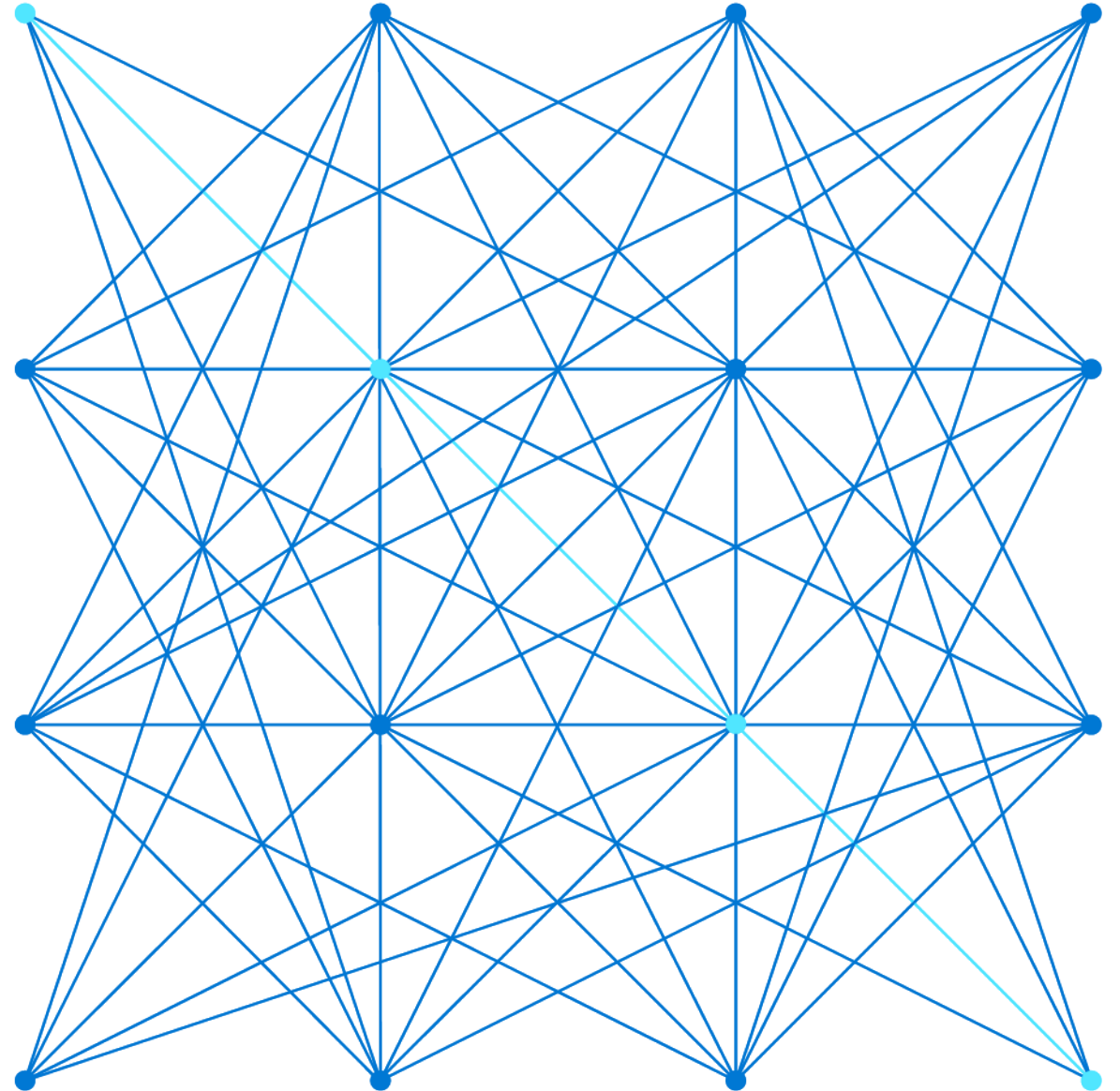


Azure Architects Connect "Azure Landing Zones / Deep Dive Network"

Christopher Feussner, Security Cloud Solutions Architect

14. Oktober 2021



Agenda

Intro Azure Landing Zone & Enterprise-Scale

Critical Design Area Networking

- Considerations like IP Address Planning
- Network Topology & Segmentation
- DNS
- Connectivity to Azure (Hub & Spoke, Virtual WAN)
- Azure Firewall & Co.
- Connectivity to Azure PaaS (within Landing Zone)

Q&A

Metropolis

*Using an analogy, this is similar to how city utilities such as **water, gas,** and **electricity** are accessible before new houses are constructed. In this context, the network, IAM, policies, management, and monitoring are shared '**utility**' services that **must be readily available** to help streamline the application migration process.*



Enterprise-scale?

Enterprise-scale is an **architecture approach and reference implementation** that enables effective **construction** and **operationalization** of landing zones on Azure, at scale and **aligned** with **Azure Roadmap** and **Microsoft Cloud Adoption Framework for Azure**.

Authoritative

Provides holistic design decision framework for Azure Platform.

Proven

Based on success of large-scale migration projects at-scale.

Prescriptive

Apply it on clearly plan and design your Azure environment.

Enterprise-scale Design Principles

Enable Autonomy for Innovation and Transformation

Security and Compliance By-Default

Governance At-Scale with Sustainable Cloud Engineering



Subscription Democratisation



Policy Driven Governance



Single Control and Management Plane



Application Centric and Archetype-Neutral



Azure Native Design and Platform Roadmap Alignment

Enterprise-scale Design Guidelines



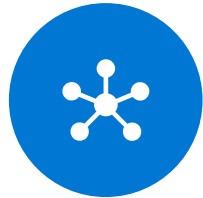
Enterprise Enrolment
& Azure AD Tenants



Identity & Access
Management



Management Group
& Subscription
Organisation



Network Topology &
Connectivity



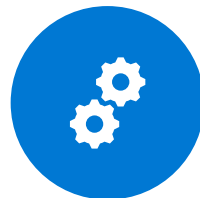
Management &
Monitoring



Business Continuity
& Disaster Recovery

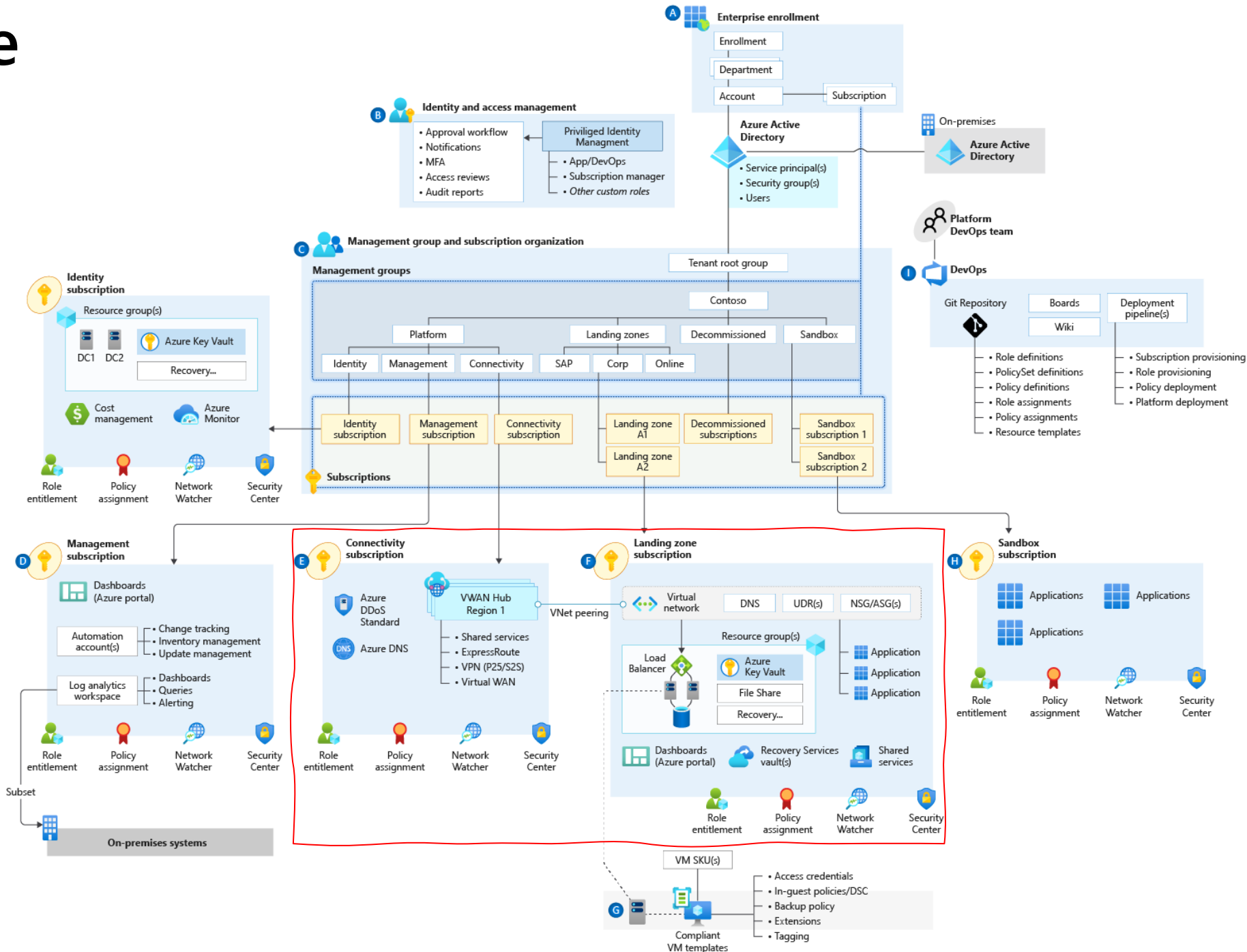


Security, Governance
& Compliance



Platform Automation
& DevOps

Enterprise-scale



What are you going to build?



A house



A stadium



A bridge

All foundations are NOT created equal



A house



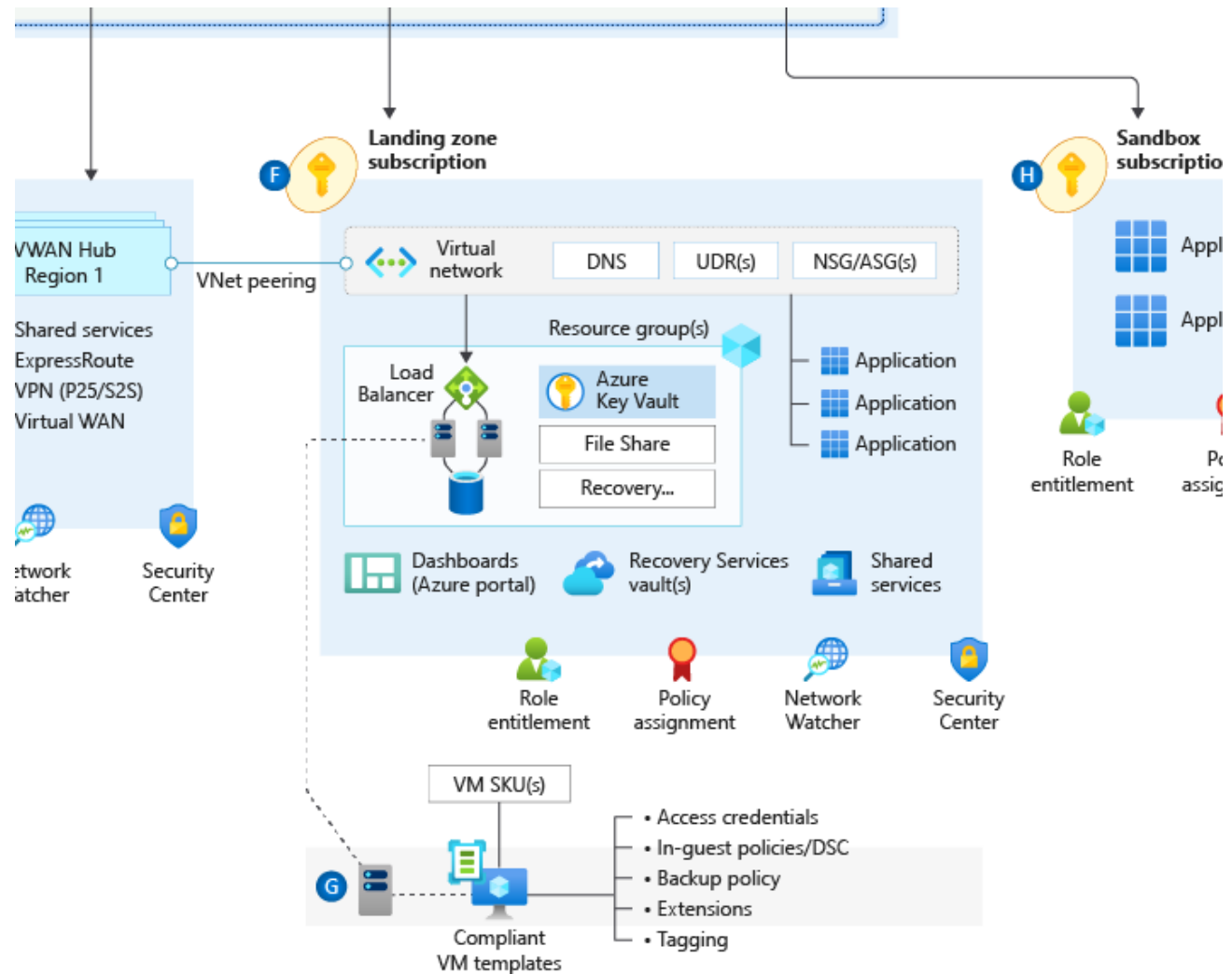
A stadium



A bridge

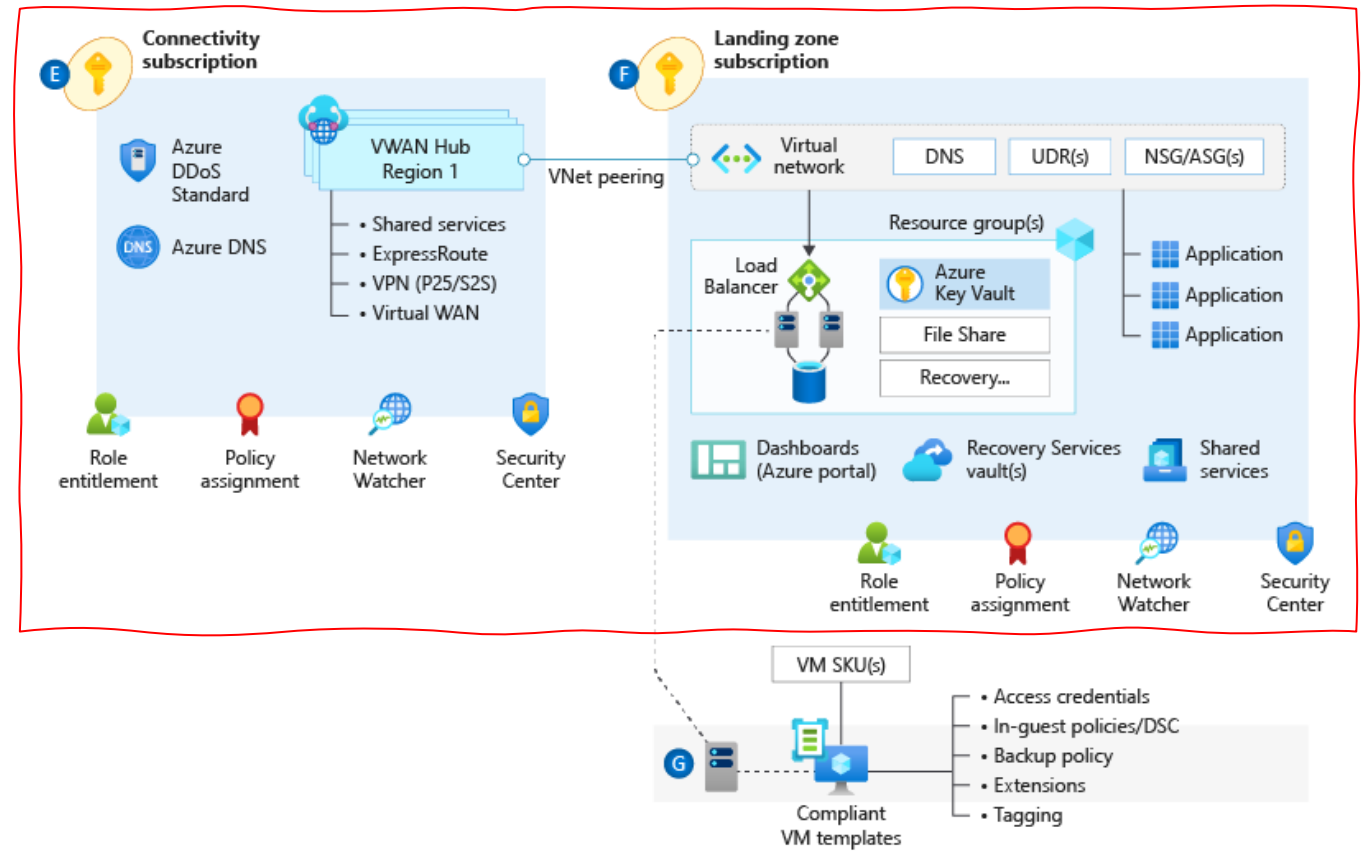
Enterprise-scale landing zone(s)

The principle purpose of the "Landing Zone" is therefore to ensure that when an application or workload lands on Azure, the required "plumbing" is already in place, providing greater agility and compliance with enterprise security and governance requirements.





Network Topology & Connectivity



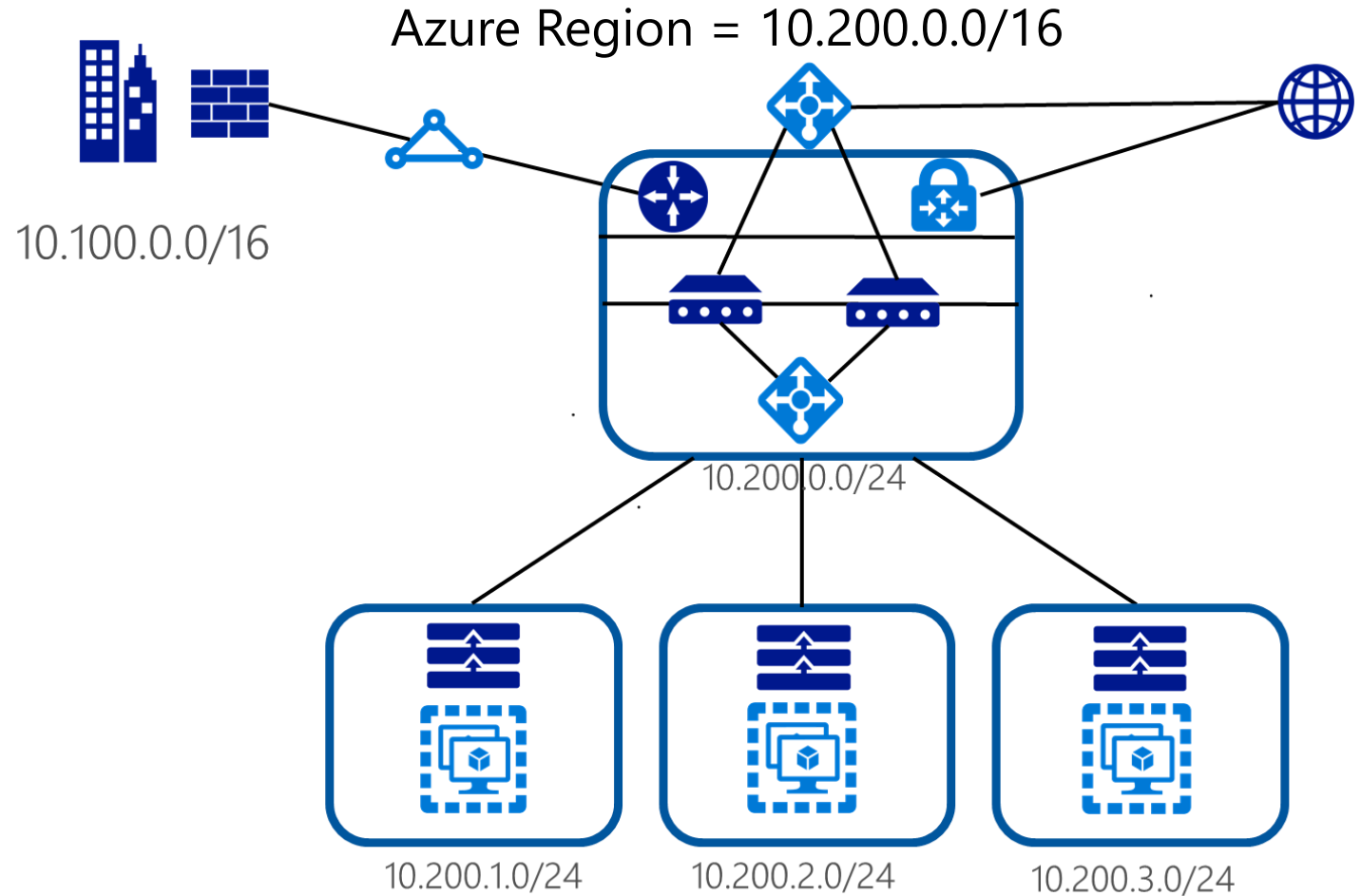
Overview

Consider the following design elements:

- IP Address planning
- Configure DNS
- Define Azure Network topology
- Azure Virtual WAN (Microsoft Managed)
- Traditional Azure networking (Customer Managed)
- Connectivity to Azure
- Azure Firewall & Co.
- Connectivity to Azure PaaS (within Landing Zone)



Network Topology & Connectivity



IP Addressing

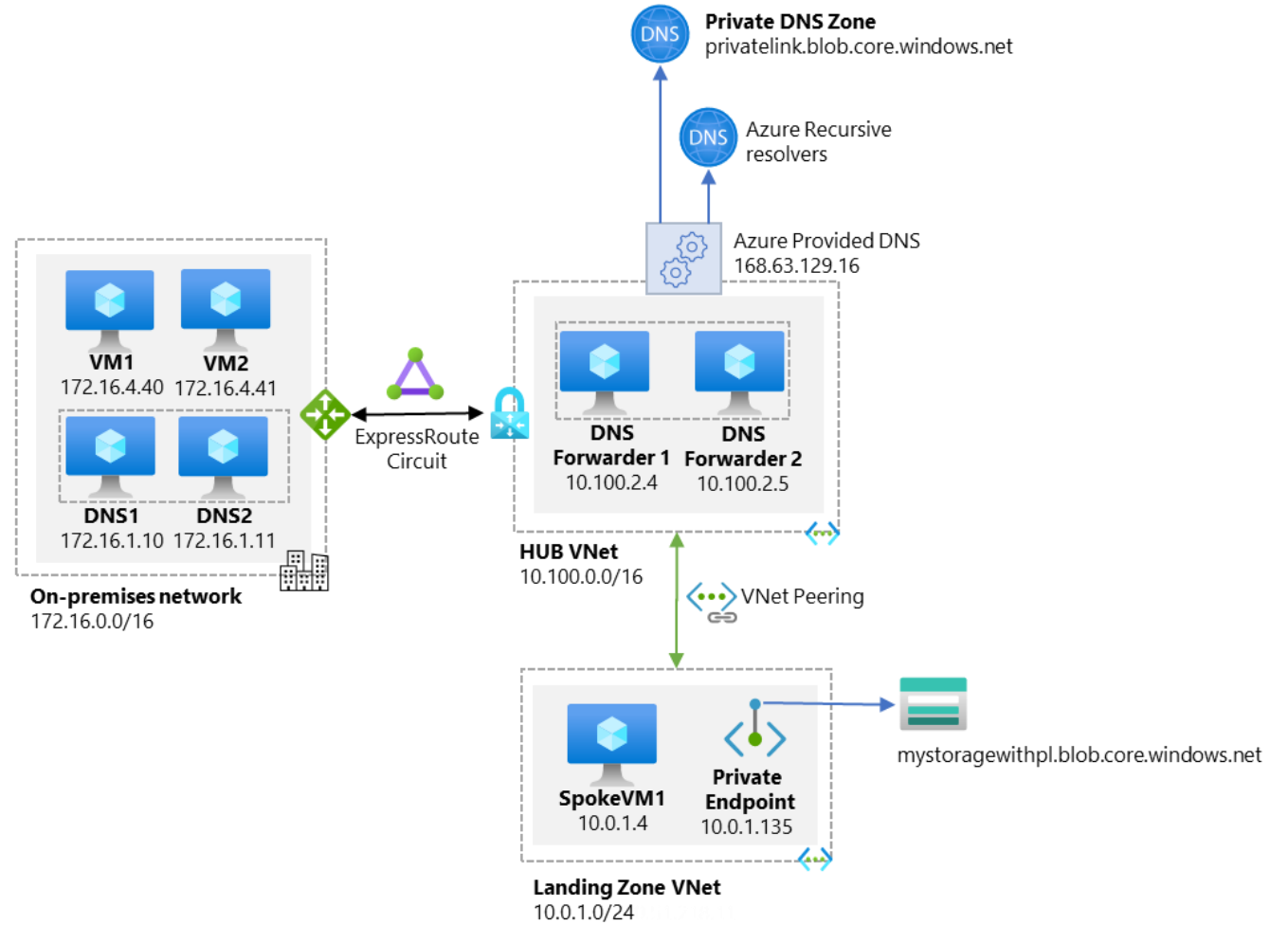
- No IP address overlap, no public IP's internal
- Size not to big, not to small, purpose driven
- Usage of private IP addresses (RFC1918)



Network Topology & Connectivity

DNS

Example - DNS resolution flow when a VM in a VNET tries to resolve private endpoint:



- Azure DNS Private and Public



Network Topology & Connectivity

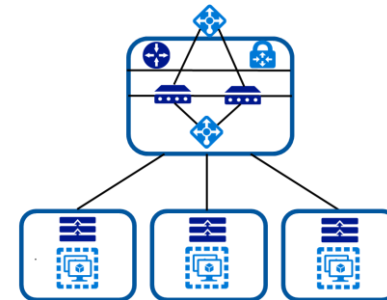
Define an Azure Networking Topology

Choose the right technologies and topology approaches for Azure deployments

Is there a need for branch-to-branch connectivity?



Is there a need granular control of connectivity?

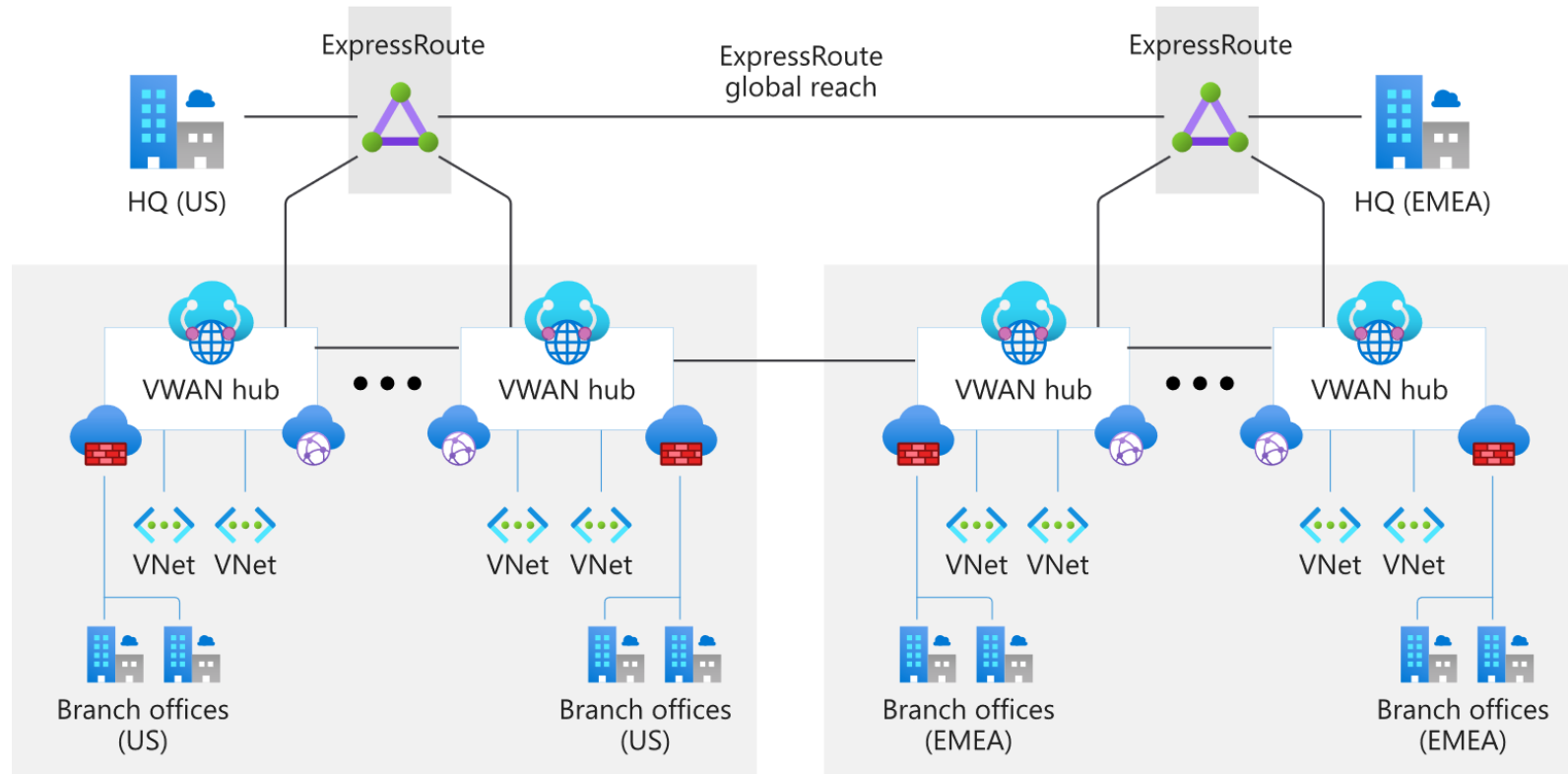




Network Topology & Connectivity

Virtual WAN

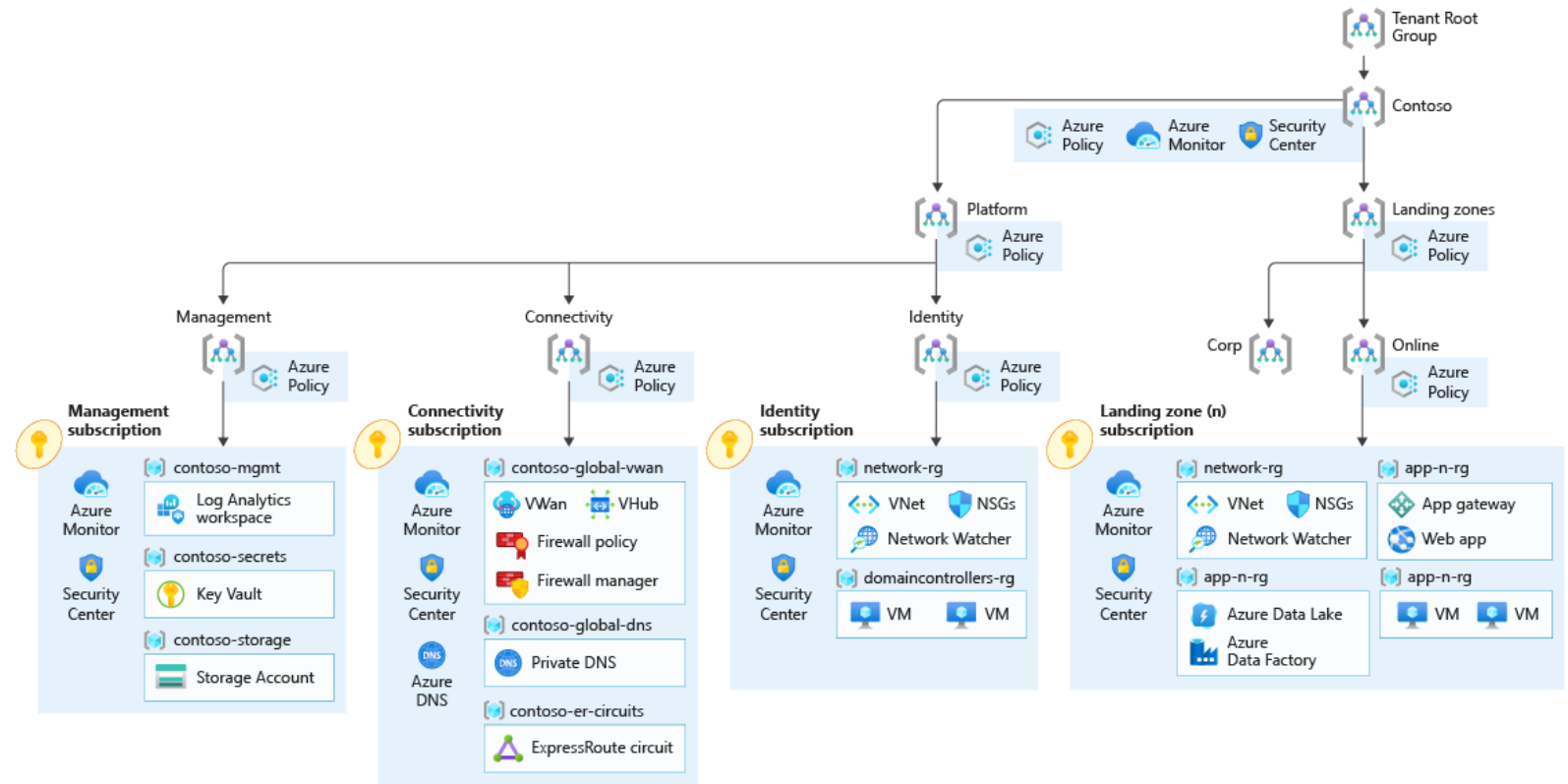
Virtual WAN Global Transit Network





Network Topology & Connectivity

Enterprise-Scale with Azure Virtual WAN



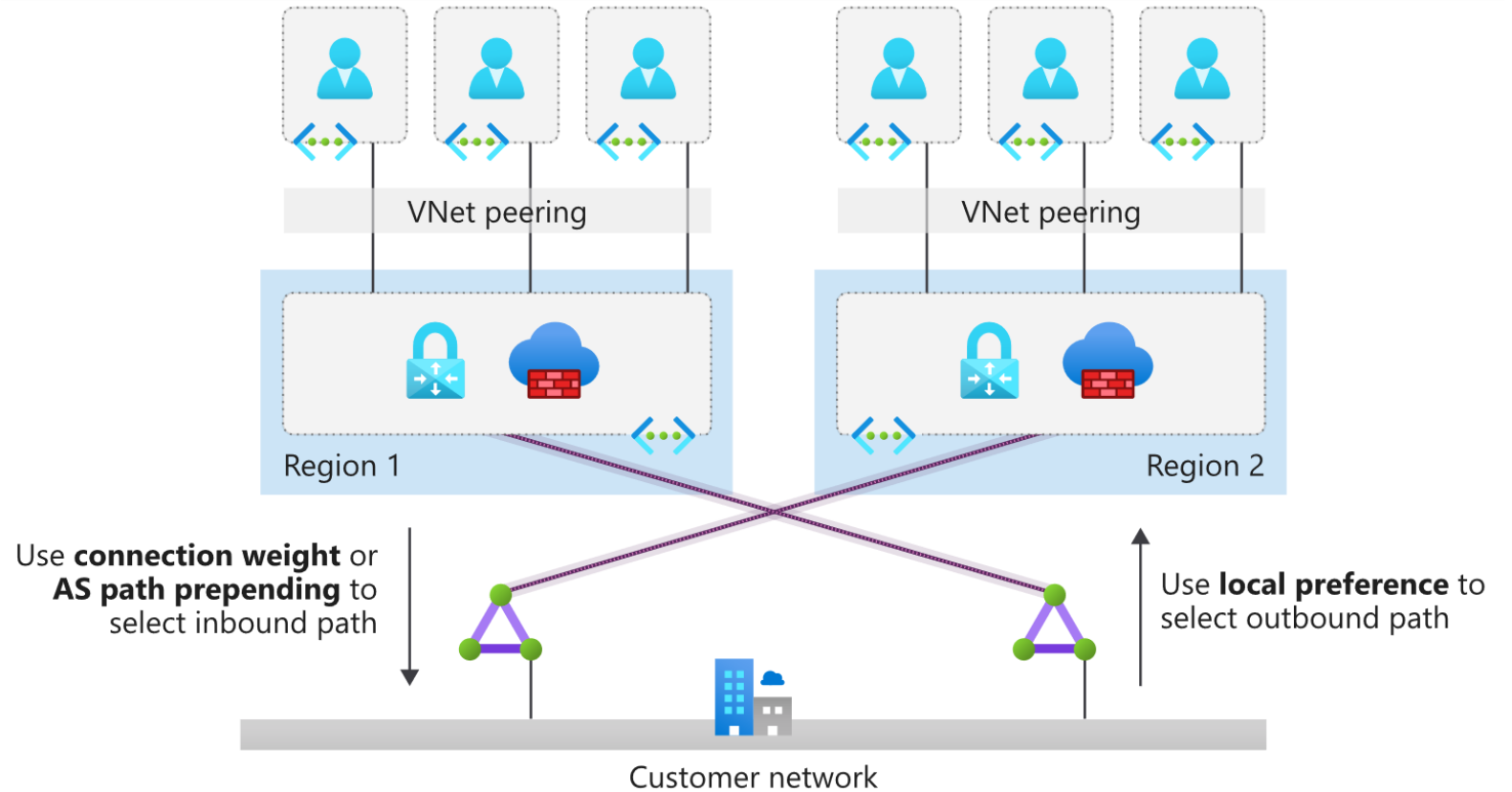
Virtual WAN

[Enterprise-Scale/Readme.md at main · Azure/Enterprise-Scale · GitHub](#)



Network Topology & Connectivity

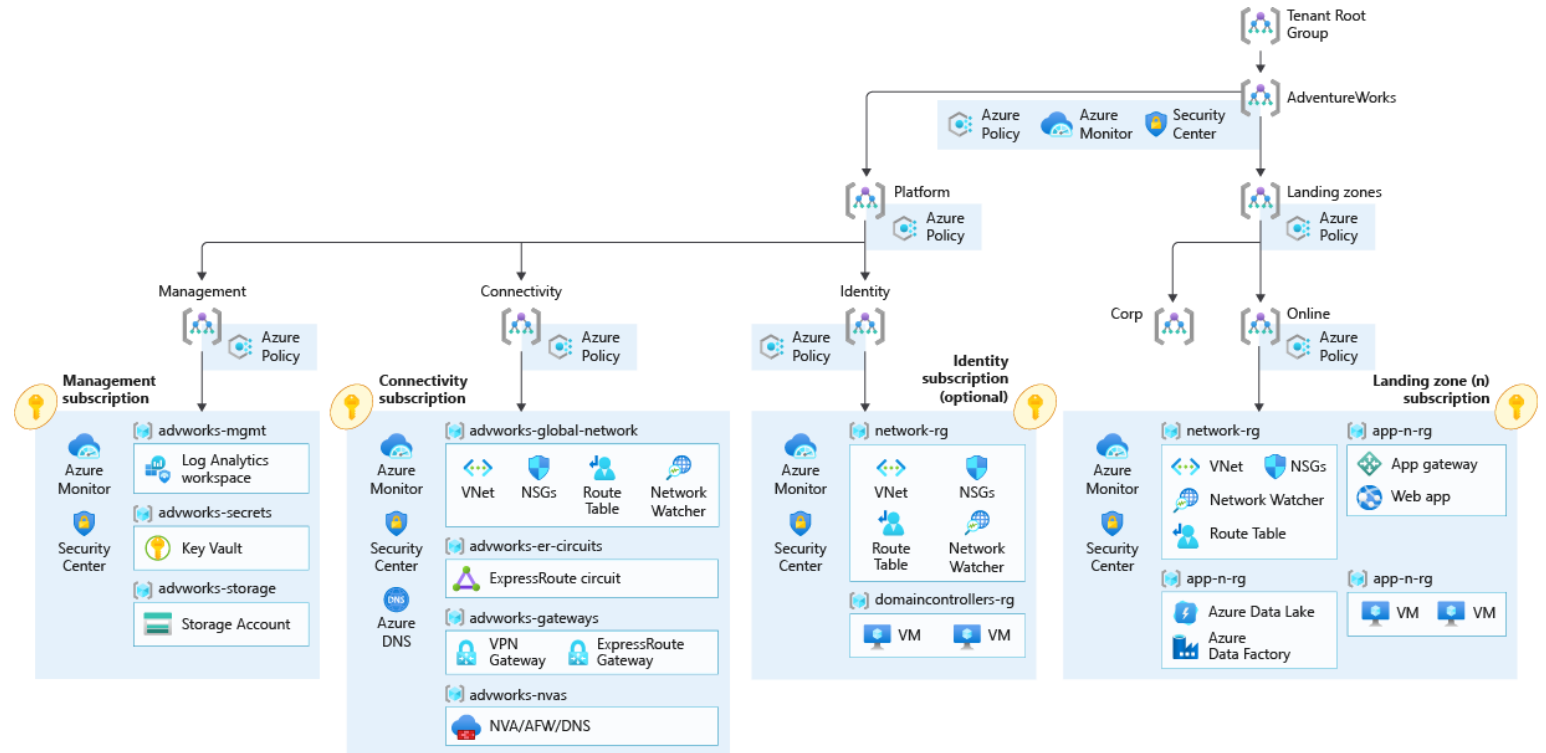
Traditional Hub and Spoke





Network Topology & Connectivity

Enterprise-Scale with Hub & Spoke



Traditional Hub and Spoke

[Enterprise-Scale/README.md at main · Azure/Enterprise-Scale · GitHub](#)

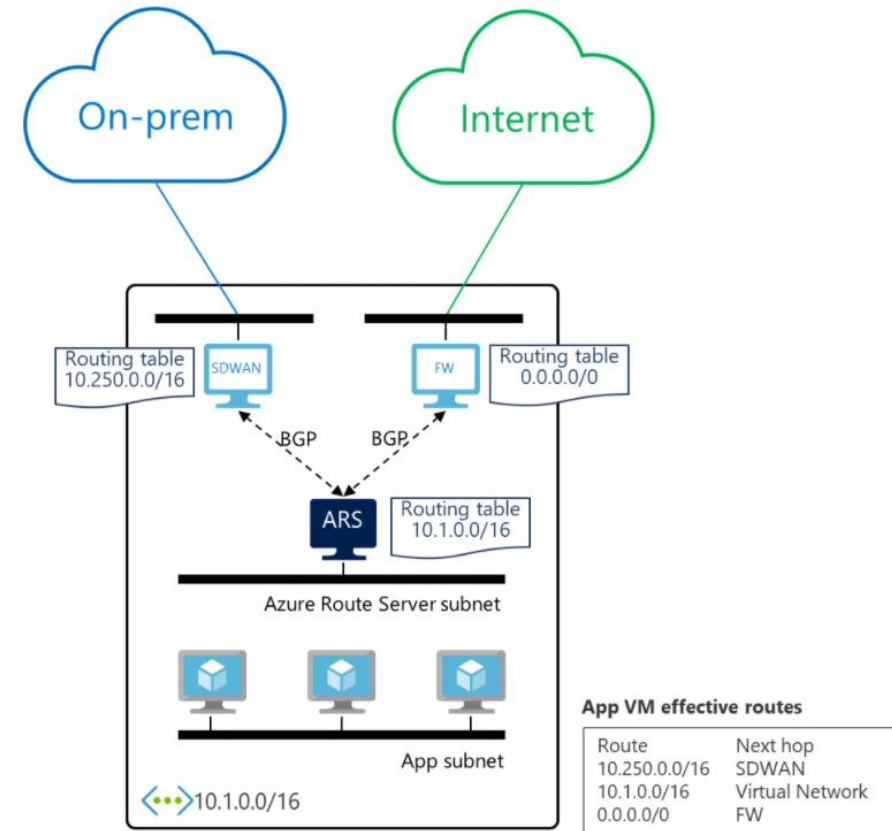


Network Topology & Connectivity

Azure Route Server (ARS) enables network appliances to exchange route information with Azure virtual networks dynamically.

Azure Route Server supports Azure ExpressRoute and VPN gateways to automatically take the latest route information from Azure Route Server instead of manually talking to each network.

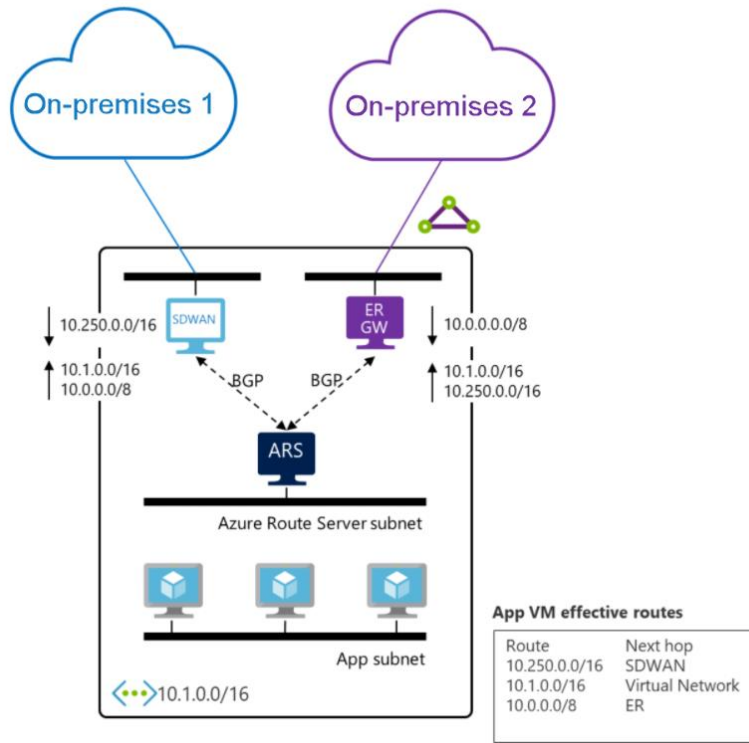
Azure Route Server



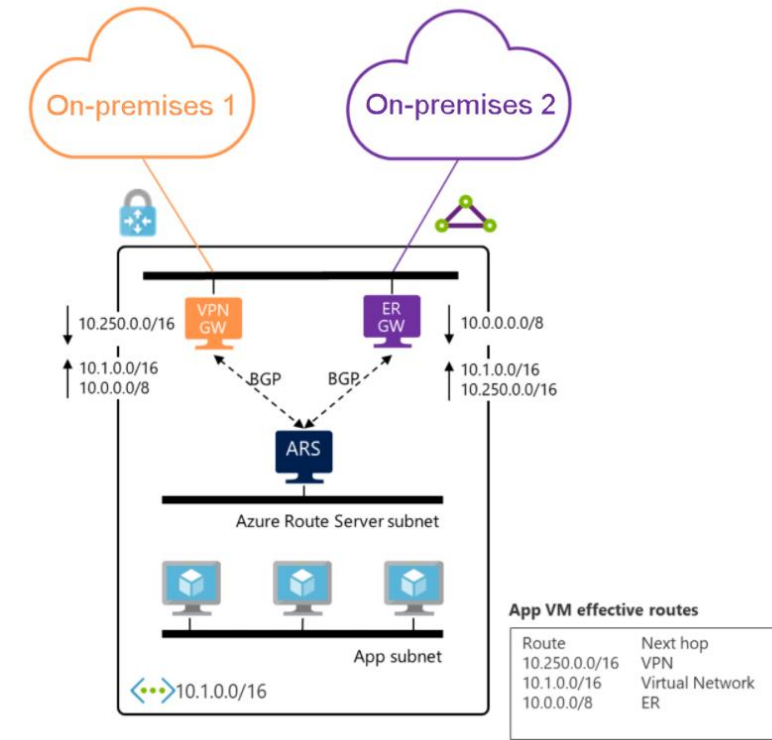


Network Topology & Connectivity

Azure Route Server



SDWAN

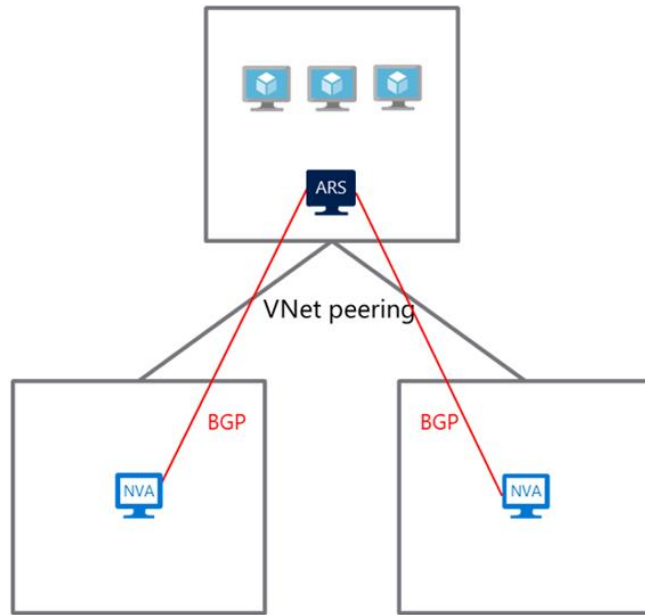


VPN GW

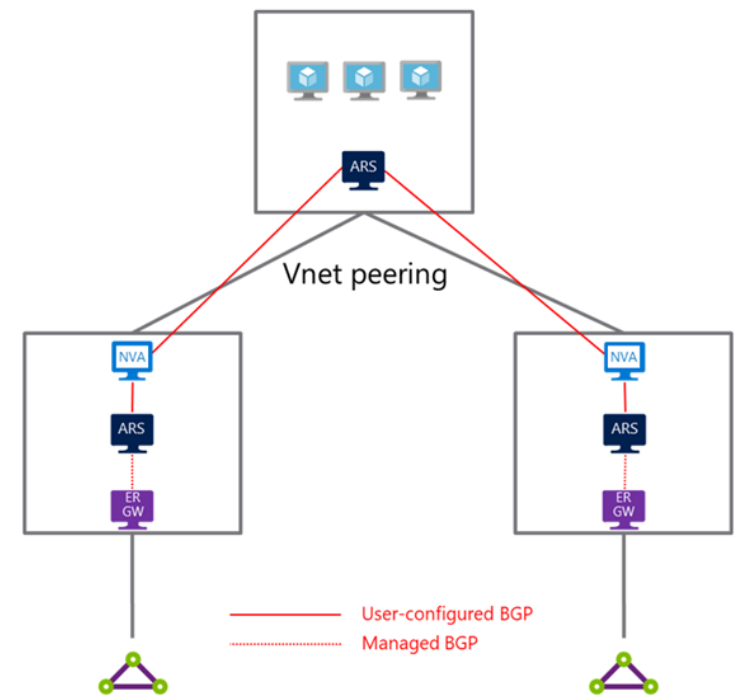


Network Topology & Connectivity

Azure Route Server



Dual-homed network with
Azure Route Server



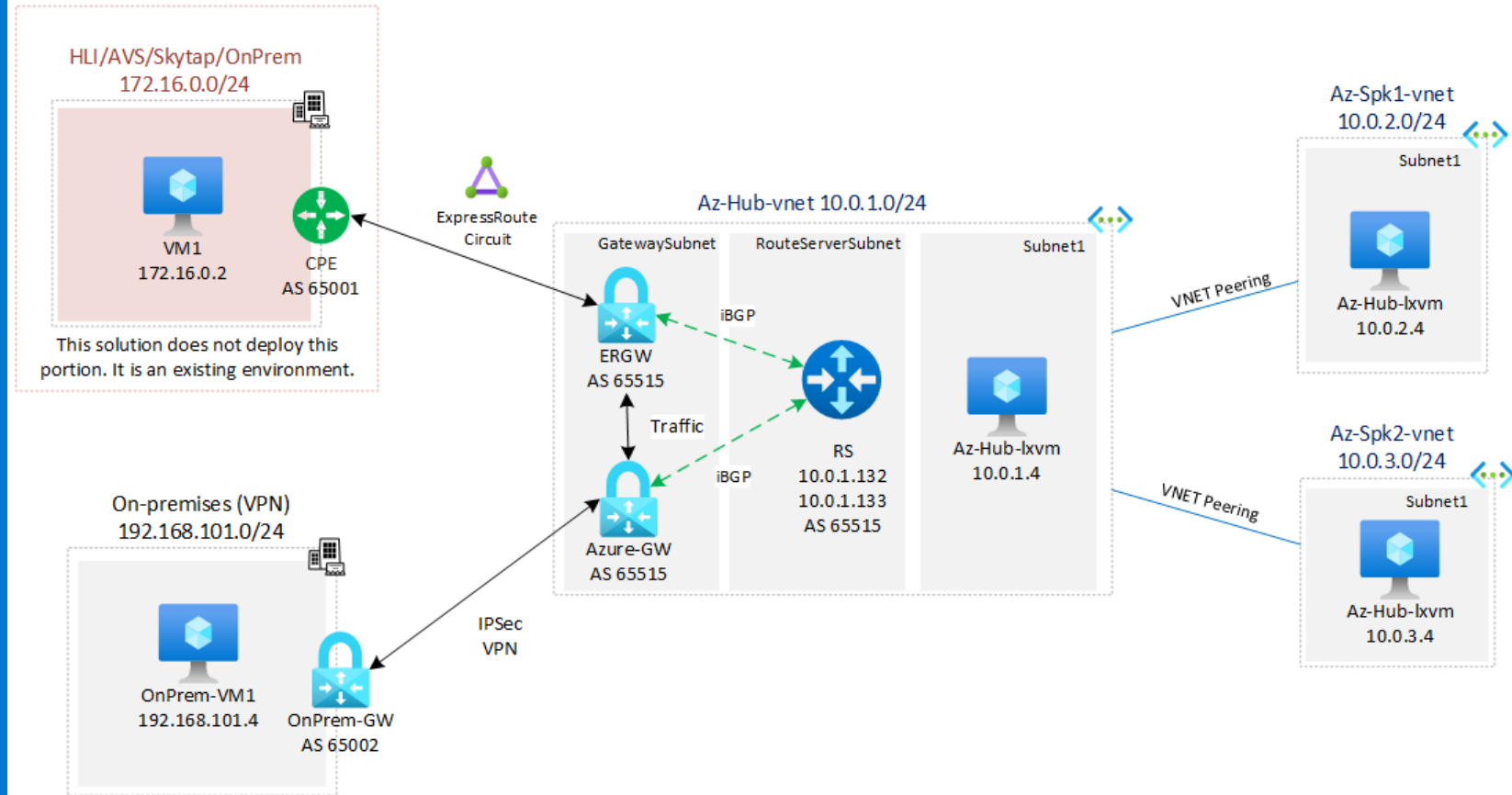
Integration with ExpressRoute



Network Topology & Connectivity

Azure Route Server

Azure Route Server Example Scenario



[Lab/RS-ER-VPN-Gateway-Transit at master · dmauser/Lab · GitHub](https://github.com/dmauser/Lab/tree/master/Lab/RS-ER-VPN-Gateway-Transit)



Network Topology & Connectivity

Segmentation

- Landing zone owners should be able to create subnets and manage Network Security Groups (NSGs)
- Use NSG flow logs and traffic analytics
- Use Application Security Groups (ASGs) for intra-vnet controls
- Inter-landing zone traffic can be NSG, Azure Firewall or NVA
- Deploy WAFs inside landing zones



Network Topology & Connectivity

Connectivity to Azure

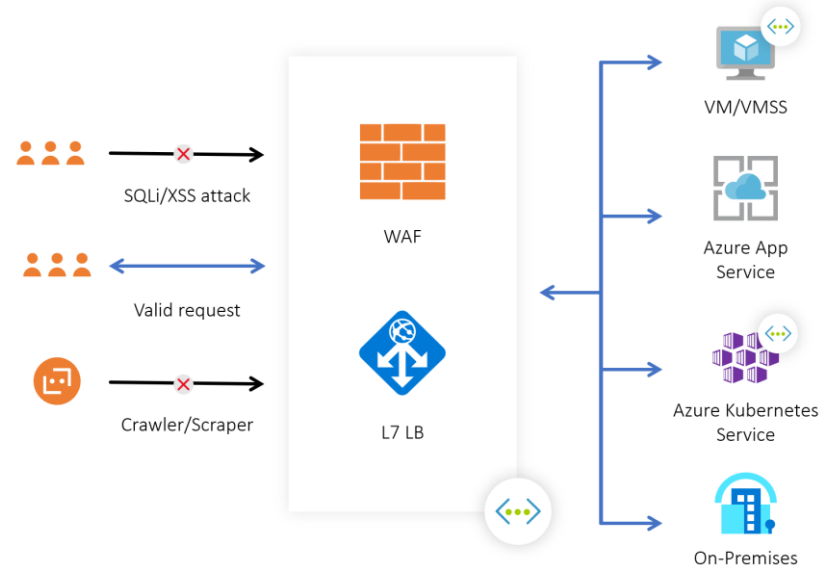
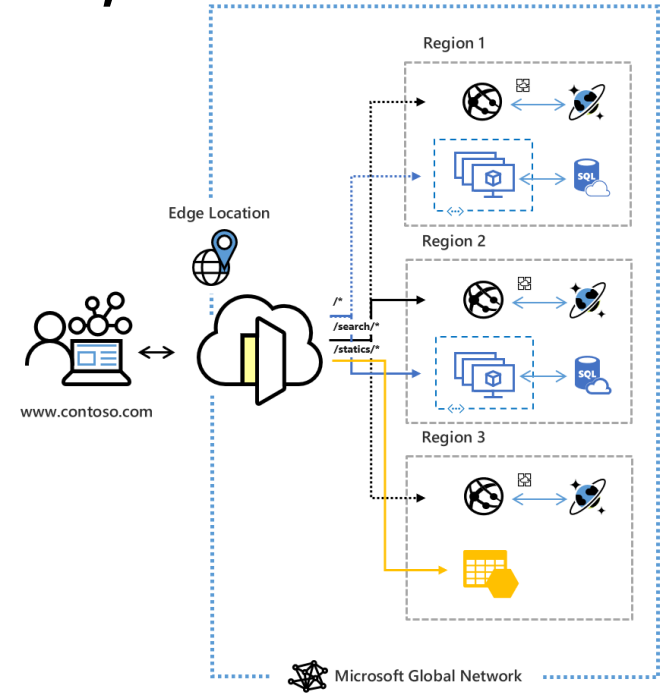
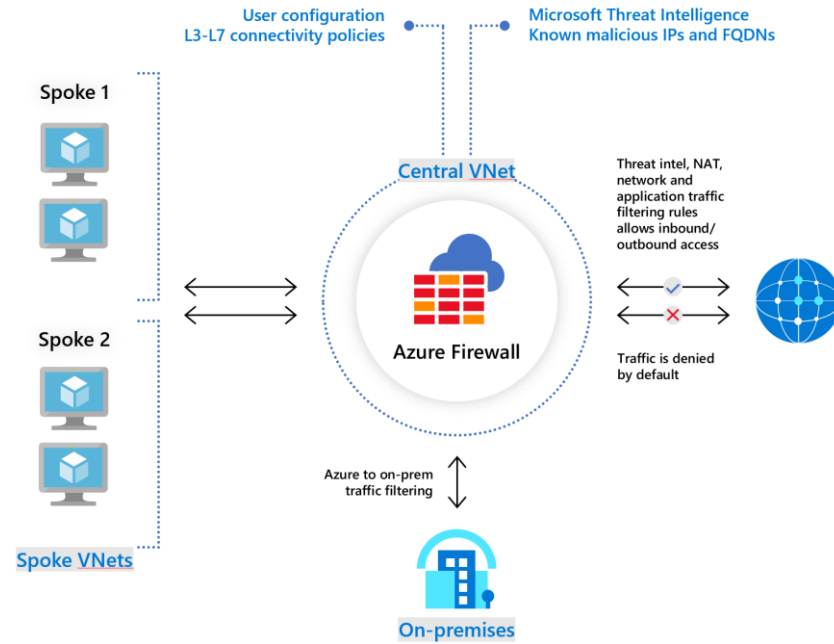
- Use ExpressRoute as the primary connectivity
- When over 10 Gbps is needed use ExpressRoute Direct
- Use multiple peering locations for resiliency
- Enable Fast Path to lower latency



Network Topology & Connectivity

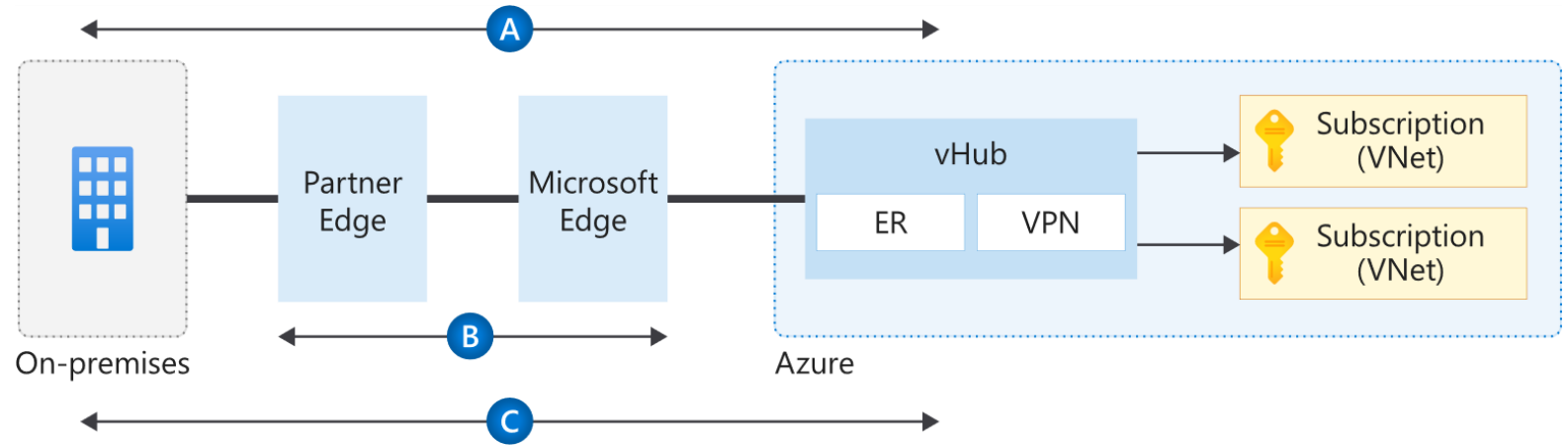
Internet Connectivity

Azure Firewall, Load Balancer, Front Door and Web Application Firewall





Network Topology & Connectivity



- VPN connection by using IPsec (A)
- Use MACsec for ExpressRoute Direct customers (B)
- IPsec over ExpressRoute private peering for virtual WAN (C)
- VNET to VNET VPN Gateways for inter-landing zone encryption

Encryption Options



Network Topology & Connectivity

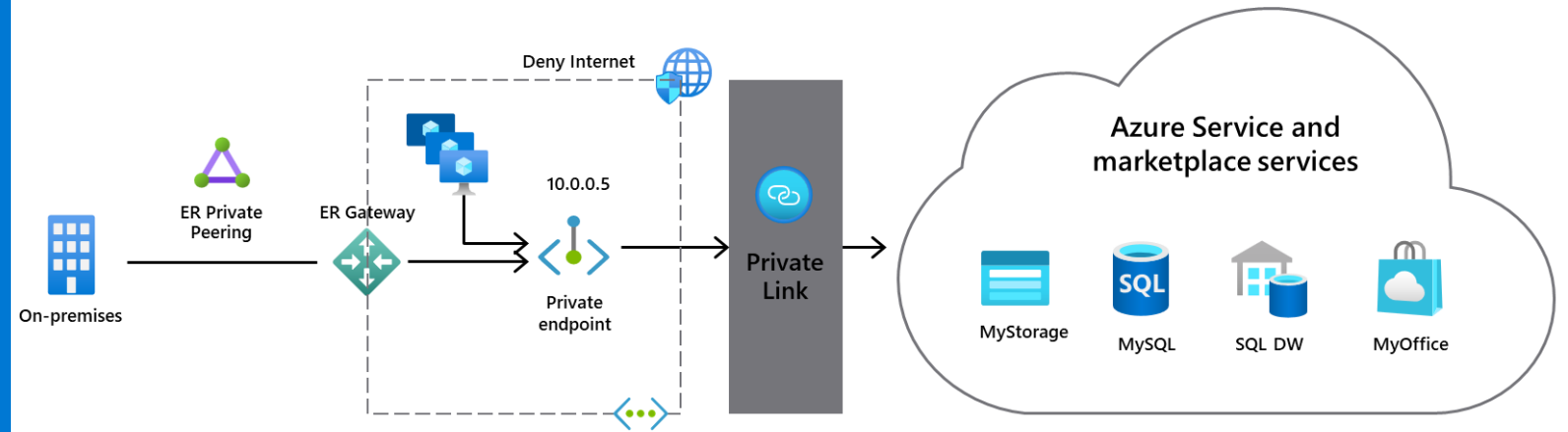
Traffic Inspection

- Use Network Watcher packets to capture despite the limited capture window.
- Evaluate whether the latest version of NSG flow logs provides the level of detail that you need
- Use partner solutions for scenarios that require deep packet inspection
- Don't develop a custom solution to mirror traffic. Complexity and supportability issues may arise.



Network Topology & Connectivity

Azure Private Endpoint & Private Link



Private Link for Azure Services

Private access from Virtual Network resources, peered networks and on-premise networks

In-built Data Exfiltration Protection

PaaS resources secured from public networks

Unified experience across PaaS, Customer Owned and marketplace Services

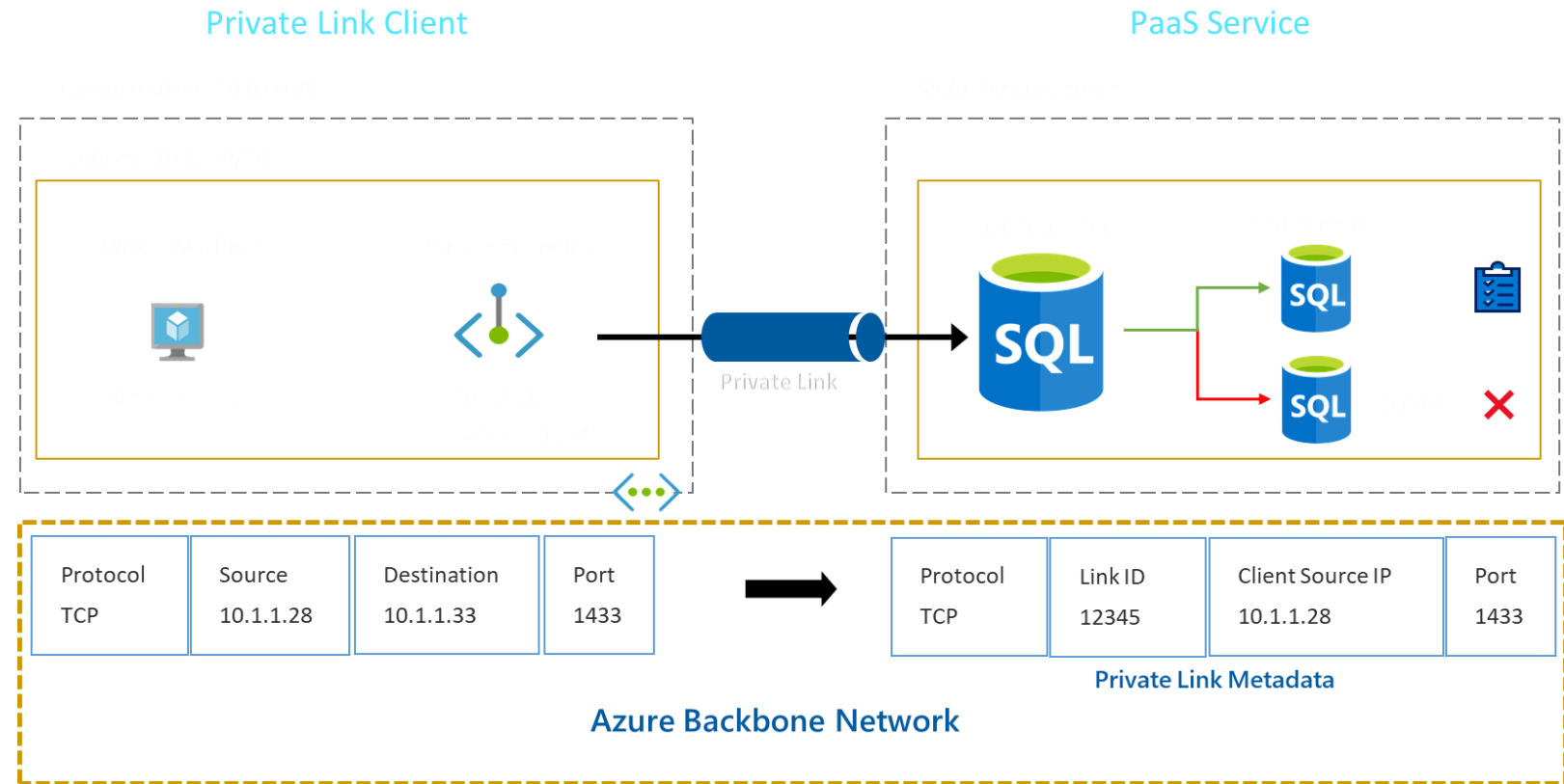
Connectivity to Azure PaaS



Network Topology & Connectivity

Connectivity to Azure PaaS

Azure Private Endpoint & Private Link





Network Topology & Connectivity

Reference Implementation

- Enterprise-scale design principles and implementation can be adopted by all customers, no matter what size and history their Azure estate.
- Reference implementations enable security, monitoring, networking, and any other plumbing needed for landing zones autonomously through policy enforcement.



[Enterprise-Scale Reference Implementation](#)

Deploy Reference Implementation

Reference implementation	Description	ARM Template	Link
Contoso	On-premises connectivity using Azure vWAN	Deploy to Azure	Detailed description
AdventureWorks	On-premises connectivity with Hub & Spoke	Deploy to Azure	Detailed description
WingTip	Azure without hybrid connectivity	Deploy to Azure	Detailed description
Trey Research	For small Enterprises	Deploy to Azure	Detailed description

Q & A

