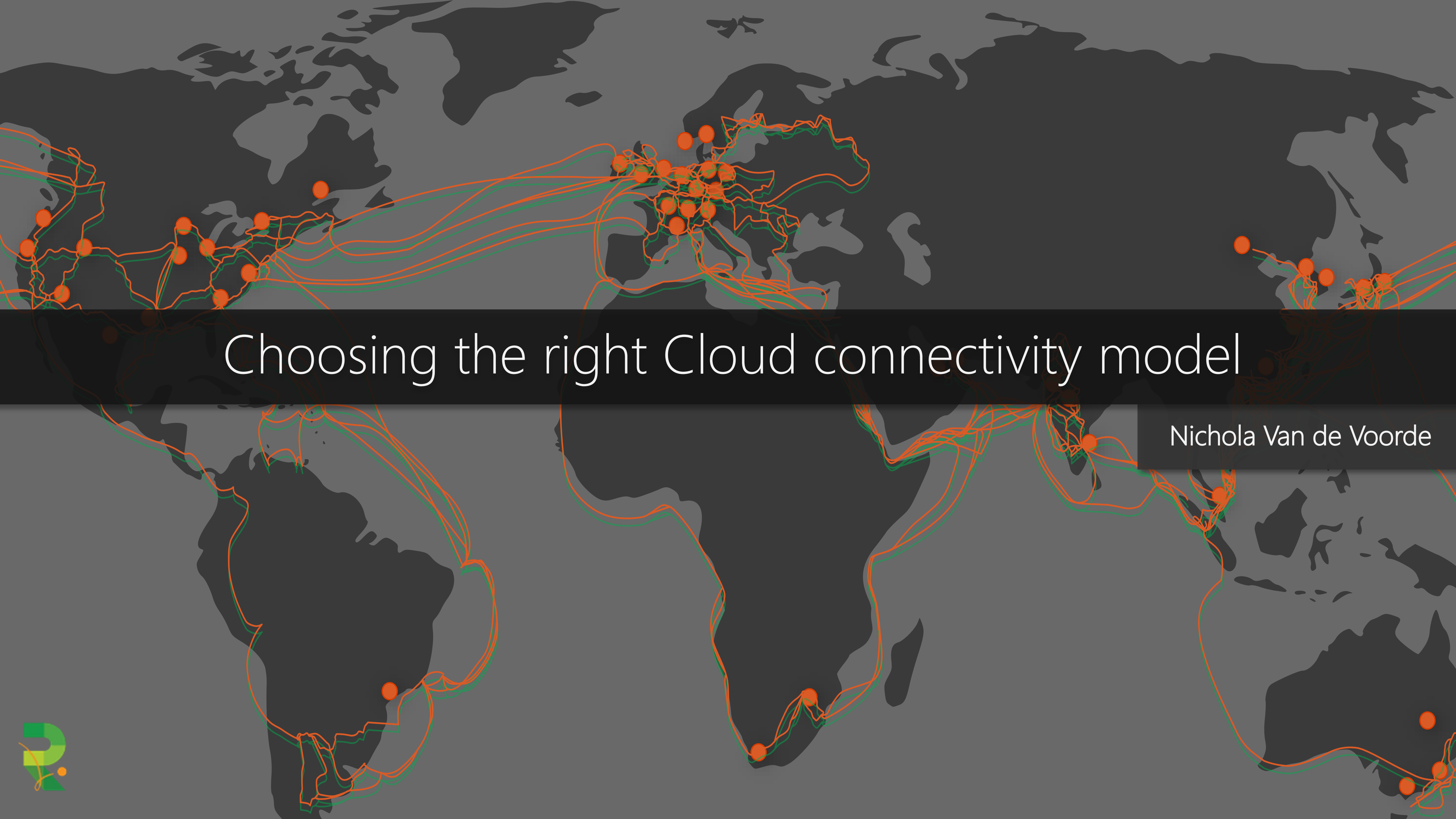


Choosing the right Cloud connectivity model

Nichola Van de Voorde

Paving the way…

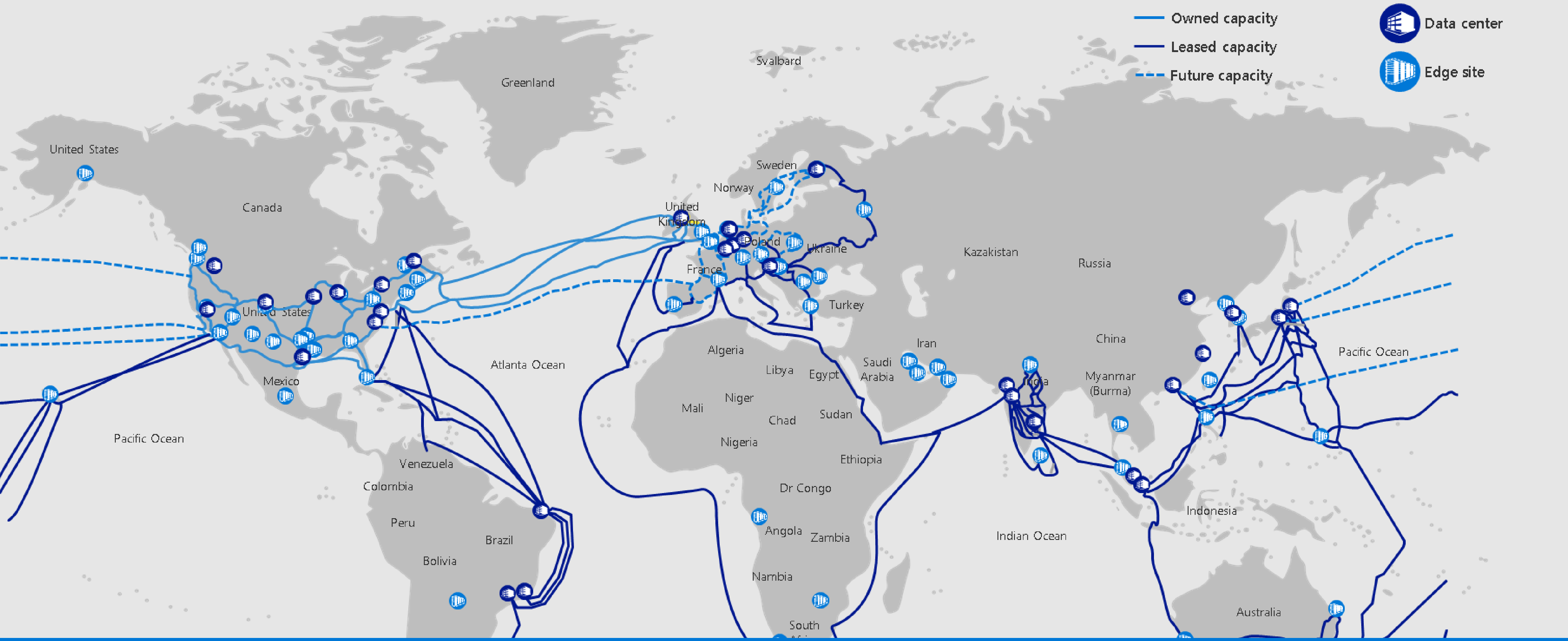
- Connecting the global dots
- Cloud Connectivity Models
- ExpressRoute
- Azure Virtual WAN
- Use Case

Connecting the global dots

Microsoft backbone infrastructure

- Second biggest network in the world
- Edge sites
  - 130+ Point of Presence aka the last mile
  - Bringing the Microsoft datacenter one step closer to the customer
- Microsoft regions
  - 54 regions worldwide
  - 100+ datacenters
  - Microsoft Azure available in 140 countries
- Physical network infrastructure
  - Owned capacity
  - Leased Capacity
  - +150k kilometers of fibre

Azure inter-DC dark fiber backbone

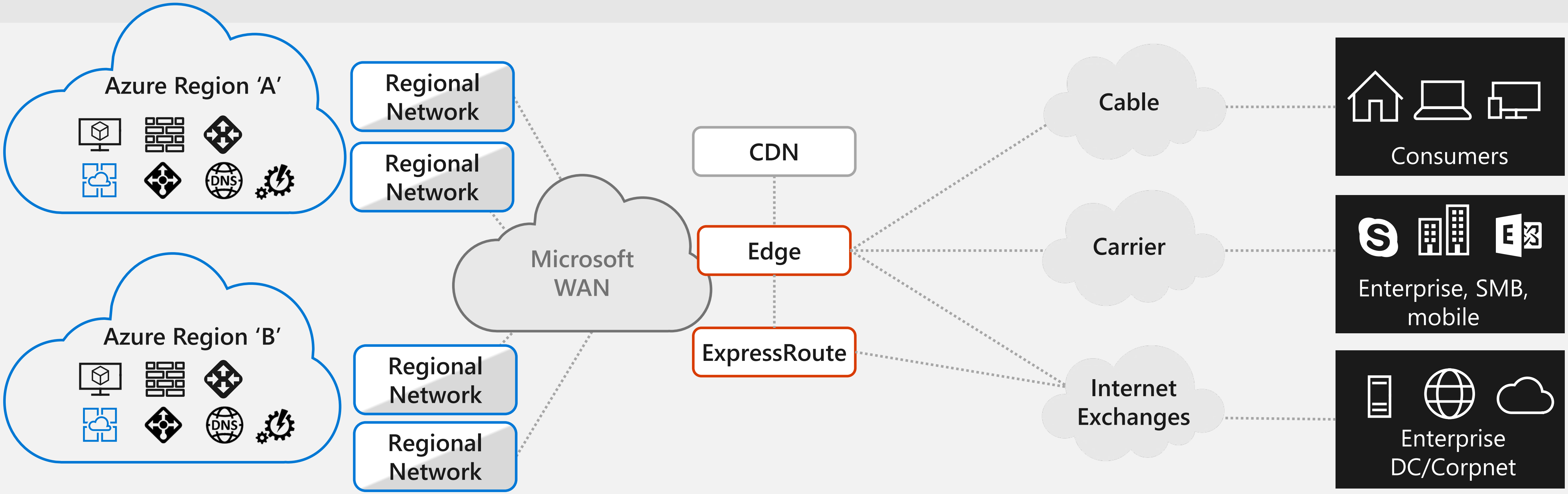


Interactive map: https://tinyurl.com/rdlovesazure

MAREA Cable

- Long transatlantic communications cable
  - Owned and funded by Microsoft and Facebook
  - Between Virginia Beach (US) and Bilbao (Spain)
  - Operational since february 2018
  - 6600 kilometers long
  - 5 million kilograms
  - 8 fibre-optic thread bundle
  - Size of a garden hose
  - 160 Terabits per second

Azure Networking



DC Hardware	Services	Intra-Region	WAN Backbone	Edge and ExpressRoute	CDN	Last Mile
• SmartNIC/FPGA • SONiC	• Virtual Networks • Load Balancing • VPN Services • Firewall • DDoS Protection • DNS & Traffic Management	• DC Networks • Regional Networks • Optical Modules	• Software WAN • Subsea Cables • Terrestrial Fiber • National Clouds	• Internet Peering • ExpressRoute	• Acceleration for applications and content	• E2E monitoring (Network Watcher, Network Performance Monitoring)

Azure Network Emulator

What it is

Containerized router VMs linked via VXLAN tunnels to create a faithful replica of production network

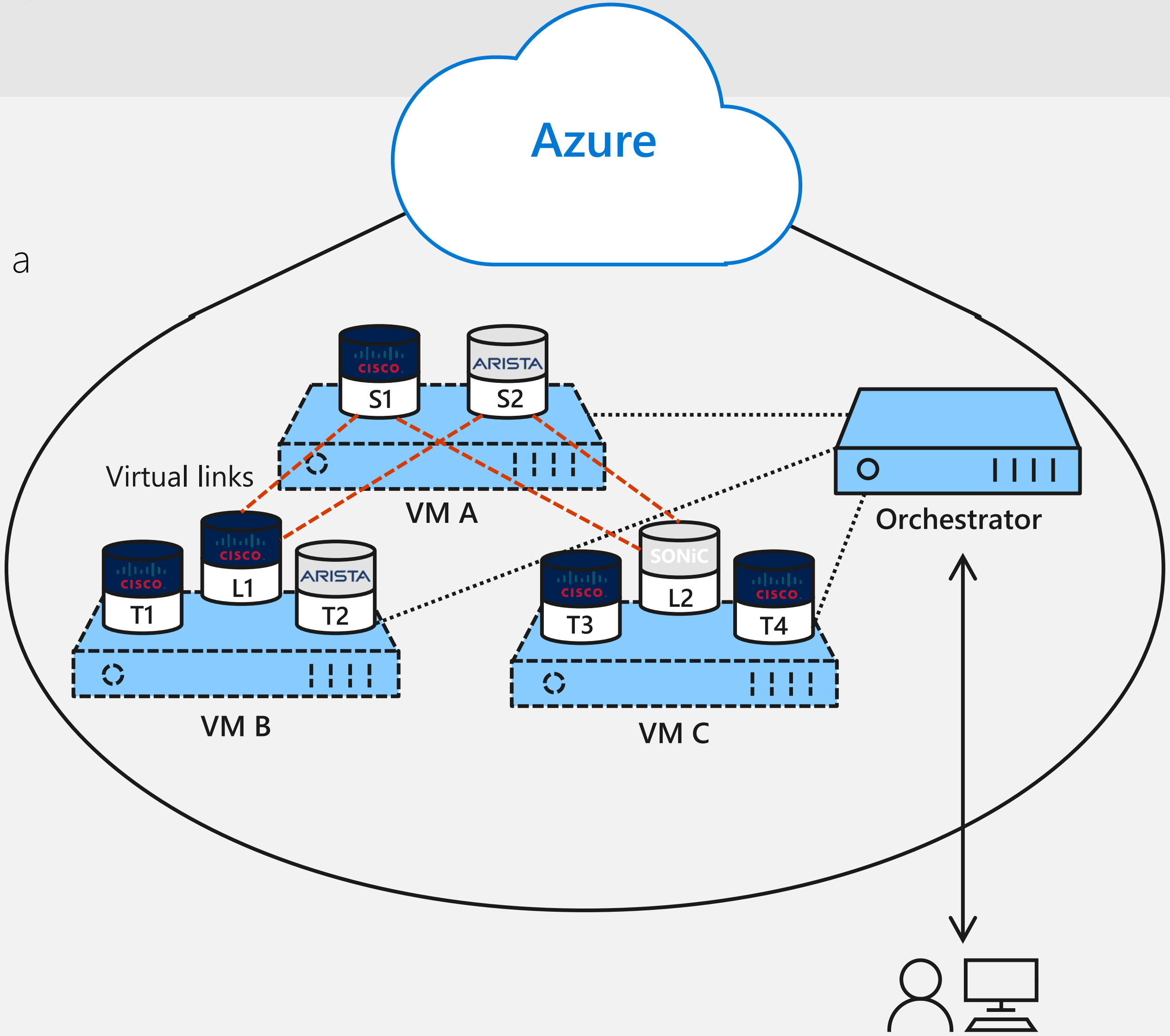
“Bug compatible” emulation of production network gives network engineers realistic test environment

Status

Used daily to de-risk major network operations

Over 12 million core-hours spent on emulation in last six months

Numerous bugs caught before hitting production network



Cloud Connectivity Models

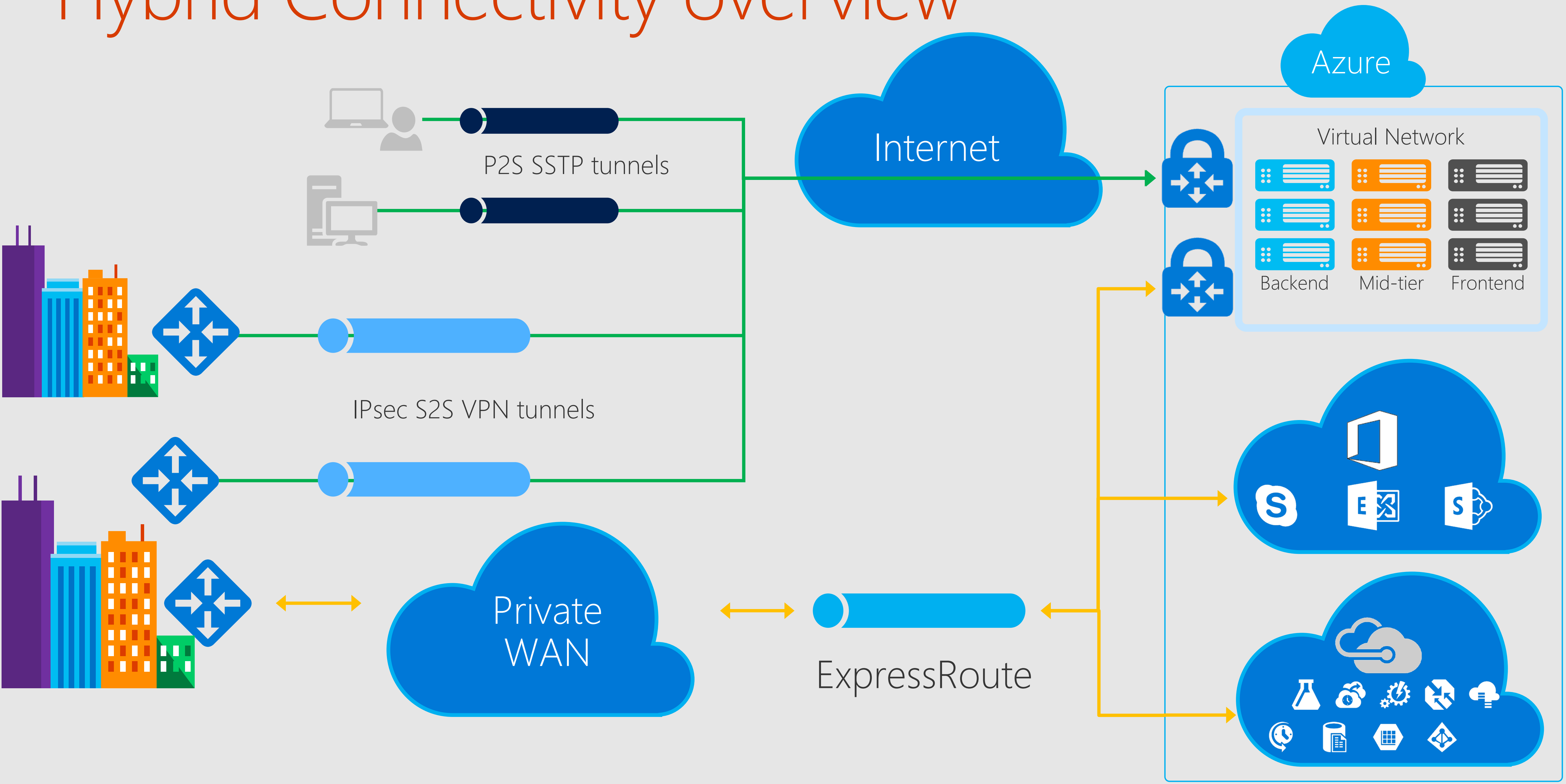
Connectivity to Azure

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

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

Hybrid Connectivity overview

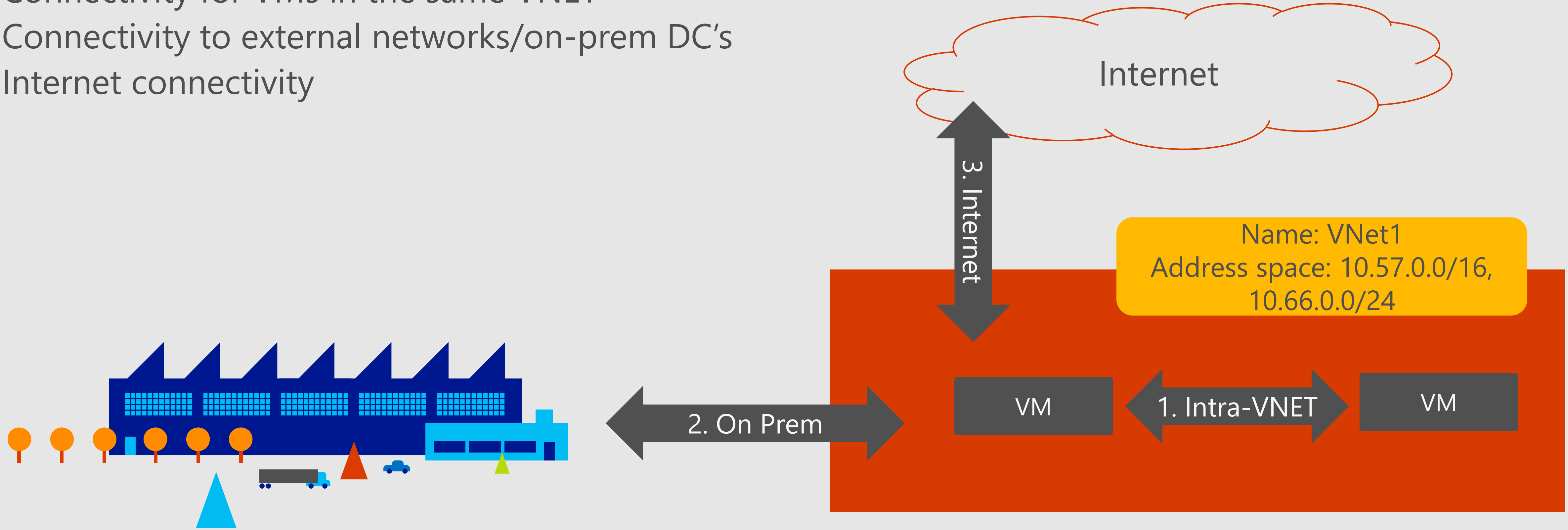


Virtual Network

Isolated, logical network that provides connectivity for Azure VMs

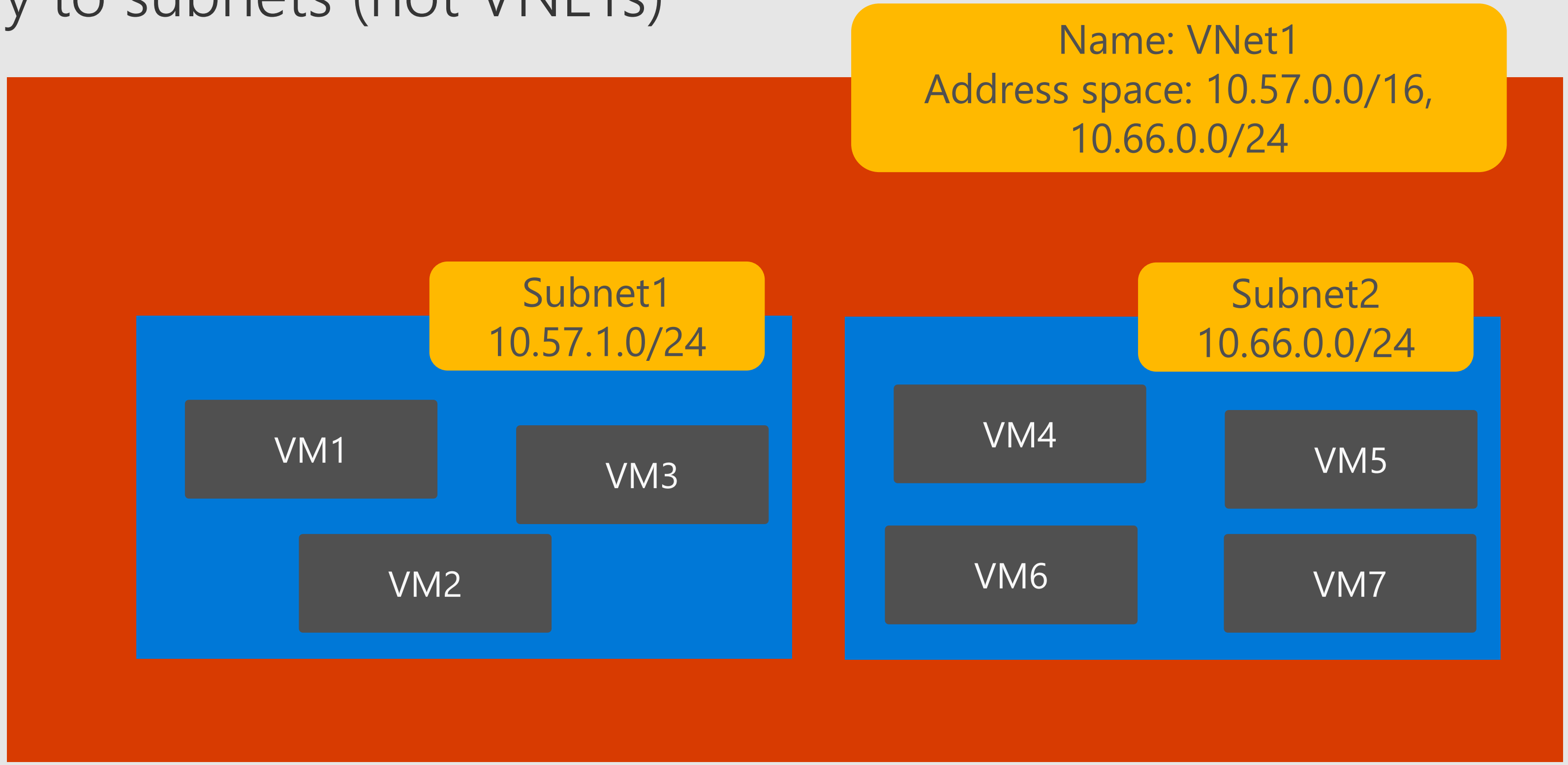
User-defined address space (can be one or more IP ranges, not necessarily RFC1918)

1. Connectivity for VMs in the same VNET
2. Connectivity to external networks/on-prem DC’s
3. Internet connectivity



Subnet

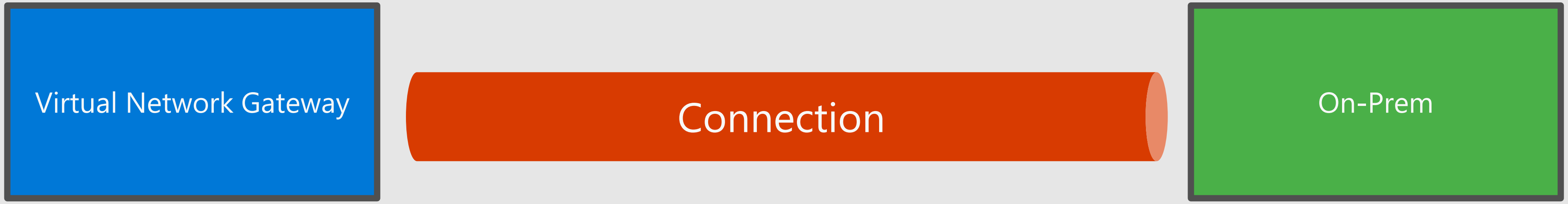
- IP subnet
  - Provides full layer-3 semantics and partial layer-2 semantics (DHCP, ARP, no broadcast/multicast)
  - Subnets can span only one range of contiguous IP addresses
  - VMs can be deployed only to subnets (not VNETs)



Configuring cross-premises connectivity

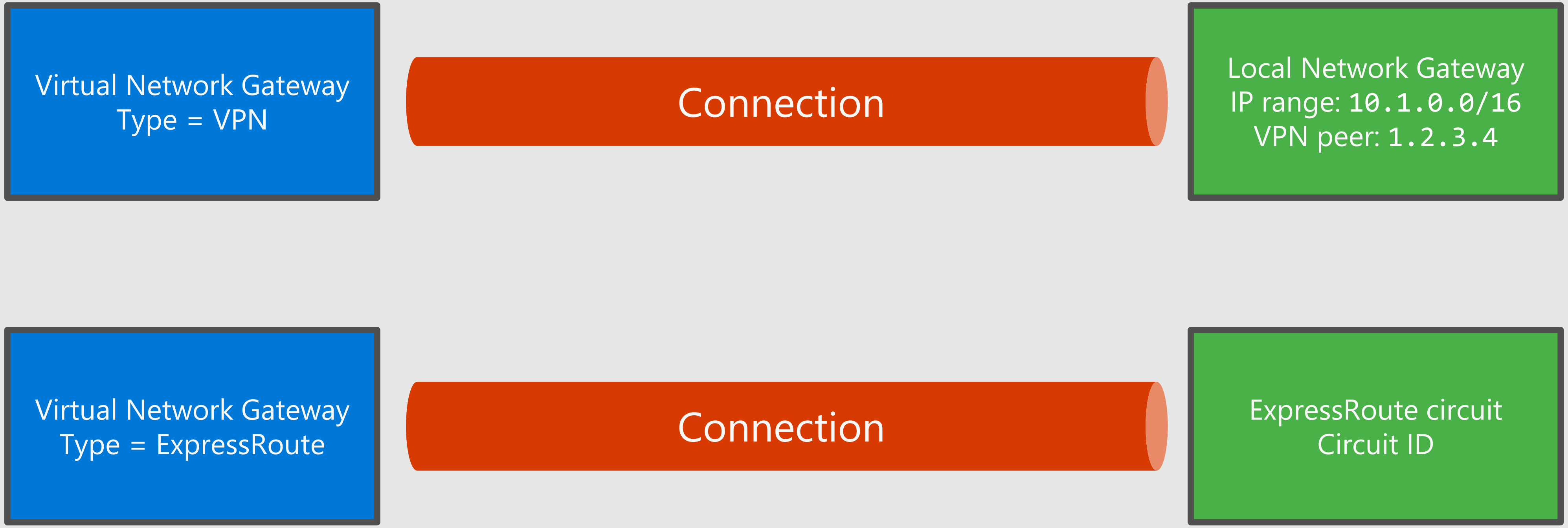
Cross-Premises connections require three things

- A virtual network gateway
- An object describing the << on-prem side >>
- A connection between the two



Configuring cross-premises connectivity

IPSec and ER connections share the same model

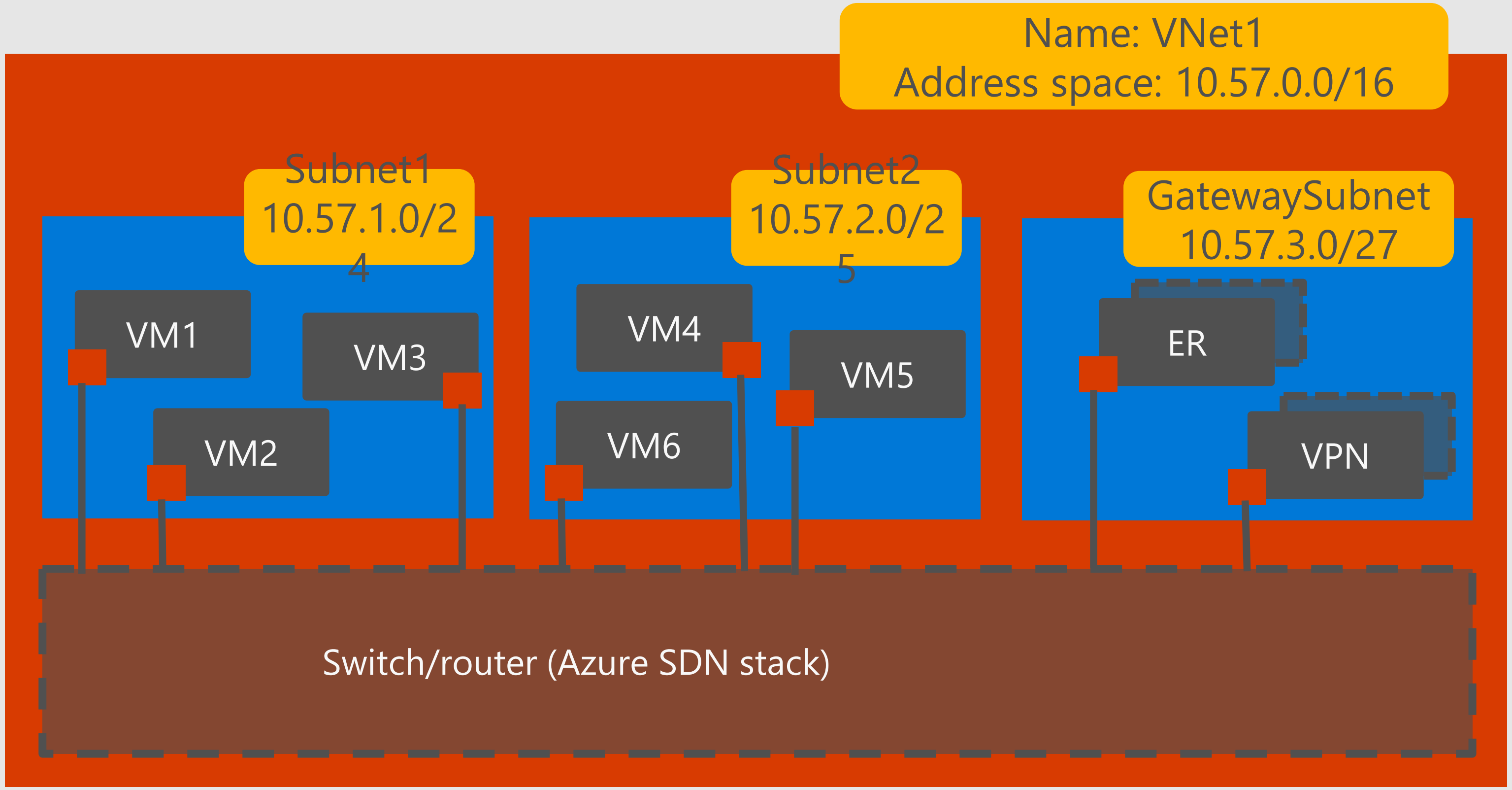


Local Network Gateways describe an on-prem network

Reference to a physical connection to an on-prem network

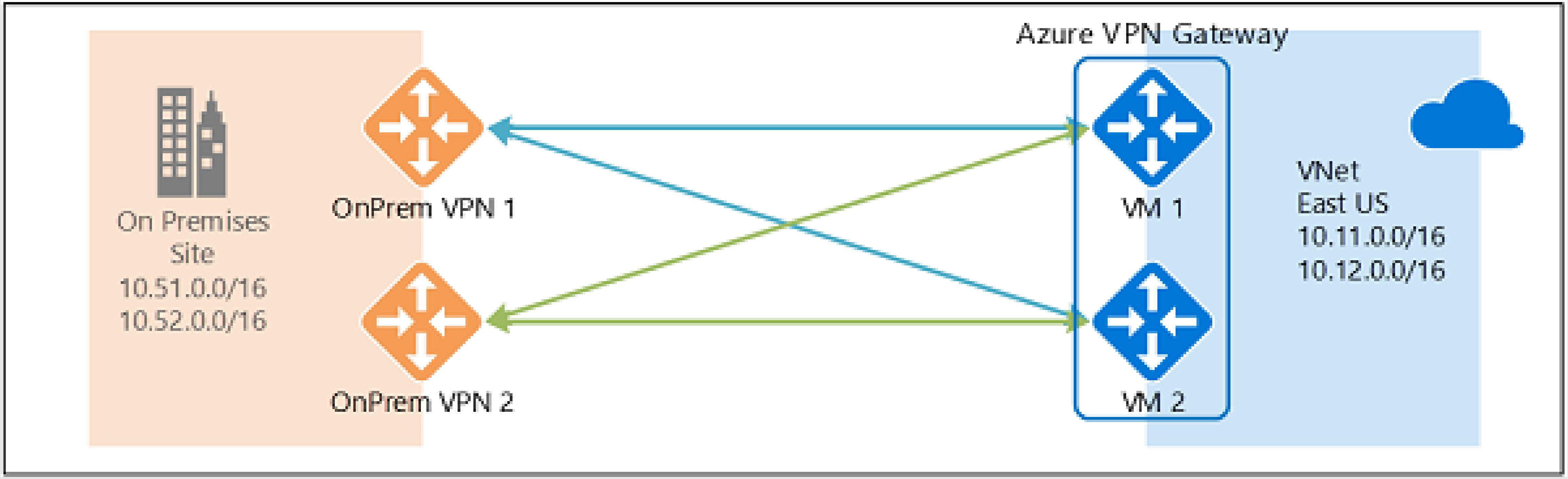
Virtual Network Gateway

Gateway types: «Vpn» or «ExpressRoute»

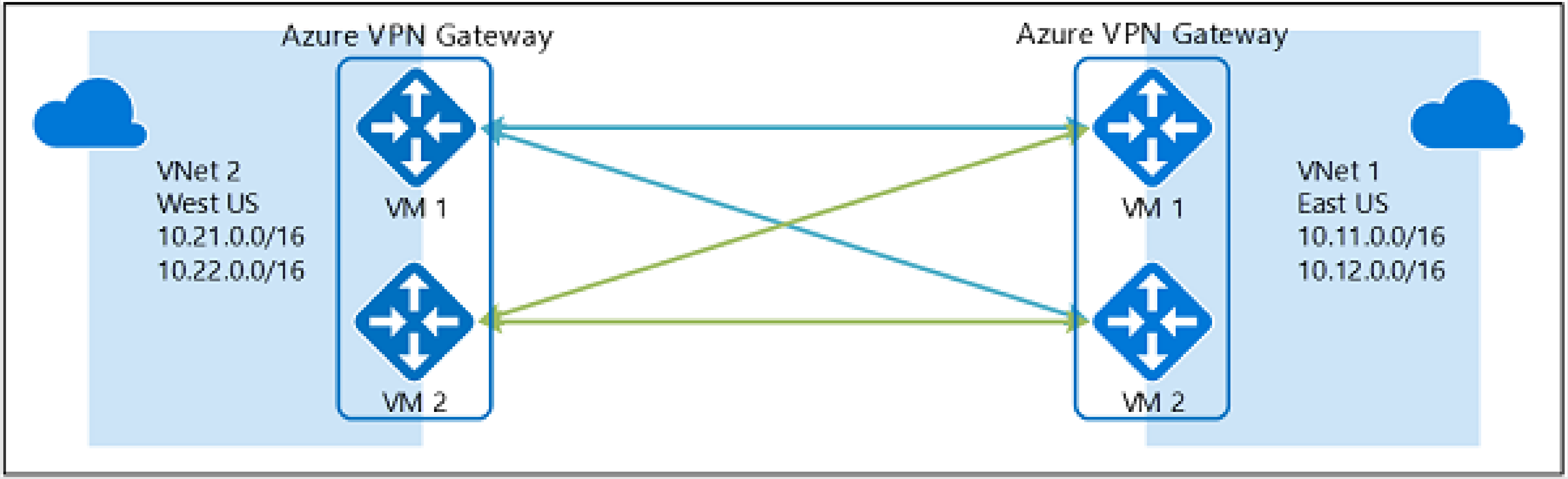


- Vpn gateways: route traffic to remote networks over internet-based IPSec tunnels
- ExpressRoute gateways: route traffic to on-prem networks over dedicated connectivity
- Can coexist in the same VNet (if /27 or larger)

Active-active VPN gateway, redundant on-prem devices

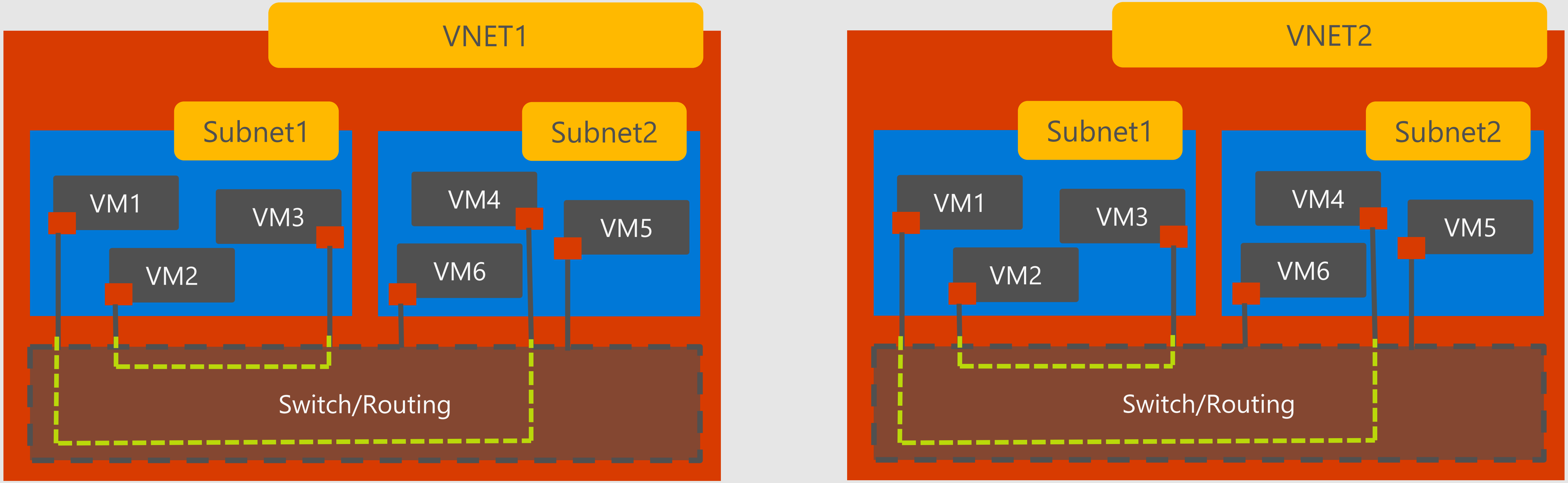


Vnet-2-Vnet with active-active VPN gateways



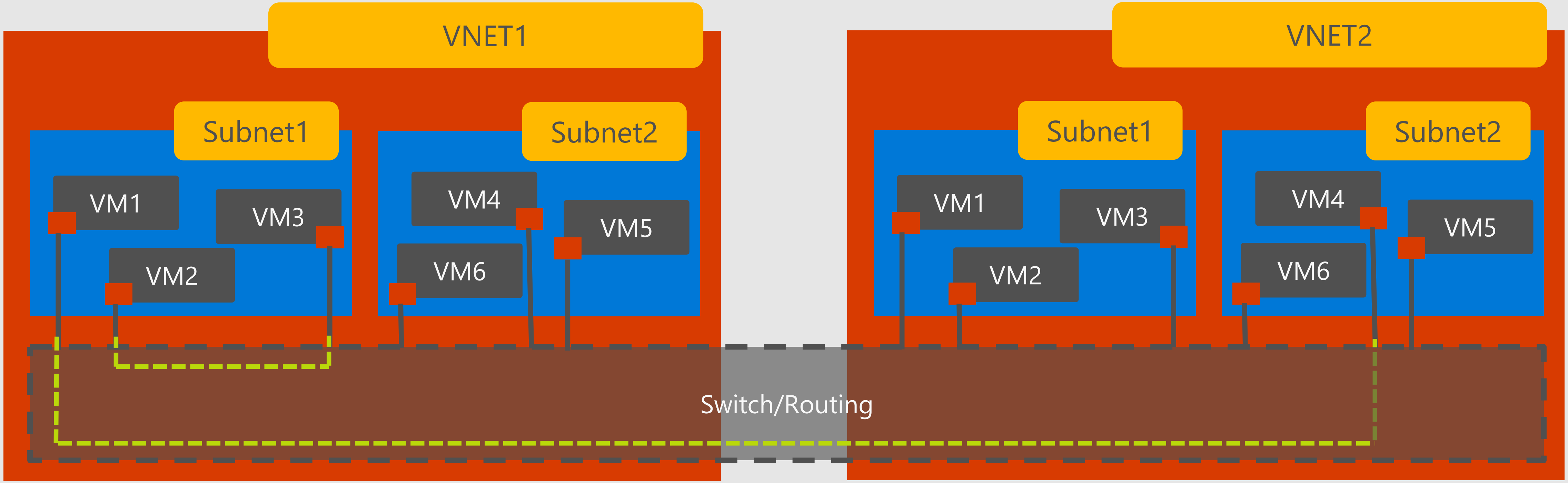
What is VNet peering?

- Ability to “merge” two Azure VNets, so that VMs in the two VNets can communicate with each other as if they were on the same VNet



What is VNet peering?

- Ability to “merge” two Azure VNets, so that VMs in the two VNets can communicate with each other as if they were on the same VNet



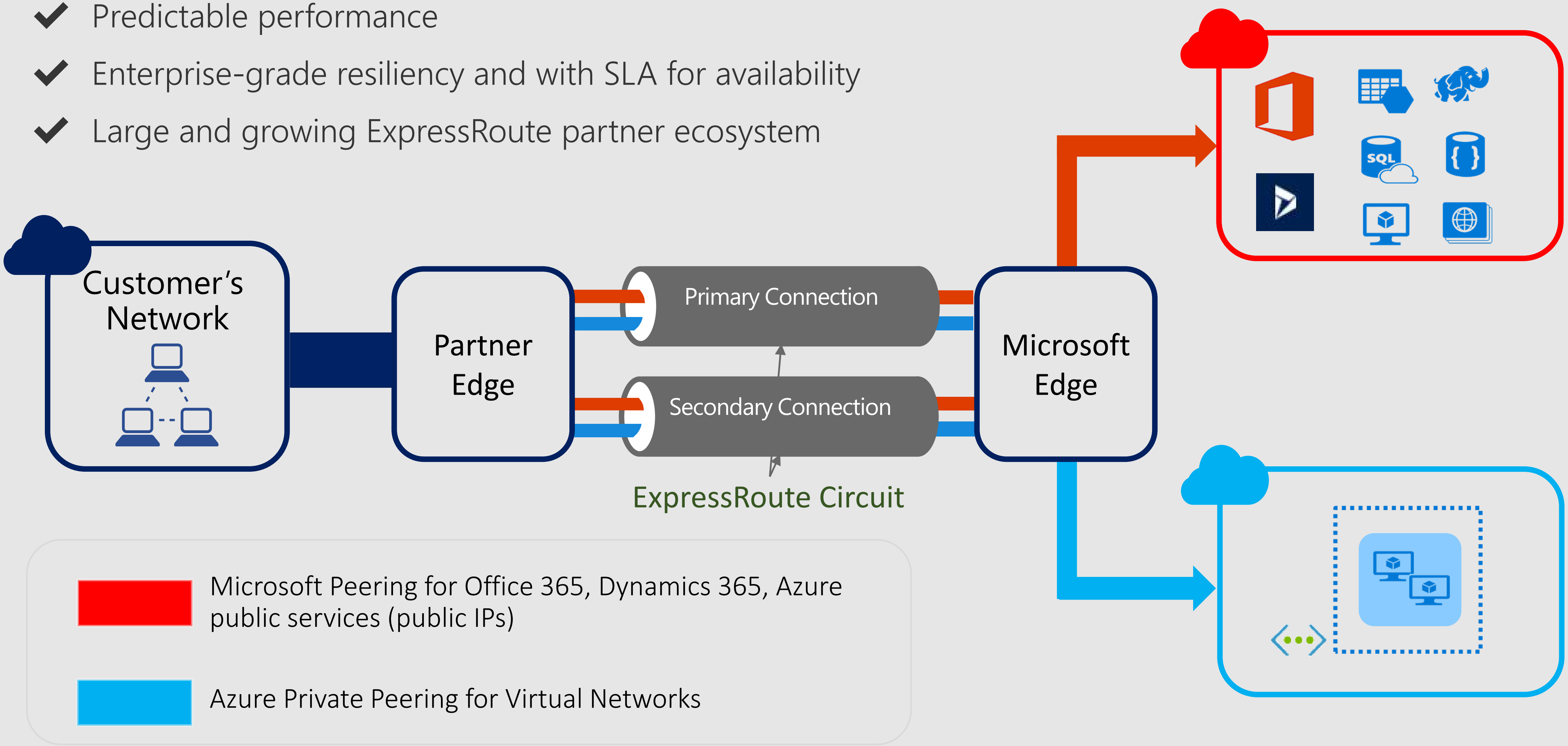
VNet peering key facts

- Traffic across peering VNets is managed in a very similar way to intra-VNet traffic
- Works for VNets cross-region
- Provides the same performance as intra-VNet traffic
- Works across subscriptions attached to the same or different AAD tenant

ExpressRoute

ExpressRoute

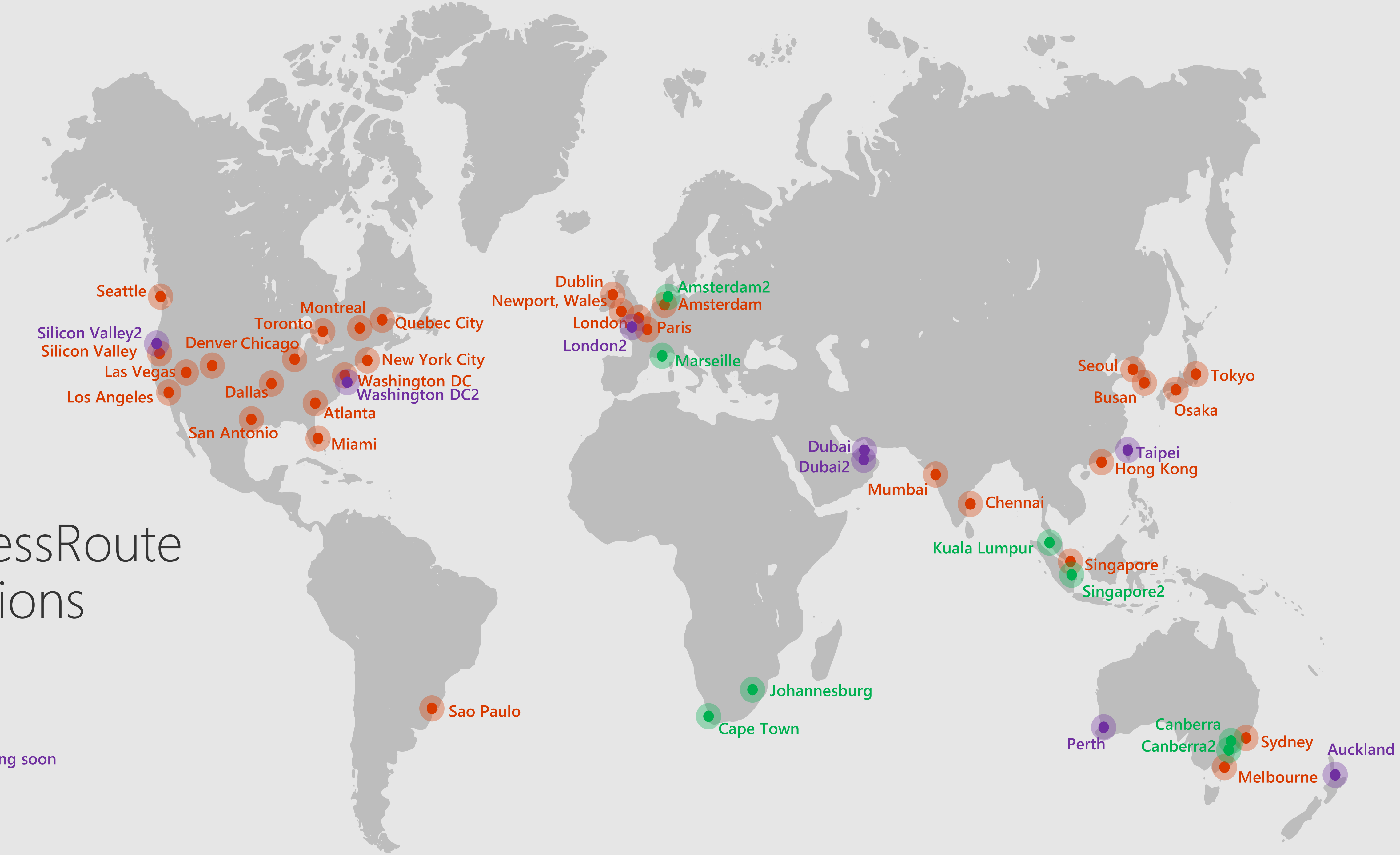
- ✓ Unified connectivity to Microsoft Cloud Services
- ✓ Predictable performance
- ✓ Enterprise-grade resiliency and with SLA for availability
- ✓ Large and growing ExpressRoute partner ecosystem



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

🟦 Azure Private Peering for Virtual Networks

ExpressRoute locations

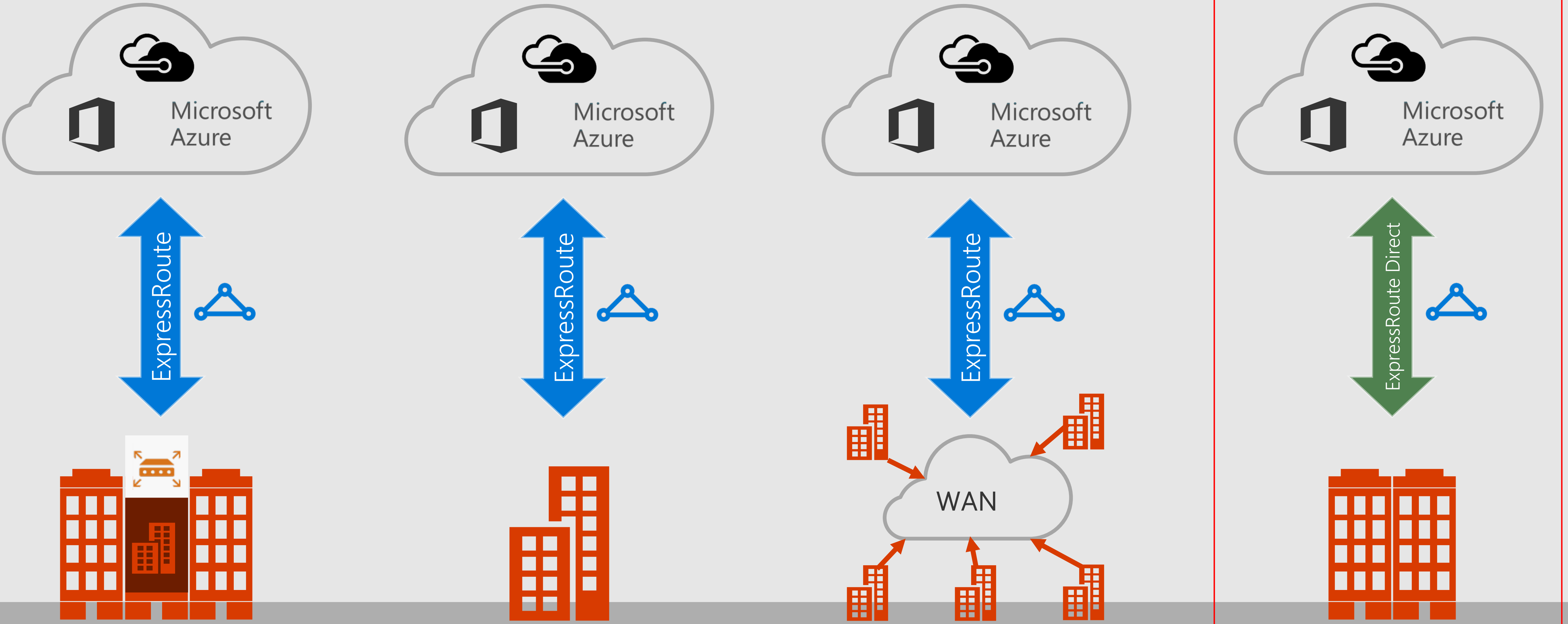


● New

● Coming soon

Preview

ExpressRoute connectivity models



Cloud exchange co-location

Point-to-point Ethernet connection

Any-to-any (IPVPN) connection

ExpressRoute Peering Location

Preview

ExpressRoute and 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
- Premium Add-on
  - Increased routes limit
  - Provides global connectivity
  - Accross geopolitical region

- 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

alaska COMMUNICATIONS
altice
aarnet Australia's Academic and Research Network
AIRGATE MAKING THINGS SMARTER
airtel
ARTERIA
Aryaka
Ascenty
AT&T
5G Innovations
Bell
Bezeq International
BT
C3NTRO
cdc
CenturyLink
中国电信 CHINA TELECOM
COGECO PEER 1
cologix
colt
COMCAST BUSINESS
CORESITE
COX Business
1CLOUDSTAR
CyrusOne
DATA FOUNDRY
DIGITAL REALTY
DISA
edgeconneX
eir
epsilon
EQUINIX
e-shelter
eurofiber
eunetworks
exponential-e applied innovation
FASTWEB
GÉANT
GLOBAL CLOUD XCHANGE A RELIANCE COMPANY
gtt
Hso
IIJ Internet Initiative Japan
INTERNET 2
interCloud
IS.
interxion
ixreach connecting networks
Jisc
KINX
kpn
Level(3) COMMUNICATIONS
LIQUID TELECOM
LGA
lightower
LG CNS
MACROVIEW TELECOM
macquarie TELECOM
MASERGY
Megaport
MTN
Neutrona Neutral. On Net. Anywhere.
NexGen NETWORKS
NGD NEXT GENERATION DATA NOWHERE SAFER
NEXTDC
nianet Danmarks Erhvervsfibernet
NTT Communications
NTT EAST
NTT Smart Connect
OPTUS
orange™
PCCW 電訊盈科
packetfabric
QSC AG
ROGERS
RagingWire DATA CENTERS
SEJONG TELECOM
sify
SINET5
Singtel
SoftBank
TELMEX
Sprint
T5 T5DataCenters Top Tier. Bottom Line.
TERACO AFRICA'S DATA CENTRE
TATA COMMUNICATIONS
Telia Carrier
TelecityGroup
Telefonica
KDDI TELEHOUSE
telenor
Telstra
TELUS
transtelco
TIME
T··Systems·
UIH your future is our passion
UOL DIVEO
verizon
vodafone
webair Secure. Managed. Scalable.
windstream
zayo
zertia
ZIRRO
zain

200+ ExpressRoute Partners

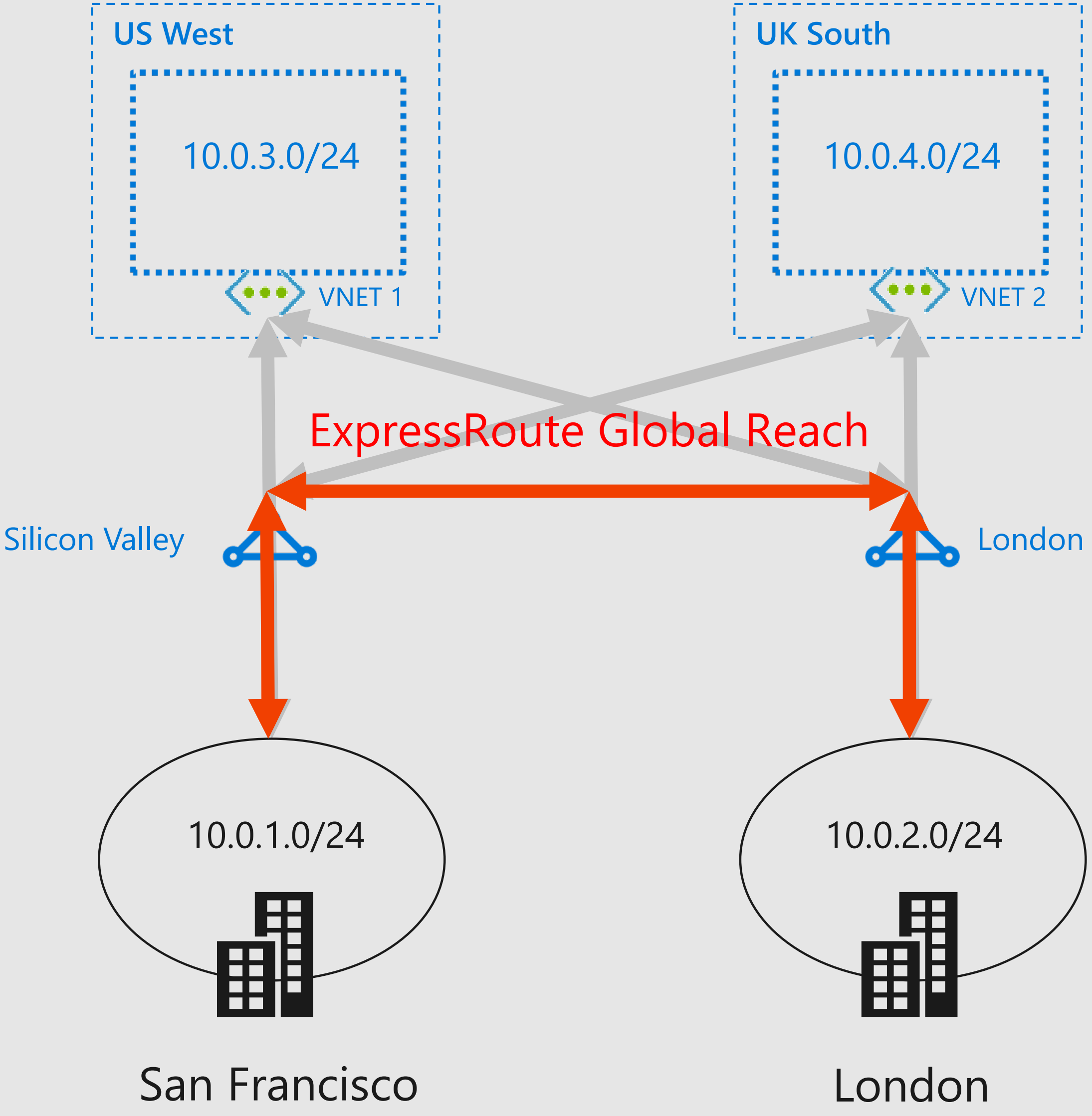
ExpressRoute Global Reach

ExpressRoute enables you to connect to Azure

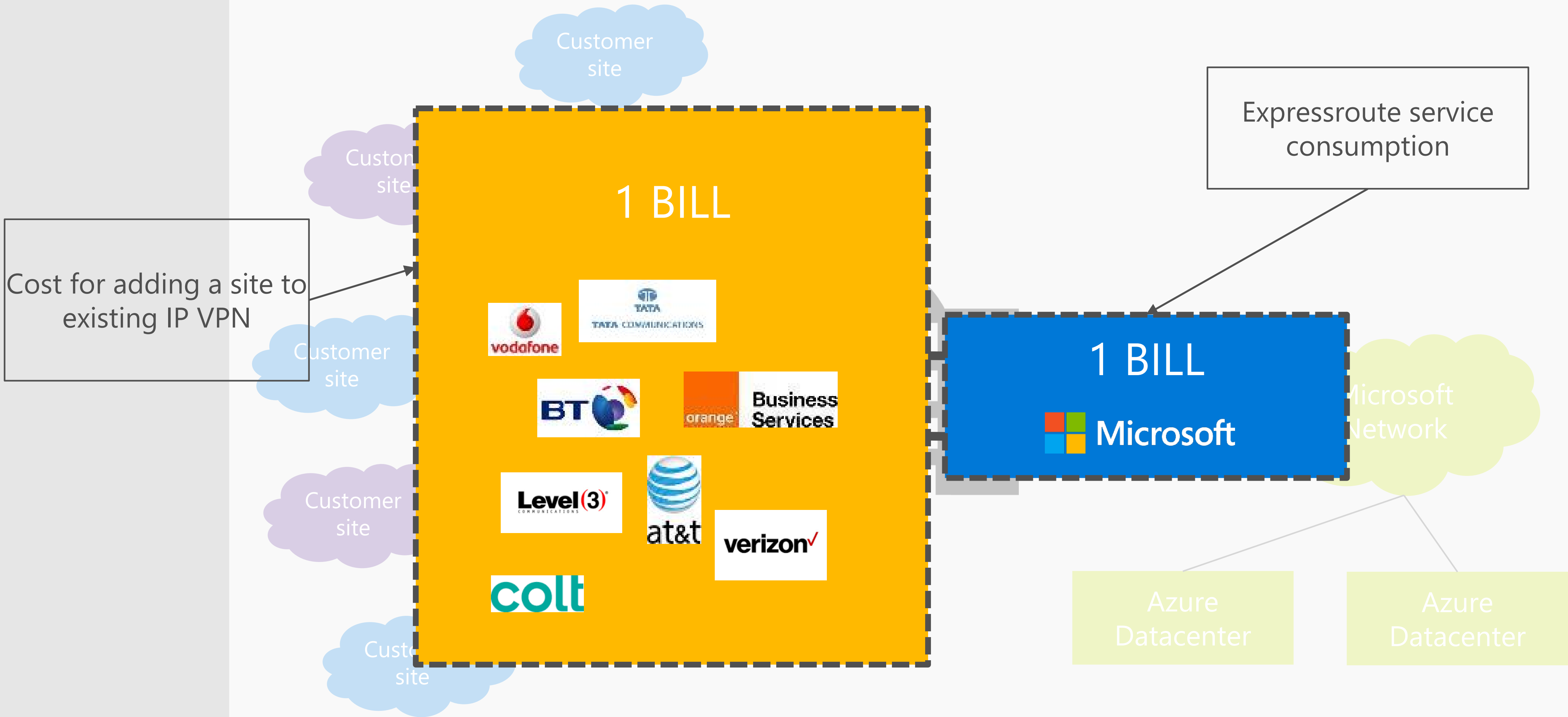
ExpressRoute Global Reach enables you to connect your sites

- On-demand connectivity using your existing ExpressRoute circuits
- Traffic staying on Microsoft's global network

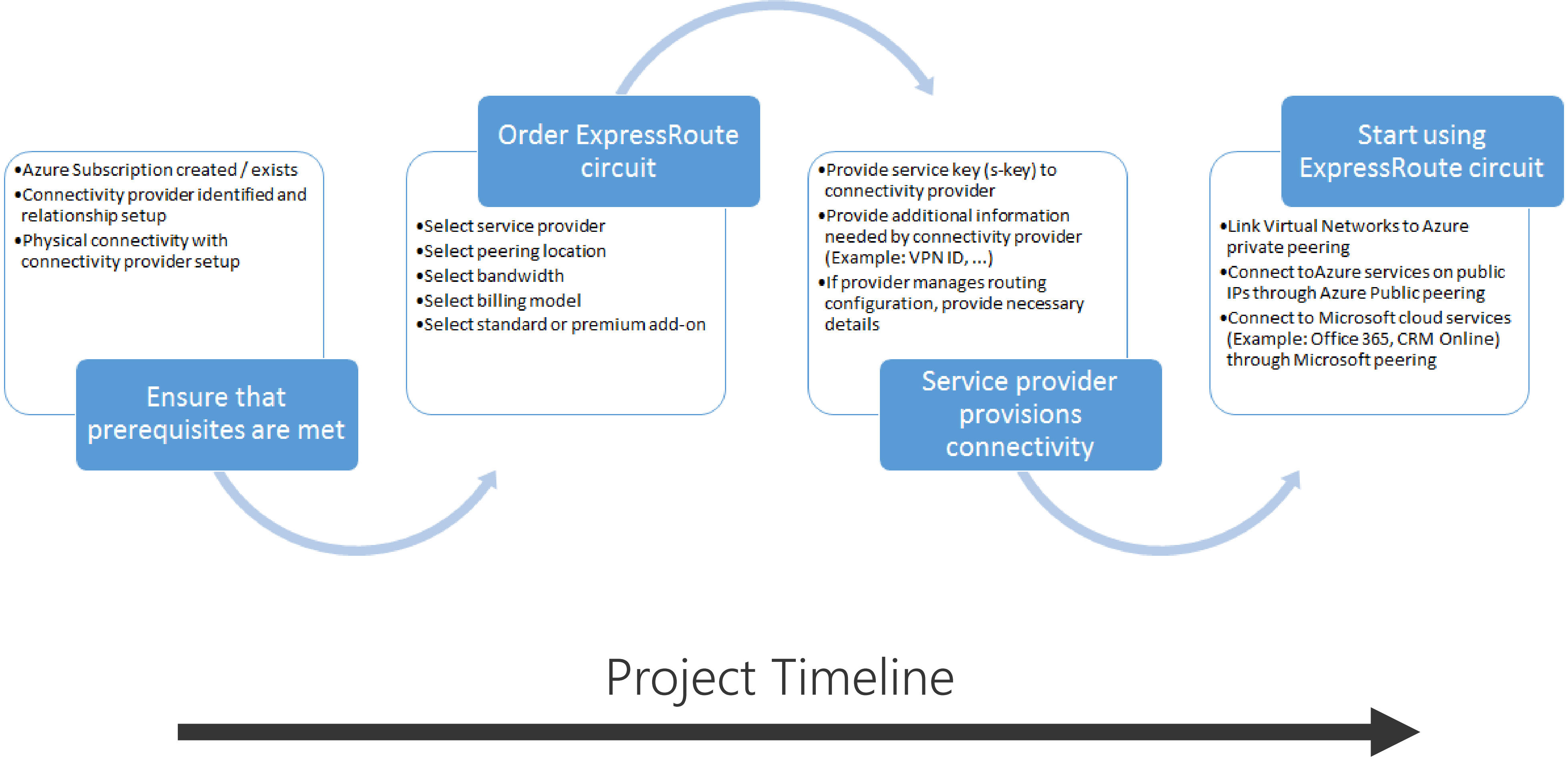
Complement your service provider's WAN solution



Example: IP VPN Connection Cost structure



ExpressRoute implementation



Ensure that prerequisites are met

- Azure Subscription created / exists
- Connectivity provider identified and relationship setup
- Physical connectivity with connectivity provider setup

Order ExpressRoute circuit

- Select service provider
- Select peering location
- Select bandwidth
- Select billing model
- Select standard or premium add-on

Service provider provisions connectivity

- Provide service key (s-key) to connectivity provider
- Provide additional information needed by connectivity provider (Example: VPN ID, …)
- If provider manages routing configuration, provide necessary details

Start using ExpressRoute circuit

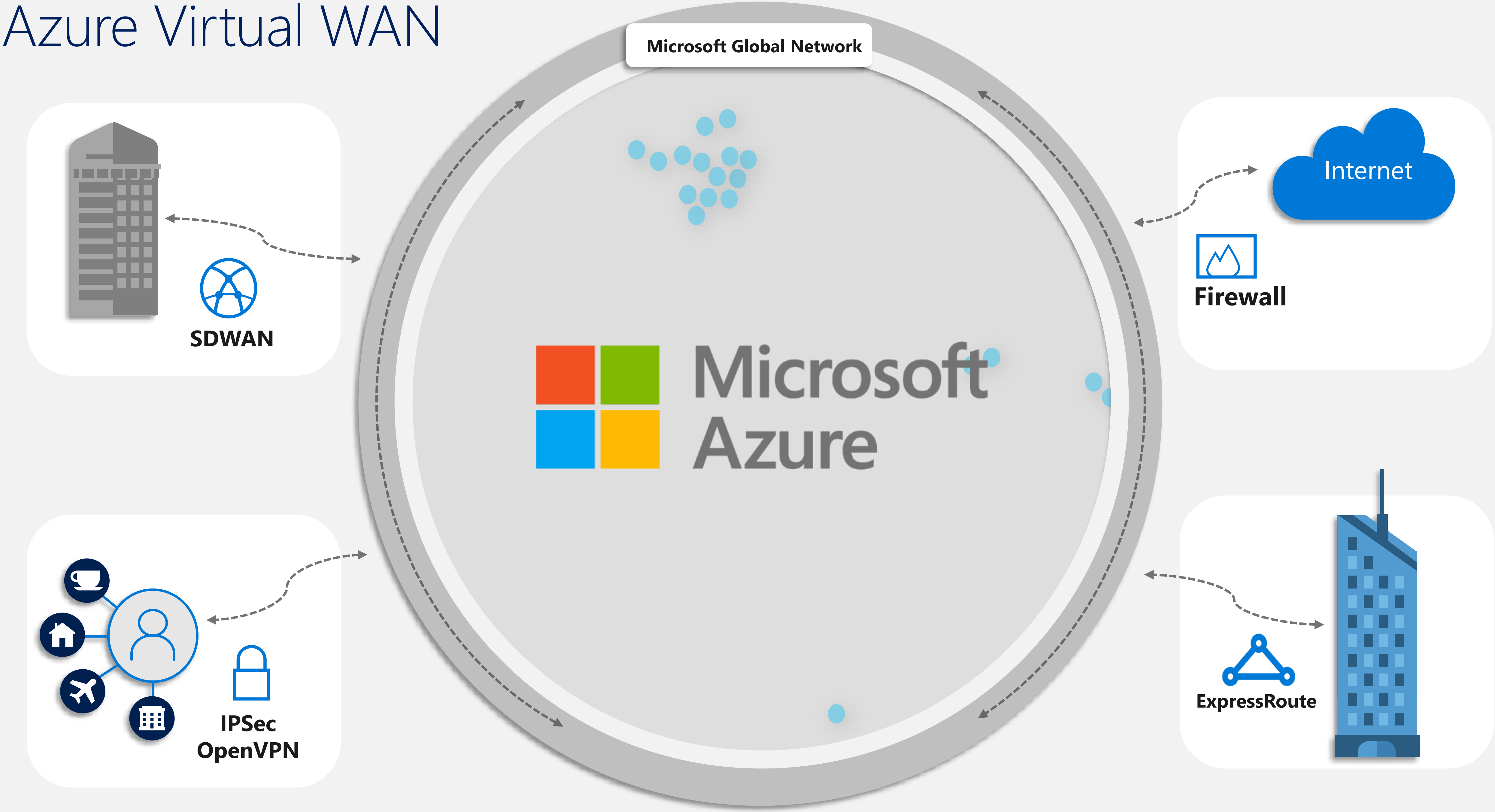
- Link Virtual Networks to Azure private peering
- Connect toAzure services on public IPs through Azure Public peering
- Connect to Microsoft cloud services (Example: Office 365, CRM Online) through Microsoft peering

Project Timeline

6 weeks - …

Azure Virtual WAN

Azure Virtual WAN



Virtual WAN General availability

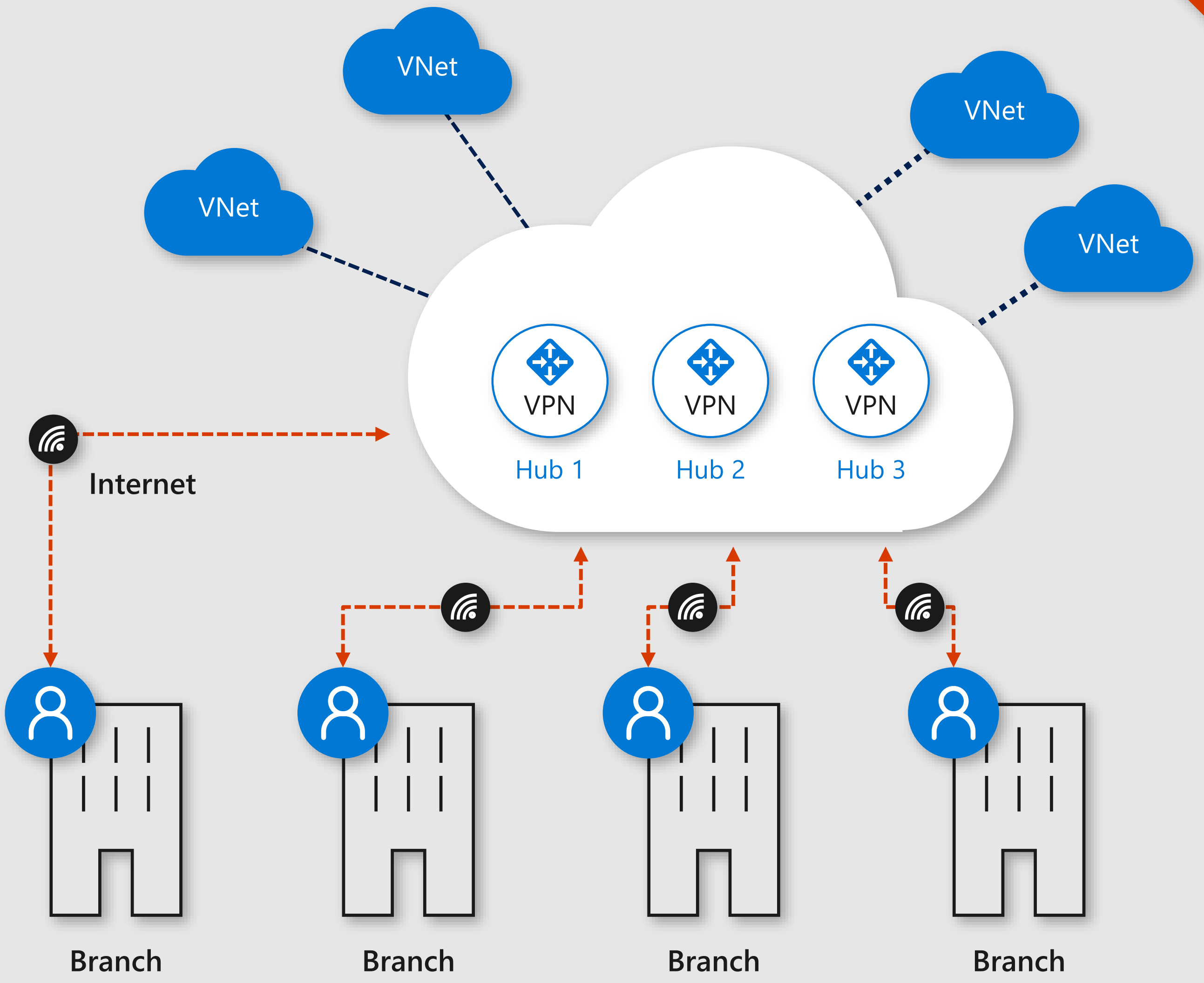
GA

Branch-to-Azure, branch-to-branch

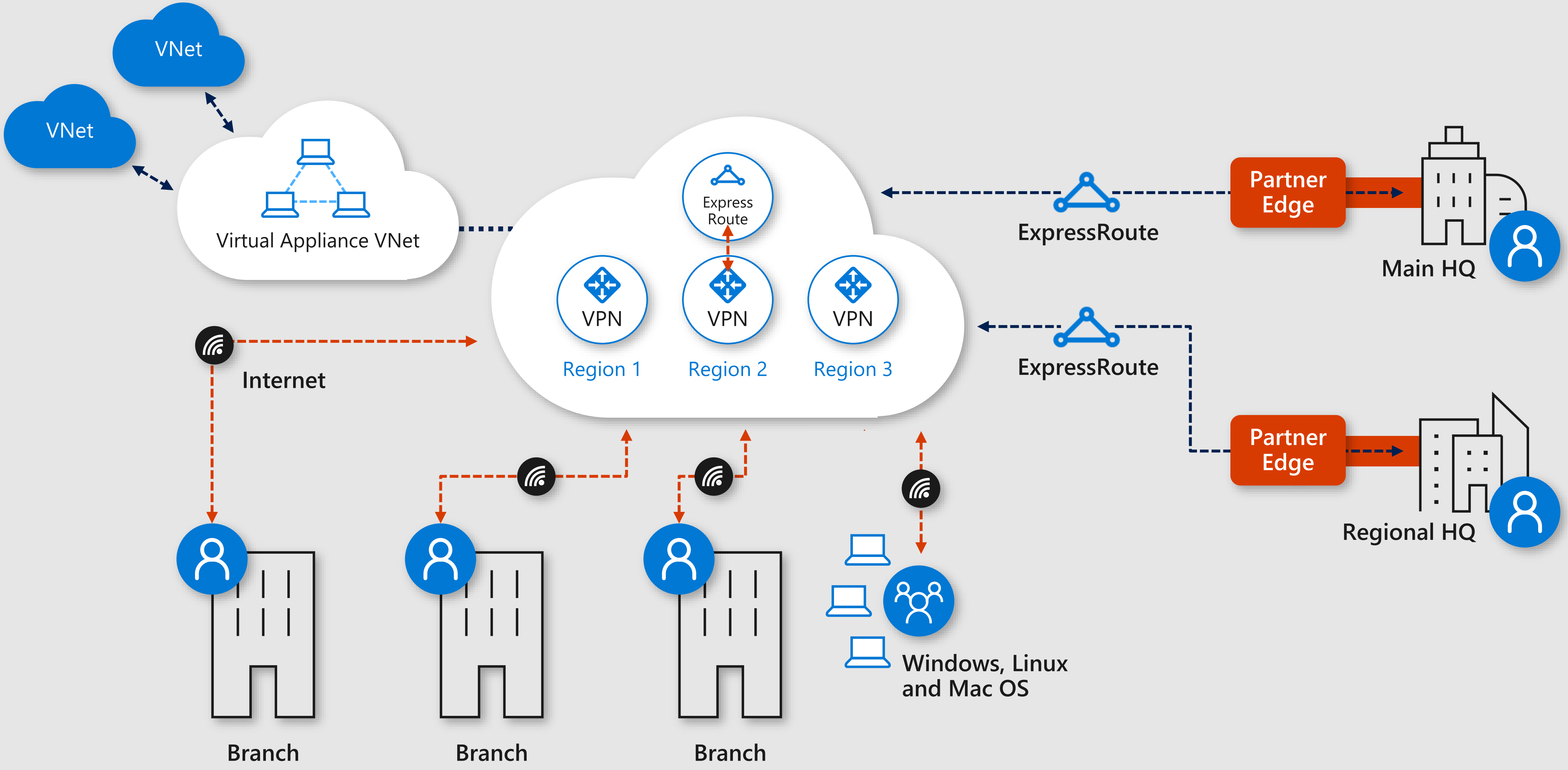
Automated provisioning and configuration

Scalability and high throughput

Large and growing integrated partner ecosystem



Virtual WAN - preview features



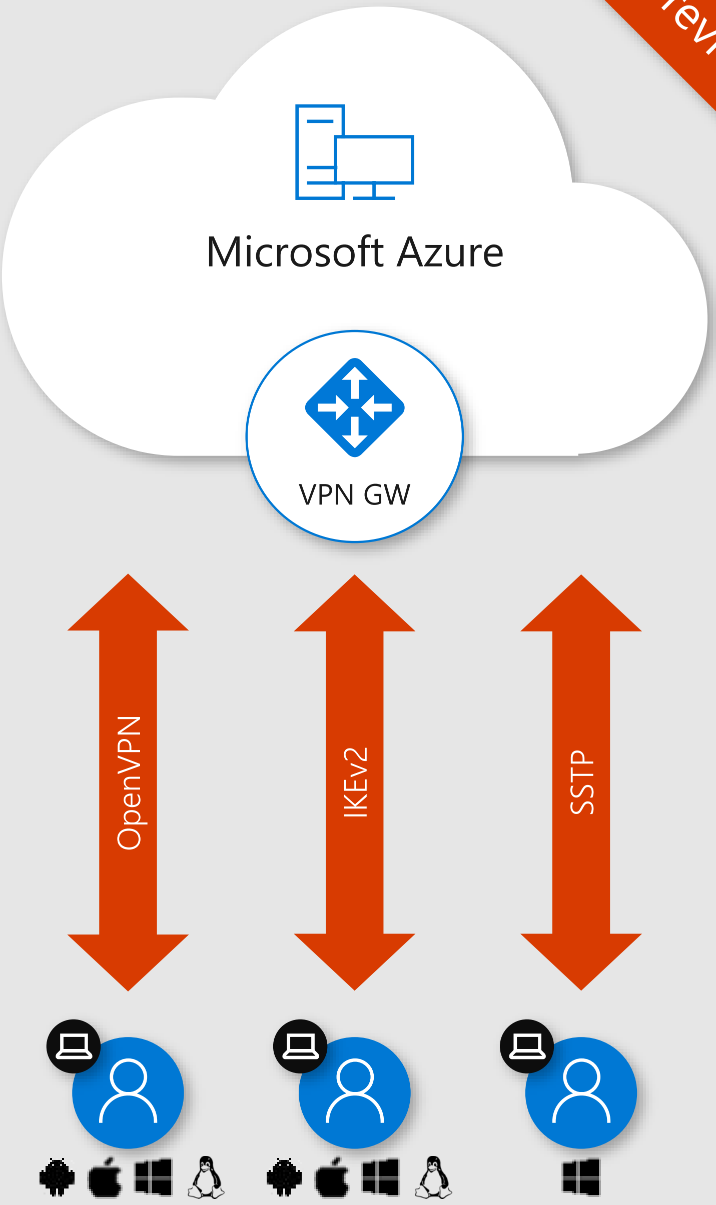
Point-to-site VPN

Preview

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

Azure Virtual WAN supports OpenVPN® and IKEv2 for connectivity

	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



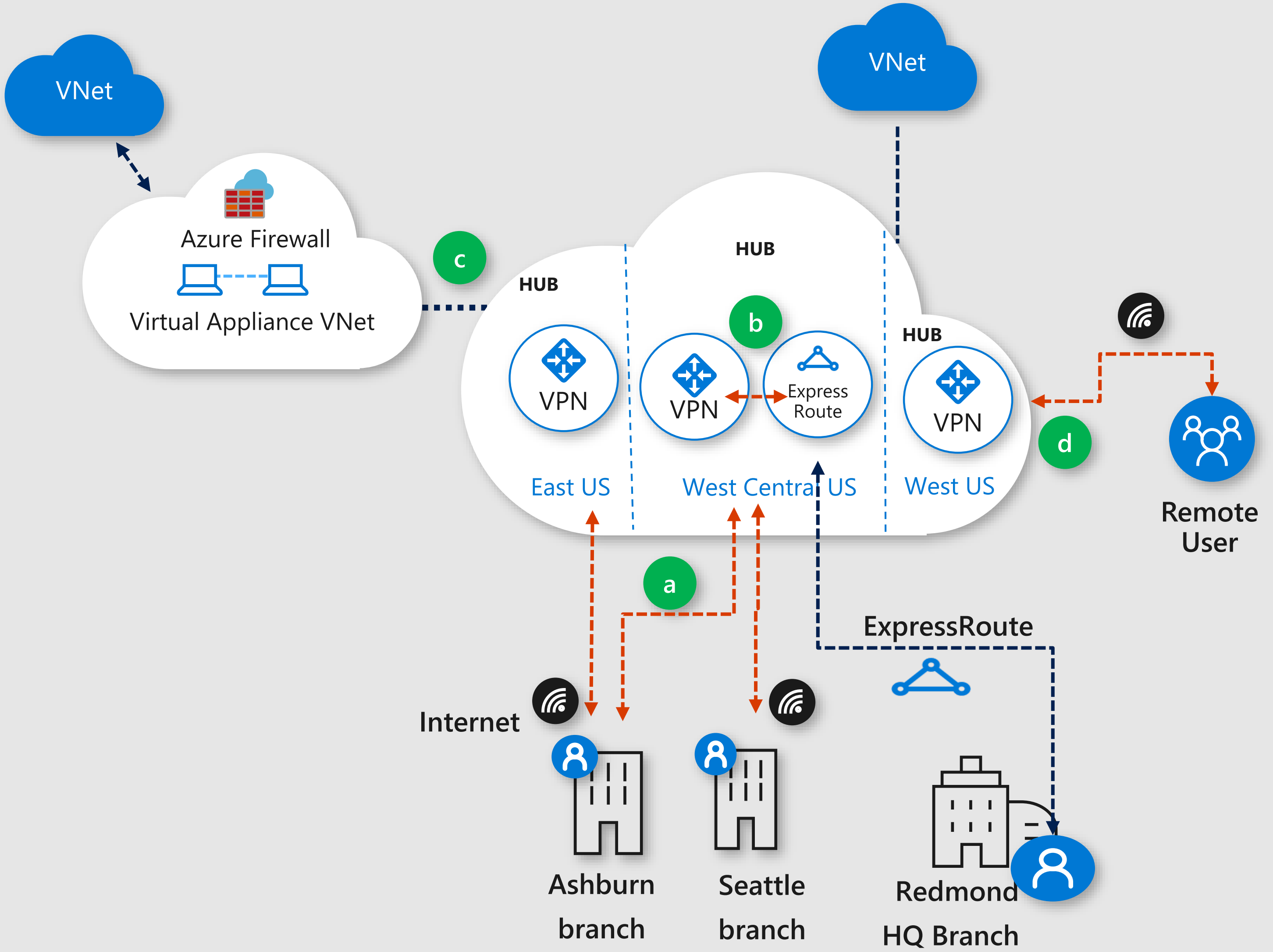
Demo architecture

a. Branch to branch

b. Branch to branch (VPN<->ER)

c. Branch to Azure : connect workload VNet with Virtual Appliance , Azure Firewall

d. Connect Mobile device



Azure Virtual WAN—summary

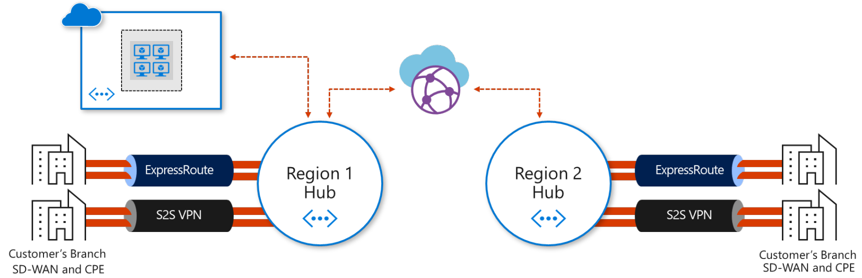
GA: global-scale branch connectivity

- Branch-to-Azure, branch-to-branch
- Automated provisioning and configuration
- Large and growing Integrated partner ecosystem

Public preview

- ExpressRoute
- Point-to-Site
- Office 365 Policy

Software defined connectivity



ExpressRoute
S2S VPN
Region 1 Hub
Region 2 Hub
ExpressRoute
S2S VPN
Customer's Branch SD-WAN and CPE
Customer's Branch SD-WAN and CPE

Available today

CITRIX, riverbed, NETFOUNDRY SPIN UP YOUR NETWORK, Check Point SOFTWARE TECHNOLOGIES LTD., 128 TECHNOLOGY, Barracuda, paloalto NETWORKS

Coming soon

CLOUDGENIX NETWORKS WITHOUT NETWORKING, velocloud Now part of VMware, silver peak, VERSA NETWORKS, nuagenetworks From Nokia

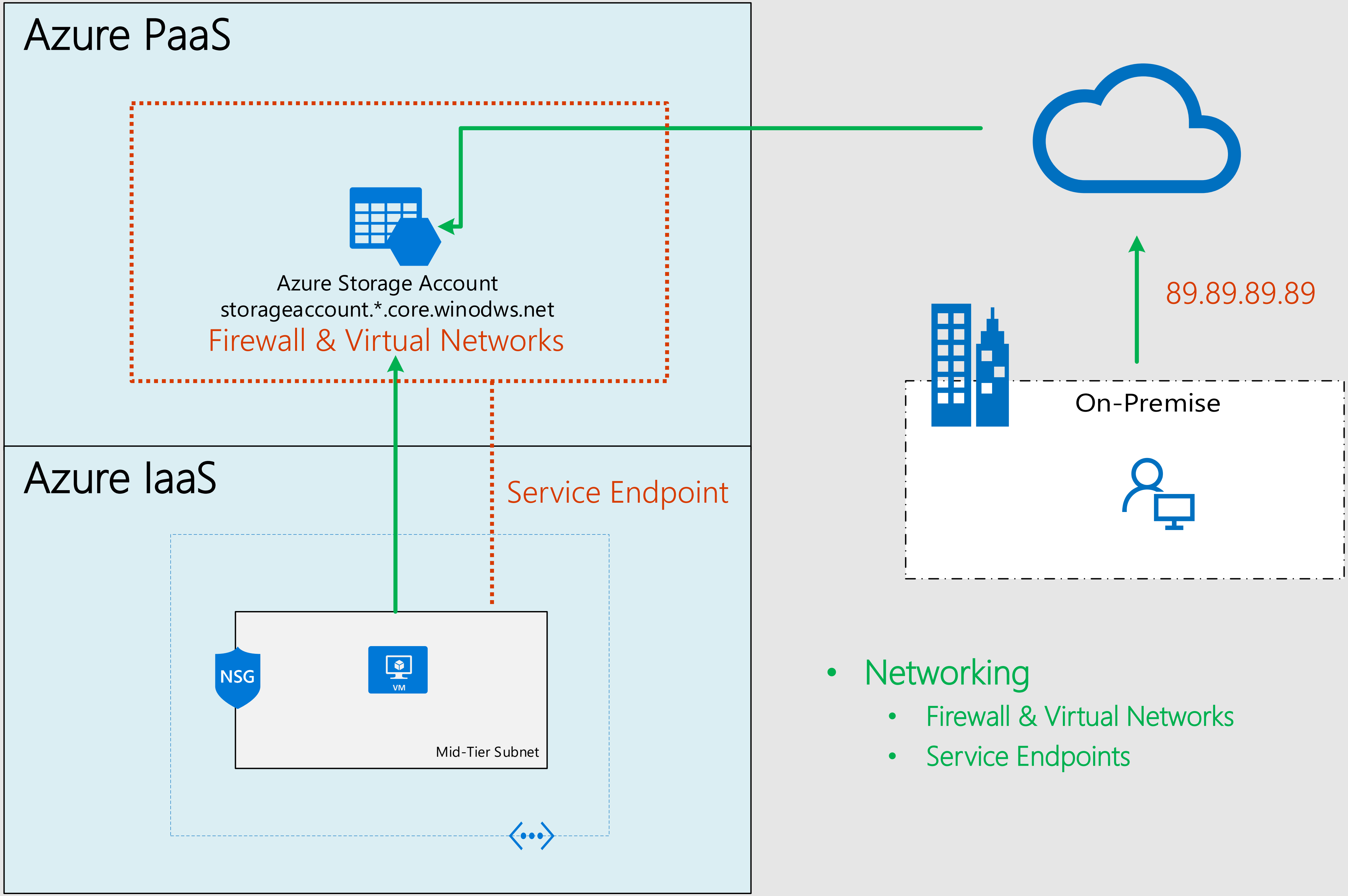
Use case: Azure Storage PaaS

Use case: Azure storage account

- Azure Storage Account
  - PaaS component
  - Commonly used
  - Unique Public Endpoint
  - Contains all sort of data types (blob, files, table…)
  - Different Blob Tiers (Hot, Cold, Archive)

Use case: Azure storage account

- Networking
  - Public endpoint, no no no…!
- Security
  - How secure is my data?
  - How secure is the access to the data?
- Identity
  - Who can access when?
  - Can I secure the management plane (who can manage what?)



- Networking
  - Firewall & Virtual Networks
  - Service Endpoints

Azure Storage Security

Management plane

- The management plane consists of the resources used to manage your storage account
- Access is granted by assigning the appriopriate Role Based Access Control to Azure AD users, Groups, Applications, at the right scope
- Predefined RBAC roles exist and custom roles can be created
- RBAC roles are defined at Azure AD level and can be scoped on subscription level and finegrained on underlying Azure resources
- Storage Keys can be used to access the data objects stored in the storage account, for example blobs, table, que, files on Azure file share

Data plane

- Data Plane Security refers to the methods used to secure the data objects stored in Azure Storage – the blobs, queues, tables, and files. We've seen methods to encrypt the data and security during transit of the data, but how do you go about controlling access to the objects?
- Three authorization options
  1. Using Azure AD (Preview)
  2. Using Storage Account Keys
  3. Using Shared Access Signatures to grant controlled permissions
- Limit access to the storage account based on network rules (firewall)
- Privatize Azure storage accounts to a VNET with service endpoints
- Ability to create stored access policies for service-level SAS (account-level not supported atm)
- Use Immutable Storage for legal hold or time-based retention

Encryption plane

In Transit

- Use HTTPS when calling REST APIs or accessing storage objects
- Enforce HTTPS when creating SAS tokens
- SMB 3.0 encryption support for Azure Files
- Use Client-Side encryption to secure data that you send to storage

At Rest

- Use Azure Disk Encryption (ADE) to encrypt the OS and data disks in IaaS VMs
- ADE leverages Bitlocker for Windows VMs
- ADE leverages DM-Crypt for Linux VMs
- Storage Service Encryption (SSE) automatically encrypts your data when writing it to Azure Storage
- SSE supports custom keys managed by Azure Key Vault

Analytics plane

- Leverage Storage Analytics (SA) to gain storage insights
- SA will allow you to monitor storage authorization
- SA will allow you to perform logging and store metrics data

Main Challenge

- Involve all stakeholders
  Human design!
- Agree on a final solution
- Push your business forward!

Firewall!!!!
Sigh!
Sorry Sarah, won't be possible!
Oi! What did you built ?

Sarah
Business Development Manager

Jack
IT Magician

Vladimir
Security Team

What's Next ?

	Technical Track	Services & Management Track
15:00-15:30	Break	
15:30-16:15	Improve your security score with Azure Security Center *Bart Verboven*	Discover new insights with Azure's Data Science Services *Tim Van Durme*