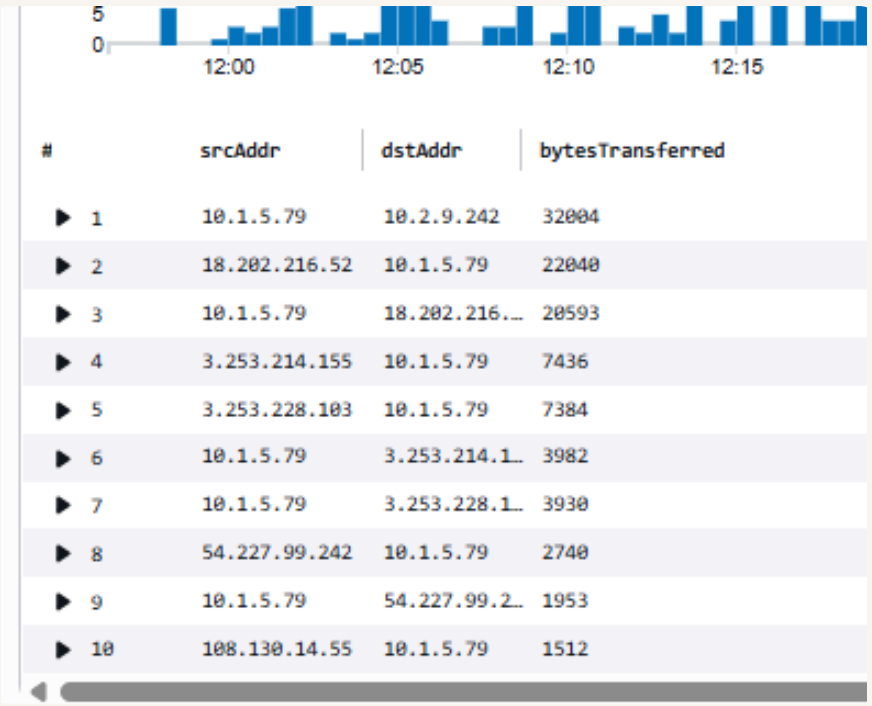
nextwork.org

VPC Monitoring with Flow Logs

OR ucbethuel



#	srcAddr	dstAddr	bytesTransferred
1	10.1.5.79	10.2.9.242	32004
2	18.202.216.52	10.1.5.79	22040
3	10.1.5.79	18.202.216.…	20593
4	3.253.214.155	10.1.5.79	7436
5	3.253.228.103	10.1.5.79	7384
6	10.1.5.79	3.253.214.1…	3982
7	10.1.5.79	3.253.228.1…	3930
8	54.227.99.242	10.1.5.79	2740
9	10.1.5.79	54.227.99.2…	1953
10	108.130.14.55	10.1.5.79	1512

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is Virtual Private Cloud and it is useful because it helps us create private network and connect our resources together

How I used Amazon VPC in this project

In today's project, I used Amazon VPC Flow log to keep track of traffic in out VPC which are stored and analyse in Amazon CloudWatch.

One thing I didn't expect in this project was...

none yet

This project took me...

This project took me 2 and half hour

In the first part of my project...

Step 1 - Set up VPCs

In this step, I will be creating two VPC from scratch.

Step 2 - Launch EC2 instances

In this step, I will Launch an EC2 instance in each VPC, so we can use them to test your VPC peering connection later.

Step 3 - Set up Logs

In this step, I will 1. Set up a way to track all inbound and outbound network traffic. 2. Set up a space that stores all of these records.

Step 4 - Set IAM permissions for Logs

In this step, I will 1. Give VPC Flow Logs the permission to write logs and send them to CloudWatch. 2. Finish setting up your subnet's flow log.

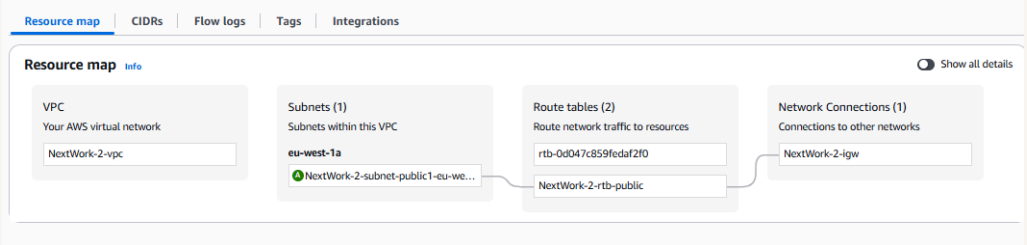
Multi-VPC Architecture

I started my project by launching my VPC using the VPC wizard, and in each VPC i have one subnet which is a public subnet connected to the internet gateway. within each at the moment, no private subnet, makes makes it a total of 1 subnet each.

The CIDR blocks for VPCs 1 and 2 are 10.1.0.0/16 and 10.2.0.0/16 respectively. They have to be unique because to avoid overlapping of IP addresses since we are peer connecting.

I also launched EC2 instances in each subnet

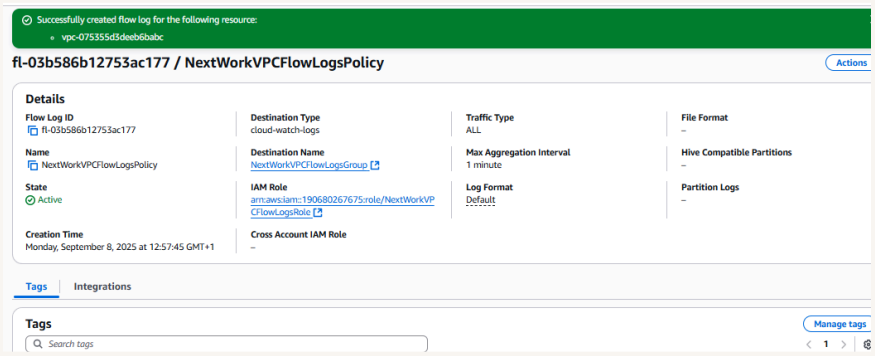
My EC2 instances' security groups allow ICMP traffic form any IP addresses, This is because we need to quick test the connectivity of both VPC.



Logs

Logs are activities of my computer been recorded.

Log groups are like folders that collects related logs together.



IAM Policy and Roles

I created an IAM policy because by default do not send logs entries to cloudWatch.

I also created an IAM role because my flow log needs a service role, which is yet to be created.

A custom trust policy is kind of IAM policy but not it, it used to very narrowly define who can use a role.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Principal": {
                "Service": "vpc-flow-logs.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

In the second part of my project...

Step 5 - Ping testing and troubleshooting

In this step, I will Get Instance - EC2 1 to send test messages to Instance - EC2 2.

Step 6 - Set up a peering connection

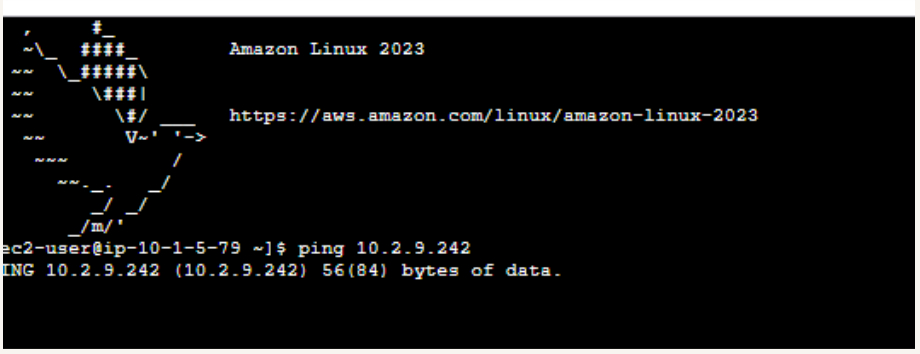
In this step, I will Set up a connection link between your VPCs.

Step 7 - Analyze flow logs

In this step, I will 1. Review the flow logs recorded aboout VPC 1's public subnet. 2. Analyse the flow logs to get some tasty insights

Connectivity troubleshooting

My first ping test between my EC2 instances had no replies, which suggest there could be a problem, let me troubleshoot.



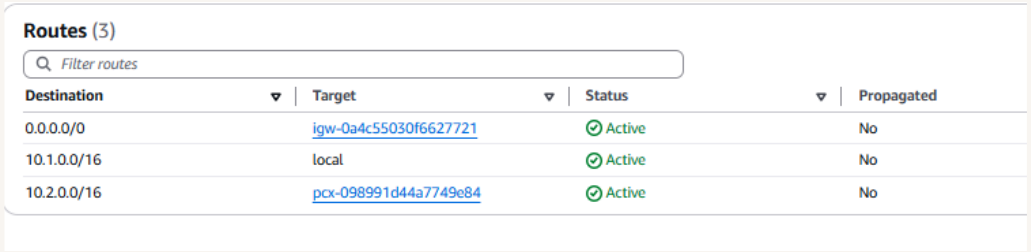
I could receive ping replies if I ran the ping test using the other instance's public IP address, which means both VPC can communicate over the internet.

Connectivity troubleshooting

Looking at VPC 1's route table, I identified that the ping test with Instance 2's private address failed because base on self discovery, we are yet to create a "peering connection" and also update the route table of each vpc.

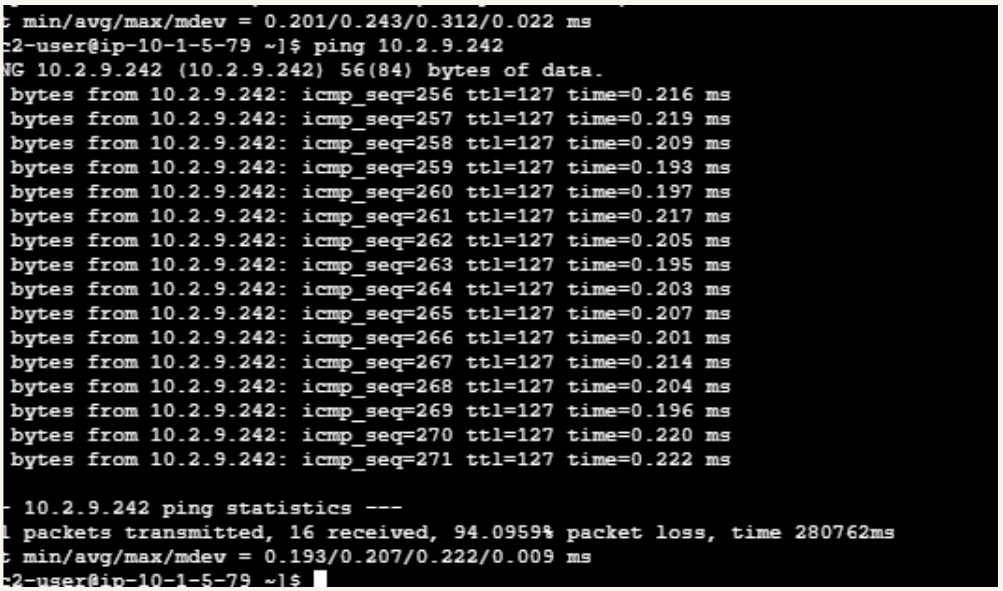
To solve this, I set up a peering connection between my VPCs

I also updated both VPCs' route tables so that in order to direct traffic to the appropriate destination.



Connectivity troubleshooting

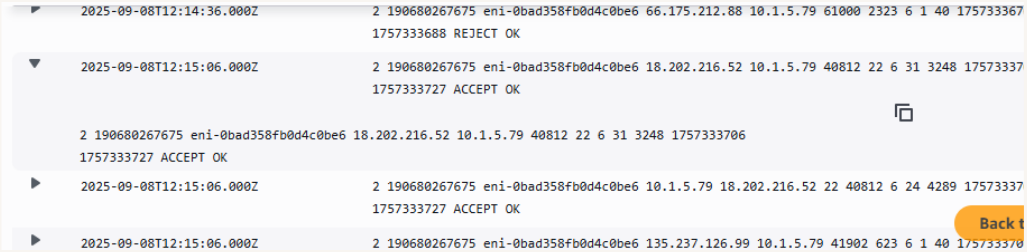
I received ping replies from Instance 2's private IP address! This means both vpc can now communicate internally.



Analyzing flow logs

Flow logs tell us about the inbound and outbound traffic of a network.

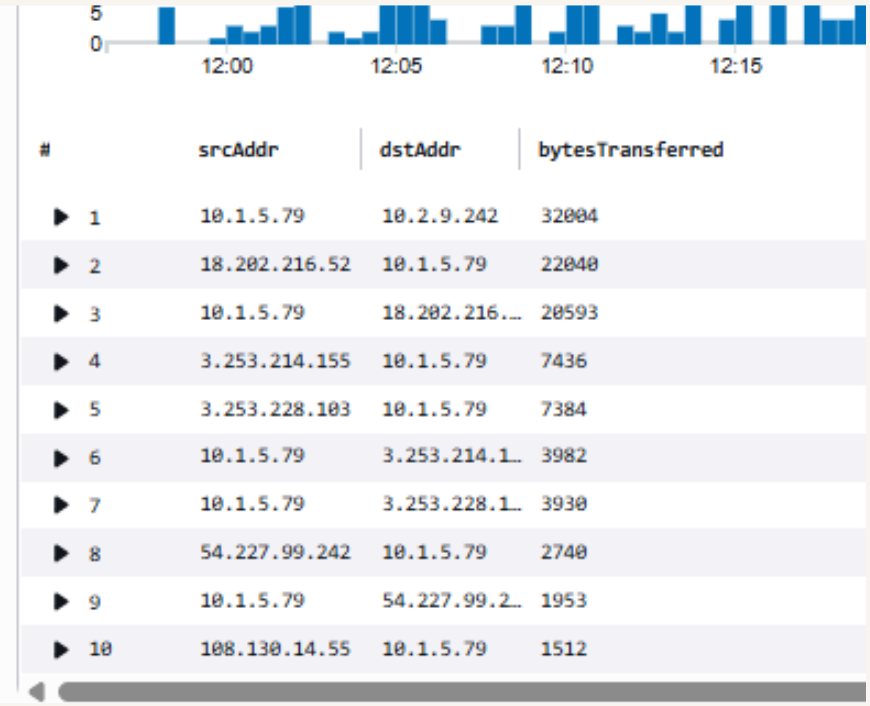
For example, the flow log I've captured tells us that a traffic from ip:18.202.216.52 went to ip:10.1.5.79 though the port 22 of tcp, with a 31 data packet which amount to 3248 bytes of data. Also the transfer was accepted and ok.



Logs Insights

Logs Insights is helps us to visualize and run queries partaining to out traffic registered.

I ran the query top 10 inbound and outbound, This query analyzes top ten inbound and outbound traffic captured.



#	srcAddr	dstAddr	bytesTransferred
1	10.1.5.79	10.2.9.242	32004
2	18.202.216.52	10.1.5.79	22040
3	10.1.5.79	18.202.216.…	20593
4	3.253.214.155	10.1.5.79	7436
5	3.253.228.103	10.1.5.79	7384
6	10.1.5.79	3.253.214.1…	3982
7	10.1.5.79	3.253.228.1…	3930
8	54.227.99.242	10.1.5.79	2740
9	10.1.5.79	54.227.99.2…	1953
10	108.130.14.55	10.1.5.79	1512

The place to learn & showcase your skills

Check out nextwork.org for more projects