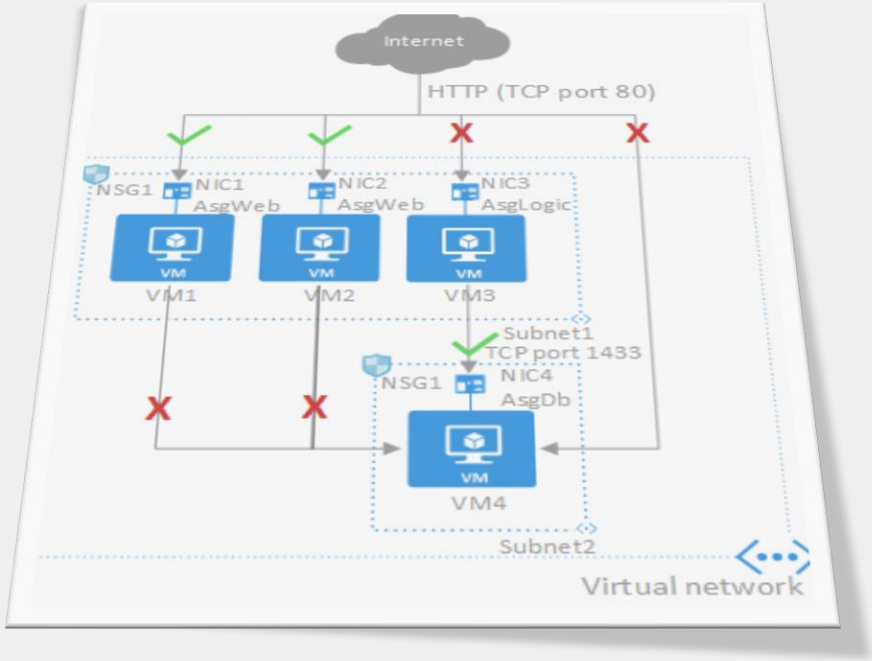
Microsoft

Azure Networking

Virtual Network

- Logical isolation with control over the network
- Create subnets and isolate traffic with network security groups
- Support for Static IP addresses
- Support for Internal Load Balancing
- DNS options – BYO or Microsoft Azure-provided
- Extend your trust boundary – VMs on the same Network

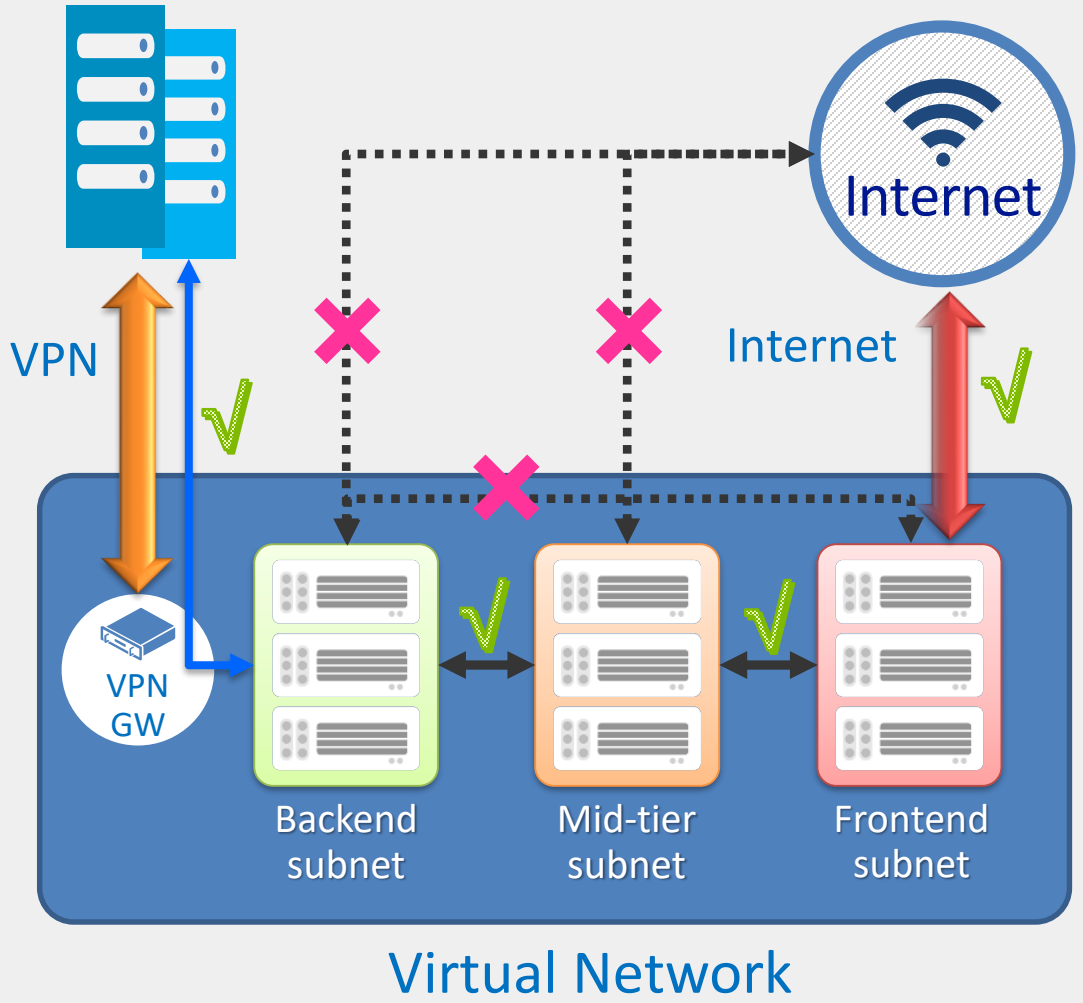


Connectivity within Azure

Cloud		Cloud	Characteristics
	VNet Peering		• Same-/cross-region direct, private VM-to-VM connectivity • NSG & UDR across VNets • GatewayTransit for hub-and-spoke
	VNet-to-VNet via Gateways		• Transitive routing via BGP and VPN gateways • Secure connectivity via IPsec/IKE across Azure WAN links

Network Security Groups (NSG)

- Enables network segmentation & DMZ scenarios
- Access Control List
  - Filter conditions with allow/deny
  - Individual addresses, address prefixes, wildcards
- Associate with network interfaces of VMs or subnets



Protecting your application

From the Internet

Within the VNet

Within Azure

Simplified Security Group Management

Network Security Groups (NSG)

IP based network ACL

Attach: Subnet and NICs

Service Tags

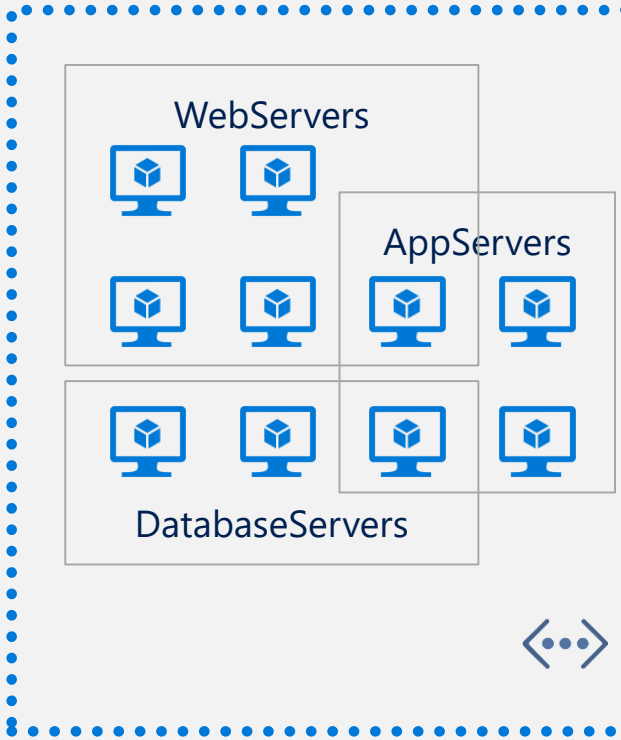
Named monikers for Azure service IPs

SQL, Storage, Traffic Manager supported

Application Security Groups (ASG)

Named monikers for custom grouping of VMs

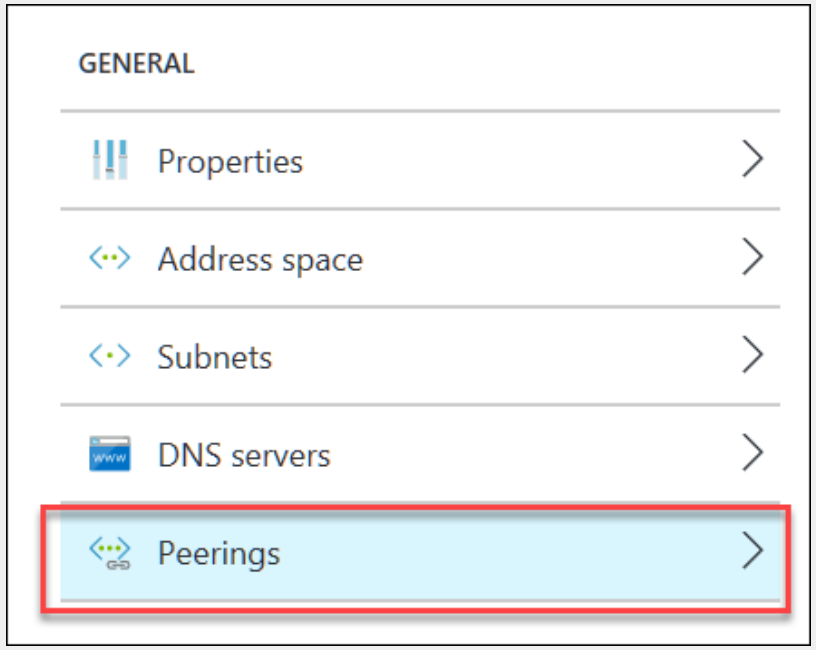
Natural expression of application security



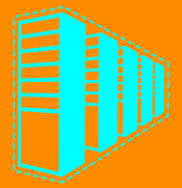
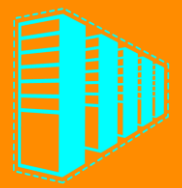
	Name	Source	Destination	Port
Allow	AllowInternetToWeb	Internet	WebServers	80,8080 (HTTP)
Allow	AllowAppToOnPrem	AppServers	10.10.128.0/22, 10.20.36.0/20, 192.168.65.0/20, 192.168.10.0/24	22, (SSH) 21, (FTP) 3389, (RDP) 3306 (MySQL)
Allow	AllowAppToExternalAPI	AppServers	148.234.0.0/16, 190.22.33.8/30	443 (HTTPS)
Allow	AllowDBServerToStorage	DatabaseServers	Storage	Any
Deny	DenyAll	Any	Any	Any

VNET Peering

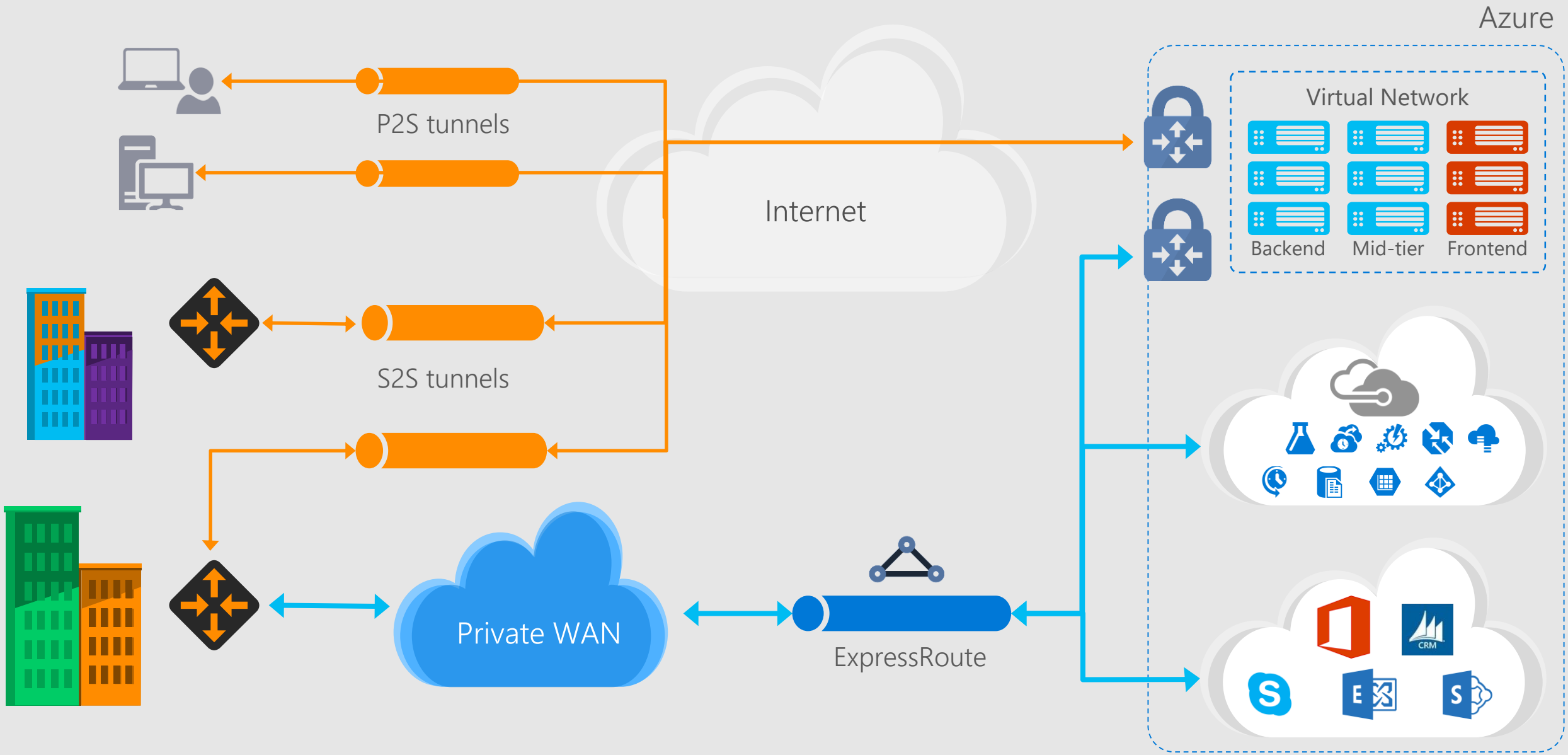
- Low-latency, high-bandwidth connection between VNETs
- Connect two VNETs
- Utilizes the Azure Backbone network
- No Encryption as traffic is isolated and on the MS backbone
- VNET address spaces cannot overlap
- VNET peering is between 2 VNETs
- VNETs can be in different subscriptions but in same Azure Tenant
- There is no virtual networks, and there is no derived transitive relationship
- Ability to use resources as transit points in a peered VNET



Connectivity to Azure

Cloud		Customer	Characteristics
	Internet Connectivity		• Internet facing with public IP addresses in Azure • DNS, load balancing, DDoS protection, WAF
	Remote access point-to-site connectivity		• Remote Access to VNet/On-prem • Connect from anywhere • Mac, Linux, Windows • Radius/AD authentication
	Site-to-site VPN connectivity		• High throughput, secure cross-premises connectivity • BGP, active-active for high availability & transit routing
	ExpressRoute private connectivity		• Private connectivity to Microsoft services (O365, Azure PaaS services) • Mission critical workloads

Cross-premises connectivity



Robust networking infrastructure services

Virtual Network

Provision private networks, optionally connect to on premise datacenters. NSG, User Defined Routes, & IP addresses.

Load Balancer

Deliver high availability and network performance to your applications

Application Gateway/WAF

Build scalable and highly-available web front ends in Azure

DDoS Protection

Protect your Azure resources from DDoS attacks

VPN Gateway

Establish secure, cross-premise connectivity

Azure DNS

Host your DNS domain in Azure

Content Delivery Network

Ensure secure, reliable content delivery with broad global reach

Traffic Manager

Route incoming traffic for high performance and availability

ExpressRoute

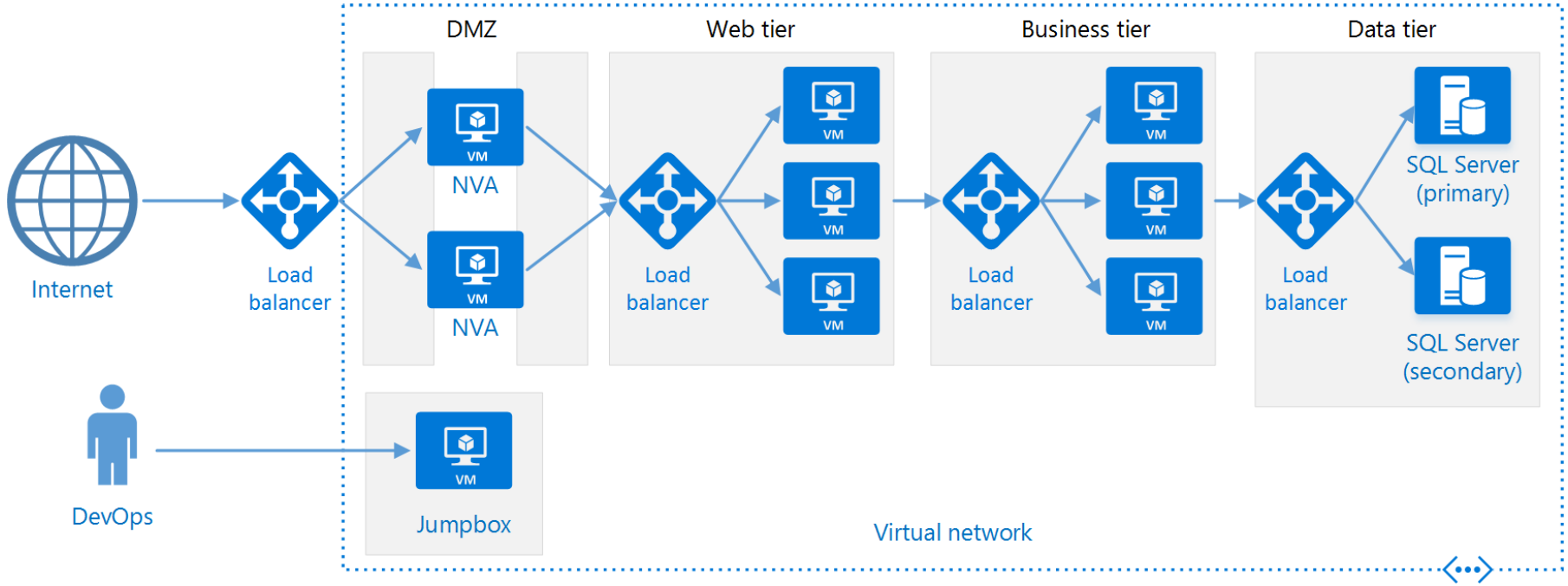
Dedicated private network fiber connections to Azure

Network Watcher

Network performance monitoring and diagnostics solution

Reference Architecture

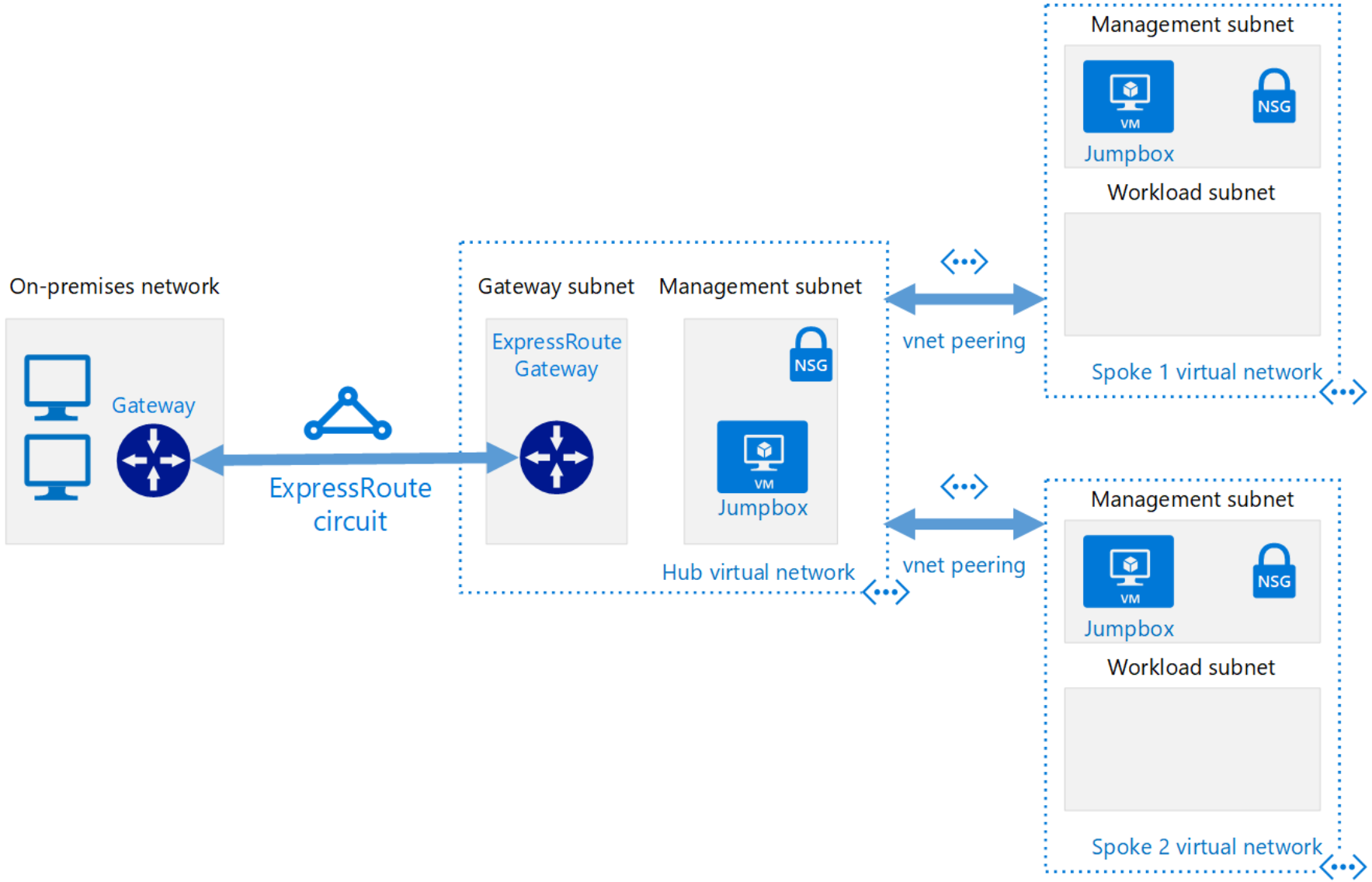
N-Tier Application



https://docs.microsoft.com/en-us/azure/architecture/guide/architecture-styles/n-tier

Reference Architecture

Hub & Spoke



https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke

Microsoft

Azure Networking Hands-On Lab

https://github.com/erjadi/TME-Enablement/tree/master/02.Networking