To implement a Hub and Spoke topology in Azure, where the hub contains centralized components and spokes have specific resources like Web App and Storage account, you need to follow a series of steps to ensure secure connections, DNS resolution, traffic routing, and SSL offloading. Here's a detailed guide:

1. Set Up Hub and Spoke VNets

Step 1: Create Hub VNet
1. Navigate to Azure Portal: [Azure Portal](https://portal.azure.com)
2. Create VNet:
- Go to "Create a resource" -> "Networking" -> "Virtual network".
- Name: HubVNet
- Address space: 10.0.0.0/16
- Subnets: Create subnets for Firewall, Application Gateway, DNS Forwarding VM, Bastion.

Step 2: Create Spoke VNets
1. Spoke 1 (Web App):
- Name: Spoke1VNet
- Address space: 10.1.0.0/16
- Subnets: Create a subnet for the Web App.

2. Spoke 2 (Storage Account):
- Name: Spoke2VNet
- Address space: 10.2.0.0/16
- Subnets: Create a subnet for the Storage Account.

2. Establish Secure Connections

Step 1: VNet Peering
1. Hub to Spoke Peering:
- Go to "HubVNet" -> "Peerings" -> "Add".
- Name: HubToSpoke1, HubToSpoke2
- Select the corresponding Spoke VNet.
- Allow forward and reverse traffic.

2. Spoke to Hub Peering:
- Go to "Spoke1VNet" -> "Peerings" -> "Add".
- Name: Spoke1ToHub
- Select the Hub VNet.
- Allow forward and reverse traffic.
- Repeat for Spoke2VNet.

Step 2: VPN Gateway
1. Create VPN Gateway in HubVNet:

- Go to "Create a resource" -> "Networking" -> "Virtual network gateway".
- Name: HubVNetGateway
- SKU: VpnGw2 (or appropriate SKU)
- Public IP: Create new
- Virtual network: HubVNet
- Gateway type: VPN
- VPN type: Route-based

2. Configure On-Premises Connection:
- Create a Local Network Gateway with the on-premises address space and public IP.
- Create a Site-to-Site connection between the VPN Gateway and the Local Network Gateway.

3. DNS Configuration

Step 1: Deploy DNS Forwarding VM in HubVNet
1. Create VM:
- Deploy a VM (e.g., Windows Server) in the DNS subnet of HubVNet.
- Install DNS role on the VM.
- Configure forwarders to Azure's 168.63.129.16 and on-premises DNS servers.

Step 2: Configure Custom DNS
1. Hub VNet:
- Go to "HubVNet" -> "DNS servers".
- Add the DNS Forwarding VM's IP.

2. Spoke VNets:
- Go to each Spoke VNet -> "DNS servers".
- Add the DNS Forwarding VM's IP.

4. Traffic Routing

Step 1: Deploy Azure Firewall in HubVNet
1. Create Azure Firewall:
- Go to "Create a resource" -> "Networking" -> "Azure Firewall".
- Name: HubFirewall
- Virtual network: HubVNet
- Public IP: Create new

2. Configure Route Tables:
- Create a Route Table in HubVNet.
- Add routes to direct traffic through Azure Firewall.
- Associate the Route Table with subnets in Hub and Spoke VNets.

Step 2: Deploy Application Gateway in HubVNet

1. Create Application Gateway:

- Go to "Create a resource" -> "Networking" -> "Application Gateway".
- Name: HubAppGateway
- Virtual network: HubVNet
- Subnets: Application Gateway subnet
- Frontend IP: Create both Public and Private IPs
- Backend pools: Configure pools with respective backends (e.g., Web App in Spoke1, Storage Account in Spoke2)

2. Configure SSL Offloading:

- Upload SSL certificate to Application Gateway.
- Configure listeners for SSL offloading.
- Set up HTTP settings for SSL offload.

5. Configure Listeners and Routing Rules

1. Create Listeners:

- Go to "Application Gateway" -> "Listeners".
- Add multiple listeners for different frontend IPs and ports.

2. Set Up Routing Rules:

- Go to "Application Gateway" -> "Rules".
- Create rules to route traffic based on listeners to appropriate backend pools.

6. Monitor and Manage

Step 1: Monitor Traffic

1. Network Watcher:

- Use Azure Network Watcher to monitor VNet peering and traffic flow.
- Enable NSG flow logs for subnets.

2. Application Gateway Logs:

- Enable diagnostic settings for Application Gateway to monitor traffic and performance.

Step 2: Manage DNS Queries

1. Configure DNS Forwarding VM:

- Ensure the DNS Forwarding VM can resolve queries for Azure, On-Premises, and hybrid environments.
- Use Azure Private DNS Zones for Azure resources.