AZ-700 Azure Networking Mastery Deck

Mahdi Sheikhi

2025/08/05

Contents

01 | Exam Blueprint & Strategy

02 | Hybrid Connectivity Deep Dive

03 | Core Network Fabric

04 | Private Access & DNS

05 | Security & Monitoring

Contents

01
Traffic Distribution & Delivery

02
Operations & Exam Drill

01

Exam Blueprint & Strategy

AZ-700 Domain Breakdown & Win Path

01

Exam Domains Overview

The AZ-700 exam is divided into five key domains, each with specific weightings. Understanding these domains is crucial for targeted preparation. The exam consists of 40-60 questions, with a passing score of 700. Focus on high-yield tasks like sketching hybrid topologies and verifying GatewaySubnet configurations.

02

Key Skills Measured

Candidates must master hybrid networking, core infrastructure design, private access and name resolution, network security, and traffic distribution. Each skill area requires a blend of theoretical knowledge and practical application, ensuring comprehensive readiness for real-world scenarios.

03

Time Management Tips

Allocate 60 seconds per question to manage time effectively. Prioritize questions you are confident about and flag uncertain ones for later review. This strategy ensures you cover all questions without rushing, maximizing your chances of success.

Question Traps & Cognitive Strategy

01

Common Exam Traps

Be wary of common distractors such as GatewaySubnet naming errors, incorrect health probe methods, and misconceptions about Basic DDoS auto-mitigation. TLS inspection is only available in the Premium tier of Azure Firewall. Understanding these nuances can save crucial points.

02

Elimination Flowchart

Use a structured approach to tackle questions: classify the scenario, identify the service tier, and validate redundancy options. This flowchart helps eliminate incorrect choices systematically, improving accuracy. Remember the 30-second flag-and-skip rule for complex questions.

02

Hybrid Connectivity Deep Dive

VPN Gateway Build Order & IKE Choices

Deployment Sequence

Deploy the /26 GatewaySubnet first, followed by the public IP, VPN Gateway, local network gateway, and connection object. This sequence ensures a seamless setup without configuration conflicts.

Authentication Methods

For Point-to-Site (P2S) connections, prioritize certificate authentication for security, followed by RADIUS and Azure AD. Each method has its use cases, but certificates offer the highest level of security.

IKE Protocol Options

Choose between route-based and policy-based VPNs, with IKEv1 and IKEv2 available. Custom traffic selectors allow fine-tuned control over encrypted traffic. Select the appropriate protocol based on your security and performance requirements.

VNet-to-VNet Connections

Ensure matching IKE versions for VNet-to-VNet connections to avoid compatibility issues. This detail is often overlooked but critical for maintaining stable hybrid connectivity.

ExpressRoute Peering & FastPath

01

Peering Types

Understand the roles of Private, Microsoft, and retired Public peering. Each type serves different connectivity needs, with Private peering being the most commonly used for secure, private connections.

FastPath Optimization

02

FastPath bypasses the Gateway for sub-millisecond latency, significantly improving performance. This feature is essential for latency-sensitive applications, ensuring optimal user experience.

03

ExpressRoute Direct & Global Reach

ExpressRoute Direct offers 10 Gbps minimum throughput, while Global Reach enables inter-region branch connectivity. These features enhance the robustness and reach of your hybrid network.

VPN vs ExpressRoute Decision Matrix

01

Service Comparison

Compare VPN and ExpressRoute based on bandwidth, SLA, cost, encryption, and setup time. VPN is quick and cost-effective, while ExpressRoute offers higher performance and reliability.

02

Hybrid Use Case

In hybrid scenarios, use ExpressRoute as the primary connection with VPN as a backup. This setup ensures high availability and failover capabilities, crucial for maintaining business continuity.

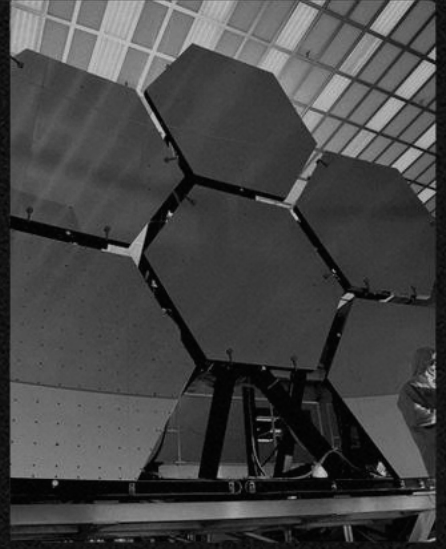
Azure Network Adapter & Windows Admin Center

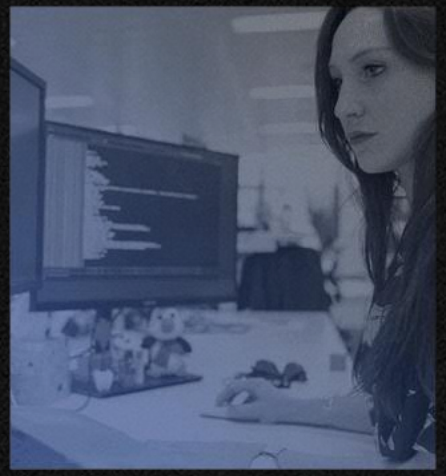
Simplified Connection

Azure Network Adapter offers a simplified S2S connection for single on-premises servers via Windows Admin Center. This method is ideal for quick setup without the need for complex on-premises appliances.

Requirements & Limitations

Ensure your environment meets the requirements, such as Windows Server 2019+ and Azure subscription owner rights. Note that this method is not suitable for multi-subnet on-premises networks.





03

Core Network Fabric

VNet CIDR Design & Address Exhaustion Guard

01

CIDR Planning

Plan your VNet CIDR blocks carefully to avoid address space exhaustion. Use RFC 1918 non-overlapping ranges across regions and subscriptions to ensure seamless connectivity.

02

Subnet Sizing

Allocate /16 per region and /24 per subnet, reserving the first four and last IP addresses. This strategy provides flexibility for future growth and avoids the need for re-addressing.

03

Hub-Spoke Topology

Implement a hub-spoke topology with a /26 GatewaySubnet, /24 shared services subnet, and /25 spokes. This design optimizes resource management and security.

VNet Peering Constraints & Global Reach

01

Peering Limitations

Be aware of VNet peering constraints, such as non-transitive routing, non-overlapping address spaces, and the requirement for VNets to be in the same Azure AD tenant.

Global Peering

Global peering allows cross-region connectivity but incurs costs based on ingress and egress traffic. Plan your peering strategy to balance performance and cost.

02

NAT Gateway vs Load Balancer Outbound SNAT

NAT Gateway Features

01

NAT Gateway dynamically allocates SNAT ports, supports TCP/UDP, and offers zonal redundancy. It scales to 64k ports per IP, making it suitable for large-scale outbound internet management.

Load Balancer SNAT

02

Load Balancer uses ephemeral ports for SNAT. While it offers similar functionality, NAT Gateway provides more scalable and flexible outbound connectivity options.

Cost & Scalability

03

Consider the cost per processed GB when using NAT Gateway. It is essential to balance scalability needs with cost implications for optimal network performance.

Azure Bastion & NSG Integration

01

Bastion Features

Azure Bastion provides secure RDP/SSH access over SSL without exposing public IPs on VMs. It integrates seamlessly with NSGs for enhanced security.

02

Deployment Requirements

Ensure the Bastion subnet is named AzureBastionSubnet and is /26 or larger. This configuration is crucial for proper functionality and security.

Route Server & BGP with NVA

01

Route Server Benefits

Route Server simplifies dynamic routing by automatically exchanging BGP routes between NVAs and Azure SDN. This eliminates the need for manual UDR maintenance.

02

Deployment Requirements

Deploy Route Server in a dedicated subnet /27 or larger. Use ASN 65515 for Azure and ensure support for eBGP multi-hop. Validated partner images ensure compatibility.

03

Memory Cue

Think of Route Server as the post office for NVAs, efficiently managing and distributing routing information to maintain network connectivity.

04

Private Access & DNS

DNS Private Resolver Architecture

Inbound & Outbound Endpoints

DNS Private Resolver features inbound endpoints for on-premises conditional forwarders and outbound endpoints for Azure VMs. It integrates seamlessly with private DNS zones.

Serverless Design

The resolver is serverless, eliminating the need for VM patching and management. Ensure it is deployed in the same VNet as the VMs requiring outbound resolution.

Private Endpoint & Private Link Service

01

Private Endpoint Features

Private Endpoints provide secure access to PaaS services using private IPs within the VNet. They disable public endpoints by policy, enhancing security.

Private Link Service

Service providers create Private Link Services behind Standard Load Balancers. Consumers can select these shared services for secure access.

02

03

NVA Inspection

For advanced security, use NVAs with hair-pinning capabilities to inspect traffic. This ensures compliance with organizational security policies.

Service Endpoint vs Private Endpoint Revisited

01

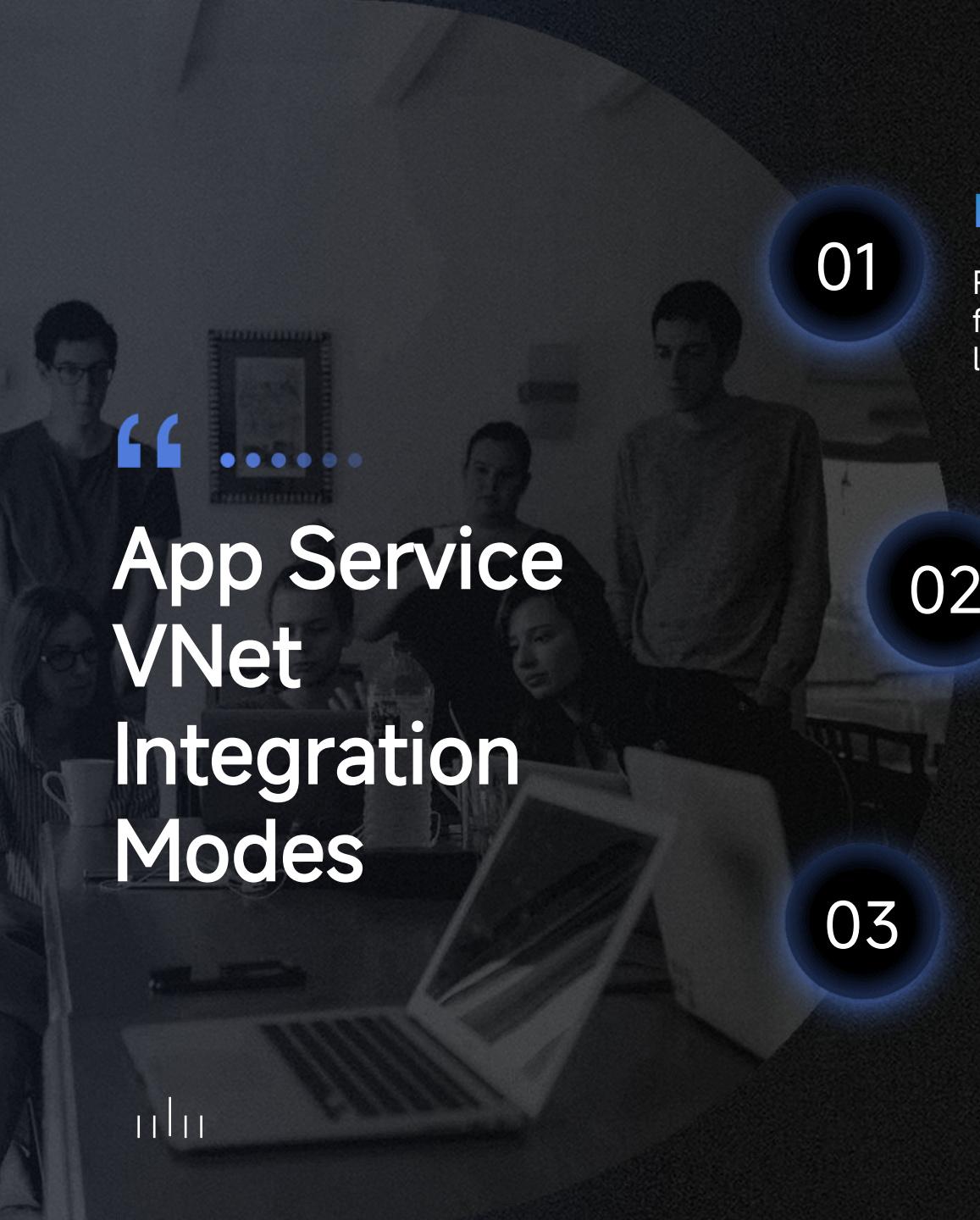
Traffic Path Comparison

Service Endpoints keep traffic on the Microsoft backbone but use public IPs, while Private Endpoints use private IPs within the VNet for enhanced security.

02

Use Case Guidance

Choose Service Endpoints for cost-effective solutions and Private Endpoints for secure on-premises access. Understand the trade-offs to make informed decisions.



App Service VNet Integration Modes

01

Regional Integration

Regional VNet integration is newer and faster, eliminating the need for a gateway. It is ideal for modern applications requiring low-latency connections.

02

Gateway-Required Integration

Legacy applications may require gateway mode, which has a 1.5 Gbps limit. Ensure subnet delegation and route table propagation for seamless connectivity.

03

Outbound IPs

Note that outbound IPs may still change unless using NAT Gateway. This consideration is crucial for applications relying on static IPs.

05

Security & Monitoring

Azure Firewall Rule Types & Priority

Rule Hierarchy

Azure Firewall rules follow a hierarchy: DNAT has the highest priority, followed by Network and Application rules. Lower numbers indicate higher priority.

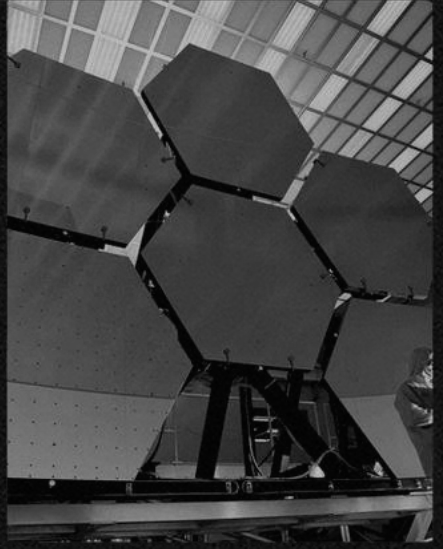
Threat Intelligence

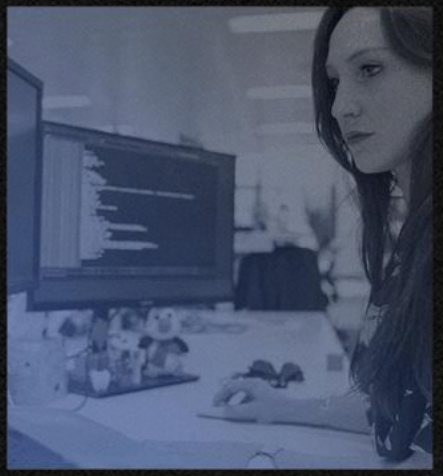
Threat Intelligence mode can be set to Alert or Deny. It provides real-time protection against known malicious IPs and domains, enhancing security.

Premium Features

Premium tier adds TLS inspection, IDPS signatures, and Web Categories. These features provide advanced security capabilities for critical environments.

NSG Flow Logs v2 & Traffic Analytics Setup





- ## Setup Prerequisites

  Enable NSG Flow Logs v2 with prerequisites such as NSG association, storage v2, Log Analytics workspace, and a minimum 10-minute retention period.

- ## Data Enrichment

  Flow Logs v2 provides enriched data including latency, geography, and threat intel. Use Kusto queries to analyze logs and identify malicious IPs.

DDoS Protection Plans & Cost Guardrails

DDoS Protection Tiers

Compare Basic (platform-native) and Standard (auto-mitigation, cost protection, telemetry) DDoS protection plans. Standard offers superior protection with a 60-second detection SLA.

Cost Management

Standard tier provides cost protection up to 100 Tbps. Link VNets to protection plans to ensure comprehensive coverage without unexpected costs.

06

Traffic Distribution & Delivery

Load Balancer SKUs & HA Ports

SKU Comparison

Compare Basic (retired) and Standard Load Balancer SKUs. Standard offers backend any zone, HA ports for all TCP/UDP, outbound rules, and a global SLA.

Health Probes

Standard Load Balancer supports various health probe types including TCP, HTTP, and HTTPS. Use HEAD requests for efficient health checks.

High Availability

HA ports are essential for NVAs in active-active configurations. Ensure proper setup to maintain high availability and avoid single points of failure.

Application Gateway Components & WAF

Key Components

Application Gateway includes listeners, rules, backend pools, health probes, and HTTP settings. These components work together to ensure efficient traffic distribution and application performance.

WAF Configuration

Configure WAF modes (Detection vs Prevention), OWASP 3.2 rules, and exclusion lists. Note that only software-validated SSL certificates are supported in GWv1.

Front Door Routing & Origin Health

Routing Methods

Front Door supports latency, priority, and weighted routing methods. Choose the appropriate method based on your application's requirements for optimal performance.

Origin Health Probes

Configure health probes using HEAD requests to ensure origin group health. This proactive monitoring helps maintain application availability and user experience.

Private Link Integration

Integrate Front Door with App Service via Private Endpoint for secure access. This setup ensures that traffic remains within the private network, enhancing security.

07

Operations & Exam Drill

Network Watcher Toolkit Essentials

Key Tools

Network Watcher includes Connection Monitor for VM-to-VM latency, Packet Capture for detailed traffic analysis, NSG diagnostics for rule hits, and next-hop verification.

Deployment Considerations

Note that one Network Watcher is automatically created per region. Packet Capture requires a storage account in the same region, ensuring data locality and compliance.

Scenario Matrix & Decision Flowchart

Scenario Analysis

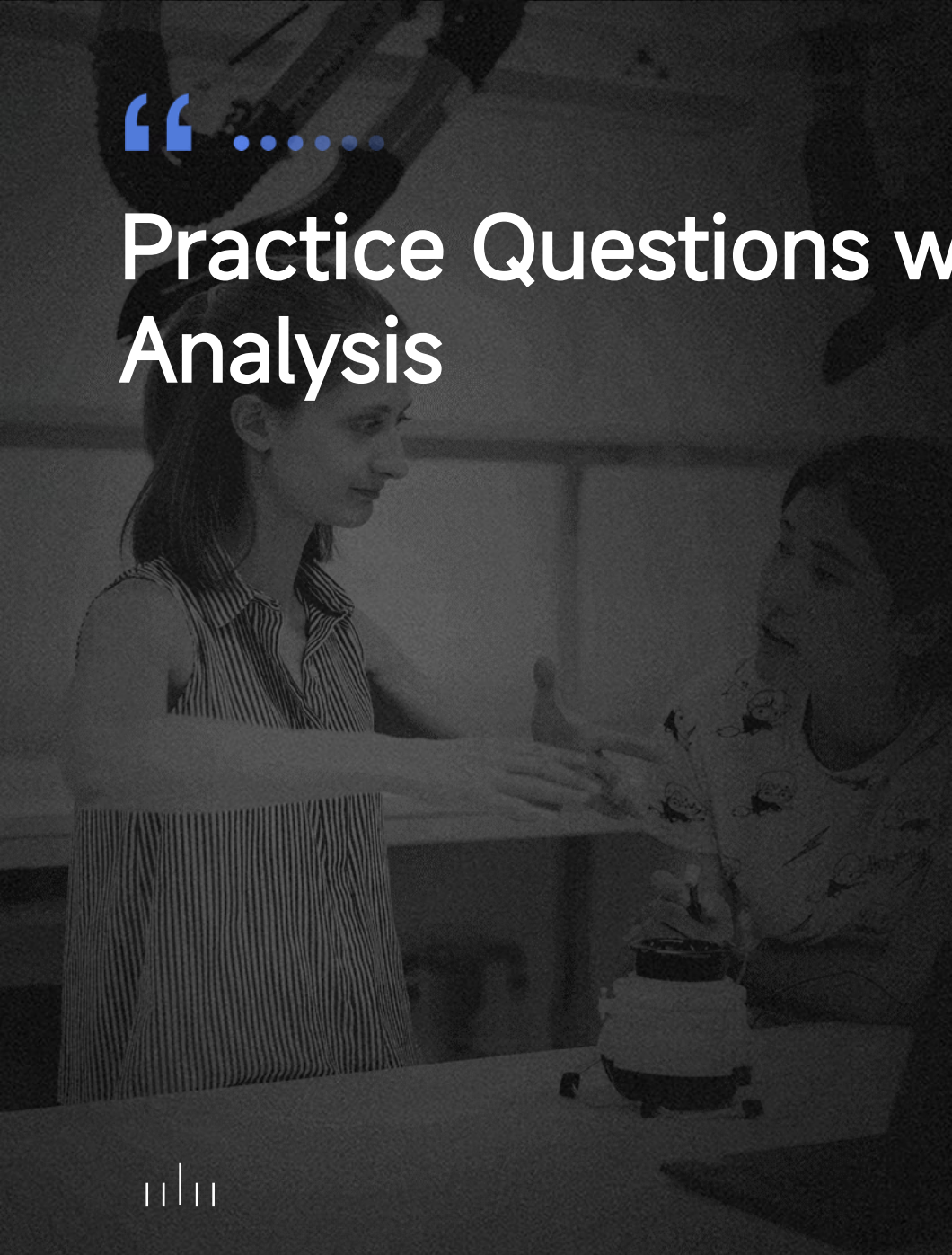
Review common exam scenarios such as on-premises to Azure SQL, global web app failover, NVAs with BGP, private SaaS access, and zero-trust RDP. Understand the unique challenges of each scenario.

Time Management

Adopt a write-skip-review timing strategy to manage exam time effectively. Allocate sufficient time for each section to ensure thorough analysis and accurate responses.

Decision Flowchart

Use a decision flowchart to systematically choose the right connectivity type, security service, routing configuration, and monitoring setup. This structured approach ensures comprehensive solutions.



Practice Questions with Gotcha Analysis

Question Examples

Sample questions cover GatewaySubnet size, ExpressRoute peering order, Application Gateway probe method, NSG flow log scope, and Front Door origin timeout. Each question includes detailed reasoning and common distractor analysis.

Time Management

Aim for an average of 90 seconds per question to ensure thorough analysis. Practice under timed conditions to build speed and accuracy, crucial for exam success.

Key Terms Recap & Memory Hooks

Core Terms

Define key terms such as VNet Peering, Private Link, NAT Gateway, Route Server, DNS Private Resolver, ExpressRoute, Azure Firewall, Bastion, Front Door, and GatewaySubnet. Ensure a clear understanding of each term.

Memory Hooks

Use mnemonics to remember each term. For example, think of Route Server as the post office for NVAs. These memory hooks aid retention and quick recall during the exam.

Daily Review

Adopt a 15-minute daily review routine using flashcards. This consistent practice reinforces learning and ensures long-term retention of key concepts.

Lab Checklist & Microsoft Learn Links

Lab Activities

Complete hands-on labs such as creating a VPN with BGP, deploying an ExpressRoute circuit, configuring Azure Firewall DNAT, enabling Traffic Analytics, and setting up Private Endpoints. Practical experience reinforces theoretical knowledge.

Learning Resources

Use Microsoft Learn links for guided tutorials. Repeat each lab within 24 hours to solidify understanding. This active learning approach ensures you are well-prepared for the exam.

Cost Optimization Cheat Sheet

Cost-Efficient Practices

Adopt cost optimization strategies such as using regional VNet integration, choosing NAT Gateway over multiple Load Balancer outbound IPs, sharing ExpressRoute circuits, and selecting Standard Load Balancer with zone redundancy.

Cost Calculator

Use the Azure cost calculator to estimate expenses. Input parameters such as resource types, usage patterns, and regions to get accurate cost projections.

DDoS Protection

Enable DDoS protection only on production VNets to avoid unnecessary costs. Understand the cost implications of each service to make informed decisions.

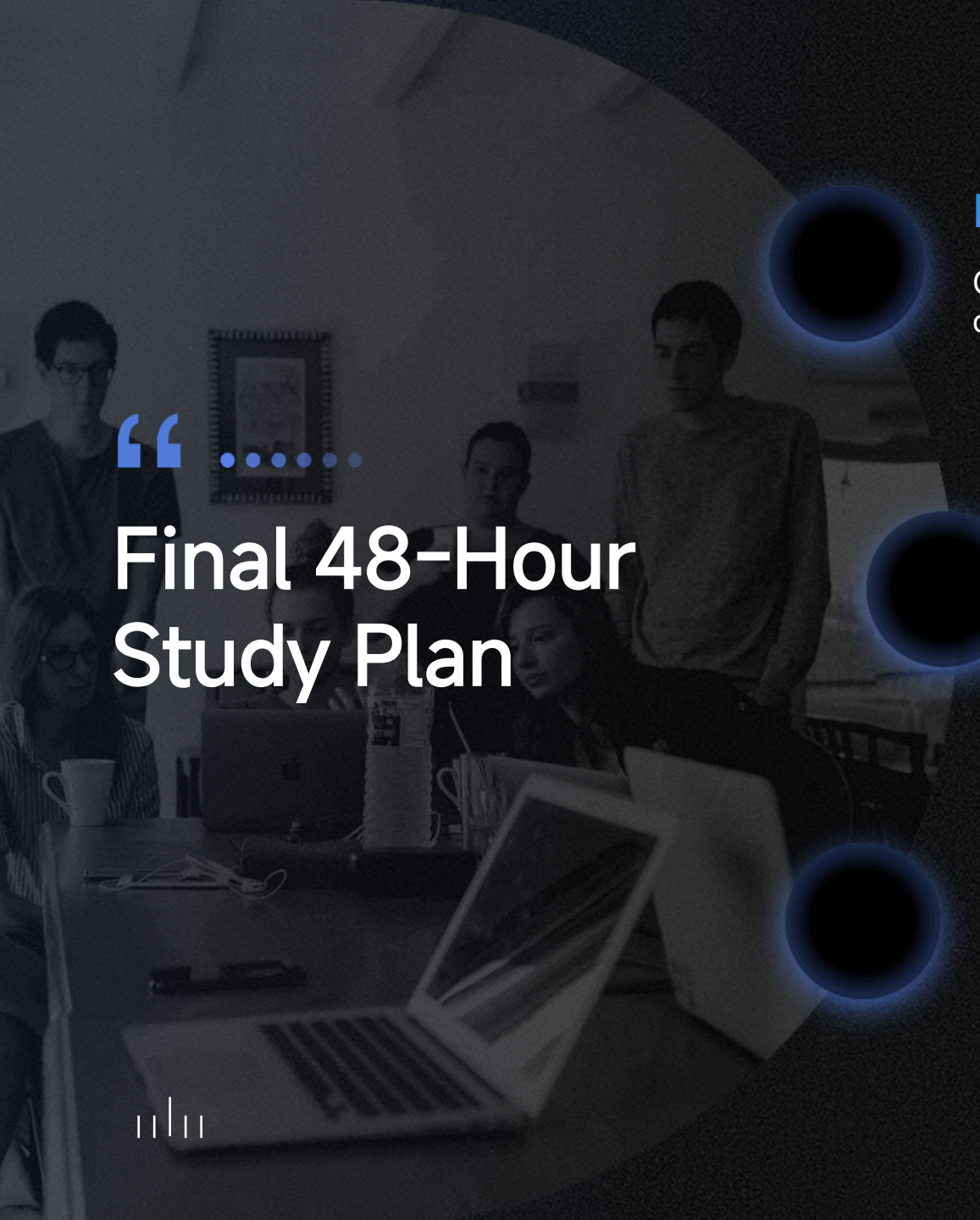
Security Integration Overview

Integration with Sentinel & Defender

Map networking services to Azure Sentinel data connectors and Defender for Cloud recommendations. This integration enhances security monitoring and threat detection capabilities.

Policy Enforcement

Use Azure Policy built-ins for automatic remediation of private endpoints. Ensure compliance with organizational security policies through proactive enforcement.



Final 48-Hour Study Plan

Day 1 Review

On day 1, review a full mock exam to identify knowledge gaps. Focus on areas needing improvement and reinforce key concepts.

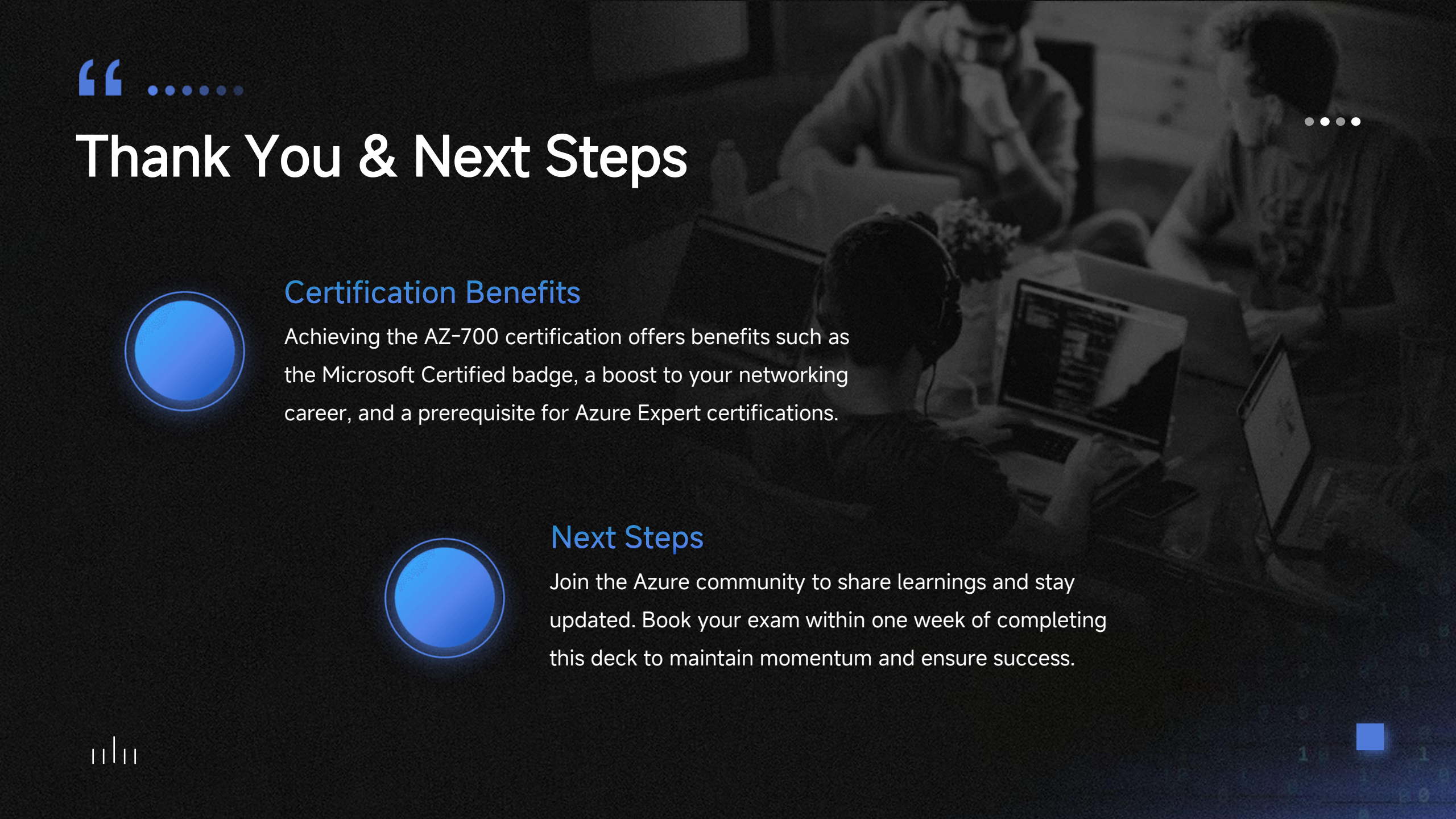
Day 2 Preparation

On day 2, spend the morning reviewing flashcards and the afternoon repeating hands-on labs. This active learning reinforces understanding and retention.

Exam Day Tips

Ensure you have your passport, know the exam reschedule window, and arrive early at the test center. Get a good night's sleep and trust your preparation.

Thank You & Next Steps



Certification Benefits

Achieving the AZ-700 certification offers benefits such as the Microsoft Certified badge, a boost to your networking career, and a prerequisite for Azure Expert certifications.

Next Steps

Join the Azure community to share learnings and stay updated. Book your exam within one week of completing this deck to maintain momentum and ensure success.

THANK YOU

Mahdi Sheikhi

2025/08/05