Azure Networking – Deep Dive / Best Practices

Eric Berg
Microsoft MVP – Azure and CDM

Eric Berg

Global Subject Lead - Cloud Compute

MVP Azure & CDM, LinkedIn Learning Trainer

Cloud, Datacenter and Management

info@ericberg.de

@ericberg_de | @GeekZeugs

www.ericberg.de | www.geekzeugs.de

AGENDA

- Networking Overview
- Networking Basics
- Connectivity
- Security
- Integration
- Q&A

Networking Overview

High Level Azure Services

Management

- Azure Monitor
- Log Analytics
- Azure Policy
- Azure Blueprints
- Azure Backup
- Site Recovery
- Azure Migrate
- Databox Family
- Cost Management

Platform as a Services (PaaS)

Compute/Containers

- Functions
- Kubernetes Service
- Container Instance
- Service Fabric

Web/Mobile

- Web Apps
- Logic Apps
- API Apps
- Mobile Apps
- Notification Hubs
- SignalR Service

DevOps/Developer

- Azure DevOps
- Lab Services
- Application Insights
- SDK

Integration

- API Management
- Logic Apps
- Service Bus
- Event Grid

IoT

- IoT Hub
- IoT Central
- Time Series Insights
- Azure Digital Twins
- IoT Edge

AI

- Cognitive Services
- Machine Learning Studio
- Machine Learning Service
- Bot Services
- Azure Search

Analytics

- SQL Data Warehouse
- Azure Databricks
- Apache Spark
- Stream Analytics
- Data Lake Storage Gen2

Data Services

- SQL Database
- SQL Data Warehouse
- Database for MySQL
- Cosmos DB
- Database for PostgreSQL
- Data Factory
- Database for MariaDB
- Azure Cache for Redis
- Database Migration Service
- Table Storage

Media/CDN

- Media Services
- Content Protection
- Video Indexer
- Content Delivery Network

Security

- Security Center
- Azure AD
- Azure AD for Domain Services
- Azure AD B2C
- DDoS Protection
- Key Vault
- Multi-Factor Authentication
- Azure ATP
- Role- based access control

Infrastructure as a Services (IaaS)

Compute

- Virtual Machine Scale Sets
- Linux Virtual Machine

Storage

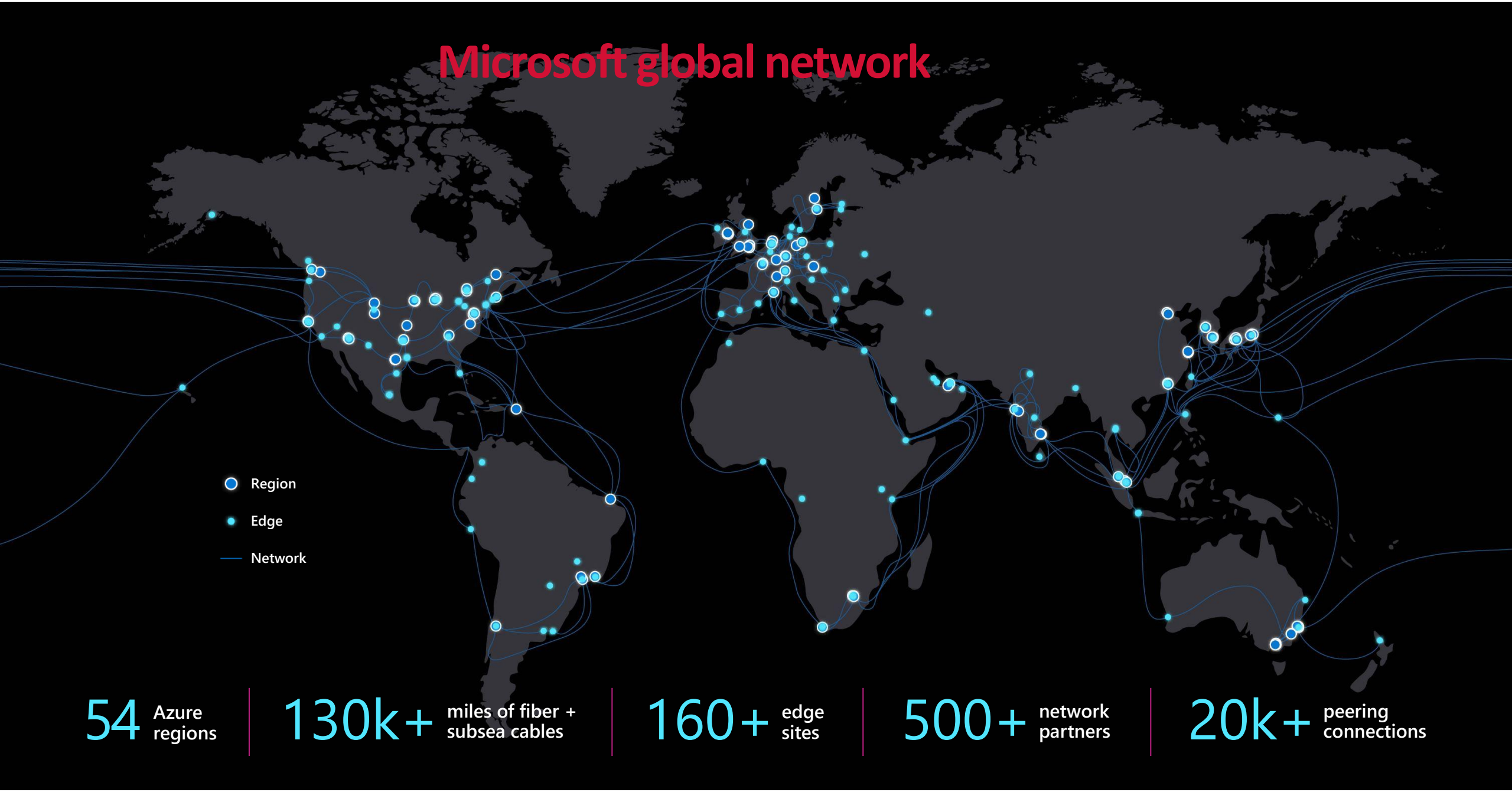
- Disk Storage
- Managed Disks

Networking

- Virtual Network
- VPN Gateway
- Express Route
- Load Balancer
- Azure Firewall
- Virtual WAN
- Network Watcher

Azure Datacenter Infrastructure

Microsoft global network



54 Azure regions

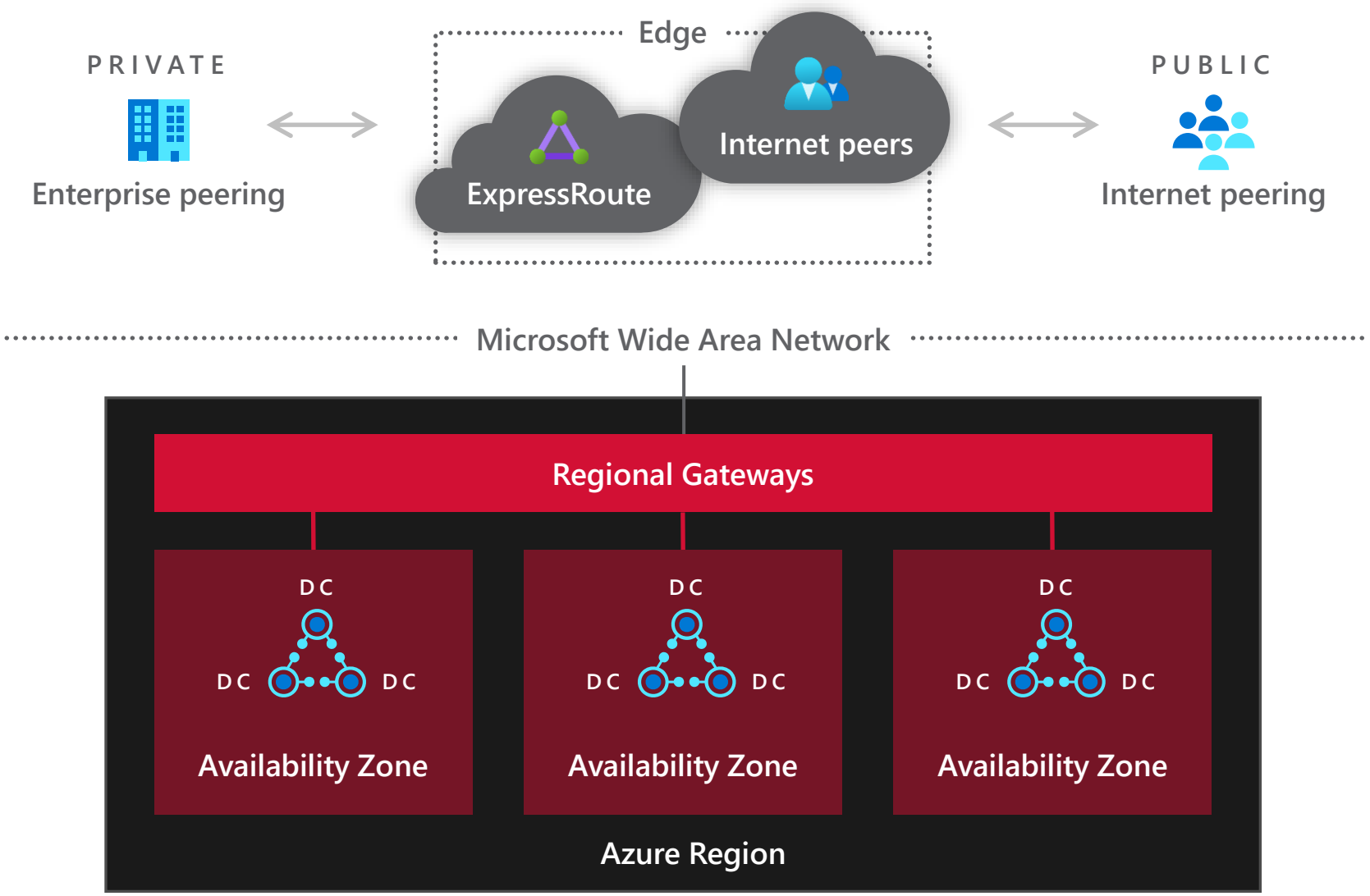
130k+ miles of fiber + subsea cables

160+ edge sites

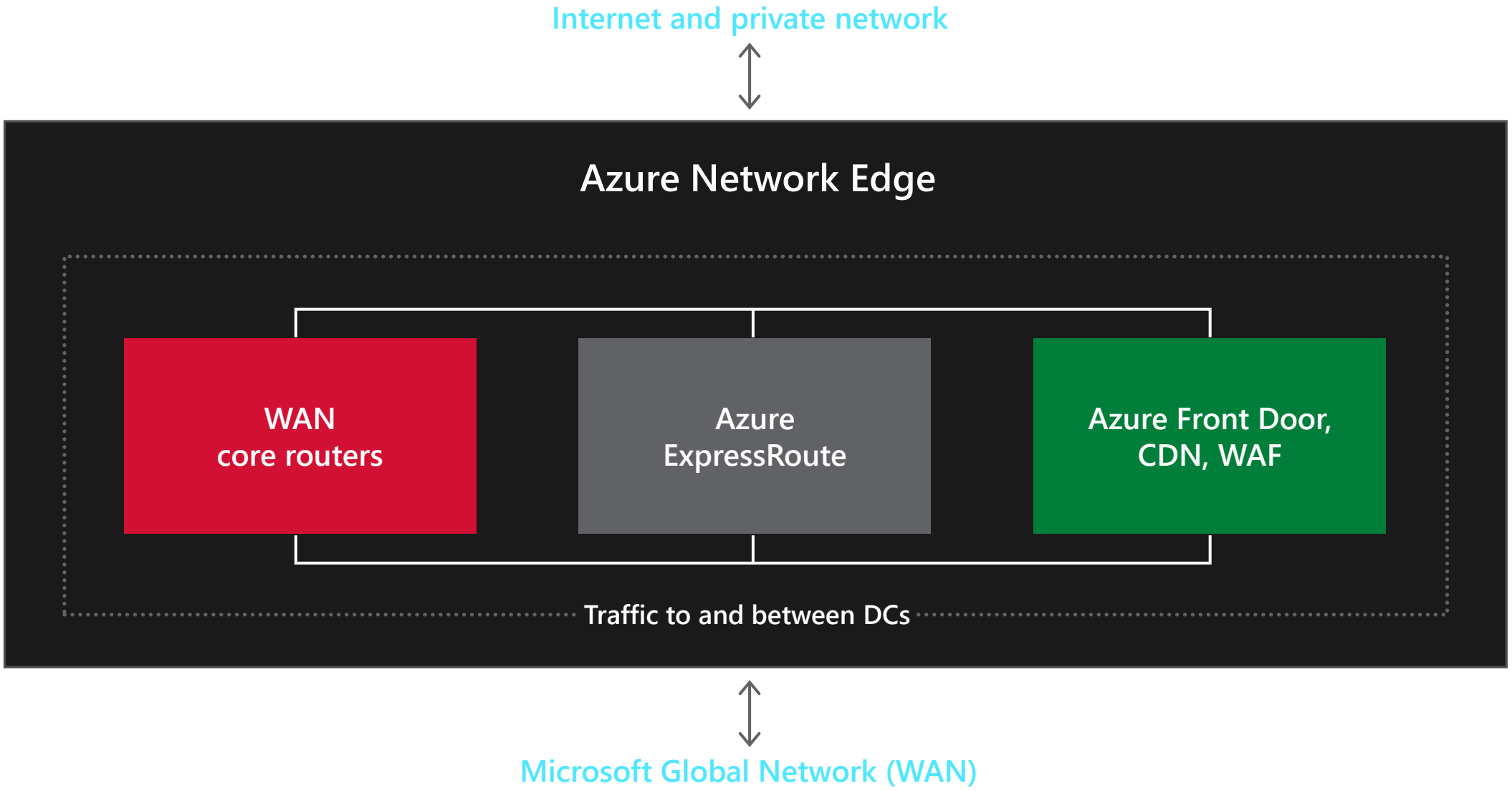
500+ network partners

20k+ peering connections

Connecting Azure regions to the global network



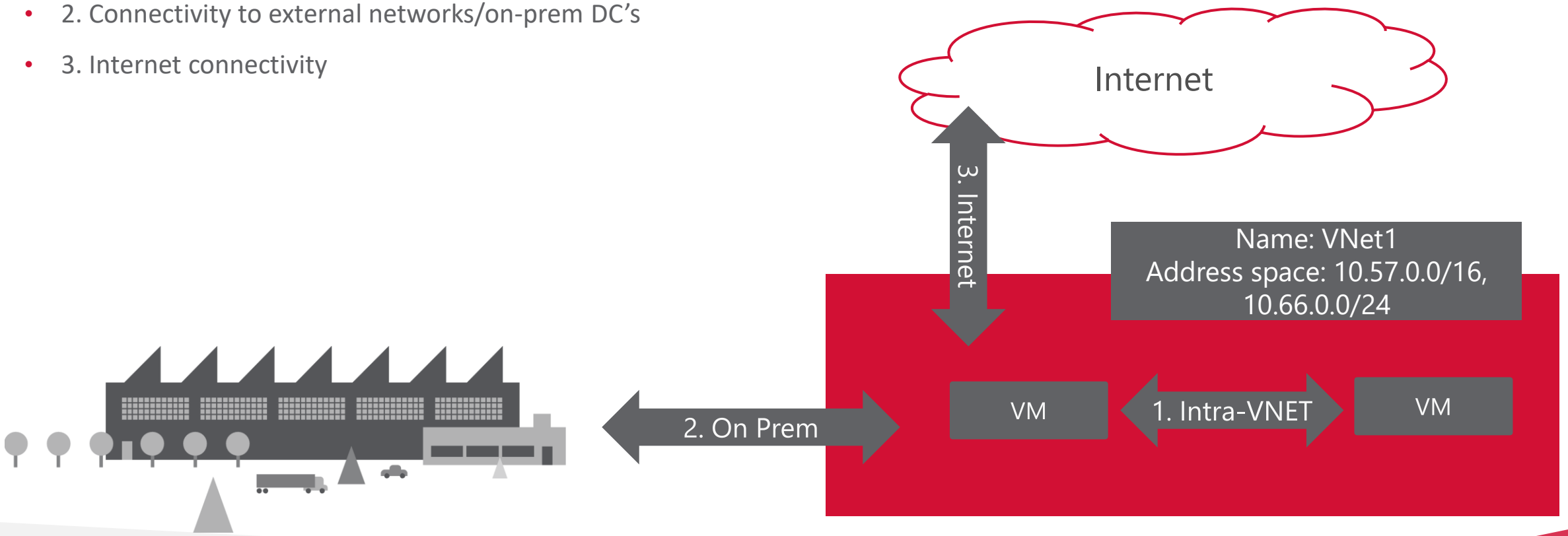
The Azure Network Edge



Basics

Virtual Network

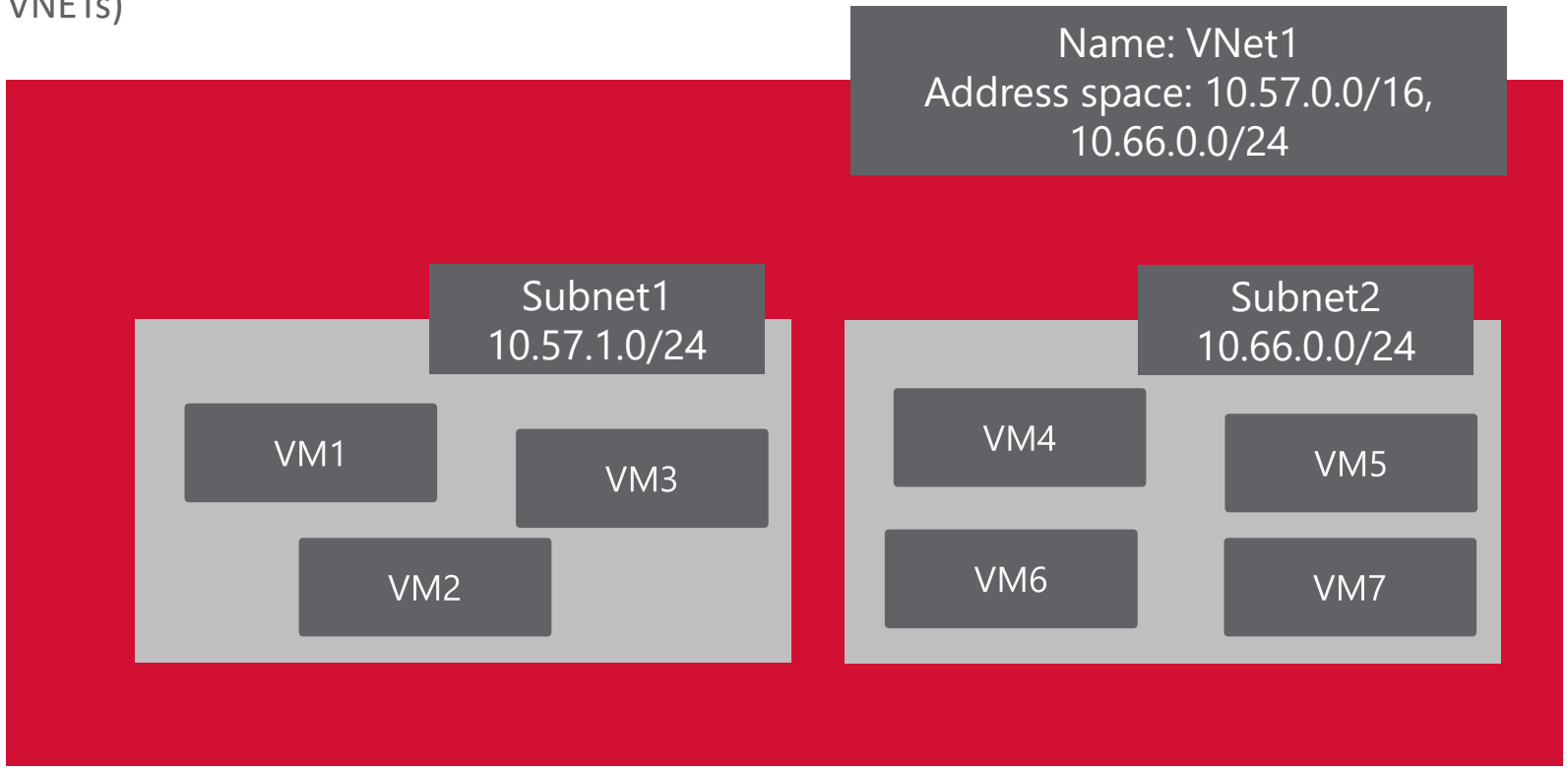
- Isolated, logical network that provides connectivity for Azure Virtual Machines
  - User-defined address space (can be one or more IP ranges, not necessarily RFC1918)
  - 1. Connectivity for VMs in the same VNET
  - 2. Connectivity to external networks/on-prem DC's
  - 3. Internet connectivity



Subnet

IP subnet

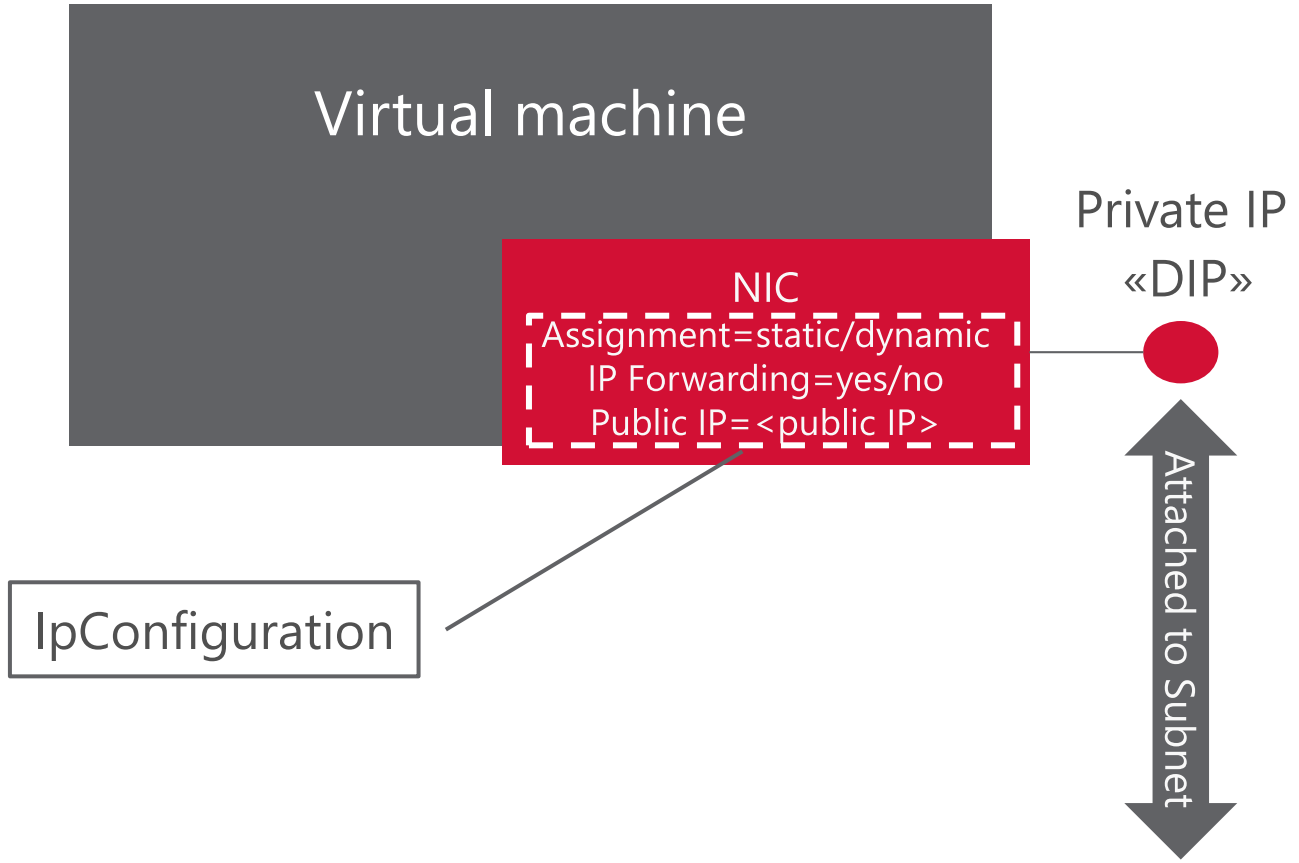
- Provides full layer-3 semantics and partial layer-2 semantics (DHCP, ARP, no broadcast/multicast)
- Subnets can span only one range of contigous IP addresses
- VMs can be deployed only to subnets (not VNETs)



Network Interface

- Virtual NIC that connects a VM to a Subnet
  - One private IP address (private == included in the subnet's IP range, not necessarily RFC1918)
  - Private IP address always assigned via Azure DHCP

- Dynamic assignment = DHCP assigns new IP when VM is restarted
- Static assignment =DHCP assigns always the same IP
- IP forwarding = NIC can receive packets with dest IP address different from its private IP
- Public IP = NAT address associated to the NIC (more on this later). AKA «VIP»



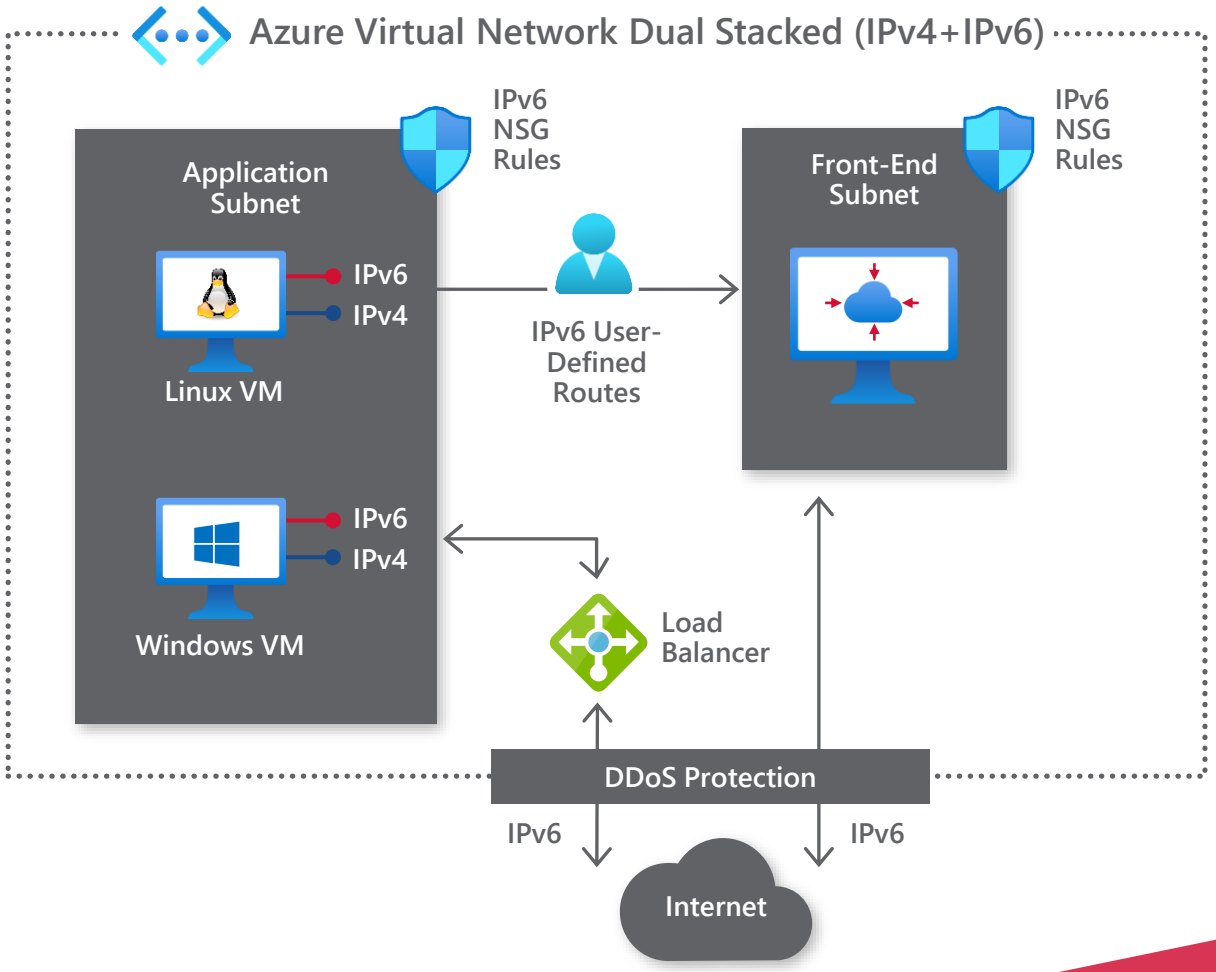
IPv6 in Azure VNETs

GA

Native IPv6 all the way to the VMs

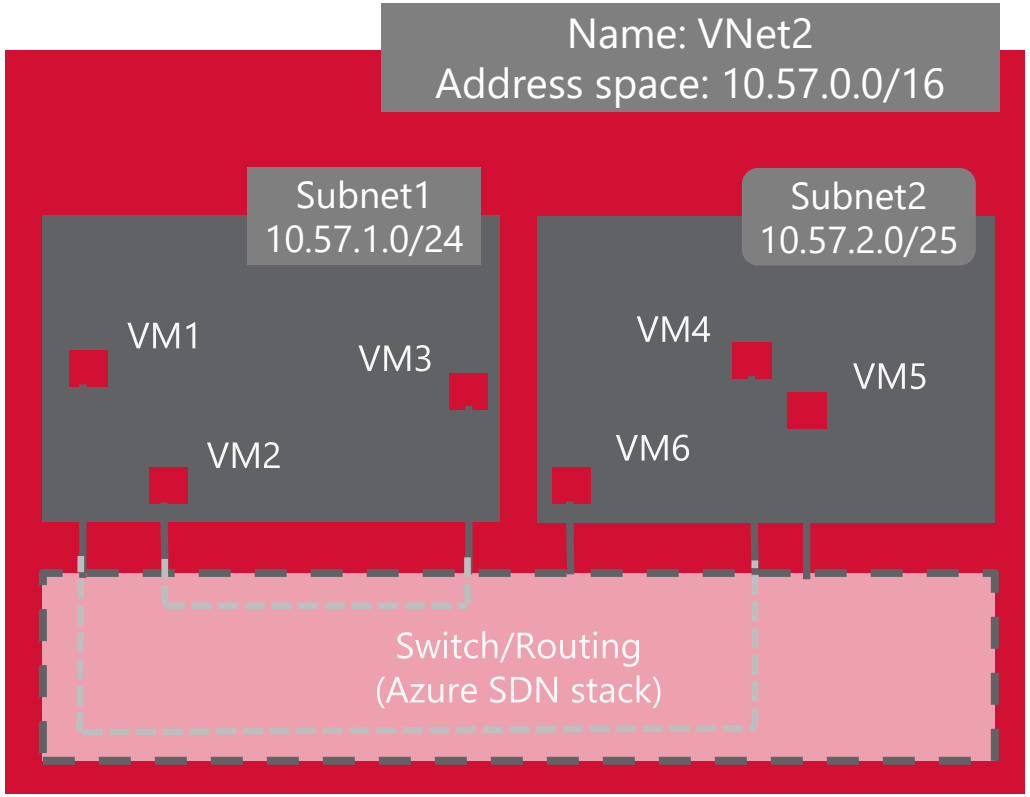
Private IPv6 addresses for VMs and NICs

Dual stacked IPv4/IPv6 VMs for max flexibility



Switching/Routing in Azure VNETs

- A VNET provides a switching/routing functionality that allows VMs to talk to each other



Please note that, in an Azure VNet, packets can flow between to different subnets without explicitly traversing any layer-3 device. Azure's network virtualization stack effectively works as a layer-3 switch

Connectivity

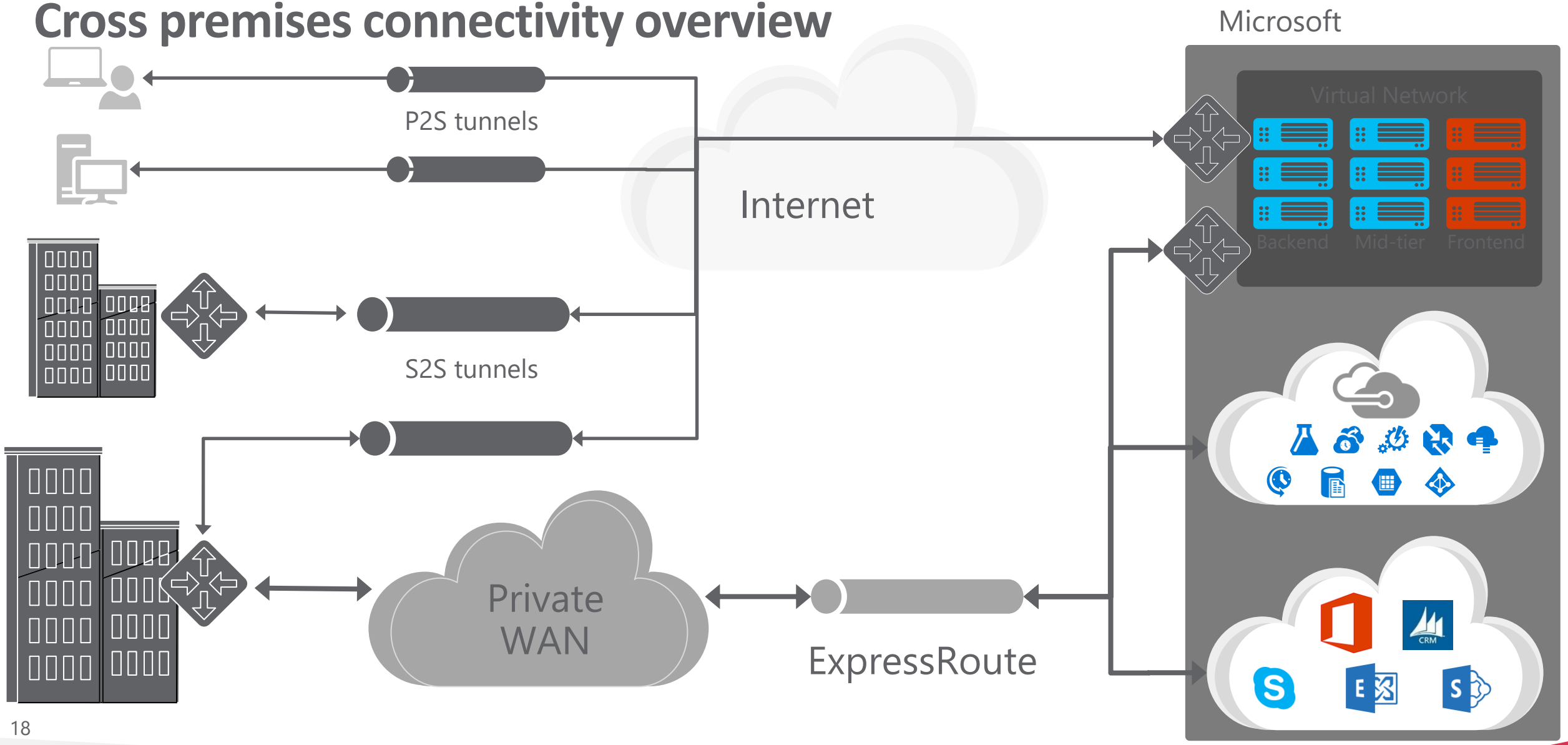
Connecting *to* Azure

Cloud		Customer	Characteristics
	Internet Connectivity		• Internet facing with public IP addresses in Azure • VPN connectivity with virtual appliances (Marketplace)
	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

Connecting *in* 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
	VNet-to-VNet via ExpressRoute circuit		• Traverse (“hairpin”) through ExpressRoute circuit & gateways • Traffic is not encrypted

Cross premises connectivity overview



VPN

S2S

High throughput VPN – 10Gbps

- Azure VPN gateways – VpnGw2/3/4/5
- Up to 10 Gbps aggregate
- Up to 10,000 P2S connections (Gw5)

IKEv1 + IKEv2 on VpnGw1-5

- IKEv1 on new VpnGw SKUs (1 ~ 5)
- Multiple IKEv1 S2S tunnels
- IKEv1 and IKEv2 on the same VPN gateway

VPN gateway packet capture

- With 5-tuple packet filter
- ETW or PCAP formats

Custom IKE traffic selectors

P2S

AAD auth + MFA

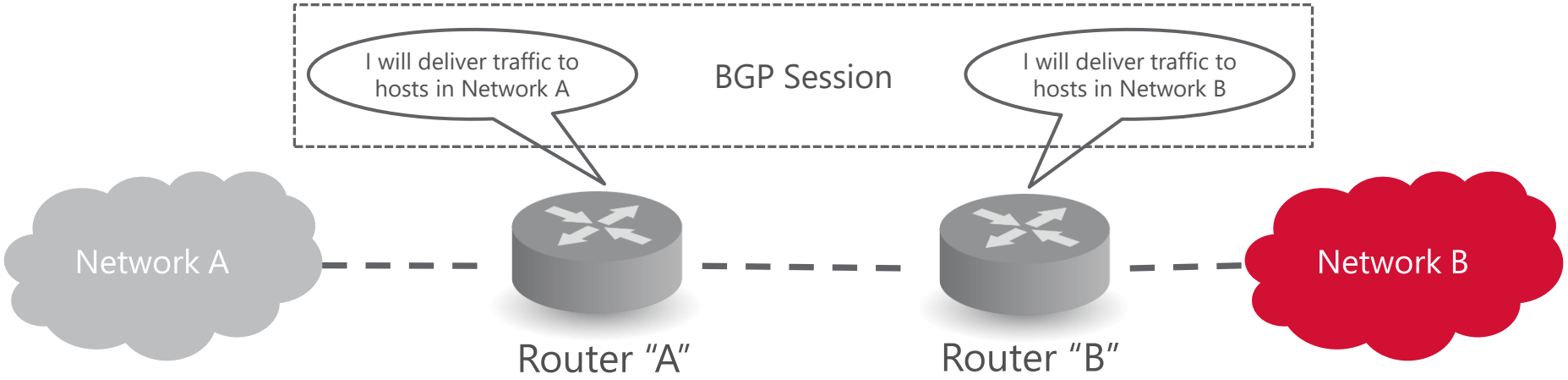
Azure VPN Client (Windows App)

- OpenVPN protocol
- Native AAD authentication with MFA
- Client-side Diagnostics, Logs, & Metrics

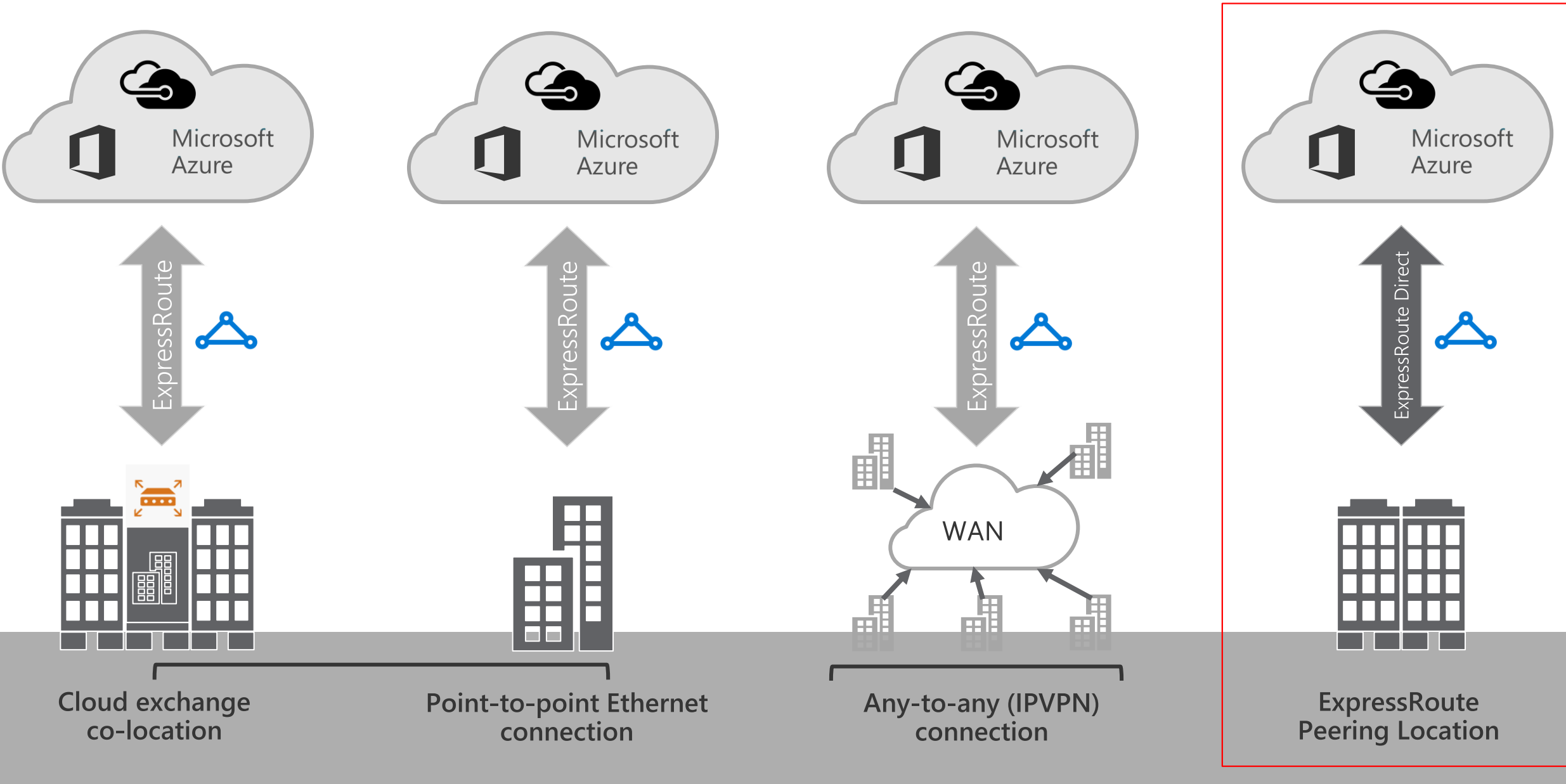
SKUs	Aggregate throughput	P2S connections	IKEv1/v2
VpnGw1	650 Mbps	250	IKEv1+IKEv2
VpnGw2	1 Gbps	500	IKEv1+IKEv2
VpnGw3	2.5 Gbps	1000	IKEv1+IKEv2
VpnGw4	5 Gbps	5,000	IKEv1+IKEv2
VpnGw5	10 Gbps	10,000	IKEv1+IKEv2

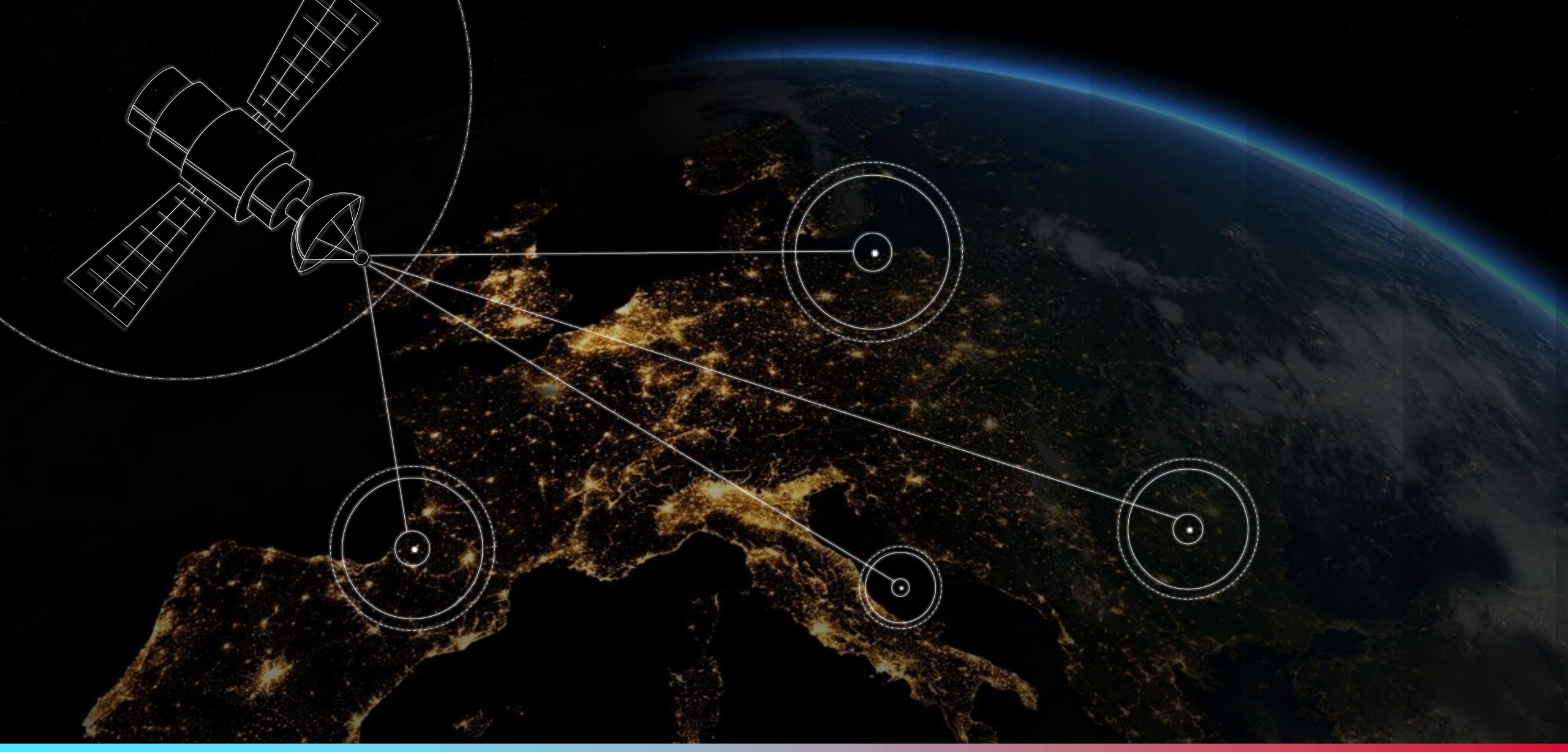
First: BGP Basics as needed for Express Route

- BGP
  - Border Gateway Protocol
  - Protocol used by routers to agree which traffic they can exchange
- BGP Session
  - A logical connection whereby two routers agree to exchange traffic to/from a set of IP addresses

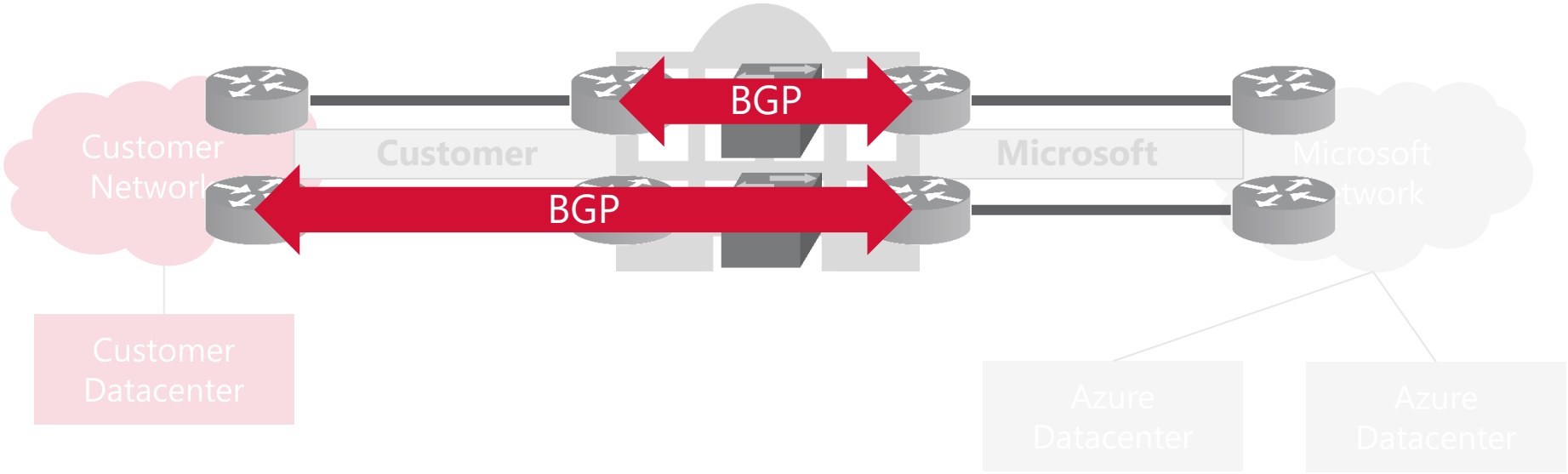


ExpressRoute connectivity models

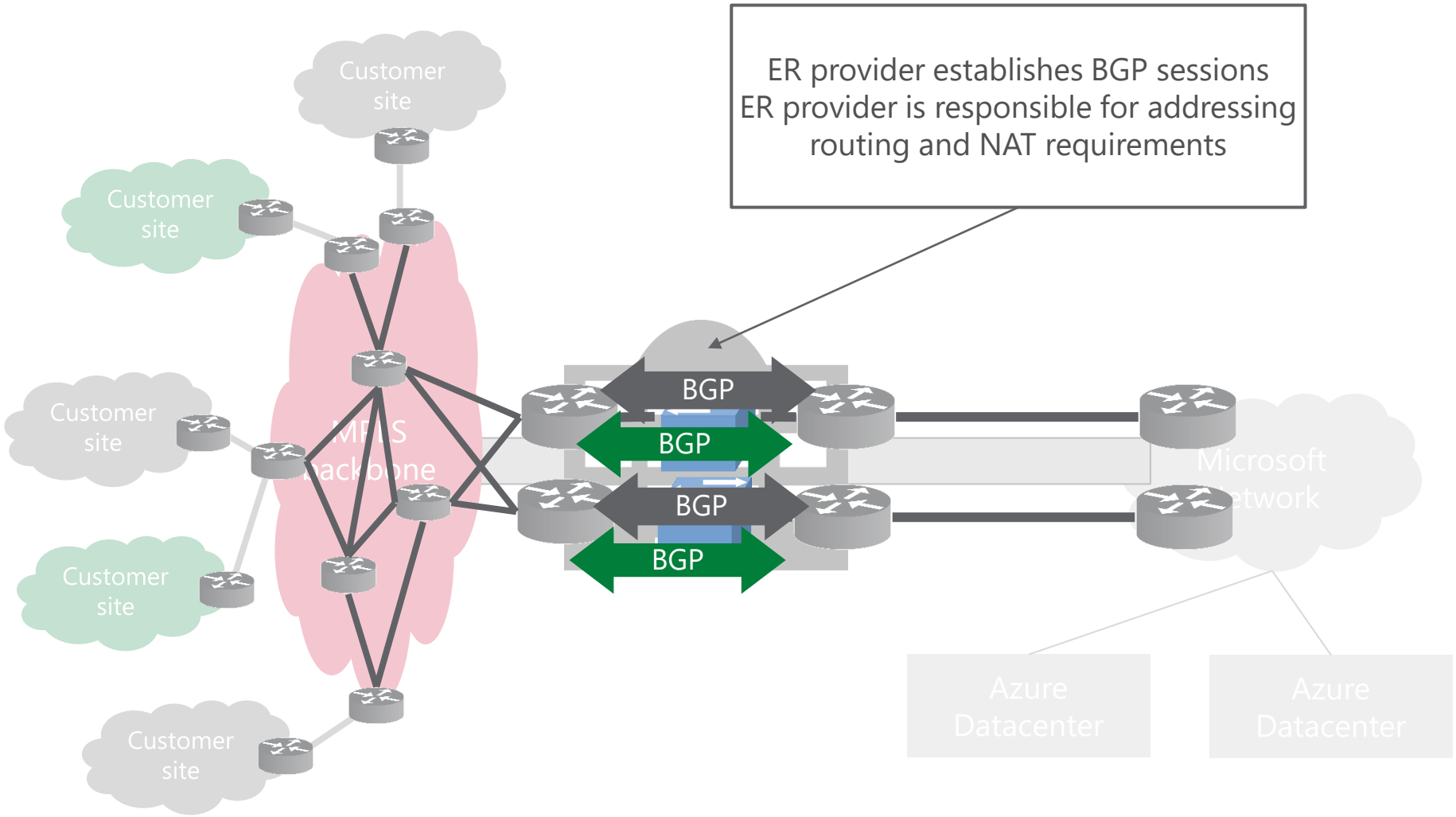




Cloud exchange colocation BGP Sessions

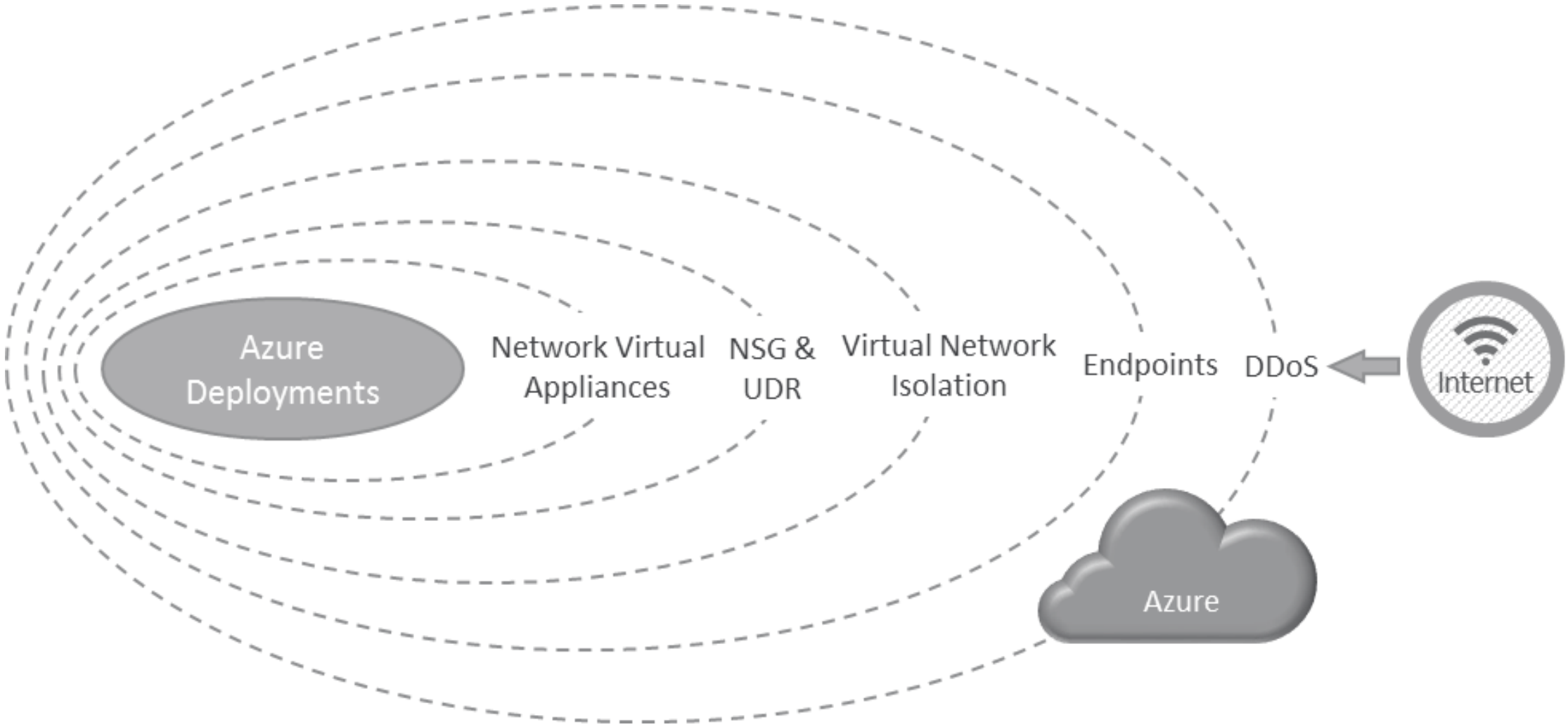


IP VPN ConnectionBGP Sessions



Security

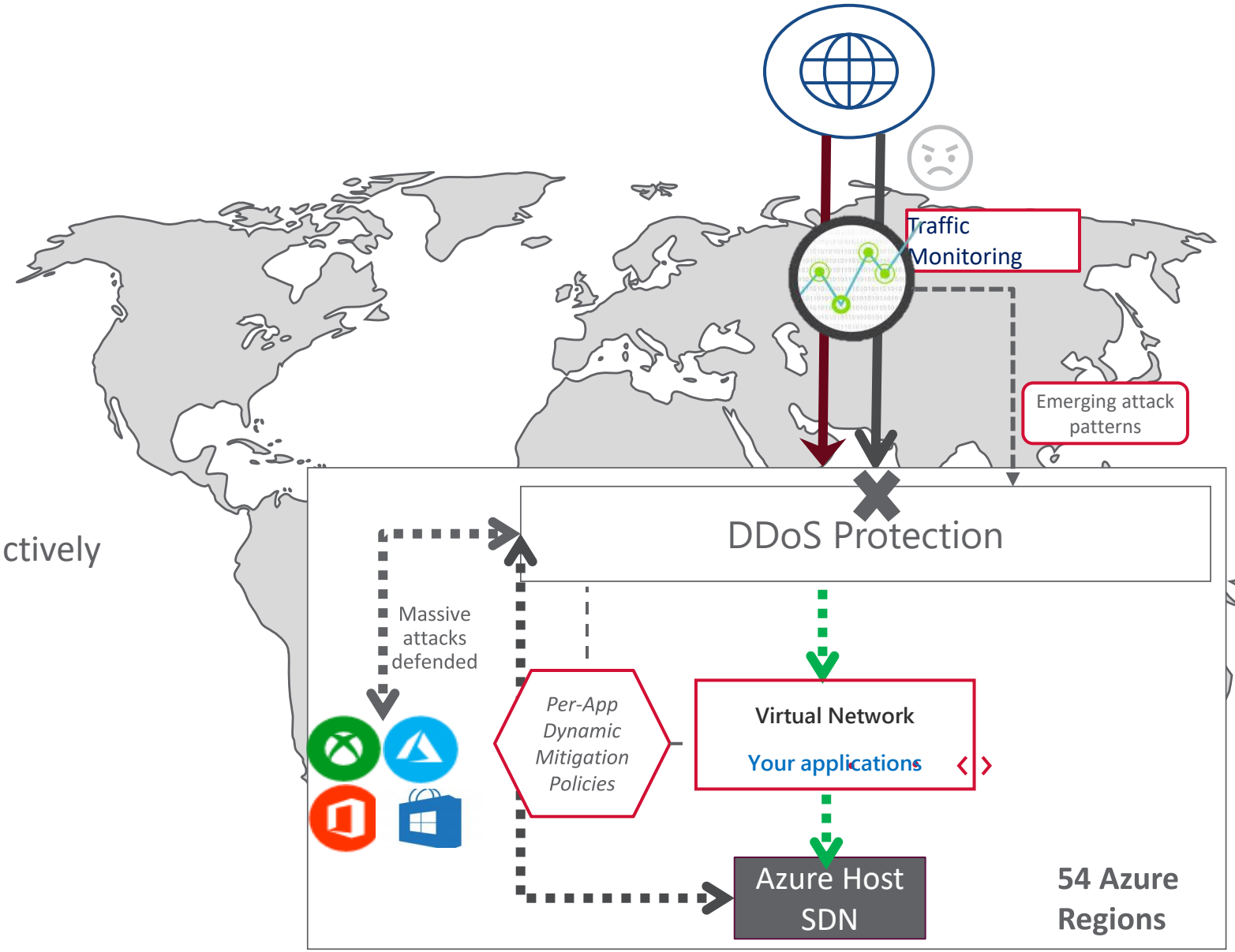
Security layers



DDoS Defense

DDoS protection

- Designed into the global network
- Global distribution of the attack during
- large scale attacks
  - 25+ Tbps global mitigation capacity
- Continuous monitoring and learning to proactively detect emerging threats and attack vectors
- Proven defense for Microsoft Services
- Specifically tuned protection for you app

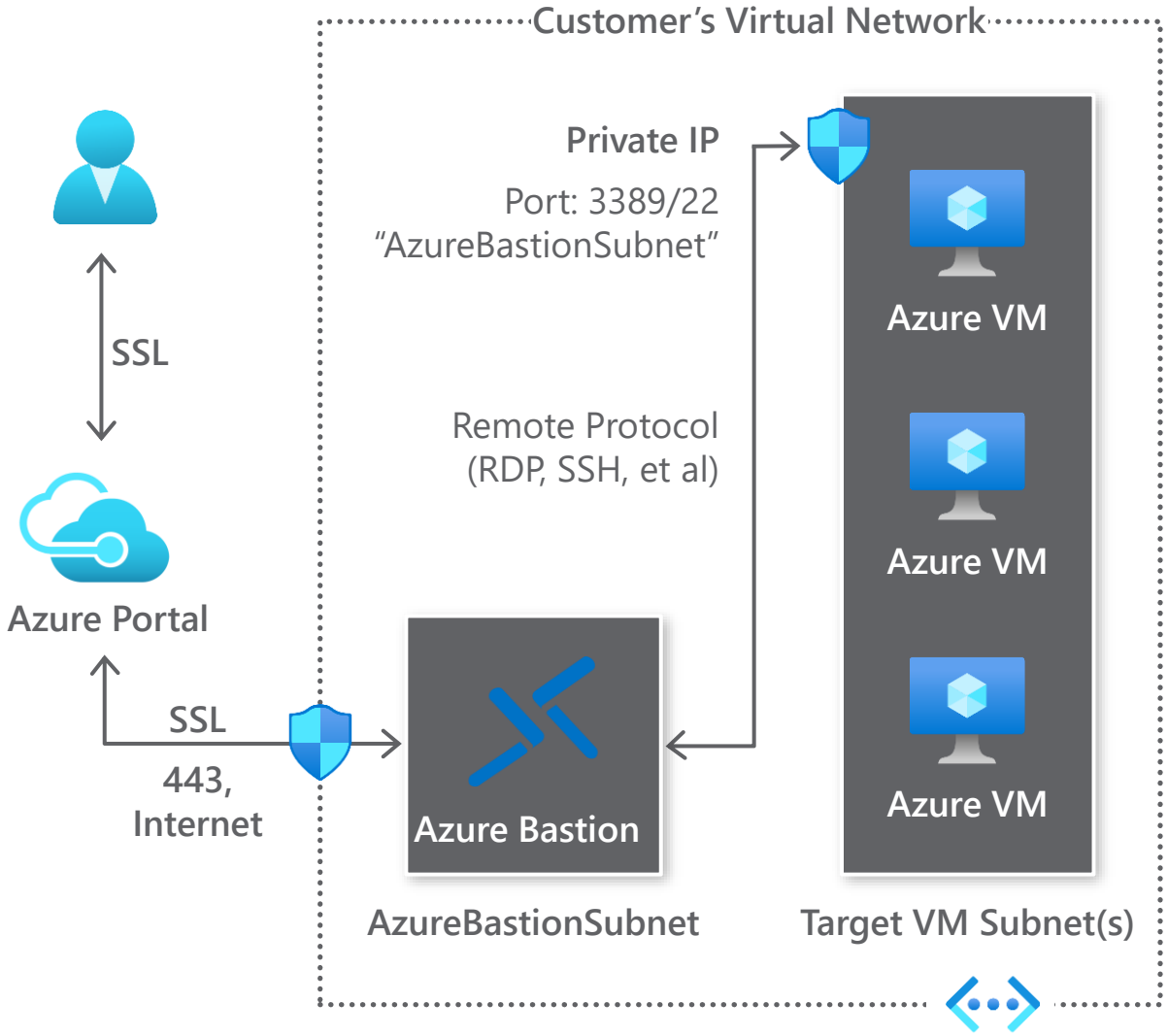


Azure Bastion

RDP/SSH to your workload using HTML5 standards-based web-browser, directly in Azure Portal

Resources can be accessed without public IP addresses

Supported Azure resources include VMs, VM Scale Sets, Dev-Test Labs



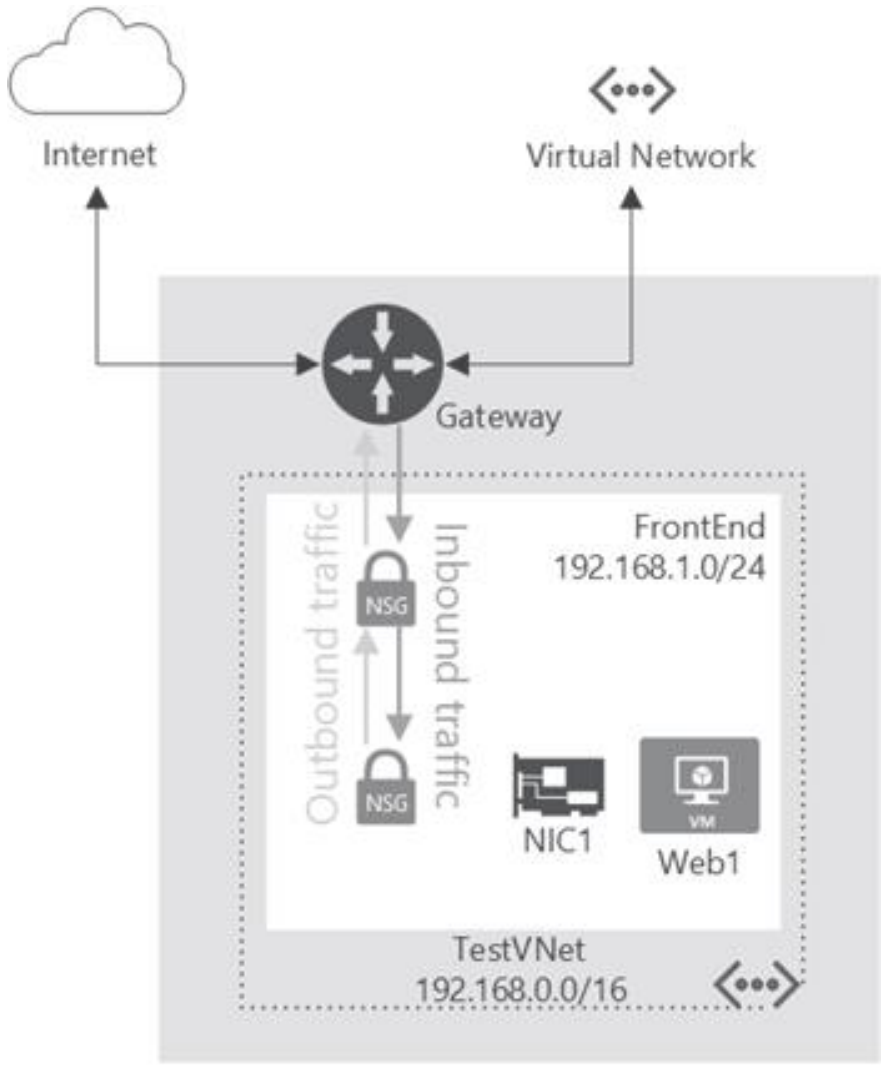
NSG key facts

- 5-tuple ACL's
  - Source IP, Destination IP, Source Port, Destination Port, Protocol (TCP, UDP, any)
  - Actions: allow or deny
  - Directions: inbound, outbound
  - Priority: 100-4096 (lower value = higher priority)

- Stateful
  - No need to define rules for «return traffic»

- Can be applied to NICs and Subnets (ARM)
  - Inbound connections: subnet-level NSG evaluated first, NIC-level NSG evaluated next
  - Outbound connections: NIC-level NSG evaluated first, subnet-level NSG evaluated next

Subnet-level and NIC-level NSG



NSG rules

- Default inbound rules
  - Allow any connections from other VMs in the same Vnet
  - Allow any connections from Azure Load Balancer (probes)
  - Deny all (minimum priority)

- Default outbound rules
  - Allow any connections to other VMs in the same Vnet
  - Allow any connections to the public internet
  - Deny all (minimum priority)

- Default tags
  - VIRTUAL_NETWORK, AZURE_LOADBALANCER, INTERNET

Azure Load Balancer

Azure Load Balancer

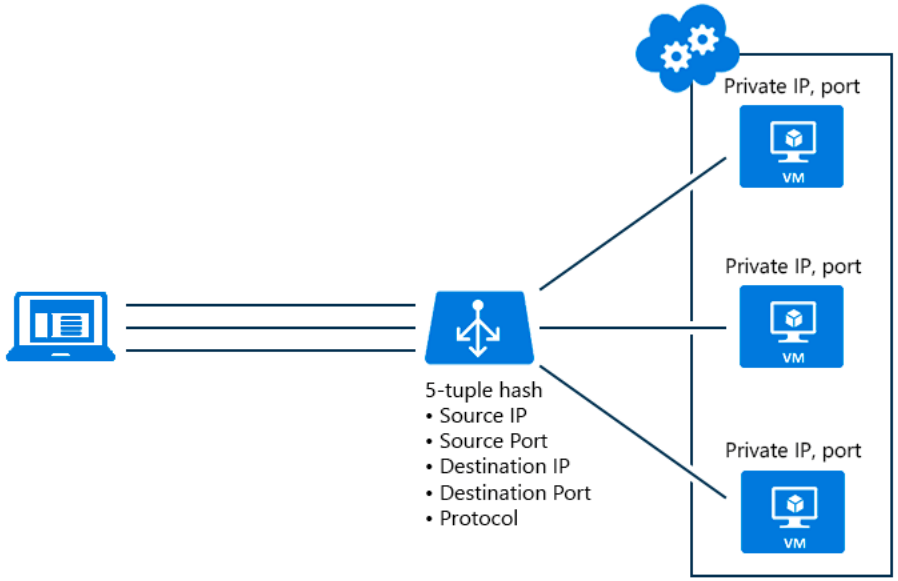
Allows you to scale your applications and create **high availability** and **resiliency** for your services and applications

Public

A public Load Balancer maps the public IP address and port number of incoming traffic to the private IP address and port number of the VM and vice versa.

Internal

An internal Load Balancer directs traffic only to resources that are inside a virtual network or that use a VPN to access Azure infrastructure.



Public Load Balancer

A public Load Balancer maps the **public IP address** and port number of incoming traffic to the **private IP address** and port number of the VM

Automatic reconfiguration

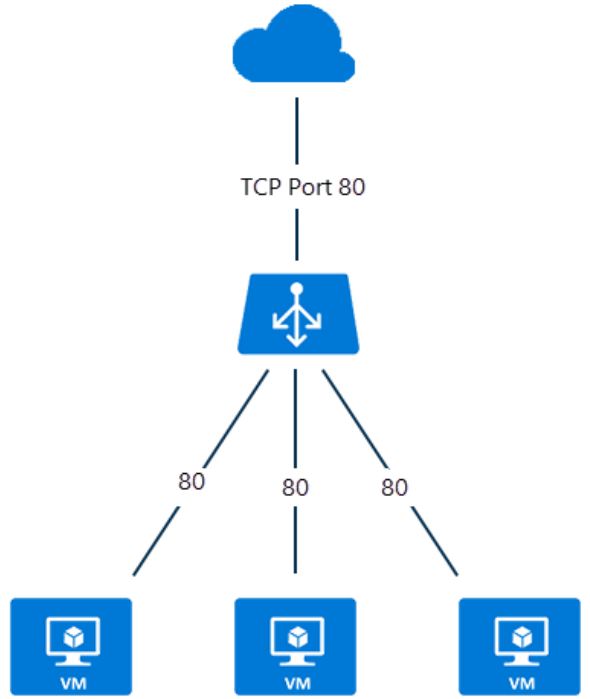
Instantly reconfigures itself as you scale instance up or down

Outbound connections (SNAT)

All outbound flows from private IP addresses inside your virtual network to public IP addresses on the internet can be translated to a frontend IP address of the Load Balancer

Default Distribution Mode

Azure Load Balancer distributes traffic evenly amongst multiple VM instance



Internal Load Balancer

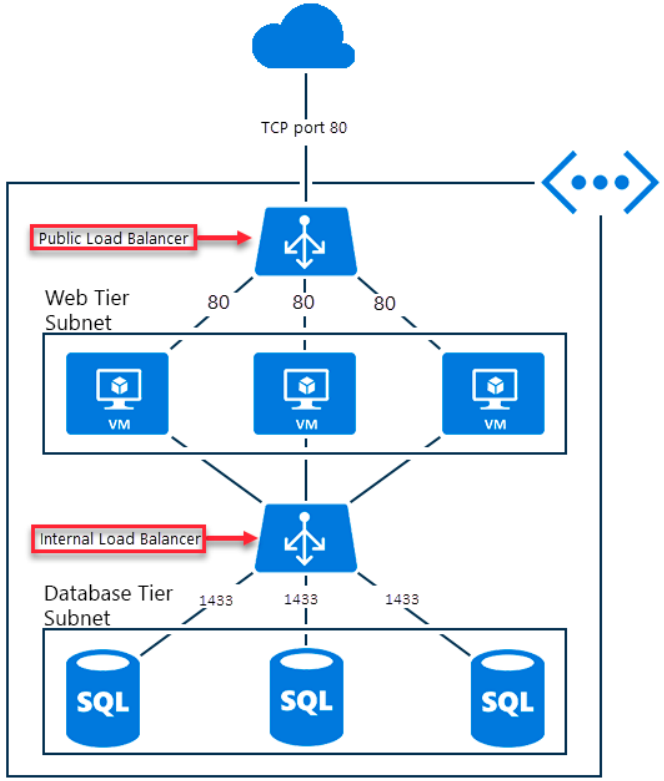
An internal Load Balancer directs traffic only to resources **inside a virtual network** or that use a VPN to access Azure infrastructure

Within a virtual network

Cross-premises virtual network

Multi-tier applications

Line-of-business applications



Azure Application Gateway (AppGW) and Web Application Firewall (WAF)

Azure Application Gateway (V2)

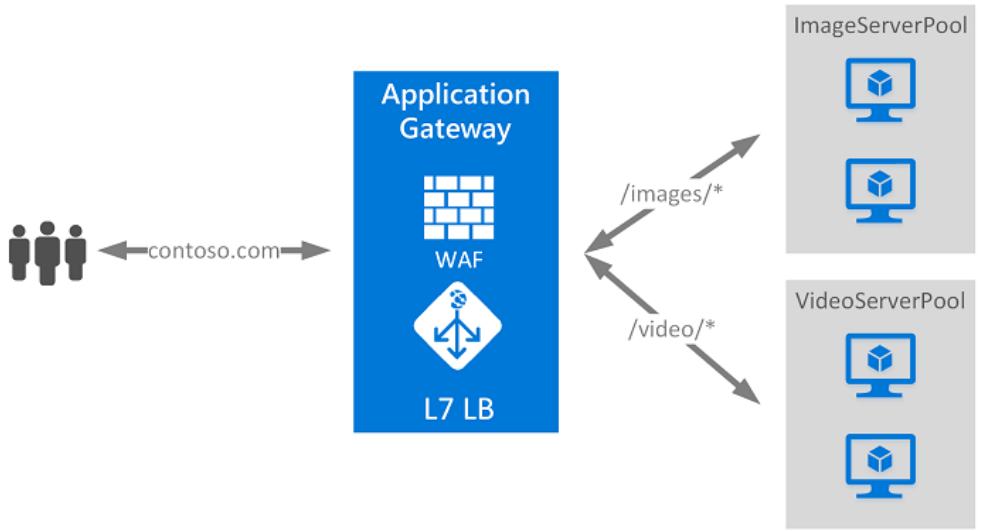
Azure Application Gateway is a **web traffic load balancer** that enables you to manage traffic to your web applications

Scalable

Web Application Firewall

SSL Offload

Integrated with Other Azure services



Application Gateway

Azure Kubernetes Services (AKS) Ingress Controller

Ingress for one or more AKS clusters in backend

Enhanced performance - use private IP of AKS pods

Azure Key Vault integration

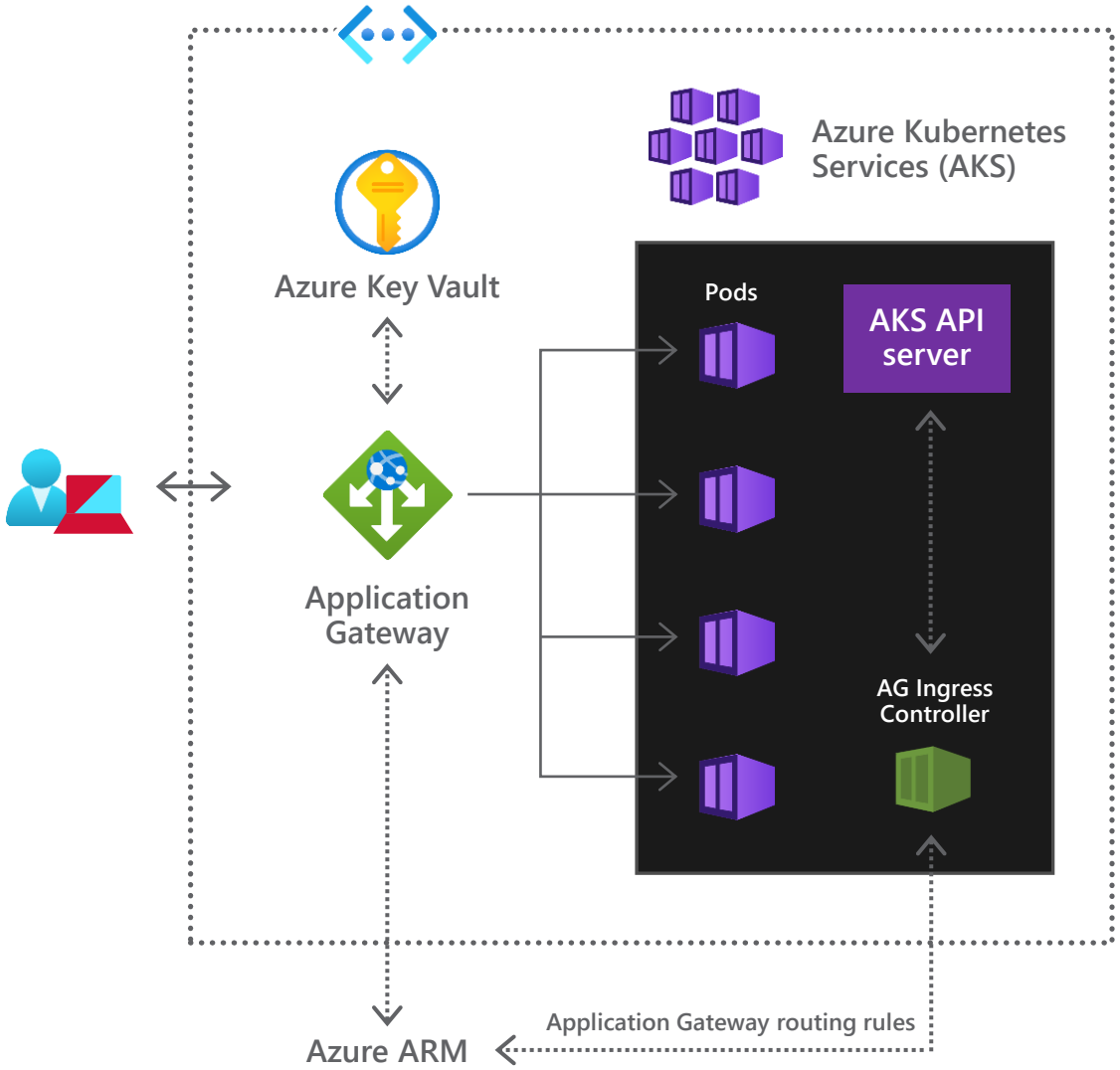
Centrally manage SSL certificates in Azure Key Vault

Enhanced Metrics

End to end latency, backend latency, backend error code, RPS/node metrics

Wildcard listener

Listeners enhanced to accept wildcards. No need to create new listener for each subdomain



Azure WAF

Unified WAF offering

Protect your apps at network edge or in Azure regions

Microsoft threat intelligence

Protect apps against automated attacks

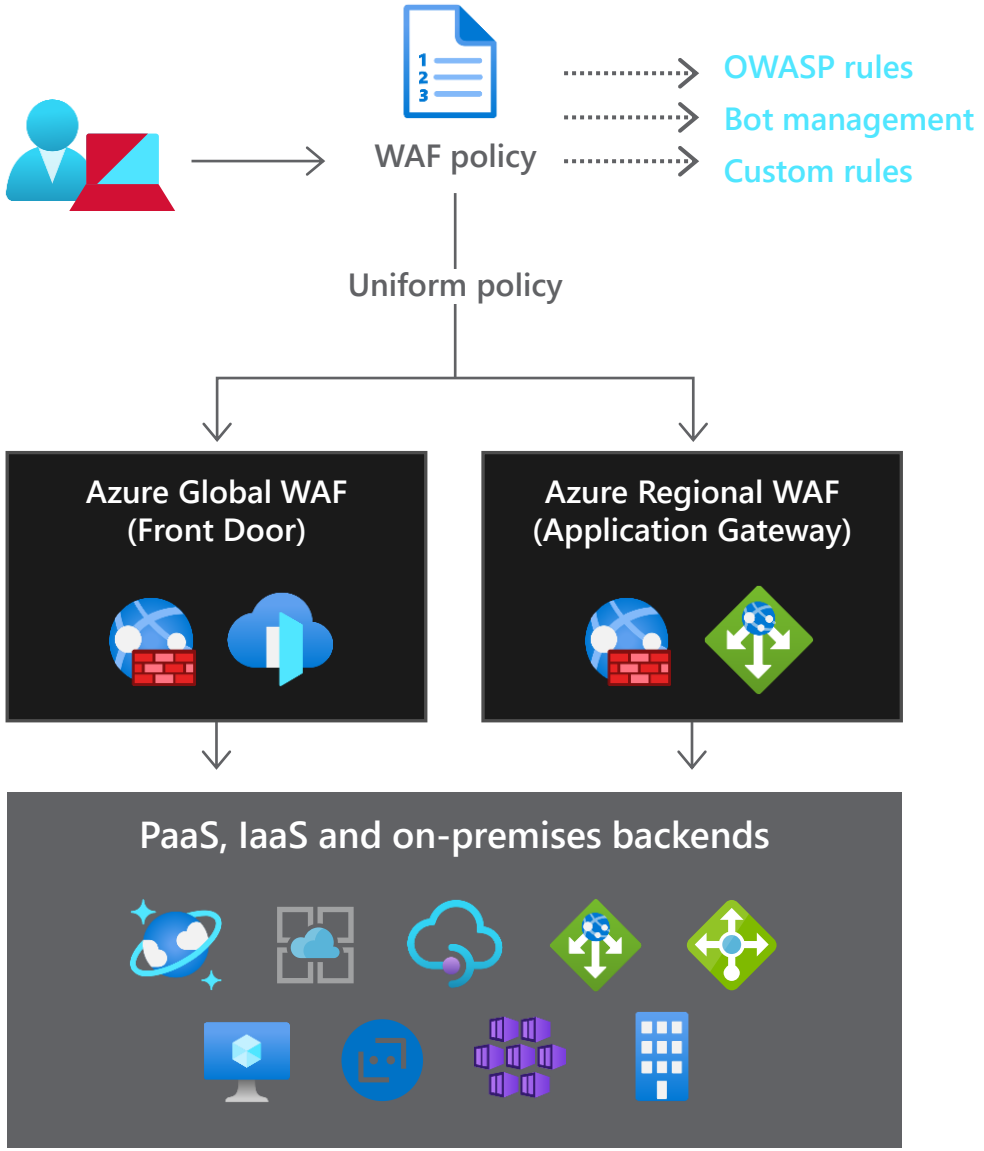
Manage good/bad bots with Azure BotManager RuleSet

Site and URI path specific WAF policies

Customize WAF policies at regional WAF for finer grained protection at each host/listener or URI path level

Geo filtering on regional WAF

Enhanced custom rule matching criterion includes filtering by country



Azure Traffic Manager (TM)
Azure Front Door (AFD)

Azure Traffic Manager

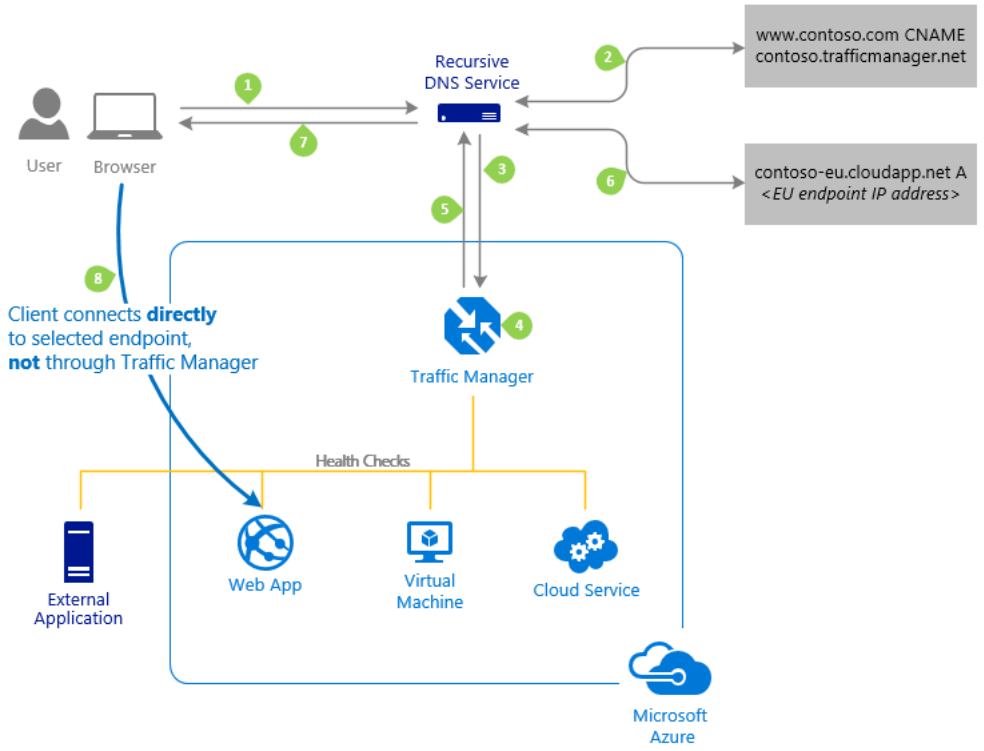
Azure Traffic Manager is a **DNS-based traffic load balancer** that enables you to distribute traffic optimally to services across global Azure regions

Global DNS load balancing

Automatic failover when an endpoint goes down

Combine with hybrid applications
Supports external, non-Azure endpoints so that it can be used with hybrid cloud and on-premises deployments

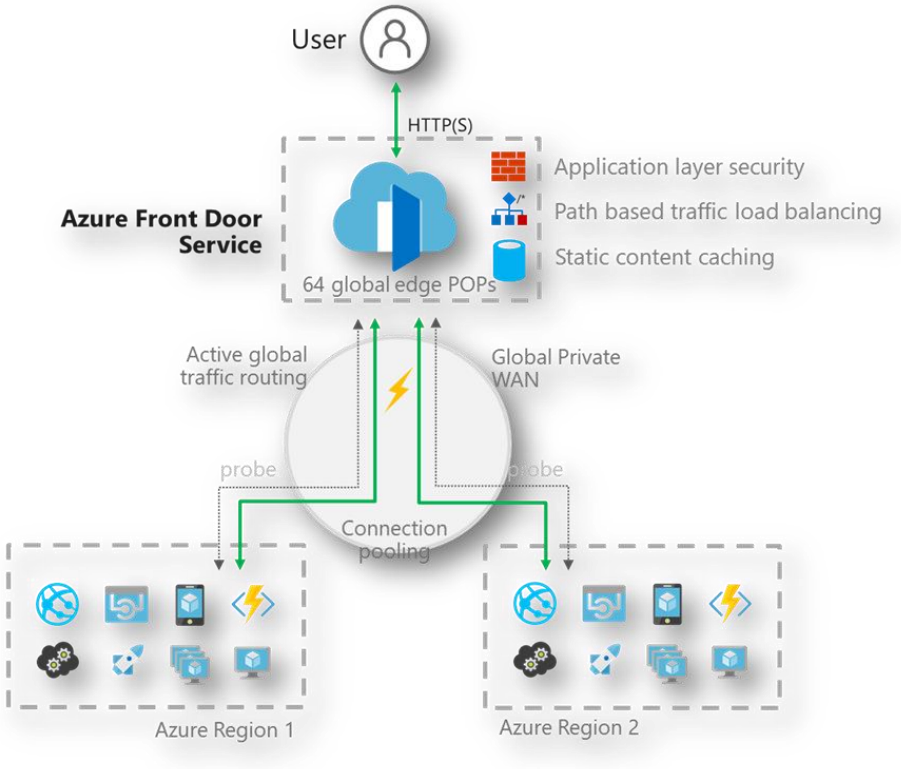
Distribute traffic for complex deployments
Use nested Traffic Manager profiles for sophisticated, flexible rules for complex deployments



Azure Front Door

Azure Front Door Service provides a **scalable and secure entry point** for fast delivery of your global web applications

- SSL offload and application acceleration
- Global HTTP load balancing with instant failover
- Application Firewall and DDoS protection
- Centralized traffic orchestration view



Azure Front Door

Single or multi-region app and API acceleration

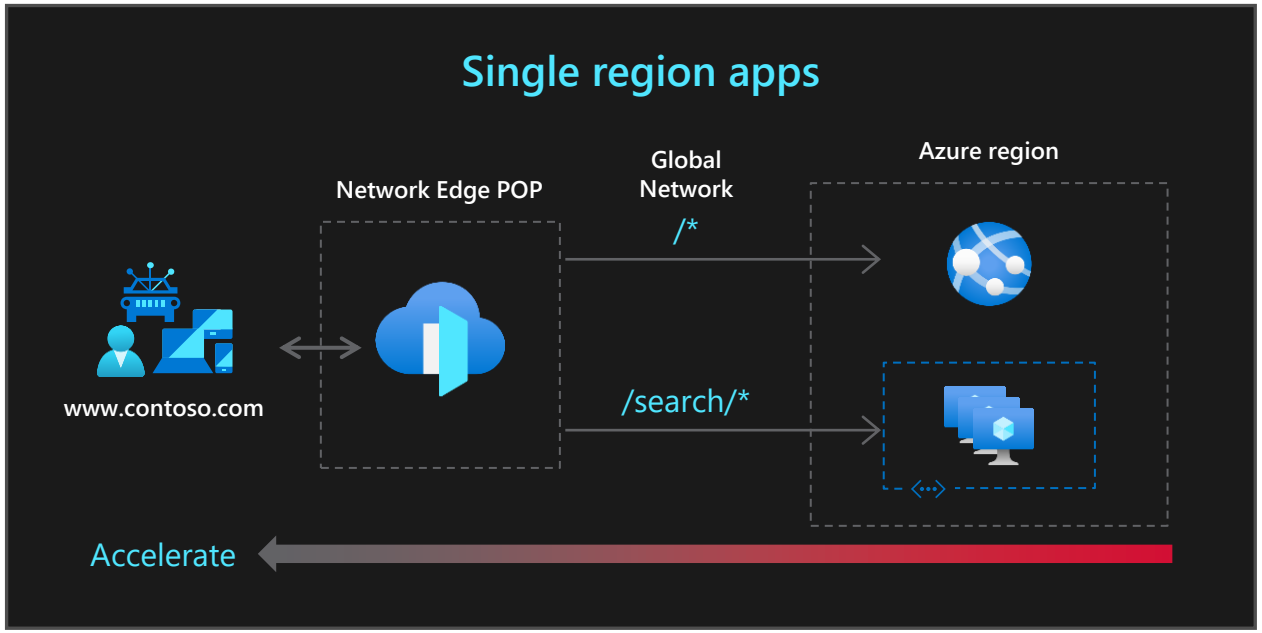
Improve HTTP performance and reduce page load times

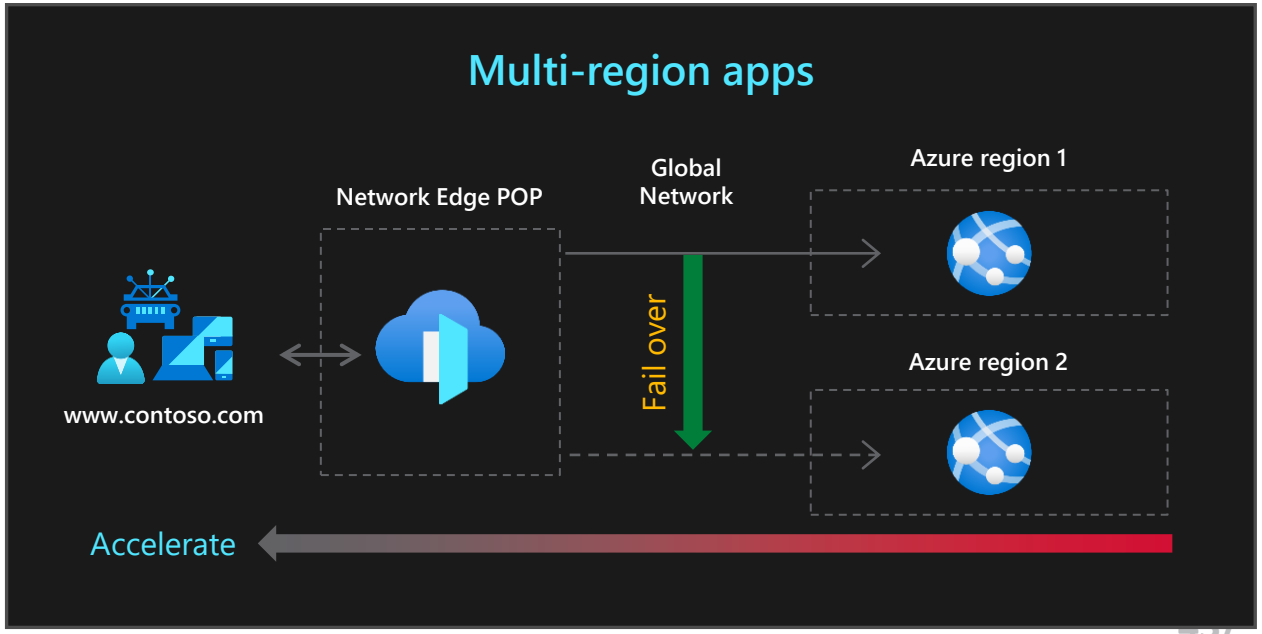
Load balancing at the Edge and fast-failover

Build always-on application experiences that fail-fast (safely)

Integrated SSL, WAF and DDoS

Protect and scale your application to global users, devices, traffic and attacks

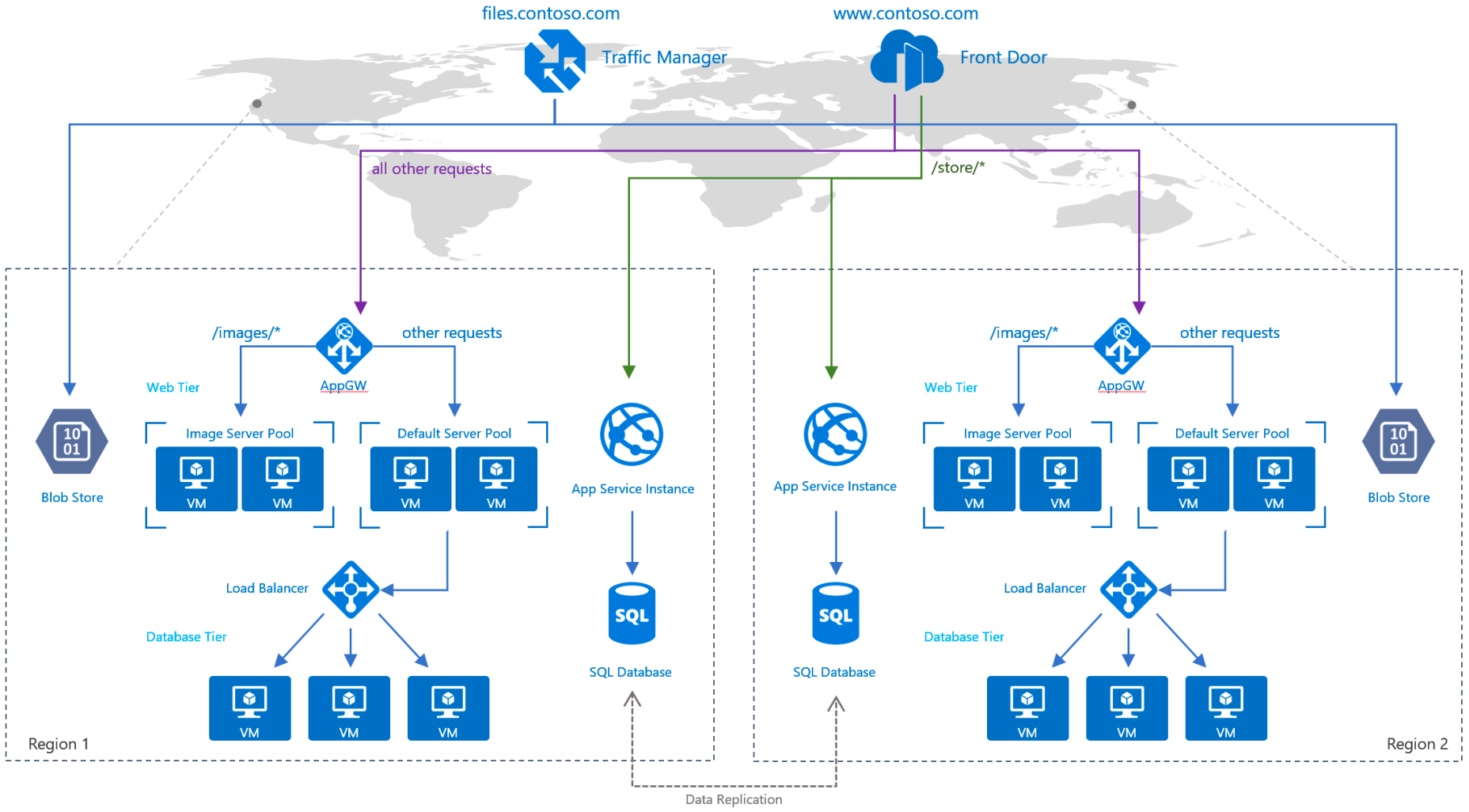




Traffic Manager or Front Door?

Traffic Manager	Front Door
Any protocol: Because Traffic Manager works at the DNS layer, you can route any type of network traffic; HTTP, TCP, UDP, etc.	HTTP acceleration: With Front Door traffic is proxied at the Edge of Microsoft's network. Because of this, HTTP(S) requests see latency and throughput improvements reducing latency for SSL negotiation and using hot connections from AFD to your application
On-premise routing: With routing at a DNS layer, traffic always goes from point to point. Routing from your branch office to your on-premises datacenter can take a direct path; even on your own network using Traffic Manager	Independent scalability: Because Front Door works with the HTTP request, requests to different URL paths can be routed to different backend/regional service pools (microservices) based on rules and the health of each application microservice
Billing format: DNS-based billing scales with your users and for services with more users, plateaus to reduce cost at higher usage	Inline security: Front Door enables rules such as rate limiting and IP ACL-ing to let you protect your backends before traffic reaches your application

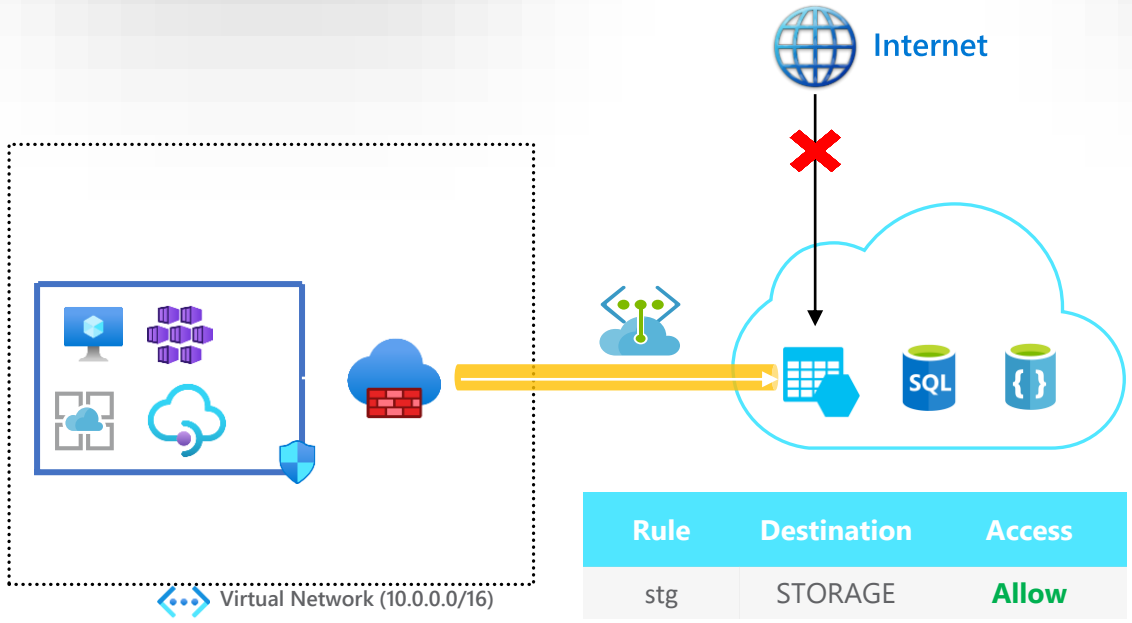
Traffic Manager or Front Door?



Service Endpoints and Private Link

Private PaaS

SERVICE ENDPOINT



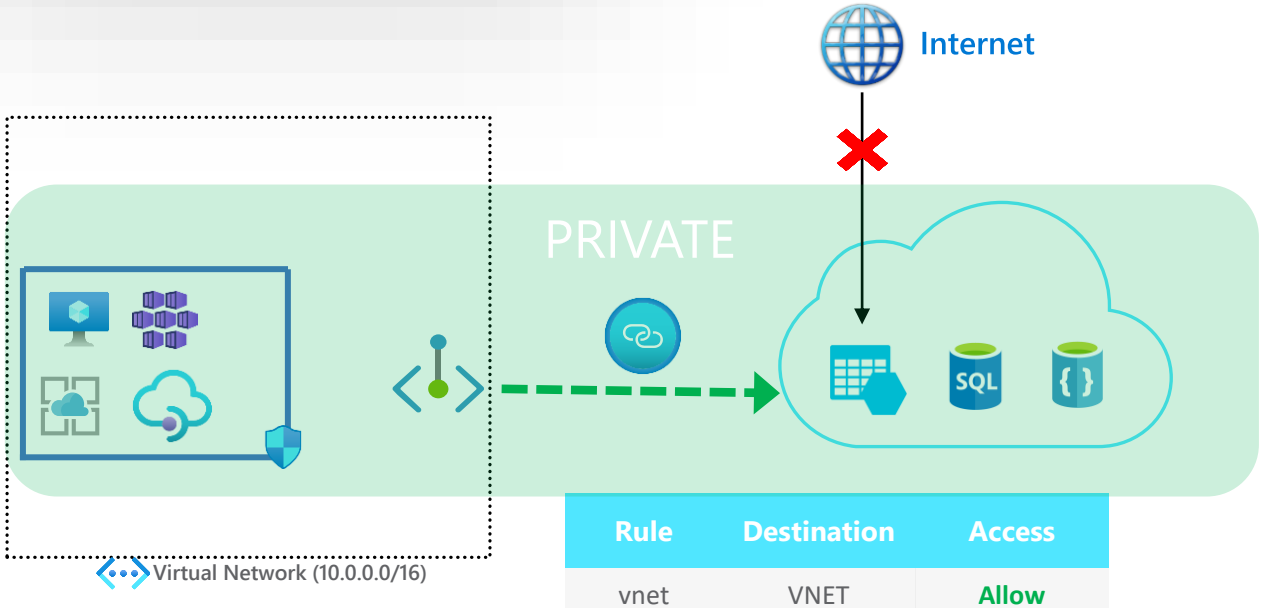
Rule	Destination	Access
stg	STORAGE	Allow
vnet	VNET	Allow
internet	INTERNET	Deny

VNet to PaaS service via the Microsoft backbone

Destination is still a public IP address. NSG opened to Service Tags

Need to pass NVA/Firewall for exfiltration protection

PRIVATE LINK – PRIVATE ENDPOINT



Rule	Destination	Access
vnet	VNET	Allow
internet	INTERNET	Deny

VNet Paas via the Microsoft backbone

PaaS resource mapped to Private IP Address. NSGs restricted to VNet space

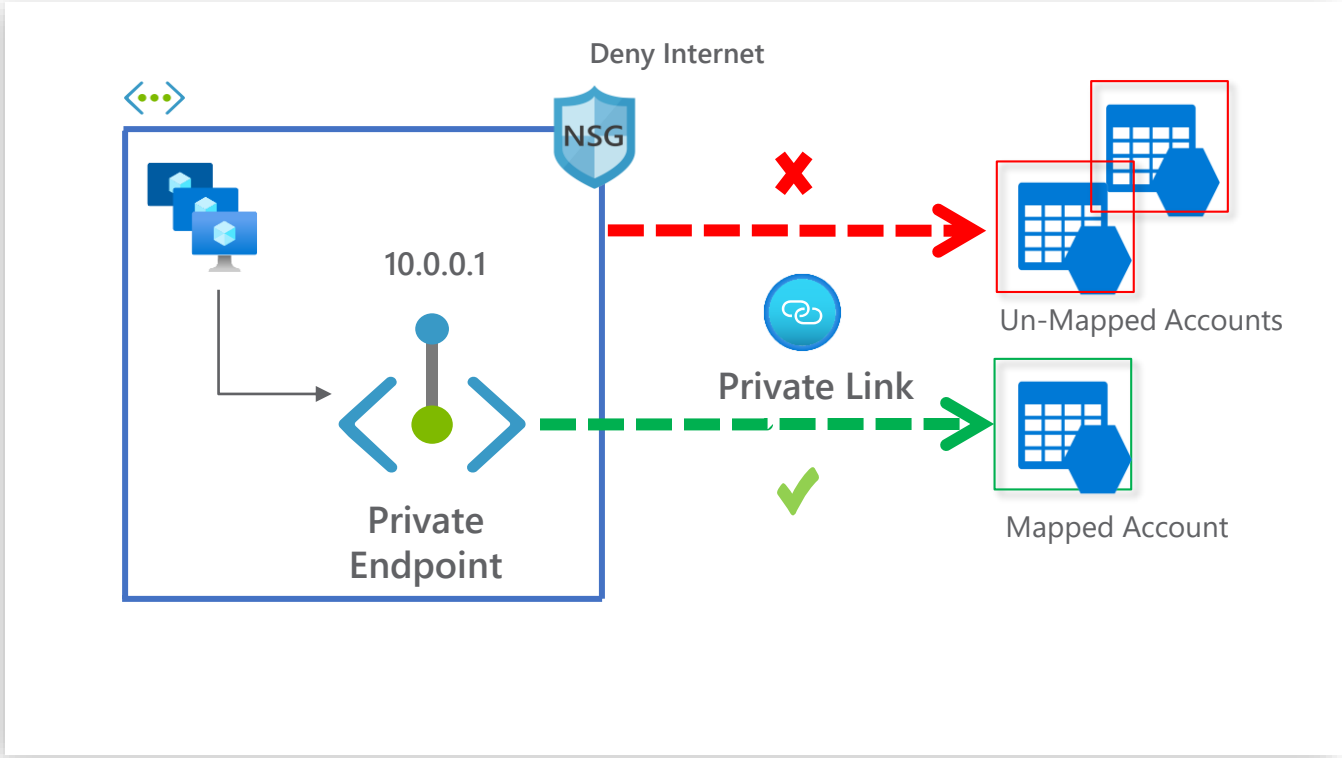
In-built data exfiltration protection

Data Exfiltration Protection

Private Endpoint maps specific PaaS resource to an IP address, not the entire service

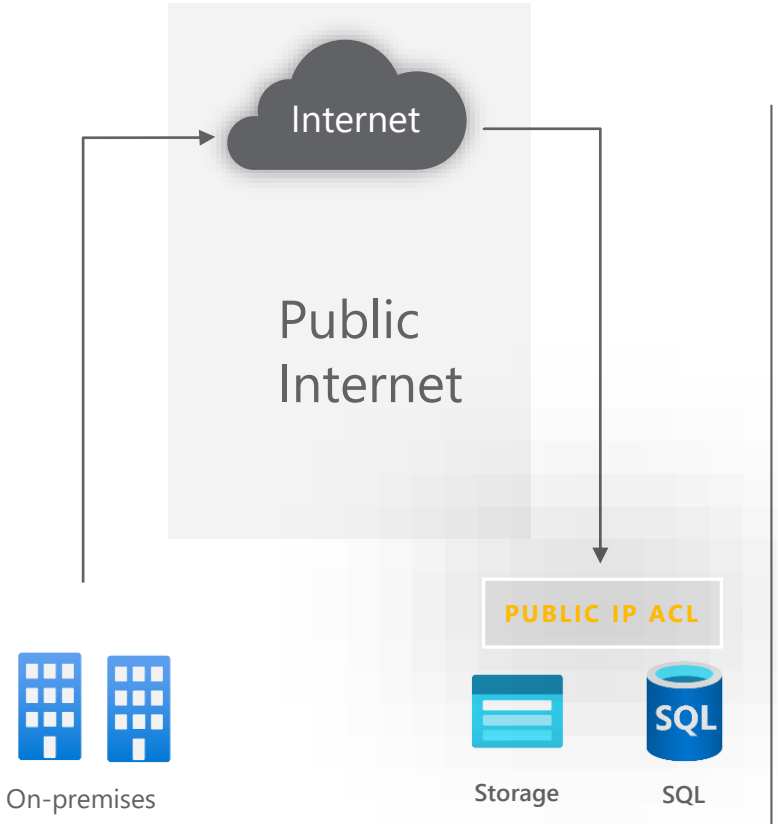
Access only to mapped PaaS resource

Data exfiltration protection is in-built



Secure connectivity from on-premises

Good

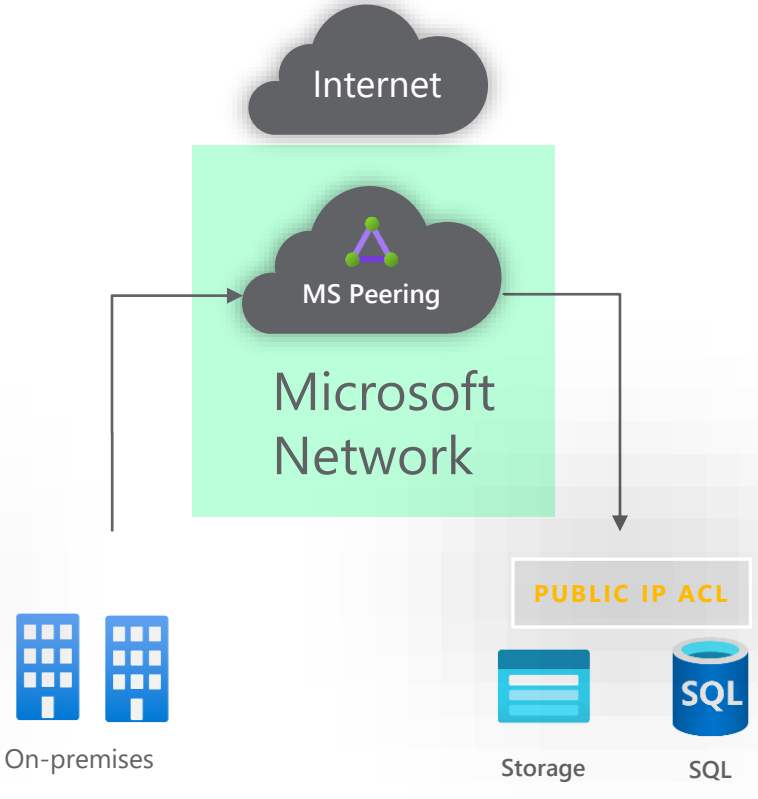


Traffic traverses the Internet

Secured using ACLs on Public Ips

Corporate firewall open to Azure Public IPs

Better

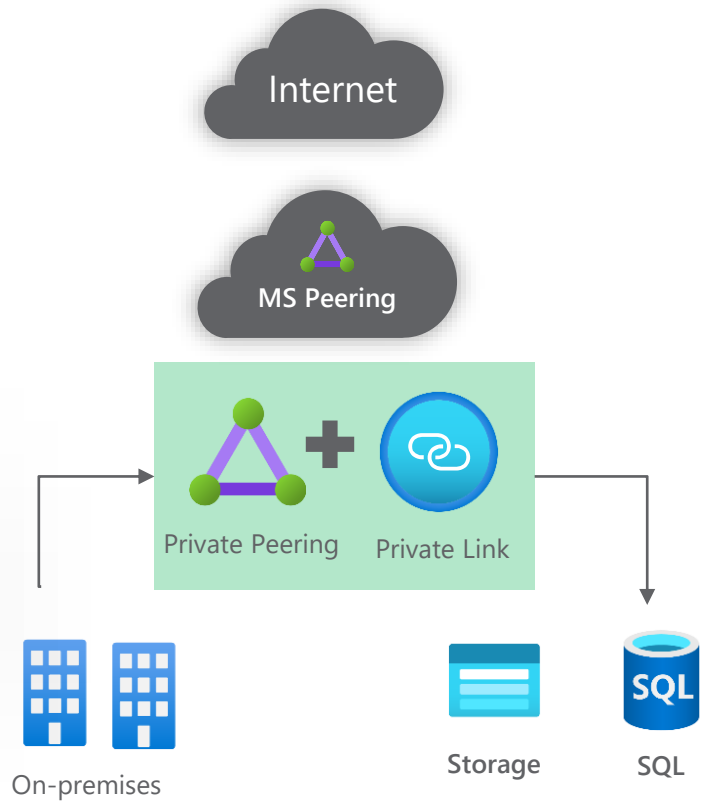


Traffic stays within Microsoft and partner network

MS Peering draws Microsoft Public IP traffic

Corporate Firewall open to Azure Public IPs

Best

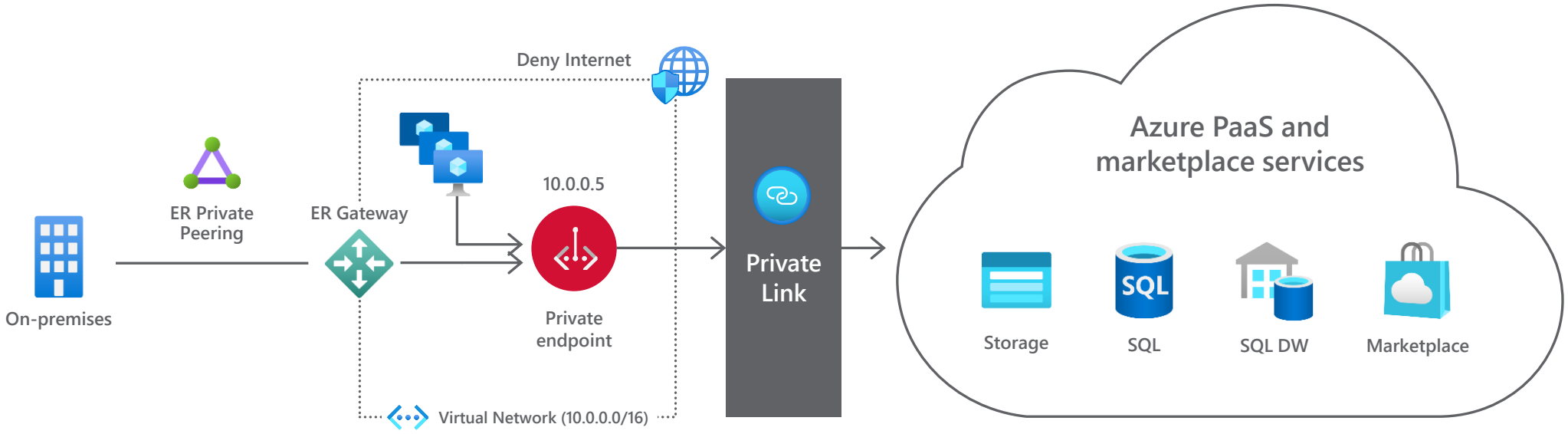


Traffic is fully private traversing the Microsoft network

No exposure of public IPs on either side

Corporate Firewall open only to private

Azure Private Link



Private Link for Azure Storage, SQL DB and customer own service

Private access from Virtual Network resources, peered networks and on-premise networks	In-built Data Exfiltration Protection	Predictable private IP addresses for PaaS resources	Unified experience across PaaS, Customer Owned and marketplace Services

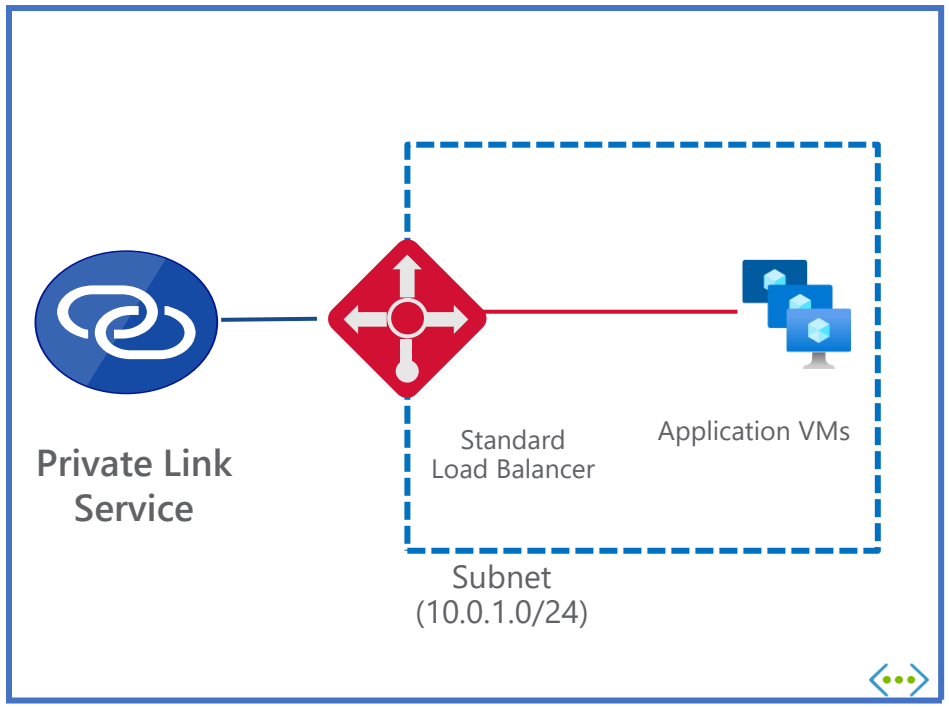
Your Own Private Link Service

- Create or Convert your existing services into Private Link Service
- VNet-VNet Connectivity without worrying about overlapping IP Space
- No regional, tenant, subscription or RBAC restrictions
- Easily Scale and manage your service

Private Link Service

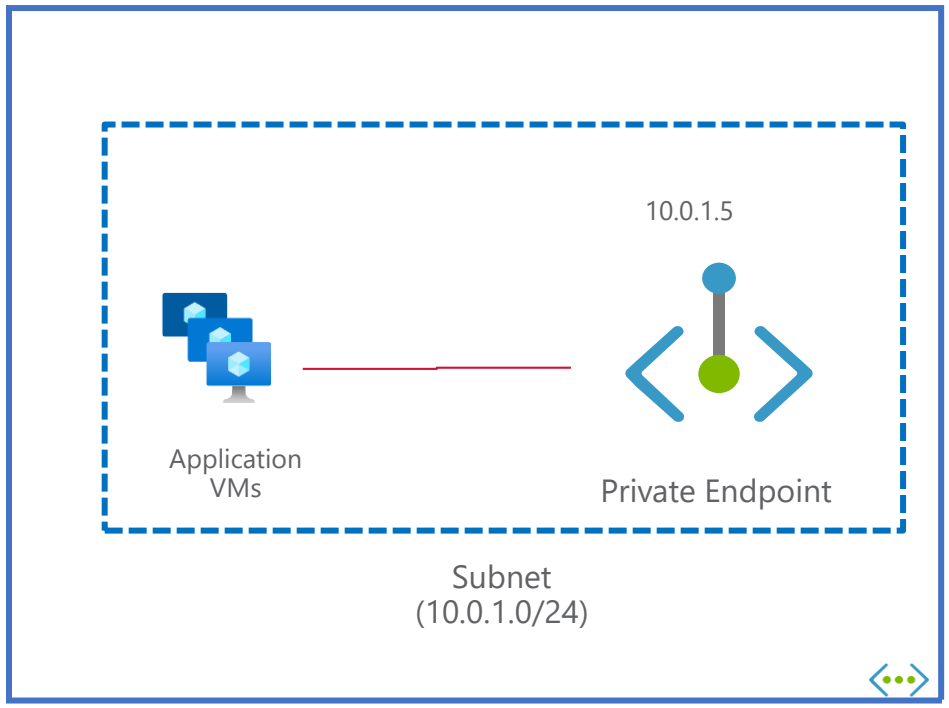
Create Private Link Service

- Application running behind Standard Load Balancer can be converted into Private Link service with one click of a button/one API call
- Private Link Service tied to Frontend IP configuration of Standard Load Balancer
- Frontend IP Configuration can be either Public or Private



Consume Private Link Service

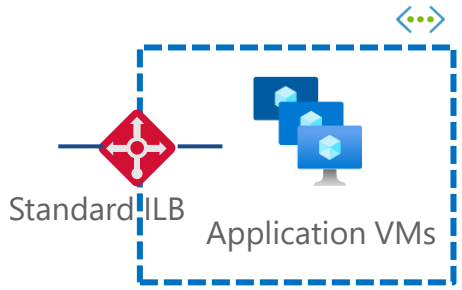
- Create a Private Endpoint in your VNet linking to Private Link Service.
- Multiple consumers can connect to same service. No RBAC restrictions.



Approval Workflow

Service Consumer

Service Provider



1. Create your application behind a standard Load Balancer.

2. Create a Private Link Service attached to SLB FE IP.

Subnet

3. Share the private link service ID (Alias/ARM URI) with consumers. You can either do it offline or advertise publicly.

<ServiceName>. <GUID>. <region>.azure.privatelinkservice

4. Create a Private endpoint in any subnet by specifying a private Link service URI/Alias.

5. Configure your DNS record for easy access using the private IP address (CA).

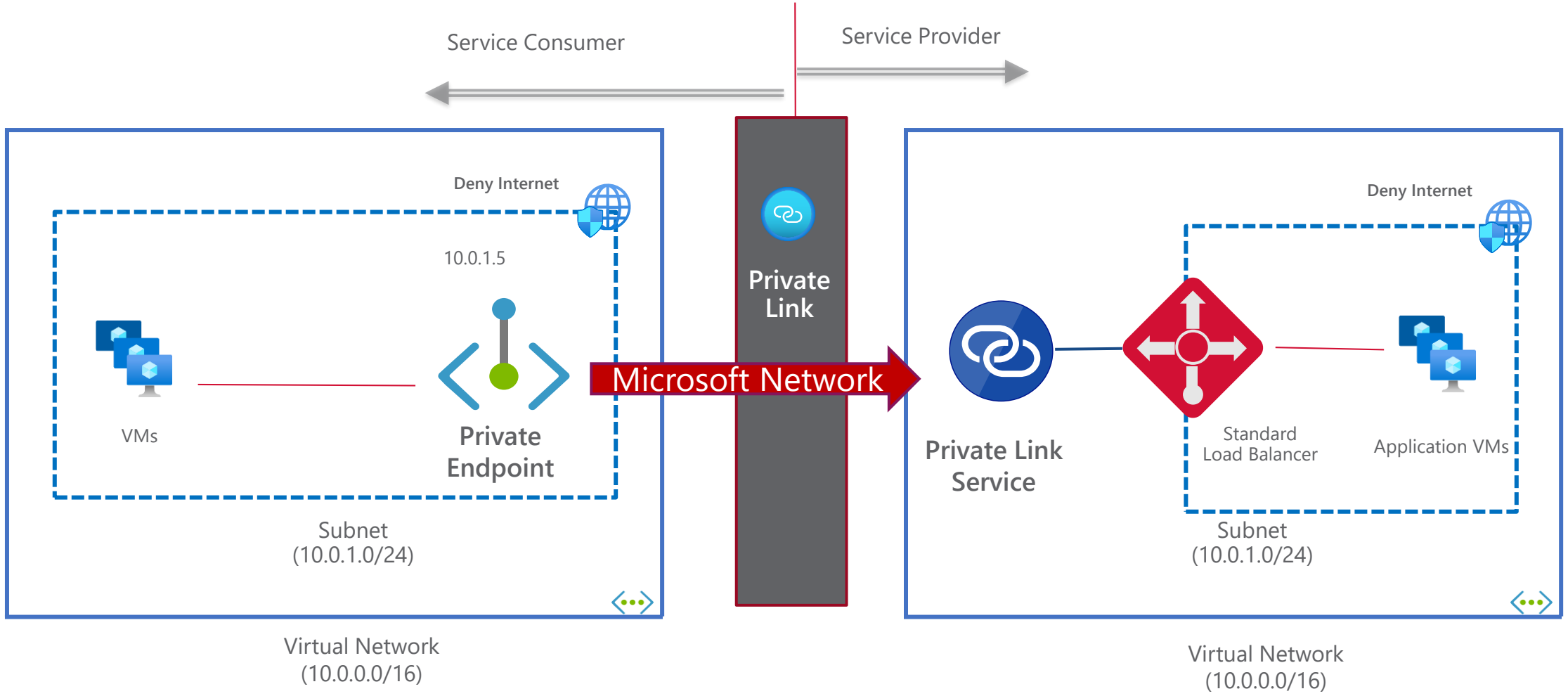
A request will be sent to provider for approval

6. Act on the request – Accept/Reject It.

7. Connection Succeeded/Rejected.

Decision sent to consumer

Complete Picture



Q&A