AZ-700: Secure Azure Private Access

Mahdi Sheikhi

CONTENTS

01 Private Endpoint Strategy

02 Creating Private Endpoints

03 Secure Endpoint Access

04 Private Link Service

05 DNS Integration Deep Dive

CONTENTS

01 On-Premises Connectivity

02 Service Endpoints Legacy

01

PART 01

Private Endpoint Strategy

When Private Endpoints Outperform VPN

01

Latency Comparison

Private endpoints offer lower latency compared to VPNs due to direct connectivity within the Azure backbone, reducing the need for internet traversal and improving performance for cloud-native applications.

02

Routing Complexity

Private endpoints simplify routing by eliminating the need for complex VPN configurations, ensuring straightforward traffic flow within the Azure network, which is crucial for maintaining security and compliance.

03

Cost and Compliance

Private endpoints are cost-effective and enhance compliance by providing secure, direct access to Azure resources without exposing them to the public internet, meeting regulatory requirements for data privacy.

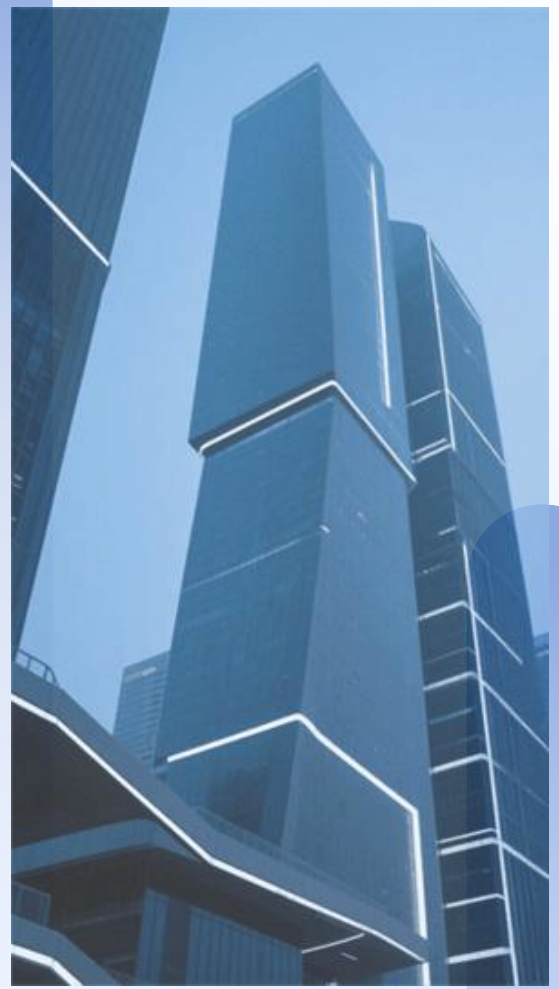
Mapping Resources to Required Subnets

One-to-Many Relationship

A single subnet can host multiple private endpoints, allowing efficient resource allocation. Inventorying VNet address space helps in planning and preventing IP exhaustion during deployment.

Service Tag Consumption

Documenting service tags that consume IP addresses ensures that there is sufficient address space available for private endpoints, avoiding conflicts and ensuring smooth rollout.



Approval Workflow and Governance Model

Manual vs. Auto-Approval

The toggle between manual and auto-approval for private endpoint connections allows flexibility in managing access requests, balancing security and operational efficiency.

RBAC Roles

Roles like Private Endpoint Contributor and Network Admin ensure proper governance. Azure Policy integration enforces tagging, maintaining organizational standards and compliance.

Lifecycle Management

From request to revocation, managing the lifecycle of private endpoints prevents sprawl and ensures that only necessary endpoints are active, enhancing security.

Compliance and Control

Implementing governance models ensures that private endpoints adhere to organizational policies, maintaining security and compliance throughout their lifecycle.

02

PART 02

Creating Private Endpoints

Portal Wizard Step-by-Step

01 Create Blade Overview

The create blade in the Azure portal guides users through selecting the target resource, sub-resource type, VNet, and subnet. It also allows setting static or dynamic IP addresses and enabling NIC-level NSGs.

02 Generated Template

Reviewing the generated ARM template provides insights into the configuration, enabling users to reproduce it via Infrastructure as Code (IaC) tools for consistency and scalability.

ARM, Bicep, Terraform Samples

ARM Templates

ARM templates offer a declarative way to deploy private endpoints, ensuring idempotency and parameterized configurations for dynamic environments.

Bicep Language

Bicep simplifies ARM template syntax, making it easier to manage complex configurations. It supports parameterized subnet IDs, enhancing flexibility.

Terraform Integration

Terraform provides reusable code snippets for private endpoints, allowing for efficient management of infrastructure. It ensures that NIC IPs are correctly outputted for DNS records.

Cross-Tenant and Multi-Region Patterns

Shared Private Link for SaaS

In SaaS scenarios, shared Private Link services enable multiple tenants to connect securely, reducing the overhead of managing individual endpoints.

Multi-Region Deployment

Deploying secondary regions with paired endpoints ensures high availability and disaster recovery. Global reach allows seamless traffic routing while maintaining a single DNS zone.

03

PART 03

Secure Endpoint Access

Default DenyAllInbound

01

Private endpoint NICs default to DenyAllInbound, ensuring that only explicitly allowed traffic can access the endpoint, enhancing security.

Allowing Corporate IPs

02

Configuring NSG rules to allow traffic from corporate IP prefixes ensures that only authorized on-premises clients can access the private endpoint.

AzurePlatformAllow

03

The AzurePlatformAllow rules must remain intact to prevent blocking platform health probes, ensuring continuous monitoring and service availability.

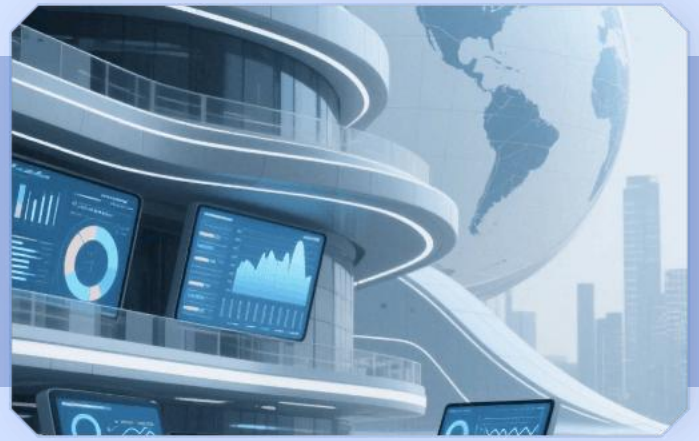
UDR and Firewall Integration

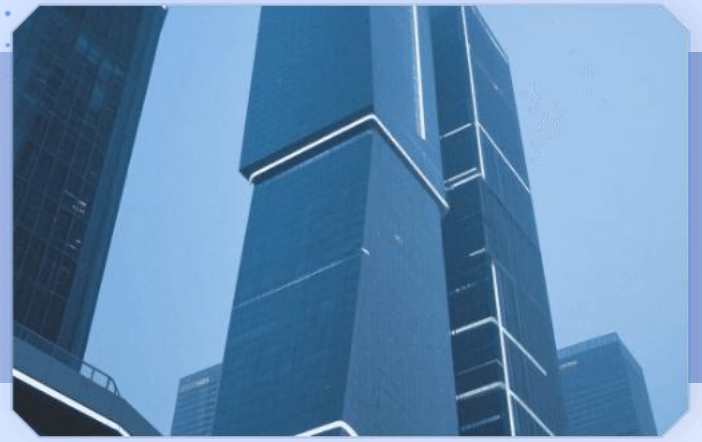
Forced Tunnelling

Using UDR with next-hop type VirtualAppliance allows traffic to be routed through NVAs, ensuring advanced security measures like firewalls are applied to private endpoint traffic.

Symmetric Routing

Maintaining symmetric routing is crucial for ensuring consistent traffic flow and preventing issues like asymmetric routing, which can lead to connectivity problems.





Monitoring with NSG Flow Logs

Enabling Flow Logs

Enabling NSG flow logs on the endpoint subnet allows detailed monitoring of traffic, helping identify unauthorized access attempts and potential security threats.

Log Analytics and Alerts

Sending flow logs to Log Analytics and creating alerts for unexpected source IPs or denied attempts enables early detection of lateral movement and enhances security.

04

PART 04

Private Link Service

Publishing Your Own Service

Private Link Service Resource

The Private Link Service resource enables organizations to expose their own services securely. It requires a Standard Load Balancer frontend and at least one NAT IP for connectivity.

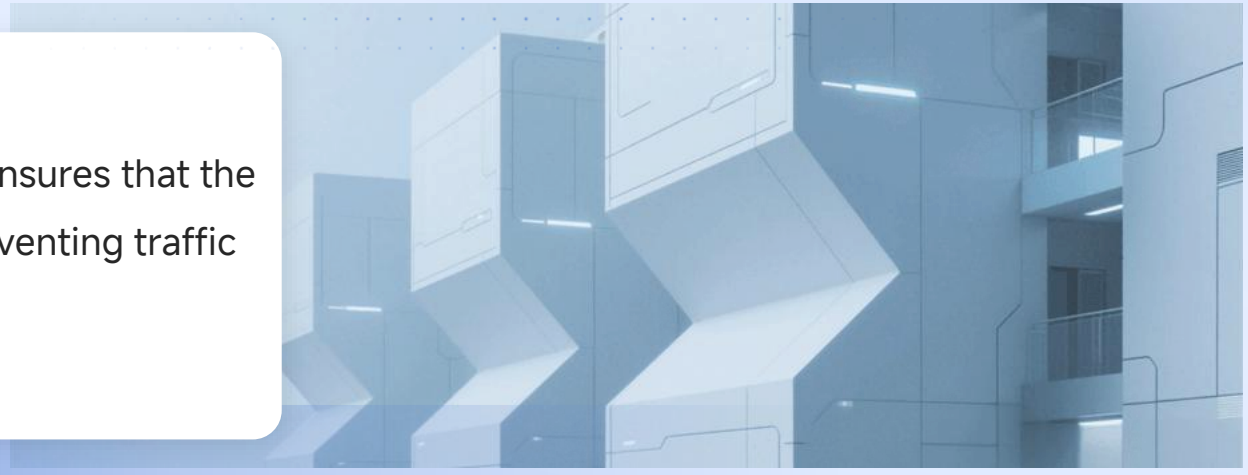
Visibility Control

Controlling visibility (tenant-only vs. public) allows organizations to decide who can request connections to their Private Link Service, enhancing security and compliance.

Load Balancer Health Probe Setup

TCP/HTTP Probes

Creating TCP or HTTP probes on standard ports (80 or 443) ensures that the load balancer can monitor the health of backend services, preventing traffic to unhealthy instances.



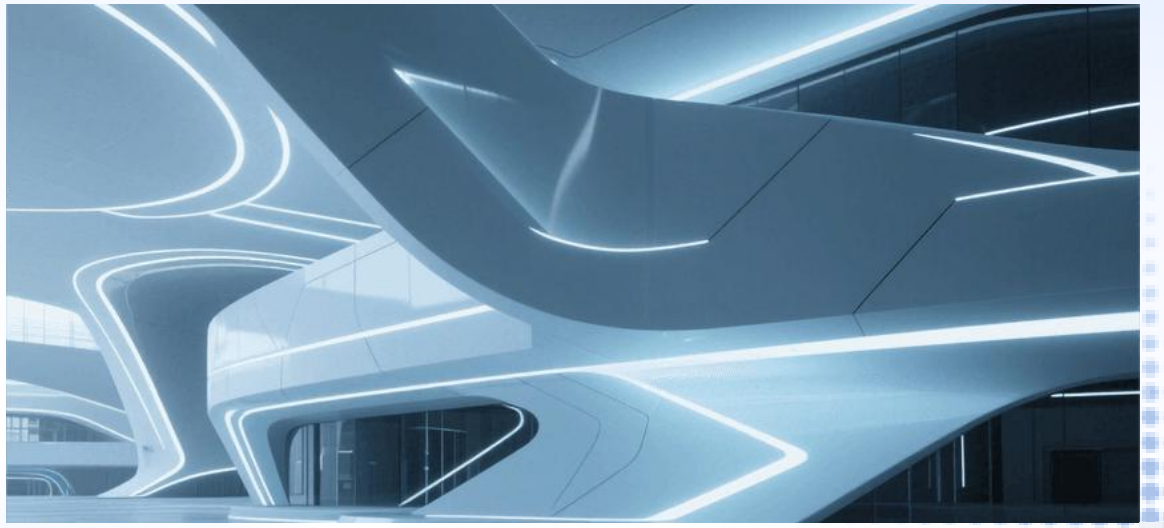
Backend Pool Linking

Linking the probe to the backend pool running the service ensures that only healthy VMs receive traffic, maintaining high availability and reliability.

Health Checks

Ensuring the probe marks VMs as healthy before allowing traffic prevents black-holing of consumer connections, ensuring seamless service delivery.

Consuming the Service Cross-Tenant



02 Connection Approval

The service owner approves connections, ensuring that only authorized consumers can access the service, maintaining control and security.

01 Service Alias Sharing

The service owner shares the alias, allowing consumers in different tenants to create private endpoints and request connections, enhancing cross-tenant collaboration.

05

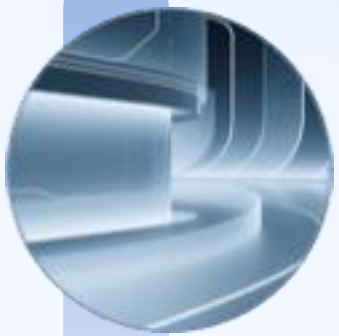
PART 05

DNS Integration Deep Dive

Private DNS Zone Architecture

Service to Zone Mapping

Each Azure service maps to a specific DNS zone name, ensuring that private endpoints resolve correctly within the Azure network, maintaining service accessibility.



Automatic A Record Injection

Azure automatically injects an A record into the private DNS zone, simplifying the process of resolving private endpoint IPs without manual intervention.

Redundancy Considerations

Understanding regional and zonal redundancy helps architects design DNS configurations that ensure high availability and fault tolerance for private endpoints.

Hybrid DNS with Windows Server

Conditional Forwarders

Setting up conditional forwarders from on-premises AD DNS to Azure private resolvers ensures that DNS queries are correctly routed, maintaining seamless connectivity.

Azure Resolver Security

Securing the Azure private resolver with VNet ACLs prevents unauthorized recursion, ensuring that DNS queries are handled securely and efficiently.

01

02

03

04

06

PART 06

On-Premises Connectivity

ExpressRoute Private Peering Path

Traffic Flow

Traffic flows from on-premises branches through the Microsoft Edge, into the VNet gateway subnet, and finally to the private endpoint, ensuring secure connectivity.

01

Symmetric Routing

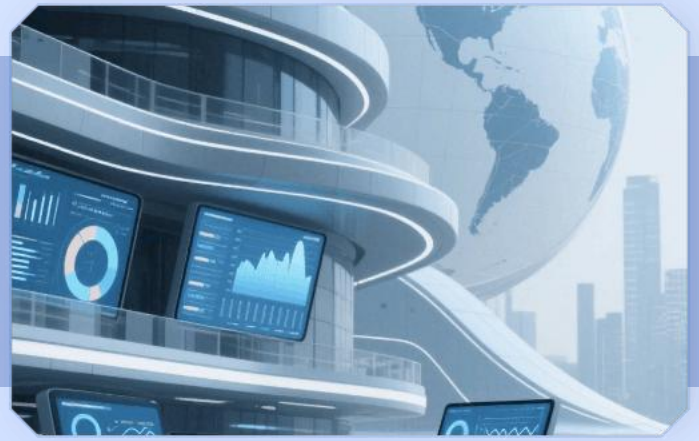
Advertising the endpoint subnet prefix to on-premises ensures that return traffic is symmetric, preventing routing issues and maintaining consistent connectivity.

02

Monitoring Tools

Using Azure Network Watcher tools like Get-AzNetworkWatcherReachabilityReport helps verify next-hop configurations and troubleshoot connectivity issues.

03



Site-to-Secure VPN with BGP

BGP Integration

Enabling BGP on the VPN gateway allows the exchange of routes with on-premises routers, ensuring that traffic destined for private endpoints is correctly routed.

Encrypted Tunnel

Using the learnt routes, traffic is steered through the encrypted VPN tunnel, maintaining secure and efficient connectivity between on-premises and Azure resources.

Troubleshooting with AzNetworkWatcher

Reachability Report

Using Get-AzNetworkWatcherReachabilityReport helps verify next-hop configurations and identify connectivity issues, ensuring smooth traffic flow.

Connection Testing

Test-AzPrivateEndpointConnectivity allows testing TCP handshake, ensuring that private endpoints are reachable and functioning correctly.

07

PART 07

Service Endpoints Legacy

Compliance Requirements

Starting with compliance requirements, the decision tree evaluates various factors to determine the most suitable connectivity option between service endpoints and private links.

Traffic Stay-on-Azure

Assessing whether traffic needs to stay within Azure helps decide between service endpoints for internal scenarios and private links for broader access.

IP Overlap Considerations

Evaluating IP overlap scenarios ensures that the chosen connectivity option does not introduce conflicts, maintaining seamless network operations.

Enabling Service Endpoints on Subnets

Portal, CLI, ARM Snippets

Using the Azure portal, CLI, or ARM templates, administrators can enable service endpoints on subnets, ensuring secure access to Azure resources.

Session Reconnect

Enabling service endpoints may cause a brief reconnect, dropping existing sessions. Scheduling during maintenance windows minimizes disruption.

Writing Effective Endpoint Policies

Policy Syntax

Endpoint policies use JSON syntax to define allow lists of Azure resource IDs or tags, ensuring precise control over allowed resources.

01

Default Deny

The default deny rule ensures that only explicitly allowed resources are accessible, enhancing security by blocking unauthorized access.

02

Evaluation Order

Understanding the evaluation order of policies helps administrators design effective rules, ensuring that the most specific policies are applied first.

03

Securing with VNet Firewall Rules

Firewall Configuration

Switching the storage firewall to ‘Selected networks’ and selecting the subnet with service endpoints ensures that traffic originates from the subnet’s public IP.

Session Verification

Using Test-NetConnection verifies that traffic originates from the correct subnet, ensuring that firewall rules are correctly applied and secure access is maintained.

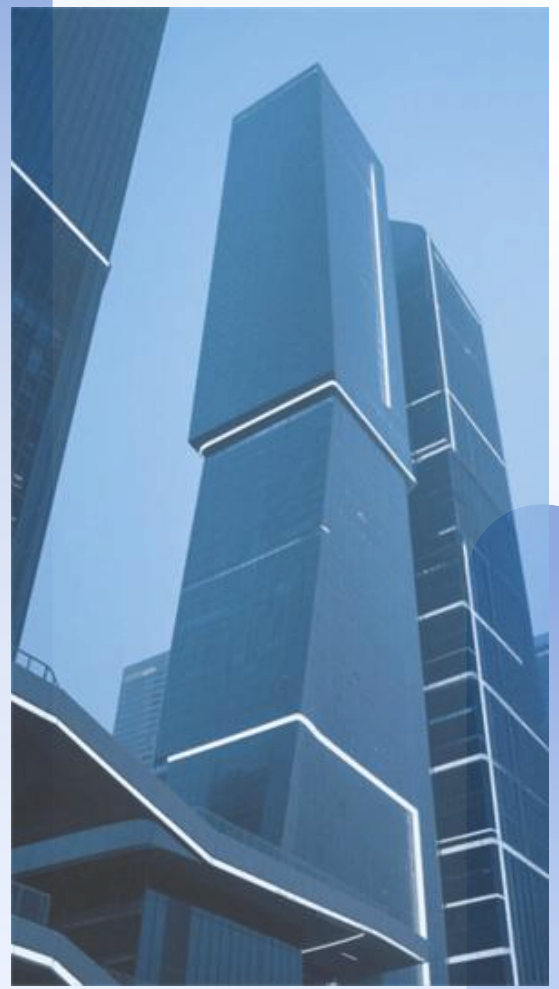
Monitoring and Audit Checklist

Diagnostic Logs

Enabling diagnostic logs for storage and sending them to a Log Analytics workspace provides detailed insights into access patterns and potential security issues.

Alert Configuration

Creating alerts for traffic originating from outside the service-endpoint-enabled subnet range helps detect and respond to unauthorized access attempts quickly.



Migration Path to Private Link

Staged Approach

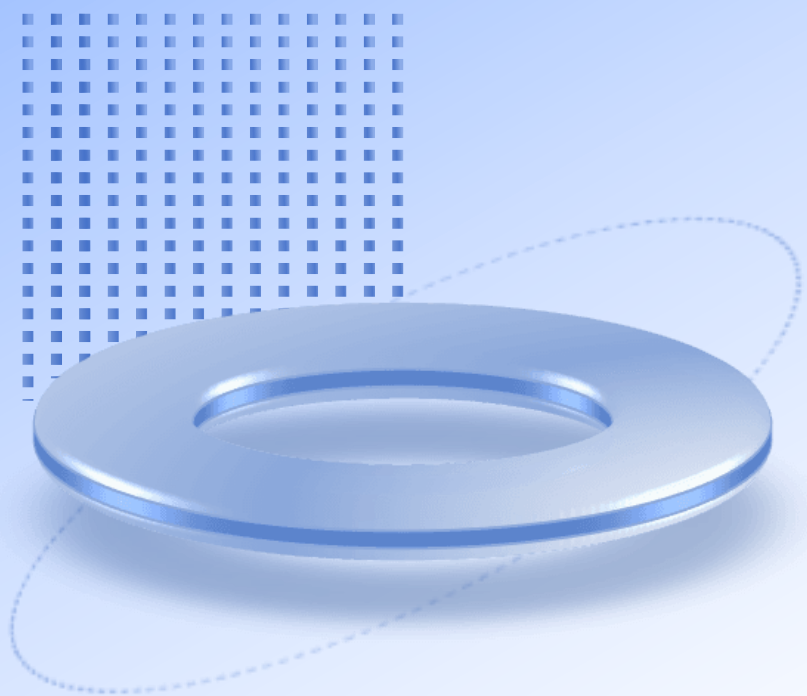
A staged migration approach ensures a smooth transition from service endpoints to private links, minimizing disruption and maintaining secure access.

DNS Record Duplication

Duplicating DNS records during migration ensures that both service endpoints and private links are accessible, allowing for a seamless transition.

Policy and Rule Updates

Updating service endpoint policies and firewall rules ensures that only private links are used after migration, enhancing security and compliance.



THANKS

Mahdi Sheikhi