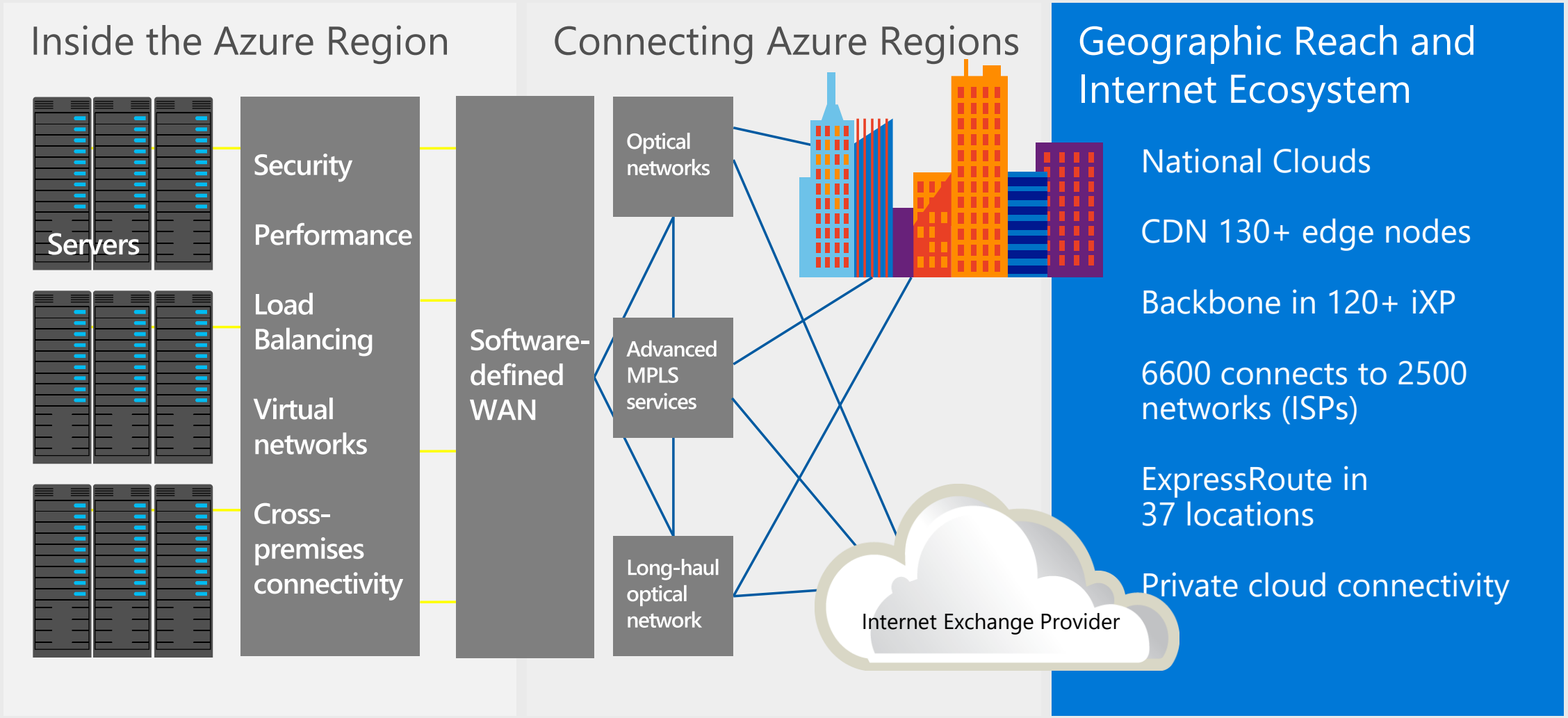
Azure Networking Essentials

Azure Networking Hyperscale



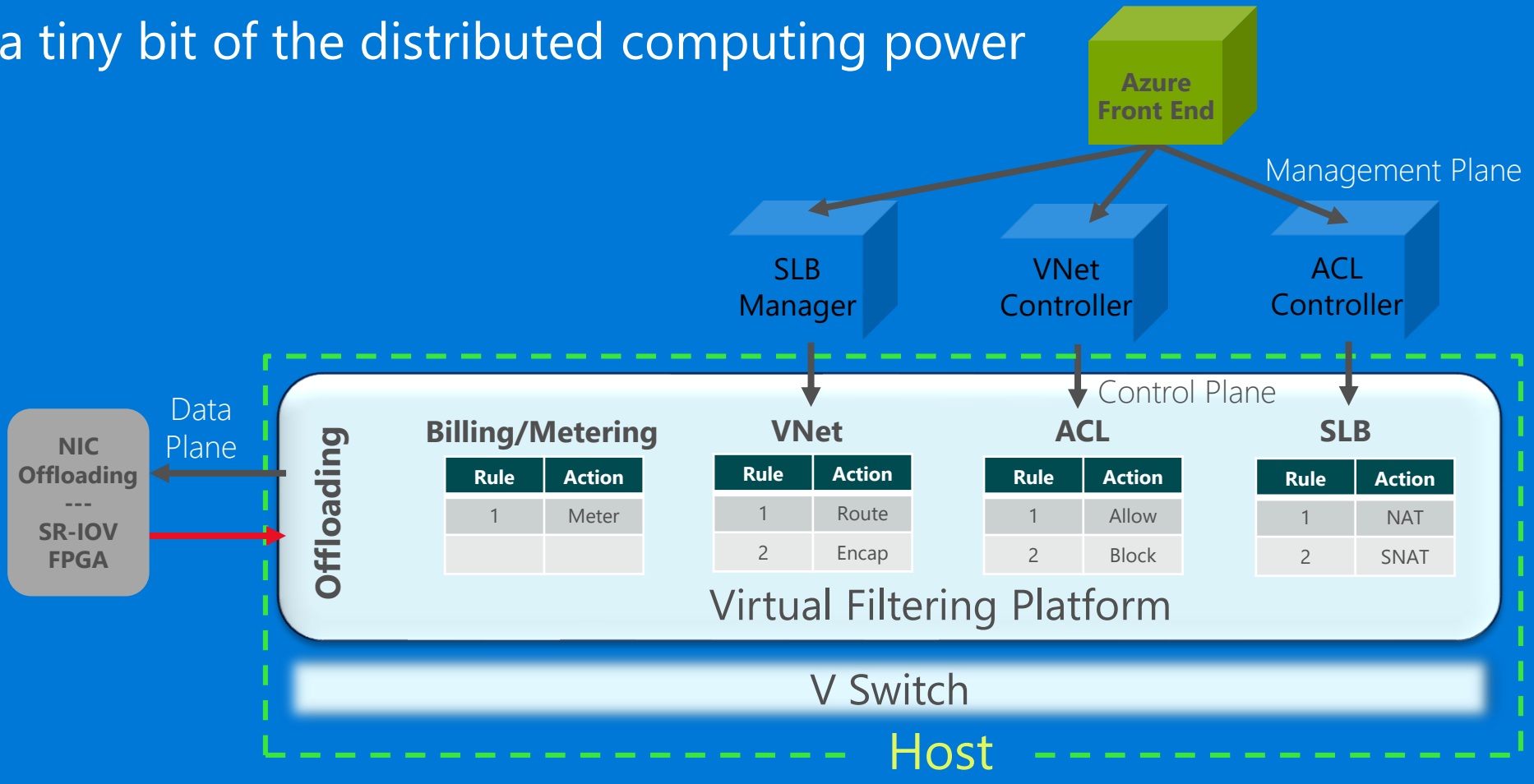
Key Concepts

- Virtual Network
- Network Load Balancing
- Application Load Balancing
- DNS
- Global Traffic Manager
- Connect to on-premises
- Virtual Data Center
- Asymmetric Routing

SDN on the Host

Applying billions of flow policy actions to packets

- Every host performs all packet actions for its own VMs
- Use a tiny bit of the distributed computing power

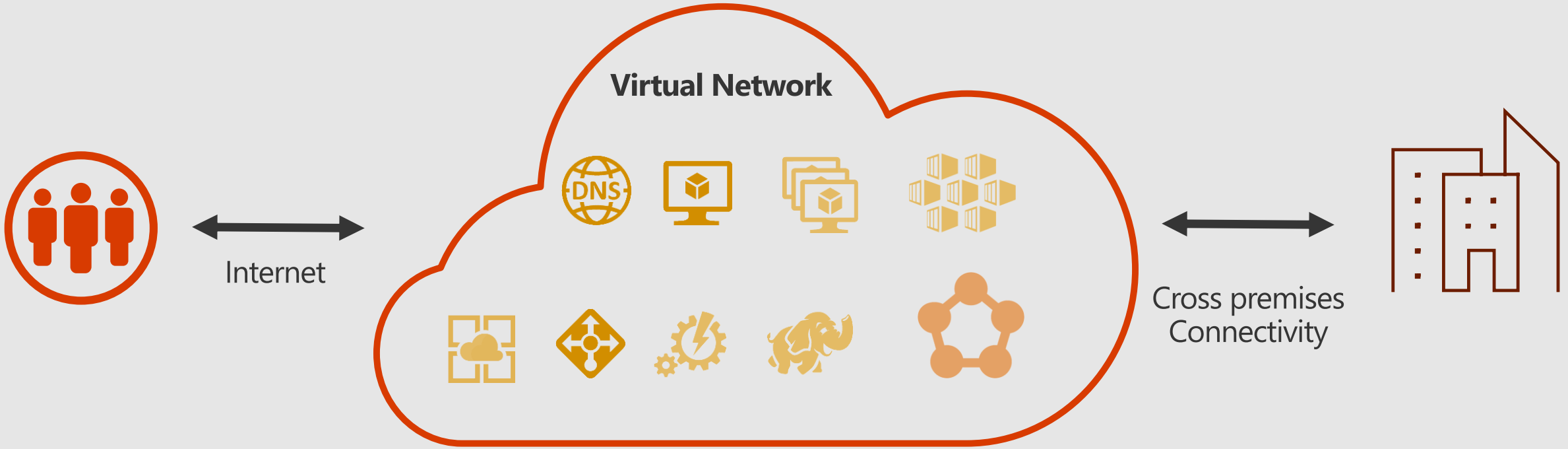


VNET

Azure Virtual Network

- Enables Azure resources like VM to communicate with each other, internet and on-premises
- Isolation and segmentation
  - Specify a private address space
  - Segment them address space into subnets
  - Provide name resolution
- Communicate with the internet
  - Outbound connectivity
  - Inbound connectivity (via Public IP address)
- Communicate between Azure Resources
  - Communicate via VNET
  - Virtual Network service endpoint

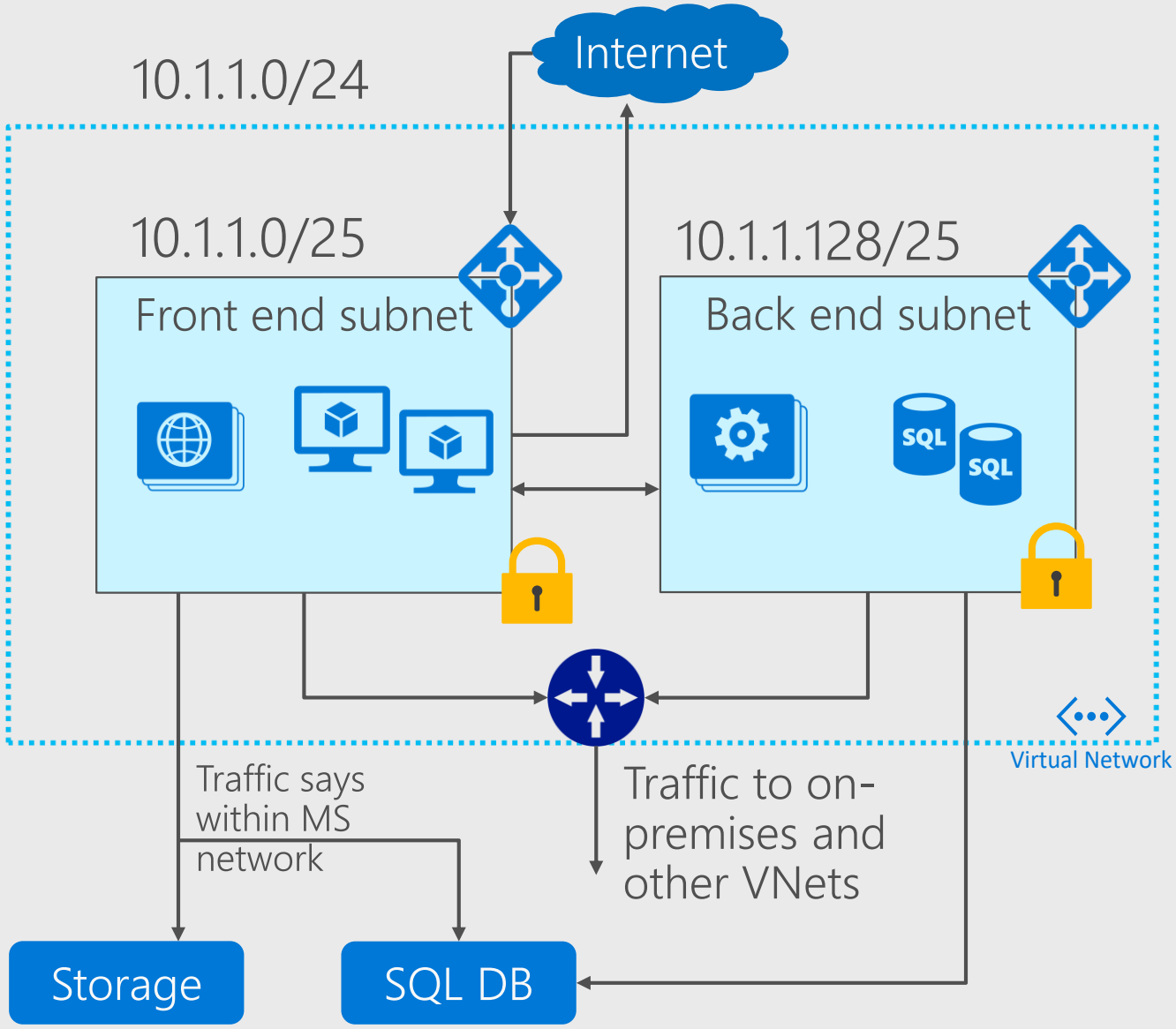
Your Network in Azure



Virtual Network

- Logical isolation of the public cloud
  - Define your address space
  - Divide address space into subnets
  - Isolate workloads. Configure fine grain policies
- Design for Scale
  - Connects VNets in a region using peering
  - Inter-connect VNets in other regions using ER
- Custom Security Policies
- Custom Routing Policies

- Template Driven
  - Click to deploy templates



Azure Virtual Network

- Communicate with on-premises resources
  - P2S VPN
  - S2S VPN
  - Azure Express Route
- Filter Traffic
  - Network Security Groups
  - Network Virtual Appliances
- Route Traffic
  - Route Tables
  - BGP Routes

Connecting VNETs

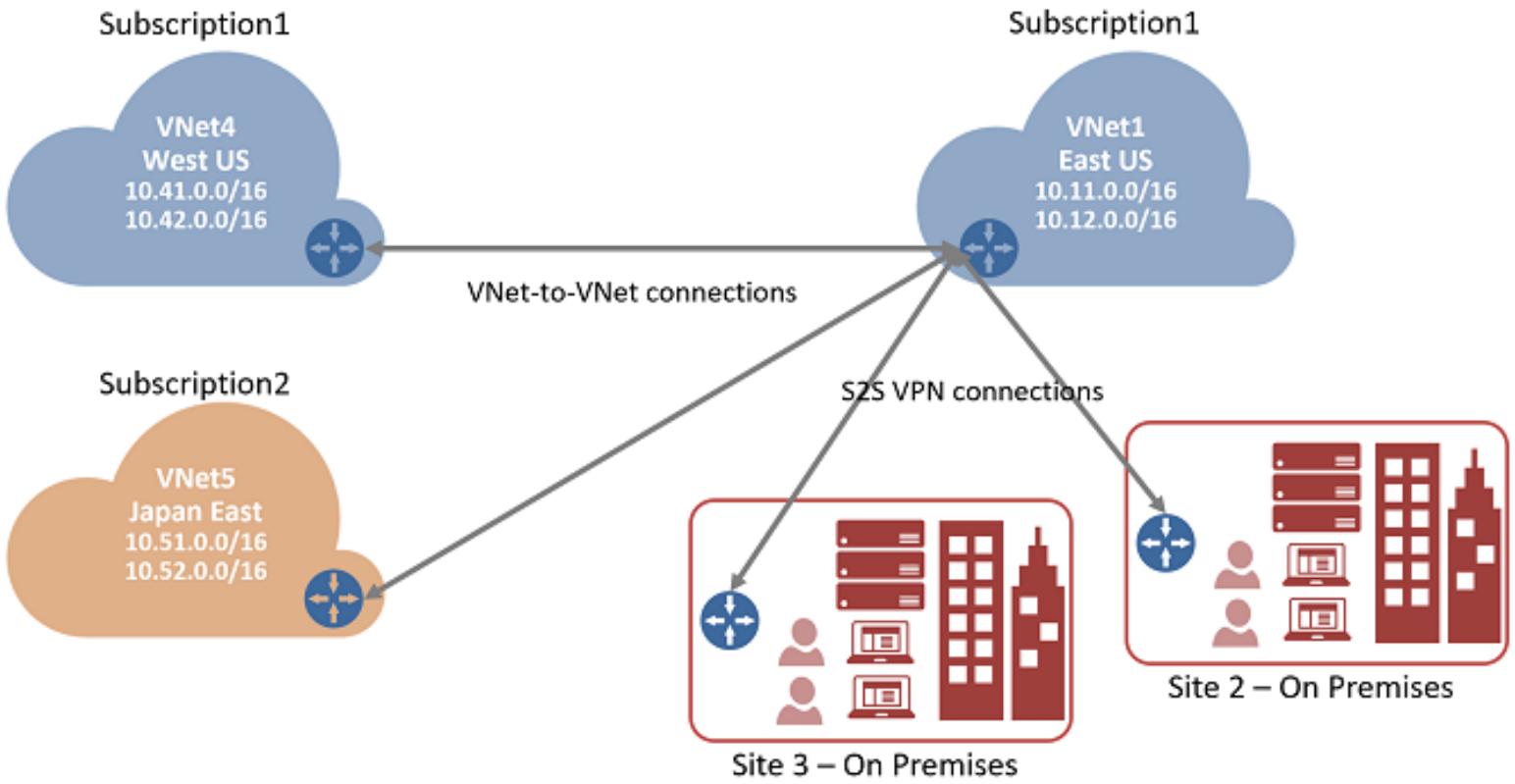
Connecting VNETs

- Cross region geo-redundancy
- Multi-tier application with isolation for each tier

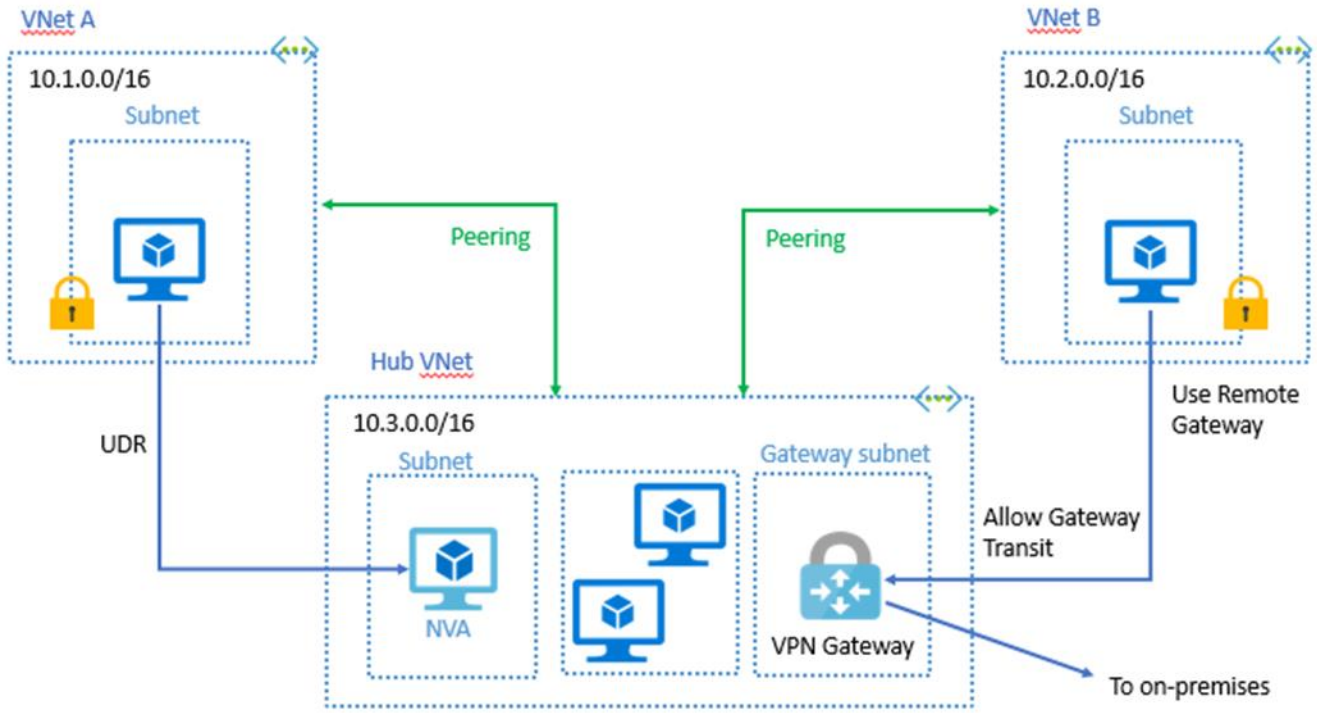
Connecting VNETs

- Peering
  - Connect with the same region (global peering now available)
  - Latency same as a VNET (within a region)
  - Traffic routed via Azure backbone
  - Create a user defined route to point to a resource in a peered VNET
- VPN Gateway
  - Traffic between VNETS flows via a VPN Gateway
  - Bandwidth limited by the VPN Gateway
  - You also create a Site to Site VPN between VNETS

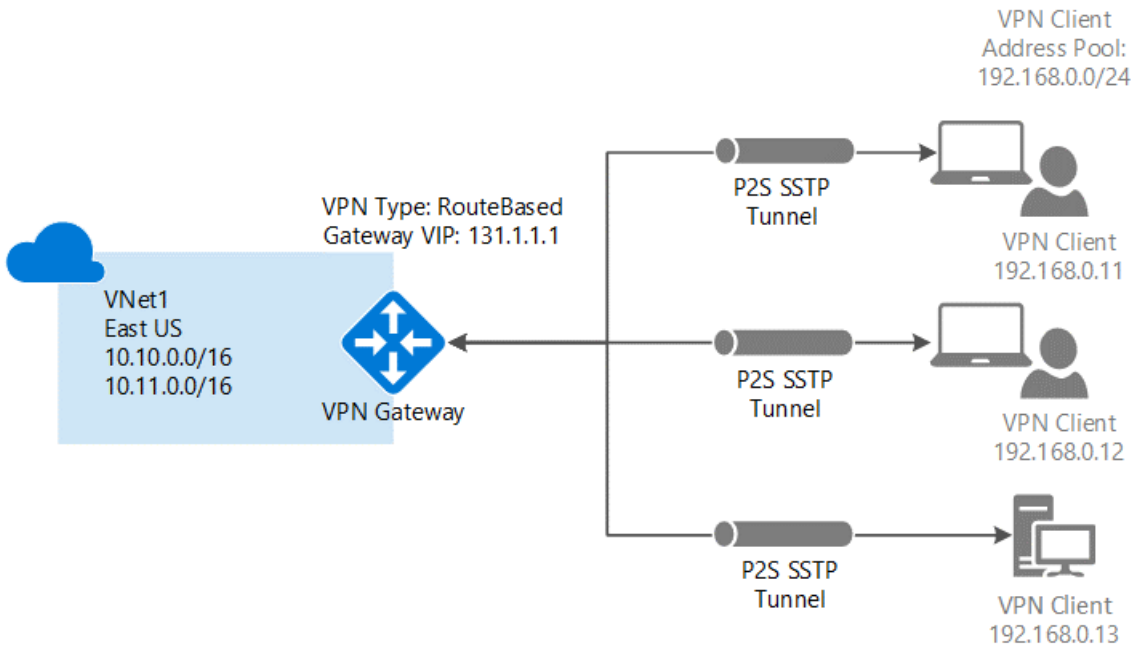
VNET-to-VNET and on premises connectivity



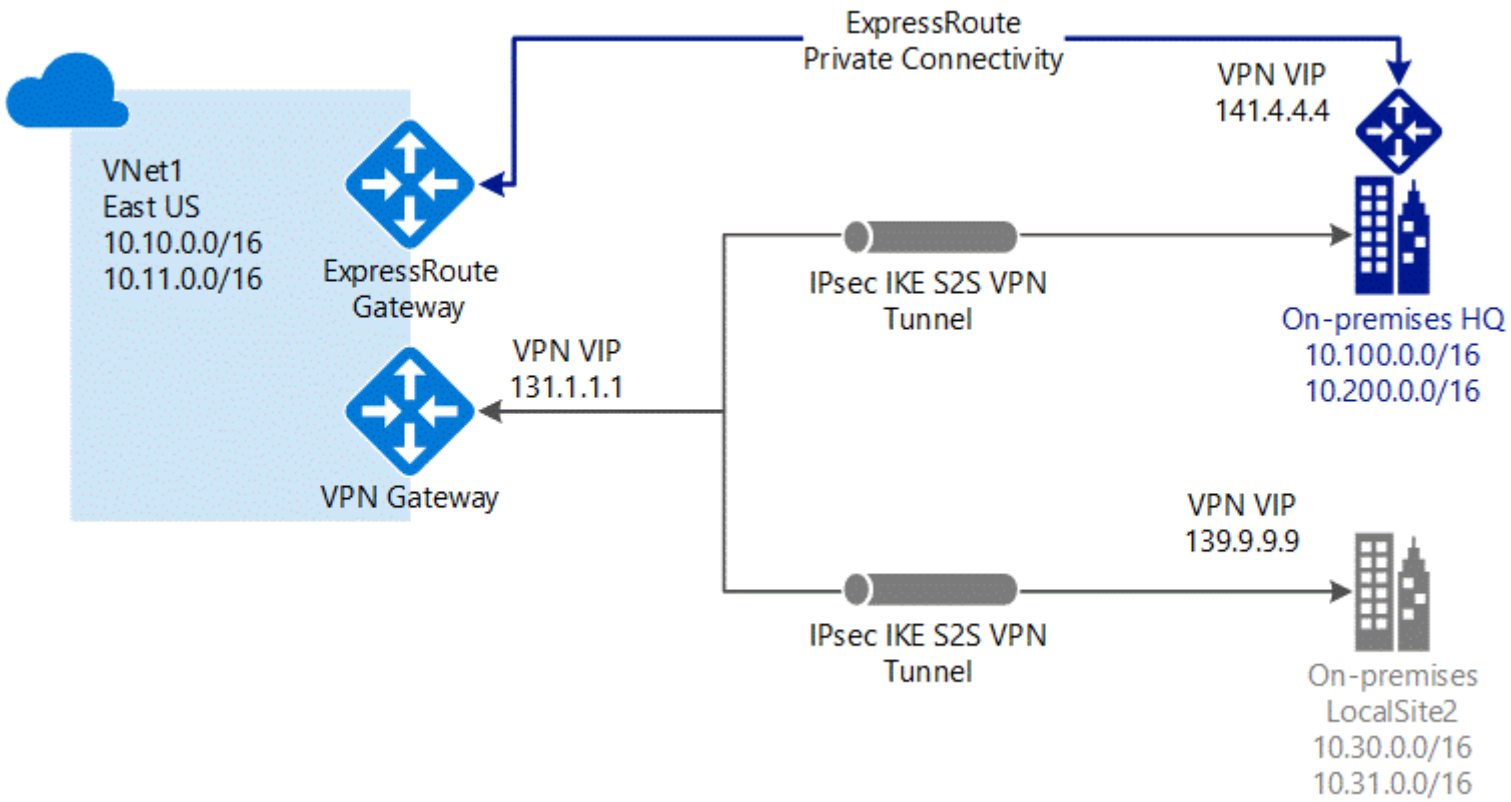
Gateway and Peering



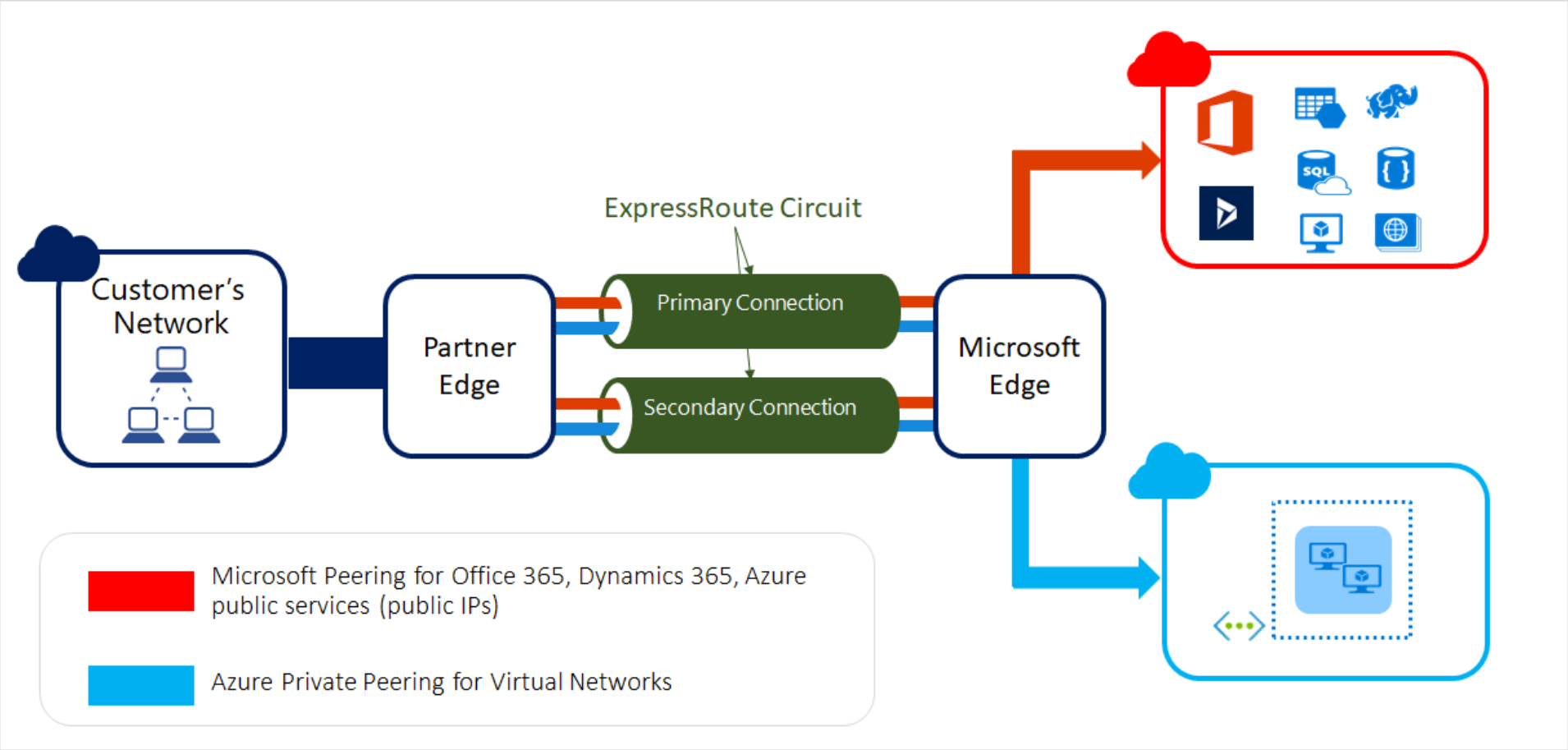
Point-to-Site (VPN over SSTP)



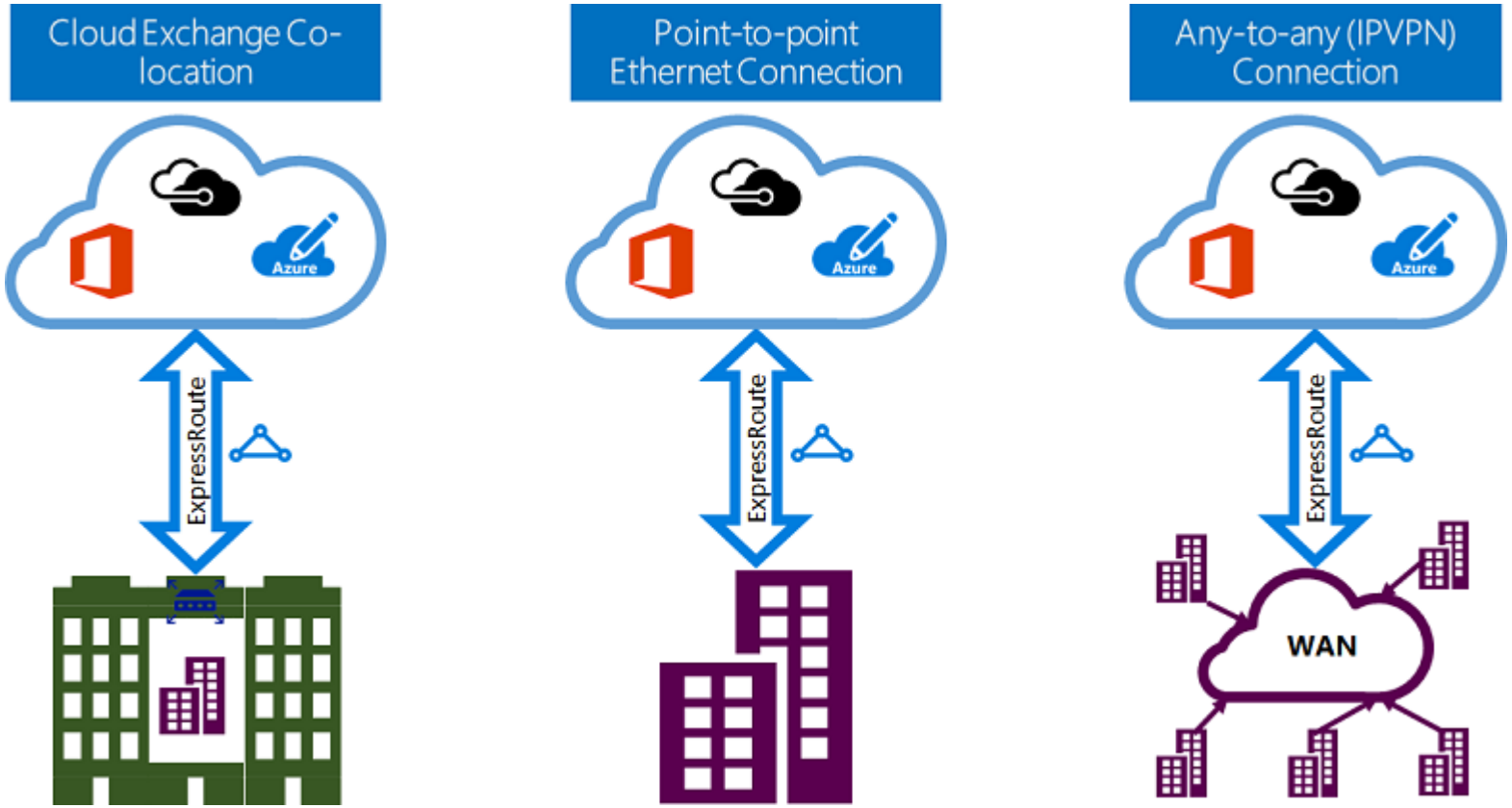
ExpressRoute (dedicated private connection)



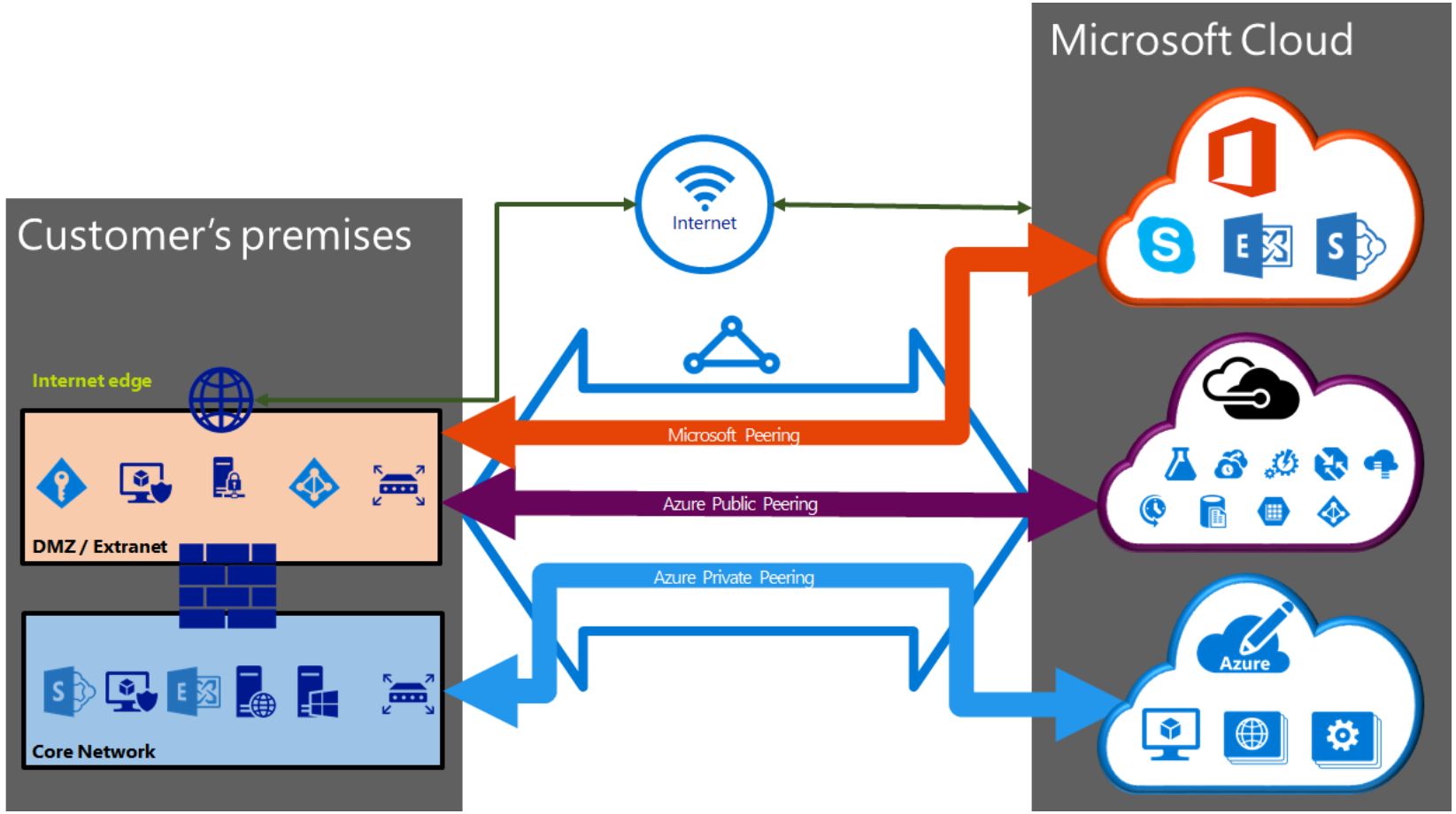
ExpressRoute (dedicated private connection)



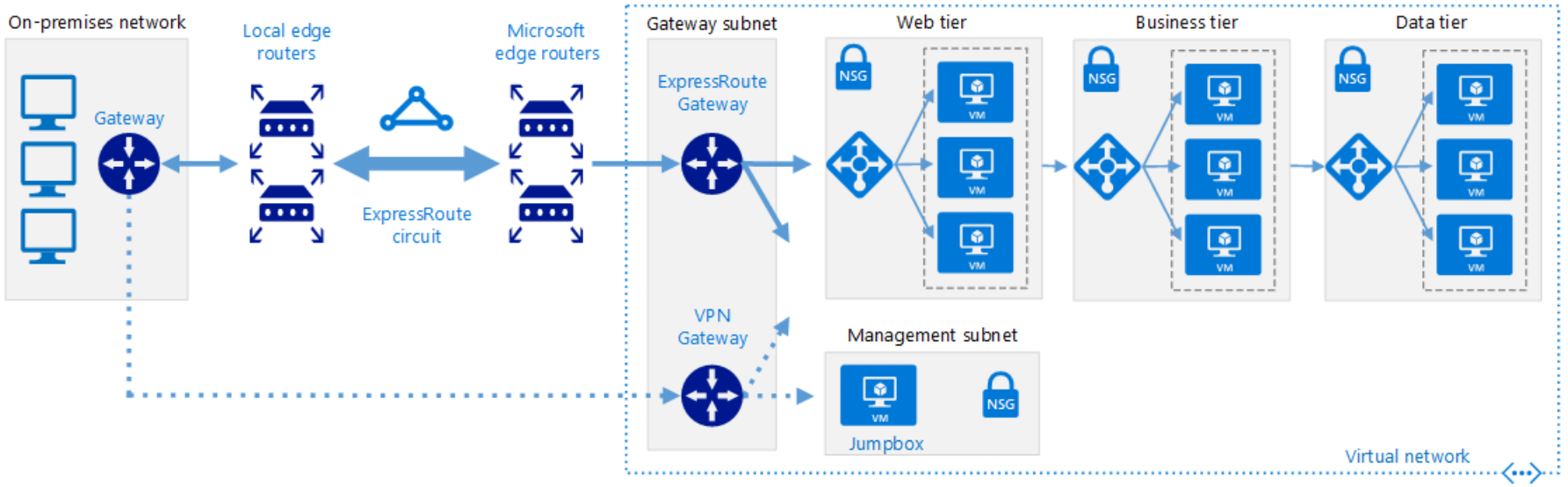
Express Route Models



ExpressRoute Routing Domains



ExpressRoute with failover



Why ExpressRoute?

- Layer 3 connectivity
- Connectivity to Microsoft cloud services across all regions in the geopolitical region (Azure, O365, Dynamics 365)
- Global connectivity to Microsoft services across all regions with ExpressRoute premium add-on (Azure Regions)
- Dynamic routing between your network and Microsoft over industry standard protocols (BGP).
- Built-in redundancy in every peering location for higher reliability.

When to use what?

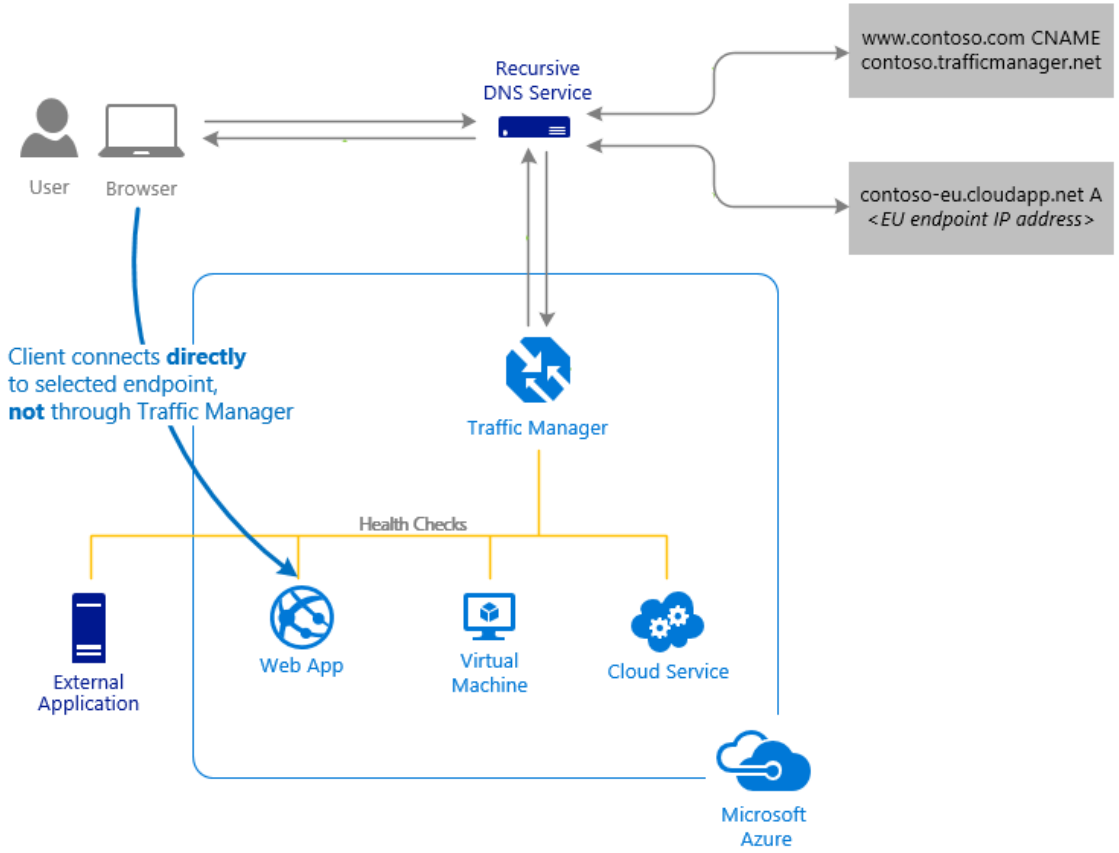
	Point-to-Site	Site-to-Site	ExpressRoute
Azure Supported Services	Cloud Services and Virtual Machines	Cloud Services and Virtual Machines	Services list
Typical Bandwidths	Typically < 100 Mbps aggregate	Typically < 1 Gbps aggregate	50 Mbps, 100 Mbps, 200 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps
Protocols Supported	Secure Sockets Tunneling Protocol (SSTP)	IPsec	Direct connection over VLANs, NSP's VPN technologies (MPLS, VPLS,...)
Routing	RouteBased (dynamic)	We support PolicyBased (static routing) and RouteBased (dynamic routing VPN)	BGP
Connection resiliency	active-passive	active-passive or active-active	active-active
Typical use case	Prototyping, dev / test / lab scenarios for cloud services and virtual machines	Dev / test / lab scenarios and small scale production workloads for cloud services and virtual machines	Access to all Azure services (validated list), Enterprise-class and mission critical workloads, Backup, Big Data, Azure as a DR site

Load Balancers

Azure Traffic Manager

- DNS based global load balancing. Routing methods
  - Geographic
  - Performance
  - Priority
  - Weighted round-robin

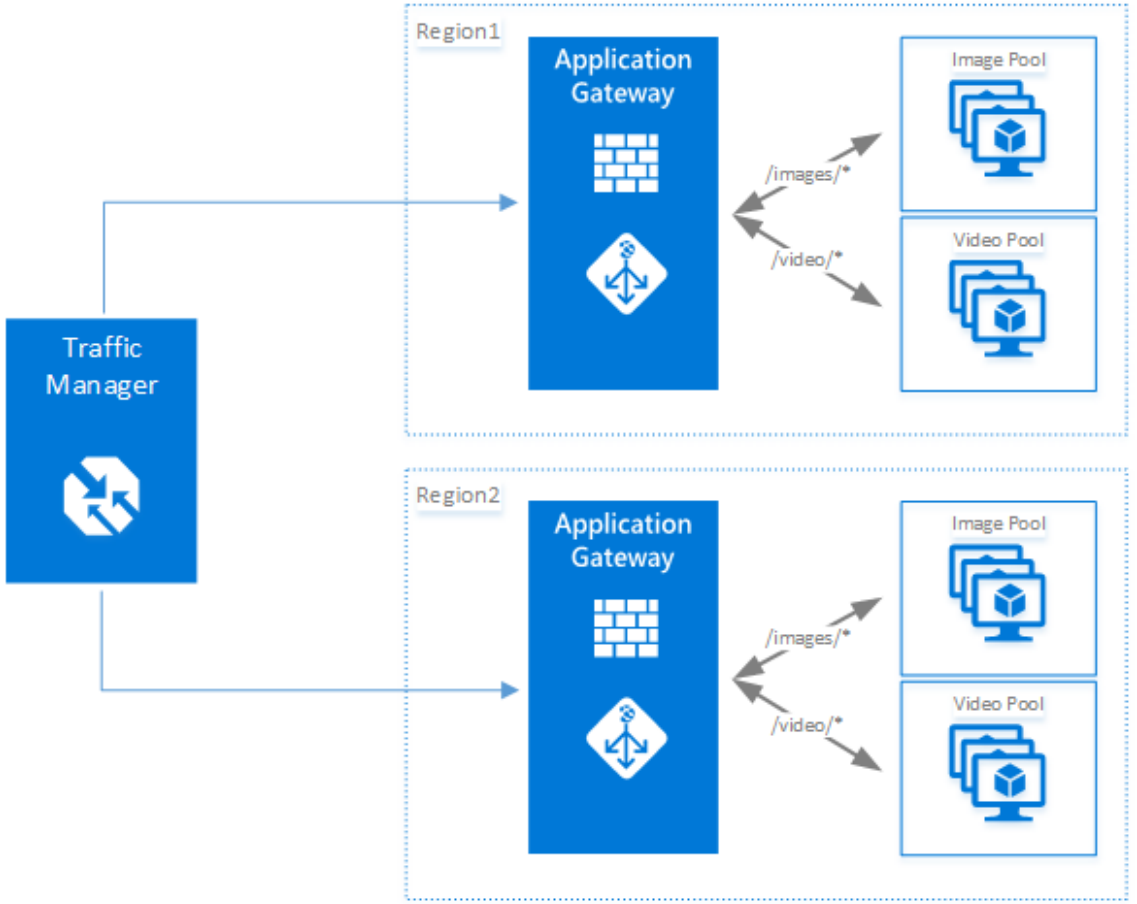
Azure Traffic Manager



Application Load Balancing

- Application Gateway
- Layer 7 service
- Routing
  - Cookie based, round-robin, URL path-based etc
- Offload SSL termination
- Fully Managed service

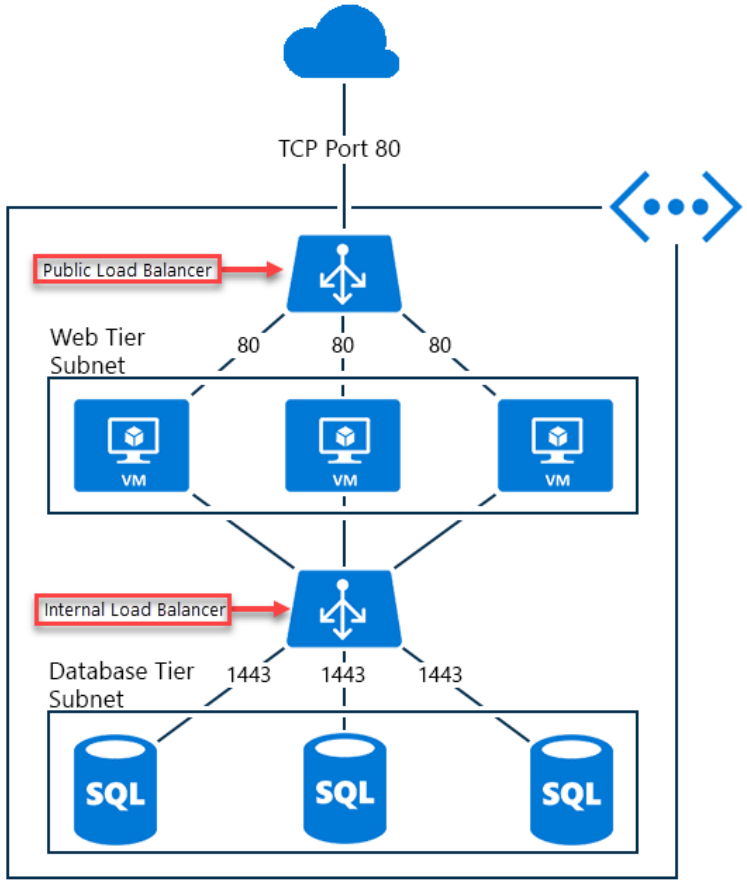
Application Gateway



Network Load Balancing

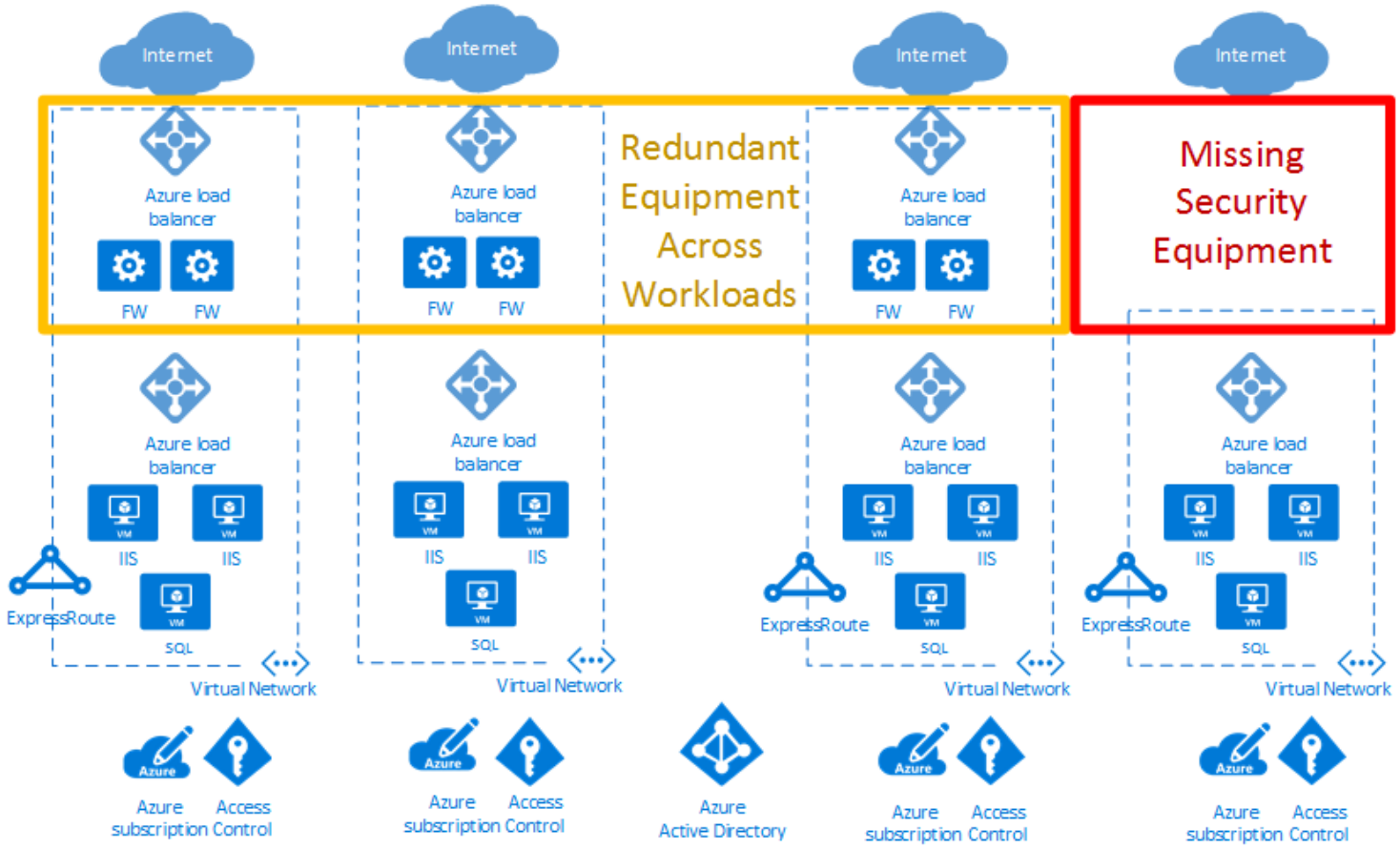
- Low-latency Layer 4 load balancing (TCP and UDP)
- Public or internal load-balanced endpoints
- Port forwarding (RDP to a VM)
- Outbound connectivity (SNAT)
- Health probes
- No SSL Termination
- Automatic reconfiguration (when you add VMs to the Pool)
- Standard and Basic SKU
- SLA 99.99%

Network Load Balancing



Virtual Data Center

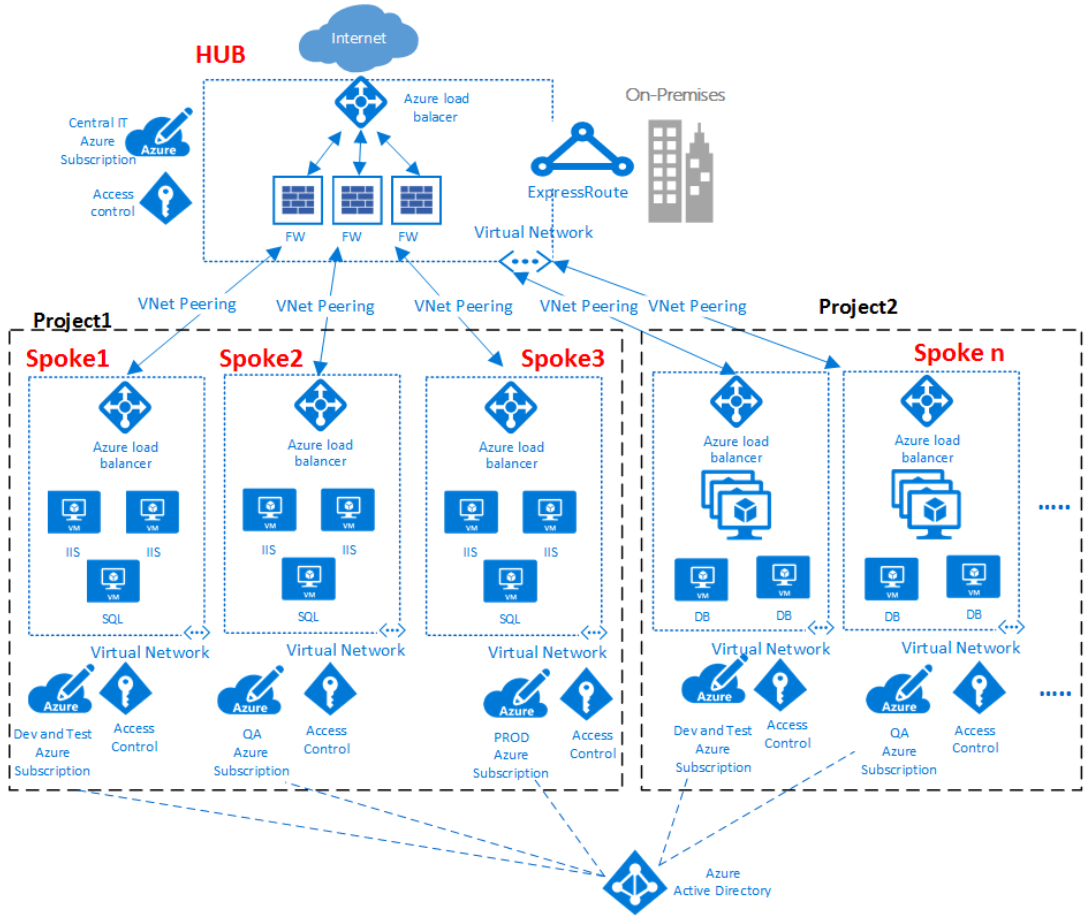
Why Virtual Data Center?



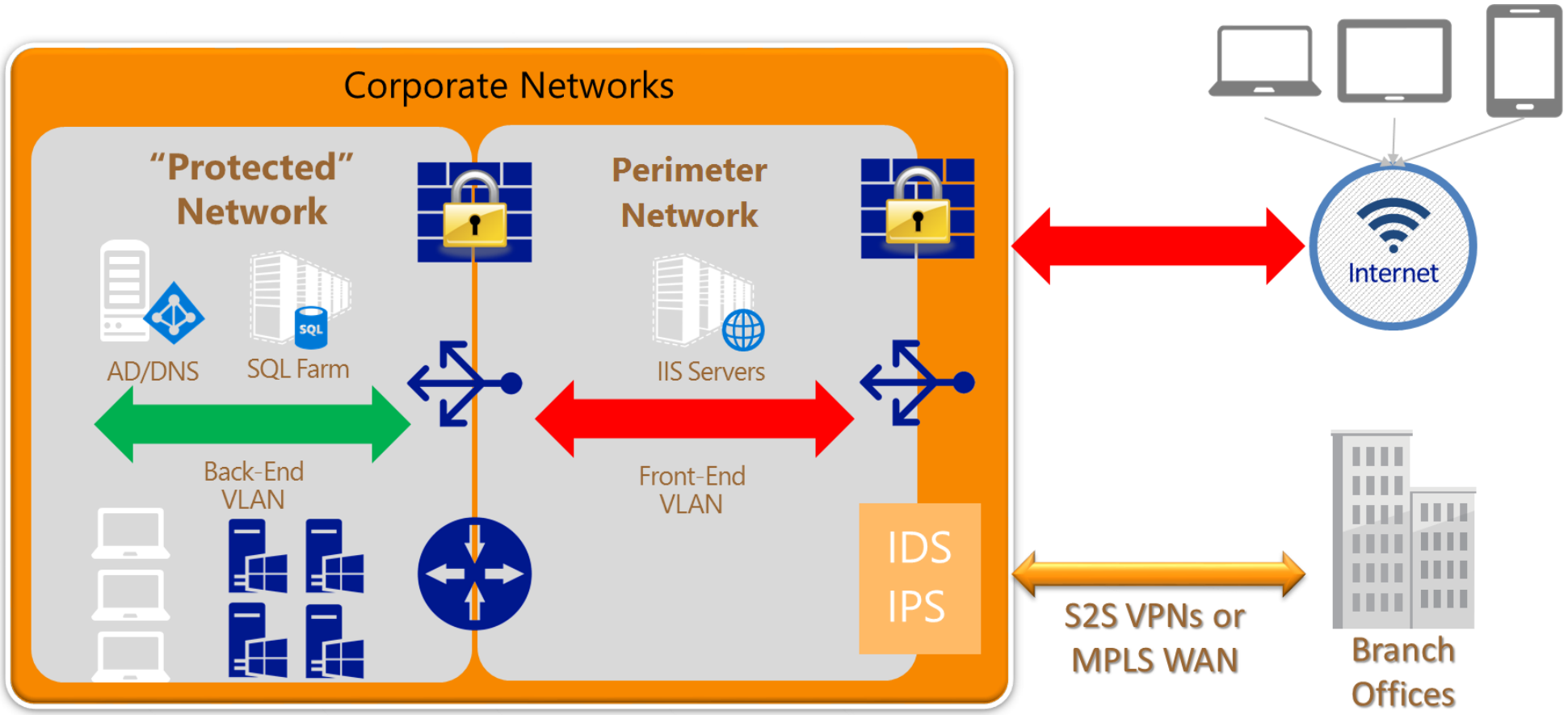
Virtual Data Center

- Going beyond a single application in the cloud to multiple applications
- Share infrastructure
  - Identity (Directory Services)
  - Security (Azure MFA, Crypto)
  - Connectivity (to and within cloud)

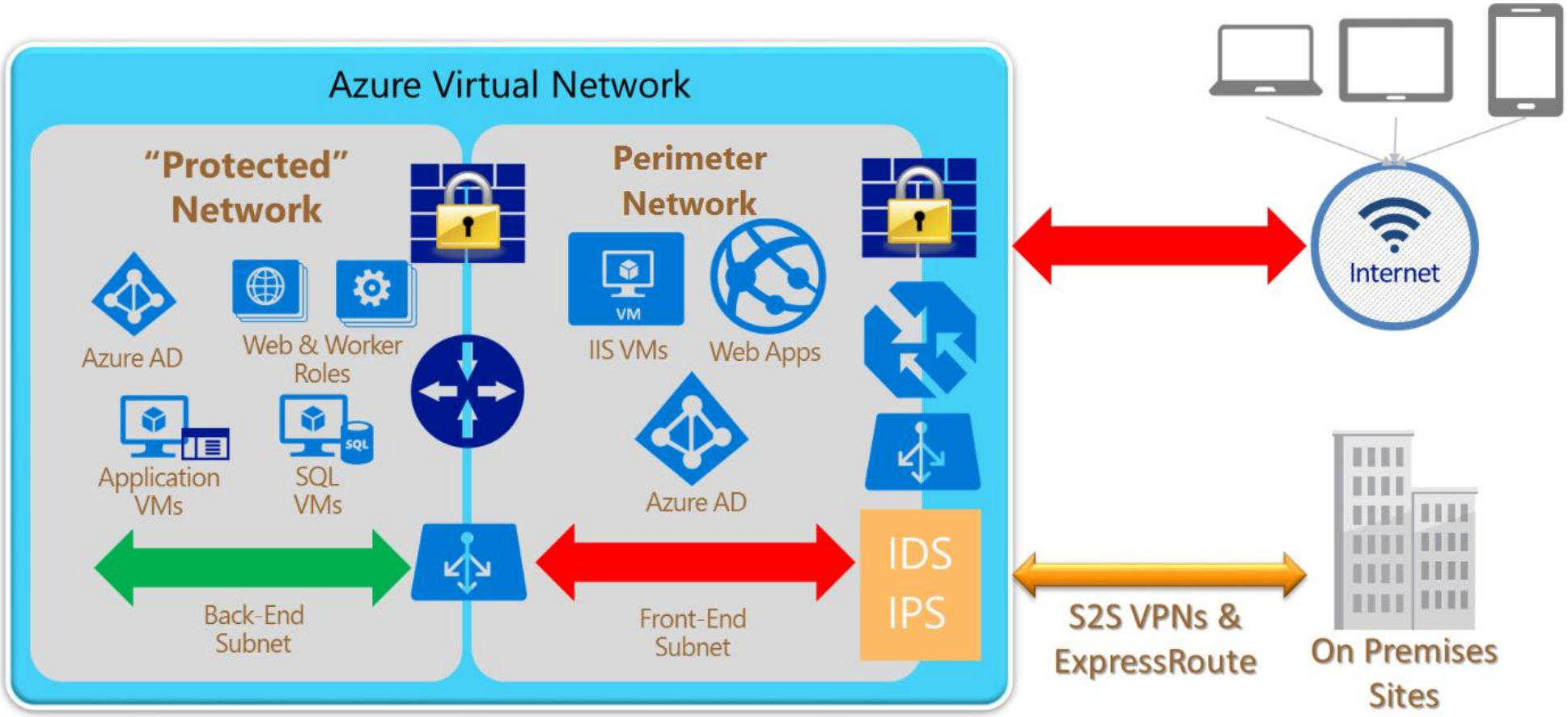
Virtual Data Center



Corporate Network



Azure Virtual Datacenter



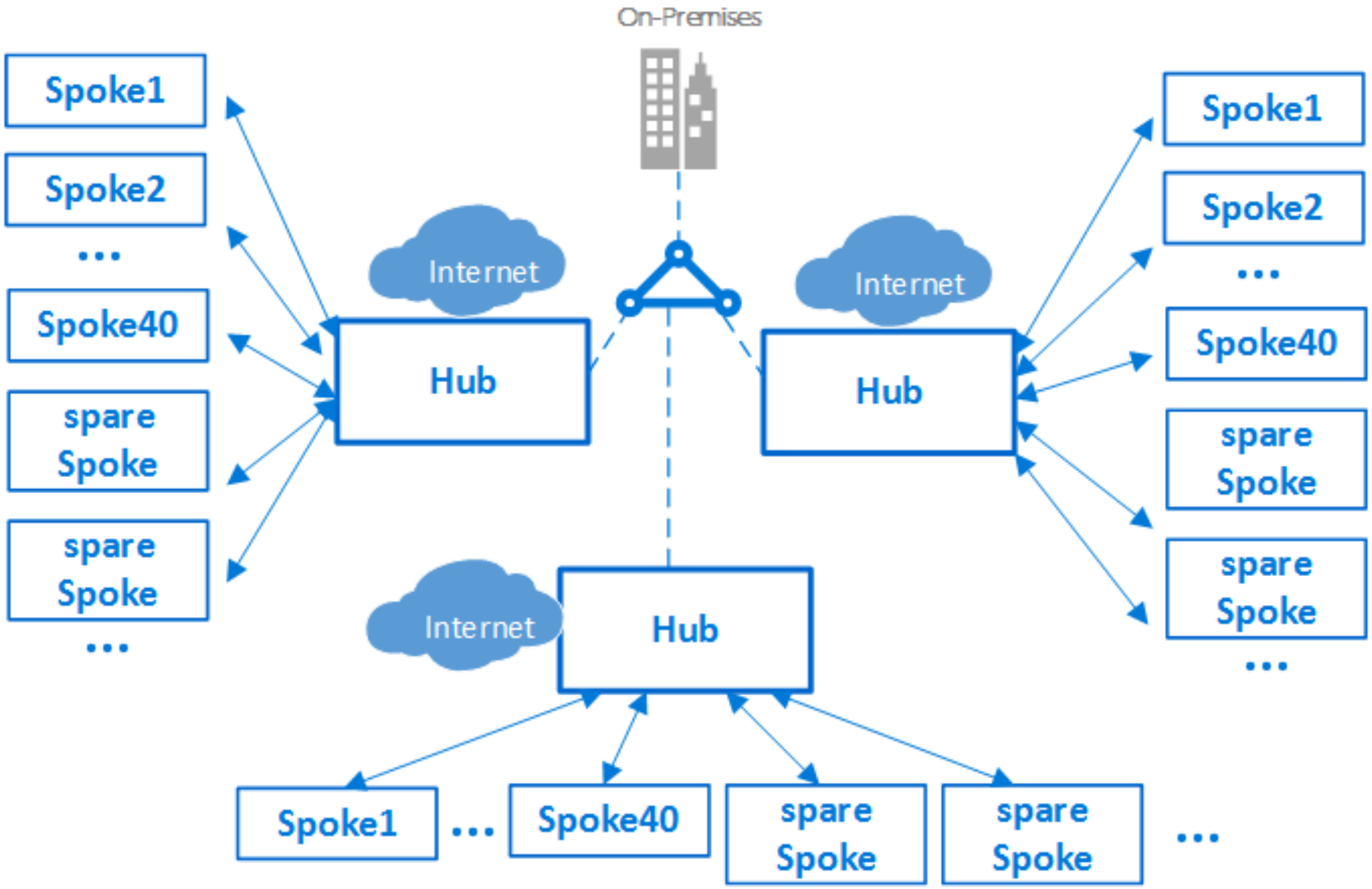
Hub and Spoke Architecture

HUB

- Centrally managed infrastructure
- Hosts Firewall, ExpressRoute, ADC

SPOKE

- Application centric
- Developer controlled
- Peer to Hub for IT services



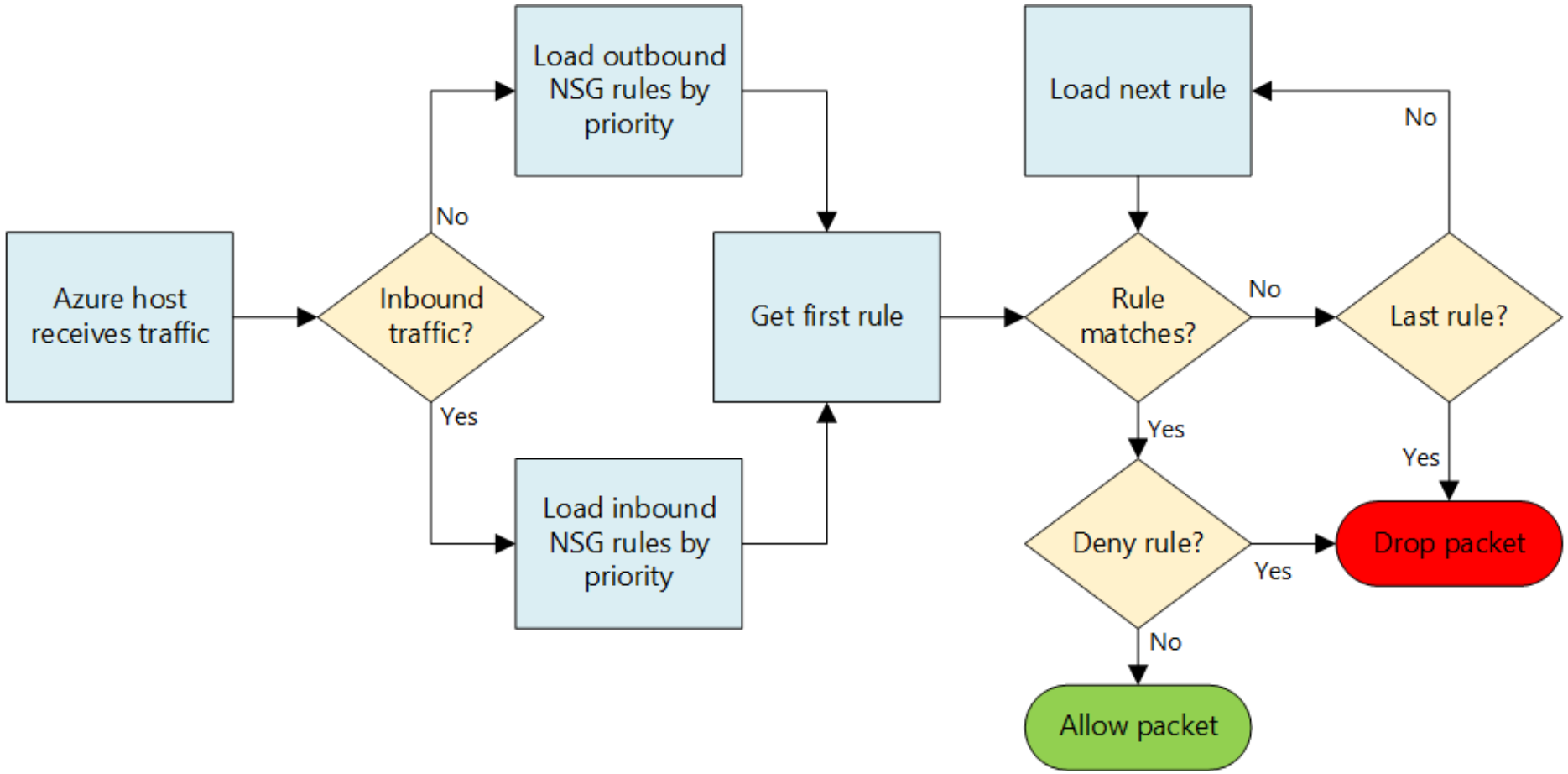
Traffic Filtering

NSGs NVA

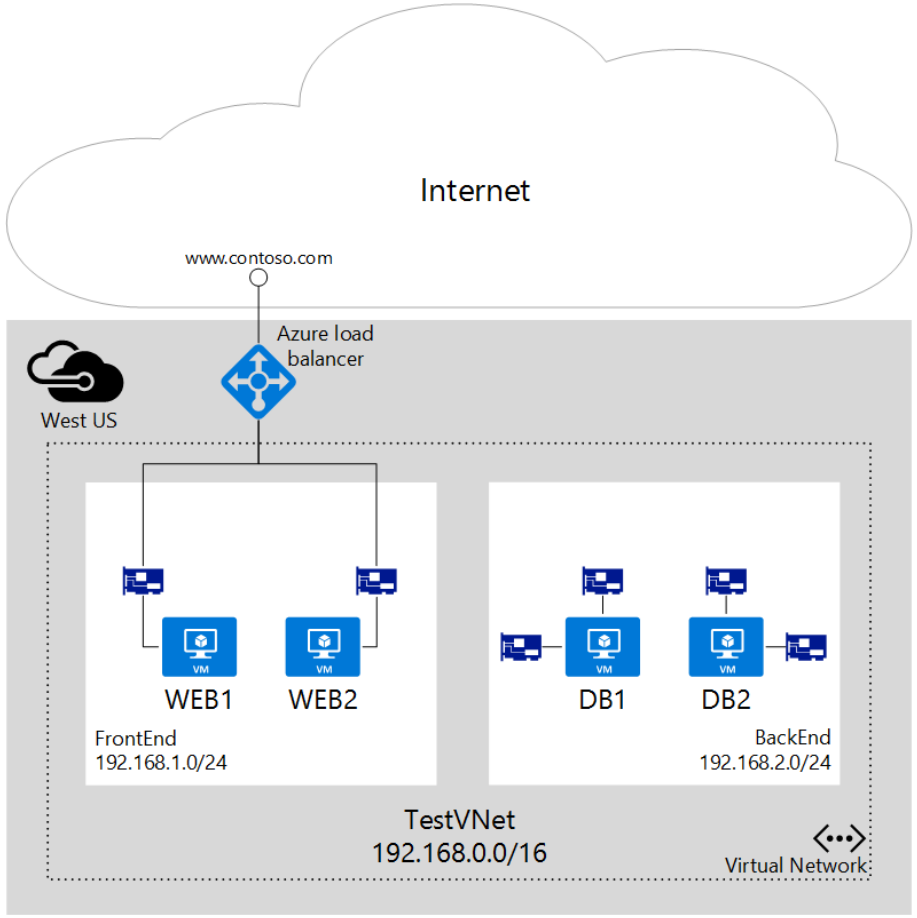
Network Security Group (NSG)

- Filter inbound and outbound traffic to Azure resources
- Each NSG contains one or more inbound and outbound rules
- Each rule specifies the source IP addresses, destination IP addresses, port, and protocol that traffic is filtered with.
- NSGs can be associated to subnets or individual VMs
- There are limits to NSGs (good idea to define NSGs at subnet level)
- Be careful not to inadvertently drop traffic to essential Azure services
  - Licensing
  - Virtual IP of the host 168.63.129.16

NSG Rule Processing



Sample NSG


Internet
www.contoso.com
Azure load balancer
West US
WEB1
WEB2
FrontEnd
192.168.1.0/24
DB1
DB2
BackEnd
192.168.2.0/24
TestVNet
192.168.0.0/16
Virtual Network

NSG Example

Rule	Access	Priority	Source address range	Source port	Destination address range	Destination port	Protocol
Allow-Inbound-HTTP-Internet	Allow	100	Internet	*	*	80	TCP
Allow-Inbound-RDP-Internet	Allow	200	Internet	*	*	3389	TCP

Rule	Access	Priority	Source address range	Source port	Destination address range	Destination port	Protocol
Deny-Internet-All	Deny	100	Internet	*	*	*	*

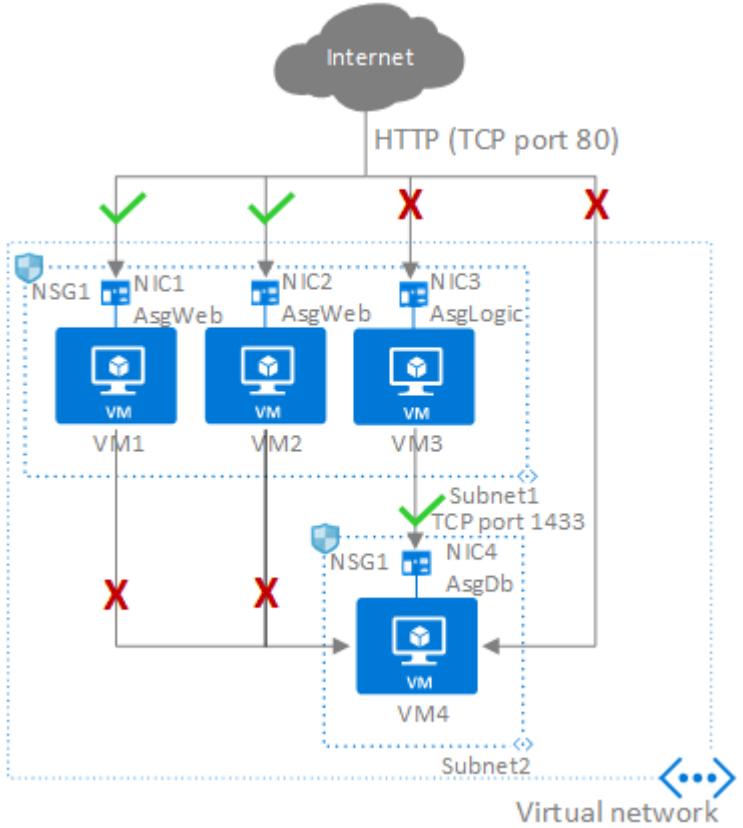
NSG Precedence (Inbound)

- If a subnet NSG has a matching rule to deny traffic, the packet is dropped.
- If VM\NIC NSG has a matching rule that denies traffic, packets are dropped at the VM\NIC, even if a subnet NSG has a matching rule that allows traffic.

NSG Precedence (Outbound)

- If a VM\NIC NSG has a matching rule that denies traffic, packets are dropped.
- If a subnet NSG has a matching rule that denies traffic, packets are dropped, even if a VM\NIC NSG has a matching rule that allows traffic.

Application Security Groups



Service Tags

- Group of IP address prefixes to help minimize complexity for security rule creation
- Cannot create your own service tag or specify which IP addresses are included within a tag
- Microsoft manages the address prefixes
  - **AzureCosmosDB** - Allow access to Cosmos DB
  - **AzureCosmosDB.[East] –** Allow access to Cosmos DB in a region

Routing

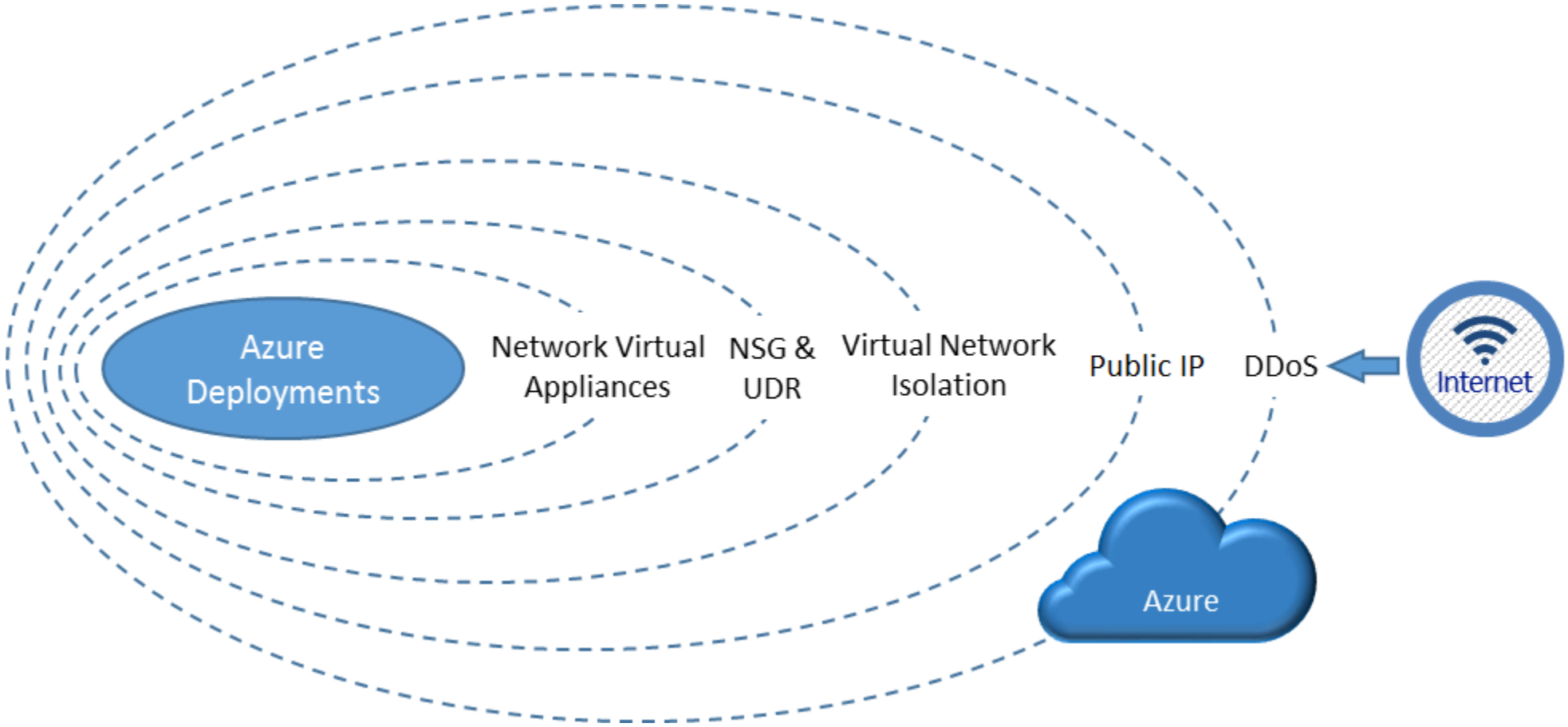
- **System Routes**
  - Default routes associated with a VNET
  - Cannot create new or delete system routes
  - Next Hop Type
    - VNET, Internet and None
  - Optional system routes
    - VNET Peering – adds routes to peered network
    - Virtual Network Gateway – add routes to virtual network gateway
    - Virtual Service Endpoint – adds Public IP of the service

Source	Address prefixes	Next hop type
Default	Unique to the virtual network	Virtual network
Default	0.0.0.0/0	Internet
Default	10.0.0.0/8	None

Routing Continued

- **User Defined**
  - Create custom route tables with routes that control where traffic is routed to for each subnet.
  - Next Hop Type
    - Virtual appliance – private IP address of the NIC (IP forwarding)
    - Virtual Network
    - None
    - Virtual Network Gateway
    - Note cannot define VNET Peering or Service Endpoints as custom routes

Layers of Network Security



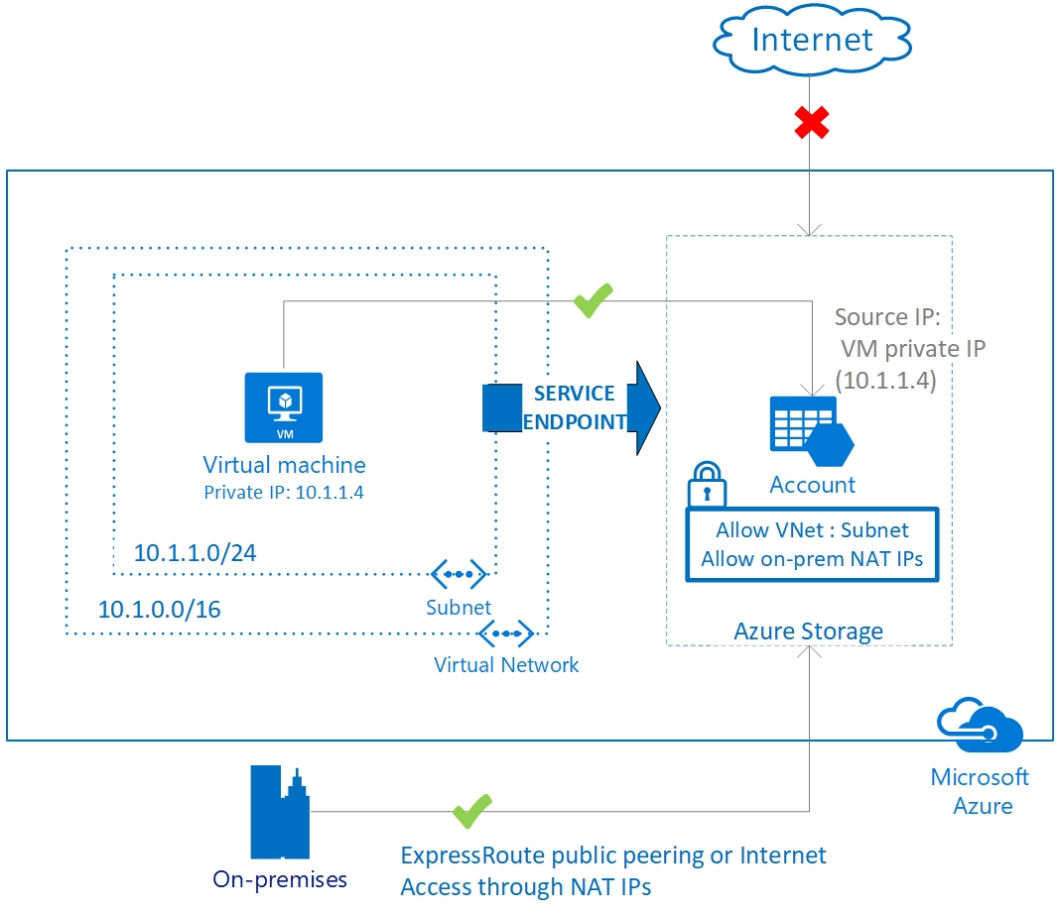
Best practices

- Logically segment subnets
- Control routing behavior
- Enable Forced Tunneling
- Use Virtual network appliances
- Deploy DMZs for security zoning
- Avoid exposure to the Internet with dedicated WAN links
- Optimize uptime and performance
- Use global load balancing
- Disable RDP Access to Azure Virtual Machines
- Enable Azure Security Center
- Extend your datacenter into Azure

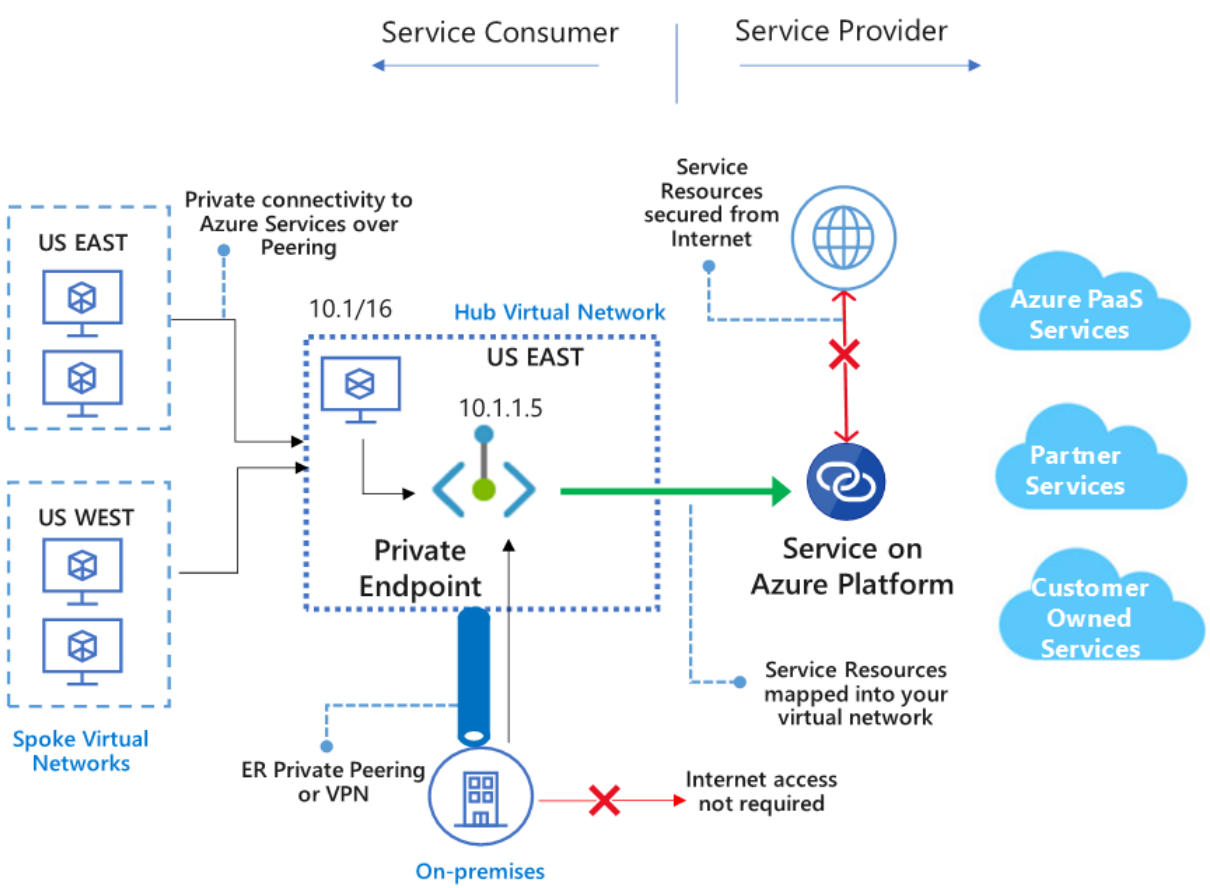
Network Service Endpoints

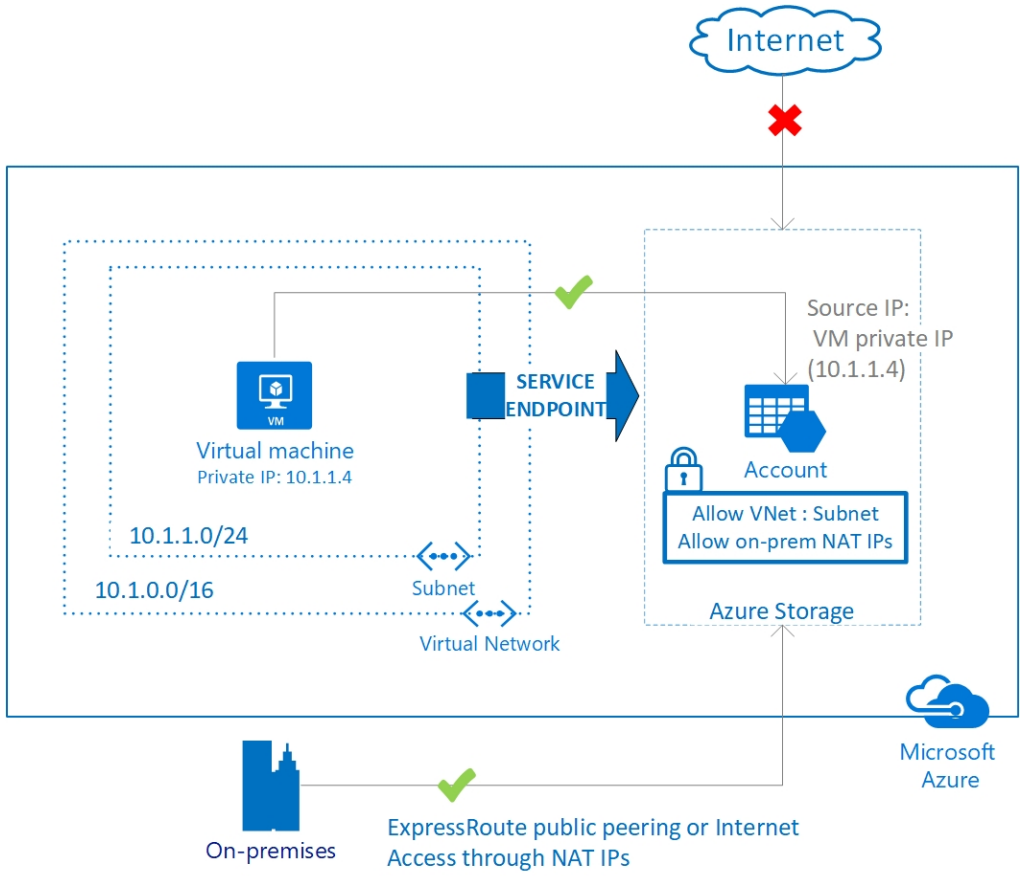
- Extend your virtual network private address space & identity of your VNet to the Azure services like Storage
- Secure your critical Azure service resources to only your virtual networks
- Traffic from your VNet to the Azure service always remains on the Microsoft Azure backbone network.
  - Azure Storage:
  - Azure SQL Database
  - Azure Cosmos DB
  - Azure SQL Data Warehouse

Network Service Endpoints



Azure Private Link





VNET Business Continuity

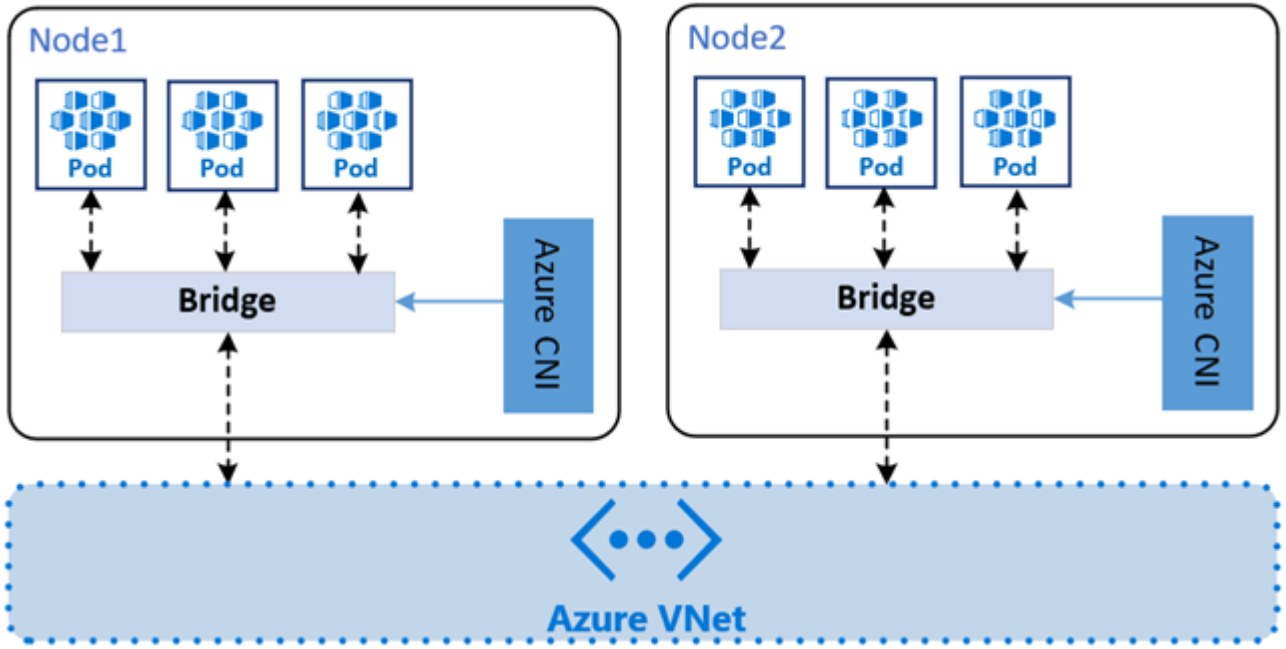
- Create two VNets using the same private IP address space and resources in two different regions ahead of time.
- At the time of outage of VNet in one region, you can connect the other VNet in the available region
- Note - you cannot connect two VNets with the same address space to your on-premises network

DDOS Protection

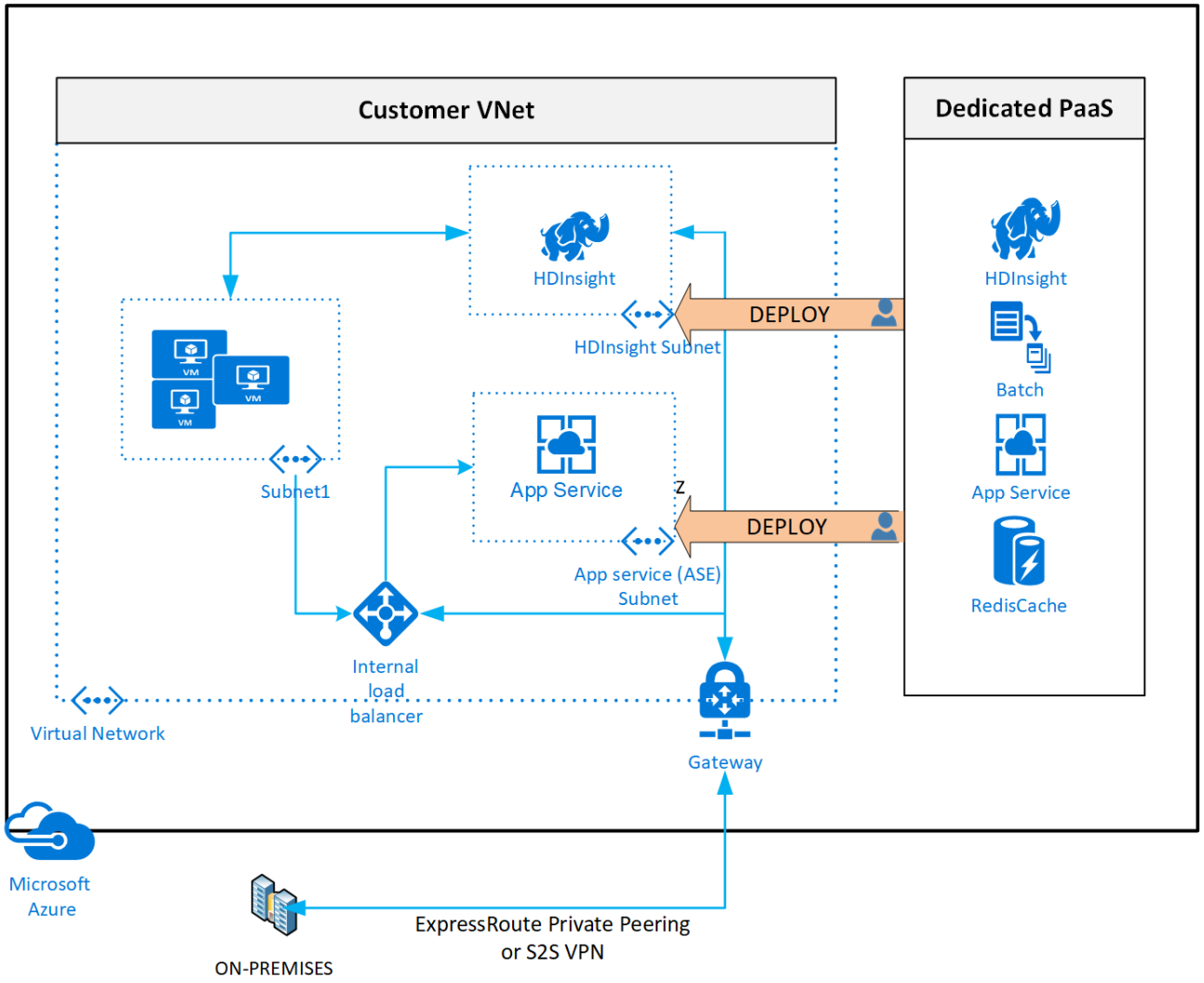
- Basic
  - Automatically enabled / no charge
- Standard
  - Tuned for your VNET (flood the network layer)
  - ML algorithms trained on your VNET
  - Policies applied to public IP addresses – Load balancer / App Gateway
- Types of attack
  - Volumetric
  - Protocol Attacks (SYN Flood attacks)
  - Application layer (HTTP protocol, SQL Injection)

Container Networking

- Each Pod gets its own IP address
- Pod can connect to other resources in resources in the VNET
- Pods can talk to Azure Services like Azure SQL Datbase via Service Endpoints
- Azure VNET CNI

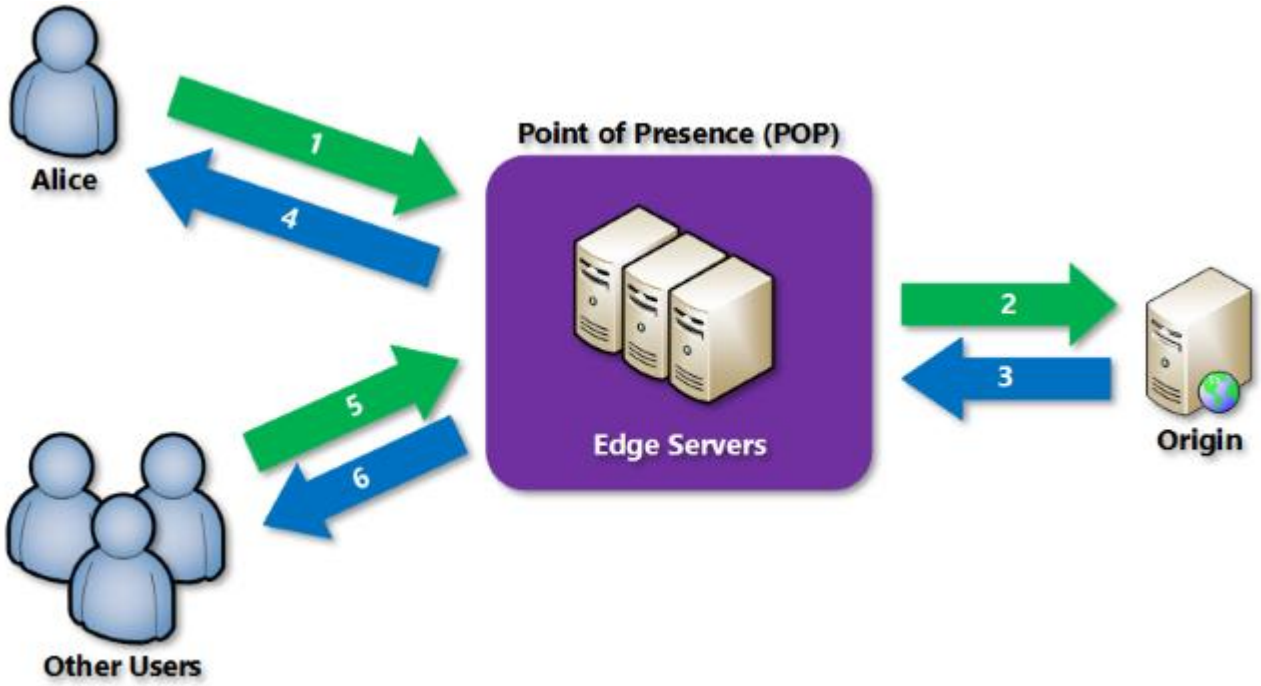


Azure VNET for Azure Services

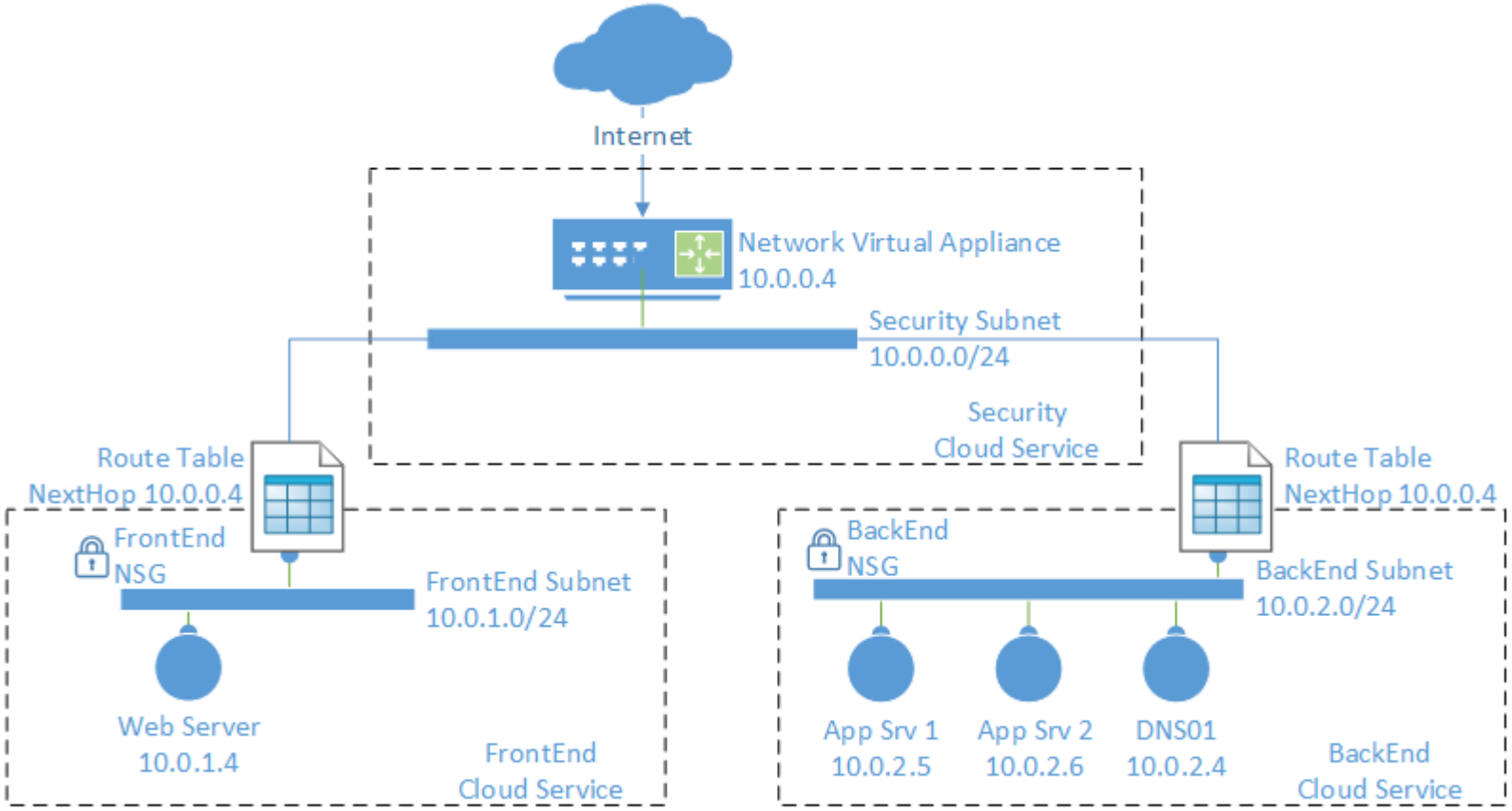


Azure CDN

- Dynamic site acceleration
- CDN caching rules
- HTTPS custom domain support
- Azure diagnostics logs
- File compression
- Geo-filtering



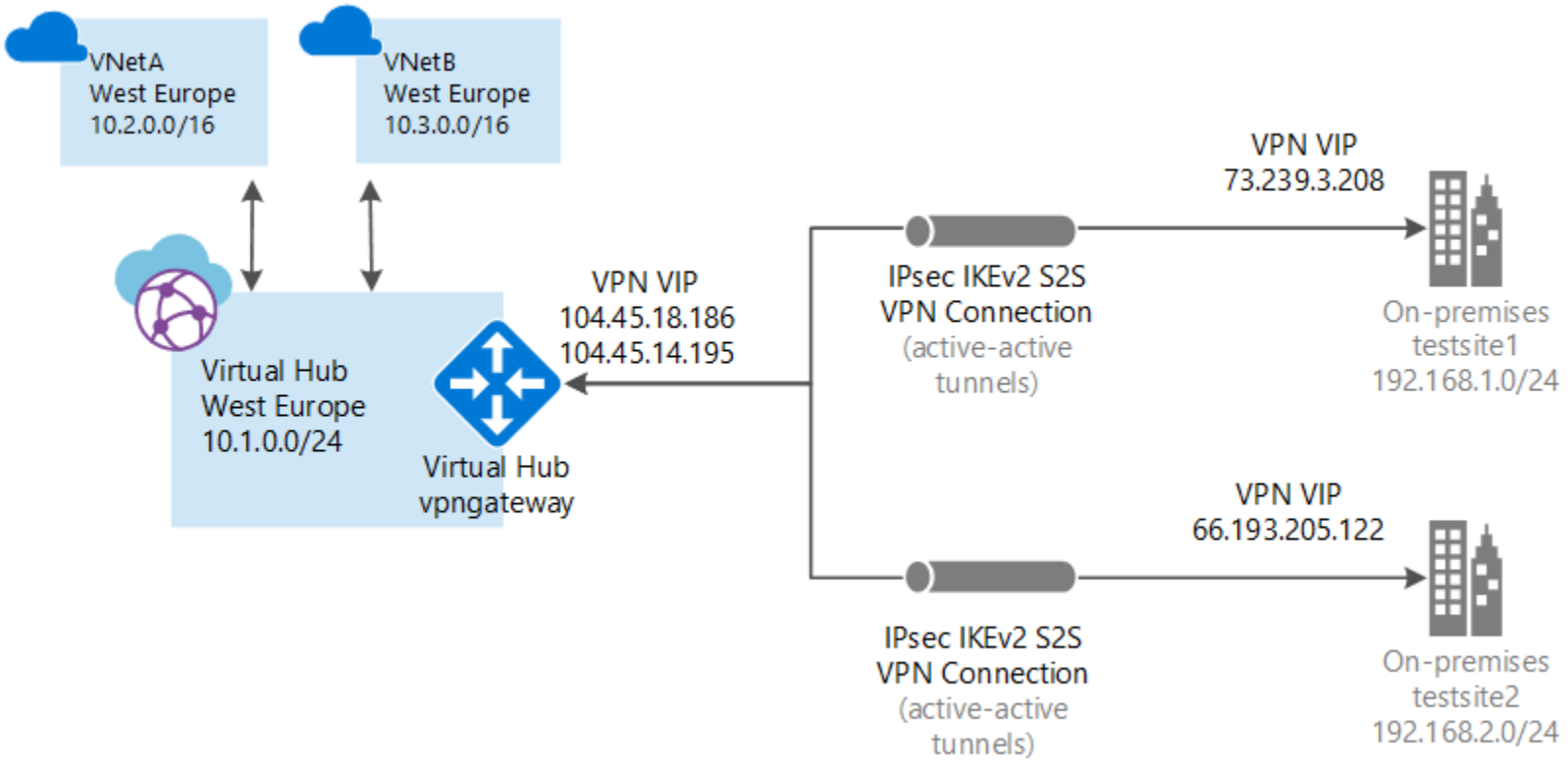
Network Virtual Appliance



Network Watcher

- Monitor a connection between VM and endpoint
- Automatically view resources
- Capture packets to and from a VM
- Determine the nexthop
- Latencies between regions
- Effective security rules for a NIC
- Metrics – capacity versus uses network resources

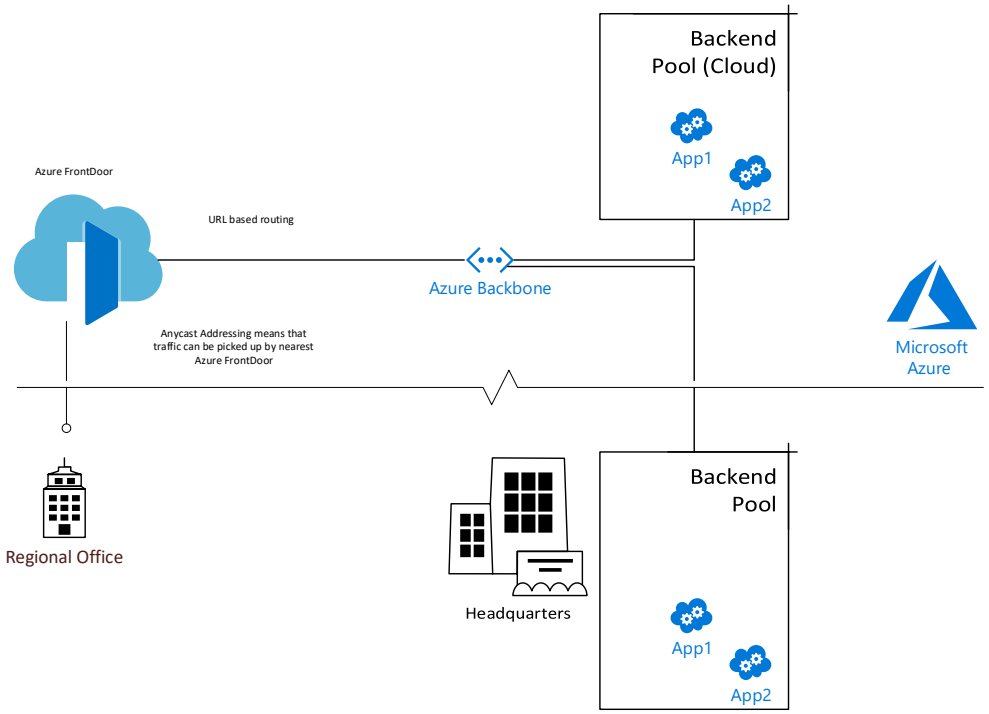
Virtual WAN


VNetA
West Europe
10.2.0.0/16
VNetB
West Europe
10.3.0.0/16
Virtual Hub
West Europe
10.1.0.0/24
Virtual Hub
vpngateway
VPN VIP
104.45.18.186
104.45.14.195
IPsec IKEv2 S2S
VPN Connection
(active-active
tunnels)
VPN VIP
73.239.3.208
On-premises
testsite1
192.168.1.0/24
IPsec IKEv2 S2S
VPN Connection
(active-active
tunnels)
VPN VIP
66.193.205.122
On-premises
testsite2
192.168.2.0/24

Azure Front Door

- Accelerate response times
- Application availability (backend pools and health probes)
- URL-based routing
- SSL termination
- WAF
- URL rewrite

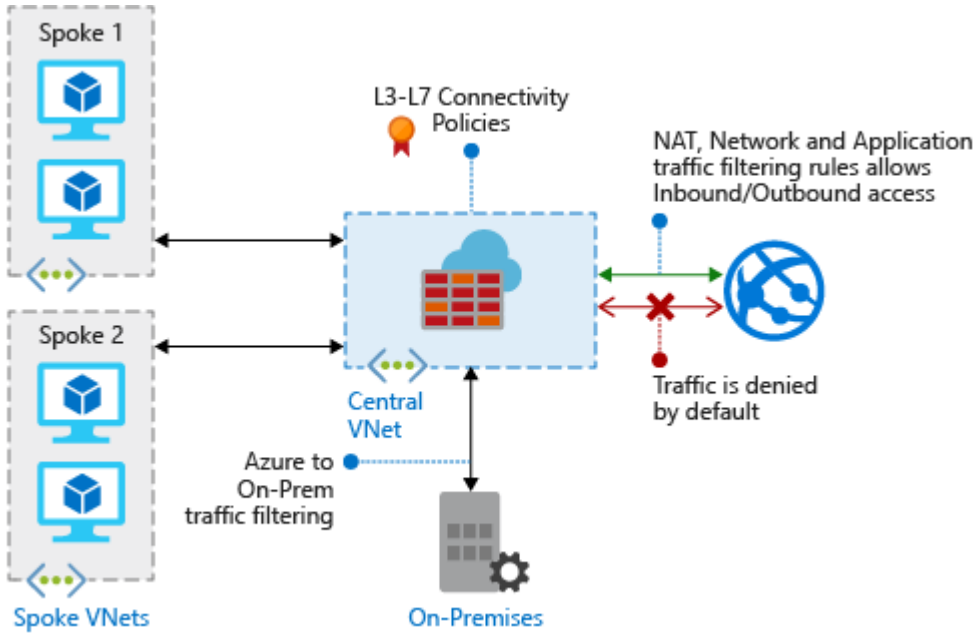
Azure Front Door Service



Network Watcher

- Monitor a connection between VM and endpoint
- Automatically view resources
- Capture packets to and from a VM
- Determine the nexthop
- Latencies between regions
- Effective security rules for a NIC
- Metrics – capacity versus uses network resources

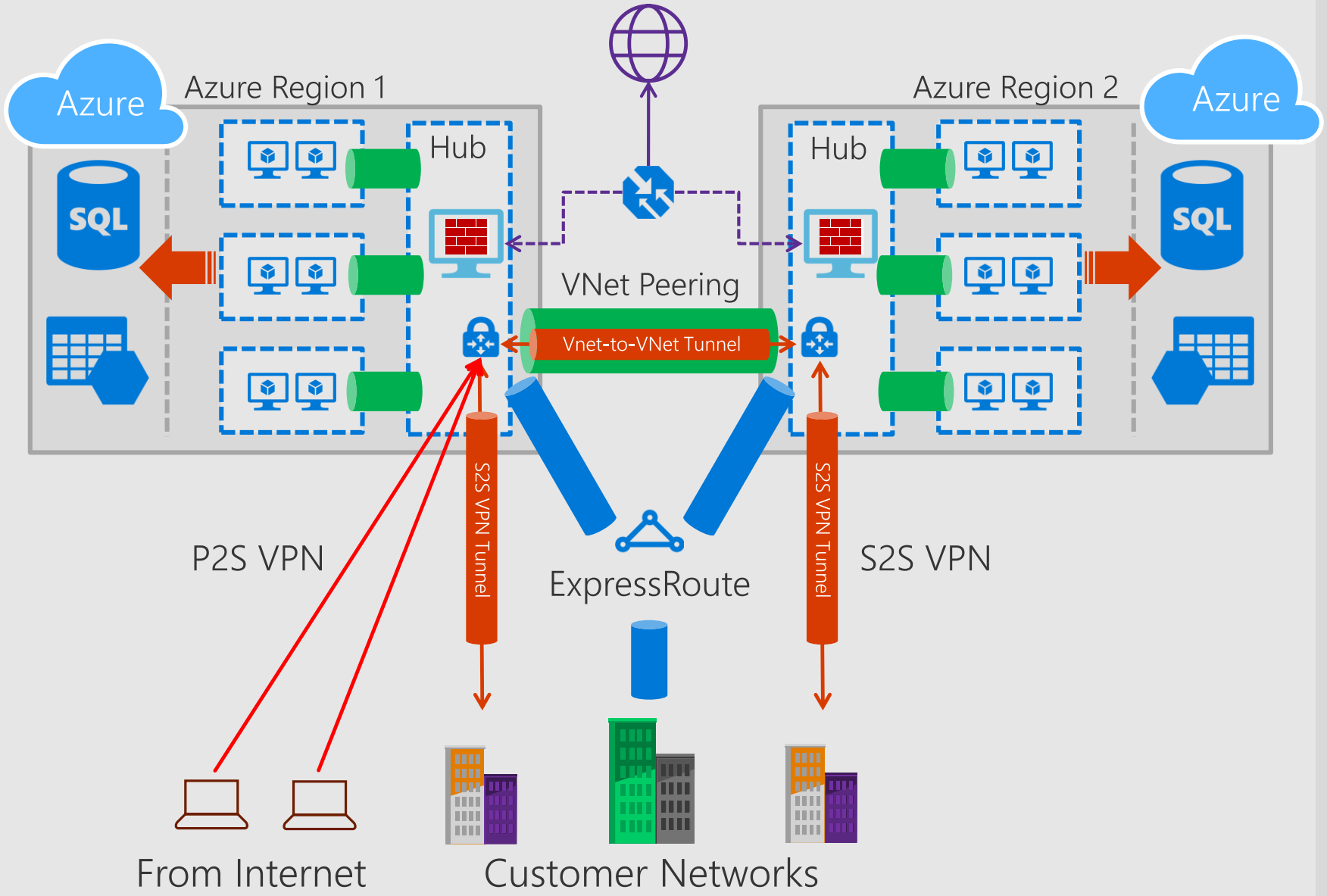
Azure Firewall



Azure Firewall

- High availability
- Scalability
- FQDN Tags (e.g. Windows Update)
- Outbound and Inbound SNAT support
- Stateful

Putting everything together



Hub-and-Spoke

- Hub-and-spoke in each region with VNet peering and Service Endpoints

Global VNet peering

- Connecting Azure regions together
- Direct VM-to-VM over Azure backbone

ExpressRoute

- Private connectivity into Microsoft Clouds
- High-throughput with carrier QoS

S2S VPN

- Cross-premises connectivity over the Internet
- Secure connectivity over Internet

P2S VPN

- Connect to Azure VNet securely from ANYWHERE
- Apple Mac, Windows with AD authentication

Demos