

Network Architecture: Design Principles

- Segmentation:** Use *VNets* for workload separation. *Subnets* for different applications (web, database, API).
- Security:** Apply *NSGs* for traffic filtering.
- Regional Architecture:** Implement *Availability Zones* for high availability.
- Scalability:** Design for automated scaling and modular structures.

Security Solutions and Standards

- Azure Firewall:** Centralized access management. Integrates with *Azure Sentinel*.
- Network Security Groups:** Control traffic via *IP*, *port*, and *protocol* for *subnets* and *VMs*.
- Azure Private Link:** Secure access via *private endpoints*, isolated from the public internet.
- Compliance Standards:** *ISO27001* and *NIS²* for documented security policies.

Network Connectivity: On-Premises Integration

- VPN Gateway:** Cost-effective secured connections with limited bandwidth.
- ExpressRoute:** Dedicated connection with high bandwidth and no internet dependency.
- Scalability:** Dynamic scaling with Azure Virtual WAN and modular extensions.

Key Metrics to Monitor

- Performance:** Check bandwidth and latency for both *VPN* and *ExpressRoute*.
- Usage:** Analyze traffic patterns with *Azure Monitor*.

Hybrid Network Infrastructure

- Architecture Components:** On-Premises Datacenter linked via *VPN Gateway* or *ExpressRoute*.
- Firewalls:** Local security segmentation and Azure integration.
- Security Mechanisms:** Use *Private Link* for secure traffic; monitor via *Azure Monitor*.

Regional Network Infrastructure

- Regions:** Select nearest *Azure region* to minimize latency; use multiple for redundancy.
- Availability Zones:** Protect against datacenter-level failures.
- Documentation:** Keep security and network topology updated.

Best Practices

- Monitoring:** Utilize *Azure Monitor* and *Log Analytics* for insights.
- Updates:** Regularly revise policies per *ISO27001* and *NIS²* standards.

Example Architecture

- Connectivity:** On-Premises VPN Gateway ↔ *Azure VPN Gateway*.
- Redundancy:** *Primary* and *Secondary Regions* configured.
- Security:** *Azure Firewall* and *NSGs* filter traffic.

Connections Overview

- Use *VPN* for secure connections or *ExpressRoute* for dedicated bandwidth.
- Prioritize security through *AZs* and *NSGs*.



By haraldthegrey

Published 9th January, 2025.
Last updated 10th January, 2025.
Page 1 of 1.

Sponsored by **Readable.com**
Measure your website readability!
<https://readable.com>