TechSolutions™

AZ-700_Designing and Implementing Microsoft Azure Networking Solutions

RATHEESH KUMAR

Cloud & DevOps Expert with **14+ Years of Experience** | Founder, TechSolutions | Kerala

+91 94463 30906

www.ratheeshtech.com

ratheesh@ ratheeshtech.com

Skills at a Glance

- Design and implement core networking infrastructure (20–25%)
- Design, implement, and manage connectivity services (20–25%)
- Design and implement application delivery services (20–25%)
- Design and implement private access to Azure services (5–10%)
- Secure network connectivity to Azure resources (15–20%)

DESIGN AND IMPLEMENT CORE NETWORKING INFRASTRUCTURE (20–25%)

Design and Implement Ip Addressing for Azure Resources

- Plan and implement network segmentation and address spaces.
- Create a virtual network (VNet)
- Plan and configure subnetting for services, including VNet gateways, private endpoints, firewalls, application gateways, VNet-integrated platform services, and Azure Bastion
- Plan and configure subnet delegation.
- Create a prefix for public IP addresses.
- Choose when to use a public IP address prefix.
- Plan and implement a custom public IP address prefix (bring your own IP)
- Create a new public IP address.
- Associate public IP addresses to resources.

Design And Implement Name Resolution

- Design name resolution inside a VNet
- Configure DNS settings for a VNet
- Design public DNS zones.
- Design private DNS zones.
- Configure a public or private DNS zone.
- Link a private DNS zone to a VNet
- Design and implement DNS private resolver.

Design and Implement VNet Connectivity and Routing

- Design service chaining, including gateway transit.
- Design virtual private network (VPN) connectivity between VNets.
- Implement VNet peering.
- Associate a route table with a subnet.
- Configure forced tunneling.
- Diagnose and resolve routing issues.
- Design and implement Azure Route Server
- Identify appropriate use cases for a network address translation.
- (NAT) gateway in the virtual network
- Implement a NAT gateway.

Monitor Networks

- Configure monitoring, network diagnostics, and logs in Azure Network Watcher
- Monitor and repair network health by using Azure Network Watcher
- Activate and monitor distributed denial-of-service (DDoS) protection
- Activate and monitor Microsoft Defender for DNS

DESIGN, IMPLEMENT, AND MANAGE CONNECTIVITY SERVICES (20–25%) Design, Implement, And Manage A Site-To-Site VPN Connection

- Design a site-to-site VPN connection, including for high availability.
- Select an appropriate VNet gateway stock-keeping unit (SKU) for site-to-site VPN requirements.
- Implement a site-to-site VPN connection.
- Identify when to use a policy-based VPN versus a route-based connection.

Design, Implement, And Manage A Point-To-Site Vpn Connection

- Select an appropriate virtual network gateway SKU for point-to-site VPN requirements.
- Select and configure a tunnel type.
- Select an appropriate authentication method.
- Implement a VPN client configuration file.
- Diagnose and resolve client-side and authentication issues.
- Specify Azure requirements for Always On authentication.
- Specify Azure requirements for Azure Network Adapter

Design, Implement, And Manage Azure EXPRESSROUTE

- Select an ExpressRoute connectivity model.
- Select an appropriate ExpressRoute SKU and tier.
- Design and implement ExpressRoute to meet requirements, including cross-region connectivity, redundancy, and disaster recovery ,
- Design and implement ExpressRoute options, including Global Reach, FastPath, and ExpressRoute Direct
- Choose between private peering only, Microsoft peering only, or both.
- Configure private peering.
- Configure Microsoft peering.
- Create and configure an ExpressRoute gateway.
- Connect a virtual network to an ExpressRoute circuit.
- Recommend a route advertisement configuration.
- Configure encryption over ExpressRoute.
- Implement Bidirectional Forwarding Detection
- Diagnose and resolve ExpressRoute connection issues.

DESIGN AND IMPLEMENT APPLICATION DELIVERY SERVICES (20–25%)

Design And Implement an Azure Load Balancer

- Map requirements to features and capabilities of Azure Load Balancer.
- Identify appropriate use cases for Azure Load Balancer
- Choose an Azure Load Balancer SKU and tier.
- Choose between public and internal.
- Choose between regional and global.
- Create and configure an Azure Load Balancer
- Implement a load balancing rule.
- Create and configure inbound NAT rules.
- Create and configure explicit outbound rules, including source network address translation (SNAT).

Design And Implement Azure Application Gateway

- Map requirements to features and capabilities of Azure Application Gateway
- Identify appropriate use cases for Azure Application Gateway
- Choose between manual and auto scale.
- Create a back-end pool.
- Configure health probes.
- Configure listeners.
- Configure routing rules.
- Configure HTTP settings.
- Configure Transport Layer Security (TLS)
- Configure rewrite sets.

Design And Implement Azure Front Door

- Map requirements to features and capabilities of Azure Front Door
- Identify appropriate use cases for Azure Front Door
- Choose an appropriate tier.
- Configure an Azure Front Door, including routing, origins, and endpoints
- Configure SSL termination and end-to-end SSL encryption.
- Configure caching.
- Configure traffic acceleration.
- Implement rules, URL rewrite, and URL redirect.
- Secure an origin by using Azure Private Link in Azure Front Door

Design And Implement Azure Traffic Manager

- Identify appropriate use cases for Azure Traffic Manager
- Configure a routing method.
- Configure endpoints.

DESIGN AND IMPLEMENT PRIVATE ACCESS TO AZURE SERVICES (5–10%)

Design and Implement Azure Private Link Service and Azure Private Endpoints

- Plan private endpoints.
- Create private endpoints.
- Configure access to private endpoints.
- Create a Private Link service.
- Integrate Private Link and Private Endpoint with DNS
- Integrate a Private Link service with on-premises clients.

Design And Implement Service Endpoints

- Choose when to use a service endpoint.
- Create service endpoints.
- Configure service endpoint policies.
- Configure access to service endpoints.

SECURE NETWORK CONNECTIVITY TO AZURE

Resources (15–20%) Implement and Manage Network Security Groups

- Create a network security group (NSG)
- Associate a NSG to a resource.
- Create an application security group (ASG)
- Associate an ASG to a network interface card (NIC)
- Create and configure NSG rules.
- Interpret NSG flow logs.
- Validate NSG flow rules.
- Verify IP flow.
- Configure an NSG for remote server administration, including Azure.
- Bastion

Design And Implement Azure Firewall and Azure Firewall Manager

- Map requirements to features and capabilities of Azure Firewall
- Select an appropriate Azure Firewall SKU
- Design an Azure Firewall deployment.
- Create and implement an Azure Firewall deployment.
- Configure Azure Firewall rules.
- Create and implement Azure Firewall Manager policies.
- Create a secure hub by deploying Azure Firewall inside an Azure Virtual WAN hub.

Design And Implement a Web Application Firewall (Waf) Deployment

- Map requirements to features and capabilities of WAF.
- Design a WAF deployment.
- Configure detection or prevention mode.
- Configure rule sets for WAF on Azure Front Door
- Configure rule sets for WAF on Application Gateway
- Implement a WAF policy.
- Associate a WAF policy.