**Use Case**: Secure Deployment of a Multi-Tier Web Application on Azure

Scenario:

Company: Contoso Ltd., a retail company that wants to migrate its e-commerce platform to the cloud to handle increasing traffic and improve security.

Objective: Deploy a multi-tier web application on Azure that can securely connect to the company’s on-premises data center, ensure high availability, scalability, and maintain strict network security between application tiers.

Challenges:

Contoso’s e-commerce platform requires different layers for the web interface, application logic, and database.

The company must ensure that all communications, both within Azure and between Azure and the on-premises data center, are secure.

The architecture must be scalable to handle peak traffic loads, such as during holiday sales.

Use Case:

Contoso Ltd. has decided to use Azure to deploy its multi-tier web application. The architecture needs to include a front-end web layer, an application processing layer, and a back-end database layer. The solution must integrate with the on-premises data center via a secure connection.

Requirement: Isolate and secure network traffic between different tiers (web, application, database) within Azure.

Solution: Implement a Hub-and-Spoke Virtual Network Architecture.

Hub Network: A central virtual network in Azure acting as a secure connectivity hub for the on-premises data center and Azure services.

Spoke Networks: Separate virtual networks for each application tier (front-end, application, database), peered with the Hub Network.

Requirement: Control and monitor traffic flow between the internet, Azure resources, and the on-premises network.

Solution: Deploy an Azure Firewall in the Hub Network.

Function: Centralizes traffic filtering and monitoring, ensuring that only authorized traffic can pass between the spokes and to/from the on-premises network.

Requirement: Handle incoming web traffic efficiently and provide SSL termination.

Solution: Use an Azure Application Gateway in the front-end spoke.

Function: Manages and distributes incoming user traffic to the web servers in the front-end tier, providing SSL offloading and application-level routing.

Requirement: Enforce granular security controls for each application tier.

Solution: Implement Network Security Groups (NSGs).

Function: Apply security rules at the subnet and NIC level within each spoke network, restricting traffic between VMs in different tiers according to the application’s needs.

Requirement: Ensure high availability and load balancing for the web and application layers.

Solution: Deploy Azure Load Balancers.

External Load Balancer: Distributes incoming traffic to the front-end VMs.

Internal Load Balancer: Balances traffic within the application and database tiers, ensuring even distribution and high availability.

Requirement: Securely connect Azure resources with the on-premises data center for hybrid operations.

Solution: Establish a Site-to-Site VPN.

Function: Creates a secure tunnel between the on-premises data center and the Azure Hub Network, enabling secure data exchange and resource access.

Outcome:

By implementing this architecture, Contoso Ltd. achieves a highly secure, scalable, and resilient environment for their e-commerce platform. The Hub-and-Spoke architecture ensures network segmentation and security, while Azure Firewall, NSGs, and the VPN connection provide robust protection and secure connectivity. The use of Application Gateway and Load Balancers ensures that the application can handle variable traffic loads, providing a seamless experience for users even during peak times.

**Setup Step by step**

Here's a step-by-step guide to implementing the scenario described for deploying a secure multi-tier web application on Azure.

### \*\*Prerequisites:\*\*

1. \*\*Azure Subscription\*\*: Ensure you have an active Azure subscription.

2. \*\*Azure CLI/PowerShell\*\*: Install Azure CLI or Azure PowerShell if you're using scripts.

3. \*\*Access to On-Premises Environment\*\*: Ensure you have access to configure your on-premises network if you plan to set up the Site-to-Site VPN.

### \*\*Step 1: Set Up Hub-and-Spoke Network Architecture\*\*

1. \*\*Create the Hub Virtual Network\*\*:

- \*\*Go to the Azure portal\*\*.

- Navigate to \*\*Virtual networks\*\* and click \*\*Create\*\*.

- Configure the Hub VNet with a suitable address space (e.g., `10.0.0.0/16`).

- Create subnets within the Hub VNet:

- \*\*GatewaySubnet\*\*: For the VPN Gateway.

- \*\*AzureFirewallSubnet\*\*: For the Azure Firewall.

- \*\*Additional subnets\*\* as needed.

2. \*\*Create Spoke Virtual Networks\*\*:

- Create separate VNets for each tier (Front-End, Application, Database) with their own address spaces (e.g., `10.1.0.0/16`, `10.2.0.0/16`, `10.3.0.0/16`).

- No need to create subnets at this point; they will be created later when deploying VMs.

3. \*\*Peer the Spoke VNets with the Hub VNet\*\*:

- Navigate to each Spoke VNet.

- Under \*\*Settings\*\*, select \*\*Peerings\*\* and create a new peering.

- Peer the Spoke VNet with the Hub VNet, and make sure to allow traffic between them.

### \*\*Step 2: Deploy Azure Firewall in the Hub Network\*\*

1. \*\*Create the Azure Firewall\*\*:

- Go to the Azure portal and navigate to \*\*Firewalls\*\*.

- Click \*\*Create\*\* and select the Hub VNet.

- Deploy the firewall into the \*\*AzureFirewallSubnet\*\* you created in the Hub VNet.

2. \*\*Configure Firewall Rules\*\*:

- Add network rules to allow or deny traffic between the Hub and Spoke VNets.

- Optionally, configure application rules if needed for specific protocols or services.

### \*\*Step 3: Set Up the Application Gateway in the Front-End Spoke\*\*

1. \*\*Create a Front-End Subnet in the Front-End Spoke\*\*:

- Go to the Front-End VNet and create a subnet (e.g., `FrontEndSubnet`).

2. \*\*Create the Application Gateway\*\*:

- Go to \*\*Application Gateways\*\* in the Azure portal and click \*\*Create\*\*.

- Choose the Front-End VNet and deploy the gateway into the `FrontEndSubnet`.

- Configure the backend pool, listener, and routing rules to direct traffic to the front-end VMs.

3. \*\*Configure SSL Termination (Optional)\*\*:

- If using SSL, upload the SSL certificate to the Application Gateway.

### \*\*Step 4: Deploy Virtual Machines in Each Tier\*\*

1. \*\*Create Subnets for Application and Database Tiers\*\*:

- Create subnets in the Application Spoke (`AppSubnet`) and Database Spoke (`DbSubnet`).

2. \*\*Deploy VMs\*\*:

- Go to \*\*Virtual Machines\*\* and create VMs in each subnet:

- \*\*Front-End VMs\*\* in `FrontEndSubnet`.

- \*\*Application VMs\*\* in `AppSubnet`.

- \*\*Database VMs\*\* in `DbSubnet`.

- Configure network interfaces to place VMs in their respective subnets.

### \*\*Step 5: Configure Network Security Groups (NSGs)\*\*

1. \*\*Create and Attach NSGs\*\*:

- Create an NSG for each subnet:

- \*\*FrontEndNSG\*\*: Attached to `FrontEndSubnet`.

- \*\*AppNSG\*\*: Attached to `AppSubnet`.

- \*\*DbNSG\*\*: Attached to `DbSubnet`.

- Define security rules to control traffic flow:

- Allow only necessary traffic between the tiers.

- Allow traffic from the Application Gateway to the Front-End VMs.

### \*\*Step 6: Set Up Load Balancers\*\*

1. \*\*Create an External Load Balancer\*\*:

- Create a load balancer for the Front-End VMs.

- Configure the frontend IP, backend pool, health probes, and load-balancing rules.

2. \*\*Create an Internal Load Balancer\*\*:

- For the Application and Database tiers, create internal load balancers.

- Configure similarly to the external load balancer, ensuring they are only accessible within the virtual network.

### \*\*Step 7: Set Up Site-to-Site VPN for On-Premises Connectivity\*\*

1. \*\*Create a VPN Gateway in the Hub Network\*\*:

- Go to \*\*Virtual Network Gateways\*\* and click \*\*Create\*\*.

- Select the Hub VNet and deploy the VPN gateway to the `GatewaySubnet`.

2. \*\*Configure the Local Network Gateway\*\*:

- Represent your on-premises network in Azure by configuring a Local Network Gateway.

- Provide the on-premises public IP address and address space.

3. \*\*Create the Site-to-Site VPN Connection\*\*:

- Create a connection between the Azure VPN Gateway and the Local Network Gateway.

- Use a shared key for the connection, which must be configured on both the Azure and on-premises VPN devices.

4. \*\*Configure On-Premises VPN Device\*\*:

- On the on-premises side, configure your VPN device (router/firewall) to establish the connection with Azure.

### \*\*Step 8: Monitor and Manage the Deployment\*\*

1. \*\*Enable Monitoring\*\*:

- Use Azure Monitor and Log Analytics to monitor network traffic, VM performance, and application health.

- Set up alerts to notify you of any potential issues.

2. \*\*Use Azure Security Center\*\*:

- Regularly review recommendations in Azure Security Center to ensure compliance and optimize security.

3. \*\*Test Connectivity and Performance\*\*:

- Test the connectivity between the on-premises network and Azure.

- Ensure that the application tiers are communicating correctly and that load balancers are distributing traffic as expected.

### \*\*Step 9: Optimize and Scale\*\*

1. \*\*Auto-Scaling\*\*:

- Configure auto-scaling rules for the VMs in the Front-End tier using Virtual Machine Scale Sets.

- Adjust rules based on load and performance metrics.

2. \*\*Cost Management\*\*:

- Use Azure Cost Management to track and optimize costs.

- Review and adjust resource allocation as necessary.