We need additional custom metrics within AWS CloudWatch Metrics to record IP address usage within AWS VPC Subnets. How would you build a solution to achieve this?

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC.

If you launch an instance into your subnet after you create a flow log for your subnet or VPC, we create a log stream (for CloudWatch Logs).

Steps for VPC Flow Logs, publish flow logs to CloudWatch:

1- VPC and subnets created.
2- Launched an Amazon Linux 2 EC2 instance in Public Subnets
3- Installed and Configured Nginx Web Server to Run a Simple Web Page on the instance
4- IAM role created for publishing flow logs to CloudWatch Logs:

Nginx-flow-logs-policy (JSON):

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource": "*"
    }
  ]
     }
```

Nginx-flow-logs-role:

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

5- Log group created in the CloudWatch console.

6- A flow log is created that publishes to CloudWatch Logs
Choose Subnets which the Nginx server inside

Subnets ➔ Actions ➔ Create Flow logs
Filter ➔ All or Reject or Accept
Destination ➔ Send to CloudWatch Logs
IAM Role ➔ Nginx-flow-logs-role
Destination log group ➔ Log group that is created
Create

Flow log created and published to CloudWatch Logs

……

To create flow logs by AWS CLI:

**$ aws ec2 create-flow-logs --resource-type Subnet --resource-ids **
**subnet-0ef7e1e37b9a7c8d1 --traffic-type ACCEPT **
--log-group-name Nginx-flow-logs --deliver-logs-permission-arn
arn:aws:iam::452889875890:policy/nginx-flow-logs-policy