**Step1: Configure AWS Security Group Rules**

**📌 AWS Security Groups (SGs) act as a virtual firewall for EC2 instances. We need to:**

* **Allow ICMP (Ping) from Azure → AWS**
* **Allow UDP 51820 (WireGuard VPN) from Azure → AWS**
* **Allow SSH (Port 22) from Azure → AWS**
* **Allow HTTP/HTTPS if needed for application traffic**

**Find the Security Group attached to the AWS EC2 instance:**

aws ec2 describe-instances --instance-ids <INSTANCE\_ID> --query 'Reservations[\*].Instances[\*].SecurityGroups[\*].GroupId'

**Verifies network reachability between AWS and Azure.**

aws ec2 authorize-security-group-ingress --group-id sg-0abcdef1234567890 --protocol icmp --port -1 --cidr <AZURE\_PRIVATE\_IP>/32

**Ensures VPN tunnel remains active.**

aws ec2 authorize-security-group-ingress --group-id sg-0abcdef1234567890 --protocol udp --port 51820 --cidr <AZURE\_PRIVATE\_IP>/32

**Allows SSH access for debugging and management.**

aws ec2 authorize-security-group-ingress --group-id sg-0abcdef1234567890 --protocol tcp --port 22 --cidr <AZURE\_PRIVATE\_IP>/32

**Allows public web access to applications running on AWS.**

aws ec2 authorize-security-group-ingress --group-id sg-0abcdef1234567890 --protocol tcp --port 80 --cidr 0.0.0.0/0

aws ec2 authorize-security-group-ingress --group-id sg-0abcdef1234567890 --protocol tcp --port 443 --cidr 0.0.0.0/0

**If all rules are applied correctly, proceed to Azure.**

aws ec2 describe-security-groups --group-ids sg-0abcdef1234567890 --query 'SecurityGroups[\*].IpPermissions'

**Step 2: Configure Azure Network Security Group (NSG) Rules**

📌 **Azure Network Security Groups (NSGs) control traffic to VMs. We need to:**

* **Allow ICMP (Ping) from AWS → Azure**
* **Allow UDP 51820 (WireGuard VPN) from AWS → Azure**
* **Allow SSH (Port 22) from AWS → Azure**
* **Allow HTTP/HTTPS if needed for application traffic**

**Find the Network Security Group (NSG) associated with the Azure VM:**

az network nic list --query "[].{NIC: name, ResourceGroup: resourceGroup}" -o table

**Then, check which NSG is linked to the NIC:**

az network nic show --name <NIC\_NAME> --query "networkSecurityGroup.id"

**Verifies AWS can reach Azure.**

az network nsg rule create --resource-group WireGuardRG --nsg-name wireguard-sg --name Allow-Ping --priority 200 --direction Inbound --access Allow --protocol Icmp --source-port-range "\*" --destination-port-range "\*" --source-address-prefix "172.31.34.15" --destination-address-prefix "\*"

**Ensures VPN tunnel remains active.**

az network nsg rule create --resource-group WireGuardRG --nsg-name wireguard-sg --name Allow-WireGuard --priority 100 --direction Inbound --access Allow --protocol Udp --source-port-range "\*" --destination-port-range 51820 --source-address-prefix “172.31.34.15” --destination-address-prefix "\*"

**Allows SSH access for debugging and management.**

az network nsg rule create --resource-group WireGuardRG --nsg-name wireguard-sg --name Allow-Ping --priority 120 --direction Inbound --access Allow --protocol tcp --source-port-range "\*" --destination-port-range 22 --source-address-prefix "172.31.34.15" --destination-address-prefix "\*"

**If hosting a web application, allow HTTP (80) and HTTPS (443):**

az network nsg rule create --resource-group WireGuardRG --nsg-name wireguard-sg --name Allow-HTTP --priority 130 --direction Inbound --access Allow --protocol Tcp --source-port-range "\*" --destination-port-range 80 --source-address-prefix "\*" --destination-address-prefix "\*"

For listening that is the connection is working or not

echo "hello" | nc -u -w1 10.1.1.4 51821

nc -u -l -p 51821

I have skipped the step of setting up the guard duty I need to see it after few days.

**Ensure AWS and Azure have proper routes for WireGuard traffic.**

**🔹 On AWS Instance**

ip route show

✅ **Expected Output:**

10.1.1.4 dev wg0 scope link

**CloudWatch:**

aws cloudwatch put-metric-alarm --alarm-name MyAlarm --metric-name CPUUtilization --namespace AWS/EC2 --statistic Average --period 300 --threshold 80 --comparison-operator GreaterThanThreshold --dimensions Name=WireGuardAWS,Value=ami-07a64b147d3500b6a --evaluation-periods 2 --alarm-actions arn:aws:sns:eu-north-1:222634378365:Wireguard

**Azure Metrics:**

**This command which is used to get the Scope ID in the next command**

az vm show --resource-group WireGuardRG --name WireGuardAzure --query id --output tsv

**This command is used to create a Metrics for alert**

az monitor metrics alert create --name MyAlert --resource-group WireGuardRG --scopes /subscriptions/25bcf5d0-16ab-458b-b03a 0d97376069e0/resourceGroups/WireGuardRG/providers/Microsoft.Compute/virtualMachines/WireGuardAzure --condition "avg Percentage CPU > 80" --window-size 5m --evaluation-frequency 1m

**CloudTrail and S3 Buckets**

aws cloudtrail create-trail --name MyTrail --s3-bucket-name my-security-logs

aws cloudtrail start-logging --name MyTrail

### Step 1: Go to S3 Console → cloudtraillogs2025 → Permissions → Bucket Policy

Paste this correct Policy (replace your bucket name & account id)

{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "AWSCloudTrailWrite",

"Effect": "Allow",

"Principal": {

"Service": "cloudtrail.amazonaws.com"

},

"Action": "s3:PutObject",

"Resource": "arn:aws:s3:::cloudtraillogs2025/AWSLogs/<Your-Account-ID>/\*",

"Condition": {

"StringEquals": {

"s3:x-amz-acl": "bucket-owner-full-control"

}

}

},

{

"Sid": "AWSCloudTrailList",

"Effect": "Allow",

"Principal": {

"Service": "cloudtrail.amazonaws.com"

},

"Action": "s3:GetBucketAcl",

"Resource": "arn:aws:s3:::cloudtraillogs2025"

}

]

}

### Create Metric Filter in CloudWatch for IAM Role Changes

aws logs put-metric-filter --log-group-name "aws-cloudtrail-logs-222634378365-6b9fb995" --filter-name "IAMRolechangealerts" --filter-pattern '{($.eventName=CreateRole) || ($.eventName=DeleteRole) || ($.eventName=AttachRolePolicy) || ($.eventName=DetachRolePolicy) || ($.eventName=UpdateAssumeRolePolicy)}' --metric-transformations metricName=IAMRoleChangeCount,metricNamespace=SecurityMetrics,metricValue=1

aws logs describe-log-groups --query "logGroups[\*].logGroupName" (To know the group name which is to be replaced with our log group name in above command)

### Create Alarm for That Metric

aws cloudwatch put-metric-alarm --alarm-name "IAM-Role-Change-Alert" --metric-name IAMRoleChangeCount --namespace SecurityMetrics –statistic Sum --period 300--threshold 1 --comparison-operator GreaterThanOrEqualToThreshold --evaluation-periods 1--alarm-actions arn:aws:sns:your-region:account-id:WireGuard

az monitor activity-log alert create --name IAM-Role-Change-Alert --resource-group YourRG --scopes /subscriptions/your-subscription-id --condition "category=Administrative and (operationName=Microsoft.Authorization/roleAssignments/write OR operationName=Microsoft.Authorization/roleAssignments/delete)" --action-group IAM-RoleChange-ActionGroup