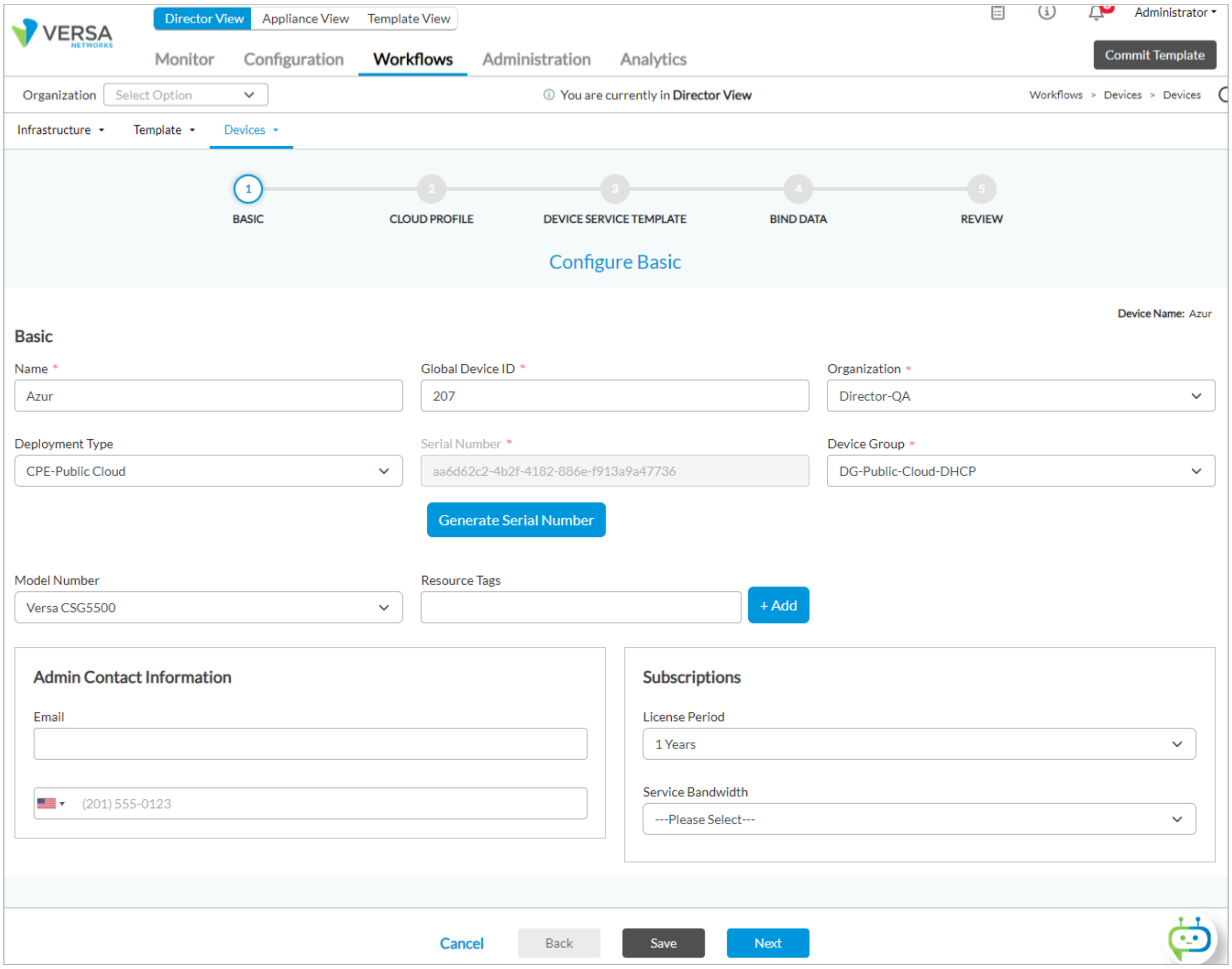
Devices

☐	Name	Global Device ID	Status	Last Modified By	Actions
☐	Branch-10-Director-QA	117	Deployed	Administrator	
☐	Branch-11-Director-QA	118	Deployed		
☐	Branch-12-Director-QA	119	Deployed		
☐	Branch-13-Director-QA	120	Deployed		
☐	Branch-14-Director-QA	121	Deployed		
☐	Branch-15-Director-QA	122	Deployed		
☐	Branch-16-Director-QA	126	Failed	Administrator	

Rows per page 25 Showing 1 - 25 of 105

Go to page 1 of 5

3. Click the + Add icon. In the Basic section, enter information for the following fields.



Organization: Select Option

You are currently in **Director View**

Configure Basic

Device Name: Azur

Basic

Name *	Azur
Global Device ID *	207
Organization *	Director-QA
Deployment Type	CPE-Public Cloud
Serial Number *	aa6d62c2-4b2f-4182-886e-f913a9a47736
Device Group *	DG-Public-Cloud-DHCP
Model Number	Versa CSG5500
Resource Tags	

Admin Contact Information

Email	
Phone	(201) 555-0123

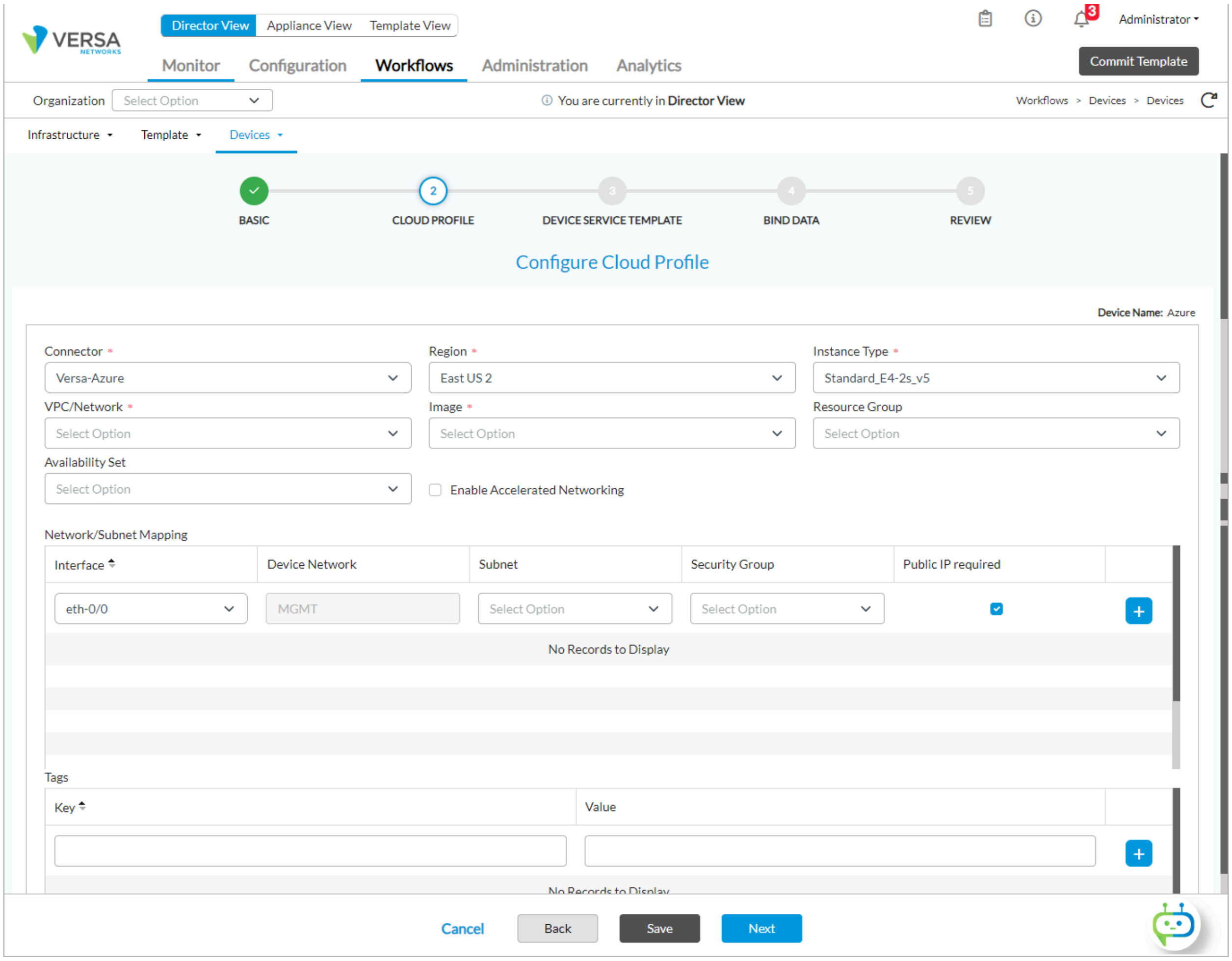
Subscriptions

License Period	1 Years
Service Bandwidth	---Please Select---

https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configura…
Updated: Wed, 23 Oct 2024 07:24:04 GMT

Field	Description
Name (Required)	Enter a name for the VOS device. The name is a text string.
Global Device ID (Required)	Displays the device ID, which is automatically assigned by the Director node.
Organization (Required)	Select the name of the organization to which the VOS device belongs.
Deployment Type	Select the deployment type as CPE-Public Cloud, to deploy the device as a gateway to the public cloud.
Serial Number (Required)	Displays the generated serial number.
Generate Serial Number	Click to assign a unique serial number to the VOS device.
Device Groups (Required)	Select the AWS or Azure device group to which the VOS device belongs.
Resource Tag	Enter a tag name, and then click Add icon to add the resource tag.
Admin Contact Information (Group of Fields)	
◦ Email	Enter the contact email address of the administrator.
◦ Phone	Enter the contact phone number of the administrator.
Subscriptions (Group of Fields)	
◦ License Period	Select the period, in years, for which the license is valid. The options are 1 year, 3 years, and 5 years.
◦ Service Bandwidth	Select the bandwidth, in Mbps or Gbps, to use for service that the device offers.

4. Click Next or select Cloud Profile.
5. In the Cloud Profile section, enter information for the following fields.



Configure Cloud Profile

Device Name: Azure

Connector *: Versa-Azure

Region *: East US 2

Instance Type *: Standard_E4-2s_v5

VPC/Network *: Select Option

Image *: Select Option

Resource Group: Select Option

Availability Set: Select Option

□ Enable Accelerated Networking

Network/Subnet Mapping

Interface	Device Network	Subnet	Security Group	Public IP required
eth-0/0	MGMT	Select Option	Select Option	☑

No Records to Display

Tags

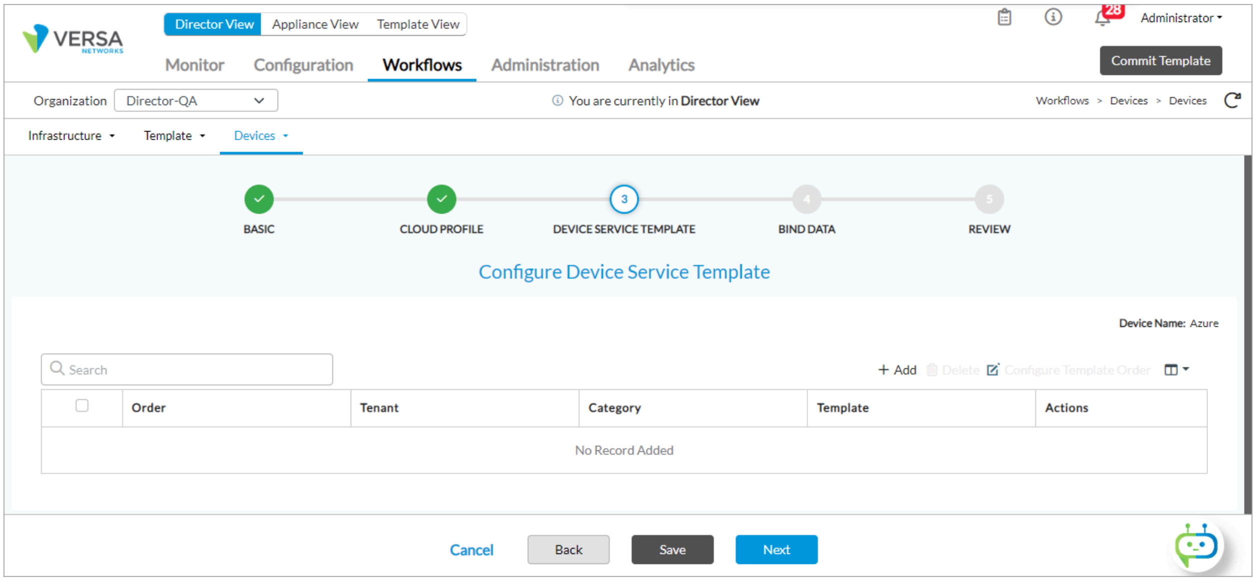
Key	Value

No Records to Display

Field	Description
Connector (Required)	Select the connector to use to establish communication between AWS or Azure and the Director node. Note that after deploying the cloud VOS branch/hub-controller with the CMS connector, you must remove the public IP address of eth0 from the cloud instance portal. The Director node will manage the VOS branch/hub-controller using the SD-WAN overlay IP address, and will not use the eth0 public IP address. Additionally, you must change the default passwords for all cloud-hosted VOS nodes, for admin and versa accounts.
Region (Required)	Select the geographic region in which to deploy the VOS device.
Instance Type (Required)	Select the VM instance type for VOS deployment.
VPC/Network (Required)	Select the type of virtual public cloud (network): ◦ VNET—For the Azure virtual public cloud ◦ VPC—For the Amazon virtual public cloud
Image (Required)	Select the VOS image to use to launch the VOS device.
◦ Availability Zone (Required)	For AWS only, select the AWS availability zone
◦ IAM Role/Instance Profile	For AWS only, click to use IAM instance credentials instead of an access key. One reason to use IAM instance credentials is so that the branch device can communicate with AWS APIs using instance credentials.
Resource Group	For Azure virtual WAN, select the resource group. If you do not select any value, a new resource group is created.
Availability Set	For Azure virtual WAN, select the availability set to

	instantiate a VOS VM.
Enable Accelerated Networking	(For Releases 22.1.1 and later.) Click to enable accelerated networking. Accelerated networking enables single root I/O virtualization (SR-IOV) on supported VMs. When you enable or disable accelerated networking on existing VMs during an upgrade, the VM shuts down and restarts after updating the accelerated networking. Note that enabling accelerated networking is supported only on VOS branch devices running Ubuntu 18.04 (Bionic). It is not supported on devices running Ubuntu 14.04 (Trusty).
Network/Subnet Mapping (Group of Fields)	Configure the subnet mapping for the VOS device.
◦ Interface	Select the interface to use for the network.
◦ Device Network	Enter the name of the device.
◦ Subnet	Select the subnetwork that you created for the device.
◦ Security Group	Select the security group to use for the subnetwork. This is the security group configured on the network interface. Be sure to check for any additional security group that is applied on an instance level and that might be blocking required traffic. Caution: You must disable all inbound ports on eth0 to restrict access from the public internet after successful deployment.
◦ Public IP Required	Click to provide a public IP address for the network interface.
Tags (Group of Fields)	
◦ Key	Enter the tag key for the VM deployed in AWS or Azure.
◦ Value	Enter the tag value for the VM deployed in AWS or Azure.

6. Click Next or select Device Service Template.
7. In the Device Service Template section, enter information for the following fields.



Organization Director-QA

You are currently in Director View

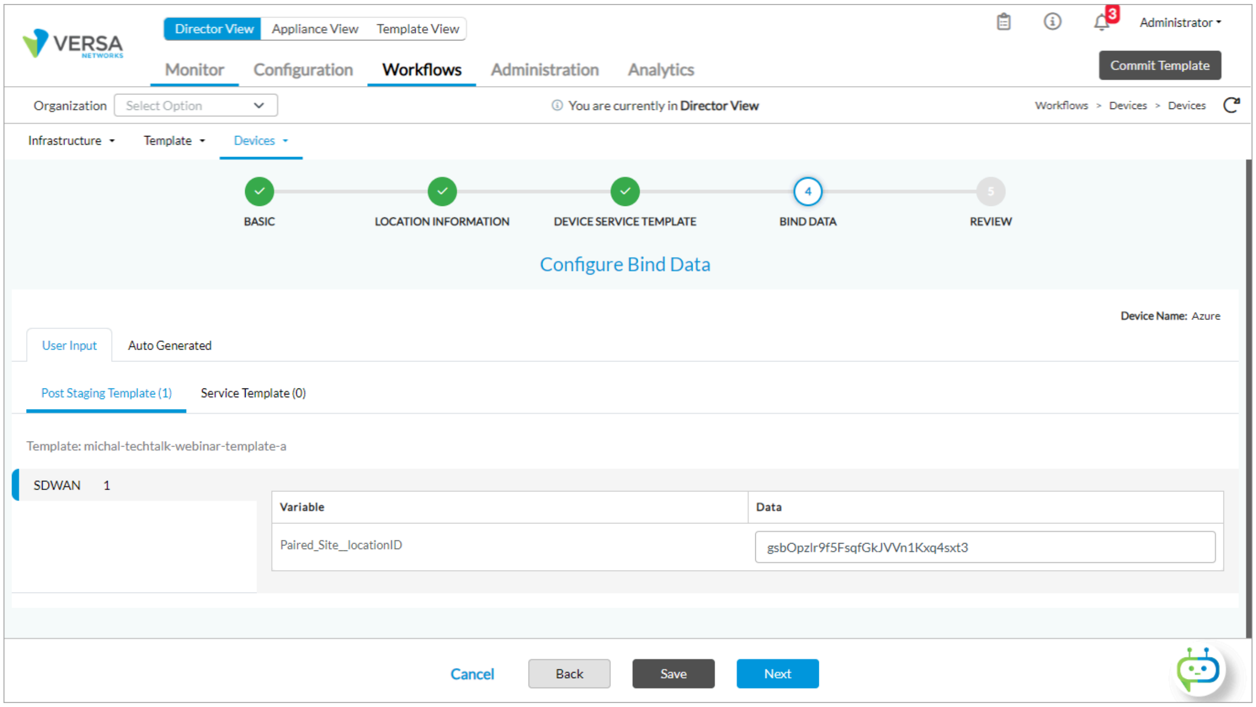
Configure Device Service Template

Device Name: Azure

☐	Order	Tenant	Category	Template	Actions
No Record Added					

Field	Description
Tenant	Select the name of the tenant.
Category	Select the category of the service template: ◦ Application Steering ◦ General ◦ NextGen ◦ QoS ◦ Statefull Firewall ◦ Service Chain ◦ Secure Access
Template	Select the template to use. The drop-down lists the templates available based on the options you select in the Tenant and Category fields.

8. Click Next or select Bind Data.
9. In the Bind Data section, add the required field values for the templates for which you have not enabled DHCP. If you enable DHCP for a template, the system populates the values dynamically. Note that the system validates the bind data variables per the specified variable type. If they do not match, an error message displays.

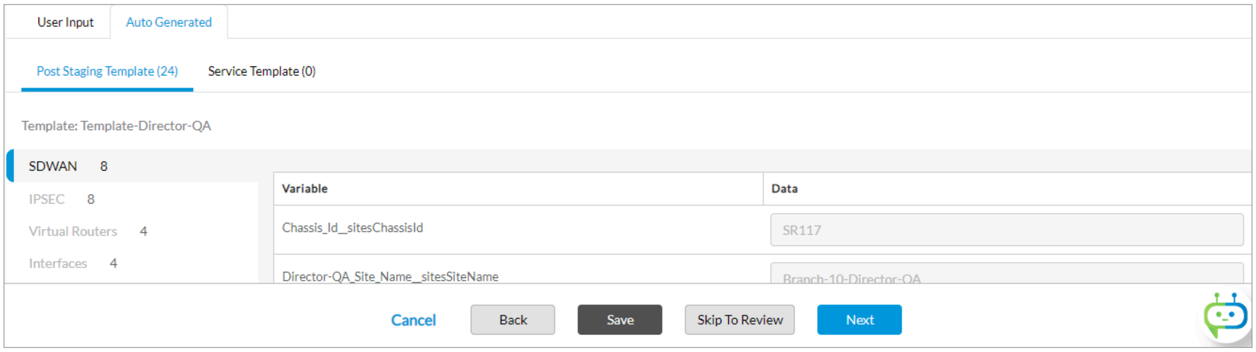


Device Name: Azure

Template: michal-techtalk-webinar-template-a

Variable	Data
Paired_Site_locationID	gsbOpzlr9f5FsqfGkJVVn1Kxq4sxt3

10. Select the Autogenerated tab to view and edit the values.



Template: Template-Director-QA

Variable	Data
Chassis_Id_sitesChassisId	SR117
Director-QA_Site_Name_sitesSiteName	Branch-10-Director-QA

11. Click Save.

Add Custom Routes in Azure to Send Traffic to the VOS Interface

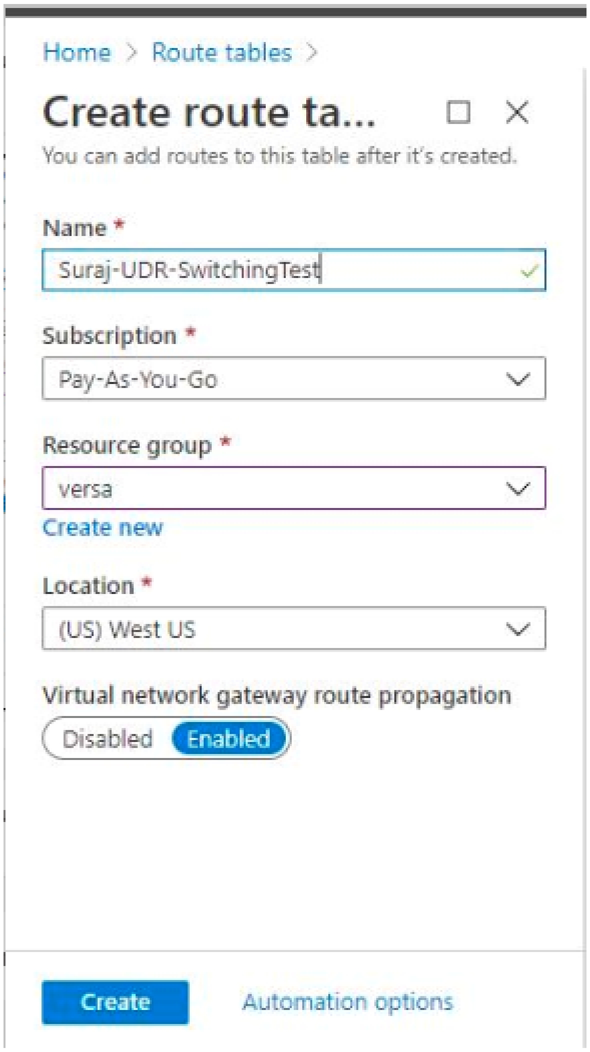
By default, Azure sends traffic to its core network. To instead send traffic to the VOS interface, you create a user-defined route in Azure. Then, to allow the network interfaces to receive and forward traffic, you enable IP forwarding. If you use a Director node to start the Azure VOS device using a CMS connector, the Director node enables IP forwarding.

Create User-Defined Routes

To create user-defined routes in Azure to send traffic towards a VOS device:

1. Log in to the Azure portal at https://portal.azure.com.

2. Create a route table. Enter information for the following fields.



Create route ta...

You can add routes to this table after it's created.

Name * Suraj-UDR-SwitchingTest

Subscription * Pay-As-You-Go

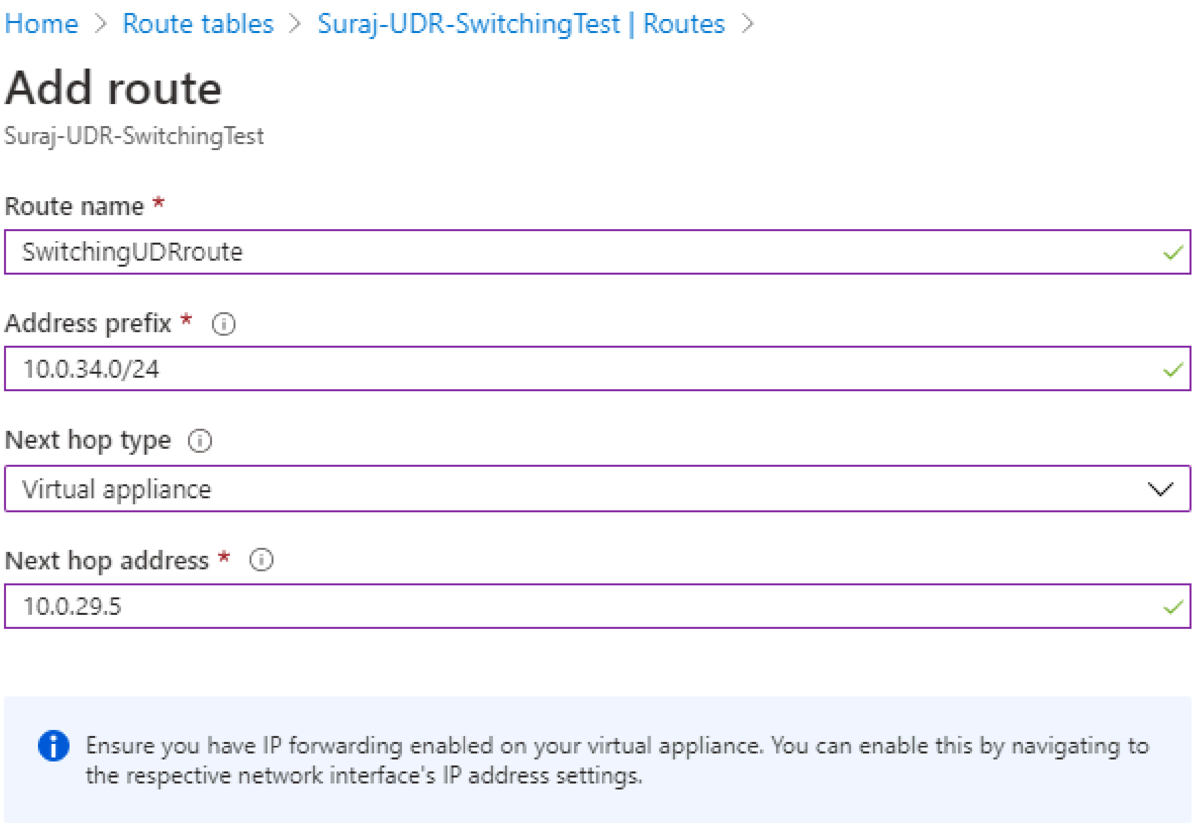
Resource group * versa

Location * (US) West US

Virtual network gateway route propagation: Disabled [✓ Enabled]

Field	Description
Name (Required)	Enter a name for the route table.
Subscription (Required)	Select the Azure subscription.
Resource Group (Required)	Select a resource group name. Click Create New to create a new resource group.
Location (Required)	Select the location of the Azure data center.
Virtual Network Gateway Route Propagation	Click Enabled.

3. Click Create.
4. Open the route table that you created in Step 2.
5. Click Routes in the left menu bar to add a route. Enter information for the following fields.



Add route

Suraj-UDR-SwitchingTest

Route name *
SwitchingUDRroute

Address prefix *
10.0.34.0/24

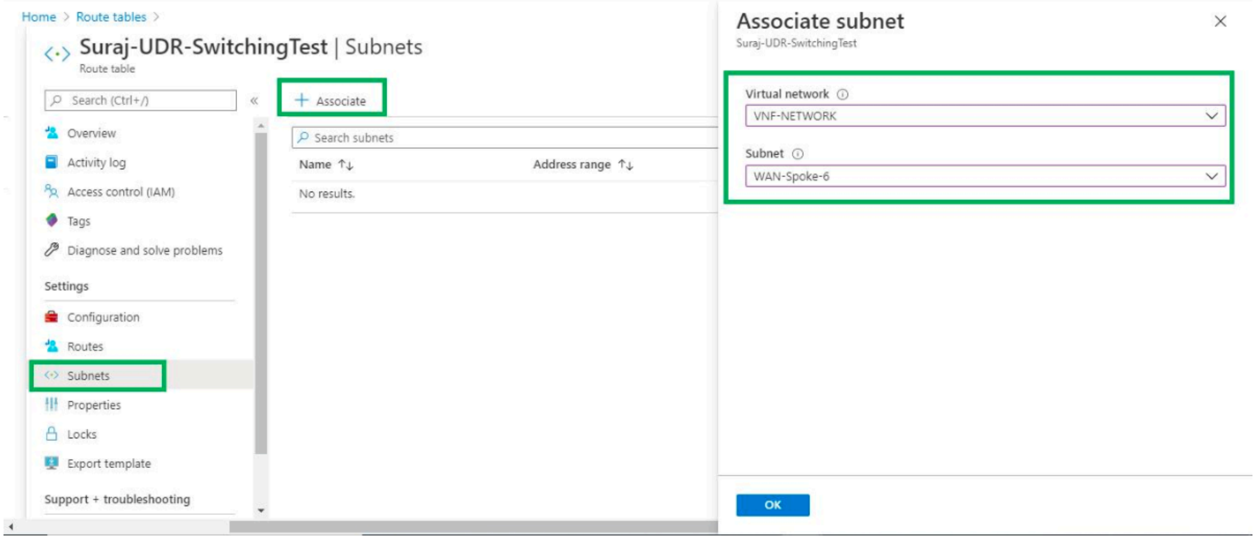
Next hop type
Virtual appliance

Next hop address *
10.0.29.5

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.

Field	**Description**
Route Name (Required)	Enter a name for the route.
Address Prefix (Required)	Enter the destination prefix for the route.
Next-Hop Type	Select Virtual Appliance.
Next-Hop Address (Required)	Enter the IP address of the VOS LAN that connects to clients in the LAN virtual router (VR).

6. Click Subnets in the left menu bar.
7. Associate the route table with LAN subnet that belongs to VOS LAN VR.



Virtual network: VNF-NETWORK

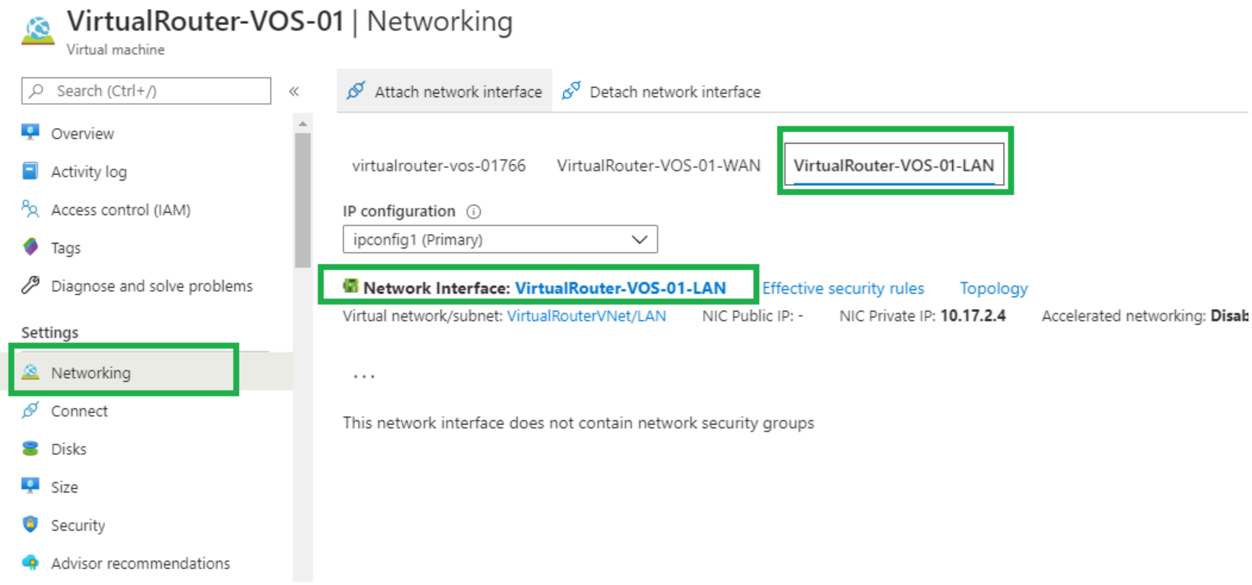
Subnet: WAN-Spoke-6

8. Click OK.

Enable IP Forwarding

If you use a Director node to start the Azure VOS device using a CMS connector, the Director node enables IP forwarding. To enable IP forwarding on the VOS LAN interface from the Azure portal:

1. Search for the VM in Azure portal, and select the VOS device on which to enable IP forwarding.
2. Select Settings > Networking in the left menu bar
3. Select the LAN interface and then click Network Interface.



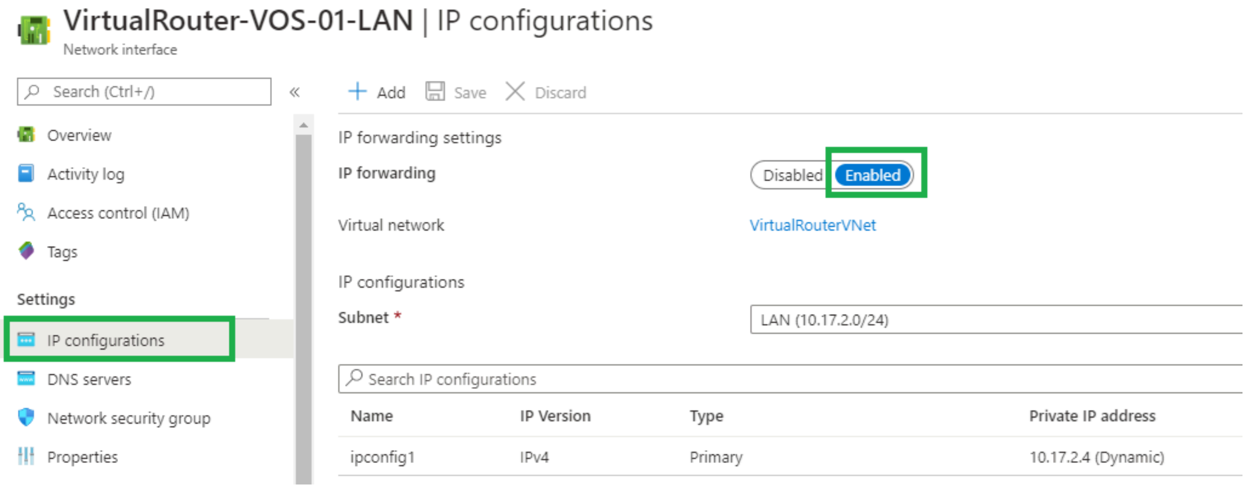
IP configuration: ipconfig1 (Primary)

Network Interface: VirtualRouter-VOS-01-LAN

Virtual network/subnet: VirtualRouterVNet/LAN NIC Public IP: - NIC Private IP: 10.17.2.4 Accelerated networking: Disab

This network interface does not contain network security groups

4. Select Settings > IP Configurations in the left menu bar.
5. In the IP Forwarding field, click Enabled.



VirtualRouter-VOS-01-LAN | IP configurations

Network interface

IP forwarding settings

IP forwarding: Disabled [✓ Enabled]

Virtual network: VirtualRouterVNet

IP configurations

Subnet *: LAN (10.17.2.0/24)

Name	IP Version	Type	Private IP address
ipconfig1	IPv4	Primary	10.17.2.4 (Dynamic)

6. Click Save.

Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Release 22.1.1 adds support for accelerated networking.

Additional Information

[Licensing Overview]

[Qualified AWS, Azure, and Google Cloud Instances]