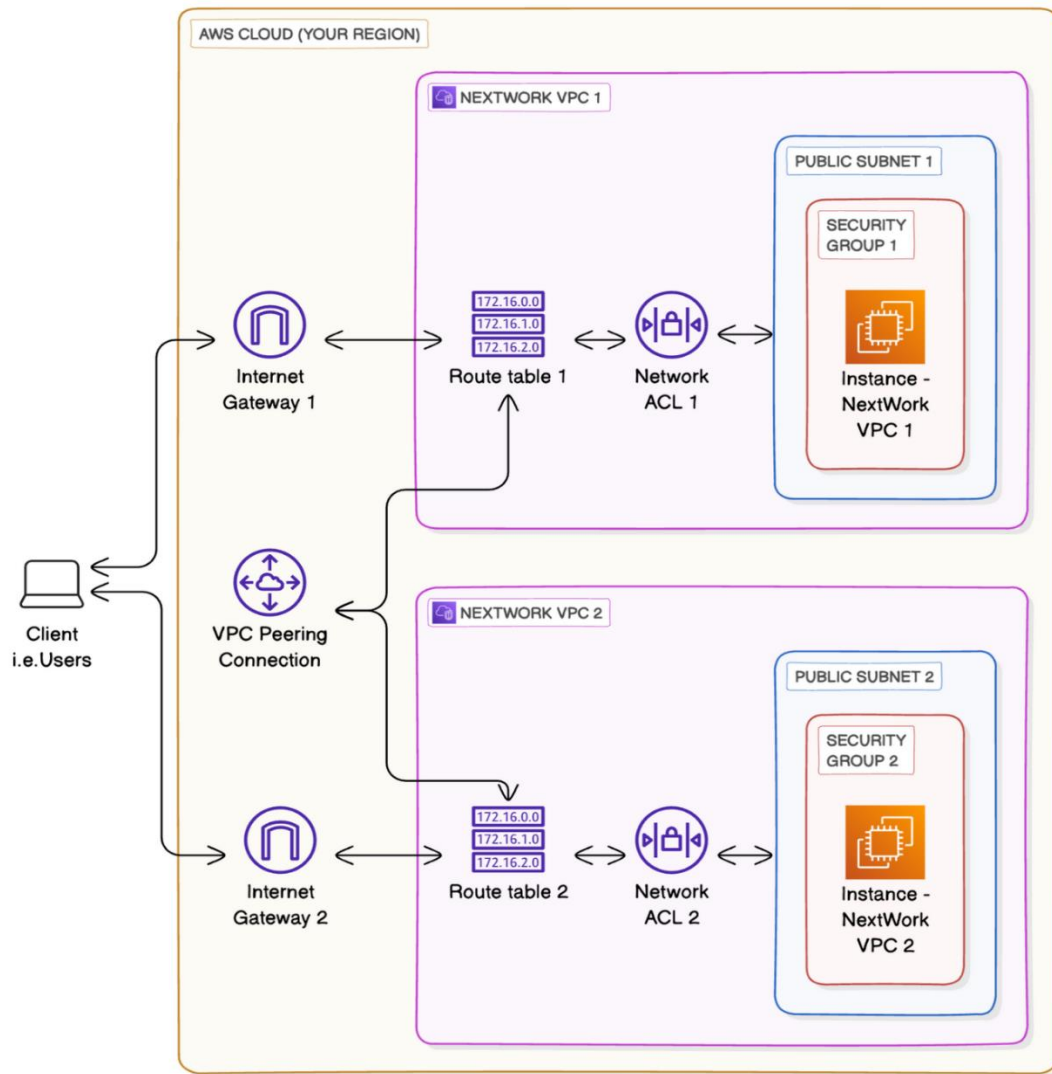


## VPC Peering

### Get ready to:

1. ☁ Set up multiple VPCs.
2. 🖥 Create a VPC peering connection - i.e. get two VPCs to talk to each other!
3. 👤 Test VPC peering with connectivity tests.



### In this step, you're going to:

1. Get Instance 1 to send test messages to Instance 2.
2. Solve connection errors until Instance 2 is able to send messages back.
3. Leave open the **EC2 Instance Connect** tab, but head back to your **EC2** console in a new tab.
4. Select **Instance - NextWork VPC 2**.
5. Copy Instance - NextWork VPC 2's **Private IPv4 address**.
6. Switch back to the **EC2 Instance Connect** tab.
7. Run ping [the Private IPv4 address you just copied] in the terminal.

- Your final result should look similar to something like ping 10.0.1.227
- Don't know where to enter this prompt? Look for the \$ sign at the bottom line of the black window, and type in your command after the \$ sign.

```

[ec2-user@ip-10-1-0-71 ~]$ ping 54.91.237.26
PING 54.91.237.26 (54.91.237.26) 56(84) bytes of data.

```

To resolve this connectivity error, let's investigate whether **Instance - NextWork VPC 2** is allowing inbound ICMP traffic.

- Leave open the **EC2 Instance Connect** tab, but head back to your **VPC** console in a new tab.
- In the VPC console, select the **Subnets** page.
- Select VPC 2's subnet i.e. **NextWork-2-subnet-public1-...**
- Let's investigate the **Route tables** and **Network ACL** tabs for your public subnet.
- The network ACL allows all types of inbound traffic from anywhere! So this looks perfectly fine.
- Before we finish, let's check the security groups!
- Copy the **VPC ID** of VPC 2.

	Name	Subnet ID	State	VPC
<input checked="" type="checkbox"/>	NextWork-2-subnet-public1-us-west-2a	subnet-0537f7f54f69c76d6	Available	vpc-06d02f389a538a18a

- Select **Security groups** from the left hand navigation panel.
- Paste the **VPC ID** in the search bar, and select the suggested filter.
- Check your security group's **Inbound rules** tab - does this security group allow ICMP traffic from sources outside of VPC 2? (Nope!)
- Aha! Mystery solved.

Let's fix this by letting inbound ICMP traffic from VPC 1.

- Select **Edit inbound rules**.
- Select **Add new rule**.
- Change the **Type** to **All ICMP - IPv4**.
- Set the **Source** to traffic coming from VPC 1 - 10.1.0.0/16
- Select **Save rules**.

[Edit inbound rules](#) [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules

Info

Security group rule ID

Type

Info

Protocol

Info

Port range

Info

Source

Info

Description - optional

Info

sgr-0325d6e4ae42c762c	All traffic	All	All	Custom	Q		Delete
					sg-039d532ed1499a5b8		
-	All ICMP - IPv4	ICMP	All	Custom	Q 10.1.0.0/16		Delete
					10.1.0.0/16		

Add rule

Revisit the **EC2 Instance Connect** tab that's connected to Instance - NextWork VPC 1.

```

- \      #####
--   \_#____#\
--       \###|
--         \|/
--           v~'-'> https://aws.amazon.com/linux/amazon-linux-2023
               /
            ____/
        _.._/
    _./m/'

Last login: Sun Jul 28 03:30:03 2024 from 18.237.140.165
ec2-user@ip-10-1-14-132 ~]$ ping 10.2.10.154
PING 10.2.10.154 (10.2.10.154) 56(84) bytes of data:
64 bytes from 10.2.10.154: icmp_seq=1 ttl=127 time=0.424 ms
64 bytes from 10.2.10.154: icmp_seq=2 ttl=127 time=0.407 ms
64 bytes from 10.2.10.154: icmp_seq=3 ttl=127 time=0.433 ms

```