

We created a **VPN using a Hub-and-Spoke architecture** in Azure.

- In the **Hub VNet**, we configured the **VPN Gateway**.
- In the **Spoke VNet** (where the application server is located), we **peered it with the Hub VNet**.

Our **database is in AWS** (in a VPC).

The Azure App Server (private IP) and AWS DB (private IP) must **communicate privately** even though they are in different cloud data centres.

To achieve this, we use a **VPN connection** between Azure and AWS.

In AWS, we also created a **Virtual Private Gateway (VPG)**.

The traffic flows over the **internet**, but through a **secure encrypted tunnel**.

Three Main Ways to Connect (Azure)

1. Site-to-Site VPN

- This connects **two networks** (Azure VNet \leftrightarrow AWS VPC).
- Traffic travels through a **private VPN tunnel**.
- All data is **encrypted and decrypted** over the internet.

2. Point-to-Site VPN

- Used by **individual users**, like Work-From-Home employees.
- They connect to the VPN **on demand**, and disconnect after work.
- This is not used between clouds, but to connect laptops to the cloud.

3. ExpressRoute

- This is a **dedicated private physical connection** (e.g., Hyderabad to Chennai).
- Cloud providers use **partner networks** like Jio, Airtel, Nokia, BSNL to provide it.
- This avoids the public internet and gives higher reliability, but is expensive.

Azure VM \leftrightarrow AWS VM Private Communication

Even though the Azure VM and AWS VM are in **different clouds**, we make them communicate privately by:

In AWS

- Create **VPC**
- Create **subnets**
- Create **Internet Gateway (if needed for outbound access)**
- Create **Route Table**
- Create **Security Groups**
- Launch **EC2 instance**
- Create **AWS VPN Gateway (VPG)**

In Azure

- Create **Hub and Spoke VNets**
- Create **VPN Gateway in Hub**
- Peer **Hub ↔ Spoke**
- App VM lives in Spoke
- Use **Bastion** to log into the Azure VM securely

The VPN gateways in Azure and AWS establish a **site-to-site connection**, allowing **private IP-to-private IP** communication.

Enable the option in peering :

Enable the “**Allow gateway or route server to forward traffic**” option on the VNET peering between VNET01 (Hub/VPN VNet) and VNET02 (App Server VNet) to ensure proper traffic flow between the Azure VPN gateway and the application servers.

VIRTUAL PRIVATE NETWORK

Create RG and VPN Gateway, you create a special subnet called vpnSubnet

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with links for Gmail, YouTube, Maps, Microsoft Azure (with an 'Upgrade' button), Copilot, and user information. Below the navigation bar, the main title is 'Create a resource group'. The 'Basics' tab is selected. Under 'Subscription', it shows 'Azure subscription 1'. Under 'Resource group name', the input field contains 'rg01'. Under 'Region', it shows '(US) West US'. At the bottom of the screen, there are three buttons: 'Previous', 'Next', and 'Review + create'. The 'Review + create' button is highlighted in blue.

Create a VPN

The screenshot shows the Microsoft Azure portal interface under the 'Hybrid connectivity' section. The main heading is 'Hybrid connectivity | E'. Below it, there's a 'Preview' link next to a lock icon. On the left, there's a navigation sidebar with a search bar, a back arrow, and a plus sign for adding new resources. The sidebar lists several options: 'Overview' (selected), 'ExpressRoute' (under a dropdown menu), 'VPN gateway' (selected), 'Set up VPN Gateway' (with a house icon), 'VPN gateways' (selected, with a star icon), 'VPN connections' (with a circular arrow icon), 'Local network gateways' (with a green diamond icon), and 'Virtual WAN' (under a dropdown menu). The 'VPN gateway' option is currently selected.

VIRTUAL PRIVATE NETWORK

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. [Learn more](#)

Subscription *

Resource group

Instance details

Name *

Region * Deploy to an Azure Extended Zone [Learn more](#)

Gateway type * VPN ExpressRoute

SKU *

Generation

[Review + create](#) [Previous](#) [Next : Tags >](#) [Download a template for automation](#)



Home > Hybrid connectivity | VPN gateways >

Create virtual network gateway

Virtual network * Create virtual network

Subnet

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

Public IP address

Public IP address * Create new Use existing

Public IP address name *

Public IP address SKU Standard

Assignment Dynamic Static

Enable active-active mode * Enabled Disabled

Configure BGP * Enabled Disabled

Authentication Information (Preview)

Enable Key Vault Access Enabled Disabled

[Review + create](#) [Previous](#) [Next : Tags >](#) [Download a template for automation](#)



Home > Microsoft.VirtualNetworkGateway-20251125230902 | Overview

 Deployment

[Delete](#) [Cancel](#) [Redeploy](#) [Download](#) [Refresh](#)

Your deployment is complete

Deployment name : Microsoft.VirtualNetworkGateway-20251125230902 Start time : 11/25/2025, 11:15:13 PM
Subscription : Azure subscription 1 Correlation ID : 8d71f3f0-3bc7-4dbb-92bb-e6ddc5f46b3d
Resource group : rg01

[Deployment details](#) [Next steps](#)

[Go to resource](#)

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 >](#)

Add or remove favorites by pressing **Ctrl+Shift+F**

AWS Setup — Short Steps (for example)

1. Create VPC

- Go to **VPC** → **Your VPCs** → **Create VPC**
- Give name → Add CIDR (example: 10.0.0.0/16) → Create.

2. Create Subnets

- Go to **Subnets** → **Create subnet**
- Choose the VPC
- Create:

3. Create Internet Gateway (IGW)

- Go to **Internet Gateways** → **Create**
- Attach it to the VPC.

4. Create Route Tables

- Add route: 0.0.0.0/0 → Target: IGW

5. Create Security Groups

- Go to **Security Groups** → **Create**
- Add inbound rules (example: SSH 22 from your IP, HTTP 80 if needed).

6. Launch EC2 Instance

- Go to **EC2** → **Launch Instance**
- Select VPC + public subnet
- Enable public IP
- Choose key pair
- Select security group
- Launch.

7. Create AWS VPN Gateway (VGW)

- Go to **Site-to-Site VPN** → **Virtual Private Gateways** → **Create**
- Attach to VPC
- Create **Customer Gateway** (use Azure VPN public IP)
- Create **VPN Connection** (VGW ↔ Customer Gateway)

8. Add VPN Route

- In **private route table**, add:
 - Destination = Azure network CIDR

VIRTUAL PRIVATE NETWORK

VPC dashboard > Your VPCs

Your VPCs

VPCs | VPC encryption controls - new

Your VPCs (1) Info

Name	VPC ID	State	Encryption c...	Encryption control ...	Block Public...	IPv...
vpcgw	vpc-0bf58600d1218c632	Available	-	-	Off	172

vpc-0bf58600d1218c632 / vpcgw

Details | Resource map | CIDRs | Flow logs | Tags | Integrations

Details

VPC ID vpc-0bf58600d1218c632	State Available	Block Public Access Off	DNS hostnames Disabled
DNS resolution Enabled	Tenancy default	DHCP option set opt-0ff69eaecc2d4289a	Main route table rtb-0b62cd2f6ef97519d
Main network ACL None	Default VPC	IPv4 CIDR 172.16.0.0/16	IPv6 pool

Last updated less than a minute ago | Actions | Create VPC

CloudShell Feedback Console Mobile App

aws | **Search** [Alt+S]

VPC dashboard > Subnets

Subnets

Subnets (1) Info

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
sb	subnet-0e4645b3fd8026ed5	Available	vpc-0bf58600d1218c632 vpcgw	Off	172.16.1.0/24

Select a subnet

VPC dashboard > Internet gateways

Internet gateways

Internet gateways (1) Info

Name	Internet gateway ID	State	VPC ID	Owner
igw	igw-0881d12e3619f8b9d	Attached	vpc-0bf58600d1218c632 vpcgw	796586190907

Select an internet gateway above

VIRTUAL PRIVATE NETWORK

VPC dashboard > Route tables

Route tables (1) Info

Last updated 1 minute ago | Actions | Create route table

Name	Route table ID	Explicit subnet assoc...	Edge associations	Main	VPC
rt	rtb-0b62cd2f6ef97519d	-	-	Yes	vpc-0bf58600d1218c632 vpcgw

Select a route table

rtb-0b62cd2f6ef97519d / rt

Details Info

Route table ID rtb-0b62cd2f6ef97519d	Main Yes	Explicit subnet associations -	Edge associations -
VPC vpc-0bf58600d1218c632 vpcgw	Owner ID 796586190907		

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

Routes (3)

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-0881d12e36198b9d	Active	No	Create Route
10.0.0.0/16	vgw-08b559b324ab31be9	Active	No	Create Route
172.16.0.0/16	local	Active	No	Create Route Table

EC2 > Instances

Instances (1) Info

Last updated 1 minute ago | Connect | Instance state | Actions | Launch instances

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
vrm	i-0657d1c1c9fd1a41c	Running	t3.micro	3/3 checks passed	View alarms +	us-east-1a	-

Select an instance

VIRTUAL PRIVATE NETWORK

EC2 Instance Connect | Session Manager | SSH client | EC2 serial console

Instance ID
i-0657d1c1c9fd1a41c (vm)

Connection type

Connect using a Public IP
Connect using a public IPv4 or IPv6 address

Connect using a Private IP
Connect using a private IP address and a VPC endpoint

Public IPv4 address
3.95.247.210

IPv6 address

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

ubuntu

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

Cancel

welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-1015-aws x86_64)

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

System information as of Tue Nov 25 18:33:13 UTC 2025

System load: 0.1 Temperature: -273.1 C
Usage of /: 34.6% of 6.71GB Processes: 112
Memory usage: 28% Users logged in: 0
Swap usage: 0% IPV4 address for ens5: 172.16.1.116

expanded Security Maintenance for Applications is not enabled.
17 updates can be applied immediately.
To see these additional updates run: apt list --upgradable
Enable ESM Apps to receive additional future security updates.
See <https://ubuntu.com/esm> or run: sudo pro status

*** System restart required ***
Last login: Mon Nov 24 06:01:00 2025 from 18.206.107.29
ubuntu@ip-172-16-1-116:~\$

i-0657d1c1c9fd1a41c (vm)
PublicIPs: 3.95.247.210 PrivateIPs: 172.16.1.116

VIRTUAL PRIVATE NETWORK

The screenshot shows the AWS VPC Virtual Private Gateways page. On the left, there's a navigation sidebar with sections like Network Firewall, Virtual private network (VPN), and AWS Verified Access. The main area displays a table titled "Virtual private gateways (1) Info". The table has columns: Name, Virtual private gateway ID, State, VPC attachment state, Type, and VPC. One row is shown: Name is "vpn", Virtual private gateway ID is "vgw-08b559b324ab31be9", State is "Available", VPC attachment state is "Attached", Type is "ipsec.1", and VPC is "vpc-0bf58600d1218c632". Below the table, a modal window titled "Select a virtual private gateway" is open, showing the same information. At the bottom right of the main table area, a context menu is open with options: Attach to VPC, Detach from VPC, Manage tags, and Delete virtual private gateway.

In Resource Group 2

- You created another **VNet**
- Inside that VNet you created a **Virtual Machine**

This VNet is your **SPOKE** (your application server lives here).

Next Step: VNet Peering

You connected the two VNets (HUB ↔ SPOKE) using **VNet peering**.

While creating the peering, you enabled this important option:

"Allow gateway or route server in 'VNET01' to forward traffic to 'VNET02'"

This allows the VM in the SPOKE VNet to use the **VPN Gateway** created in the HUB VNet.

VIRTUAL PRIVATE NETWORK

The screenshot shows the Microsoft Azure Resource groups page. At the top, there are navigation links for 'Home', 'Resource groups', and 'How to manage changes with deployment tools?'. A search bar is present, along with 'Copilot' and other account-related icons. The main content area displays a table of resource groups:

	Name ↑	Subscription	Location
<input type="checkbox"/>	NetworkWatcherRG	... Azure subscription 1	East US 2
<input type="checkbox"/>	rg01	... Azure subscription 1	West US
<input type="checkbox"/>	RG02	... Azure subscription 1	West US

Below the table, there is a message: 'You are viewing a new version of Browse experience. Click here to access the old experience.' Filter options include 'Filter for any field...', 'Subscription equals all', 'Location equals all', and '+ Add filter'. At the bottom, it says 'Showing 1 - 3 of 3. Display count: auto' and 'Give feedback'.

The screenshot shows the 'Create a resource group' wizard on the 'Basics' step. The top navigation bar includes links for 'Gmail', 'YouTube', 'Maps', 'Microsoft Azure', 'Upgrade', 'Search resources, services, and docs (G+)', 'Copilot', and account information. The main content area has tabs for 'Basics', 'Tags', and 'Review + create'. The 'Basics' tab is selected. It contains a description of what a resource group is, a note about the subscription, and three input fields: 'Subscription' (set to 'Azure subscription 1'), 'Resource group name' (set to 'RG02'), and 'Region' (set to '(US) West US'). At the bottom, there are 'Previous' and 'Next' buttons, and a prominent 'Review + create' button.

VIRTUAL PRIVATE NETWORK

Home > Network foundation | Virtual networks >

Create virtual network ...

X

Basics Security IP addresses Tags Review + create

Allocate using IP address pools. [Learn more](#)

+ Add a subnet

192.168.0.0/16 Delete address space

192.168.0.0/16 /16 65,536 addresses
192.168.0.0 - 192.168.255.255

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

Add IPv4 address space | ▾

Previous Next Review + create

Give feedback

aws Search [Alt+S] Account ID: 7965-8619-0907 venkata Umamaheswari

VPC > Customer gateways > Create customer gateway

Create customer gateway Info

A customer gateway is a resource that you create in AWS that represents the customer gateway device in your on-premises network.

Details

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

Value must be 256 characters or less in length.

BGP ASN - Info
The ASN of your customer gateway device.

Value must be in 1 - 4294967294 range.

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

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

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

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

VIRTUAL PRIVATE NETWORK

Create Customer Gateway

- Go to **VPC → Customer Gateway → Create**
- Enter:
 - Name: Azure-CGW
 - IP Address: **Azure VPN Gateway private IP**
- Create.

Download the customer gateway configuration → This file contains the Pre-Shared Key (PSK).

Create Local Network Gateway

- Go to Local Network Gateway → Create
- Enter:
 - Name: AWS-LNG
 - Address space: (from the downloaded file)
- Create.

Create VPN Connection

- Go to VPN Gateway → Connections → Add
- Choose:
 - Type: Site-to-site
 - Local network gateway: AWS-LNG
 - Shared key: Paste PSK from AWS file
- Create.

Test

- Go to your AWS EC2 terminal.
- Run:
`ping <Azure_VM_Private_IP>`

If you get replies → VPN working.

VIRTUAL PRIVATE NETWORK

AWS VPC Customer Gateways

You successfully created cgw-06eb48feff68960c7 / customergateway2.

Name	Customer gateway ID	State	BGP ASN	IP address	Type
customergateway2	cgw-06eb48feff68960c7	Available	65000	13.93.148.105	ipsec.1
azurevpn1p	cgw-0538e1c1787c212a5	Available	65000	20.253.196.163	ipsec.1

Customer gateway cgw-06eb48feff68960c7 / customergateway2

Details

Customer gateway ID cgw-06eb48feff68960c7	State Available	Type ipsec.1	IP address 13.93.148.105
BGP ASN 65000	Certificate ARN -	Device -	

Microsoft Azure VM Overview

Help me copy this VM in any region | Manage this VM with Azure CLI

Standard HDD OS disks will be retired on September 8, 2028. →

Connect ▾ Start ▾ Restart ▾ Stop ▾ Hibernate ▾ Capture ▾ Delete ▾ Refresh ▾ Scale ▾ Open in mobile ▾ Feedback ▾ CLI / PS

DNS name : Not configured
Health state : -
Time created : 11/25/2025, 6:57 PM UTC

Tags (edit) : Add tags

Properties

Virtual machine	Networking
Computer name : VMO1	Public IP address : 172.185.13.82 (Network interface vmo1170)
Operating system : Linux (ubuntu 24.04)	1 associated public IPs
VM generation : V2	Public IP address (IPv6) : -
VM architecture : x64	Private IP address : 192.168.1.4
Agent status : Ready	Private IP address (IPv6) : -
Agent version : 2.15.0.1	Virtual network/subnet : VNET02/snet-westus-1
Hibernation : Disabled	DNS name : Configure
Host group : -	

Add or remove favorites by pressing Ctrl+Shift+F

AWS Route Tables Edit routes

Edit routes

Destination	Target	Status	Propagated	Route Origin	
172.16.0.0/16	local	Active	No	CreateRouteTable	
Q 0.0.0.0/0	Internet Gateway	Active	No	CreateRoute	Remove
Q 192.168.0.0/16	Virtual Private Gateway	-	No	CreateRoute	Remove
Q vgw-08b559b324ab31be9					

[Add route](#)

Cancel [Preview](#) [Save changes](#)

VIRTUAL PRIVATE NETWORK

The screenshot shows the Azure portal interface for managing Virtual Private Network (VPN) connections. On the left, a list of VPN connections is displayed with two entries: 'vpn01' (VPN ID: vpn-0ab1fb3697c29b5c) and 'awstoazure' (VPN ID: vpn-0971962). The 'vpn01' connection is selected. A modal dialog titled 'Download configuration' is open, prompting the user to download a sample configuration based on the selected customer gateway. The dialog includes fields for Vendor (Checkpoint), Platform (Gaia), Software (R77.10+), and IKE version (ikev1). There is also an option to include sample type (checkbox 'Enable'). At the bottom of the dialog are 'Cancel' and 'Download' buttons.

```

! tunnel-group 34.234.46.126 type ipsec-l2l
tunnel-group 34.234.46.126 ipsec-attributes
    pre-shared-key UPo9B.Q5hE1.rmDVfUy_B2dJ1lDOON4z
!
! This option enables IPSec Dead Peer Detection, which causes semi-periodic
! messages to be sent to ensure a Security Association remains operational.
!
    isakmp keepalive threshold 10 retry 10
exit
  
```

Home > Hybrid connectivity | Local network gateways >

Create local network gateway ...

[more ↗](#)

Project details

Subscription *

Resource group * [Create new](#)

Instance details

Region *

Name *

Endpoint [IP address](#) [FQDN](#)

IP address *

Address Space(s) [Add additional address range](#)

VIRTUAL PRIVATE NETWORK

Microsoft Azure | Hybrid connectivity | VPN gateways >

VPN Virtual network gateway

Overview

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

Name: rg01

Resource group: rg01

Location: West US

Subscription: Azure subscription 1

Subscription ID: 229e0bc6-e088-41a7-aa63-6b389ce27bf5

Virtual network: vnet01

Public IP address: 13.93.148.105 (VPNPIP)

Tags (edit) Add tags

Health check: Perform a quick health check to detect possible gateway issues. Go to Resource health

Advisor Recommendations: Check Critical, Warning, and Informational Recommendations. Go to Advisor

Show data for last: 1 hour, 6 hours, 12 hours, 1 day, 7 days, 30 days

Connections

- Point-to-site configuration
- Maintenance
- Properties
- Locks
- Monitoring
- Automation

Essentials

SKU	VpnGw1AZ
Gateway type	VPN
VPN type	Route-based
Virtual network	vnet01
Public IP address	13.93.148.105 (VPNPIP)

VPN gateways

VPN connections

Local network gateways

Virtual WAN

Microsoft Azure | Hybrid connectivity | VPN gateways > VPN | Connections >

Create connection

Basics

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*: Azure subscription 1
Resource group*: rg01 Create new

Instance details

Connection type*: Site-to-site (IPsec)
Name*: Site-to-site (IPsec)
Region*: ExpressRoute

Next : Settings >

```
exit
!
tunnel-group 34.234.46.126 type ipsec-l2l
tunnel-group 34.234.46.126 ipsec-attributes
    pre-shared-key UPo9B.Q5hE1.rmDVfUy_B2dJ1lDOON4z
```

VIRTUAL PRIVATE NETWORK

Microsoft Azure Upgrade Search resources, services, and docs (G+) Copilot

Home > Hybrid connectivity | VPN gateways > VPN | Connections >

Create connection ...

Basics **Settings** Tags Review + create

Virtual network gateway

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

Virtual network gateway *	VPN
Local network gateway *	localnetworkgateway
Authentication Method	<input checked="" type="radio"/> Shared Key(PSK) <input type="radio"/> Key Vault Certificate (Preview)
Shared Key(PSK) *	*****
IKE Protocol	<input type="radio"/> IKEv1 <input checked="" type="radio"/> IKEv2
Use Azure Private IP Address	<input type="checkbox"/>
Enable BGP	<input type="checkbox"/>
IPsec / IKE policy	<input checked="" type="radio"/> Default <input type="radio"/> Custom
Use policy based traffic selector	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
DDP timeout in seconds *	45

[Previous](#) [Next : Tags >](#)

Preview

Search Manage view Refresh Export to CSV Open query Assign tags Add to service group Group by none

Overview

Virtual network

Virtual Network overview	Resource Group	Location	Subscription
vnet01	rg01	West US	Azure subscription 1
VNET02	RG02	West US	Azure subscription 1

Virtual networks

- NAT gateways
- Public IP addresses
- Network interfaces
- Network security groups
- Application security groups
- Bastions
- Route tables
- Route servers

Private Link

DNS

Monitoring and management

Gmail YouTube Maps

Microsoft Azure Upgrade Search resources, services, and docs (G+) Copilot

Home > Network foundation | Virtual networks > vnet01

Network foundation | Virtual networks

Virtual network

vnet01 | Peering

Virtual network

Peering

Add a peering to get started

Give feedback

<https://portal.azure.com/?i=en-en-us#pataleasyapriy@gmail.onmicrosoft.com/resource/subscriptions/229e0bc6-e088-41a7-aa63-0b389ce27bf5/resourceGroups/rg01/providers/Microsoft.Network/virtualNetworks/vnet01/networkManager>

VIRTUAL PRIVATE NETWORK

Home > Network foundation | Virtual networks > vnet01 | Peerings >

Add peering ...

vnet01

Enable 'VNET02' to use 'vnet01's' remote gateway or route server

Local virtual network summary

Peering link name *

vnet2to1

Local virtual network peering settings

Allow 'vnet01' to access 'VNET02'

Allow 'vnet01' to receive forwarded traffic from 'VNET02'

Allow gateway or route server in 'vnet01' to forward traffic to 'VNET02'

Enable 'vnet01' to use 'VNET02's' remote gateway or route server

Add

Cancel

↻ Gb

Home > Network foundation | Virtual networks > vnet01 | Peerings >

Add peering ...

vnet01

Enable 'VNET02' to use 'vnet01's' remote gateway or route server

Local virtual network summary

Peering link name *

vnet2to1

Local virtual network peering settings

Allow 'vnet01' to access 'VNET02'

Allow 'vnet01' to receive forwarded traffic from 'VNET02'

Allow gateway or route server in 'vnet01' to forward traffic to 'VNET02'

Enable 'vnet01' to use 'VNET02's' remote gateway or route server

Add

Cancel

VIRTUAL PRIVATE NETWORK

Enable 'VNET02' to use 'vnet01's' remote gateway or route server

Local virtual network summary

Peering link name *

Local virtual network peering settings

Allow 'vnet01' to access 'VNET02'

Allow 'vnet01' to receive forwarded traffic from 'VNET02'

Allow gateway or route server in 'vnet01' to forward traffic to 'VNET02'

Enable 'vnet01' to use 'VNET02's' remote gateway or route server

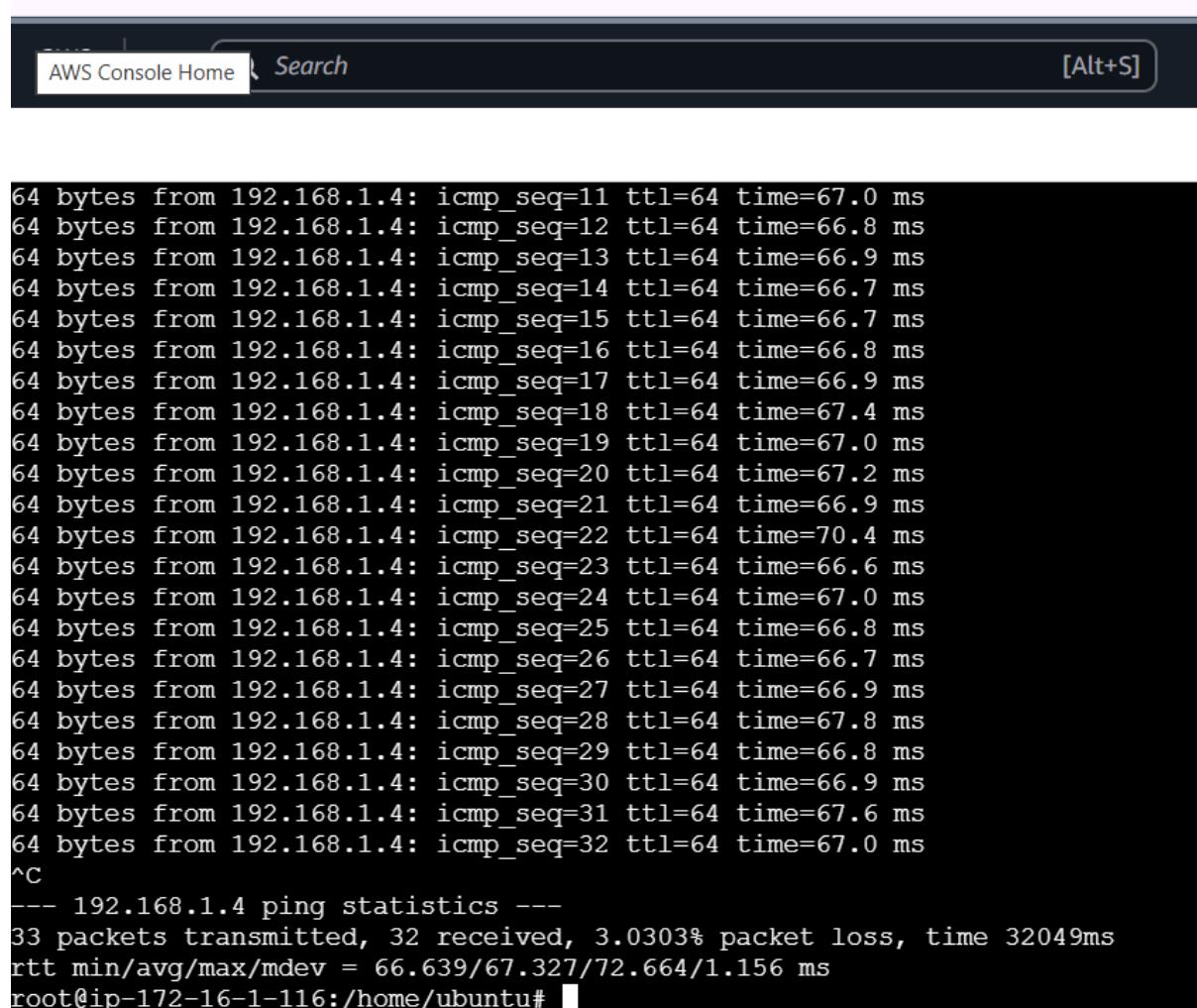


```
root@ip-172-16-1-116:/home/ubuntu# ping 192.168.1.4
PING 192.168.1.4 (192.168.1.4) 56(84) bytes of data.
64 bytes from 192.168.1.4: icmp_seq=1 ttl=64 time=67.8 ms
64 bytes from 192.168.1.4: icmp_seq=2 ttl=64 time=67.1 ms
64 bytes from 192.168.1.4: icmp_seq=3 ttl=64 time=67.1 ms
64 bytes from 192.168.1.4: icmp_seq=4 ttl=64 time=67.4 ms
64 bytes from 192.168.1.4: icmp_seq=5 ttl=64 time=67.0 ms
64 bytes from 192.168.1.4: icmp_seq=6 ttl=64 time=66.8 ms
64 bytes from 192.168.1.4: icmp_seq=7 ttl=64 time=67.0 ms
64 bytes from 192.168.1.4: icmp_seq=8 ttl=64 time=67.4 ms
64 bytes from 192.168.1.4: icmp_seq=9 ttl=64 time=72.7 ms
64 bytes from 192.168.1.4: icmp_seq=10 ttl=64 time=67.3 ms
64 bytes from 192.168.1.4: icmp_seq=11 ttl=64 time=67.0 ms
64 bytes from 192.168.1.4: icmp_seq=12 ttl=64 time=66.8 ms
64 bytes from 192.168.1.4: icmp_seq=13 ttl=64 time=66.9 ms
64 bytes from 192.168.1.4: icmp_seq=14 ttl=64 time=66.7 ms
64 bytes from 192.168.1.4: icmp_seq=15 ttl=64 time=66.7 ms
64 bytes from 192.168.1.4: icmp_seq=16 ttl=64 time=66.8 ms
64 bytes from 192.168.1.4: icmp_seq=17 ttl=64 time=66.9 ms
64 bytes from 192.168.1.4: icmp_seq=18 ttl=64 time=67.4 ms
64 bytes from 192.168.1.4: icmp_seq=19 ttl=64 time=67.0 ms
64 bytes from 192.168.1.4: icmp_seq=20 ttl=64 time=67.2 ms
64 bytes from 192.168.1.4: icmp_seq=21 ttl=64 time=66.9 ms
64 bytes from 192.168.1.4: icmp_seq=22 ttl=64 time=70.4 ms
64 bytes from 192.168.1.4: icmp_seq=23 ttl=64 time=66.6 ms
64 bytes from 192.168.1.4: icmp_seq=24 ttl=64 time=67.0 ms
```

i-0657d1c1c9fd1a41c (vm)

PublicIPs: 3.95.247.210 PrivateIPs: 172.16.1.116

VIRTUAL PRIVATE NETWORK



AWS CloudWatch terminal window showing ping statistics to 192.168.1.4. The terminal output includes 33 transmitted packets, 32 received, and a 3.0303% packet loss.

```
64 bytes from 192.168.1.4: icmp_seq=11 ttl=64 time=67.0 ms
64 bytes from 192.168.1.4: icmp_seq=12 ttl=64 time=66.8 ms
64 bytes from 192.168.1.4: icmp_seq=13 ttl=64 time=66.9 ms
64 bytes from 192.168.1.4: icmp_seq=14 ttl=64 time=66.7 ms
64 bytes from 192.168.1.4: icmp_seq=15 ttl=64 time=66.7 ms
64 bytes from 192.168.1.4: icmp_seq=16 ttl=64 time=66.8 ms
64 bytes from 192.168.1.4: icmp_seq=17 ttl=64 time=66.9 ms
64 bytes from 192.168.1.4: icmp_seq=18 ttl=64 time=67.4 ms
64 bytes from 192.168.1.4: icmp_seq=19 ttl=64 time=67.0 ms
64 bytes from 192.168.1.4: icmp_seq=20 ttl=64 time=67.2 ms
64 bytes from 192.168.1.4: icmp_seq=21 ttl=64 time=66.9 ms
64 bytes from 192.168.1.4: icmp_seq=22 ttl=64 time=70.4 ms
64 bytes from 192.168.1.4: icmp_seq=23 ttl=64 time=66.6 ms
64 bytes from 192.168.1.4: icmp_seq=24 ttl=64 time=67.0 ms
64 bytes from 192.168.1.4: icmp_seq=25 ttl=64 time=66.8 ms
64 bytes from 192.168.1.4: icmp_seq=26 ttl=64 time=66.7 ms
64 bytes from 192.168.1.4: icmp_seq=27 ttl=64 time=66.9 ms
64 bytes from 192.168.1.4: icmp_seq=28 ttl=64 time=67.8 ms
64 bytes from 192.168.1.4: icmp_seq=29 ttl=64 time=66.8 ms
64 bytes from 192.168.1.4: icmp_seq=30 ttl=64 time=66.9 ms
64 bytes from 192.168.1.4: icmp_seq=31 ttl=64 time=67.6 ms
64 bytes from 192.168.1.4: icmp_seq=32 ttl=64 time=67.0 ms
^C
--- 192.168.1.4 ping statistics ---
33 packets transmitted, 32 received, 3.0303% packet loss, time 32049ms
rtt min/avg/max/mdev = 66.639/67.327/72.664/1.156 ms
root@ip-172-16-1-116:/home/ubuntu#
```

i-0657d1c1c9fd1a41c (vm)

PublicIPs: 3.95.247.210 PrivateIPs: 172.16.1.116