#GlobalAzure

#CloudGenVerona

@cloudgen_verona

Thanks to all the sponsors

PREMIUM SPONSOR

4WARD

KIRATECH®
WE DEVOPS IT

BASIC SPONSOR

CODICEPLASTICO

dgroove
Tecnologia emozionale.

CloudGen
ominidi verso l'evoluzione

TOPIC

Azure Networking

Come realizzare architetture di rete ibride, sicure e funzionali in Azure

Who I am

Francesco Molfese

@FrancescoMolf

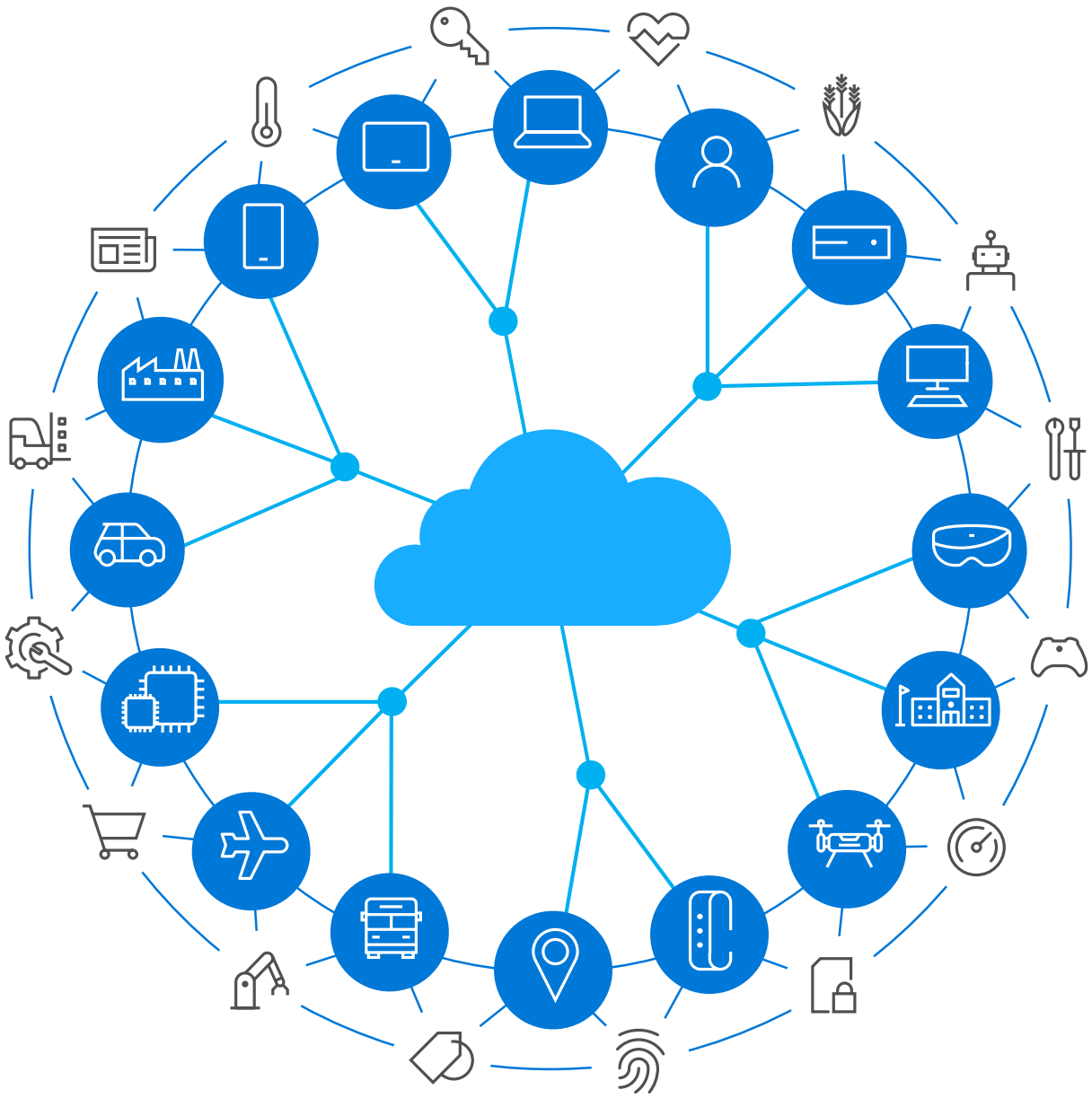
francescomolfese

https://www.linkedin.com/in/francescomolfese

Who I am

- Senior Consultant presso Progel S.p.A.
- Microsoft MVP Cloud Datacenter Management
- Microsoft Certified Trainer (MCT)
- Community Lead della Cloud Community Italiana (www.cloudcommunity.it)

How Networking is Changing

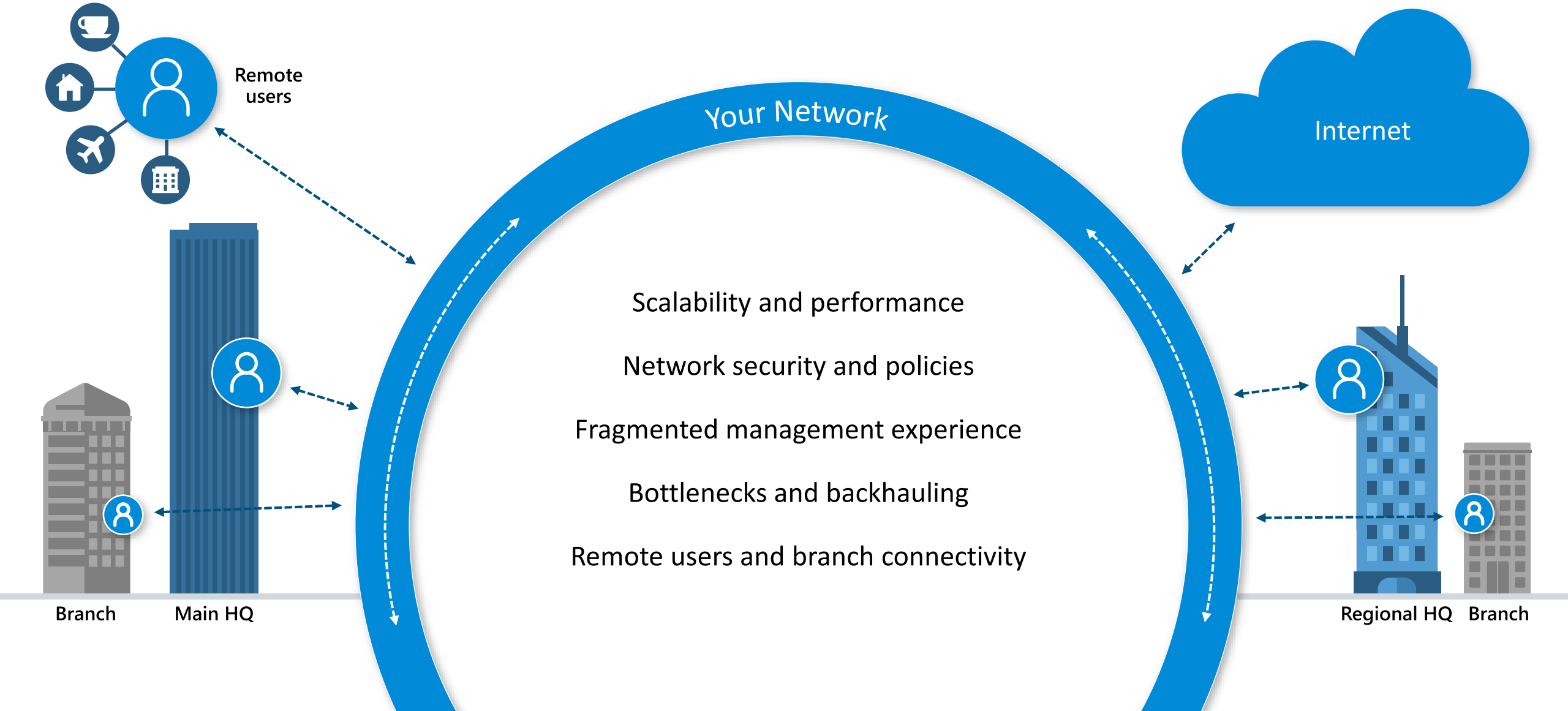


Organizations are hitting a tipping point where more traffic is going to the cloud than to on-premises datacenters

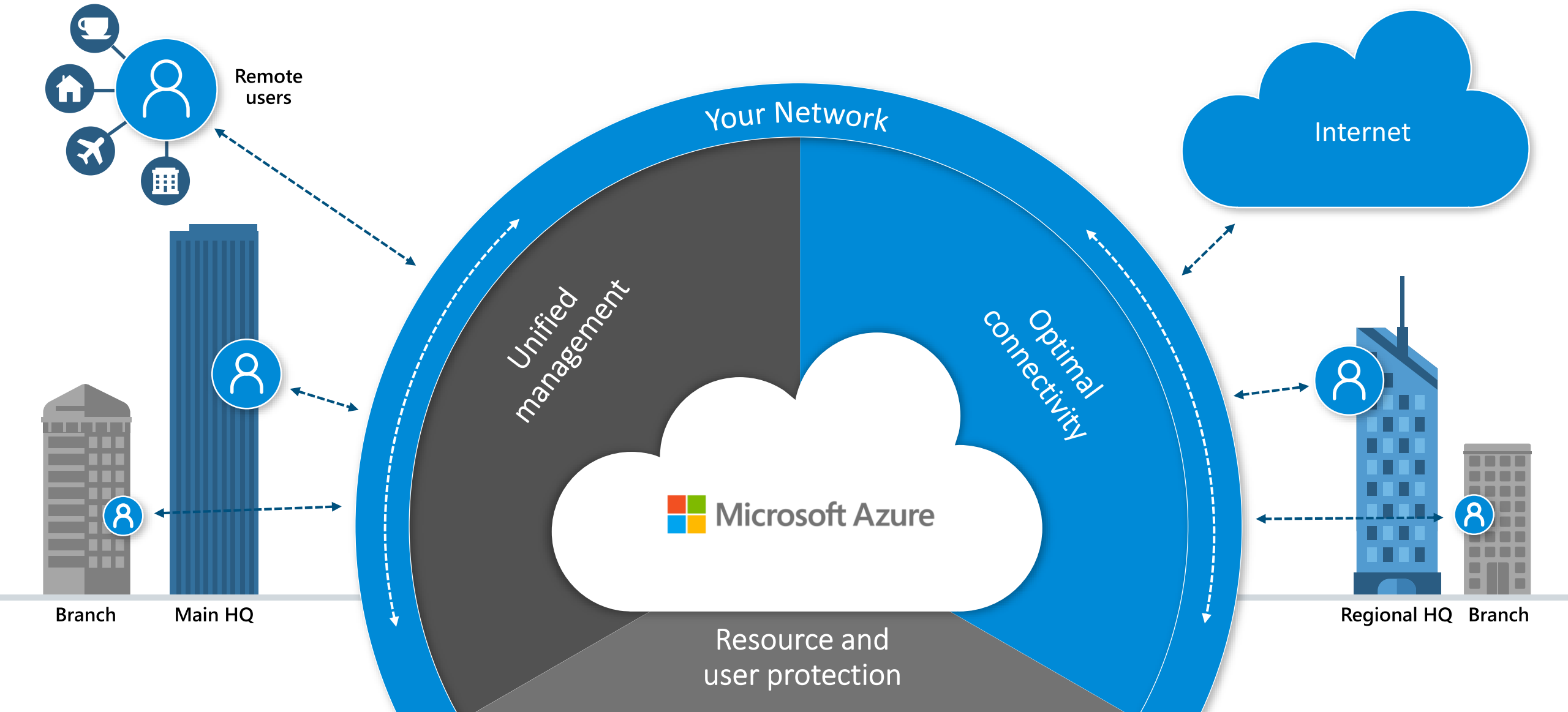
Requires foundational changes

- a new network design
- a new network security approach
- a new application delivery model
- a comprehensive monitoring approach integrated with devops

Your network strategy must address evolving needs



Build a secure, high-performant, and reliable global network in the cloud



Azure Networking Services

Connect

- Virtual Network
- Virtual WAN
- ExpressRoute
- VPN
- DNS

Protect

- DDoS Protection
- Firewall
- Network Security Groups
- Web Application Firewall
- Virtual Network Endpoints

Monitor

- Network Watcher
- ExpressRoute Monitor
- Azure Monitor
- Virtual Network TAP

Deliver

- CDN
- Front Door
- Traffic Manager
- Application Gateway
- Load Balancer

Hybrid Networking in Azure

Embracing a new era of distributed cloud connectivity

What we get asked by customers around cloud connectivity

How do I connect to Azure using high bandwidth connections?

How do I use SDWAN & Internet to connect to Azure?

How do I take advantage of Microsoft's global network?

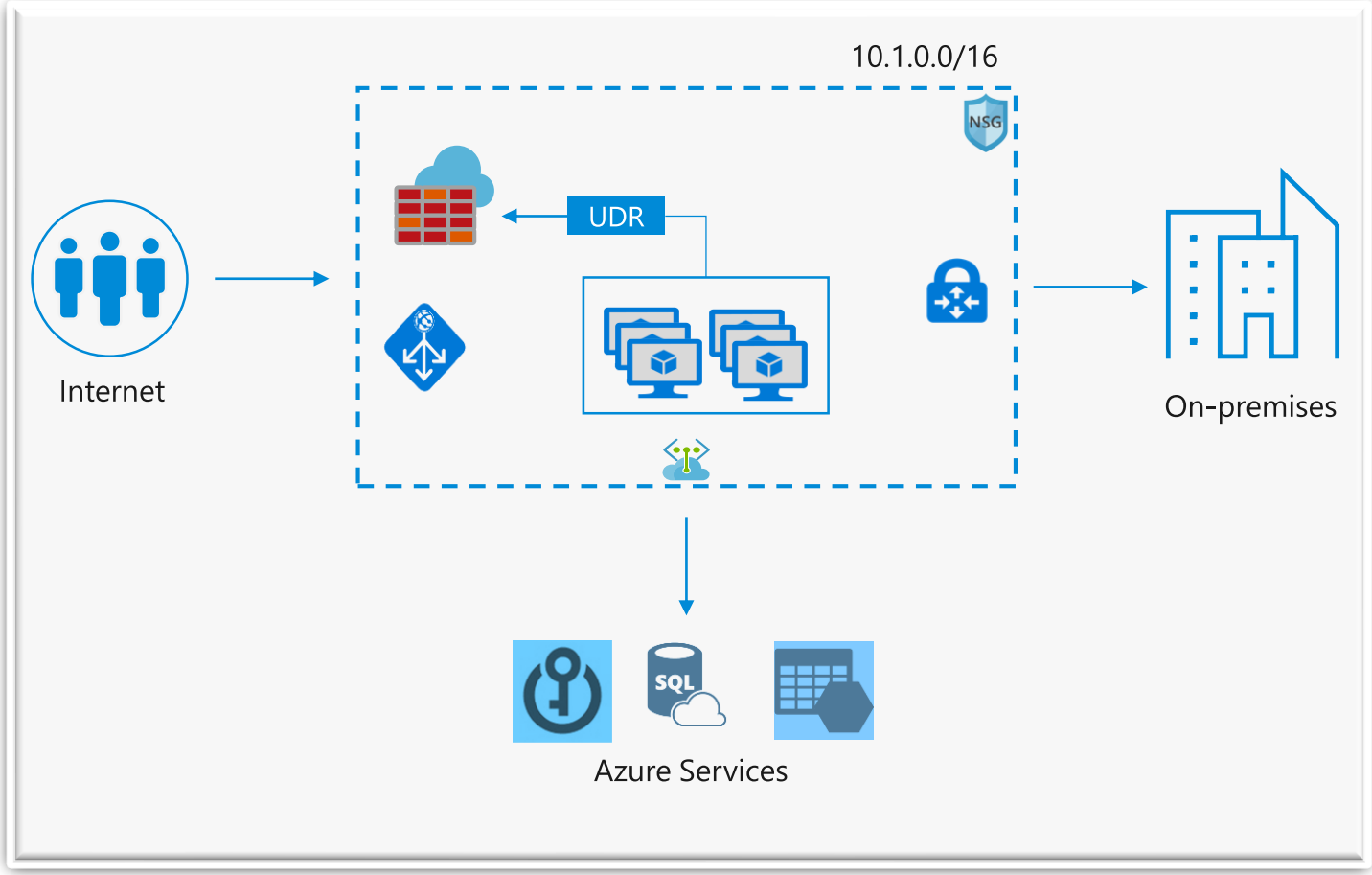
What options do I have for branch office connectivity?

How advanced are Azure Virtual Network capabilities?

Azure Virtual Networks

Your virtual private network in the cloud

- Private isolated logical network
- Supports Network ACLs and IP Management
- User defined routing for network virtual appliances
- Extends on-premises network to the cloud
- Provides secure connectivity to Azure services



Hybrid Connectivity options

Secure **point-to-site** connectivity	• POC Efforts • Small scale deployments • Connect from anywhere
Secure **site-to-site VPN** connectivity	• Connect to Azure compute from on-premises or another Azure region
VNet Peering	• VNet-to-VNet connectivity • Direct VM-to-VM connectivity • Peer VNets for routing and transit
ExpressRoute connectivity	• Connectivity from your on-premises data center to Azure virtual networks and PaaS Services

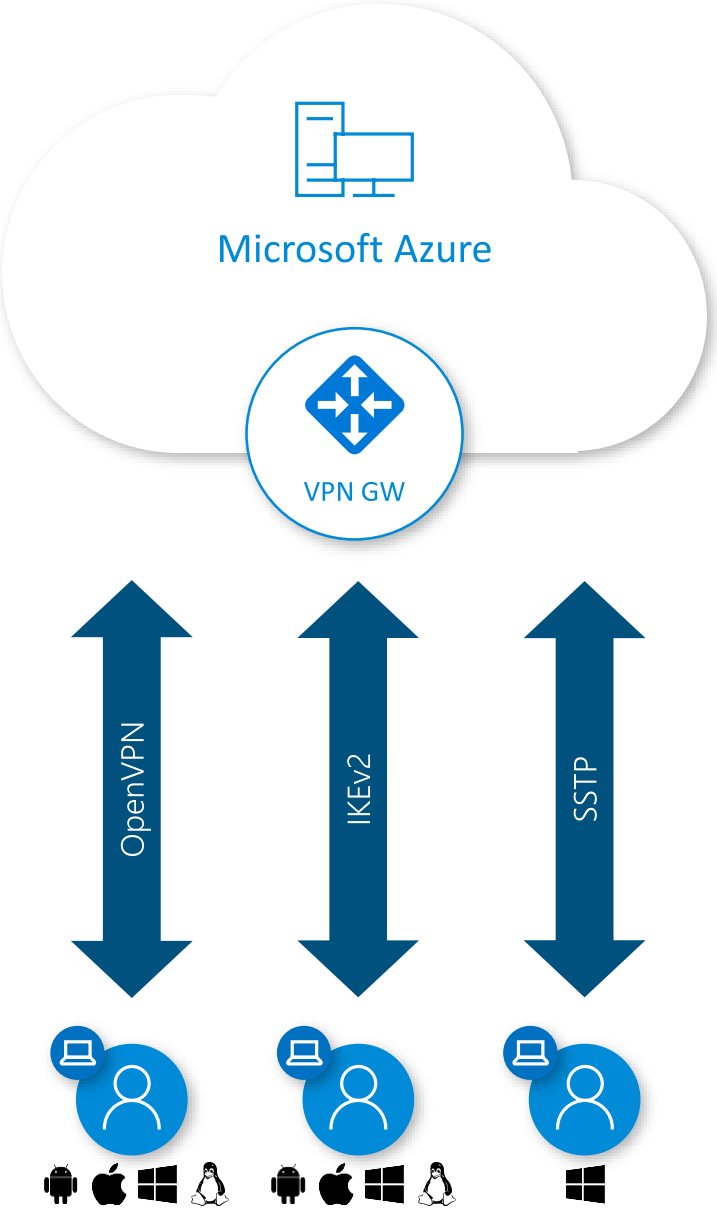
Azure VNet Demo

Comparing Hybrid Options

CAPABILITIES

	Security	Management	Workloads
ExpressRoute	Private isolated network between provider and Azure. Control over routing and traffic.	Configure once, simple to add new virtual networks	Enterprise Connectivity Mission Critical Disaster Recovery Hybrid Applications
Site-to-Site	Encrypted tunnel over the Internet	Configuration of IPSEC VPN device for each Virtual Network Created	Hybrid Applications Dev/Test Secure Management
Point-to-Site	Encrypted tunnel over the Internet	Configuration with each individual client machine.	Dev/Test Secure Management

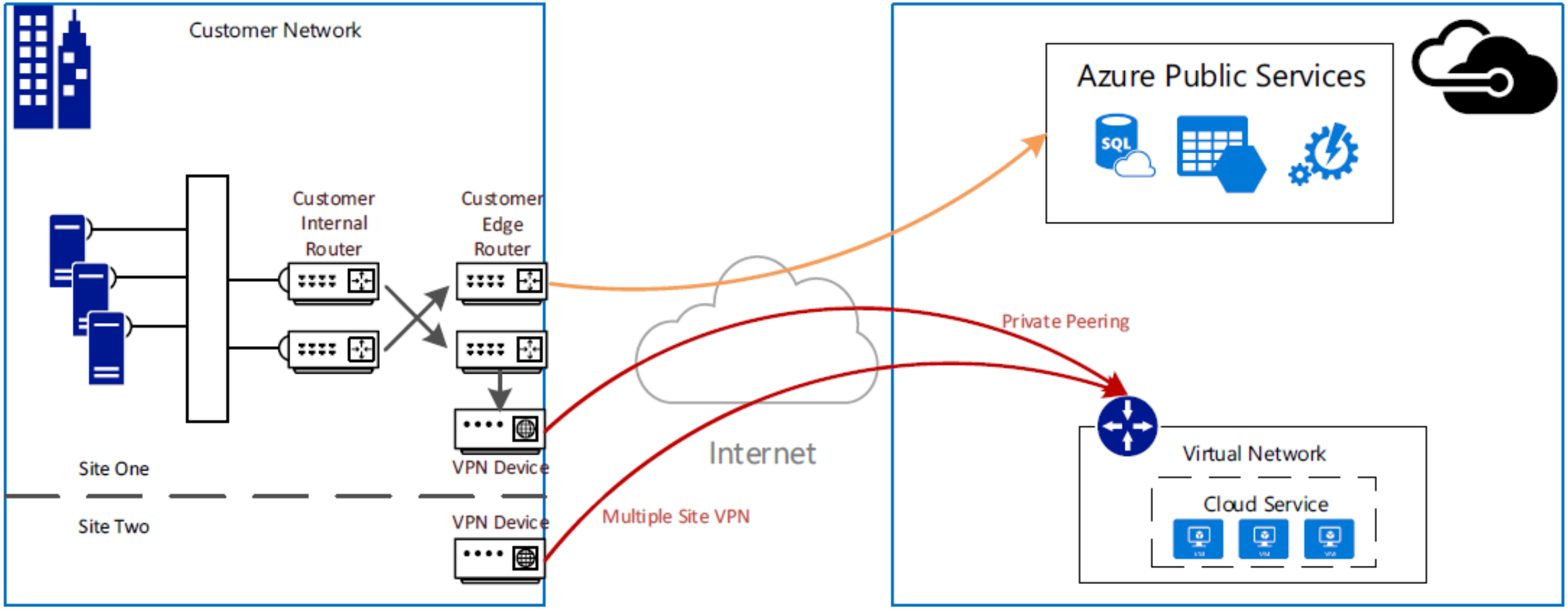
Point-to-site VPN



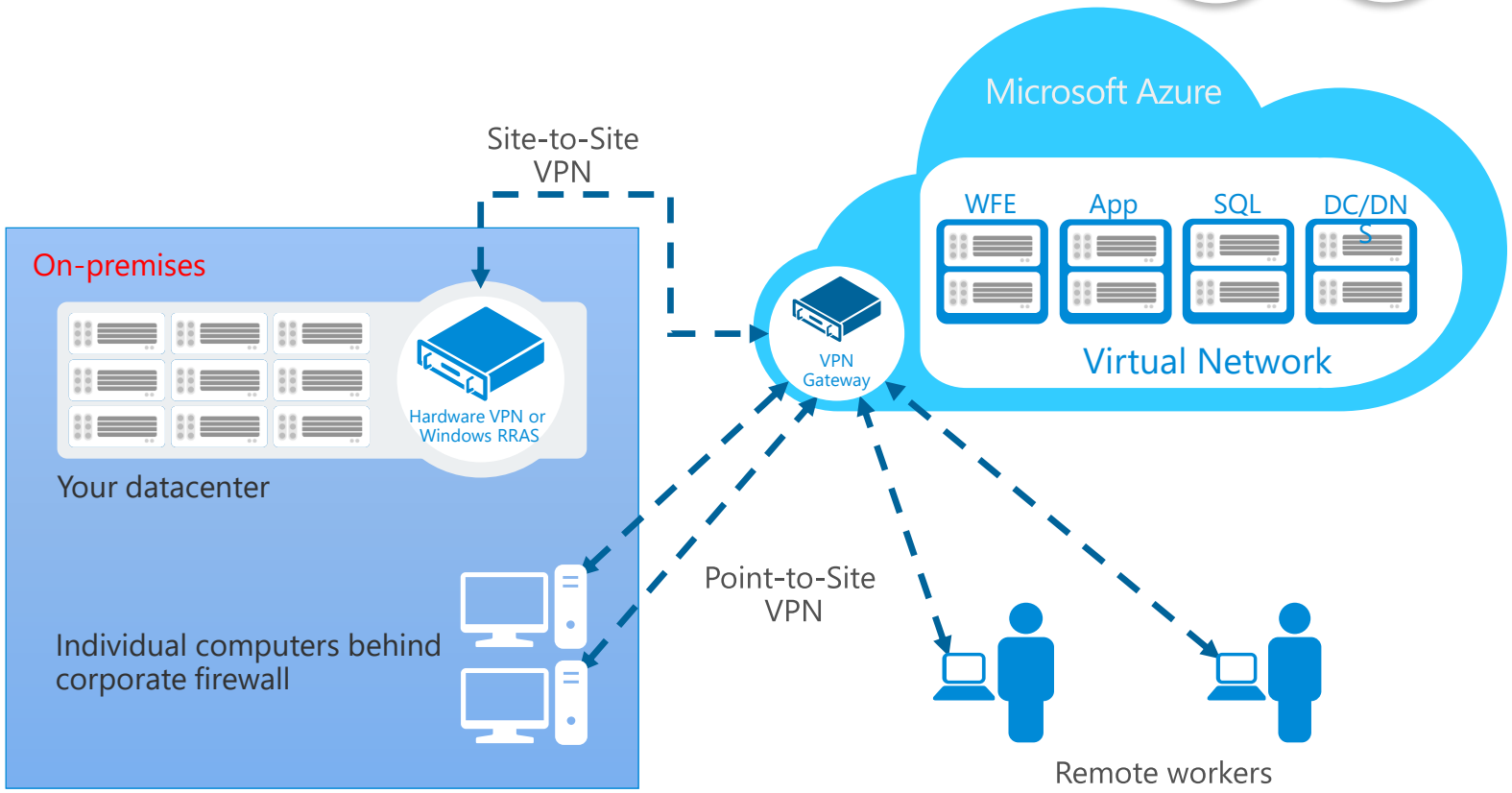
Point-to-site VPN enables remote users to access resources in Azure securely

	OpenVPN®	IKEv2
Max connections	10,000	10,000
Easy firewall traversal	Yes	No
Cross-platform support	Yes	Yes
Mobile device support	Yes	Yes
Authentication	Certificate-based	RADIUS and Certificate-based

Site-to-Site VPN connections



Site-to-Site Virtual Network

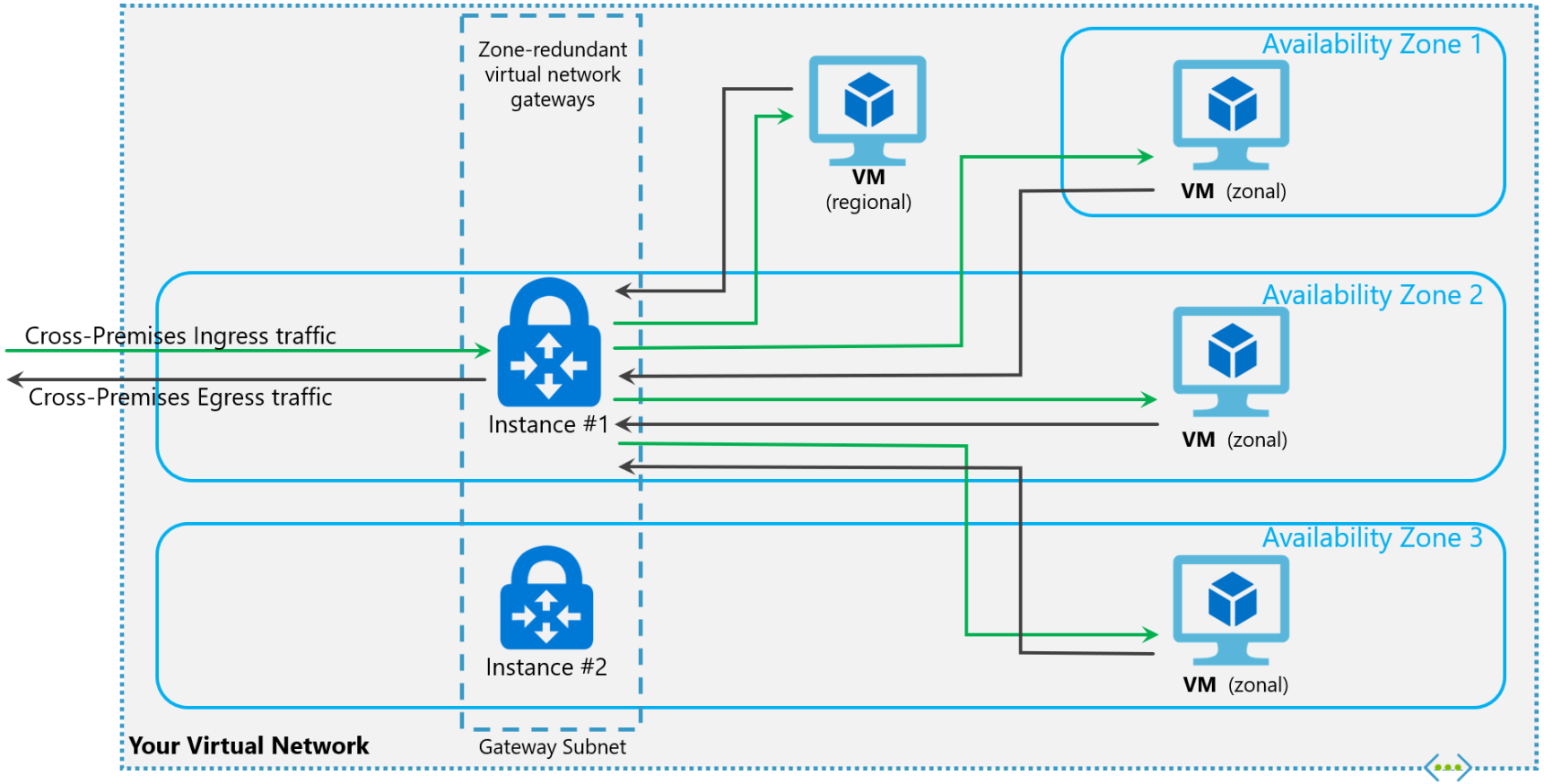


- Extend on-premises to the cloud securely
- On-ramp for migrating services to the cloud
- Use on-prem resources in Microsoft Azure (monitoring, AD, etc.)

Azure Vnet Connection Demo

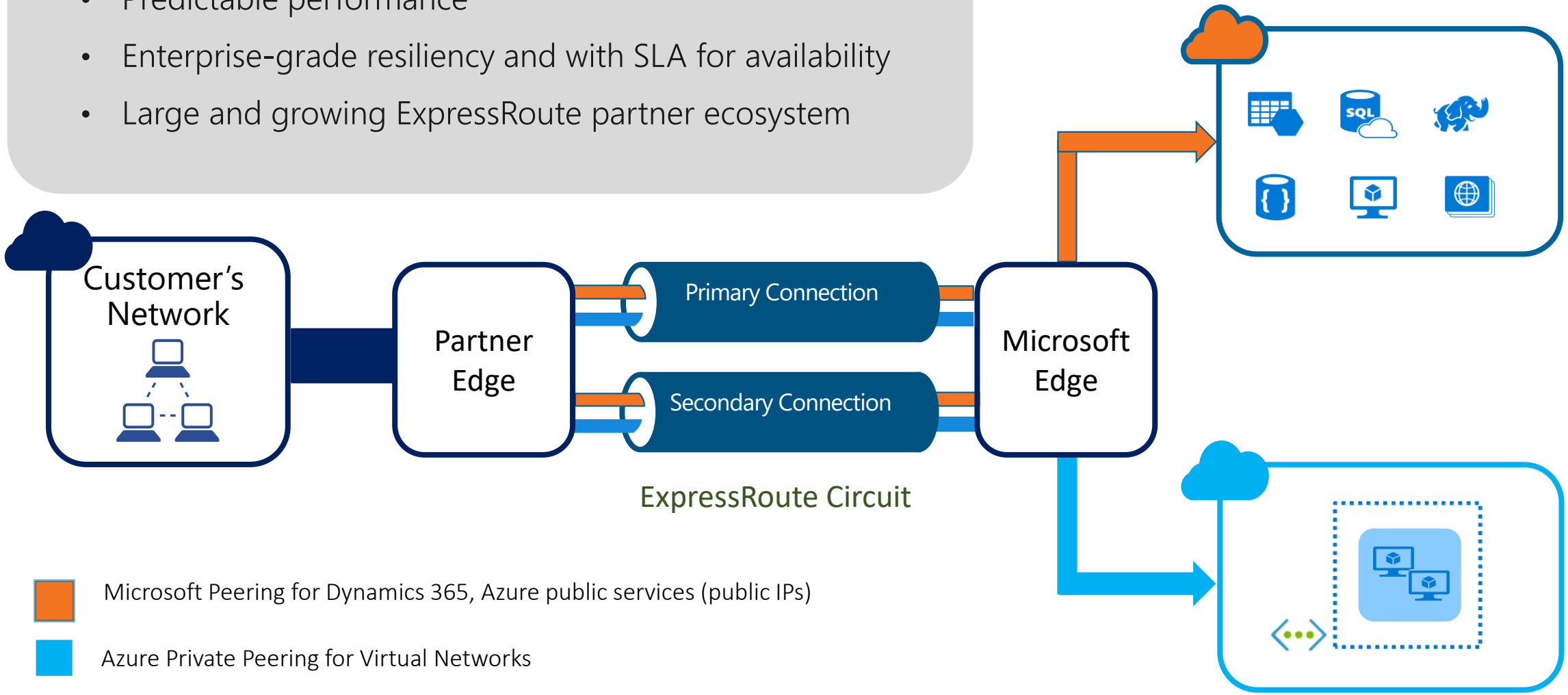
Zone redundant gateway for HA

- Gateway instances deployed in different AZs
- Physical & logical separation of AZs protecting Gateway from zone-level failure
- Feature and performance parity with current SKUs



Azure ExpressRoute

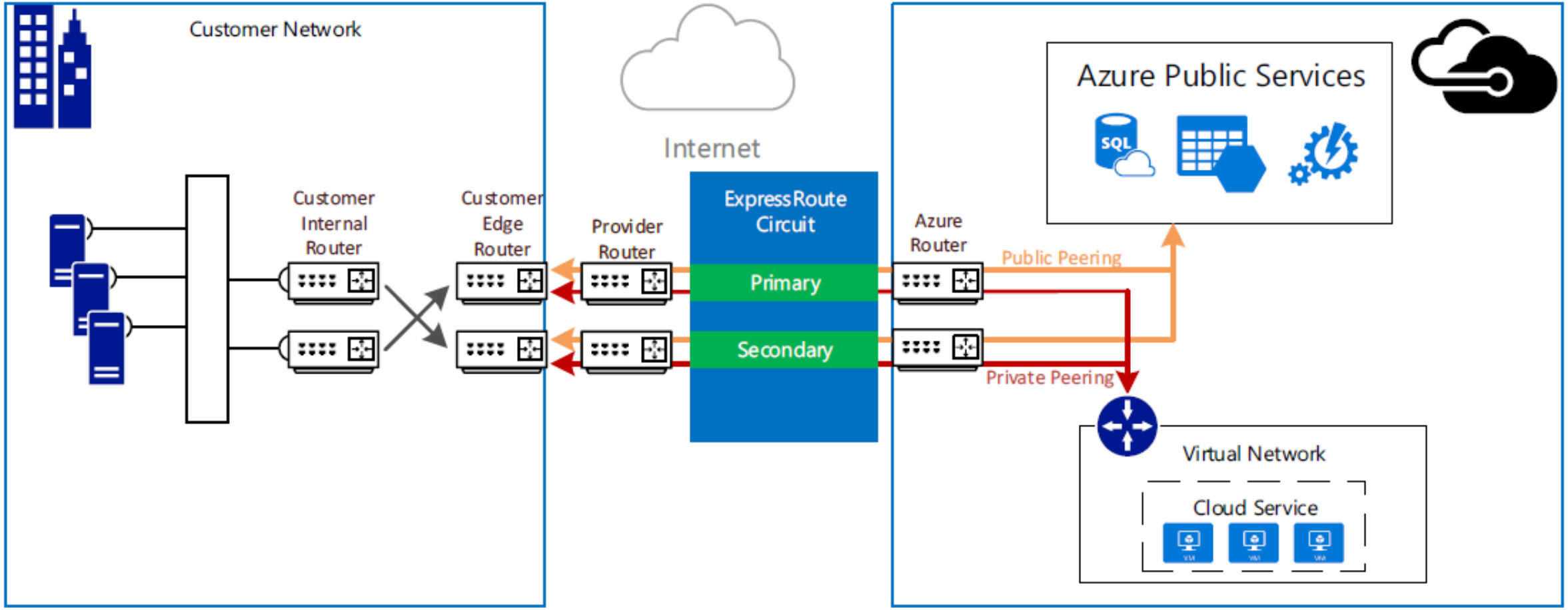
- Private connectivity to Microsoft
- Predictable performance
- Enterprise-grade resiliency and with SLA for availability
- Large and growing ExpressRoute partner ecosystem



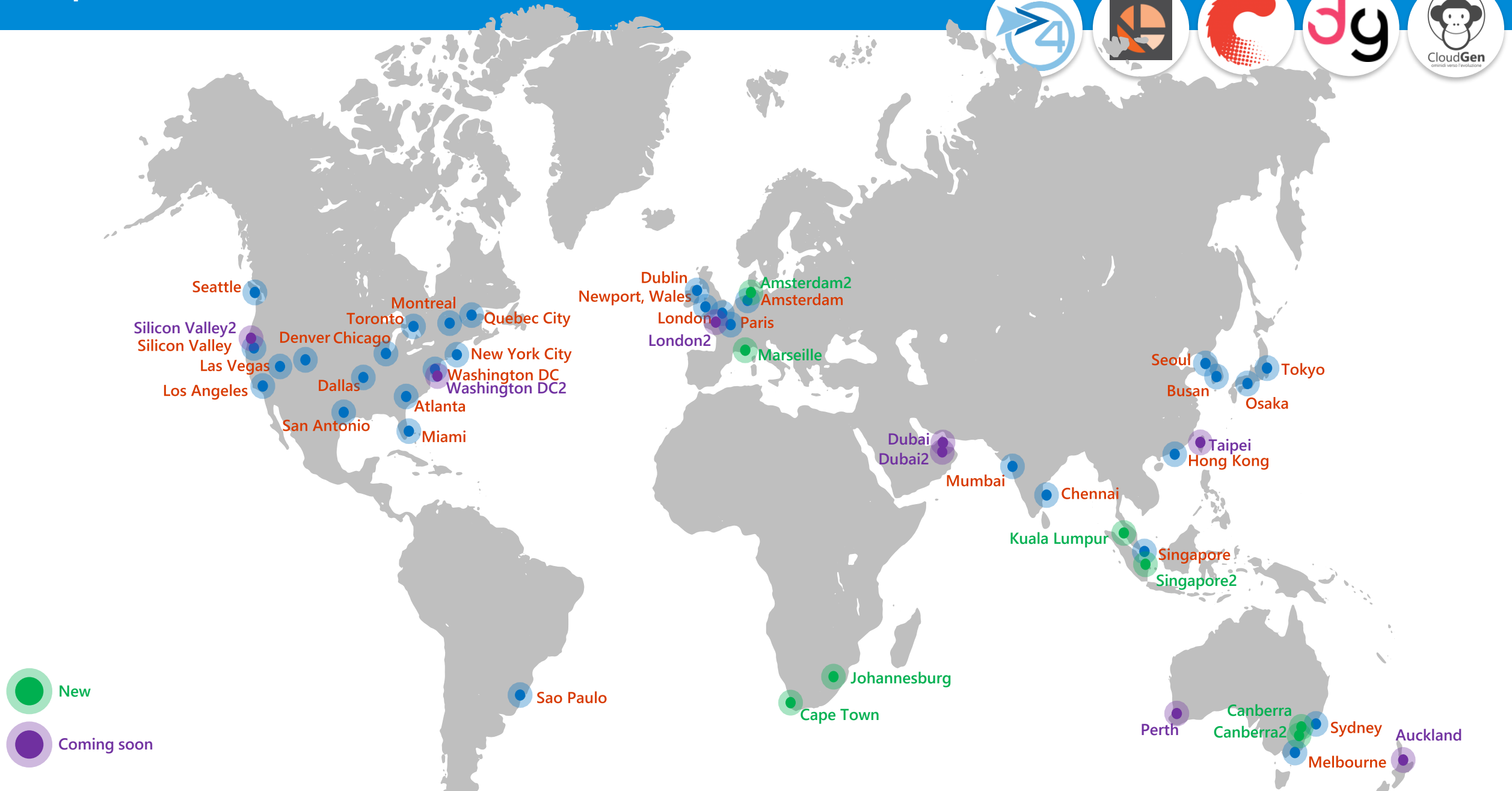
Microsoft Peering for Dynamics 365, Azure public services (public IPs)

Azure Private Peering for Virtual Networks

ExpressRoute connections



ExpressRoute locations

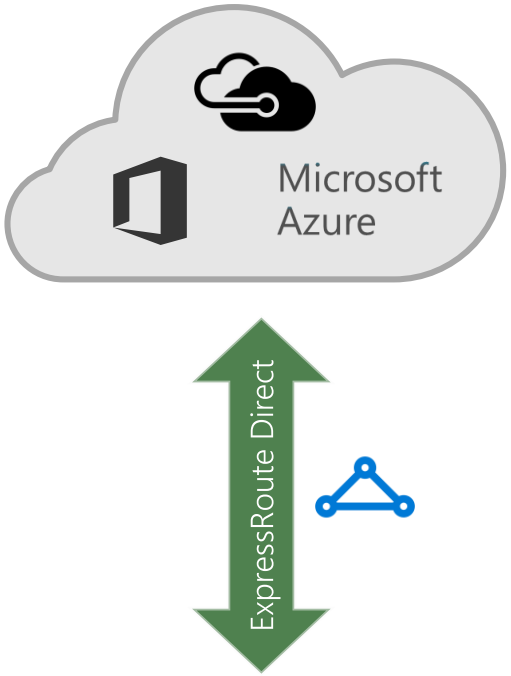


ExpressRoute locations for national clouds

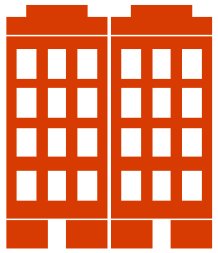
200+ ExpressRoute Partners

ExpressRoute Direct

- 100 Gbps direct to Azure
- Built for customers with extreme bandwidth needs for massive data ingestion
  - Optimized for massive data ingestion to Azure Storage, Cosmos DB, Azure SQL



Fastest private connectivity in public cloud – 100Gbps to Azure

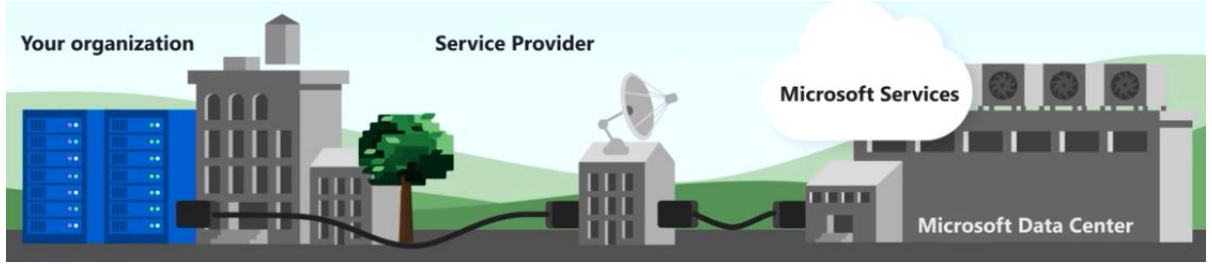


ExpressRoute Peering Location

ExpressRoute VS ExpressRoute Direct

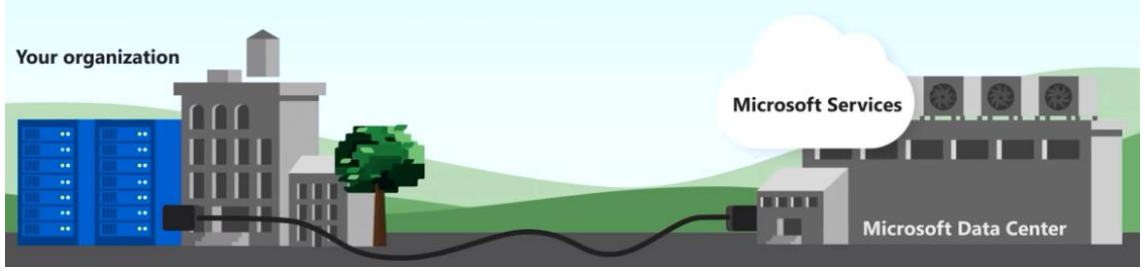
ExpressRoute

- Utilizes service provider to enable fast onboarding and connectivity into existing infrastructure
- Integrates with hundreds of providers including Ethernet and MPLS
- Circuits from 50Mbps-10Gbps
- Optimized for single tenant



ExpressRoute Direct

- Requires 100Gbps infrastructure and full management of all layers
- Direct/Dedicated capacity for regulated industries and massive data ingestion
- Circuits from 1Gbps to 100Gbps
- Optimized for single tenant/Cloud Service providers/multiple business units

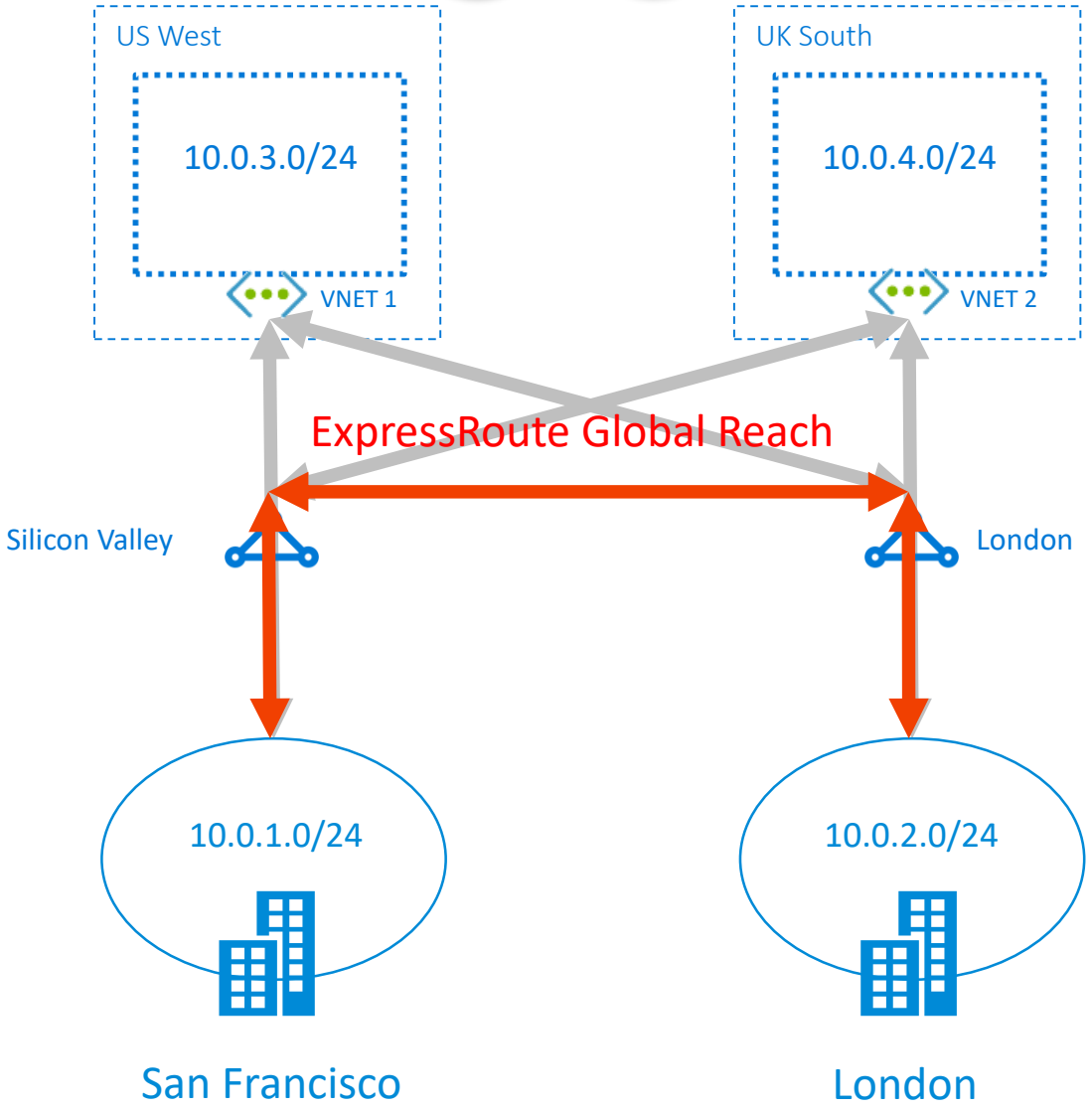


ExpressRoute Global Reach

- **ExpressRoute Global Reach** enables you to connect your sites
  - On-demand connectivity between your sites using your existing ExpressRoute circuits
  - Traffic staying on Microsoft's global network
  - Complement your service provider's WAN solution

Deploy global site-to-site connectivity using the Microsoft global network

- Available in Public Cloud
- Available in US Government Cloud
- Supported on Standard or Premium circuits with an add-on



Azure Global network

54 Azure regions

100K+ Miles of fiber and subsea cable

130+ Edge sites

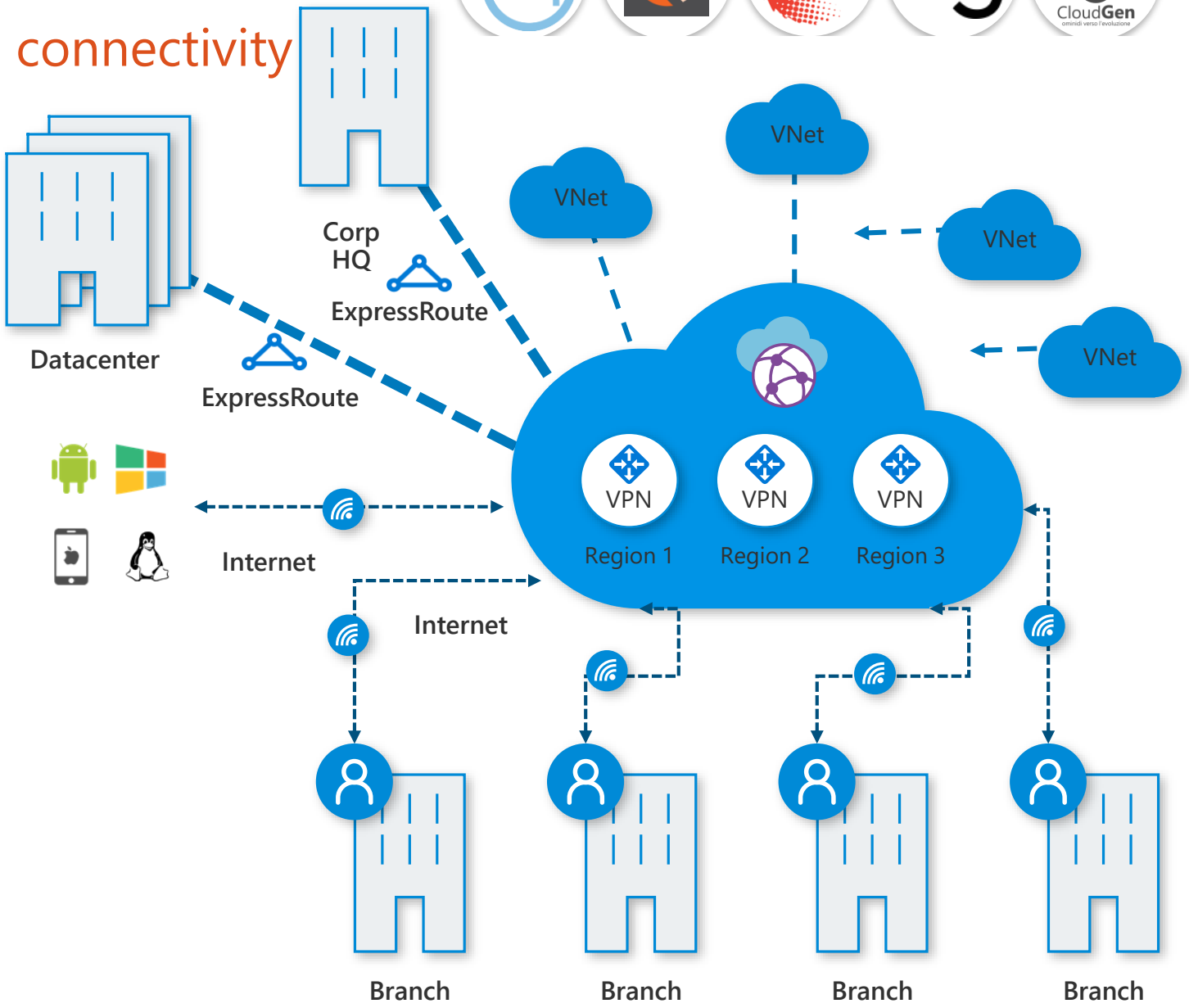
Azure Virtual WAN: unified Cloud Connectivity

Easy deployment of large-scale branch connectivity

- Branch to Azure, Branch to Branch
- Automated provisioning and configuration
- Scalability and high throughput
- Large and growing integrated partner ecosystem

Features:

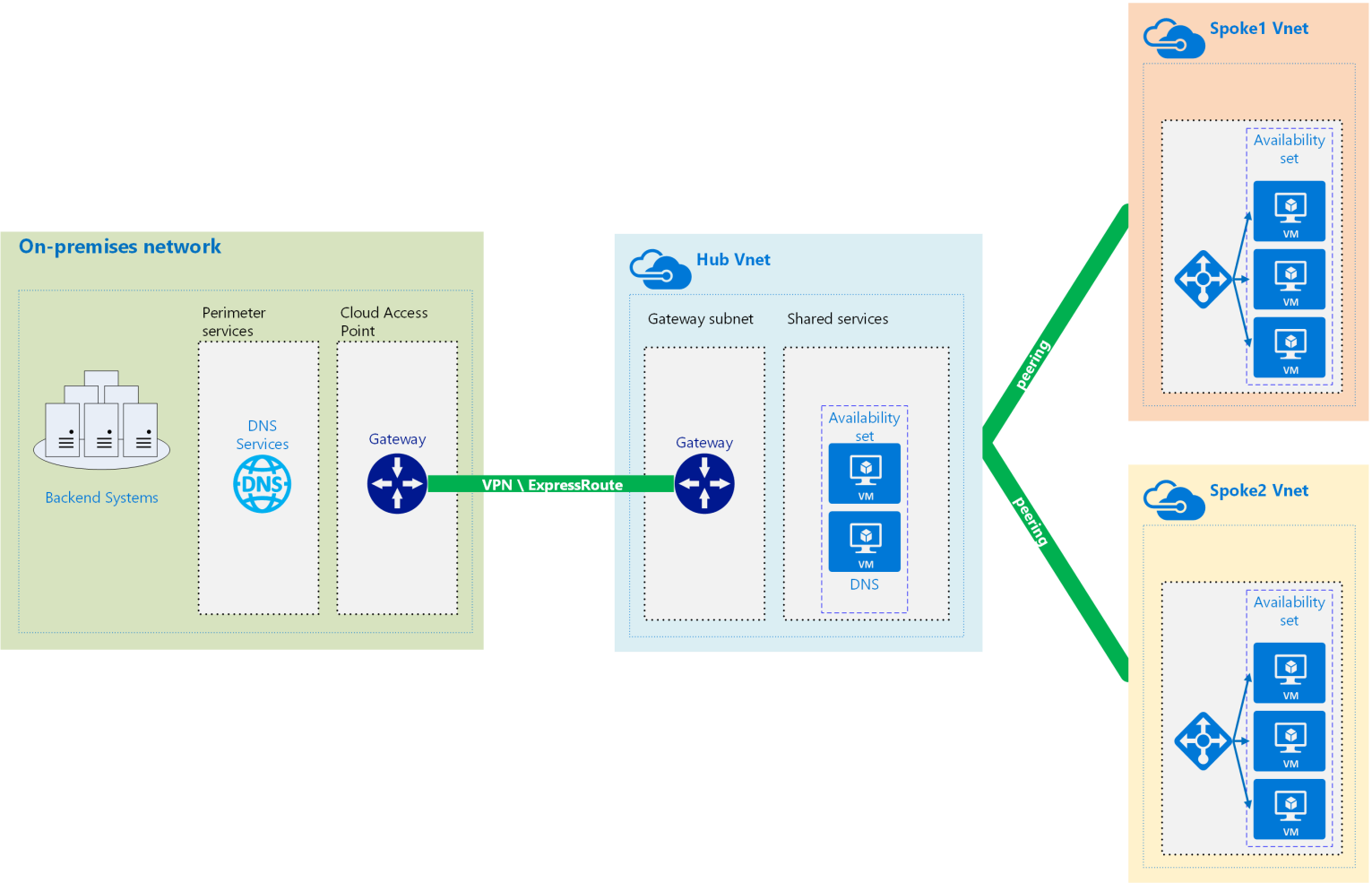
- Hubs in Azure
- Enable/disable branch to branch
- IPsec IKEv1 and IKEv2
- Scale unit-based billing
- E2E Monitoring and Resource Health
- ExpressRoute (Preview)
- P2S with IKEv2 and OpenVPN (Preview)
- O365 Policy (Preview)



Networking Security in Azure

Understand Azure network security best practice

Hub-spoke network topology in Azure



Typical uses for this architecture include:

- Workloads deployed in different environments (dev, testing, and production) that require shared services (DNS, IDS, NTP, or AD DS).
- Workloads that do not require connectivity to each other, but require access to shared services.
- Enterprises that require central control over security aspects, such as a firewall in the hub as a DMZ, and segregated management for the workloads in each spoke.

Hub-spoke benefits

- **Cost savings** by centralizing services that can be shared by multiple workloads, such as network virtual appliances (NVAs) and DNS servers, in a single location.
- **Overcome subscriptions limits** by peering VNets from different subscriptions to the central hub.
- **Separation of concerns** between central IT (SecOps, InfraOps) and workloads (DevOps).

Protection services enabling zero trust

DDoS protection

High availability for your applications with protection from excess IP traffic charges

DDOS protection tuned to your application traffic patterns

Web Application Firewall

Prevent SQL injection, stop cross site scripting and an array of other types of attacks using cloud native approach

Centralized inbound web application protection from common exploits and vulnerabilities

Azure Firewall

Better central governance of all traffic flows, full devops integration using cloud native high availability with autoscale

Centralized outbound and inbound (non-HTTP/S) network and application (L3-L7) filtering

Network Security Groups

Full granular distributed end node control at VM/subnet for all network traffic flows

Distributed inbound & outbound network (L3-L4) traffic filtering on VM, Container or subnet

Service Endpoints

Extend your Virtual Network controls to lock down Azure service resources (PaaS) access

Restrict access to Azure service resources (PaaS) to only your Virtual Network

Application protection

Segmentation

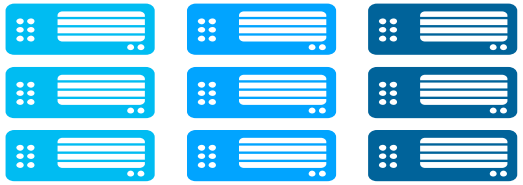
Application Access Patterns

2

Users

Internet

Your Virtual Network



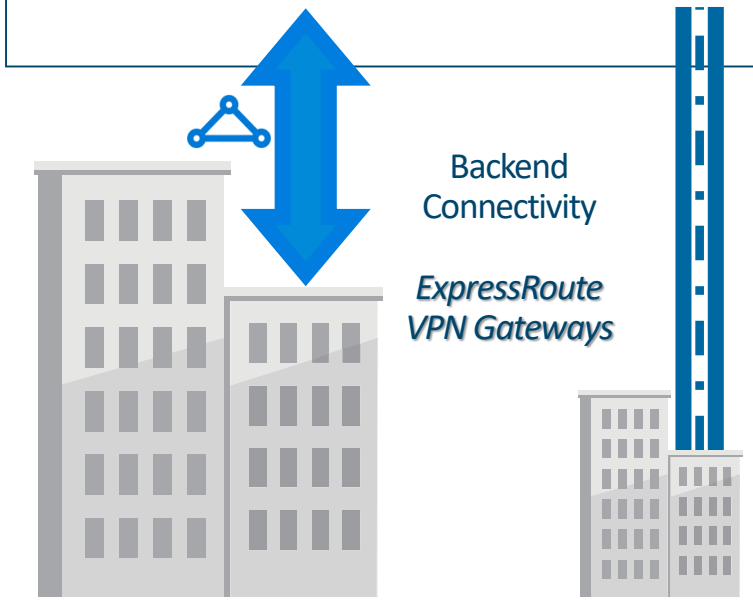
1

Access to Azure PaaS services

Service Endpoints

Access to/from Internet

- DDoS protection
- Web Application Firewall
- Azure Firewall
- Network Virtual Appliances



Backend Connectivity

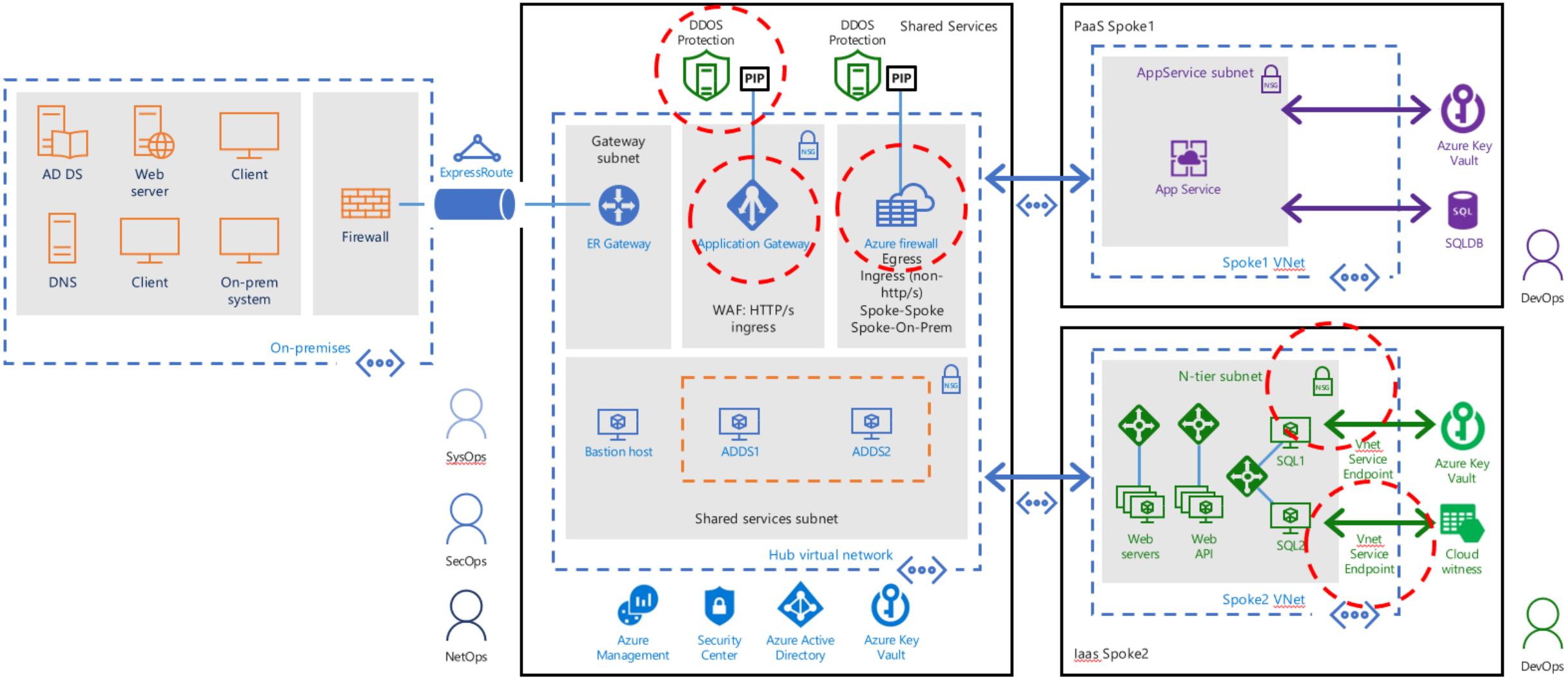
ExpressRoute
VPN Gateways

3

Access private traffic

- Network security groups (NSGs)
- Application security groups (ASGs)
- User-Defined routes (UDRs)

Hub & spoke architecture: native security services



Azure Firewall

Cloud native stateful Firewall as a service

Central governance of all traffic flows

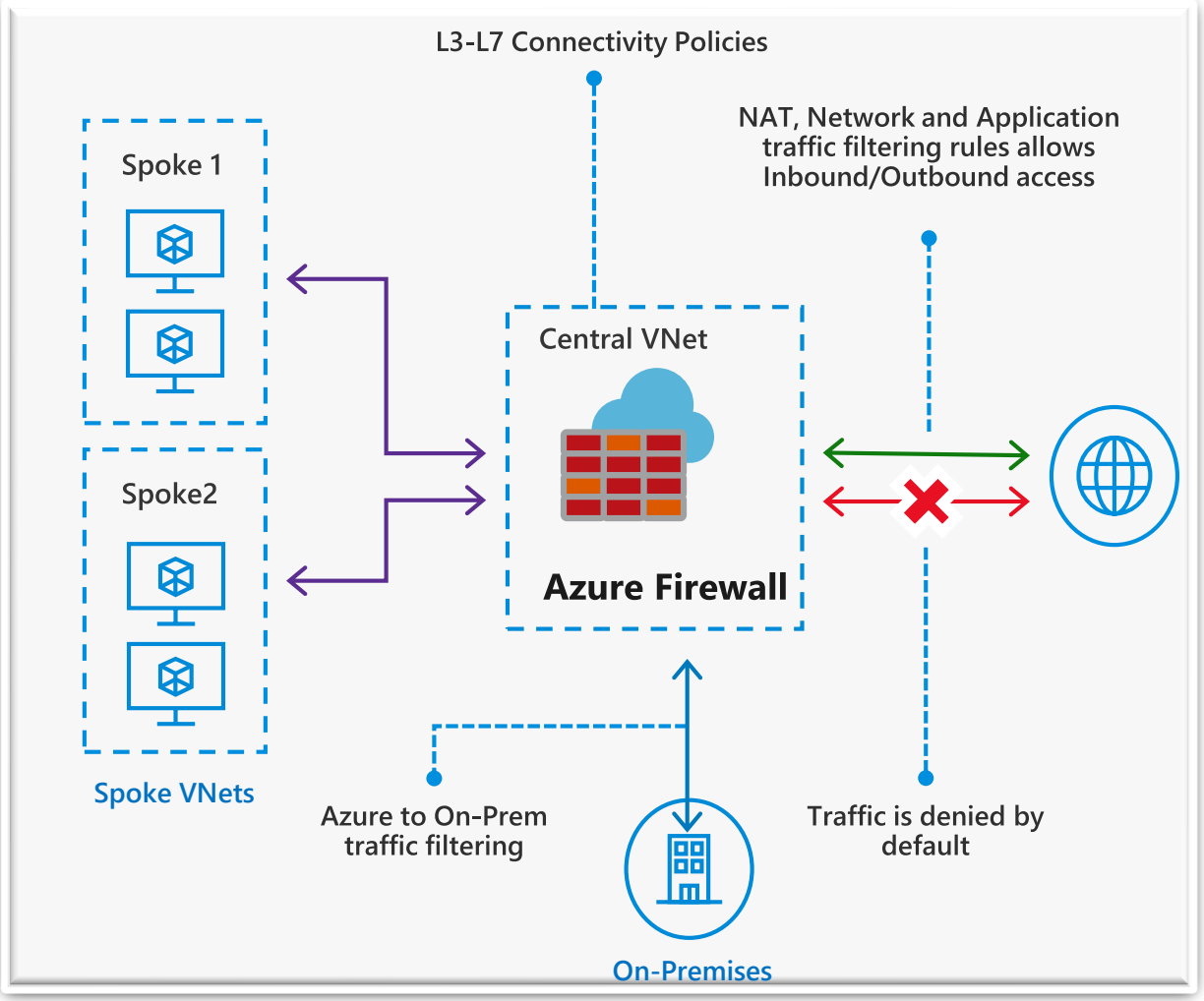
- Built-in high availability and auto scale
- Network and application traffic filtering
- Centralized policy across VNets and subscriptions

Complete VNET protection

- Filter Outbound, Inbound, Spoke-Spoke & Hybrid Connections traffic (VPN and ExpressRoute)

Centralized logging

- Archive logs to a storage account, stream events to your Event Hub, or send them to Log Analytics or Security Integration and Event Management (SIEM) system of choice



Azure Firewall Demo

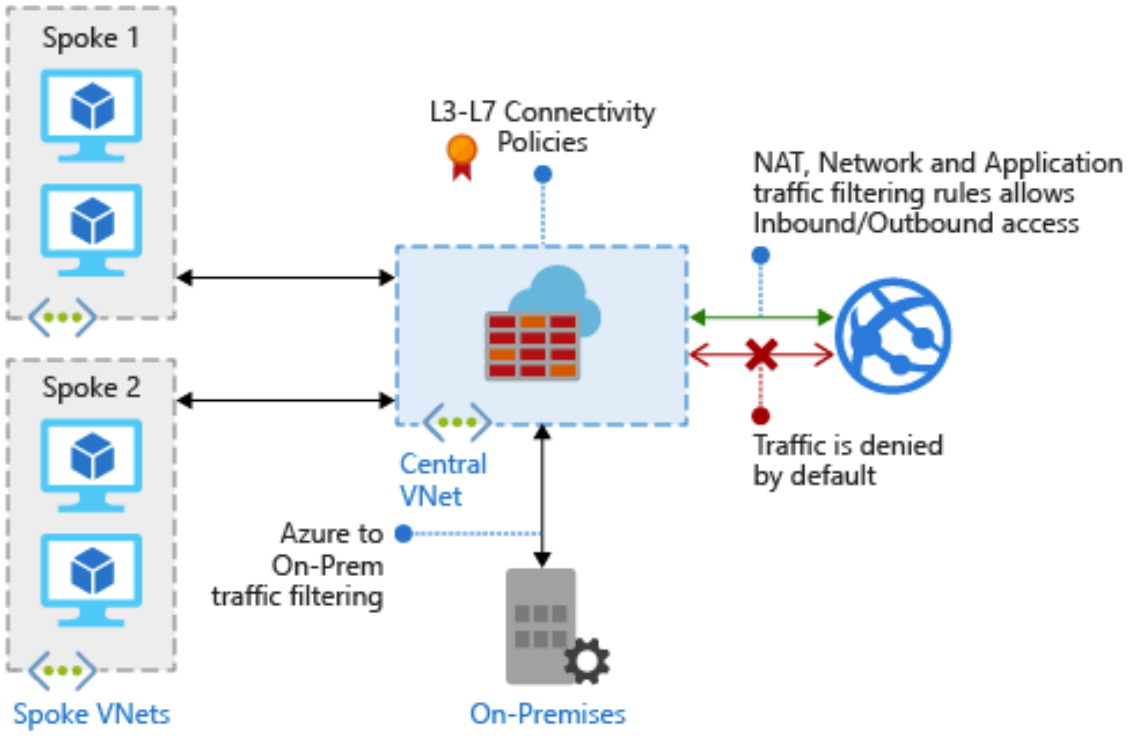
Azure Firewall for hybrid links

Traffic filtering between Azure VNETs and on-premises networks

Works with either Azure VPN Gateway or Express Route Gateway

No support for traffic routing from on-premises to internet

This is a key roadmap feature for Azure Firewall in a Virtual WAN Hub



Recap Azure network security best practice

- Pick network security offerings based on application access patterns
- Layer security by mix-and-match based on your requirements
- Scale the security model, as your workloads scale

Thanks

Questions?

francescomolfese

@FrancescoMolf

francescomolfese