1. Create accounts for Amazon Web Services and Microsoft Azure portal and log into both
2. Create a virtual network and subnet in Azure
    a. Open up azure portal first and on the search bar type in Virtual Networks and navigate to that section
    b. Create a virtual network and create a new resource group and call the resource group *AWSConnectionArchitecture*
    c. Call the Virtual network name *AzureVNet* and select the region that your Azure is currently connected in and click IP Addresses on the top bar
    d. Change the IPv4 address under the button “Add a subnet” to *10.1.0.0/16*
    e. Click add a subnet on the top of the screen
    f. Select the Subnet purpose as *Virtual Network Gateway*
    g. Set the IPv4 Address range to 10.1.0.0/16
    h. Set the starting address as *10.1.1.0* and size as */24*
    i. Click Review+Create and click create
    j. Let the deployment be created and complete
3. Create a Virtual Network Gateway in Azure
    a. In azure portal on the search bar, type in Virtual Network Gateways and navigate there
    b. Click Create VIrtual Network Gateway
    c. Name the gateway *Azure-VPN-Gateway*
    d. Select the SKU as *VpnGw2*
    e. Select *Generation 2* as the Generation
    f. Select the Virtual Network as *AzureVNet*
    g. Create a new Public IP Address and call it *Azure-To-AWS-PublicIP*
    h. Create the Second Public IP Address and call it *Azure-To-AWS-PublicIP-2*
    i. Click Review + Create and click create
    j. Let the deployment be created and complete
4. Create a VPC(Virtual Private Cloud) in AWS
    a. Open up the AWS portal and search VPC and navigate there
    b. Click create VPC on the top of the screen
    c. Select VPC only on the left panel
    d. Name the VPC *AWSVPC*
    e. Create the IPv4 CIDR address *10.2.0.0/16*
    f. Create the VPC
5. Create VPG(Virtual Private Gateway) in AWS
    a. Navigate back to VPC Dashboard and select Virtual Private Gateways
    b. Name the VPG as *AWS-VPN-Gateway*
    c. Leave the ASN as default
    d. Click the circle to select the VPG and select Actions and click Attatch to VPC
    e. When in the menu for Attatch to VPC select AWSVPC and attach
6. Create Customer Gateway in AWS
    a. Search Customer Gateway in AWS in the VPC dashboard
    b. Create a customer gateway
    c. Call the gateway *AzureCustomerGateway*

    d. Go back to Azure and search Azure-To-AWS-PublicIP and copy the IP address
    e. Go back to the customer gateway and paste the IP Address in and click create
7. Create site to site connection in AWS
    a. Search Site-to-Site VPN Connections in AWS in the VPC dashboard
    b. You will be redirected to a menu called VPN connections
    c. Click on Create VPN Connection
    d. Name the VPC Connection *AWS-Azure-VPN*
    e. Select *AWS-VPN-Gateway* for the VPG
    f. Select *AzureCustomerGateway*
    g. Set the Routing options as Static
    h. Set the Static IP Prefixes as *10.1.0.0/16*
    i. Click Create VPC connection
8. Configure Azure VPN connection
    a. Search Local Network Gateway in Azure
    b. Create a new Local Network Gateway in Azure
    c. Select *AWSConnectionArchitecture* as the resource group
    d. Call the Gateway *AWSLocalGateway*
    e. Go to AWS to the Site to Site dashboard under VPC
    f. Select *AWS-Azure-VPN*
    g. On the bottom select Tunnel Details and select one of the outside IP addresses, preferable Tunnel 1
    h. Paste in the IP address back in Azure in the IP address space
    i. For Address Space(s) set it to 10.2.0.0/16
    j. Click Review and create and create
9. Create Connection in Azure
    a. Search Connections in Azure, there will be 2 symbols, click the symbol that has a circle and “><” inside of it
    b. Create new Connection
    c. Select *AWSConnectionArchitecture* as the resource group
    d. Set the connection type as Site-to-site(IPsec)
    e. Name the connection *AzureToAWSVPN*
    f. Go to settings tab and select *Azure-VPN-Gateway* for the first Virtual Network Gateway
    g. Select *Azure-VPN-Gateway* for the Secont Virtual Network Gateway
    h. Go to AWS in the Site-to-site dashboard and select *AWS-Azure-VPN*
    i. Click Actions and select Modify VPN Tunnel Options
    j. Copy the PSK in that menu and paste it into Azure under Shared Key
    k. Select IKEv2 as the IKE protocol and click review and create
10. Configure Route Tables in AWS
    a. Search Route Table in the search bar in AWS
    b. Click the already created Route Table associated with the VPC
    c. On the bottom of the screen click Routes
    d. Click Edit Routes
    e. In the edit menu, select Add Route, and add 10.1.0.0/16 as the destination

f. Select Virtual Private Gateway as the Target, then select *AWS-VPN-Gateway*
g. Click Save Changes

11. Configure Azure Network Security Group
    a. Go to Azure and search Network Security Groups
    b. Create new Network Security Group
    c. Select *AWSConnectionArchitecture* as the subnet
    d. Name this group *Allow-AWS-To-Azure-NSG*
    e. Click Review and Create then create
    f. Click go to Resource
    g. Click settings on the left tab and select Inbound Security Rules
    h. Click Add
    i. Sekect the source as IP address
    j. Enter 10.2.0.0/16 as the IP address
    k. Write * for source port ranges
    l. Write *22* as the Destination port ranges
    m. Select *TCP* as the protocol
    n. Set the priority as *1000*
    o. Name the Security rule as *Allow-AWS-SSH*
    p. Click Add on the bottom of the screen
12. Create EC2 Instance in AWS
    a. Go to EC2 dashboard in AWS
    b. Click Launch Instance
    c. Name the Instance *AWS-EC2-Instance*
    d. Select Ubuntu as the AMI
    e. Select Ubuntu Server 22.04 LTS Free Tier
    f. Select t2.micro free tier
    g. Create new Key pair
    h. Call the name *AWS-EC2-Key*
    i. Select RSA as the key pair tupe
    j. Select .ppk as the format
    k. Click Create Key Pair
    l. Edit Network Settings
    m. Select *AWSVPC* as the VPC
    n. Click Create new Subnet
        i. Select AWSVPC as the VPC
        ii. Call the Subnet *AWSSubnet1*
        iii. Select *us-east-2a* as the availability zone
        iv. Select 10.2.0.0/16 as the IPv4 VPC CIDR block
        v. Select 10.2.1.0/24 as the subnet CIDR block
        vi. Create Subnet
    o. Select *AWSSubnet1* as the subnet
    p. Select *Enable* for Auto Assign Public IP
    q. Create new security group for firewall
    r. Click Launch Instance

13. Create a VM in Azure
    a. Search Virtual Machine in Azure
    b. Create a new Virtual Machine
    c. Select *AWSConnectionArchitechture* as the resource group
    d. Call the VM *AzureVM*
    e. Select the region as US East
    f. Scroll down to image and select Ubuntu 22.04 LTS
    g. Set size as Standard B1s
    h. Set Authentication type as SSH public key
    i. Set the username as *azureuser*
    j. Select Generate New Key Pair
    k. RSA SSH Format
    l. Call the key pair *AzureVM-key*
    m. Go to the network tab
    n. Select AzureVNet as the virtual network
    o. Create new Public IP called *AzureVM-ip*
    p. Select Advanced as the NIC network security group
    q. Select Allow-AWS-To-Azure-NSG
    r. Click Review and create then Create
    s. Download private key and create resource
14. Open EC2 instance
    a. Search Elastic IPs
    b. Allocate Elastic IP Address
    c. Leave the settings as default and click Allocate
    d. Search Internet Gateway
    e. Create Internet Gateway
    f. Call this MyIGW
    g. Click Create
    h. Click Actions
    i. Attatch to VPC
    j. Select AWSVPC
    k. Go to Route Table
    l. Click your route, and on the bottom of the screen click edit routes
    m. Add route, set destination as 0.0.0.0/0
    n. Select Internet Gateway
    o. Select MyIGW
    p. Save Routes
    q. Go back to Elastic IPS
    r. Click Action on created IP
    s. Click Associate Elastic IP Address and add EC2 and Private IP created
    t. Click on AWS-EC2-Instance in EC2 dashboard and copy the IP address, in my case, the IP address is 3.139.46.141 and I will be referencing to that for the rest of this document
    u. Open PuTTY and enter ubuntu@3.139.46.141 as the host name

v. On the left, click the plus next to SSH, The plus next to Auth, then click credentials
w. Click Browse next to Private Key File for Authentication
x. Select AWS-EC2-Key
y. Click Open

15. Open VM Instance
    a. Open Azure VM portal
    b. Click Networking and Network Settings
    c. Create Port Rule
    d. Create Inbount Rule
    e. Source
    f. IP Addresses 20.115.93.57
    g. Destination Port Range 22
    h. Protocol TCP
    i. Priority 100
    j. Name, Allow-SSH-From-Home
    k. Go to Network Interfaces
    l. Select public IP address, mine is 20.115.93.57
    m. Open PuttyGen
    n. Load the .pem key
    o. Click Save Private Key
    p. Click YES to save without passphrase
    q. Call the new key azure_key.ppk
    r. Paste 20.115.93.57 into the host name
    s. On the left, click the plus next to SSH, The plus next to Auth, then click credentials
    t. Click Browse next to Private Key File for Authentication
    u. Open azure_key.ppk
    v. Click Open
16. Test Pings in internal IPs
    a. Go to EC2 Dashboard in AWS and click instance details and copy the Private IPv4 Address, in my case it is, 10.2.1.244
    b. Go to Azure VM dashboard and Go to Overview and find private IP address, in my case it is 10.1.0.4
    c. In the AWS Terminal, labelled ubuntu@ip-10-2-1-244 on the top, type in this command to test the ping
        i. ping 10.1.0.4
    d. This will output a ping showing the connection between AWS terminal and Azure IP
    e. In the Azure Terminal, labelled, azureuser@AzureVM on the top, type this command to test the ping
        i. ping 10.2.1.244
    f. This will output a ping showing the connection between the Azure Terminal and AWS IP