Exam AZ-700: Designing and Implementing Microsoft Azure Networking Solutions – Skills Measured

This exam will be updated on November 23, 2021. Following the current exam guide, we have included a version of the exam guide with Track Changes set to "On," showing the changes that will be made to the exam on that date.

NOTE: Passing score: 700. Learn more about exam scores here.

Audience Profile

Candidates for this exam should have subject matter expertise in planning, implementing, and maintaining Azure networking solutions, including hybrid networking, connectivity, routing, security, and private access to Azure services.

Responsibilities for the Azure Network Engineer include recommending, planning, and implementing Azure networking solutions. Professionals in this role manage the solution for performance, resiliency, scale, and security. They deploy networking solutions by using the Azure Portal and other methods, including PowerShell, Azure Command-Line Interface (CLI), and Azure Resource Manager templates (ARM templates).

The Azure Network Engineer works with solution architects, cloud administrators, security engineers, application developers, and DevOps engineers to deliver Azure solutions.

Candidates for this exam should have expert Azure administration skills, in addition to extensive experience and knowledge of networking, hybrid connections, and network security.

Skills Measured

NOTE: The bullets that follow each of the skills measured are intended to illustrate how we're assessing that skill. This list is *not* definitive or exhaustive.

NOTE: Most questions cover features that are General Availability (GA). The exam may contain questions on Preview features, if those features are commonly used.

Design, Implement, and Manage Hybrid Networking (10–15%)

Design, implement, and manage a site-to-site VPN connection

- design a site-to-site VPN connection for high availability
- select an appropriate virtual network (VNet) gateway SKU
- identify when to use policy-based VPN versus route-based VPN
- create and configure a local network gateway
- create and configure an IPsec/IKE policy
- create and configure a virtual network gateway

- diagnose and resolve VPN gateway connectivity issues

Design, implement, and manage a point-to-site VPN connection

- select an appropriate virtual network gateway SKU
- plan and configure RADIUS authentication
- plan and configure certificate-based authentication
- plan and configure OpenVPN authentication
- plan and configure Azure Active Directory (Azure AD) authentication
- implement a VPN client configuration file
- diagnose and resolve client-side and authentication issues

Design, implement, and manage Azure ExpressRoute

- choose between provider and direct model (ExpressRoute Direct)
- design and implement Azure cross-region connectivity between multiple ExpressRoute locations
- select an appropriate ExpressRoute SKU and tier
- design and implement ExpressRoute Global Reach
- design and implement ExpressRoute FastPath
- 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 Core Networking Infrastructure (20–25%)

Design and implement private IP addressing for VNets

- create a VNet
- plan and configure subnetting for services, including VNet gateways, private endpoints, firewalls, application gateways, and VNet-integrated platform services
- plan and configure subnet delegation

Design and implement name resolution

- design public DNS zones
- design private DNS zones

- design name resolution inside a VNet
- configure a public or private DNS zone
- link a private DNS zone to a VNet

Design and implement cross-VNet connectivity

- design service chaining, including gateway transit
- design VPN connectivity between VNets
- implement VNet peering

Design and implement an Azure Virtual WAN architecture

- design an Azure Virtual WAN architecture, including selecting SKUs and services
- connect a VNet gateway to Azure Virtual WAN
- create a hub in Virtual WAN
- create a network virtual appliance (NVA) in a virtual hub
- configure virtual hub routing
- create a connection unit

Design and Implement Routing (25–30%)

Design, implement, and manage VNet routing

- design and implement user-defined routes (UDRs)
- associate a route table with a subnet
- configure forced tunneling
- diagnose and resolve routing issues

Design and implement an Azure Load Balancer

- choose an Azure Load Balancer SKU (Basic versus Standard)
- choose between public and internal
- create and configure an Azure Load Balancer (including cross-region)
- implement a load balancing rule
- create and configure inbound NAT rules
- create explicit outbound rules for a load balancer

Design and implement Azure Application Gateway

- recommend Azure Application Gateway deployment options
- choose between manual and autoscale
- create a back-end pool
- configure health probes

- configure listeners
- configure routing rules
- configure HTTP settings
- configure Transport Layer Security (TLS)
- configure rewrite policies

Implement Azure Front Door

- choose an Azure Front Door SKU
- configure health probes, including customization of HTTP response codes
- configure SSL termination and end-to-end SSL encryption
- configure multisite listeners
- configure back-end targets
- configure routing rules, including redirection rules

Implement an Azure Traffic Manager profile

- configure a routing method (mode)
- configure endpoints
- create HTTP settings

Design and implement an Azure Virtual Network NAT

- choose when to use a Virtual Network NAT
- allocate public IP or public IP prefixes for a NAT gateway
- associate a Virtual Network NAT with a subnet

Secure and Monitor Networks (15–20%)

Design, implement, and manage an Azure Firewall deployment

- 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
- integrate an Azure Virtual WAN hub with a third-party NVA

Implement and manage network security groups (NSGs)

- create an NSG
- associate an NSG to a resource
- create an application security group (ASG)

- associate an ASG to a NIC
- create and configure NSG rules
- interpret NSG flow logs
- validate NSG flow rules
- verify IP flow

Implement a Web Application Firewall (WAF) deployment

- configure detection or prevention mode
- configure rule sets for Azure Front Door, including Microsoft managed and user defined
- configure rule sets for Application Gateway, including Microsoft managed and user defined
- implement a WAF policy
- associate a WAF policy

Monitor networks

- configure network health alerts and logging by using Azure Monitor
- create and configure a Connection Monitor instance
- configure and use Traffic Analytics
- configure NSG flow logs
- enable and configure diagnostic logging
- configure Azure Network Watcher

Design and Implement Private Access to Azure Services (10–15%)

Design and implement Azure Private Link service and Azure Private Endpoint

- create a Private Link service
- plan private endpoints
- create private endpoints
- configure access to private endpoints
- integrate Private Link with DNS
- integrate a Private Link service with on-premises clients

Design and implement service endpoints

- create service endpoints
- configure service endpoint policies
- configure service tags
- configure access to service endpoints

Configure VNet integration for dedicated platform as a service (PaaS) services

- configure App Service for regional VNet integration
- configure Azure Kubernetes Service (AKS) for regional VNet integration
- configure clients to access App Service Environment

The exam guide below shows the changes that will be implemented on November 23, 2021.

Audience Profile

Candidates for this exam should have subject matter expertise in planning, implementing, and maintaining Azure networking solutions, including hybrid networking, connectivity, routing, security, and private access to Azure services.

Responsibilities for the Azure Network Engineer include recommending, planning, and implementing Azure networking solutions. Professionals in this role manage the solution for performance, resiliency, scale, and security. They deploy networking solutions by using the Azure Portal and other methods, including PowerShell, Azure Command-Line Interface (CLI), and Azure Resource Manager templates (ARM templates).

The Azure Network Engineer works with solution architects, cloud administrators, security engineers, application developers, and DevOps engineers to deliver Azure solutions.

Candidates for this exam should have expert Azure administration skills, in addition to extensive experience and knowledge of networking, hybrid connections, and network security.

Skills Measured

NOTE: The bullets that follow each of the skills measured are intended to illustrate how we're assessing that skill. This list is *not* definitive or exhaustive.

NOTE: Most questions cover features that are General Availability (GA). The exam may contain questions on Preview features, if those features are commonly used.

Design, Implement, and Manage Hybrid Networking (10–15%)

Design, implement, and manage a site-to-site VPN connection

- design a site-to-site VPN connection for high availability
- select an appropriate virtual network (VNet) gateway SKU
- identify when to use policy-based VPN versus route-based VPN
- create and configure a local network gateway
- create and configure an IPsec/IKE policy
- create and configure a virtual network gateway
- diagnose and resolve ~~VPN~~ virtual network gateway connectivity issues

Design, implement, and manage a point-to-site VPN connection

- select an appropriate virtual network gateway SKU
- plan and configure RADIUS authentication
- plan and configure certificate-based authentication
- plan and configure OpenVPN authentication
- plan and configure Azure Active Directory (Azure AD) authentication
- implement a VPN client configuration file
- diagnose and resolve client-side and authentication issues

Design, implement, and manage Azure ExpressRoute

- choose between provider and direct model (ExpressRoute Direct)
- design and implement Azure cross-region connectivity between multiple ExpressRoute locations
- select an appropriate ExpressRoute SKU and tier
- design and implement ExpressRoute Global Reach
- design and implement ExpressRoute FastPath
- 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 Core Networking Infrastructure (20–25%)

Design and implement private IP addressing for VNets

- create a VNet
- plan and configure subnetting for services, including VNet gateways, private endpoints, firewalls, application gateways, and VNet-integrated platform services
- plan and configure subnet delegation
- plan and configure subnetting for Azure Route Server

Design and implement name resolution

- design public DNS zones
- design private DNS zones
- design name resolution inside a VNet
- configure a public or private DNS zone
- link a private DNS zone to a VNet

Design and implement cross-VNet connectivity

- design service chaining, including gateway transit
- design VPN connectivity between VNets
- implement VNet peering

Design and implement an Azure Virtual WAN architecture

- design an Azure Virtual WAN architecture, including selecting ~~SKUs~~ types and services
- connect a VNet gateway to Azure Virtual WAN
- create a hub in Virtual WAN
- create a network virtual appliance (NVA) in a virtual hub
- configure virtual hub routing
- create a connection unit

Design and Implement Routing (25–30%)

Design, implement, and manage VNet routing

- design and implement user-defined routes (UDRs)
- associate a route table with a subnet
- configure forced tunneling
- diagnose and resolve routing issues
- design and implement Azure Route Server

Design and implement an Azure Load Balancer

- choose an Azure Load Balancer SKU (Basic versus Standard)
- choose between public and internal
- create and configure an Azure Load Balancer (including cross-region)
- implement a load balancing rule
- create and configure inbound NAT rules
- create explicit outbound rules for a load balancer

Design and implement Azure Application Gateway

- recommend Azure Application Gateway deployment options
- choose between manual and autoscale
- create a back-end pool
- configure health probes
- configure listeners
- configure routing rules
- configure HTTP settings

- configure Transport Layer Security (TLS)
- configure rewrite ~~policies~~sets

Implement Azure Front Door

- choose an Azure Front Door SKU
- configure health probes, including customization of HTTP response codes
- configure SSL termination and end-to-end SSL encryption
- configure multisite listeners
- configure back-end targets
- configure routing rules, including redirection rules

Implement an Azure Traffic Manager profile

- configure a routing method (mode)
- configure endpoints
- create HTTP settings

Design and implement an Azure Virtual Network NAT

- choose when to use a Virtual Network NAT
- allocate public IP or public IP prefixes for a NAT gateway
- associate a Virtual Network NAT with a subnet

Secure and Monitor Networks (15–20%)

Design, implement, and manage an Azure Firewall deployment

- 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
- integrate an Azure Virtual WAN hub with a third-party NVA

Implement and manage network security groups (NSGs)

- create an NSG
- associate an NSG to a resource
- create an application security group (ASG)
- associate an ASG to a NIC
- create and configure NSG rules
- interpret NSG flow logs

- validate NSG flow rules
- verify IP flow

Implement a Web Application Firewall (WAF) deployment

- configure detection or prevention mode
- configure rule sets for Azure Front Door, including Microsoft managed and user defined
- configure rule sets for Application Gateway, including Microsoft managed and user defined
- implement a WAF policy
- associate a WAF policy

Monitor networks

- configure network health alerts and logging by using Azure Monitor
- create and configure a Connection Monitor instance
- configure and use Traffic Analytics
- configure NSG flow logs
- enable and configure diagnostic logging
- configure Azure Network Watcher

Design and Implement Private Access to Azure Services (10–15%)

Design and implement Azure Private Link service and Azure Private Endpoint

- create a Private Link service
- plan private endpoints
- create private endpoints
- configure access to private endpoints
- integrate Private Link with DNS
- integrate a Private Link service with on-premises clients

Design and implement service endpoints

- create service endpoints
- configure service endpoint policies
- configure service tags
- configure access to service endpoints

Configure VNet integration for dedicated platform as a service (PaaS) services

- configure App Service for regional VNet integration
- configure Azure Kubernetes Service (AKS) for regional VNet integration

- configure clients to access App Service Environment