AZ-700 Exam Prep

Mahdi Sheikhi

2025/01/01

CONTENTS

01 AZ-700 Overview

02 Core Networking

03 Hybrid Connectivity

04 App Delivery

05 Security & Monitoring

06 Study Plan

01

AZ-700 Overview

What AZ-700 Tests

01

Role-based scenarios

Every question places you in the shoes of an Azure network engineer; expect multi-subscription, multi-region designs where you must balance security, performance, and cost while explaining your choices to stakeholders.

Hands-on configuration depth

You must know portal, CLI, ARM, and Terraform snippets; the exam tests whether you can translate architectural diagrams into precise resource settings like custom BGP communities or path-based routing rules.

02

Exam Blueprint 2025

Question formats

50–60 items in 120 min: single-best-answer, multi-select, drag-and-drop sequence, hot-area diagrams, and two case studies with five questions each; no partial credit, so validate every selection.

Domain weights

Core infra 20–25 %, hybrid connectivity 20–25 %, application delivery 20–25 %, private access 5–10 %, security & monitoring 15–20 %; target your weak domains above 70 % in practice tests.

Passing mechanics

Scaled score 700/1000; unanswered items count as wrong, flag and review in final 15 min; exam rolls new questions weekly, so brain-dumps expire fast—focus on concepts.

02

Core Networking

Designing VNets & Subnets

Address-space calculus

Start with 10.0.0.0/8 or 172.16.0.0/12, reserve at least 50 % for future regions; never overlap with on-premises RFC 1918 ranges used in ExpressRoute or VPN to avoid black-holing traffic.

Subnet sizing formula

Plan for 2^(32-n) – 5 Azure-reserved IPs; a /24 yields 251 usable, but auto-scale sets may need /23; delegate separate subnets for Azure Firewall, Bastion, and Gateway to simplify UDRs.

Segmentation strategy

Use NSGs at subnet level, not NIC, to enforce zero-trust micro-perimeters; pair with Application Security Groups for workload-centric rules instead of IP addresses that change during blue-green deployments.

Cross-subscription peering

Enable global VNet peering with ‘Allow gateway transit’ and ‘Use remote gateway’ flags to share ExpressRoute or VPN gateways across subscriptions while keeping RBAC boundaries intact.

Routing Fundamentals

System vs user routes

System routes prioritize VNet, VirtualNetworkServiceEndpoint, then Internet; override with UDR having smaller prefix length or higher BGP weight; remember that 0.0.0.0/0 forced tunnel drops Azure LB health probes unless you add /32 exceptions.

Avoid asymmetric paths

When forcing traffic through an NVA, ensure return traffic follows the same path by advertising the subnet prefix via BGP from the NVA; otherwise stateful firewalls will drop flows, breaking SQL or SMB sessions.

03

Hybrid Connectivity

VPN & ExpressRoute Design

VPN SKU selection

VpnGw2 supports 1 Gbps and 30 tunnels, VpnGw5 hits 10 Gbps; activate Active-Active mode with BGP for sub-second failover; use policy-based only for legacy on-premises devices that lack route-based support.

ExpressRoute circuits

Order 100 Mbps to 100 Gbps with Premium for global reach; dual 100 Gbps circuits in different peering locations give 99.95 % SLA; use private peering for IaaS, Microsoft peering for Office 365 with route filters to limit prefixes.

Redundancy patterns

Combine VPN as a secure failover path for ExpressRoute via ‘Site-to-site VPN over ExpressRoute’; configure BGP communities 65520:100 to prefer ExpressRoute, 65520:200 to prefer VPN, ensuring automatic convergence.

Virtual WAN Architecture

Secured virtual hubs

Deploy Azure Firewall Manager into the hub, create hub routing tables with ‘None’ next hop to steer traffic through the firewall; propagate VPN, ExpressRoute, and VNet connections into the same table to achieve transitive routing without manual peerings.

04

App Delivery

Load Balancer & Gateway

Standard LB tricks

Use HA ports rule for NVA clusters, enable TCP reset for graceful failover, and tie to availability zones with zone-redundant frontend IP; remember Standard LB requires NSG allow for AzureLoadBalancer service tag on the subnet.

Application Gateway v2

Deploy with autoscaling min 0 instances for cost, enable HTTP-to-HTTPS redirect at the listener, and use WAF in prevention mode with OWASP 3.2 rules; for multi-tenant apps, leverage host-name routing to avoid dozens of public IPs.

Health-probe tuning

Set interval 5 s, timeout 30 s, unhealthy threshold 3 for fast detection; return 200 OK on /health that checks DB connectivity; avoid redirects or authentication that can trigger false positives and drain the backend pool.

Global Traffic Distribution

Front Door operates at Edge PoPs with anycast IPs, provides SSL offload, caching, and WAF; Traffic Manager is DNS-level with 30–300 s TTL, cheaper but no Layer-7 features; choose Front Door for sub-second failover, Traffic Manager for non-HTTP workloads.

Front Door vs Traffic Manager

Create Front Door origin groups with health probes every 5 s; use ‘Latency sensitivity’ of 30 ms to steer users to the nearest region; combine with Azure CDN from Microsoft tier to cache static content and reduce first-byte latency below 100 ms globally.

Latency-based routing

05

Security & Monitoring

Network Security Hardening

01

Zero-trust segmentation

Replace flat RFC 1918 allow-rules with ASG-based policies; require MFA for RDP via Azure Bastion; enforce JIT access on NSGs using Defender for Cloud so ports open only for approved IPs and time windows.

02

Azure Firewall policies

Adopt hierarchical policies with global DNAT rules at the root, regional network rules in child policies; enable IDPS in alert & deny mode; use Threat Intelligence allowlists to permit Office 365 IPs while blocking known C2 servers.

03

Private endpoints only

Disable public endpoints on storage and SQL, create private endpoints in dedicated subnet with 'PrivateEndpointNetworkPolicies' enabled; combine with service endpoint policies to prevent data exfiltration to unauthorized storage accounts.

04

DDoS Protection Standard

Enable on the VNet containing public IPs; configure alert thresholds for SYN, UDP, and volumetric floods; integrate with Sentinel playbook to auto-scale WAF rules and notify SOC via Teams when scrubbing starts.

Troubleshooting Toolkit

Network Watcher workflows

Run IP flow verify to confirm NSG denies, then effective routes to spot rogue UDRs; initiate packet capture on the NIC with 1 MB circular buffer, filter on TCP 443, and export to Storage for Wireshark analysis to prove SSL handshake failures.

KQL log analytics

Query AzureFirewallNetworkRule log to count drops by SrcIP, join with SigninLogs to map to user identity; create a timechart showing latency spikes in Front Door access logs correlating with CPU bursts in VMSS to pinpoint noisy neighbors.

06

Study Plan

30-Day Sprint Plan

Daily micro-tasks

Block 90 min before work: read one Learn module, immediately lab it with $200 sandbox; evenings do 15 practice questions, document wrong answers in OneNote; weekly reset lab subscription to avoid cost overruns and reinforce muscle memory.

Resources & Retake Tips

01

Curated content stack

Start with Microsoft Learn ‘Design and implement core networking infrastructure’ path; supplement with John Savill’s 3-hour AZ-700 cram video at 1.5× speed; finish with Whizlabs 220-question bank—aim for 85 % consistently before booking.

02

Lab every exam objective

Deploy each service twice—once via portal for UI familiarity, once via CLI for speed; store reusable snippets in GitHub Gists; break things intentionally (delete a route, stop BGP) to see how errors surface in portal and logs.

03

Retake strategy

If you score <700, screenshot the skills breakdown; focus labs on domains below 60 %; schedule free retake within 24 hours while memory is fresh; sleep 7 hours—cognitive load of scenario questions drops 20 % after a full night.

THANK YOU

Mahdi Sheikhi

2025/01/01