**Project**

**Problem Statement:**

**Implement Hub and Spoke topology where Hub contains the centralized components like Azure Firewall, Application Gateway, DNS Forwarding VM, Azure Bastion etc. and one spoke has Web App and another spoke has a Storage account with no public access.**

**1. Establishes a secure connection between the on-premises data center and the hub VNet and Spoke VNets.**

**2. Provides custom DNS on the top of Spoke VNets as DNS Forwarding VM.**

**3. Resolve all the DNS quries for Azure to On Premises, Azure to Azure and On Premises to Azure.**

**4. All the traffic should be routed through Azure Firewall.**

**5. Internet traffic will land on Application Gateway Public Fronted IP. 6. On-Premises traffic will land on Application Gateway Private Fronted IP.**

**7. SSL Offloading will be implemented on top of Application Gateway.**

**8. Set up multiple listeners to route traffic to the backend with their respective set of configurations.**

**Prerequisites**

* **Azure Subscription:** Ensure you have an active Azure subscription.
* **Azure Portal Access:** Familiarize yourself with the Azure Portal.

**Basic Step Guidelines**

**Step 1: Create Resource Groups**

1. Go to the Azure portal.
2. Click on **Resource groups** in the left-hand menu.
3. Click **+ Add** to create new resource groups.
4. Create three resource groups:
   * Name: HubResourceGroup, Location: East US
   * Name: Spoke1ResourceGroup, Location: East US
   * Name: Spoke2ResourceGroup, Location: East US

**Step 2: Create Virtual Networks (VNets)**

1. **Hub VNet:**
   * Go to **Virtual networks** and click **+ Add**.
   * Name: HubVNet
   * Address space: 10.0.0.0/16
   * Resource group: HubResourceGroup
   * Location: East US
   * Create a subnet:
     + Name: AzureFirewallSubnet
     + Address range: 10.0.1.0/24
   * Create another subnet:
     + Name: ApplicationGatewaySubnet
     + Address range: 10.0.2.0/24
2. **Spoke1 VNet:**
   * Go to **Virtual networks** and click **+ Add**.
   * Name: Spoke1VNet
   * Address space: 10.1.0.0/16
   * Resource group: Spoke1ResourceGroup
   * Location: East US
   * Create a subnet:
     + Name: WebAppSubnet
     + Address range: 10.1.1.0/24
3. **Spoke2 VNet:**
   * Go to **Virtual networks** and click **+ Add**.
   * Name: Spoke2VNet
   * Address space: 10.2.0.0/16
   * Resource group: Spoke2ResourceGroup
   * Location: East US
   * Create a subnet:
     + Name: StorageSubnet
     + Address range: 10.2.1.0/24

**Step 3: Create a DNS Forwarding VM**

1. **Create VM:**
   * Go to **Virtual machines** and click **+ Add**.
   * Resource group: HubResourceGroup
   * Virtual machine name: DNSForwarderVM
   * Region: East US
   * Image: Ubuntu Server 18.04 LTS
   * Size: Choose the appropriate size (e.g., Standard\_B1s)
   * Authentication type: SSH public key (provide your key)
   * Virtual network: HubVNet
   * Subnet: default
   * Public IP: None
2. **Configure DNS Forwarding:**
   * Connect to the VM using SSH.
   * Install dnsmasq:

bash

Copy code

sudo apt-get update

sudo apt-get install dnsmasq

* + Edit /etc/dnsmasq.conf to forward DNS queries.
  + Restart dnsmasq:

bash

Copy code

sudo systemctl restart dnsmasq

**Step 4: Create Azure Bastion**

1. **Create Public IP:**
   * Go to **Public IP addresses** and click **+ Add**.
   * Name: BastionPublicIP
   * SKU: Standard
   * Resource group: HubResourceGroup
   * Location: East US
2. **Create Bastion:**
   * Go to **Bastions** and click **+ Add**.
   * Name: HubBastion
   * Resource group: HubResourceGroup
   * Virtual network: HubVNet
   * Subnet: Create a subnet named AzureBastionSubnet with address range 10.0.3.0/24
   * Public IP: BastionPublicIP
   * Click **Review + Create** and then **Create**.

**Step 5: Create Azure Firewall**

1. **Create Public IP:**
   * Go to **Public IP addresses** and click **+ Add**.
   * Name: FirewallPublicIP
   * SKU: Standard
   * Resource group: HubResourceGroup
   * Location: East US
2. **Create Firewall:**
   * Go to **Firewalls** and click **+ Add**.
   * Name: HubFirewall
   * Resource group: HubResourceGroup
   * Virtual network: HubVNet
   * Public IP address: FirewallPublicIP
   * Click **Review + Create** and then **Create**.

**Step 6: Create and Configure the Application Gateway**

1. **Create Public IP:**
   * Go to **Public IP addresses** and click **+ Add**.
   * Name: AppGatewayPublicIP
   * SKU: Standard
   * Resource group: HubResourceGroup
   * Location: East US
2. **Create Application Gateway:**
   * Go to **Application gateways** and click **+ Add**.
   * Name: AppGateway
   * Resource group: HubResourceGroup
   * Virtual network: HubVNet
   * Subnet: ApplicationGatewaySubnet
   * Public IP address: AppGatewayPublicIP
   * Frontend IP configuration: Create two configurations (one public, one private)
   * Backend pools: Create backend pools as needed
   * Listeners: Create listeners for both HTTP and HTTPS (for SSL offloading)
   * Click **Review + Create** and then **Create**.

**Step 7: Create a Site-to-Site VPN Connection**

1. **Create Virtual Network Gateway:**
   * Go to **Virtual network gateways** and click **+ Add**.
   * Name: HubVNetGateway
   * Resource group: HubResourceGroup
   * Virtual network: HubVNet
   * Gateway type: VPN
   * VPN type: Route-based
   * SKU: VpnGw1
   * Public IP address: Create new HubVNetGatewayPublicIP
   * Click **Review + Create** and then **Create**.
2. **Create Local Network Gateway:**
   * Go to **Local network gateways** and click **+ Add**.
   * Name: OnPremisesLocalGateway
   * Resource group: HubResourceGroup
   * Gateway IP address: <OnPremisesPublicIP>
   * Address space: <OnPremisesAddressPrefix>
   * Click **Review + Create** and then **Create**.
3. **Create VPN Connection:**
   * Go to **Virtual network gateways**.
   * Select HubVNetGateway.
   * Under **Settings**, click **Connections**.
   * Click **+ Add**.
   * Name: HubToOnPremConnection
   * Connection type: Site-to-site (IPsec)
   * Local network gateway: OnPremisesLocalGateway
   * Shared key: <SharedKey>
   * Click **OK**.

**Step 8: Configure DNS Forwarding**

1. **Update VNet DNS Settings:**
   * Go to **Virtual networks**.
   * Select HubVNet, Spoke1VNet, and Spoke2VNet one by one.
   * Under **Settings**, click **DNS servers**.
   * Add the private IP address of the DNSForwarderVM.

**Step 9: Configure Private Endpoints for Storage Account**

1. **Create Private Endpoint:**
   * Go to **Private endpoints** and click **+ Add**.
   * Name: StoragePrivateEndpoint
   * Resource group: Spoke2ResourceGroup
   * Virtual network: Spoke2VNet
   * Subnet: StorageSubnet
   * Private link resource: Select your Storage Account
   * Click **Review + Create** and then **Create**.

**Step 10: Configure Network Peering**

1. **Hub to Spoke1:**
   * Go to **Virtual networks** and select HubVNet.
   * Under **Settings**, click **Peerings**.
   * Click **+ Add**.
   * Name: HubToSpoke1
   * Peer details: Select Spoke1VNet.
   * Click **Add**.
2. **Spoke1 to Hub:**
   * Go to **Virtual networks** and select Spoke1VNet.
   * Under **Settings**, click **Peerings**.
   * Click **+ Add**.
   * Name: Spoke1ToHub
   * Peer details: Select HubVNet.
   * Click **Add**.
3. **Hub to Spoke2:**
   * Repeat the process for HubVNet and Spoke2VNet.

**Step 11: Route Traffic Through Azure Firewall**

1. **Create Route Table:**
   * Go to **Route tables** and click **+ Add**.
   * Name: HubRouteTable
   * Resource group: HubResourceGroup
   * Location: East US
   * Click **Review + Create** and then **Create**.
2. **Create Routes:**
   * Select HubRouteTable.
   * Under **Settings**, click **Routes**.
   * Click **+ Add**.
   * Name: DefaultRoute
   * Address prefix: 0.0.0.0/0
   * Next hop type: Virtual appliance
   * Next hop address: <AzureFirewallPrivateIP>
   * Click **OK**.
3. **Associate Route Table with Subnets:**
   * Go to **Virtual networks**.
   * Select HubVNet, Spoke1VNet, and Spoke2VNet subnets one by one.
   * Under **Settings**, click **Subnets**.
   * Select the relevant subnet and associate the HubRouteTable.

**Step 12: Configure Application Gateway Listeners and Backends**

1. **Application Gateway Configuration:**
   * Go to **Application gateways** and select AppGateway.
   * Under **Settings**, click **Listeners**.
   * Create listeners for HTTP and HTTPS.
   * Under **Backend pools**, add backend pools.
   * Under **HTTP settings**, configure HTTP settings and SSL offloading.

**Step 13: SSL Offloading on Application Gateway**

1. **Upload SSL Certificate:**
   * Go to **Application gateways** and select AppGateway.
   * Under **Settings**, click **SSL certificates**.
   * Click **+ Add** to upload your SSL certificate.
2. **Configure SSL Offloading:**
   * Under **Listeners**, select the HTTPS listener.
   * Associate the uploaded SSL certificate.

**Step 14: Testing and Validation**

1. **Test DNS Resolution:**
   * Ensure that DNS queries are resolved correctly for Azure and on-premises resources.
2. **Test Connectivity:**
   * Test connectivity between on-premises and Azure resources.
3. **Verify Routing:**
   * Verify that all traffic is routed through the Azure Firewall.

By following these steps, you can set up a secure and well-architected Hub and Spoke topology in Azure using the Azure portal. Make sure to review Azure pricing and optimize configurations to manage costs effectively.