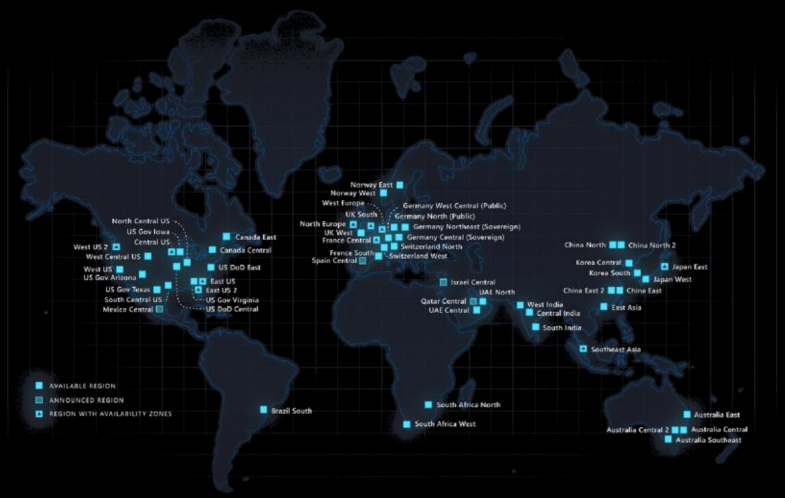
Azure Networking

Microsoft

30th June 2020

Global



60+ Azure regions

Largest geographical footprint of any cloud provider with more than **60** Azure regions

Secure

Microsoft Cyber Defense Operations Center

>3,500 full-time security professionals

6.5 trillion global signals daily

$1 billion annual cybersecurity investment

Compliant

90+ Compliance offerings

GLOBAL

- ISO 27001:2013
- ISO 27017:2015
- ISO 27018:2014
- ISO 22301:2012
- ISO 9001:2015
- ISO 20000-1:2011
- SOC 1 Type 2
- SOC 2 Type 2
- SOC 3
- CIS Benchmark
- CSA STAR Certification
- CSA STAR Attestation
- CSA STAR Self-Assessment
- WCAG 2.0 (ISO 40500:2012)

U.S. GOVT

- FedRAMP High
- FedRAMP Moderate
- EAR
- ITAR
- DoD DISA SRG Level 5
- DoD DISA SRG Level 4
- DoD DISA SRG Level 2
- DFARS
- DoE 10 CFR Part 810
- NIST SP 800-171
- NIST CSF
- Section 508 VPATs
- FIPS 140-2
- CJIS
- IRS 1075
- CNSSI 1253

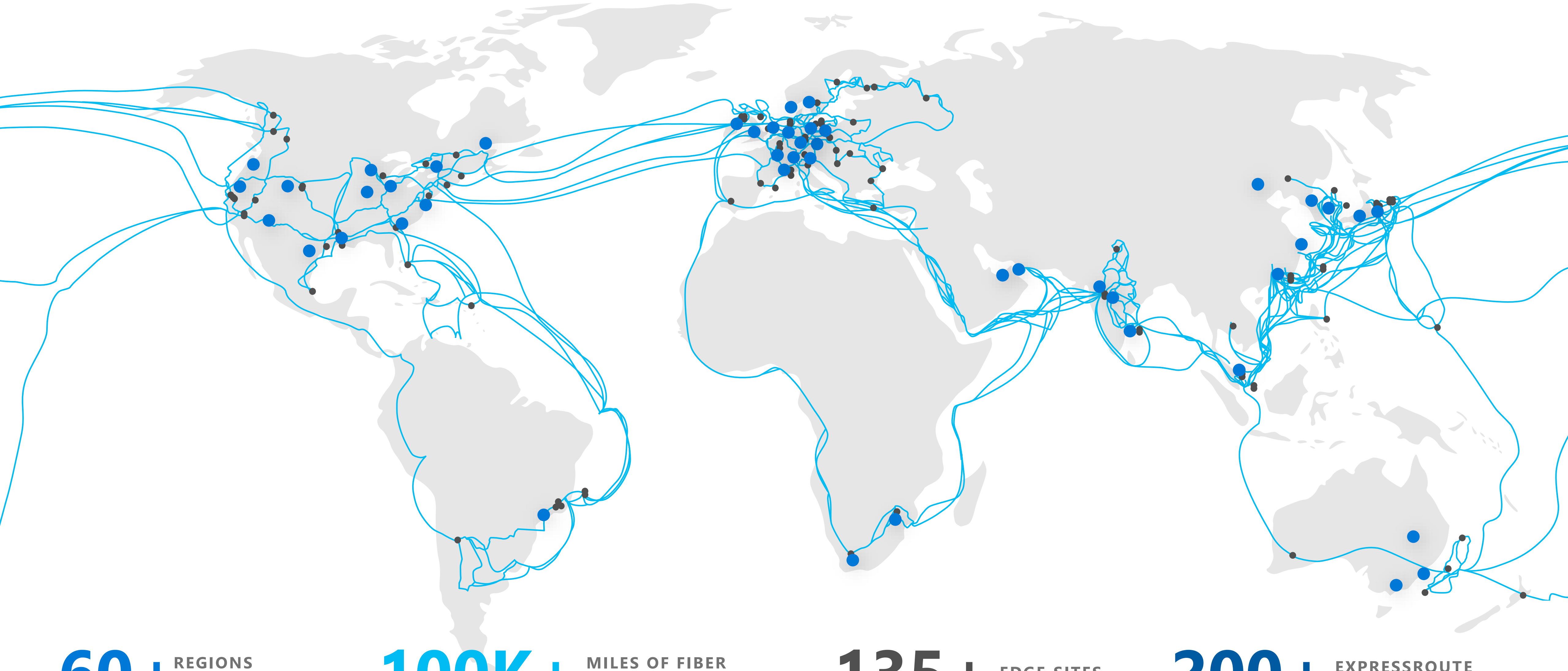
INDUSTRY

- PCI DSS Level 1
- GLBA (US)
- FFIEC (US)
- Shared Assessments (US)
- SEC 17a-4 (US)
- CFTC 1.31 (US)
- FINRA 4511 (US)
- SOX (US)
- 23 NYCRR 500 (US)
- OSFI (Canada)
- FCA + PRA (UK)
- APRA (Australia)
- FINMA (Switzerland)
- FSA (Denmark)
- RBI + IRDAI (India)
- MAS + ABS (Singapore)
- NBB + FSMA (Belgium)
- AFM + DNB (Netherlands)
- AMF + ACPR (France)
- KNF (Poland)
- European Banking Authority (EBA)
- FISC (Japan)
- HIPAA BAA (US)
- HITRUST Certification
- GxP (FDA 21 CFR Part 11)
- MARS-E (US)
- NHS IG Toolkit (UK)
- NEN 7510:2011 (Netherlands)
- FERPA (US)
- CDSA
- MPAA (US)
- FACT (UK)
- DPP (UK)

REGIONAL

- Argentina PDPA
- Australia IRAP Unclassified
- Australia IRAP PROTECTED
- Canada Privacy Laws
- China GB 18030:2005
- China DJCP (MLPS) Level 3
- China TRUCS / CCCPPF
- EU EN 301 549
- EU ENISA IAF
- EU Model Clauses
- EU – US Privacy Shield
- GDPR
- Germany C5
- Germany IT-Grundschutz workbook
- India MeitY
- Japan CS Mark Gold
- Japan My Number Act
- Netherlands BIR 2012
- New Zealand Gov CIO Framework
- Singapore MTCS Level 3
- Spain ENS High
- Spain DPA
- UK Cyber Essentials Plus
- UK G-Cloud
- UK PASF

Gain global scale with local presence



60+ REGIONS WORLDWIDE

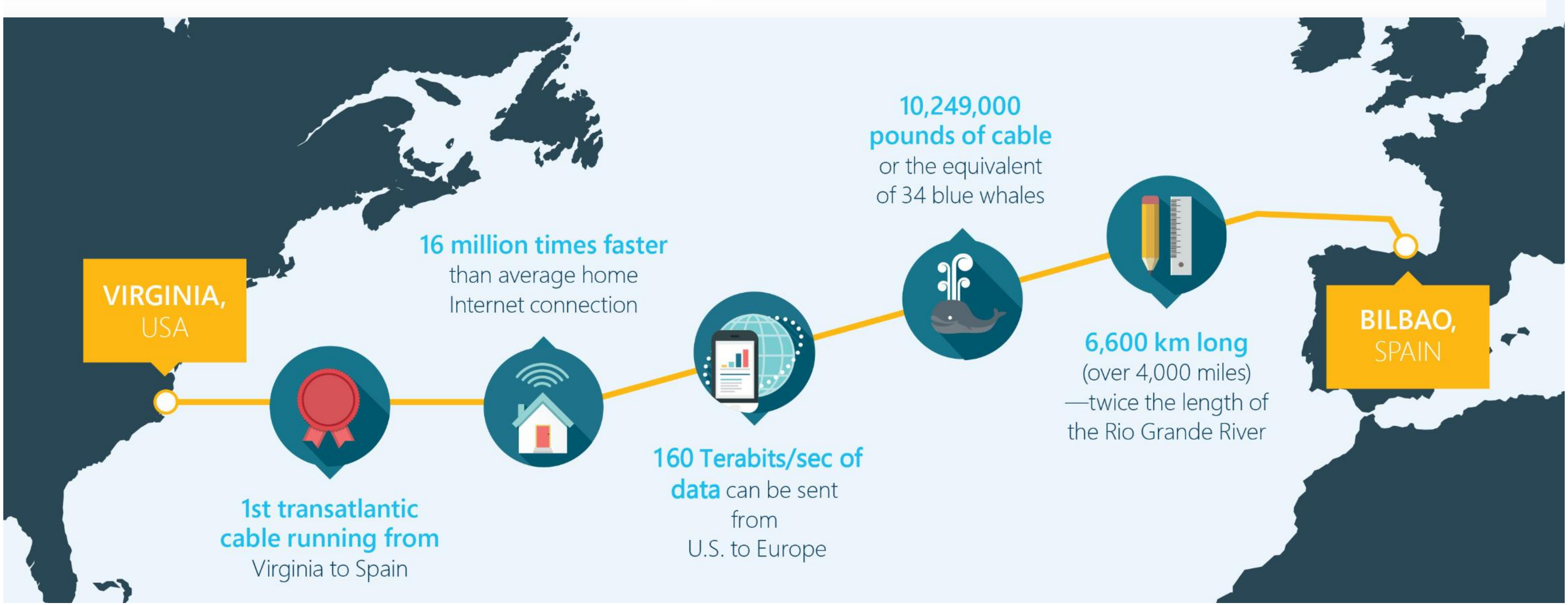
100K+ MILES OF FIBER AND SUBSEA CABLE

135+ EDGE SITES

200+ EXPRESSROUTE PARTNERS

MAREA TRANSATLANTIC SUBSEA CABLE

Faster. Stronger. More Resilient.



VIRGINIA, USA

1st transatlantic cable running from Virginia to Spain

16 million times faster than average home Internet connection

160 Terabits/sec of data can be sent from U.S. to Europe

10,249,000 pounds of cable or the equivalent of 34 blue whales

6,600 km long (over 4,000 miles) —twice the length of the Rio Grande River

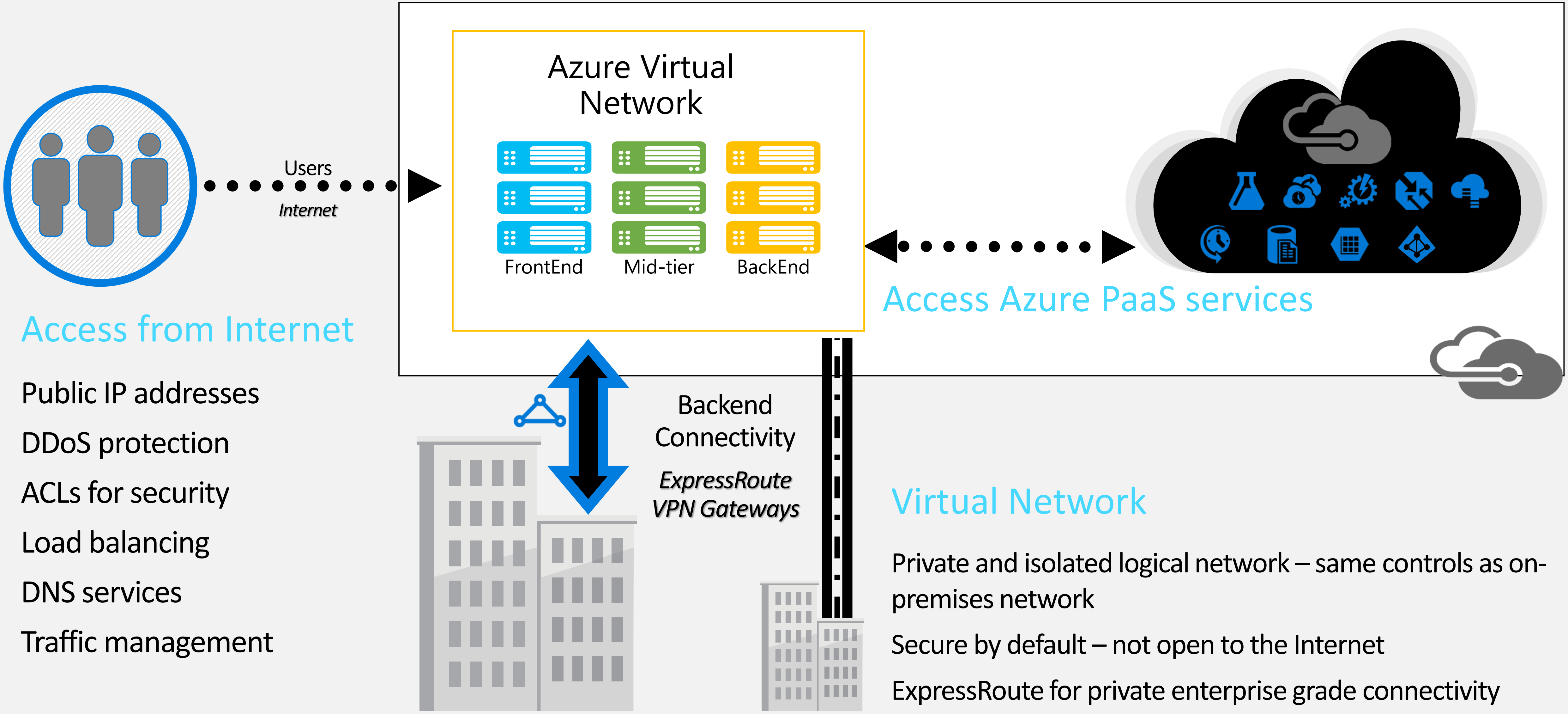
BILBAO, SPAIN

Microsoft TELXIUS facebook

Microsoft

Azure Virtual Network - Concepts

Network – The Big Picture



Access from Internet

Public IP addresses

DDoS protection

ACLs for security

Load balancing

DNS services

Traffic management

Access Azure PaaS services

Virtual Network

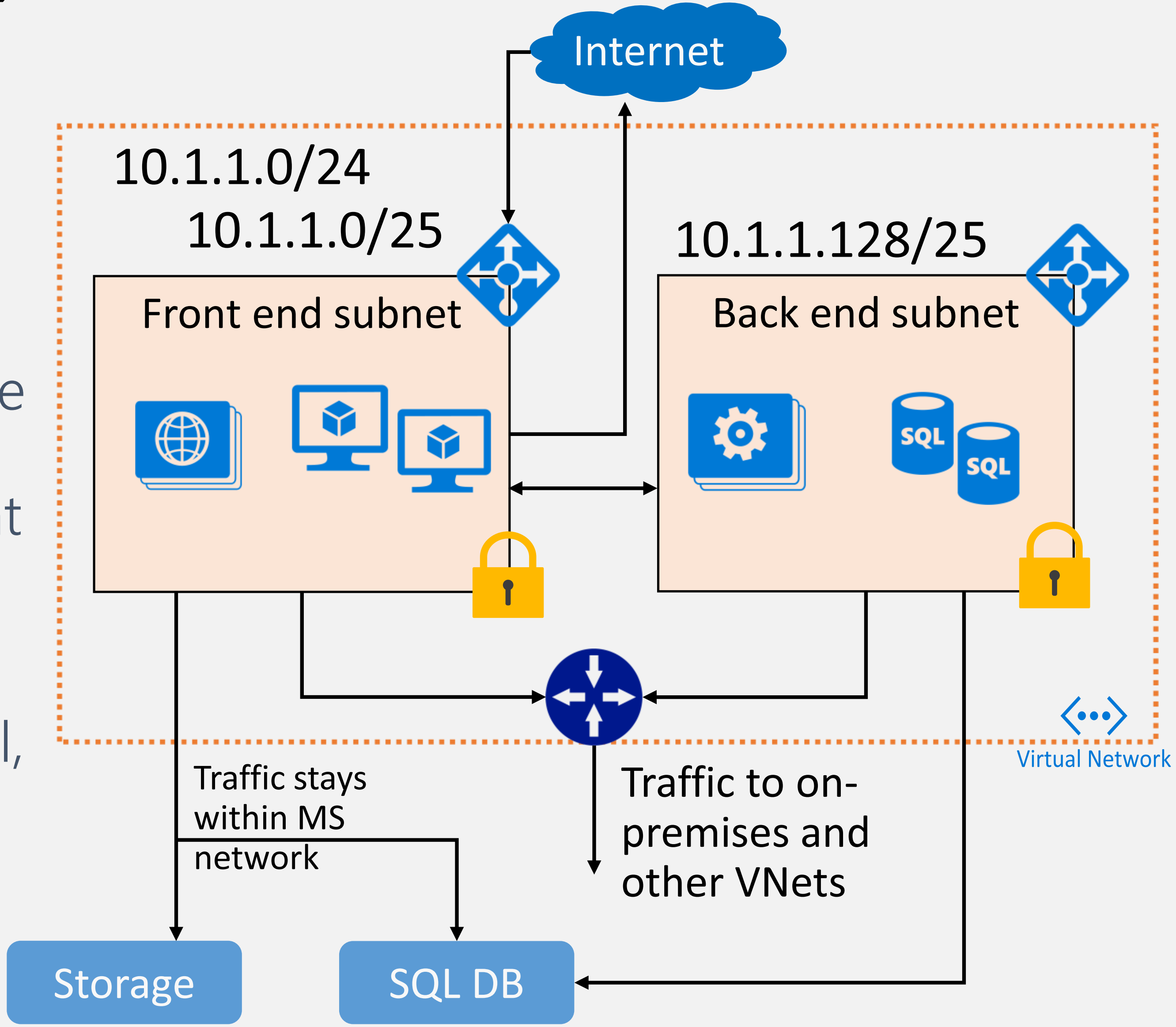
Private and isolated logical network – same controls as on-premises network

Secure by default – not open to the Internet

ExpressRoute for private enterprise grade connectivity

Virtual Network (VNet)

- ✓ Logical isolation of the public cloud
- ✓ “Bring your own” network
- ✓ Public or Private (RFC1918) address space
- ✓ Address space only reachable within that VNet and connected networks
- ✓ Network Security through NSGs, Firewall, NVAs



Network Security Groups (NSG)

✓ Enables network segmentation

✓ Provides Layer 3 or Layer 4 filtering

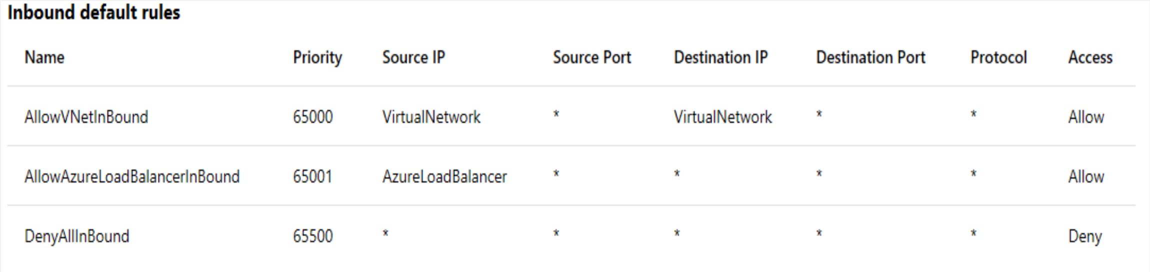
✓ Eases IP Management for Firewall rules

✓ Associate with VMs or subnets

✓ Access Control List

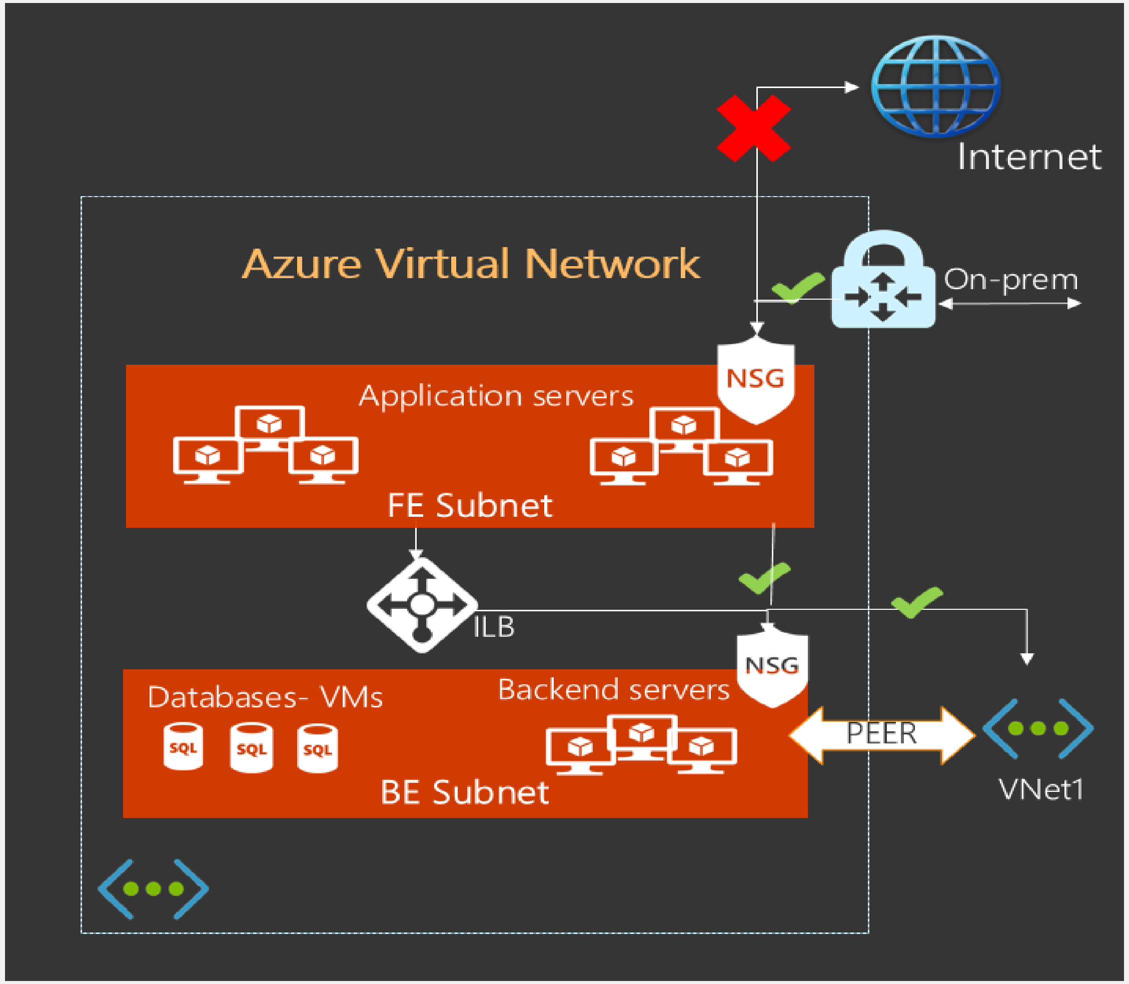
- Filter conditions with allow/deny
- Individual addresses, address prefixes, wildcards

✓ Sample NSG



Inbound default rules

Name	Priority	Source IP	Source Port	Destination IP	Destination Port	Protocol	Access
AllowVNetInBound	65000	VirtualNetwork	*	VirtualNetwork	*	*	Allow
AllowAzureLoadBalancerInBound	65001	AzureLoadBalancer	*	*	*	*	Allow
DenyAllInBound	65500	*	*	*	*	*	Deny

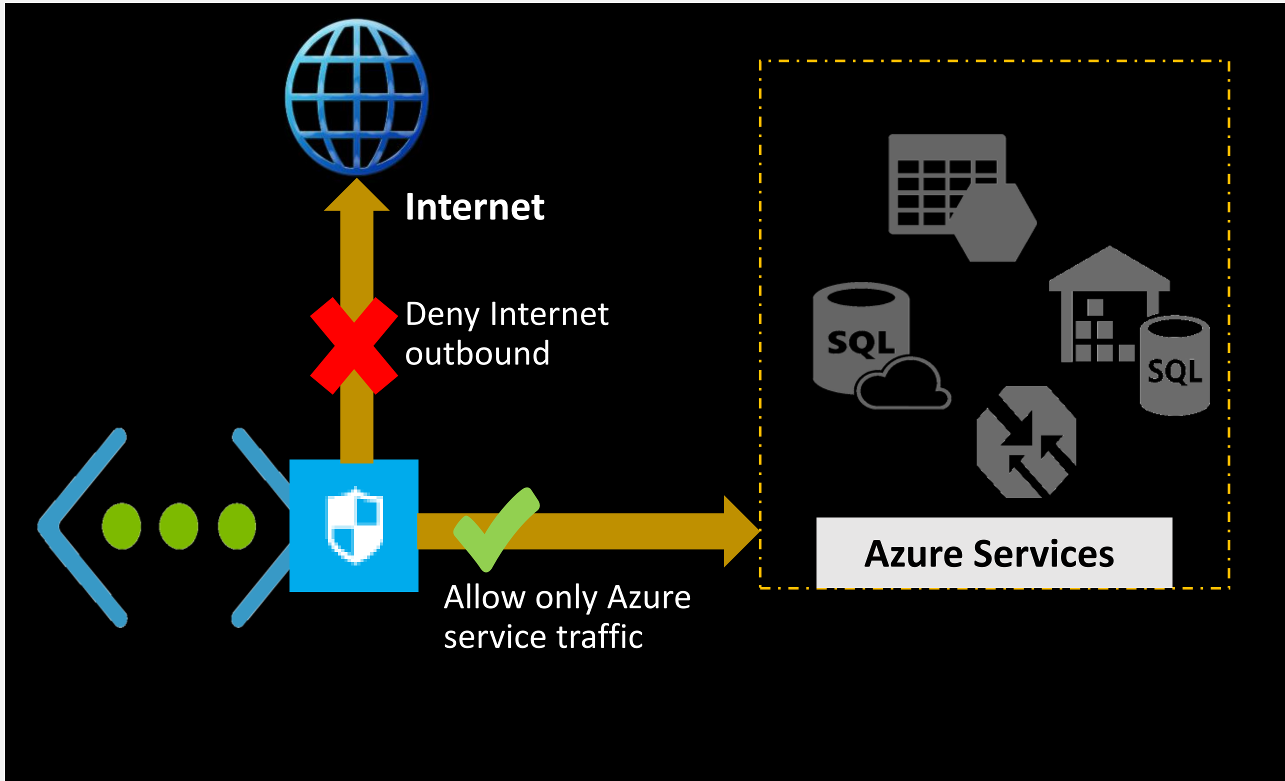


NSGs: Service Tags

✓ Restrict network access to just the Azure services you use.

✓ Maintenance of IP addresses for each tag provided by Azure

✓ Support for global and regional tags (varies by service)

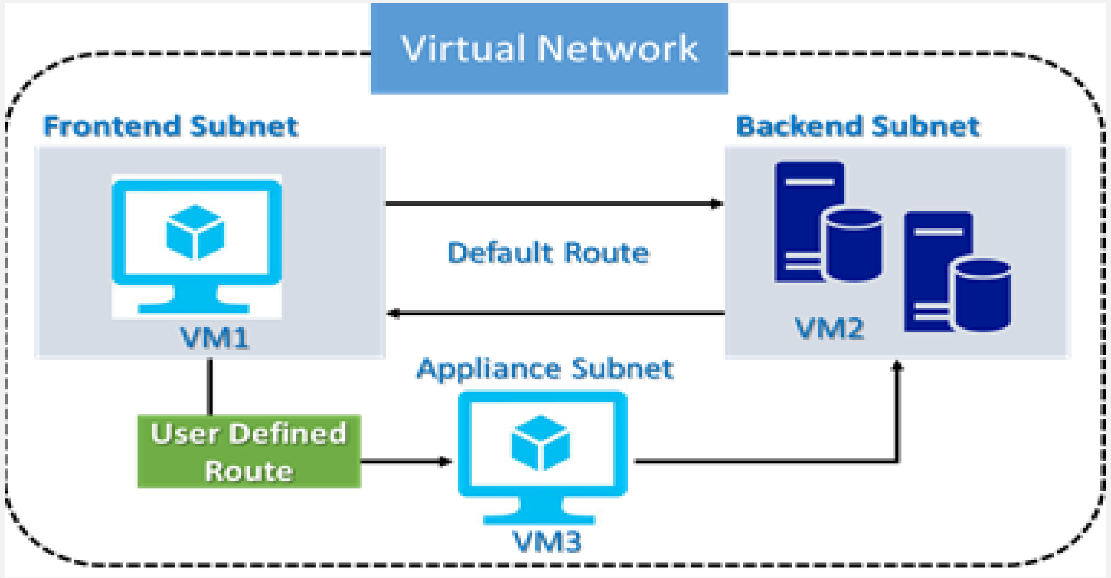


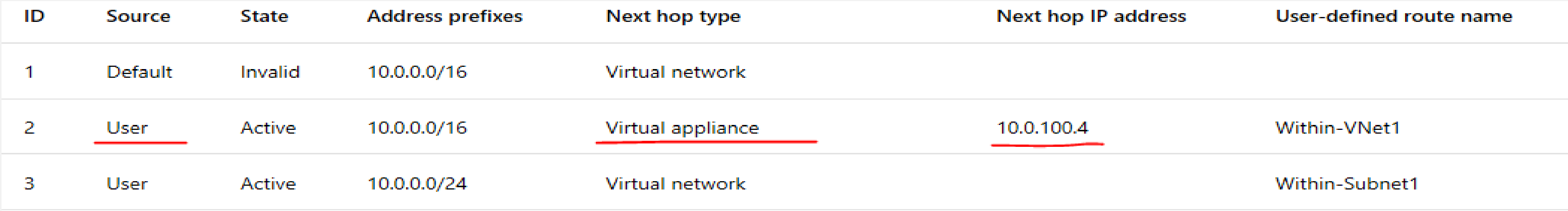
Network Security Group (NSG)

Action	Name	Source	Destination	Port
Allow	AllowStorage	VirtualNetwork	**Storage**	Any
Allow	AllowSQL	VirtualNetwork	**Sql.EastUS**	Any
Deny	DenyAllOutBound	Any	Any	Any

User Defined Routes (UDR)

- ✓ User Defined Custom Routes
- ✓ Override Default Routes or add additional routes to subnet
- ✓ Route traffic to Virtual Appliances, VPN Gateways, Internet and so on

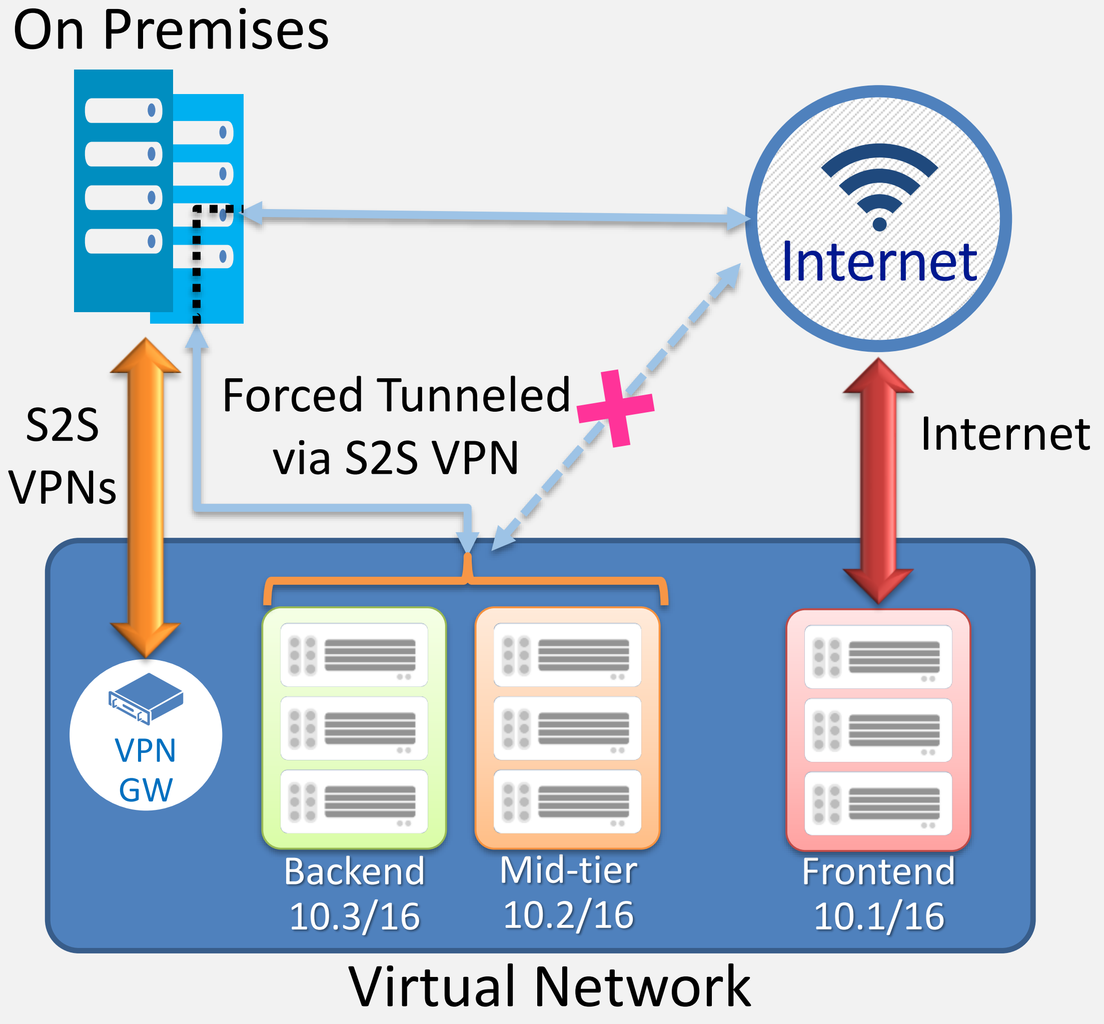




ID	Source	State	Address prefixes	Next hop type	Next hop IP address	User-defined route name
1	Default	Invalid	10.0.0.0/16	Virtual network		
2	User	Active	10.0.0.0/16	Virtual appliance	10.0.100.4	Within-VNet1
3	User	Active	10.0.0.0/24	Virtual network		Within-Subnet1

Auditing Internet Traffic/Routes

- ✓ "Force" or redirect customer Internet-bound traffic to an on-premises site
- ✓ Auditing & inspecting outbound traffic from Azure
- ✓ Needed by many scenarios for critical security and IT policy requirements

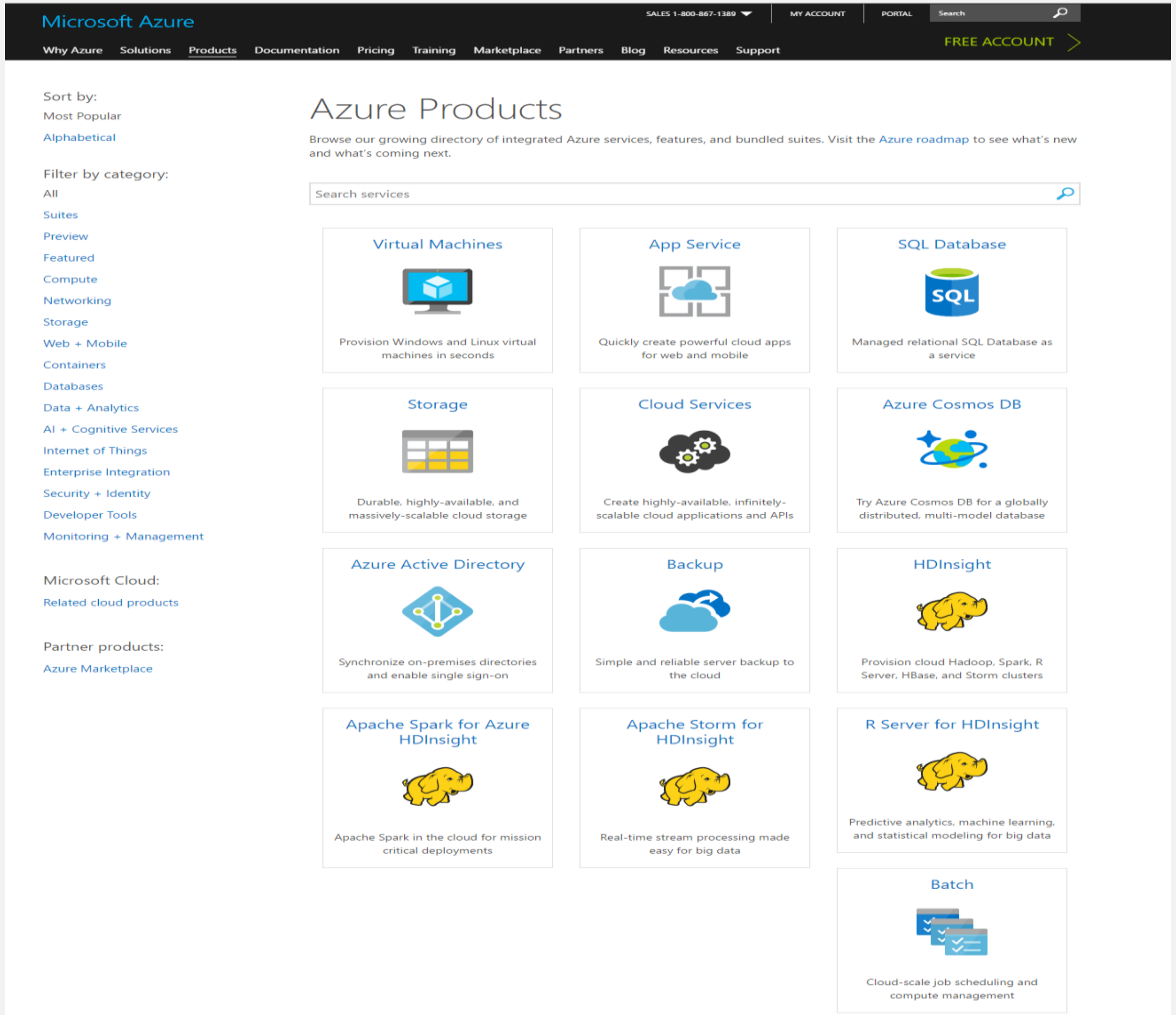


Microsoft

Accessing Azure Services

Azure Services

- ✓ Provide dynamic scaling for cloud workloads
- ✓ Availability/Reliability guarantees offered by the services
- ✓ Ease of management : No manual patching/updates
- ✓ Cost-Effective : Pay for what you use



Microsoft Azure

SALES 1-800-867-1389 | MY ACCOUNT | PORTAL | Search

Why Azure | Solutions | Products | Documentation | Pricing | Training | Marketplace | Partners | Blog | Resources | Support

FREE ACCOUNT

Sort by:
Most Popular
Alphabetical

Filter by category:
All
Suites
Preview
Featured
Compute
Networking
Storage
Web + Mobile
Containers
Databases
Data + Analytics
AI + Cognitive Services
Internet of Things
Enterprise Integration
Security + Identity
Developer Tools
Monitoring + Management

Microsoft Cloud:
Related cloud products

Partner products:
Azure Marketplace

Azure Products

Browse our growing directory of integrated Azure services, features, and bundled suites. Visit the Azure roadmap to see what's new and what's coming next.

Search services

Virtual Machines
Provision Windows and Linux virtual machines in seconds

App Service
Quickly create powerful cloud apps for web and mobile

SQL Database
Managed relational SQL Database as a service

Storage
Durable, highly-available, and massively-scalable cloud storage

Cloud Services
Create highly-available, infinitely-scalable cloud applications and APIs

Azure Cosmos DB
Try Azure Cosmos DB for a globally distributed, multi-model database

Azure Active Directory
Synchronize on-premises directories and enable single sign-on

Backup
Simple and reliable server backup to the cloud

HDInsight
Provision cloud Hadoop, Spark, R Server, HBase, and Storm clusters

Apache Spark for Azure HDInsight
Apache Spark in the cloud for mission critical deployments

Apache Storm for HDInsight
Real-time stream processing made easy for big data

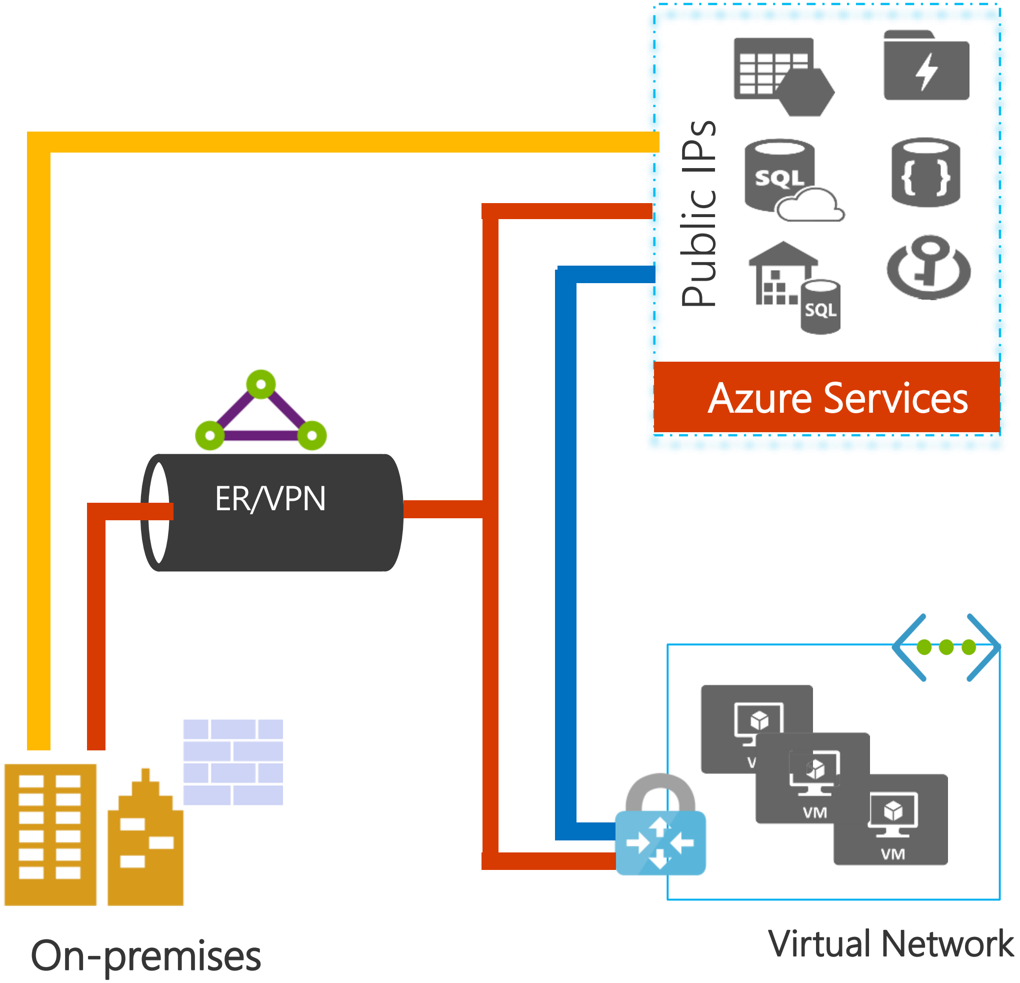
R Server for HDInsight
Predictive analytics, machine learning, and statistical modeling for big data

Batch
Cloud-scale job scheduling and compute management

https://azure.microsoft.com/en-us/services

Azure services – Access

- ✓ Azure services are generally accessible over Public IP addresses*
- ✓ Customers connect to Services primarily from their VNets and On-Prem
- ✓ Services are reachable from anywhere.

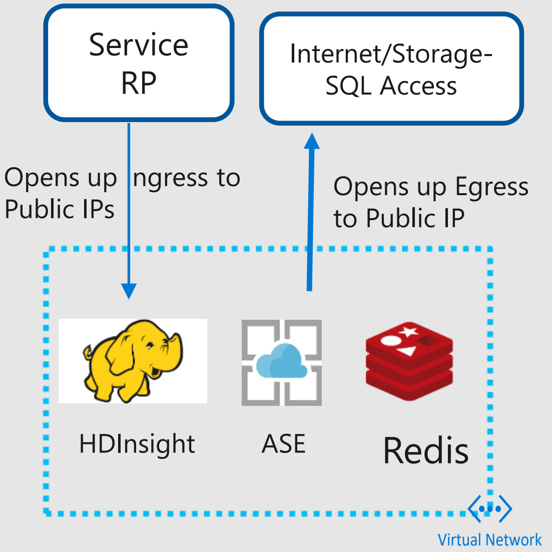


*Public IPs are internet routable addresses

Azure Services - Integration Patterns

VNet Injection

Service deploys dedicated instances into customer's VNet



Service RP

Internet/Storage-SQL Access

Opens up Ingress to Public IPs

Opens up Egress to Public IP

HDInsight

ASE

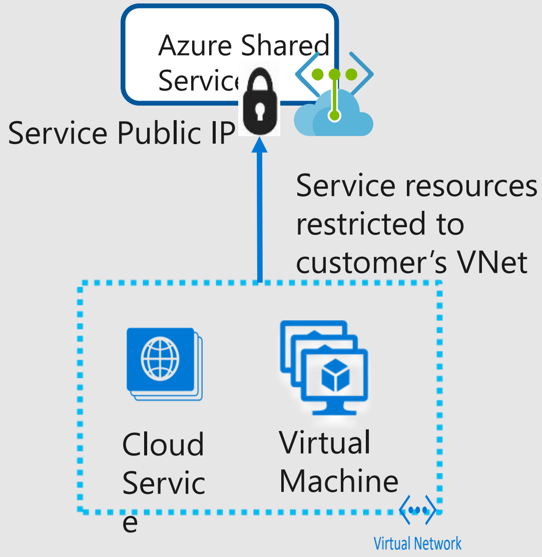
Redis

Virtual Network

Inbound/outbound access to VNets; Single-Tenancy

VNet Service Endpoints

Secure Azure resources by extending VNets to multi-tenant service



Azure Shared Service

Service Public IP

Service resources restricted to customer's VNet

Cloud Service

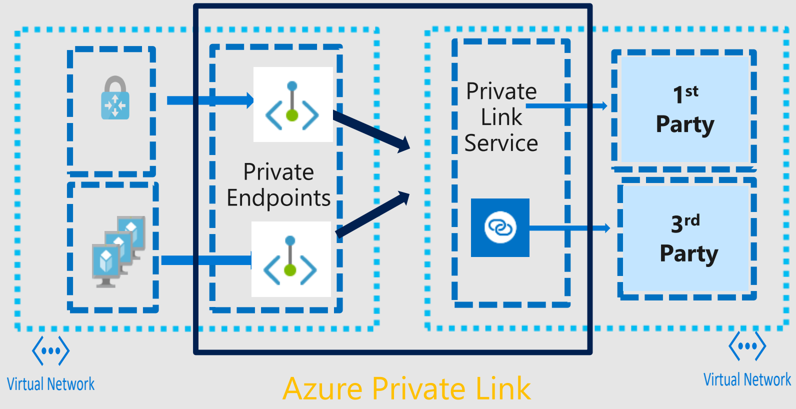
Virtual Machine

Virtual Network

Outbound-only access from VNets; Multi-Tenant Service

Azure Private Link

Connect to Azure resources privately



Private Endpoints

Private Link Service

1st Party

3rd Party

Virtual Network

Azure Private Link

Virtual Network

Private connectivity to services delivered on Azure

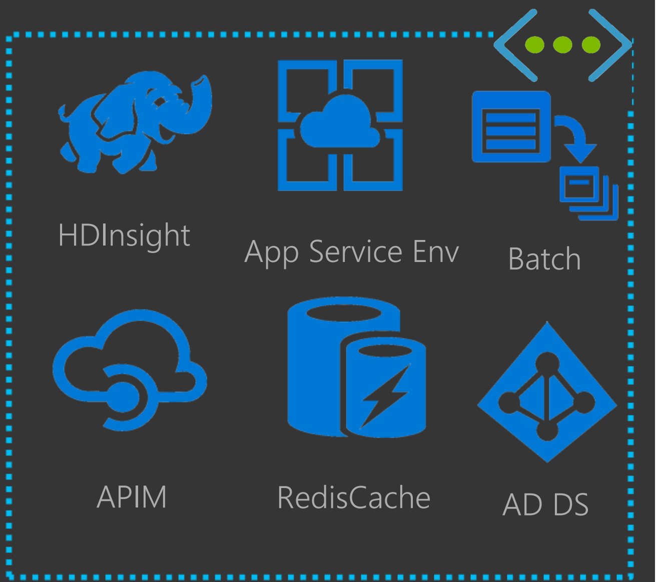
Microsoft

VNet Integration for Azure Services

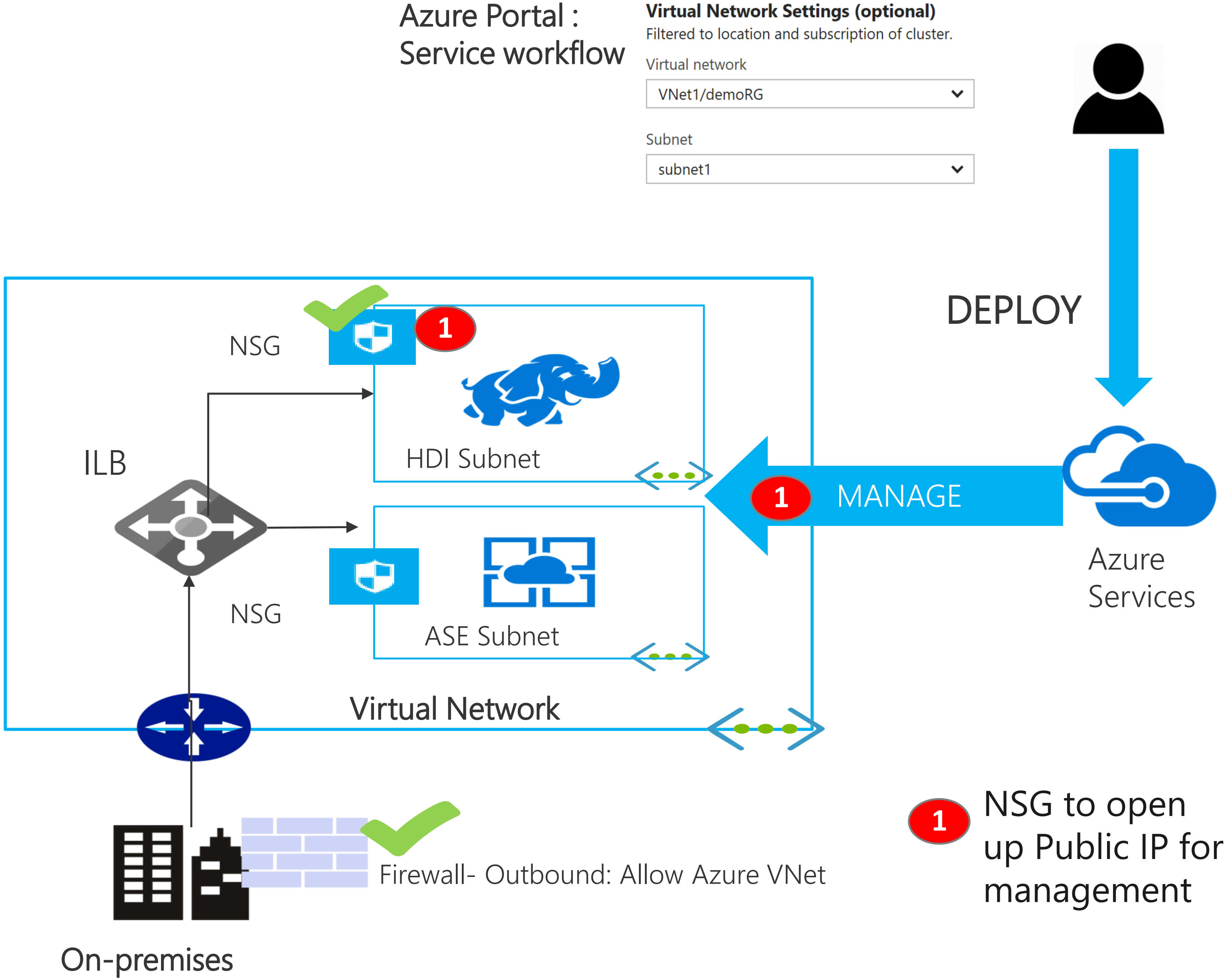
- VNet Injection
- VNet Service Endpoints
- Private Link

VNet Injection

- ✓ Services in your VNet, managed by Azure!
- ✓ Private IPs for service resources
- ✓ On-premises through Site-to-Site or ER private peering



Azure Portal : Service workflow



Virtual Network Settings (optional)

Filtered to location and subscription of cluster.

Virtual network: VNet1/demoRG

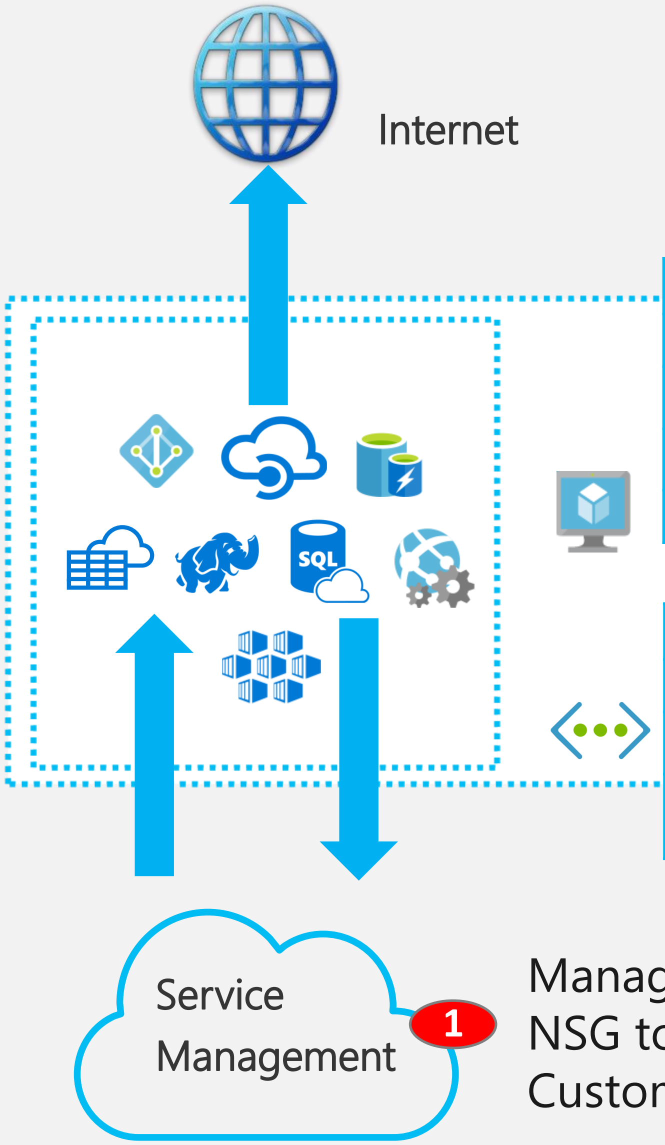
Subnet: subnet1

1 NSG to open up Public IP for management

VNet Injection

- ✓ Services in your VNet, managed by Azure!
- ✓ Private IPs for service resources
- ✓ On-premises through Site-to-Site or ER private peering

VNet Injection



Network Security with NSG & User Defined Routes

Network Security Group

Action	Direction	Name	Source/Destination
Allow	Inbound	Management	**HDInisghts**
Allow	Outbound	Management	**AzureMachineLearning**
Allow	Outbound	InternetDependencies	List of Services Tags

Route Table

Name	Address Prefix	Next Hop
Management	*Service Management IP Addresses*	Internet
InternetDependency	List of Services Tags List explicit IP addresses	Internet

Management over public IPs
NSG to open up Public IP for management
Customers in control of NSGs and UDRs

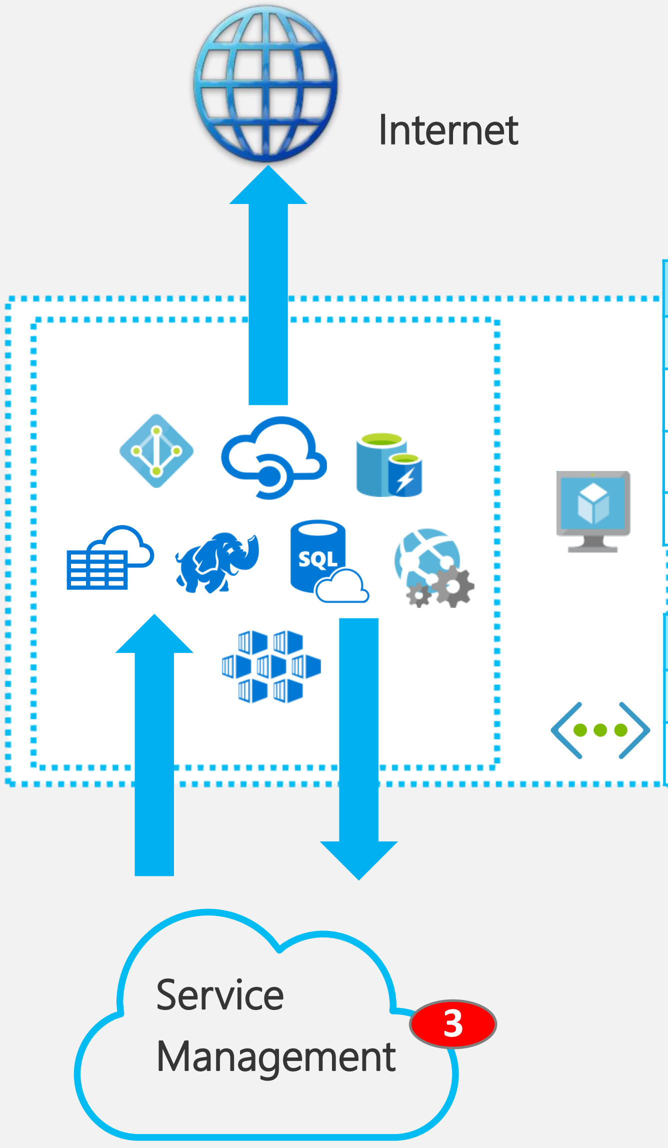
VNet Injection

1. Management IP addresses maintain with Service Tags

2. UDR support for tags for management traffic

3. Easier configuration with automatic preparation

Subnet delegation and easier configuration



Network Security with NSG & User Defined Routes

Network Security Group

Action	Direction	Name	Source/Destination
Allow	Inbound	Management	*ServiceManagementTag*
Allow	Outbound	Management	*ServiceManagementTag*
Allow	Outbound	InternetDependencies	List of Services Tags

1

Route Table

Name	Address Prefix	Next Hop
Management	*ServiceManagementTag*	Internet

2

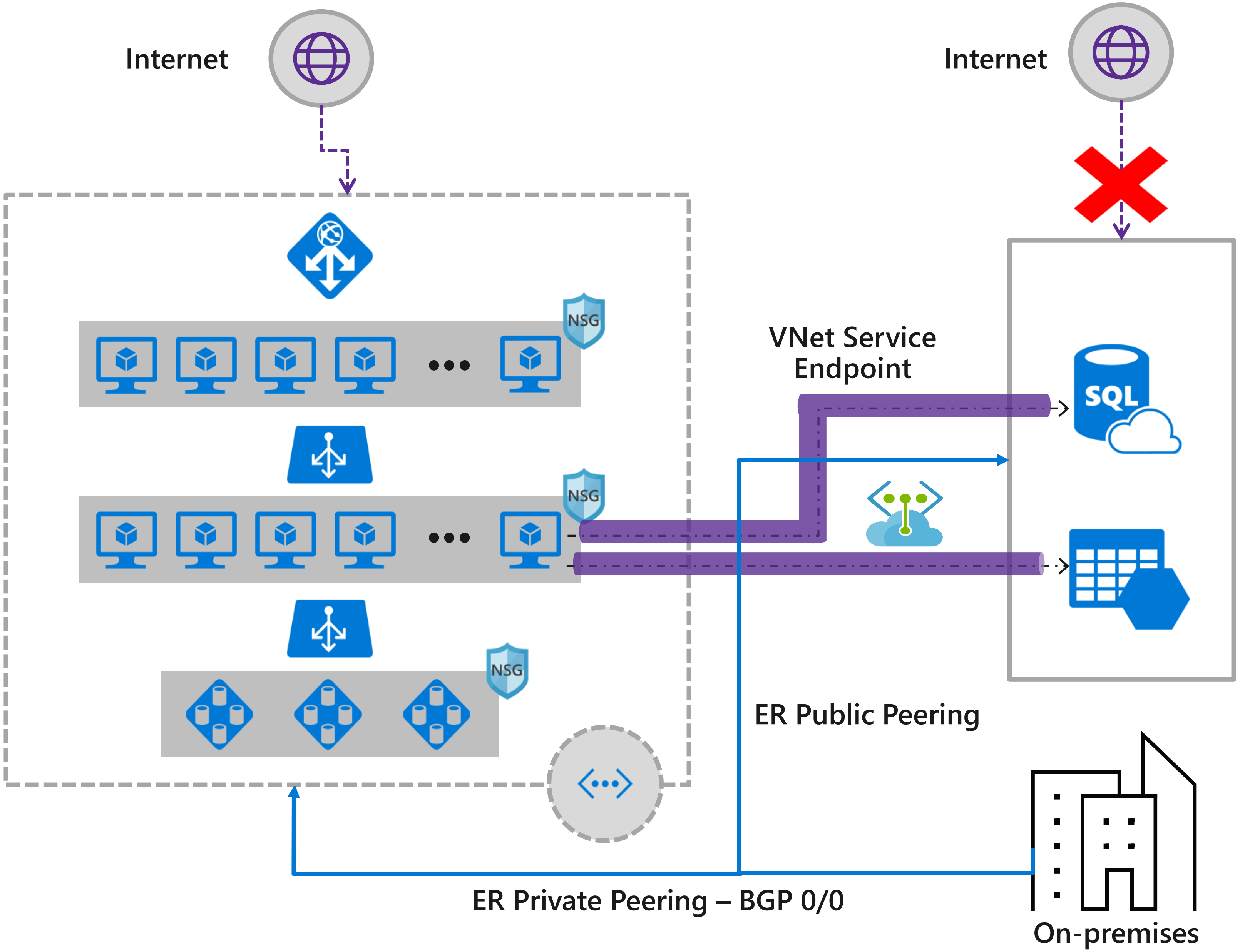
VNet Integration for Azure Services

- VNet Injection
- VNet Service Endpoints
- Private Link

VNet Service Endpoints

Shared resources secured to customer's VNet

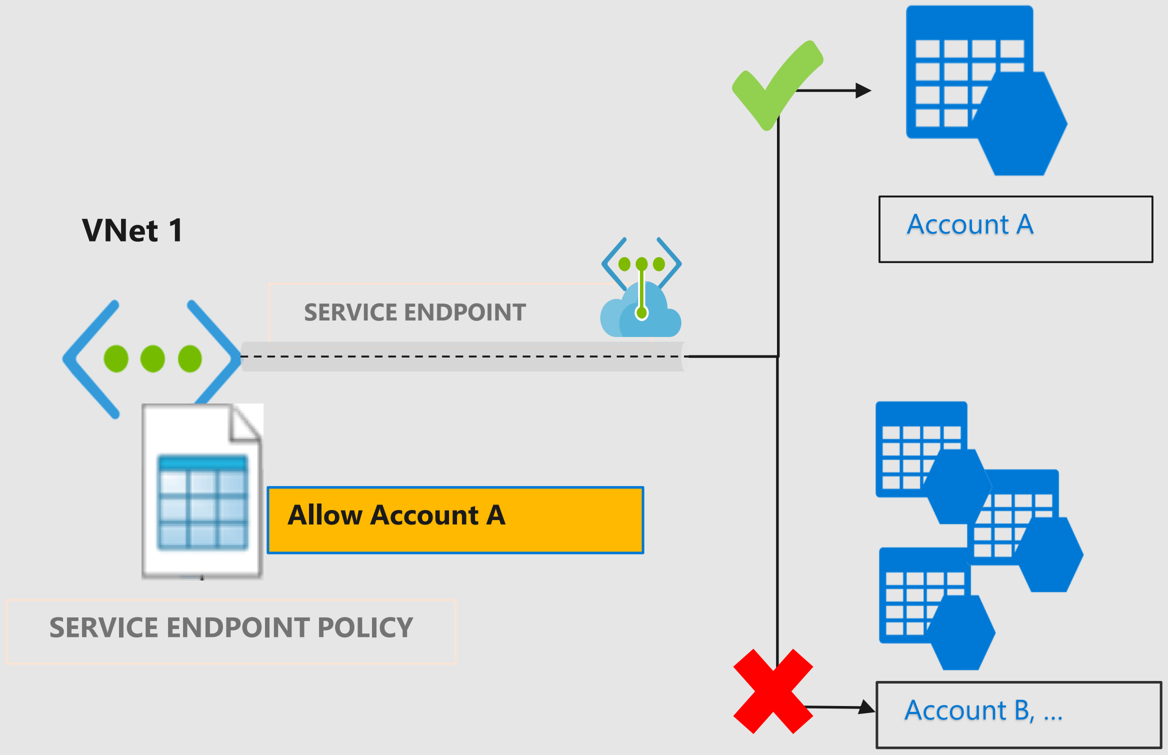
- ✓ Directly extends VNet to the service
- ✓ Secure critical Azure resources to only your VNet
- ✓ Traffic remains on the Microsoft backbone
- ✓ On-premises access through ER public peering
- ✓ Forced Tunneling overridden
- ✓ Cosmos DB, KeyVault and EventHub now supported



Service Endpoints Policies

Enhanced VNet security for Azure services

- Prevent unauthorized access to storage accounts
- Restrict Virtual Network access to specific Azure Storage Accounts
- Granular access control over service endpoints

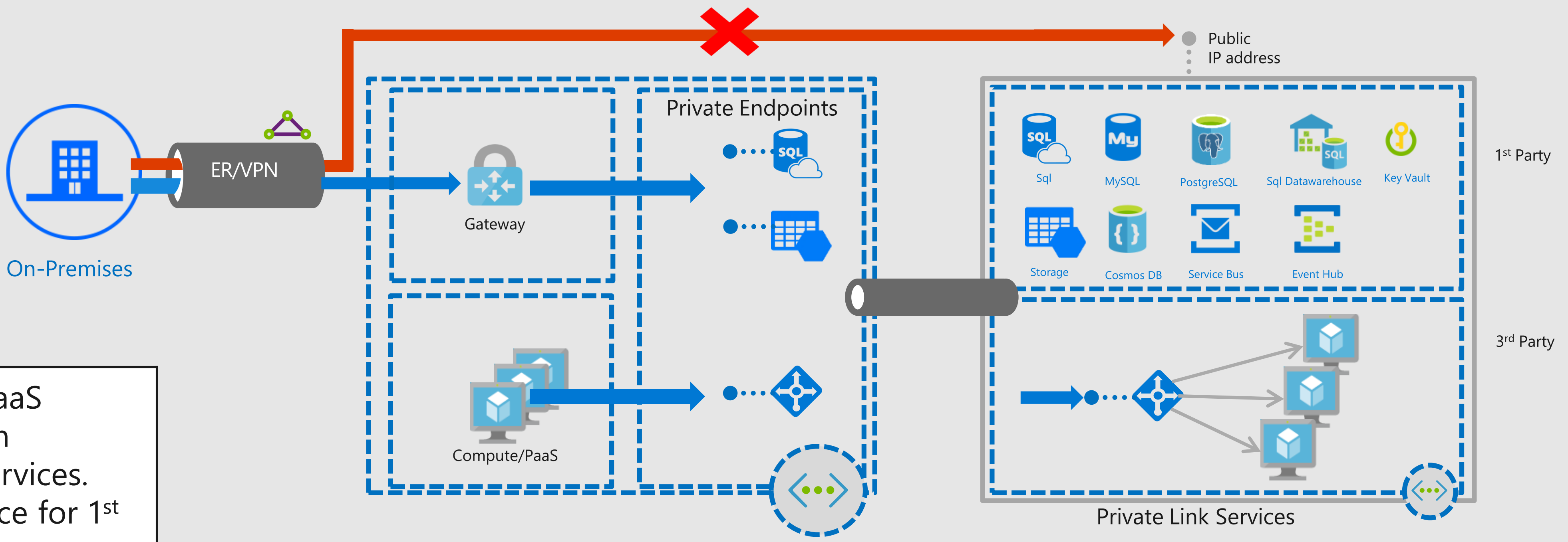


Microsoft

VNet Integration for Azure Services

- VNet Injection
- VNet Service Endpoints
- Private Link

VNet Integration – Private Link



Private Endpoints : Map PaaS resources into a private IP in customer VNet for Azure services. Same connectivity experience for 1st party and 3rd party services.

Private Link Service: Build or consume your own service privately. Approval workflow for new connections

Private Endpoints

Connectivity to PaaS services using Virtual Networks

From on premises

✓ Direct connectivity from on premises using ER private peering or VPN tunnels, removing internet traffic.

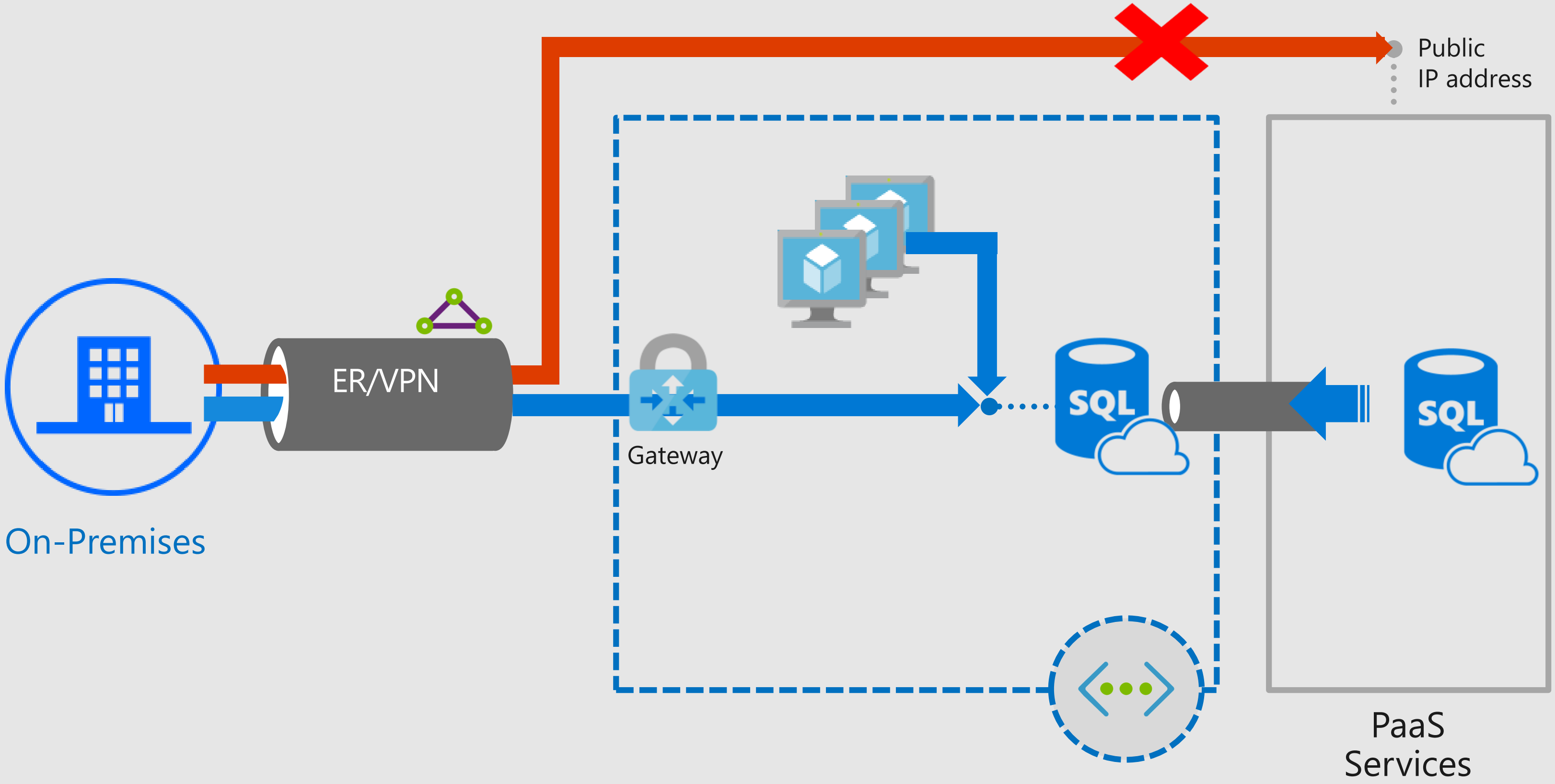
Within the VNet

✓ Connect privately to Azure PaaS resources within your VNet.

Security simplified

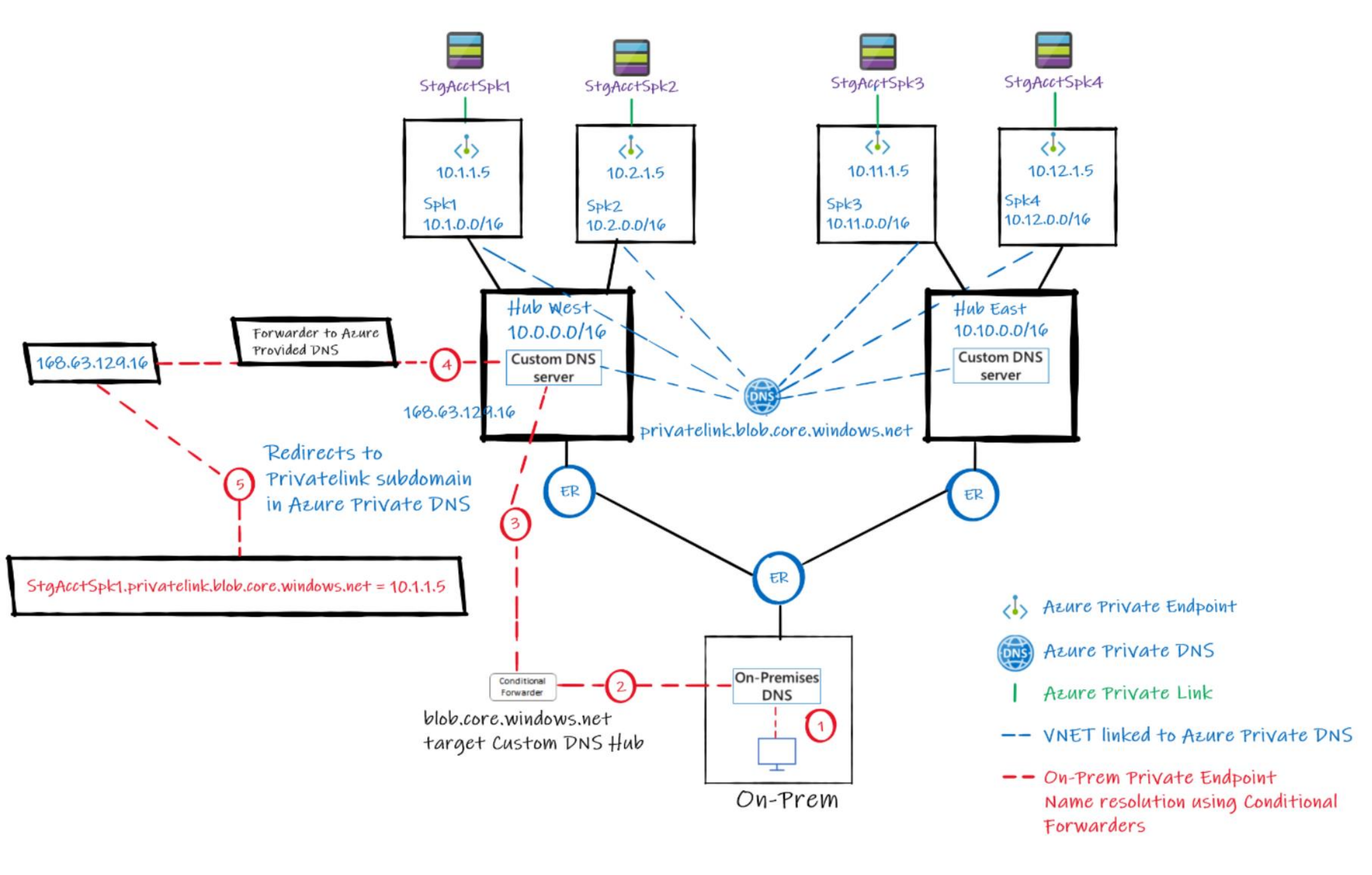
✓ NSG & Firewall configuration clean within customer address space

✓ Predictable IP addresses for PaaS resources



Private Endpoints
DNS Integration

DNS will be the most important consideration when using Private Link in Azure



Further Reading

- Azure Networking
- VNET Injection
- Service Endpoints
- Private Link
- Private Link DNS Integration