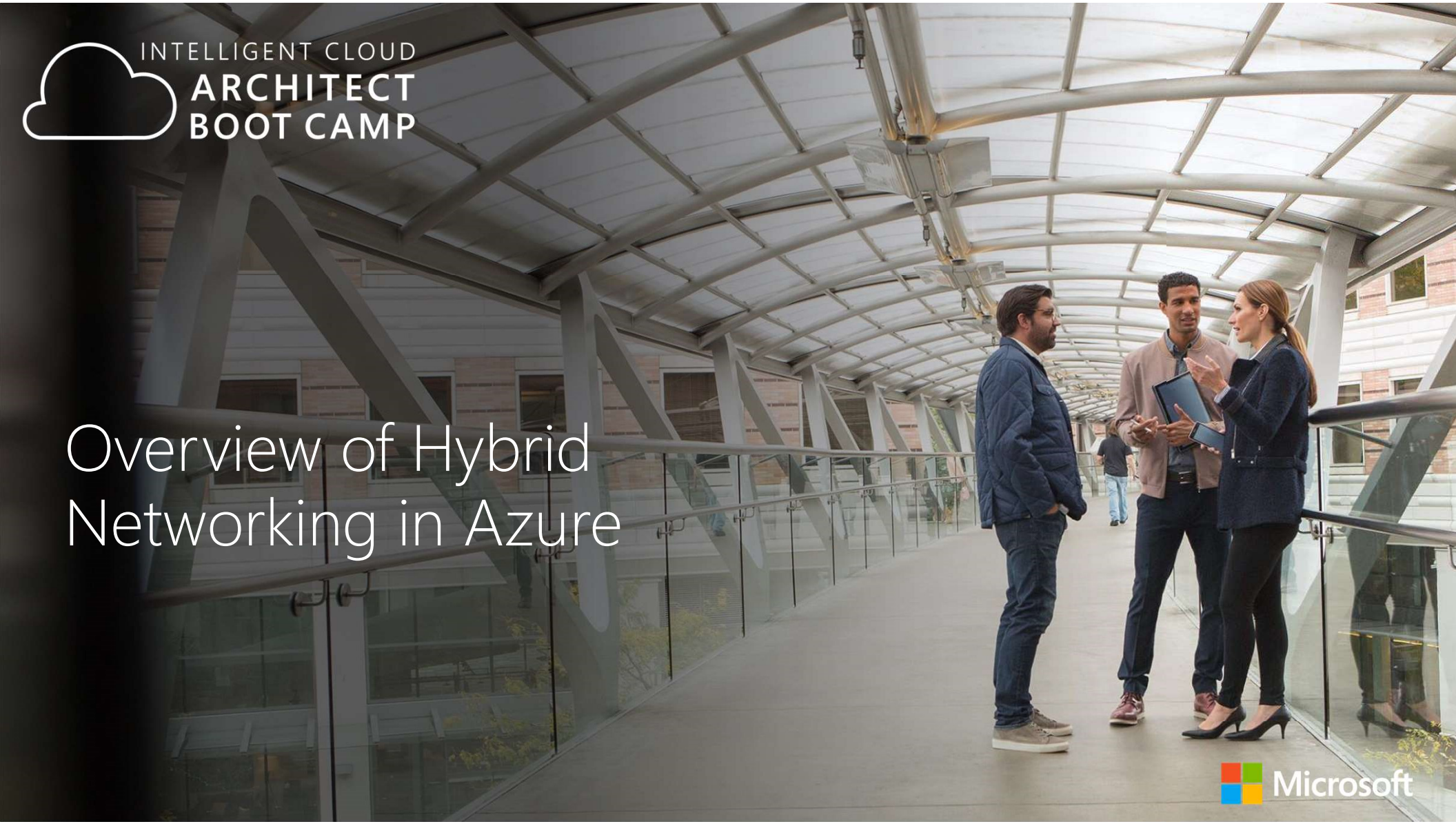

INTELLIGENT CLOUD
ARCHITECT
BOOT CAMP
Overview of Hybrid Networking in Azure
Microsoft

Session Objectives & key takeaways

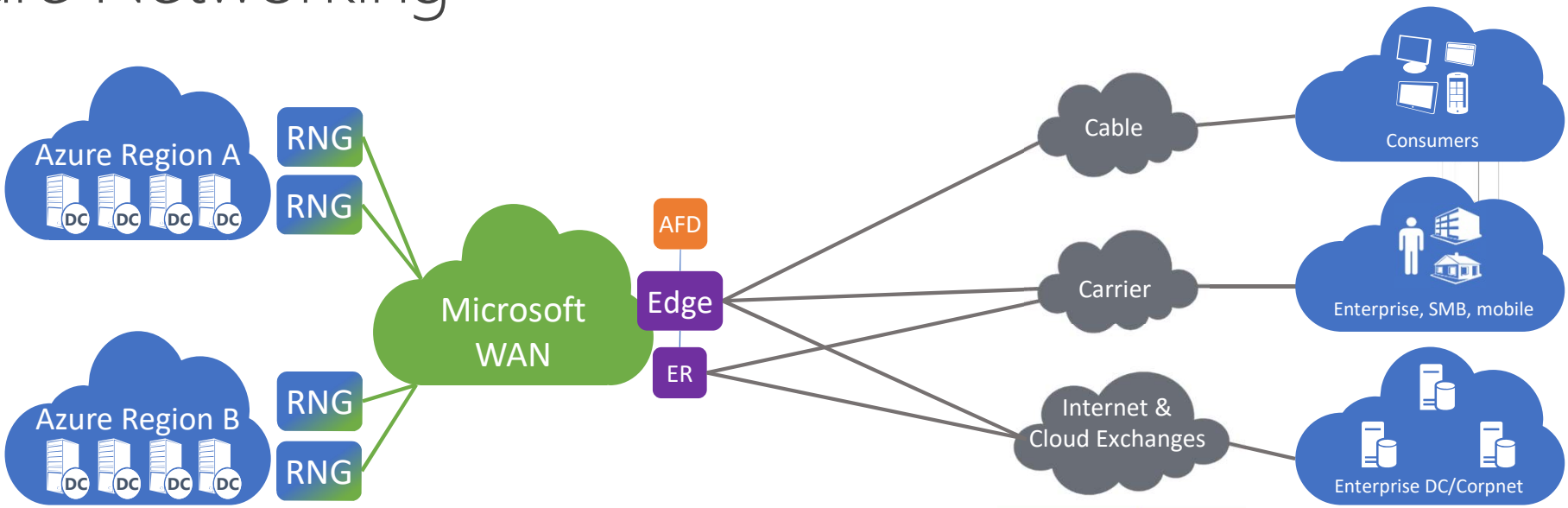
At the end of this session you will be better able to

- decide which cross-premises connectivity options for your customers
- base on architecture, topology, security, and performance requirements
- understand routing between on-premises and clouds, across the clouds, and within the clouds

Agenda

- Introduction
- ExpressRoute
- S2S VPN
- P2S VPN
- Routing in Azure

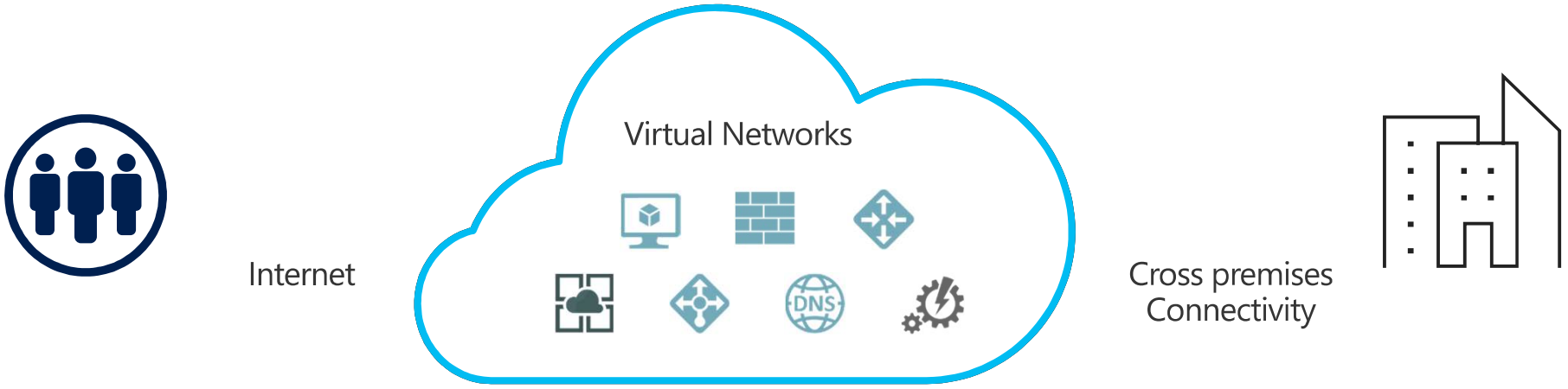
Azure Networking



Hardware	Intra-Region	Services	WAN Backbone	Edge and ExpressRoute	FrontDoor/CDN	Last Mile
• SmartNIC/FPGA • SONiC • Madison Optics	• DC Networks • Regional Networks	• Virtual Networks • Load Balancing • Firewall, DDoS • VPN Services • Security • DNS	• Software WAN • National Clouds	• Internet Peering • ExpressRoute	• Acceleration for O365, Bing, Windows Store	• E2E monitoring

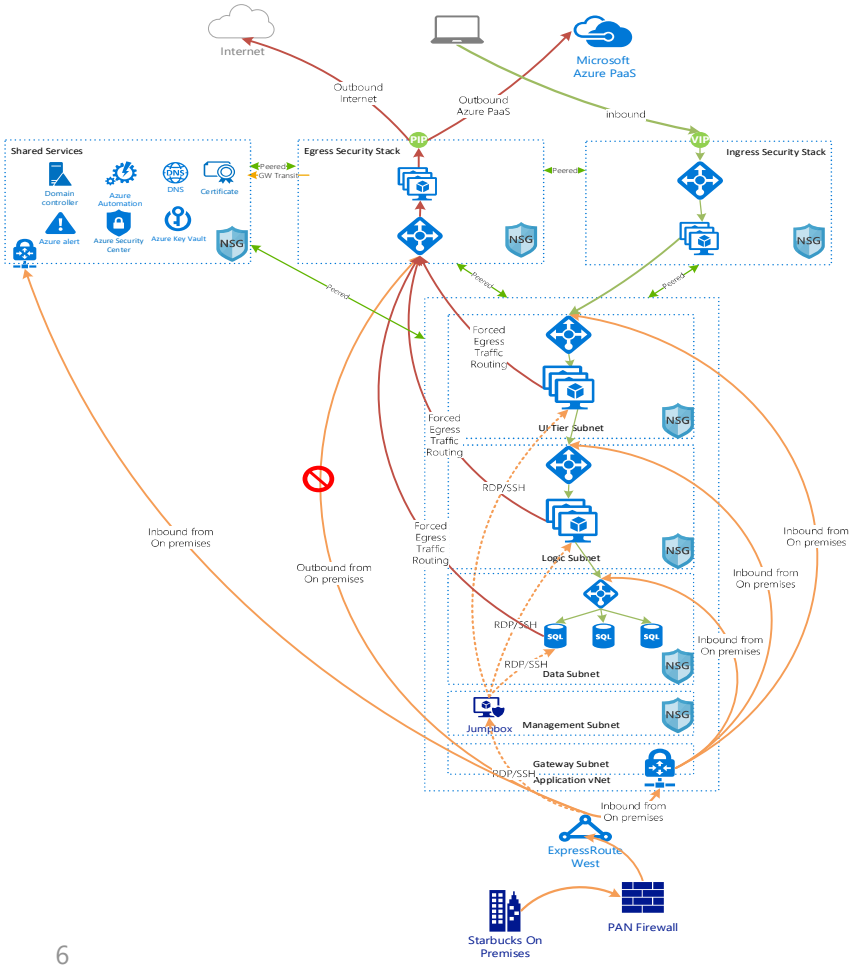
Operations, Monitoring, Buildouts
Partner Ecosystems

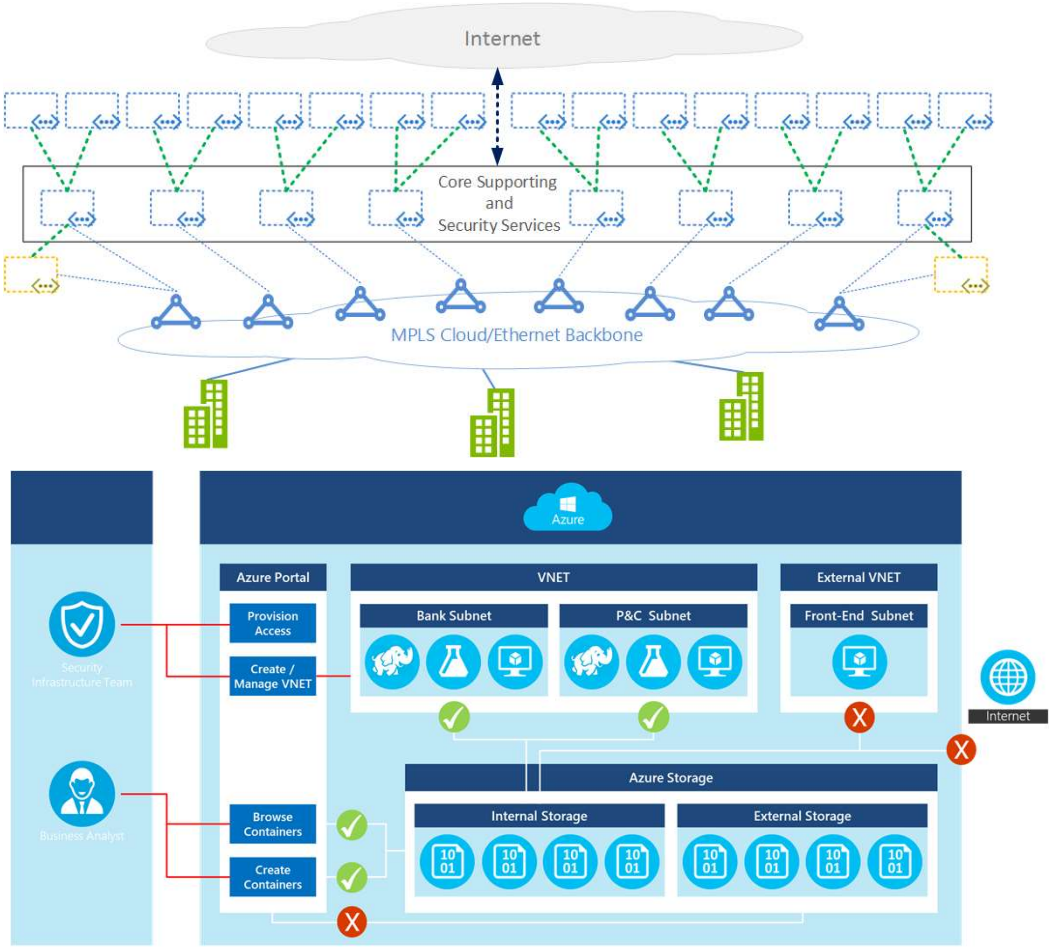
This is how we present the Cloud



- Secure per customer virtual datacenter in the cloud
- Instantiate and configure complex topologies in minutes
- Rich security and networking services

This is what the customers need …





Building Blocks

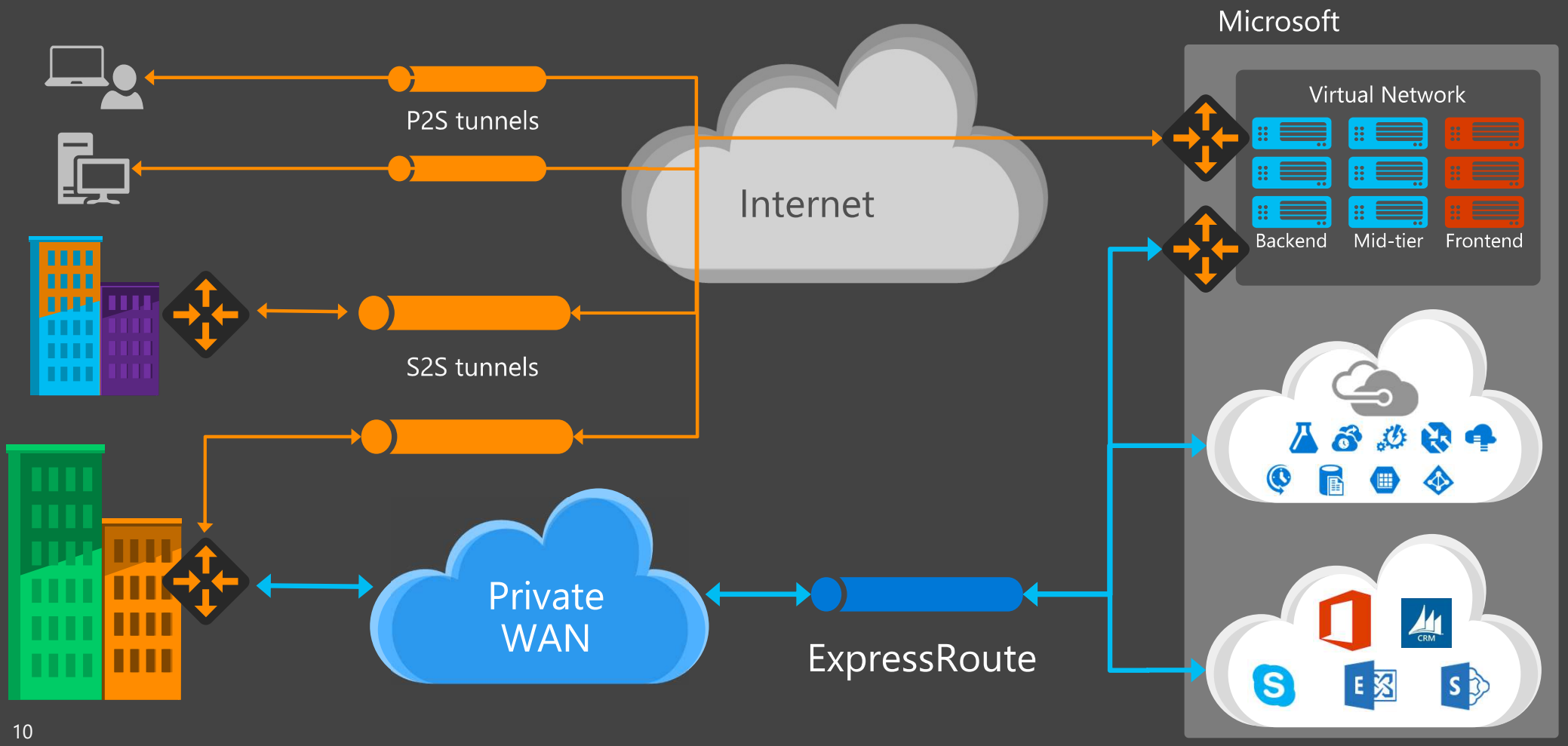
Connecting to Azure

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

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

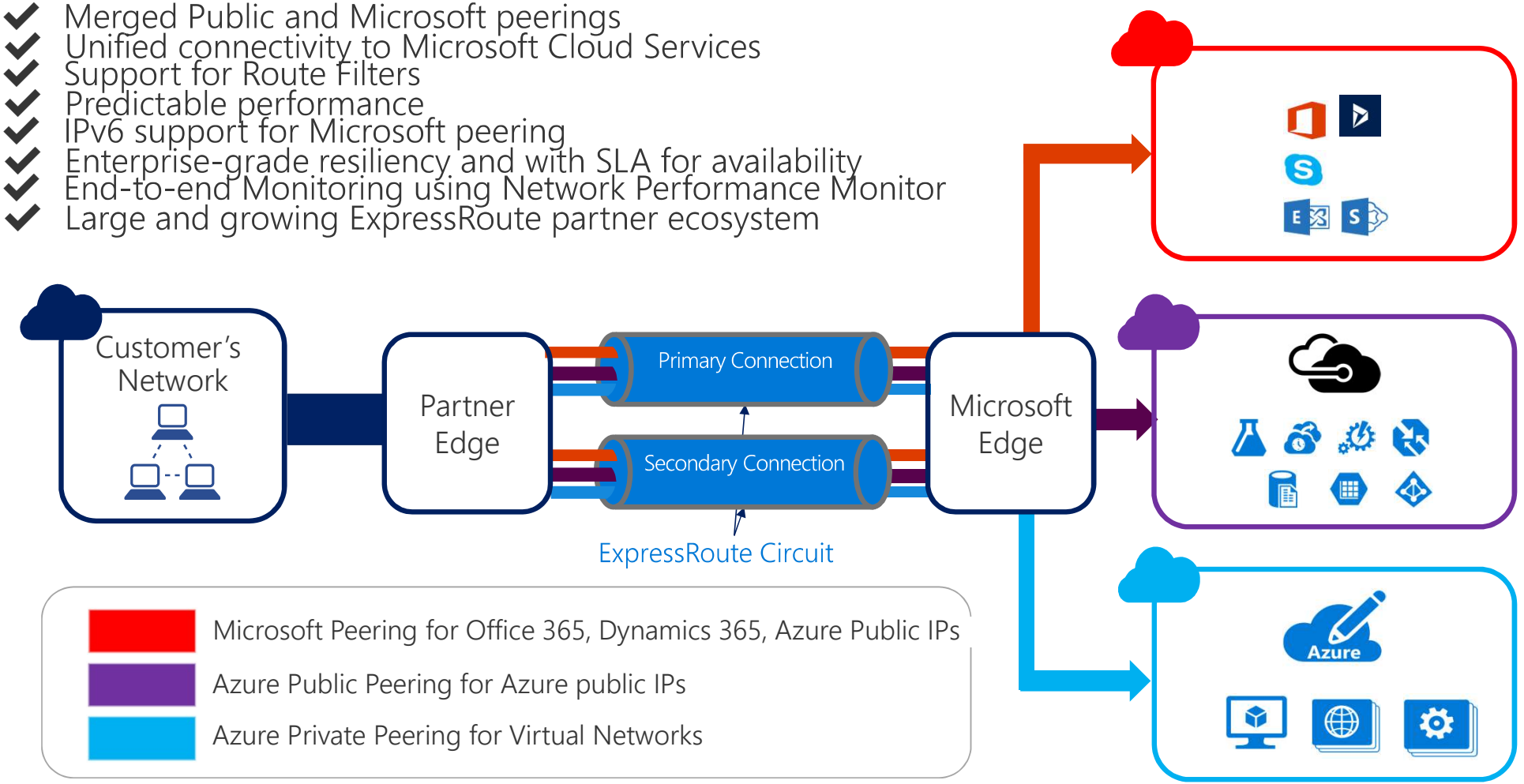
Cross Premises Connectivity



ExpressRoute

ExpressRoute

- Merged Public and Microsoft peerings
- Unified connectivity to Microsoft Cloud Services
- Support for Route Filters
- Predictable performance
- IPv6 support for Microsoft peering
- Enterprise-grade resiliency and with SLA for availability
- End-to-end Monitoring using Network Performance Monitor
- Large and growing ExpressRoute partner ecosystem

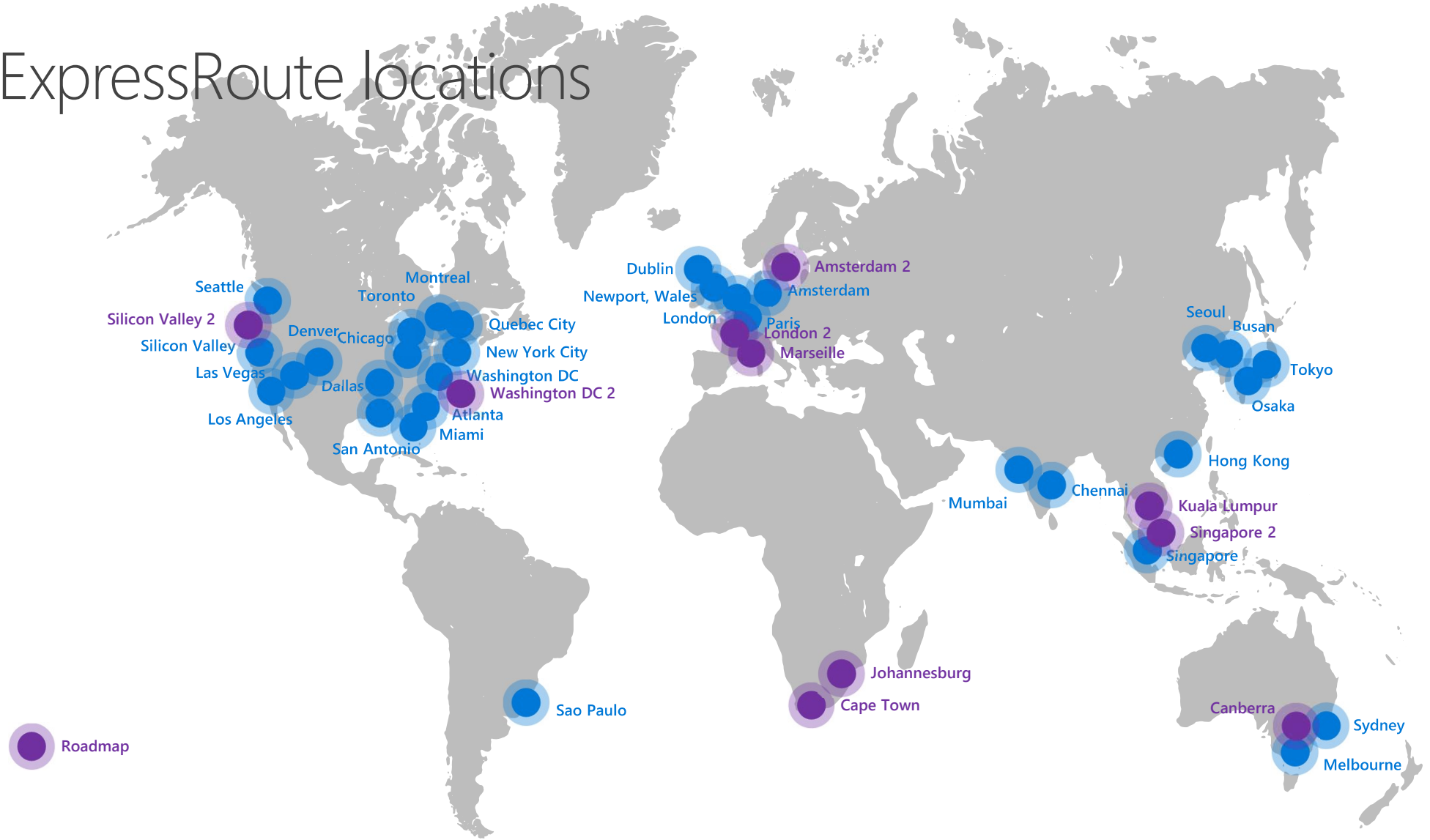


Terminology & concepts

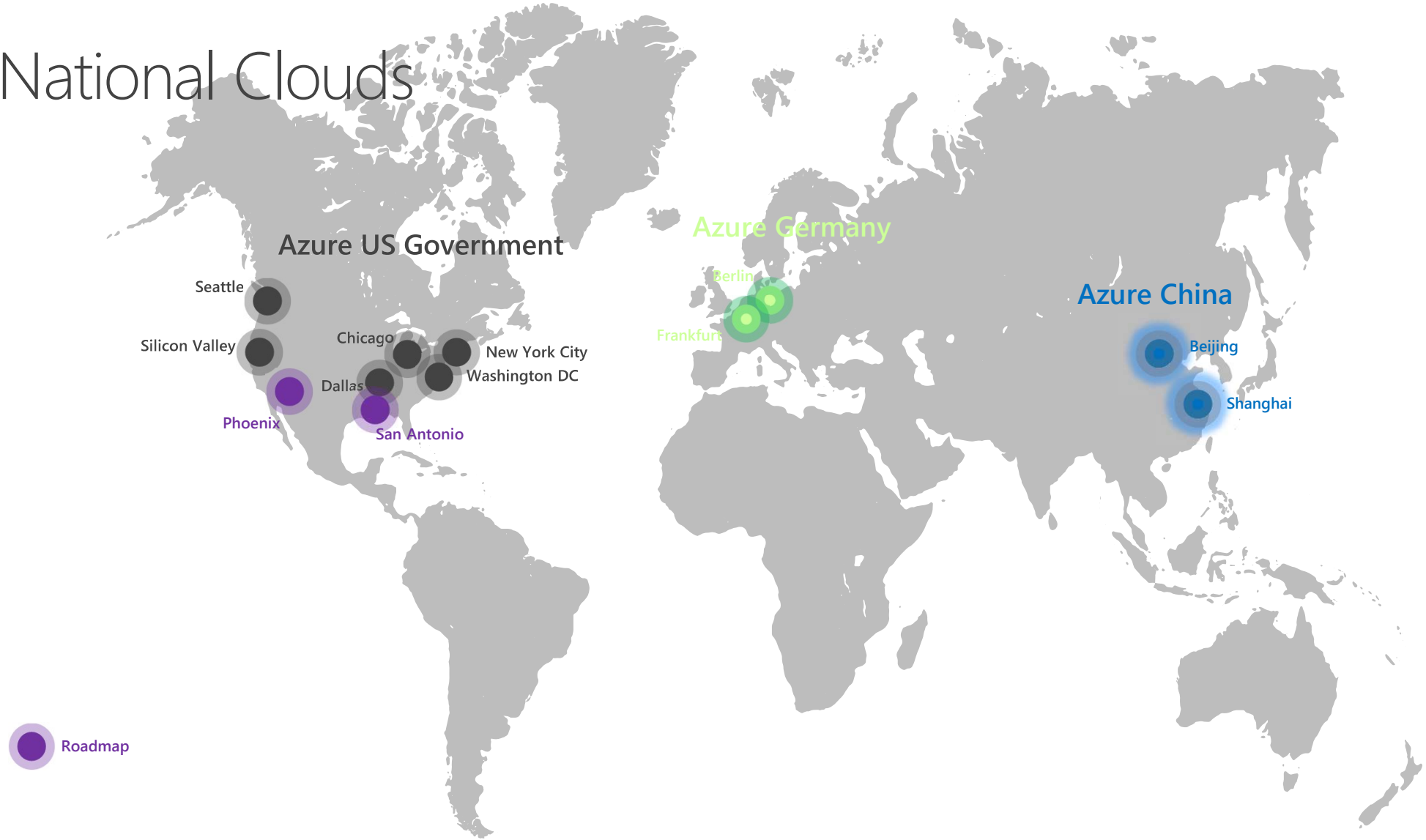
- Circuit
  - The unit of ExpressRoute “connectivity”
  - Bandwidth (50M-10G), provider, location (e.g., 1Gbps, Verizon, Chicago)
- Peering
  - Connectivity types – to customer “private” networks (VNets) or to “Microsoft” services – Azure PaaS, O365, Dynamics
- Route filter & BGP community
  - Specify (route filters) or identify (BGP community) what services to connect from on-premises to Microsoft Services
- Gateway & connection
  - Connecting an ExpressRoute circuit to Azure Virtual Networks

MICROSOFT CONFIDENTIAL – INTERNAL ONLY

ExpressRoute locations



National Clouds

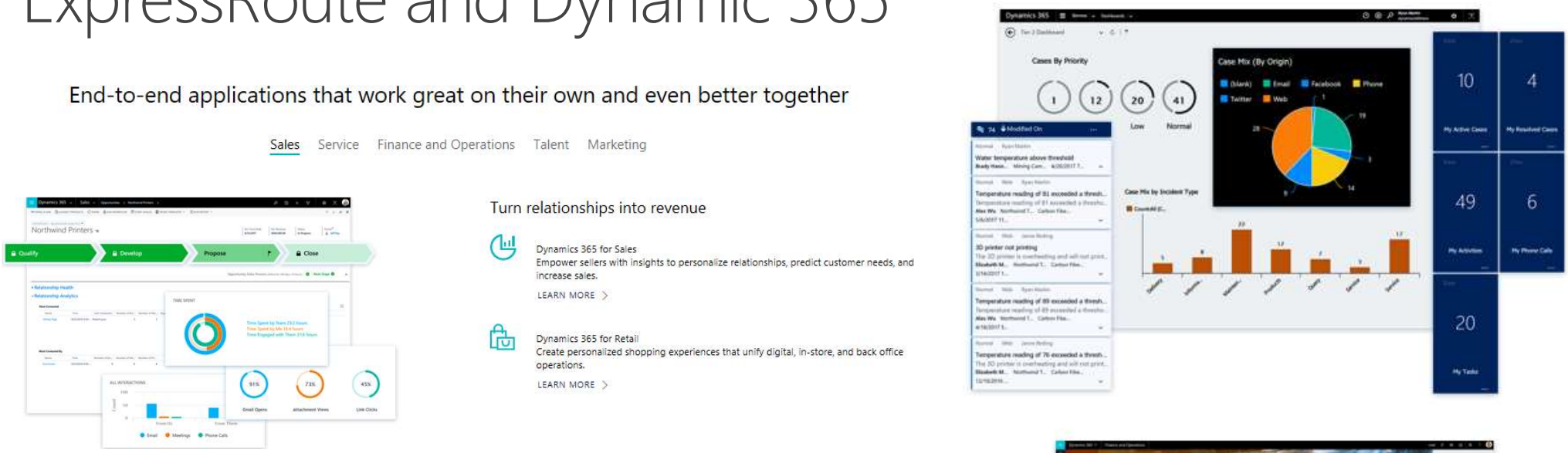


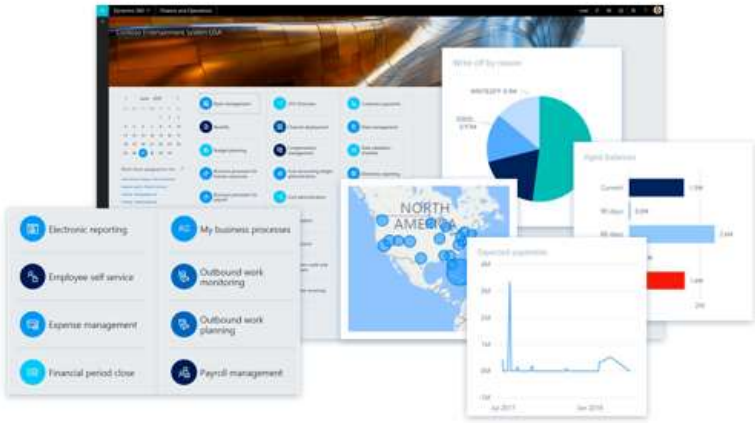
ExpressRoute Providers/Partners

ExpressRoute and Office 365

- ExpressRoute for Office 365 is only recommended in specific scenarios
  - Regulatory requirements that mandate a private connection
  - Network assessment for Skype for Business/Teams shows network deficiencies ExpressRoute can address
- Enabling Office 365 requires review and approval from Microsoft
  - Customers cannot create route filters for Office 365 if their subscription is not whitelisted by O365 team. More info on http://aka.ms/ExpressRouteOffice365
- Office 365 promotion of ExpressRoute Premium Add-On ending
  - New customers will no longer be eligible for free ExpressRoute Premium Add-On
- Office 365 SLA requires ExpressRoute connectivity at multiple sites
  - Customer's connectivity to O365 must not be dependent on a single ExpressRoute circuit

ExpressRoute and Dynamic 365





- Dynamics 365 services available on Microsoft Peering
  - Dynamics 365 for Sales
  - Dynamics 365 for Customer Service
  - Dynamics 365 for Field Service
  - Dynamics 365 for Project Service
  - Dynamics 365 for Finance and Operations (Dynamics AX Online)
- Dynamics 365 on ExpressRoute is self-service

S2S VPN

VPN Gateways

SKU	Workload	Throughput*	S2S/V2V	SLA
VpnGw1	Production	650 Mbps	Max. 30	99.95%
VpnGw2	Production	1 Gbps	Max. 30	99.95%
VpnGw3	Production	1.25 Gbps	Max. 30	99.95%
Basic	Dev/Test	100 Mbps	Max. 10	99.9%

- Type
  - Route-based – router (IKEv2)
  - Policy-based – firewall (IKEv1)
- SKUs
  - Mainly differentiate on throughputs
  - Same feature sets (except Basic)

- Features
  - BGP, transit routing, forced tunneling
  - Gateway transit (VNet peering)
  - Active-active
  - Custom policy – IPsec/IKE

MICROSOFT CONFIDENTIAL – INTERNAL ONLY

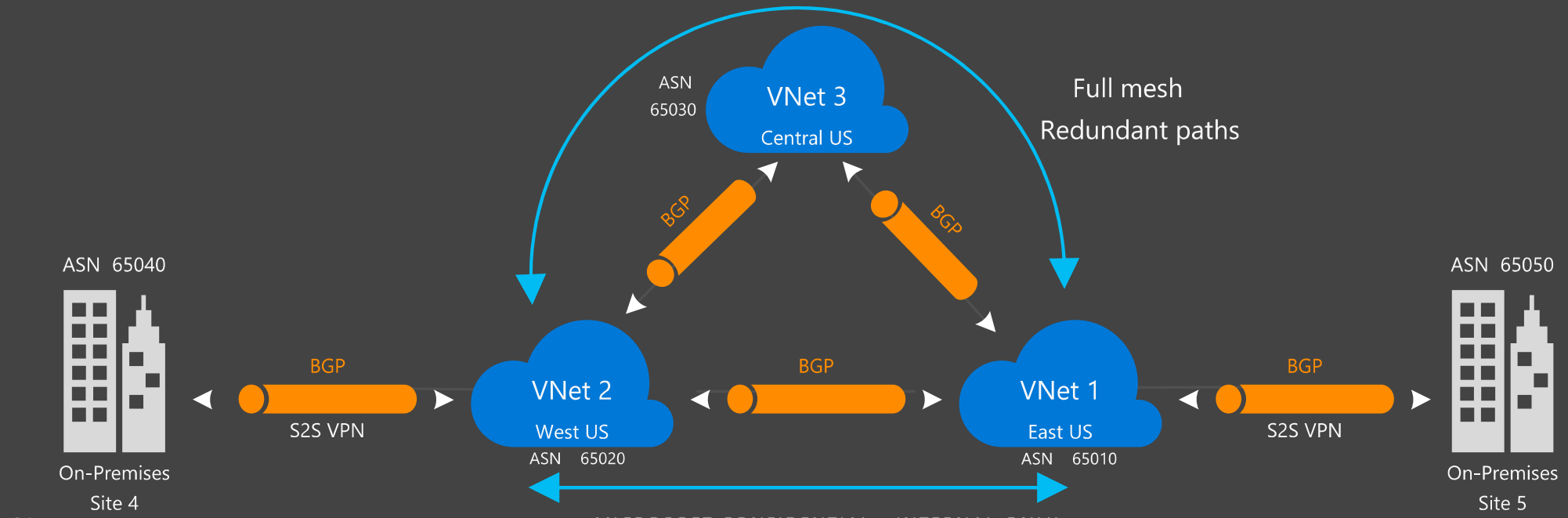
Secure VPN Transit

BGP for redundant paths and dynamic routing

Automatic shortest path selection and failover

Transit over Microsoft global network

Secure connectivity using Internet only for "last mile"

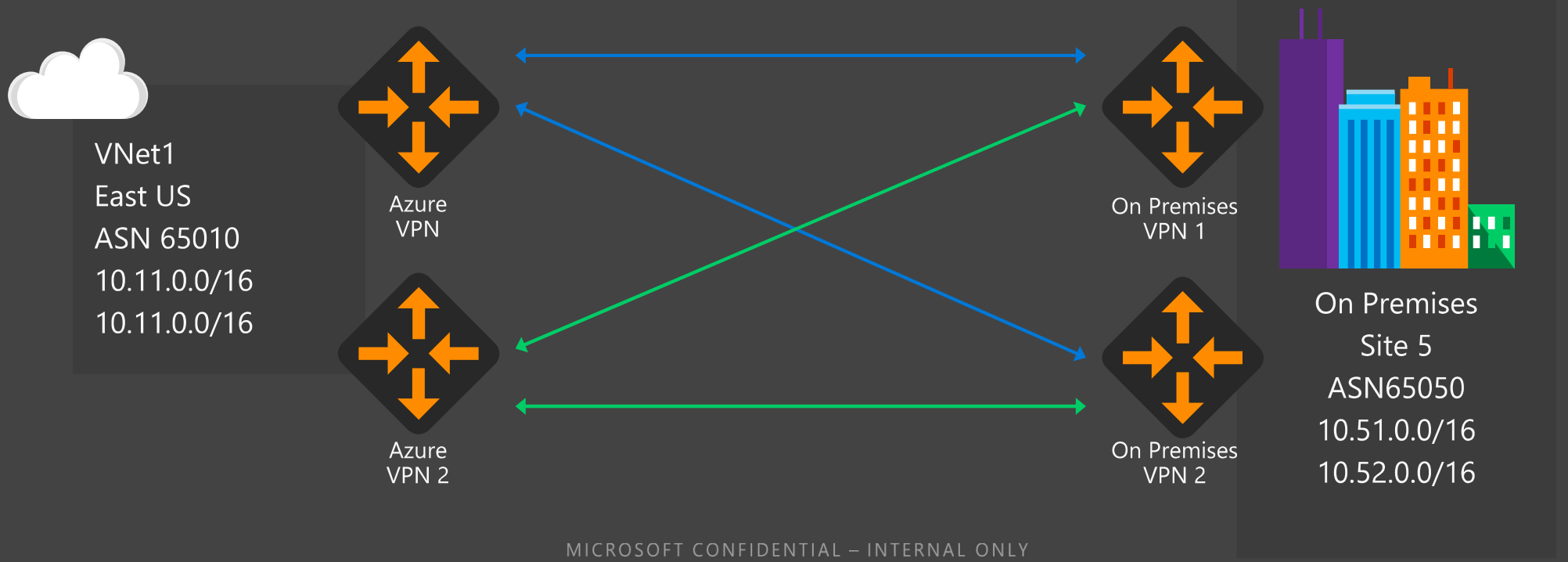


MICROSOFT CONFIDENTIAL – INTERNAL ONLY

Active-active for dual redundancy

Zero downtime during planned maintenance

From active-standby to active-active
Support both cross-premises and VNet-to-VNet connectivity
Spreading traffic over multiple tunnels simultaneously

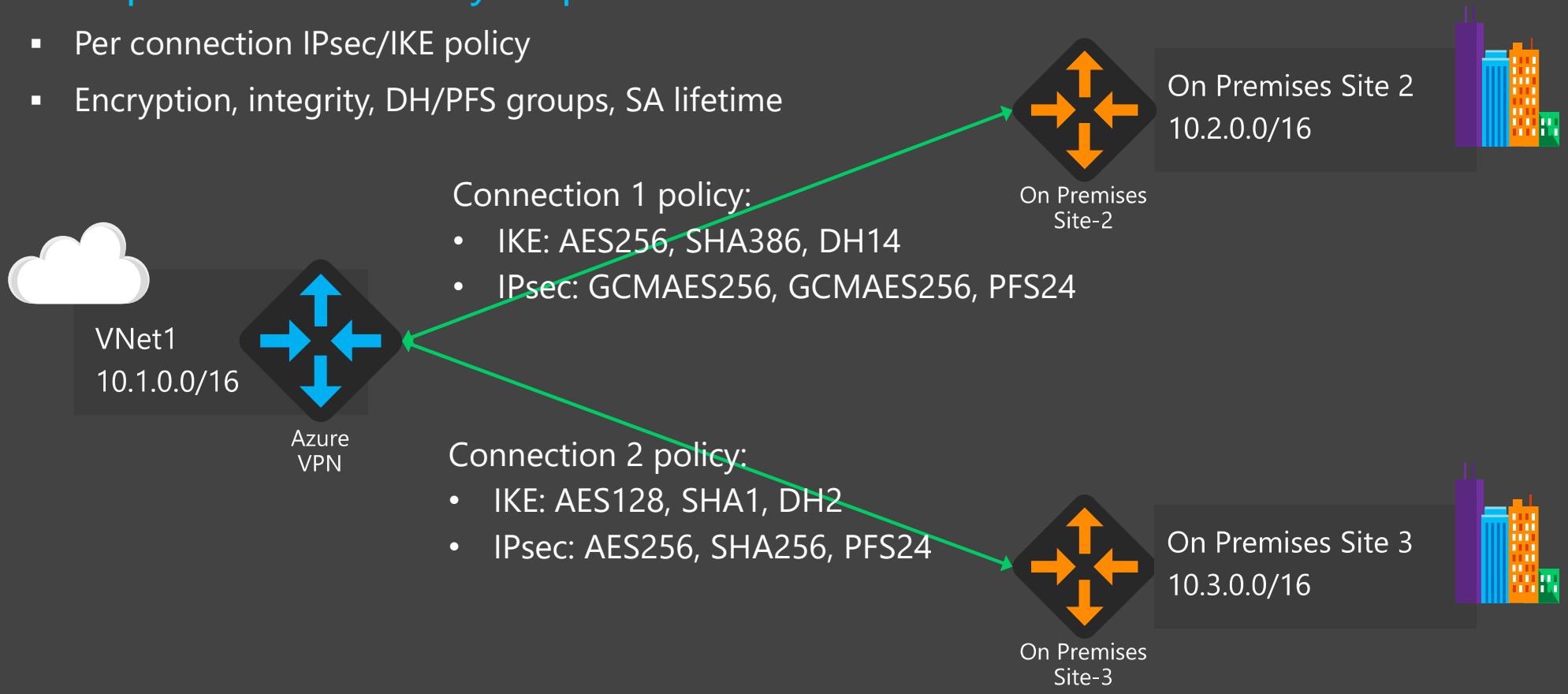


MICROSOFT CONFIDENTIAL – INTERNAL ONLY

Configurable IPsec/IKE Policy

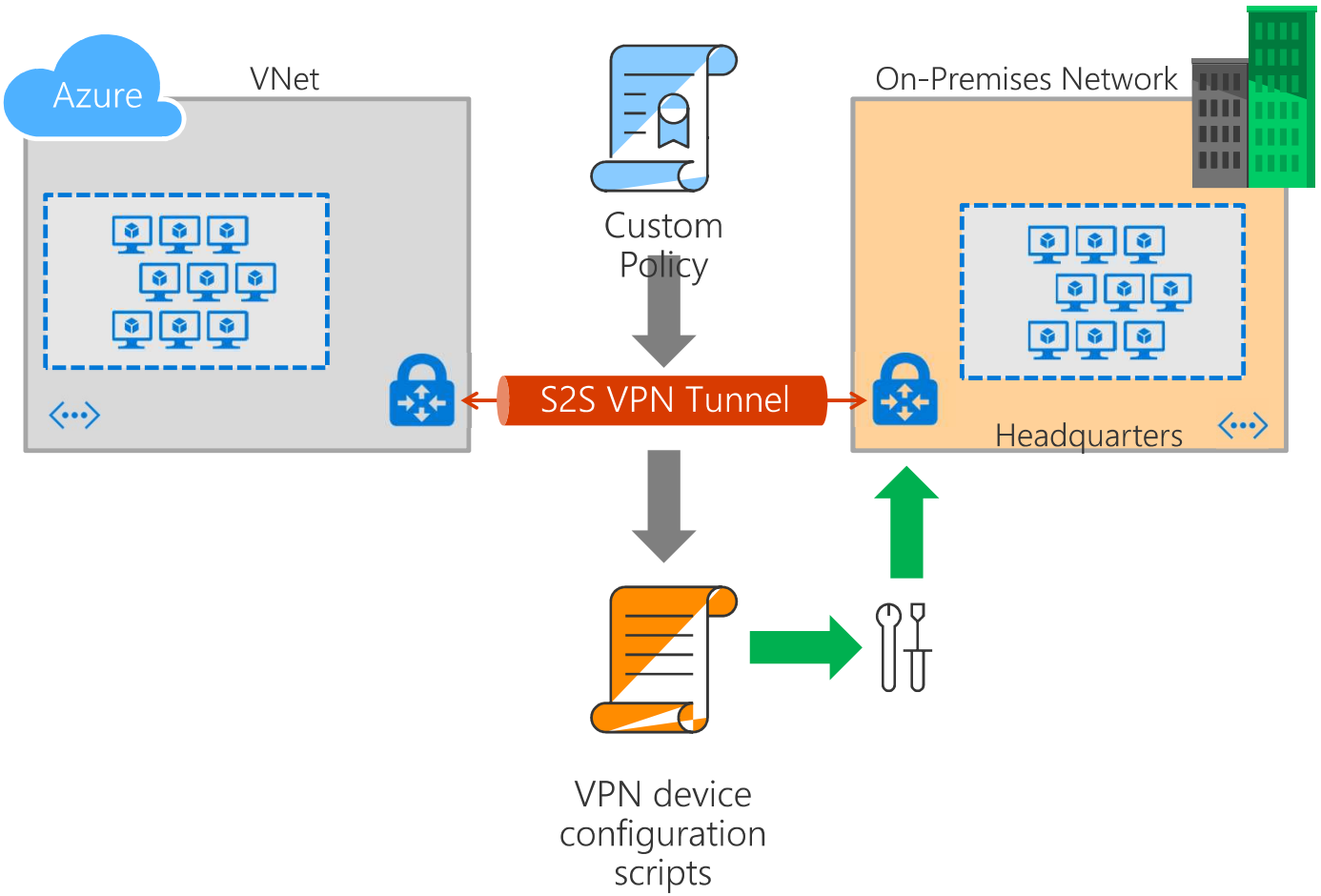
Compliance & security requirements

- Per connection IPsec/IKE policy
- Encryption, integrity, DH/PFS groups, SA lifetime



MICROSOFT CONFIDENTIAL – INTERNAL ONLY

Configure On-Premises VPN devices

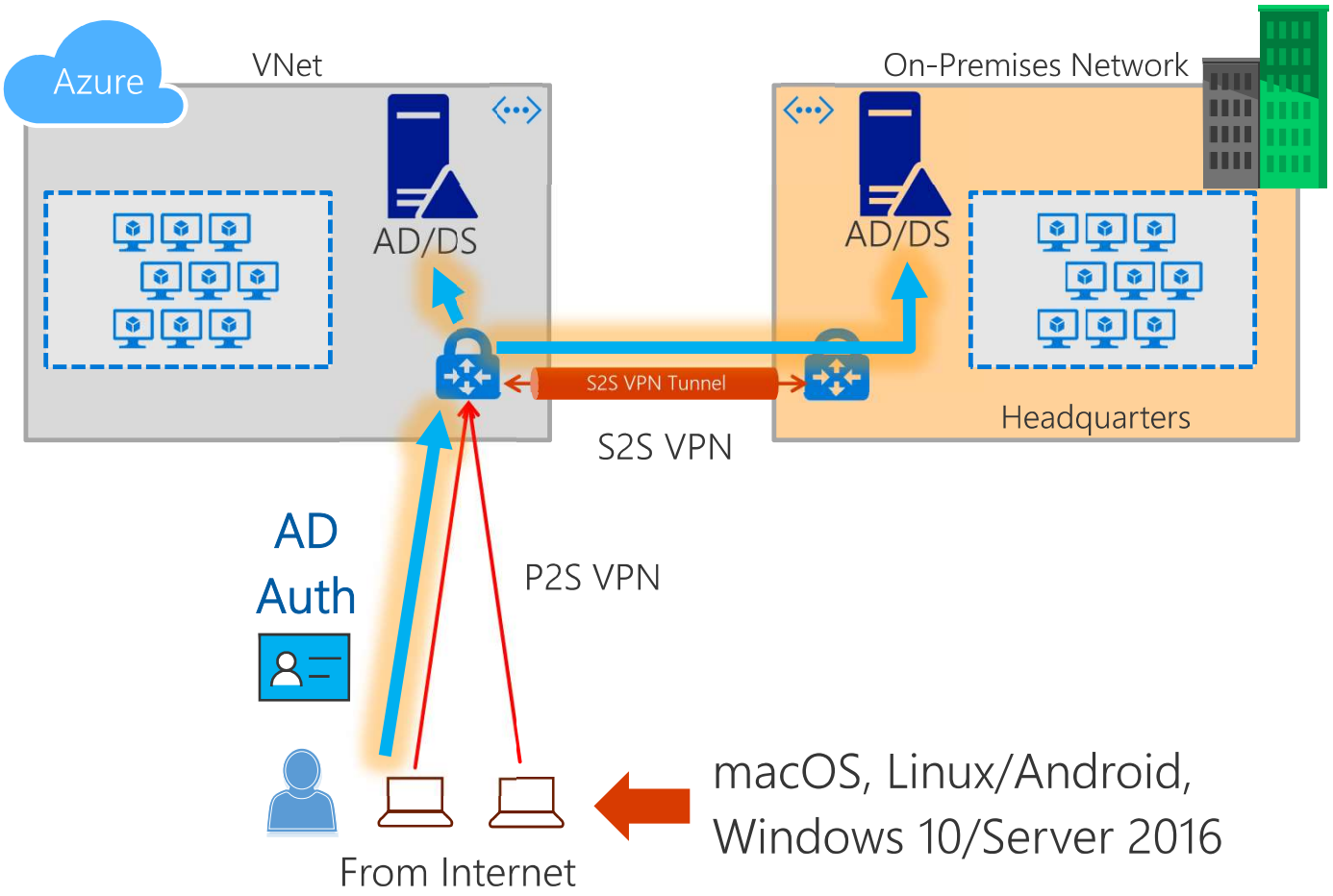


S2S VPN

- Apply custom IPsec/IKE policy for compliance (encryption/integrity, PFS, DH)
- Download VPN device scripts for seamless configurations

P2S VPN for Remote Access

P2S VPN with AD authentication



P2S VPN

- P2S VPN for mobile users & developers to connect from anywhere
- Now supporting macOS, Linux, and Windows
- AD/Radius authentication for enterprise grade identity solution

Large scale, multi-platform P2S VPN

- Roadmap – 8x P2S VPN connections

SKU	P2S – IKEv2*	P2S – SSTP	S2S/V2V	Throughput
VpnGw3	**1,000**	128	Max. 30	1.25Gbps
VpnGw2	**500**	128	Max. 30	1.00Gbps
VpnGw1	**250**	128	Max. 30	650Mbps
Basic	N/A	128	Max. 10	100Mbps

- Active-active allows bursting up to 2x P2S connections (2000, 1000, 500)

P2S with IKEv2

- Windows 10 & Windows Server 2016*
- Linux & Android via StrongSwan
- Mac (macOS 10.12 and higher)

Radius/AD authentication

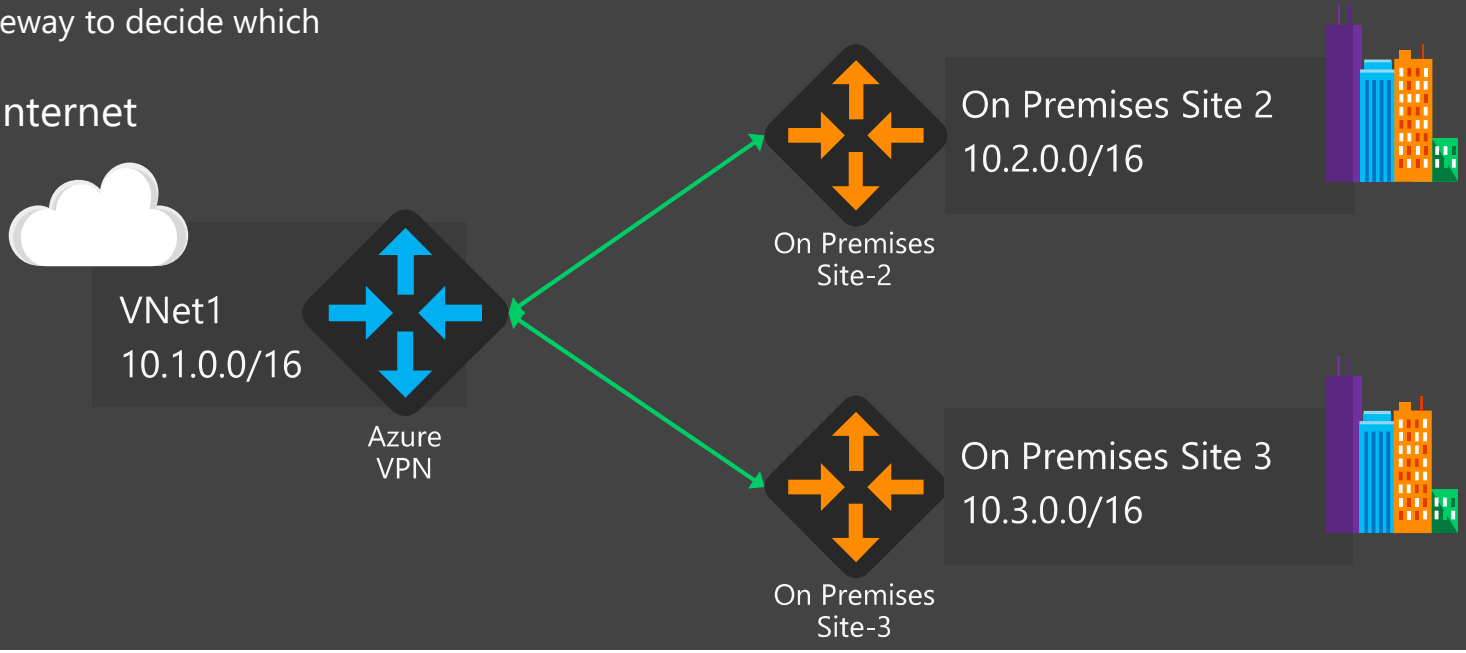
- Username/password
- Certificate-based (EAP-TLS)
- MFA via NPS extension + Azure MFA**

Routing in Azure

Azure Routing 101

Routing & forwarding

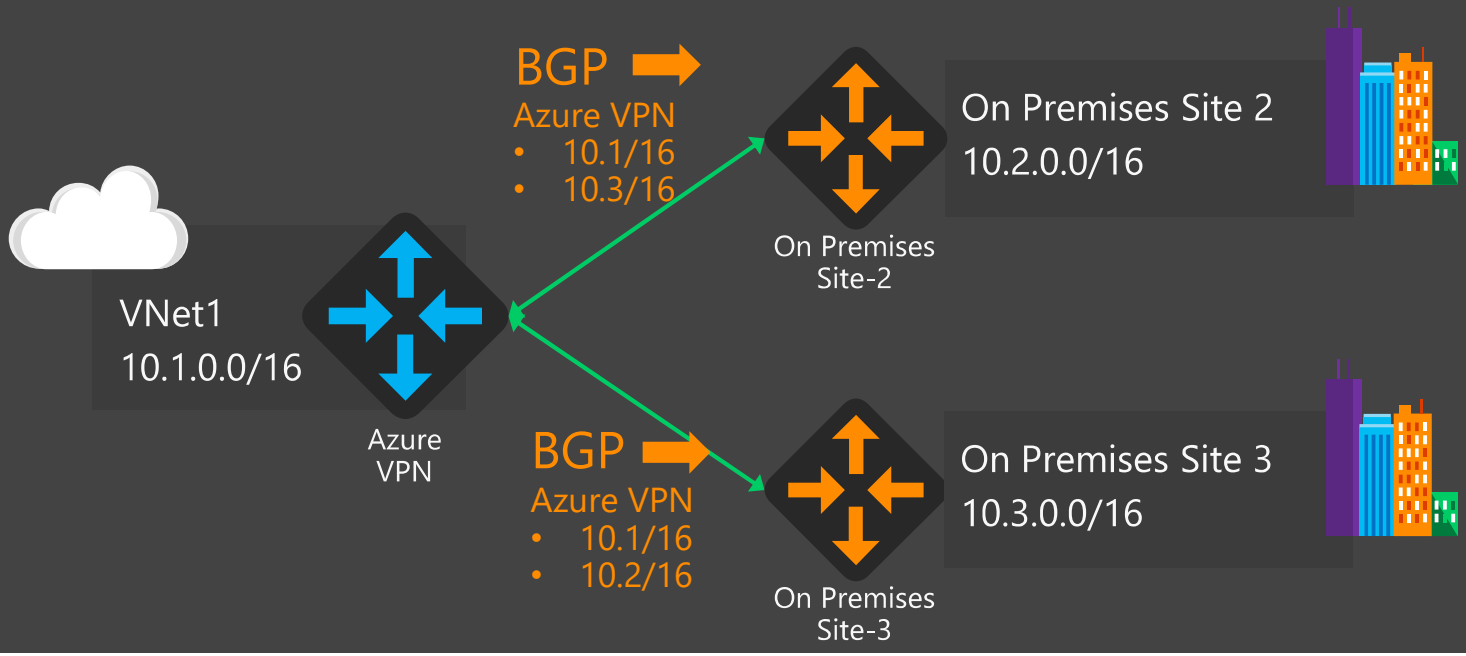
- Based on destination (IP), decide where (nexthop) to send a packet
  - Longest prefix match – the most specific route wins
  - 10.0.0.0/**16** vs. 10.0.0.0/**24**
- Intra VNet – send directly among VNet VMs
- Cross-premises – nexthop Azure VPN gateway
  - Same routing lookup in VPN gateway to decide which IPsec tunnel to send the packet
- Default route (0.0.0.0/0) ➔ Internet



Azure Routing 102

BGP (Border Gateway Protocol) & gateway routes

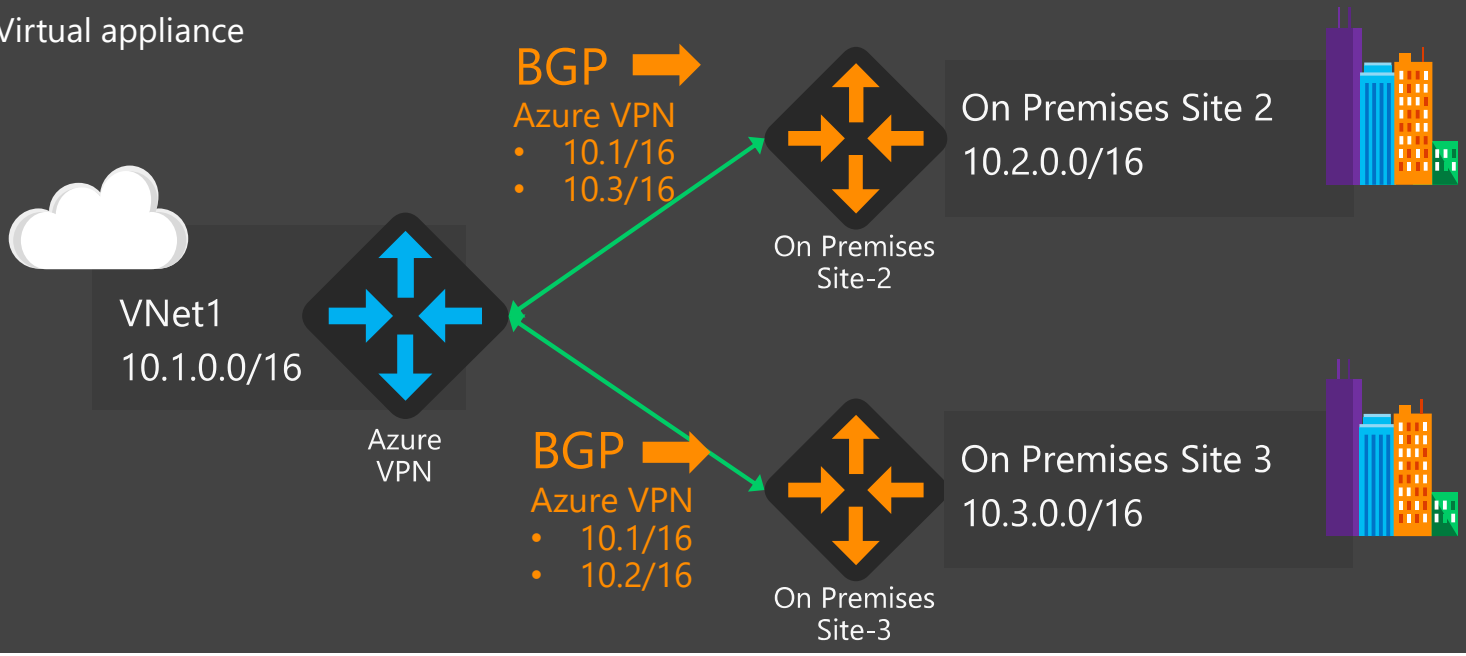
- Dynamic routing – allows gateways to exchange routes dynamically, and propagate to all other connected gateways
- Can be overridden by static (manual) routes
- VPN & ExpressRoute gateway will "**inject**" routes to the entire virtual network
  - Can be disabled by Routing Table option "Disable BGP route propagation" on individual subnets



Azure Routing 103

UDR – User-Defined Routes

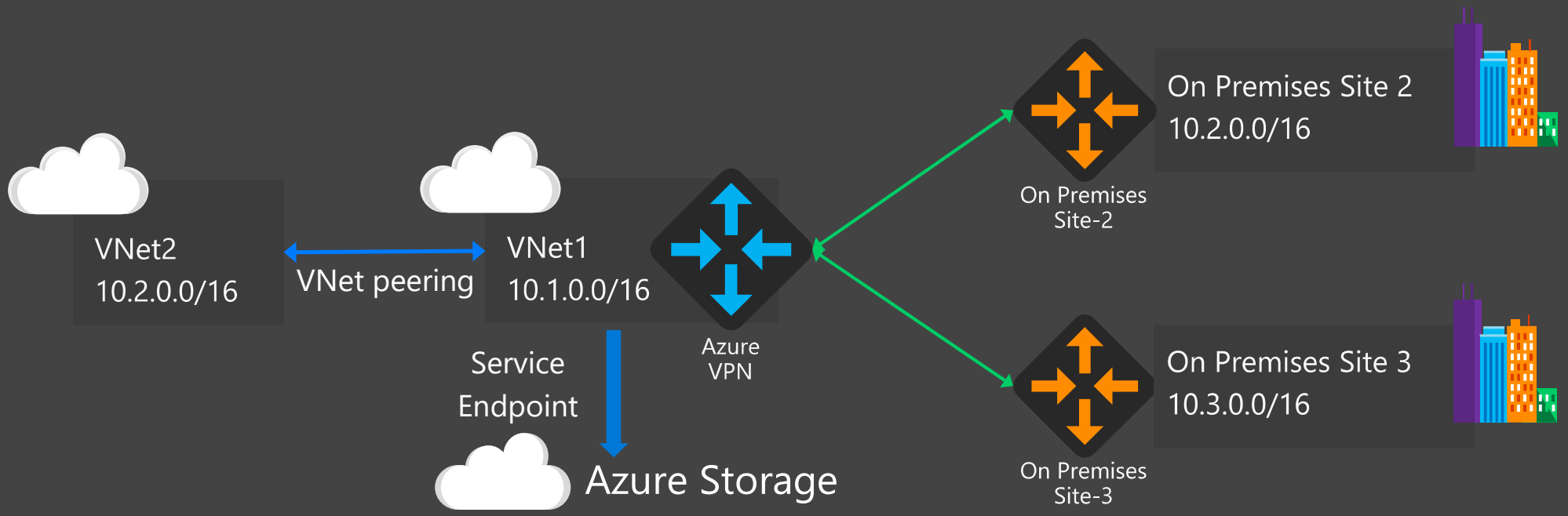
- Manual/static routes added to a subnet
- Overrides BGP/dynamic routes and system default in **tie breaker**
  - Longest prefix match still wins (e.g., 10.100.0.0/**24**)
  - Routes for the same destination AND prefix
  - ( ) Dynamic 10.100.0.0/16 ➔ Azure VPN gateway
  - (√) UDR 10.100.0.0/16 ➔ Virtual appliance



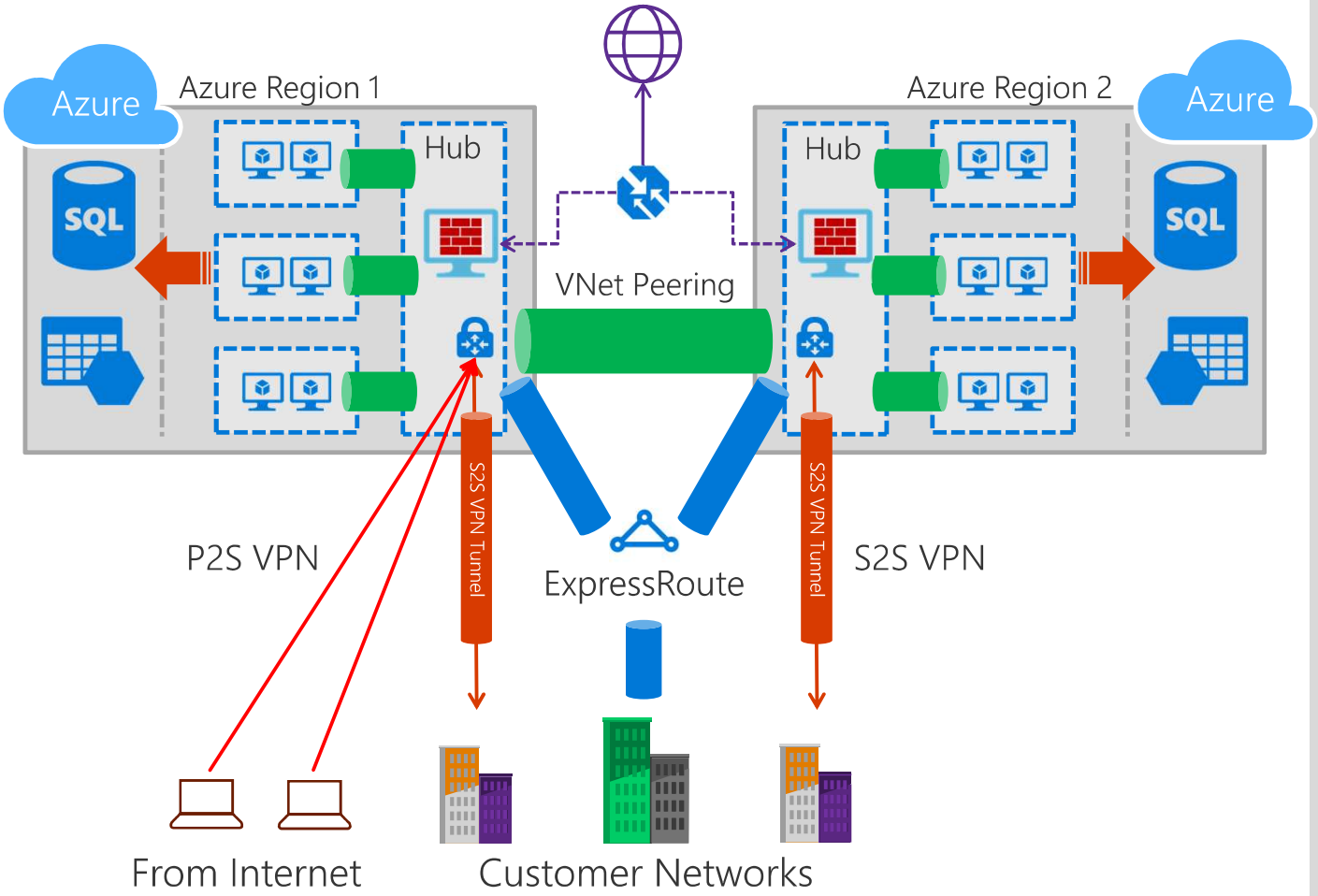
Azure Routing 104

System routes – "Effective routes"

- System default – (1) Intra-VNet ➔ direct; (2) Default route ➔ Internet
- VNet injected routes into UDR
  - VNet peering ➔ Adding peered VNet prefixes (e.g.,10.20.0.0/16) ➔ VNet peering
  - Service endpoints ➔ Adding public IP address(es) for a service (e.g., Azure storage) ➔ Service Endpoint



Azure Routing 400



Can a hub talk to another hub?

- VNet Peering, ExpressRoute, or VPN?

Can a spoke talk to another spoke in the same hub?

Can a spoke talk to another spoke in a different hub?

- Global VNet Peering, ExpressRoute, or VPN?

Would Service Endpoint access get forced tunneled?

Would BGP advertised peered VNets prefixes to on-premises?

Would it take ExpressRoute or VPN to the on-premises networks?

- Multiple ExpressRoute circuits?
- Co-existence?
- VPN Active-active?

Can P2S connect to on-premises?

How do I know which route to take?

LPM (Longest Prefix Match) rules!

- Routes with the longest prefix match of the destination will be taken
- LPM == "more specific route"
- 10.0.0.0/24 is more specific then 10.0.0.0/16

Tie breaker – Static >> BGP >> System

1. Static routes
   - User-defined routes
   - Service endpoints*
   - VNet peering*
   - (*) Added by the system in UDR, but you can add routes to override
2. BGP / Gateway routes
   - BGP routes advertised via ExpressRoute or VPN ➔ Inject into the whole VNet
   - VPN gateway static routes
3. System routes
   - Intra-VNet direct & default to Internet

Hub-and-Spoke routing

- Prefer VNet peering over ExpressRoute or VPN VNet-to-VNet
- Prefer VNet Service Endpoints (Storage & SQL) over BGP routes (forced tunneling)
- Prefer ExpressRoute over VPN in co-existence scenarios
- Prefer ExpressRoute connections with higher connection weight
- Prefer "shortest" path – honor AS prepending
- Spoke-to-spoke in one hub is NOT connected by default – VNet peering is non-transitive
- Spoke-to-spoke between two hubs works through gateway transit

How do I control which route to take?

ECMP – Equal-Cost, Multi-Path

- "When in doubt, spread …"
- Multiple paths (nexthops) to the same destination
  - Two UDR routes to different virtual appliances
  - Active-active VPN gateway
  - Multipath topology via BGP routing
- Spreading is on "flows"
  - Packets of one flow always follow the same path (gateways, tunnels)
  - Flow - 5-tuple (TCP/UDP)

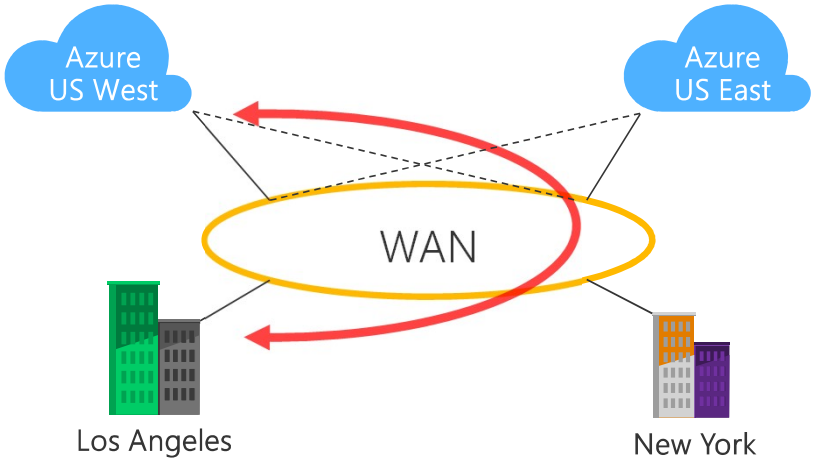
Prefer one path over the others

- MUST be done on BOTH ends
  - Prevent asymmetric routing
- Azure ➔ on-premises network
  - AS-prepending – create longer AS paths for certain routes
  - Azure gateways will favor or prefer routes with shorter AS paths
  - ExpressRoute connection weight – prefer connections with higher weights
  - Apply higher connection weights to the closer ExpressRoute circuits
- On-premises network ➔ Azure
  - Local preference

Common routing problems

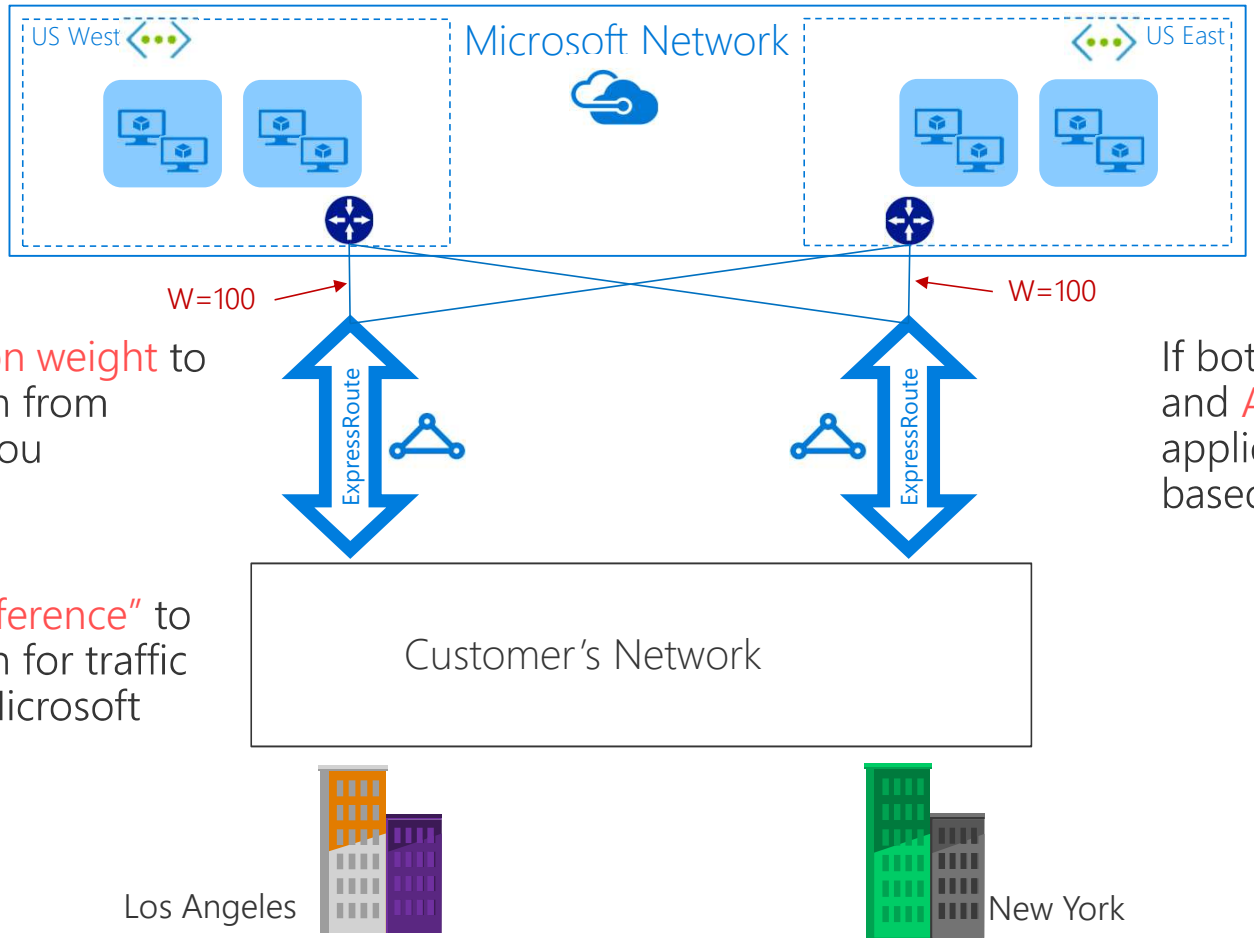
- Forced tunneling
  - Everything goes back to on-premises for inspection/auditing
  - Compliance requirement for most enterprises
  - Breaks Internet-facing VMs
    - Internet ➔ VM public IP: 128➔151
    - VM ➔ on-premises proxy / NAT ➔ Internet: 181➔128
  - Breaks first party "VNet injection" services
    - Azure App Service Environment (ASE)
    - VPN/ExpressRoute gateways
- On-premises networks to Azure PaaS
  - ExpressRoute Microsoft peering only
- On-premises networks to Service Endpoints
  - No (*)

- (Sub-) Optimal routing



- Asymmetric routing
  - Two paths to MS (O365)
    - Internet & ExpressRoute
  - O365 reaches corp via Internet
  - Response goes through ExpressRoute

Connection weight and BGP attributes



Use connection weight to select the path from Microsoft to you

Use "local preference" to select the path for traffic from you to Microsoft

If both connection weight and AS-path prepending are applied, path is selected based on the former

Roadmap

Roadmap

Security

DDoS Protection GA

VNet Service Endpoints for SQL and Storage GA

- Cosmos DB, Key Vault, ADLS coming soon

Application Security Groups GA

Application Gateway and WAF enhancements

Monitoring

Azure Monitor—Network metrics and diagnostics

Resource Health Check for network resources

Network Watcher—Flow log analytics, connectivity checker

Traffic Manager—Traffic View, Real User Measurements

Connectivity

Global VNet Peering GA

ExpressRoute – BFD, higher bandwidth

S2S – higher throughput, more tunnels

P2S – higher scale, AAD authentication

Performance

Accelerated Networking for more VM SKUs

30 Gbps VM to VM bandwidth world's fastest

DPDK partner enablement

Availability

New Azure Standard Load Balancer GA

Internal Load Balancer HA Ports GA

Managed NAT

Additional Resources

- Azure Networking documentation
- https://docs.microsoft.com/en-us/azure/#pivot=products&panel=network
- Networking overview
- https://docs.microsoft.com/en-us/azure/networking/networking-overview
- Intelligent Cloud resource
- Internal Microsoft FTE's: http://aka.ms/icpst

INTELLIGENT CLOUD ARCHITECT BOOT CAMP

Session Objectives & key takeaways

At the end of this session you will be better able to

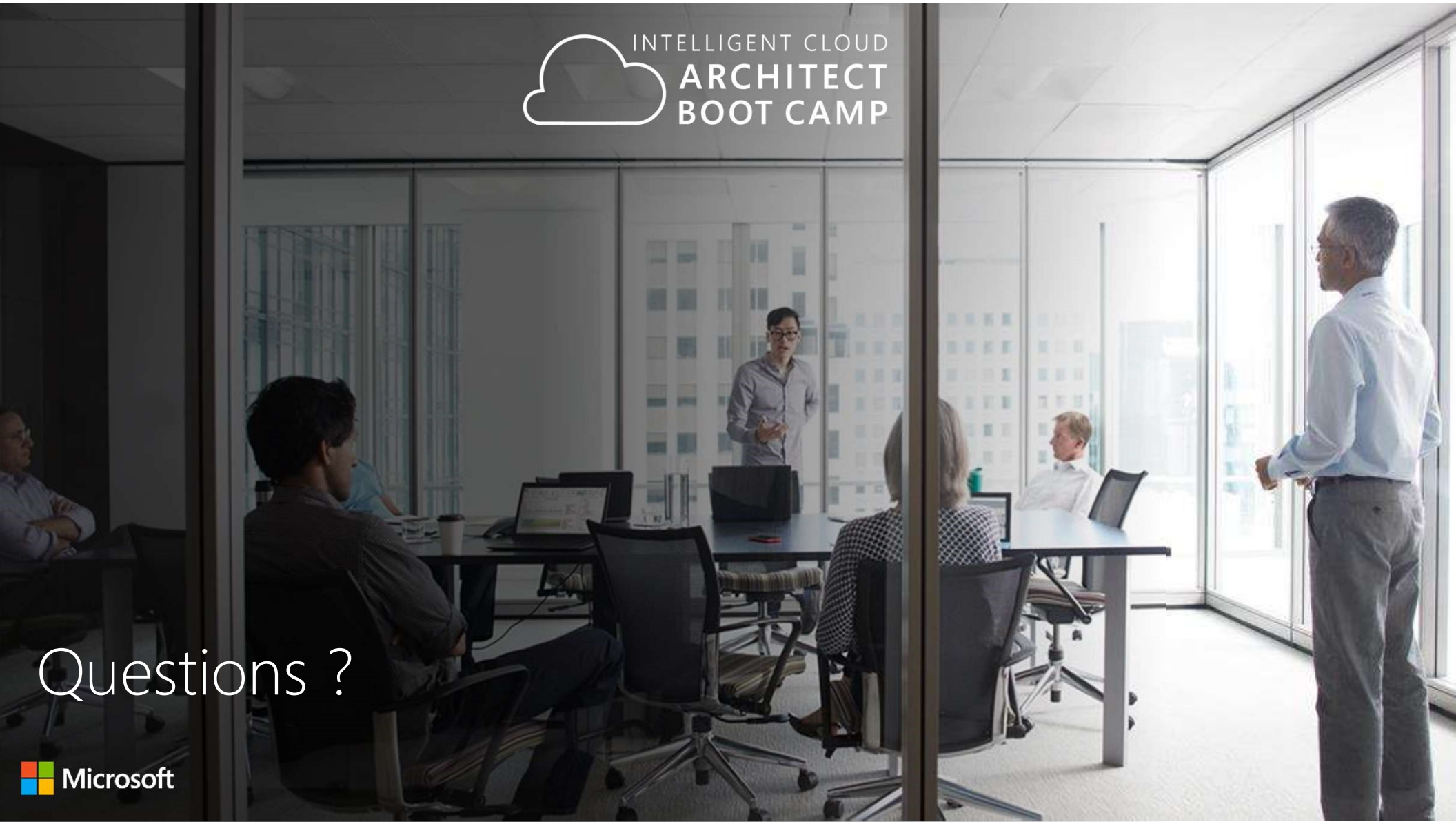
- decide which cross-premises connectivity options for your customers
- base on architecture, topology, security, and performance requirements
- understand routing between on-premises and clouds, across the clouds, and within the clouds

Enjoy a session

Fill out an evaluation

Make Boot Camp better

Please remember to complete your evaluations!


INTELLIGENT CLOUD
ARCHITECT
BOOT CAMP
Questions ?
Microsoft

© Copyright Microsoft Corporation. All rights reserved.