cloudFRIDAYS

Azure Networking

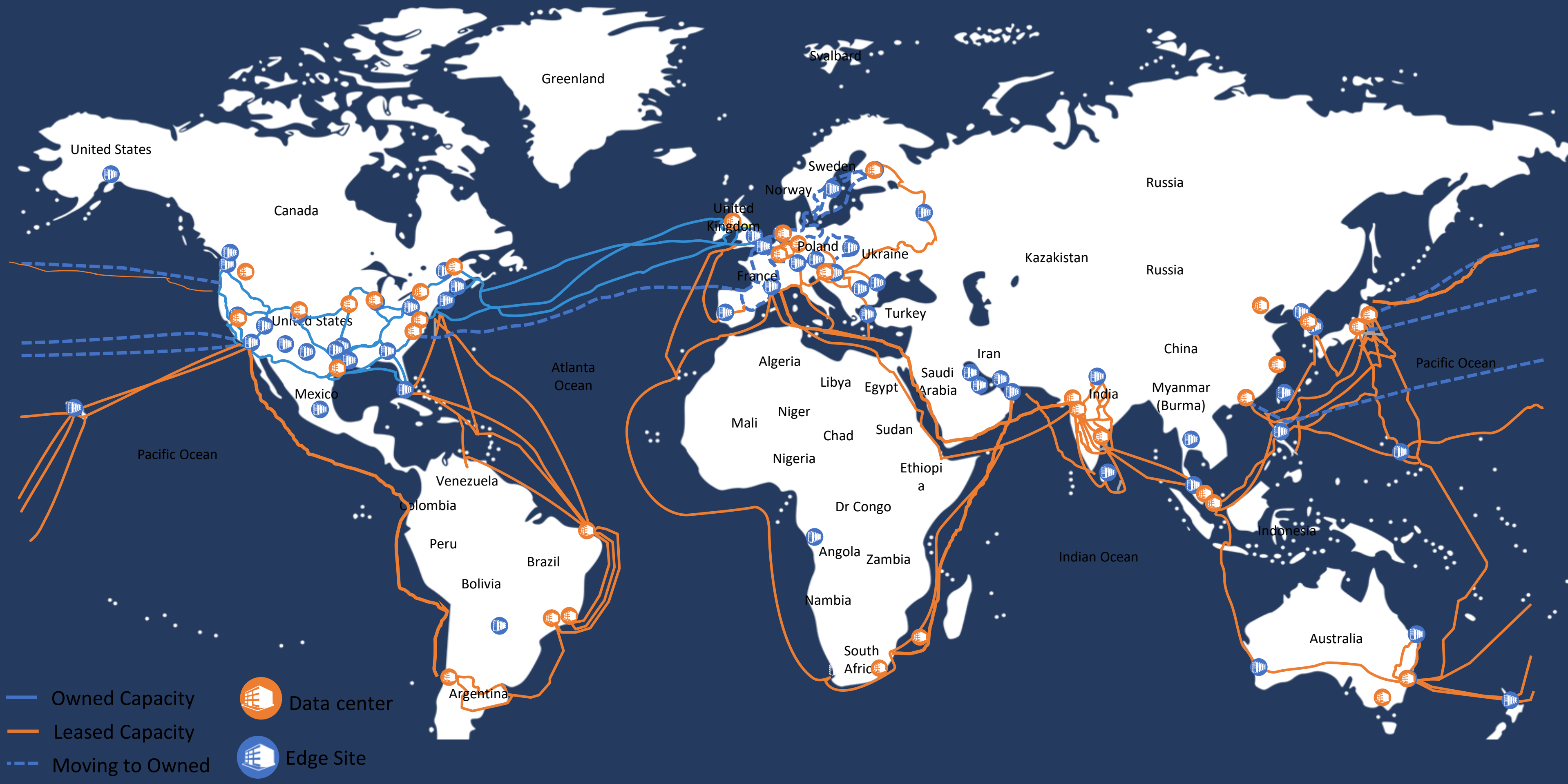
Vnets, Load Balancer, VPN Gateway, Application Gateway, ExpressRoute

Matthew Levy

Enterprise Mobility MVP

@skrods

Microsoft Global Network



One of the largest private networks in the world

- 8,000+ ISP sessions
- 130+ edge sites
- 44 ExpressRoute locations
- 33,000 miles of lit fiber
- SDN Managed (SWAN, OLS)

DCs and Network sites not exhaustive

Robust networking infrastructure services

Virtual Network

Provision private networks, optionally connect to on premise datacenters. NSG, User Defined Routes, & IP addresses.

Load Balancer

Deliver high availability and network performance to your applications

Application Gateway/WAF

Build scalable and highly-available web front ends in Azure

DDoS Protection

Protect your Azure resources from DDoS attacks

VPN Gateway

Establish secure, cross-premise connectivity

Azure DNS

Host your DNS domain in Azure

Content Delivery Network

Ensure secure, reliable content delivery with broad global reach

Traffic Manager

Route incoming traffic for high performance and availability

ExpressRoute

Dedicated private network fiber connections to Azure

Network Watcher

Network performance monitoring and diagnostics solution

Hyperscale datacentre infrastructure

Terminology

Region

- Set of datacenters in the same metro area
- Number and exact location of DC facilities not exposed to end users
- Any two VMs hosted in the same region are less than 2ms away from each other (RTT)
- Inter-DC switching bandwidth in a region up to 1.6 Pb/s, depending on the region DC capacity (MW)

Availability zones (only in select regions)

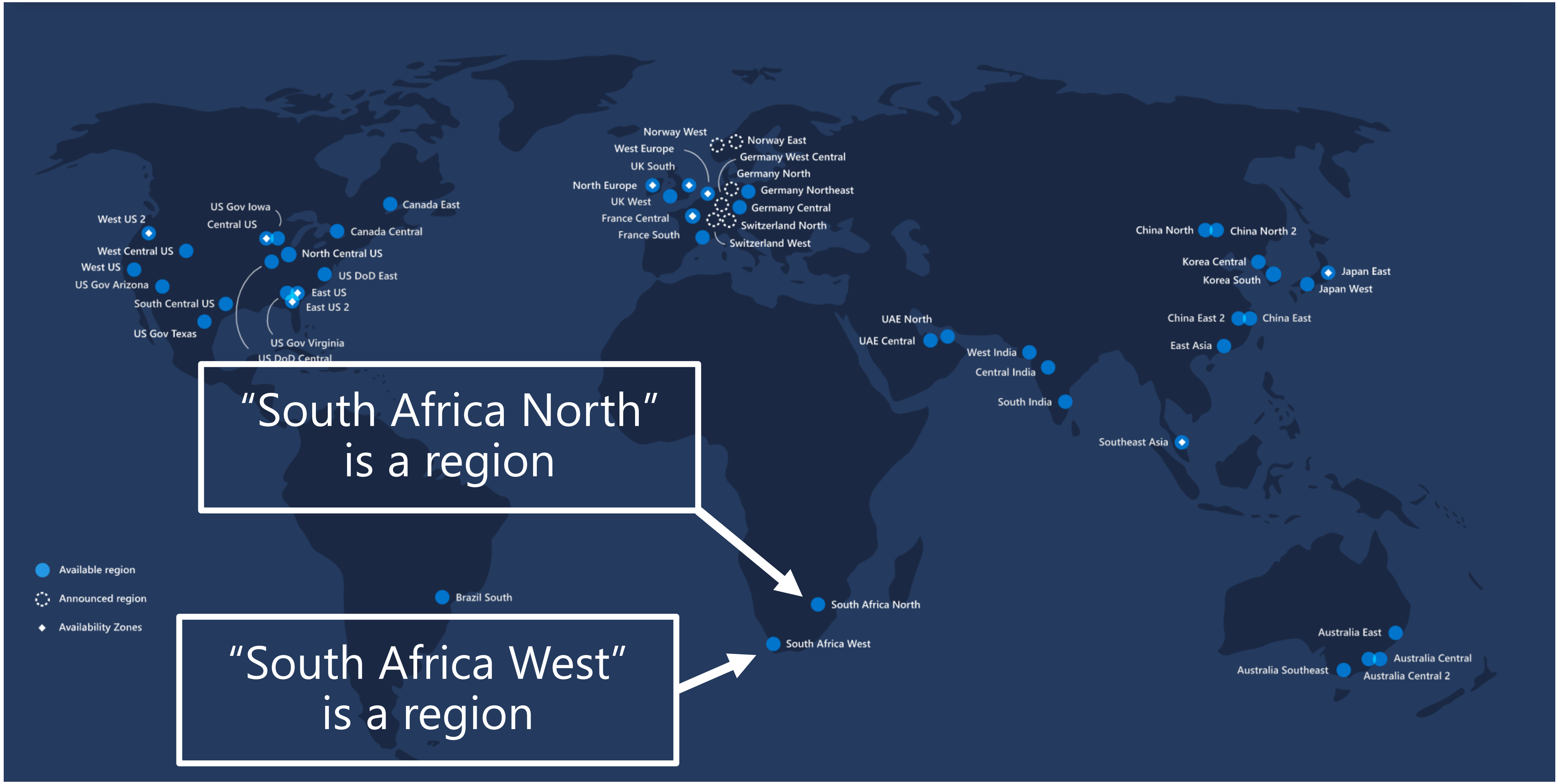
- Logical partitioning of DC facilities in a region based on geographical position
- Each partition is an availability zone
- Any two VMs in the same availability zone are less than 1ms away from each other (RTT)
- DC facilities in each zone have independent power, cooling and network
- DC facilities in each zone are distant enough from other zones not to be impacted by adverse events (e.g. fires) at the same time

Geography

- Set of regions in the same geo-political area
- Can be a country, or a continent

Hyperscale datacentre infrastructure

Terminology – RSA example

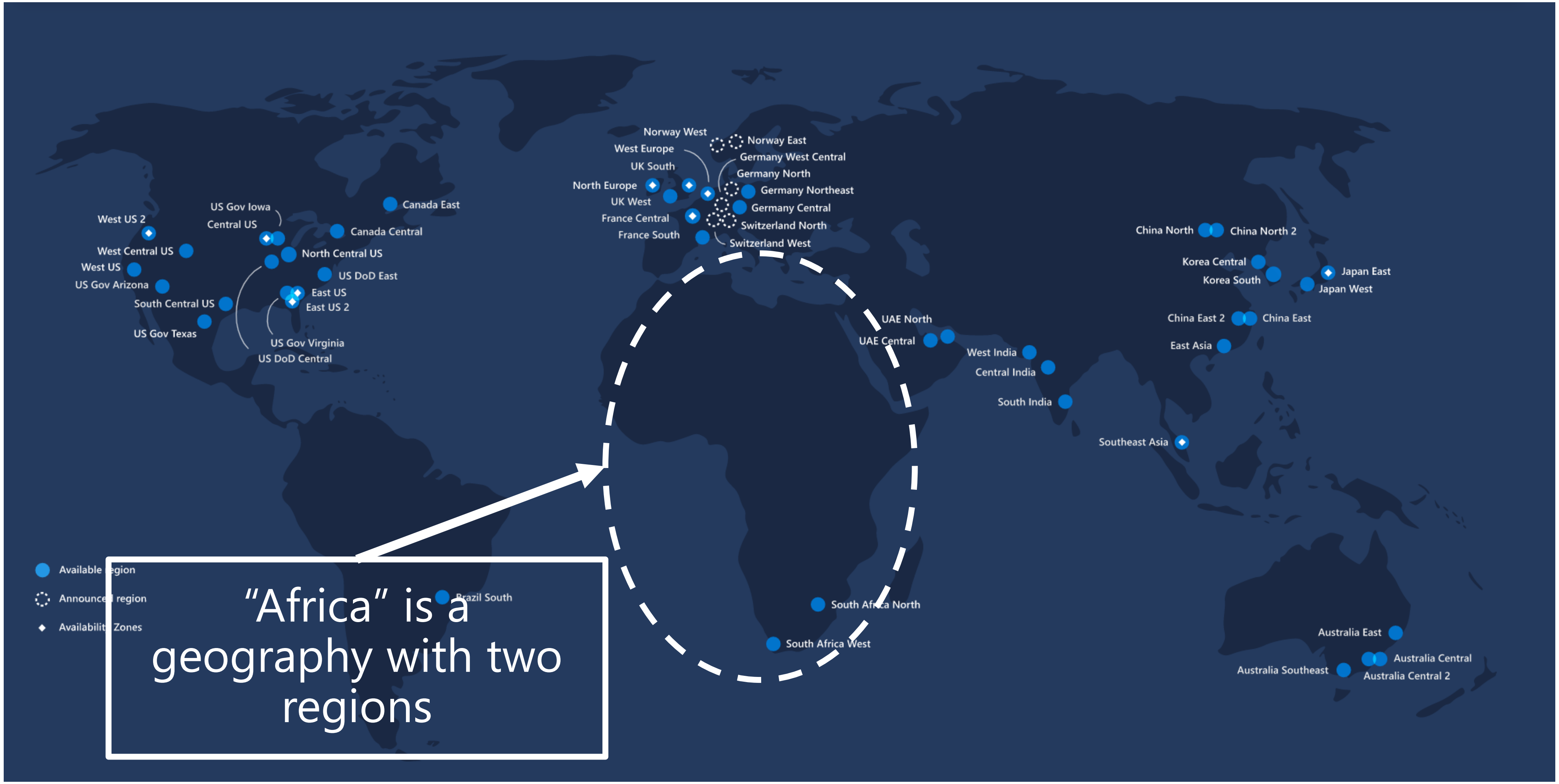


"South Africa North" is a region

"South Africa West" is a region

Hyperscale datacentre infrastructure

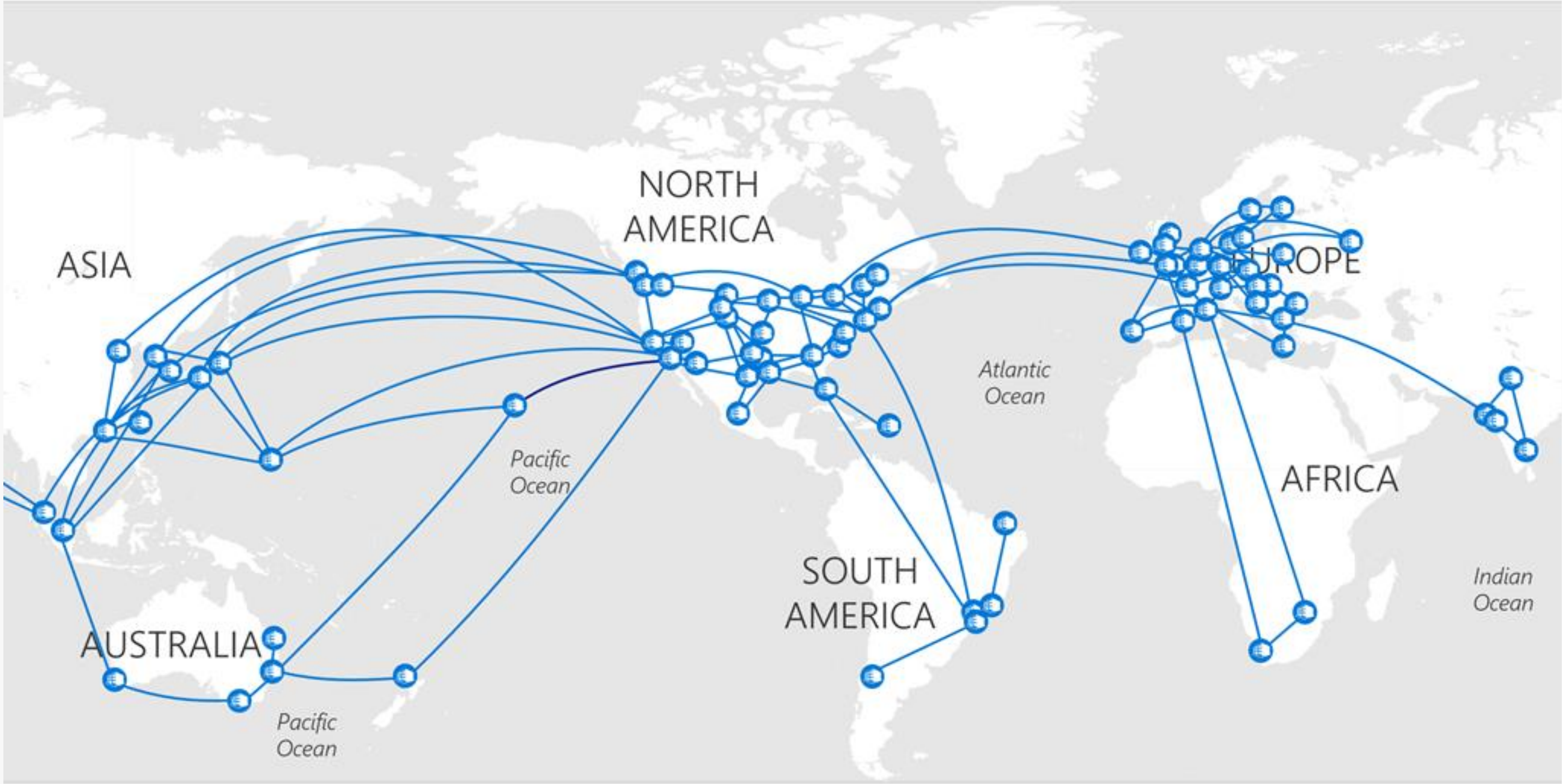
Terminology – RSA example



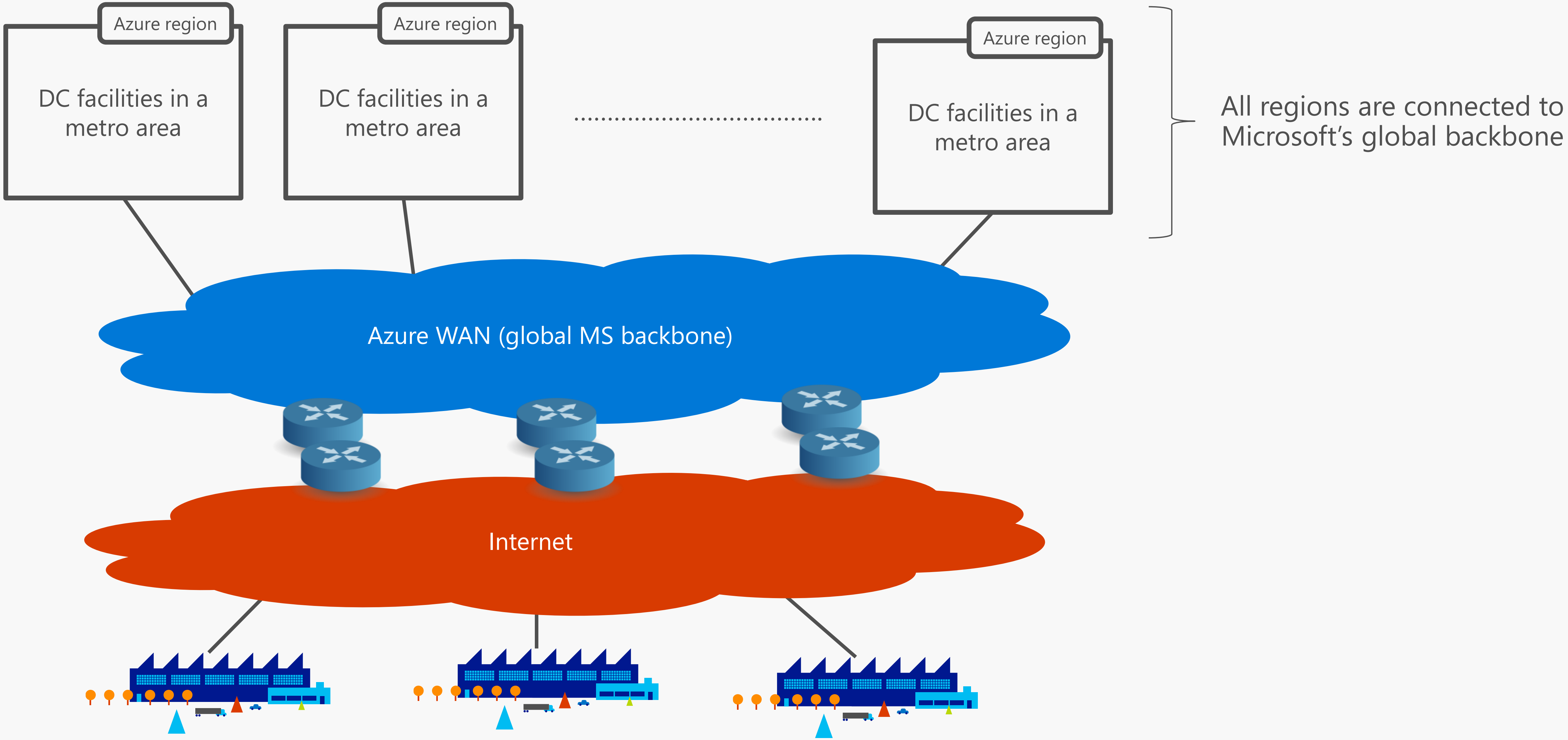
“Africa” is a geography with two regions

Azure networking fundamentals

Microsoft global WAN

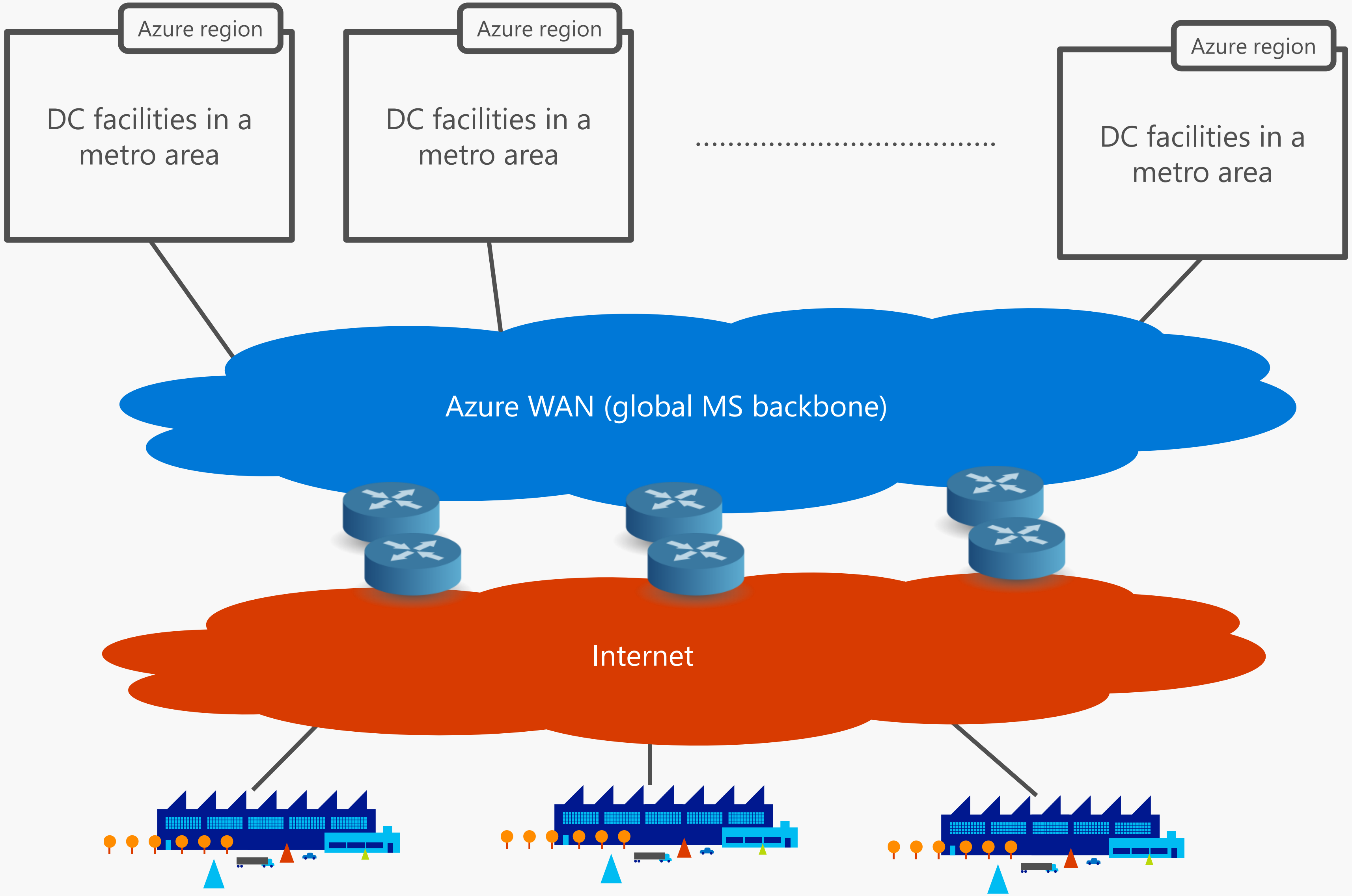


Azure high-level network architecture


Azure region
DC facilities in a metro area
Azure region
DC facilities in a metro area
Azure region
DC facilities in a metro area
Azure WAN (global MS backbone)
Internet

All regions are connected to Microsoft's global backbone

Azure high-level network architecture

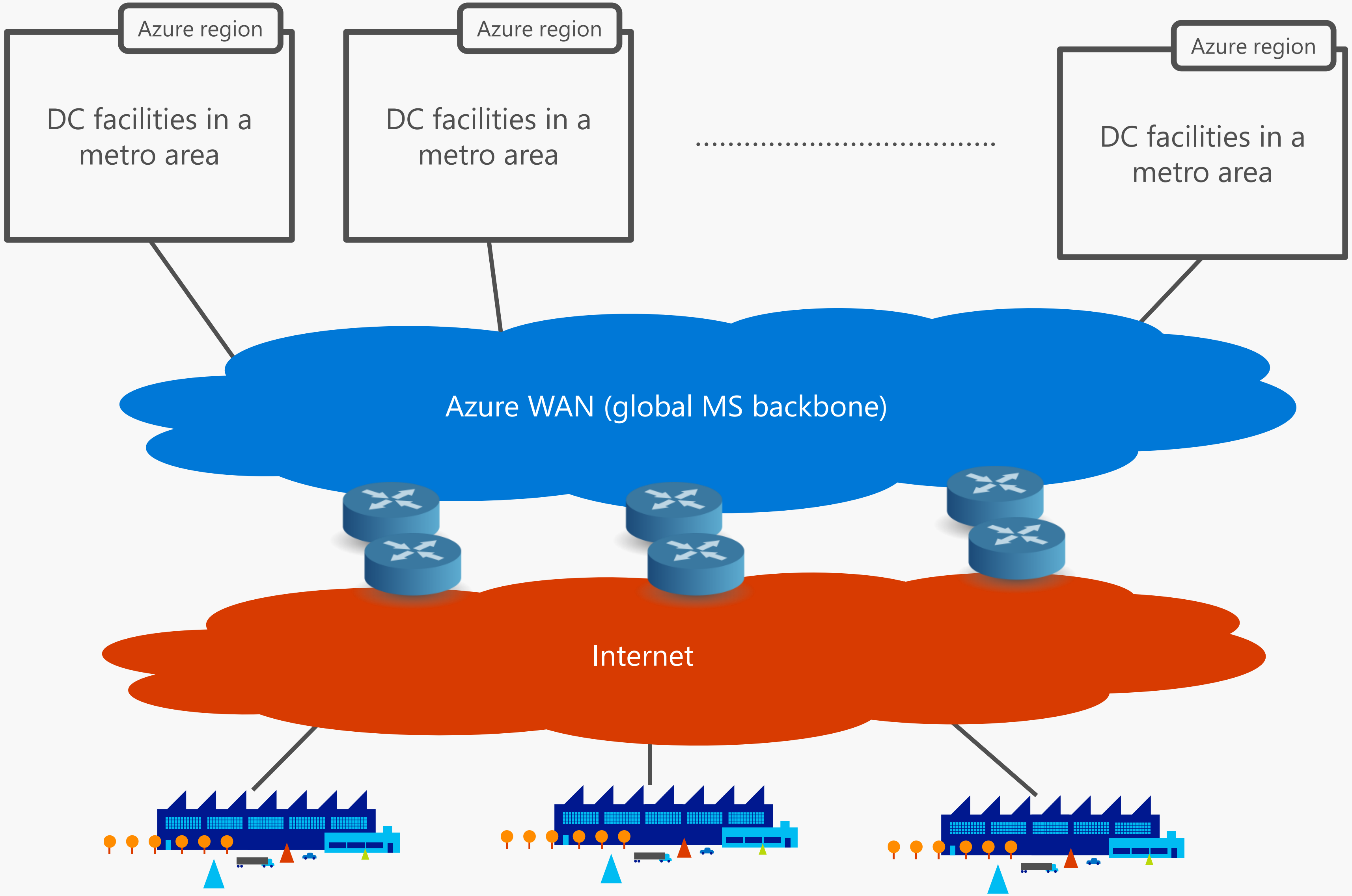

Azure region
DC facilities in a metro area
Azure region
DC facilities in a metro area
Azure region
DC facilities in a metro area
Azure WAN (global MS backbone)
Internet

All regions are connected to Microsoft's global backbone

The Microsoft backbone interconnects all regions with each other and with the public internet

The Microsoft network peers with 2500+ ISP in 130+ PoPs

Azure high-level network architecture


Azure region
DC facilities in a metro area
Azure region
DC facilities in a metro area
Azure region
DC facilities in a metro area
Azure WAN (global MS backbone)
Internet

All regions are connected to Microsoft's global backbone

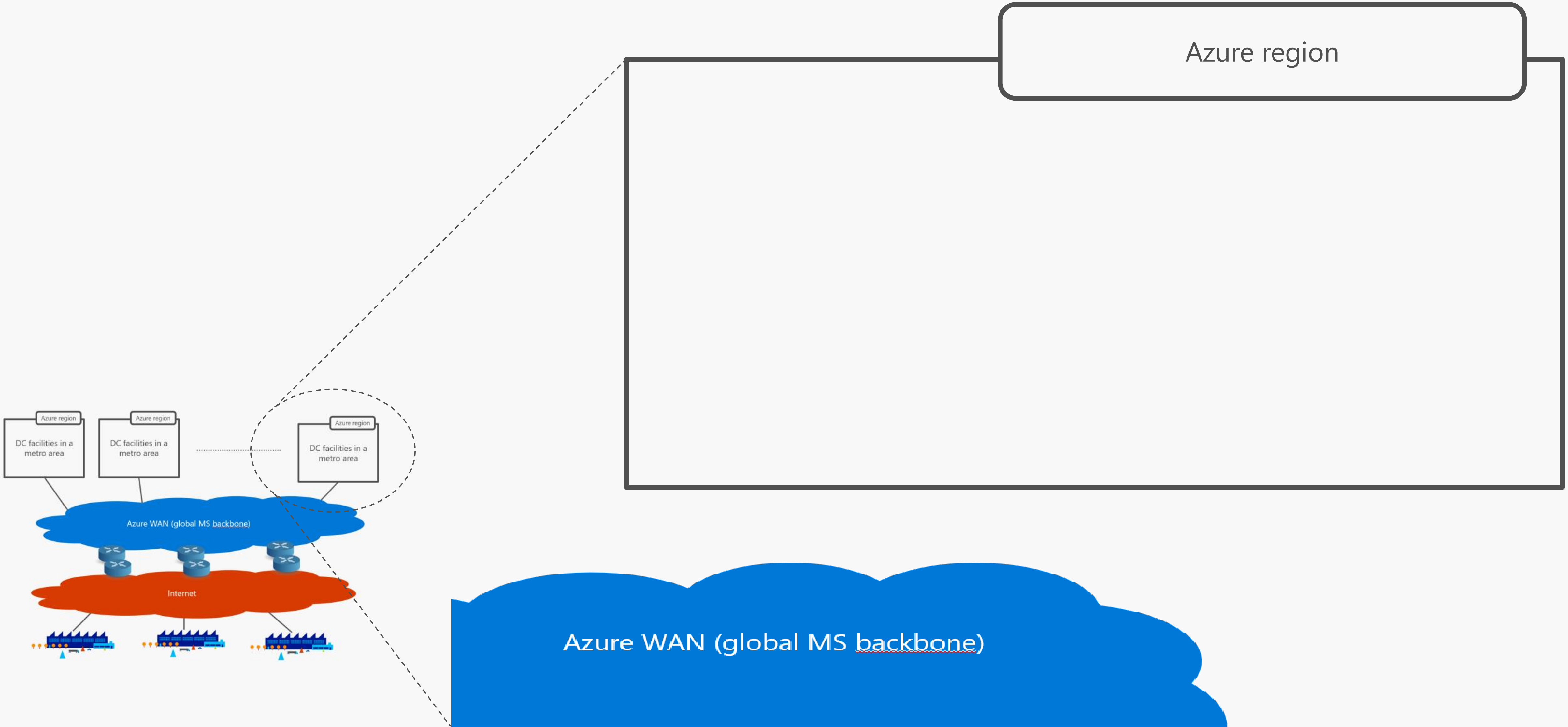
The Microsoft backbone interconnects all regions with each other and with the public internet

The Microsoft network peers with 2500+ ISP in 130+ PoPs

Customers can use their existing internet connectivity to reach the Microsoft network and consume services in Microsoft datacenters

Network connectivity for Azure services

Public vs. private services



Azure region

DC facilities in a metro area

Azure region

DC facilities in a metro area

Azure region

DC facilities in a metro area

Azure WAN (global MS backbone)

Internet

Azure region

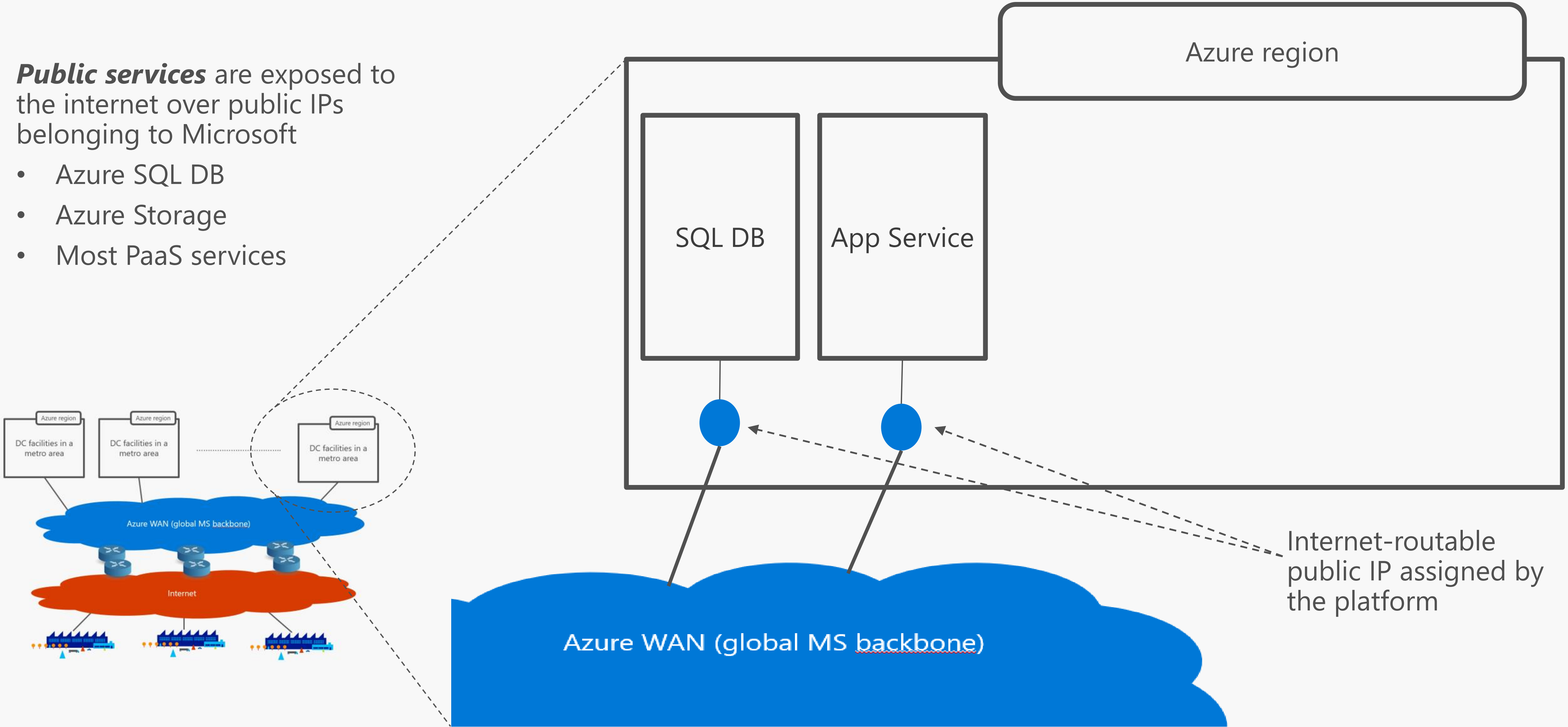
Azure WAN (global MS backbone)

Network connectivity for Azure services

Public vs. private services

Public services are exposed to the internet over public IPs belonging to Microsoft

- Azure SQL DB
- Azure Storage
- Most PaaS services



Azure region

DC facilities in a metro area

Azure WAN (global MS backbone)

Internet

SQL DB

App Service

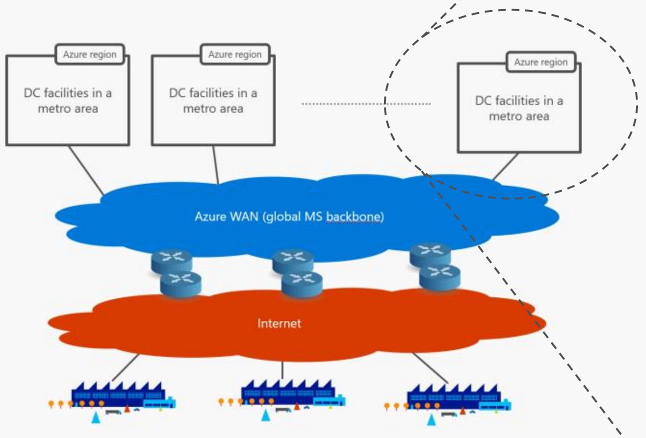
Internet-routable public IP assigned by the platform

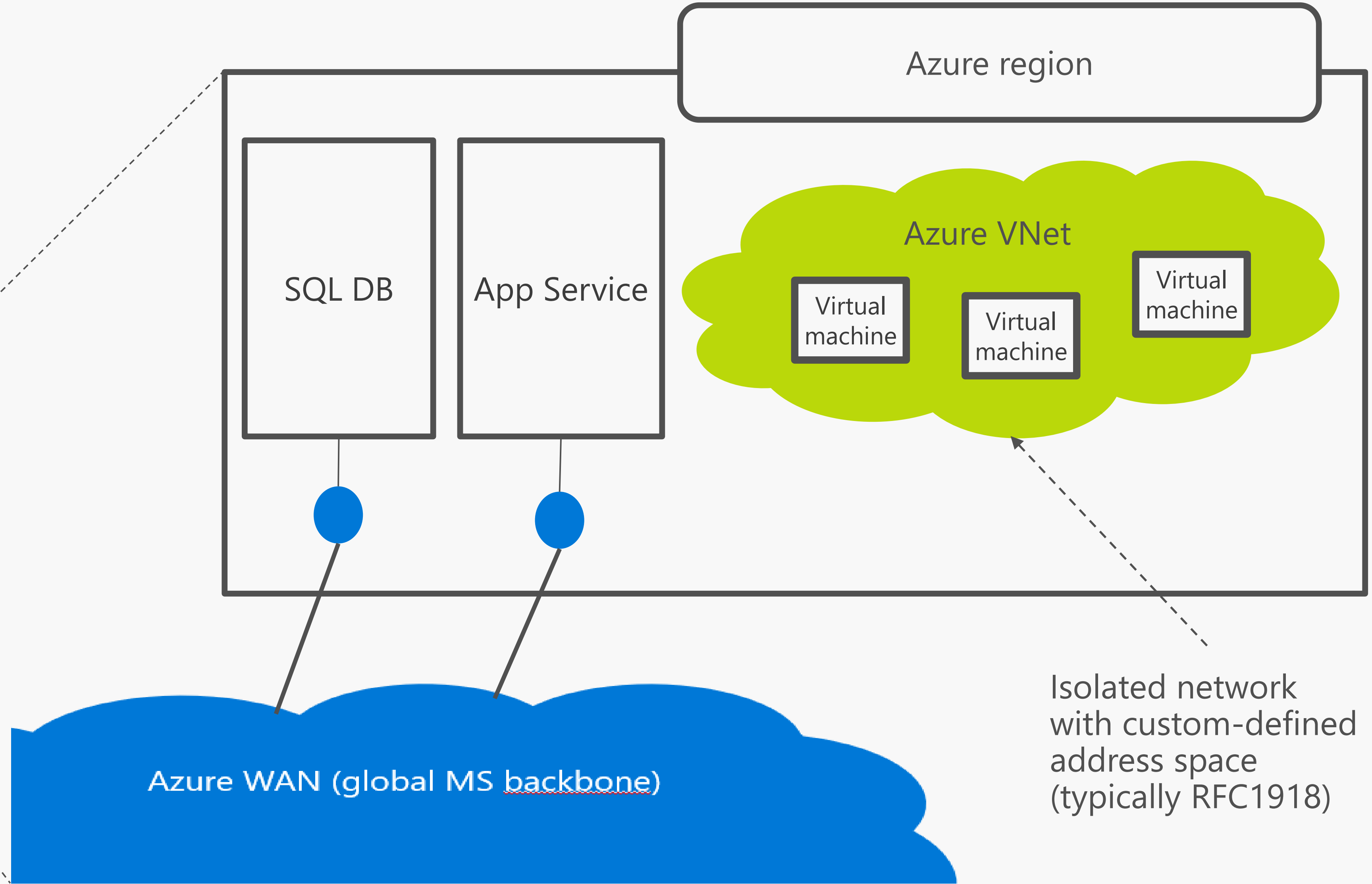
Network connectivity for Azure services

Public vs. private services

Private services are deployed within Azure Virtual Networks, and are assigned private IP addresses taken from customer-controlled address space

- Virtual Machines
- “VNet injected” services


Azure region
DC facilities in a metro area
Azure region
DC facilities in a metro area
Azure region
DC facilities in a metro area
Azure WAN (global MS backbone)
Internet

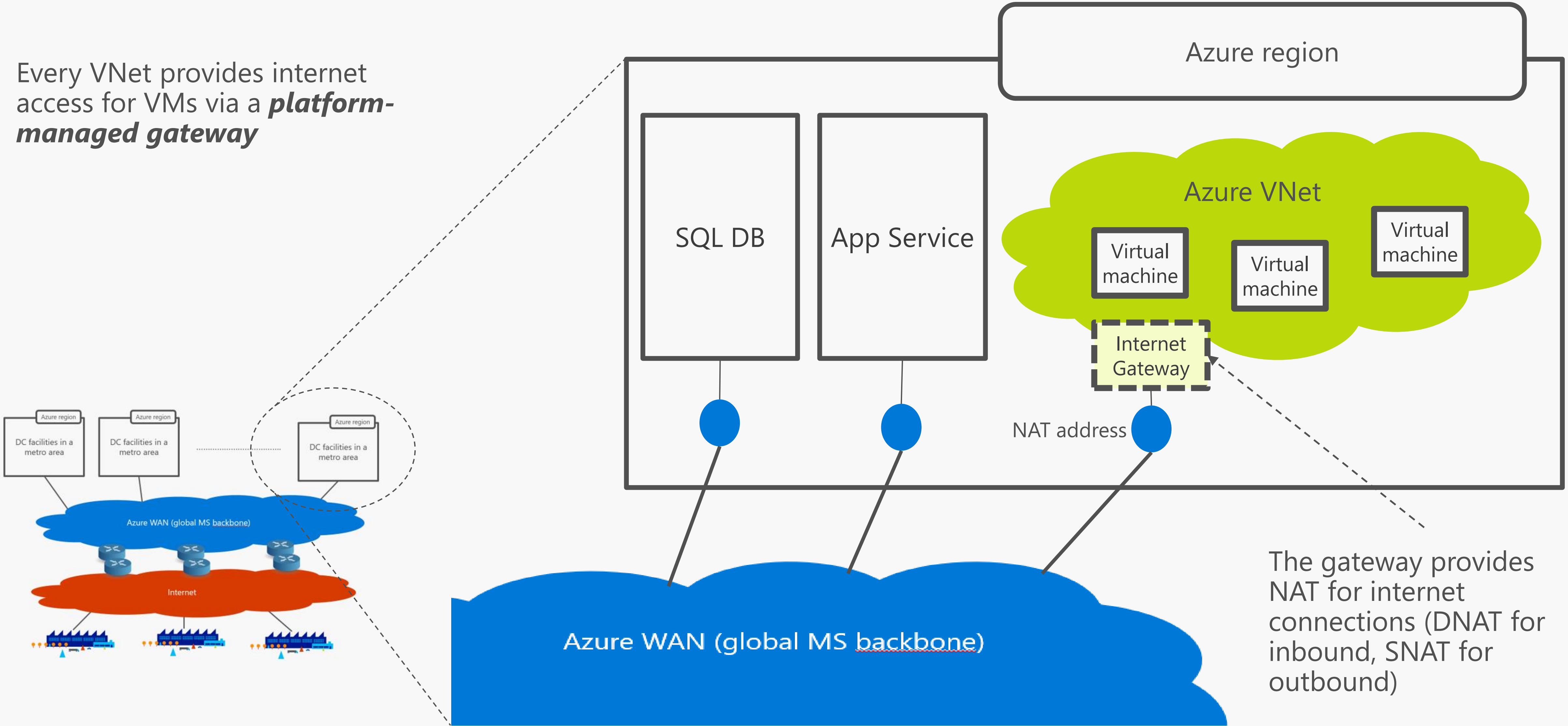


Isolated network with custom-defined address space (typically RFC1918)

Network connectivity for Azure services

Internet access for Virtual Networks

Every VNet provides internet access for VMs via a ***platform-managed gateway***

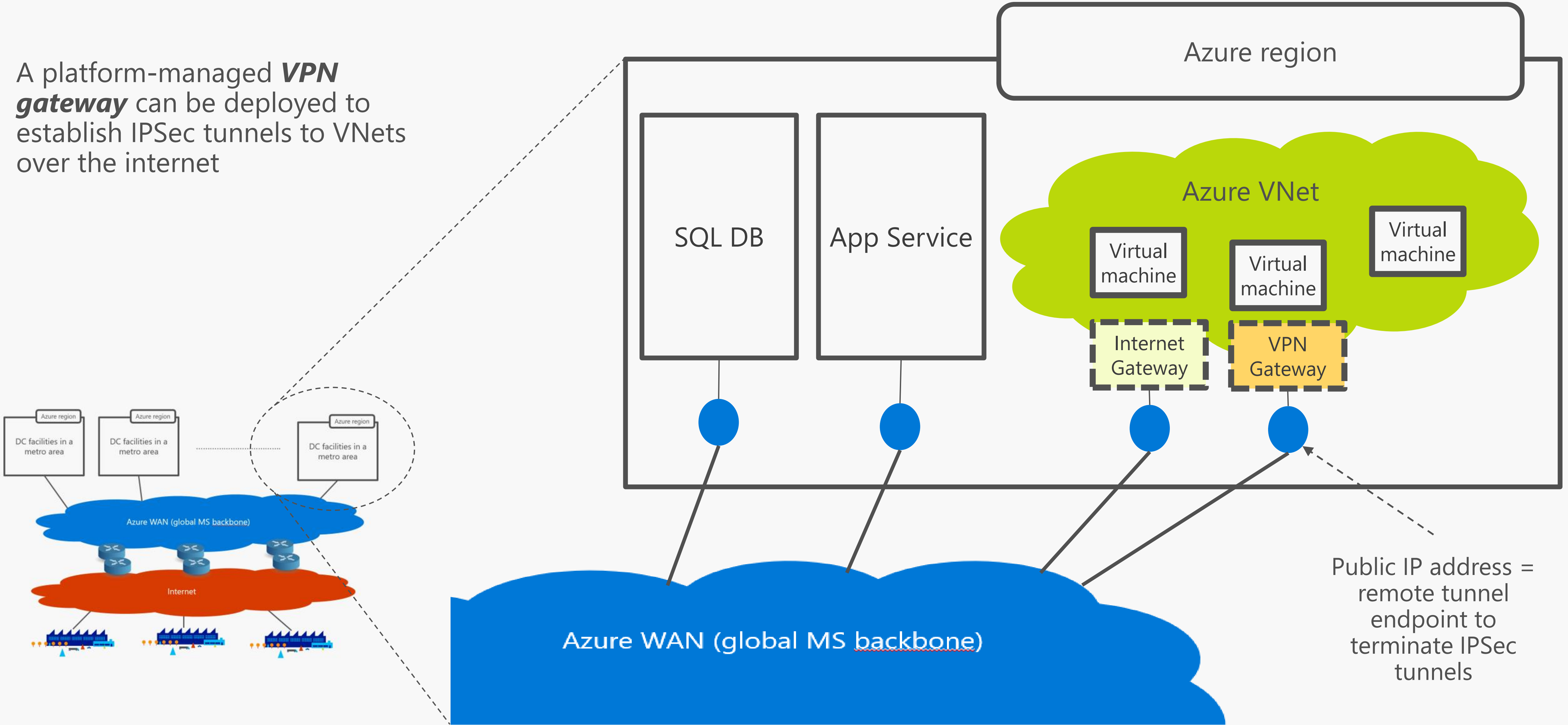


The gateway provides NAT for internet connections (DNAT for inbound, SNAT for outbound)

Network connectivity for Azure services

VPN access for Virtual Networks

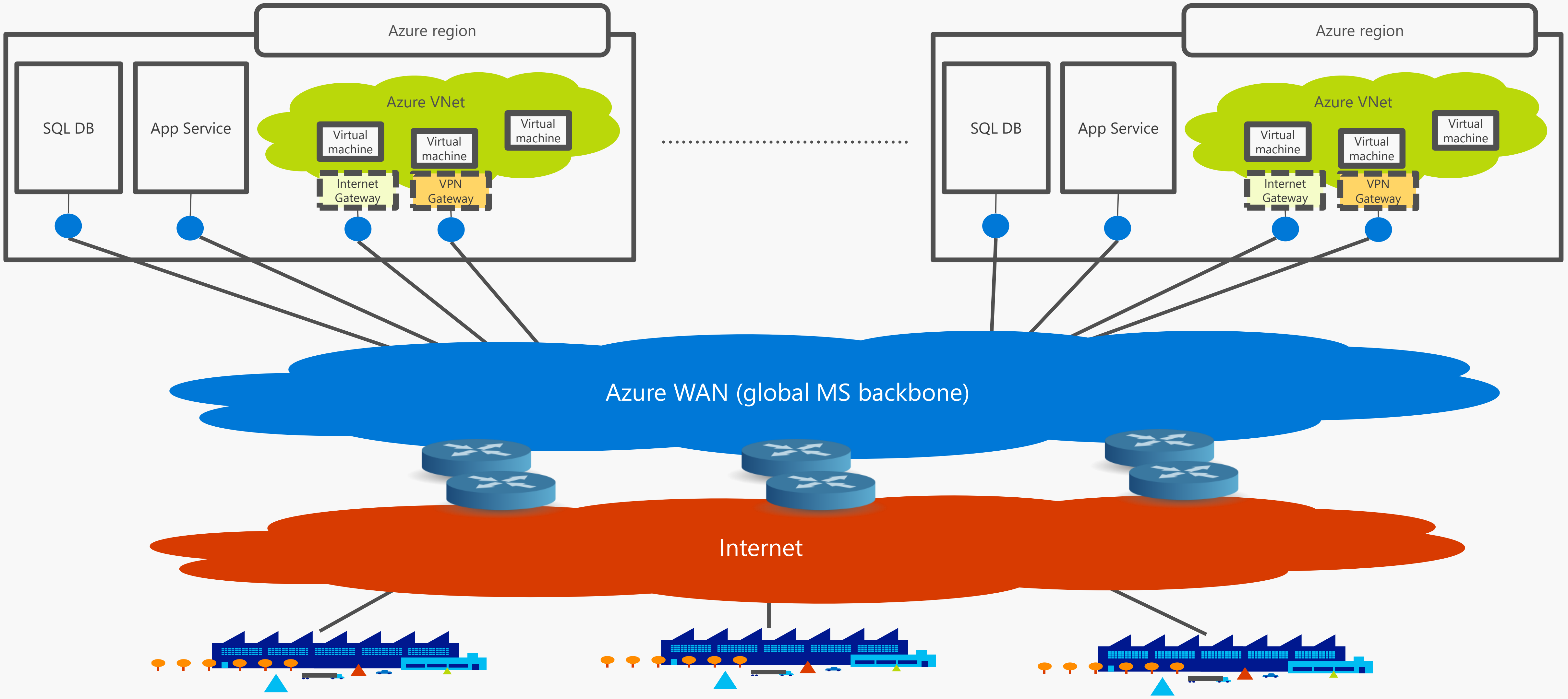
A platform-managed ***VPN gateway*** can be deployed to establish IPSec tunnels to VNets over the internet



Public IP address = remote tunnel endpoint to terminate IPSec tunnels

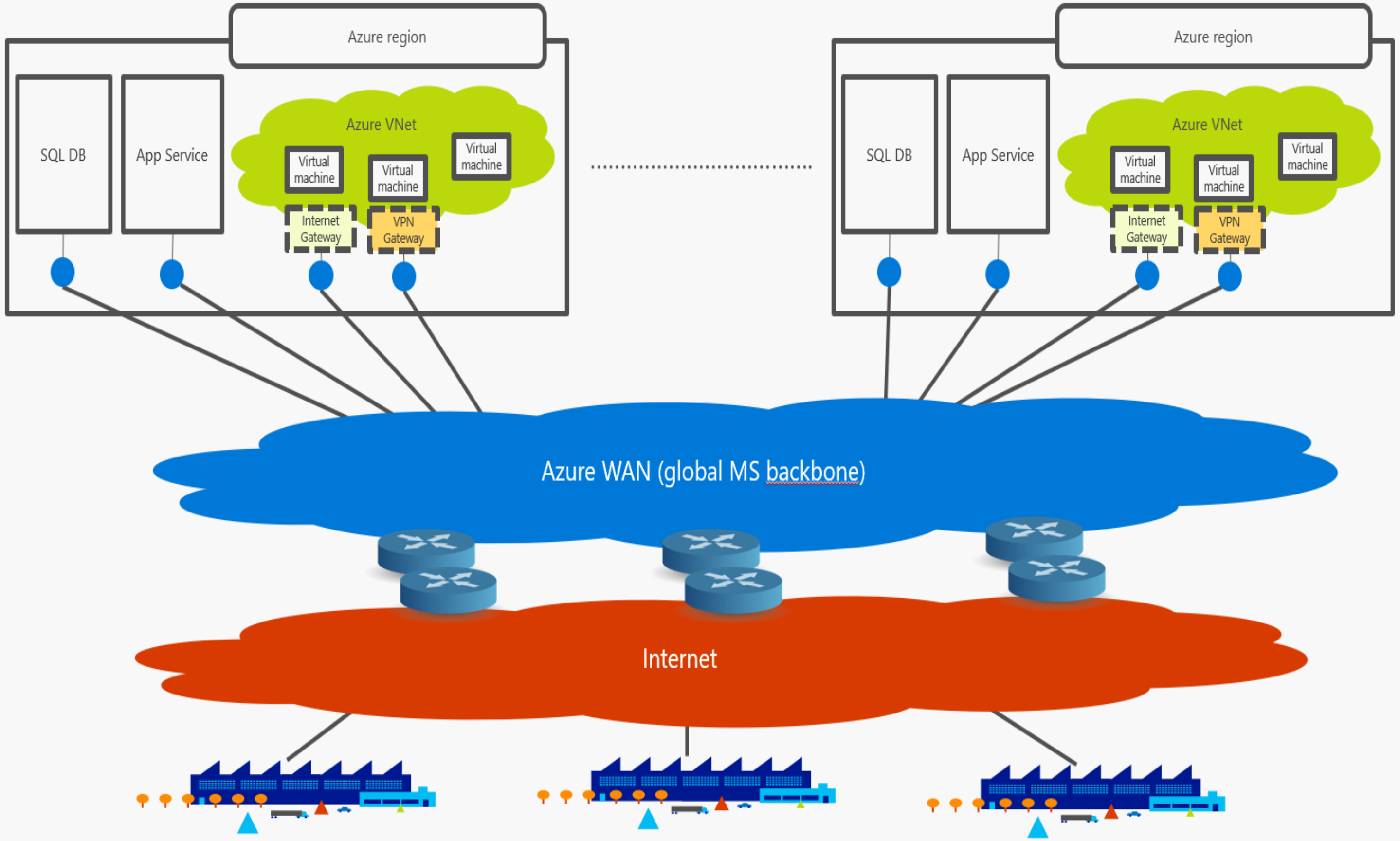
Azure high-level network architecture

The big picture



Azure high-level network architecture

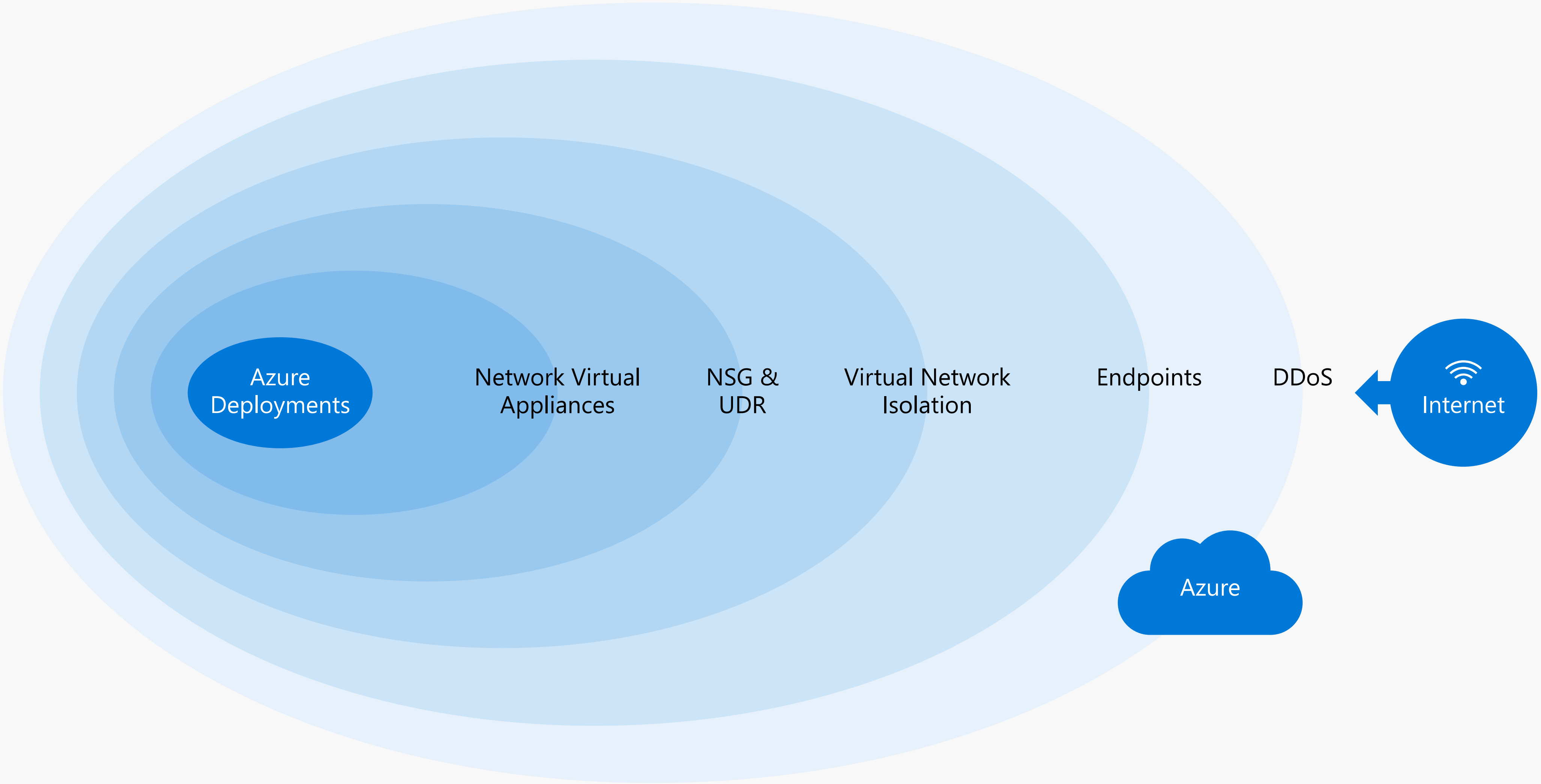
In review



Key takeaways

- Azure resources run in datacenter clusters (regions) available in 54 metros worldwide
- A global network privately owned by Microsoft connects all regions with each other and with the public internet
- Azure public services are exposed over public IP addresses belonging to the Microsoft network and are reachable from the internet
- Azure customers can build private network and connect them their corporate networks over internet-based VPNs

Logical layered isolation



...is inherent in Azure design

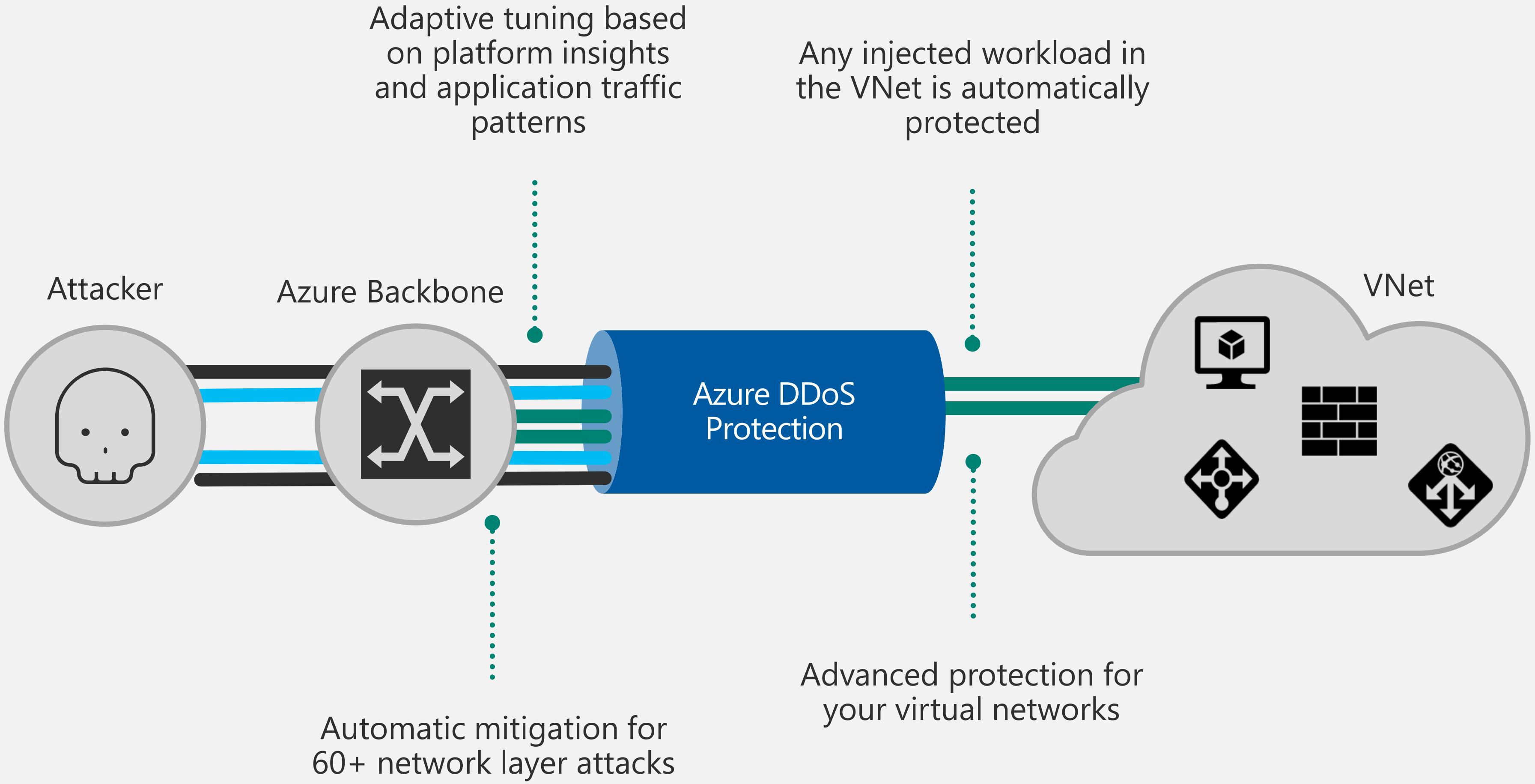
Protecting your application

From the Internet

Within the VNet

Within Azure

DDOS Protection


Adaptive tuning based on platform insights and application traffic patterns
Any injected workload in the VNet is automatically protected
Attacker
Azure Backbone
VNet
Azure DDoS Protection
Automatic mitigation for 60+ network layer attacks
Advanced protection for your virtual networks

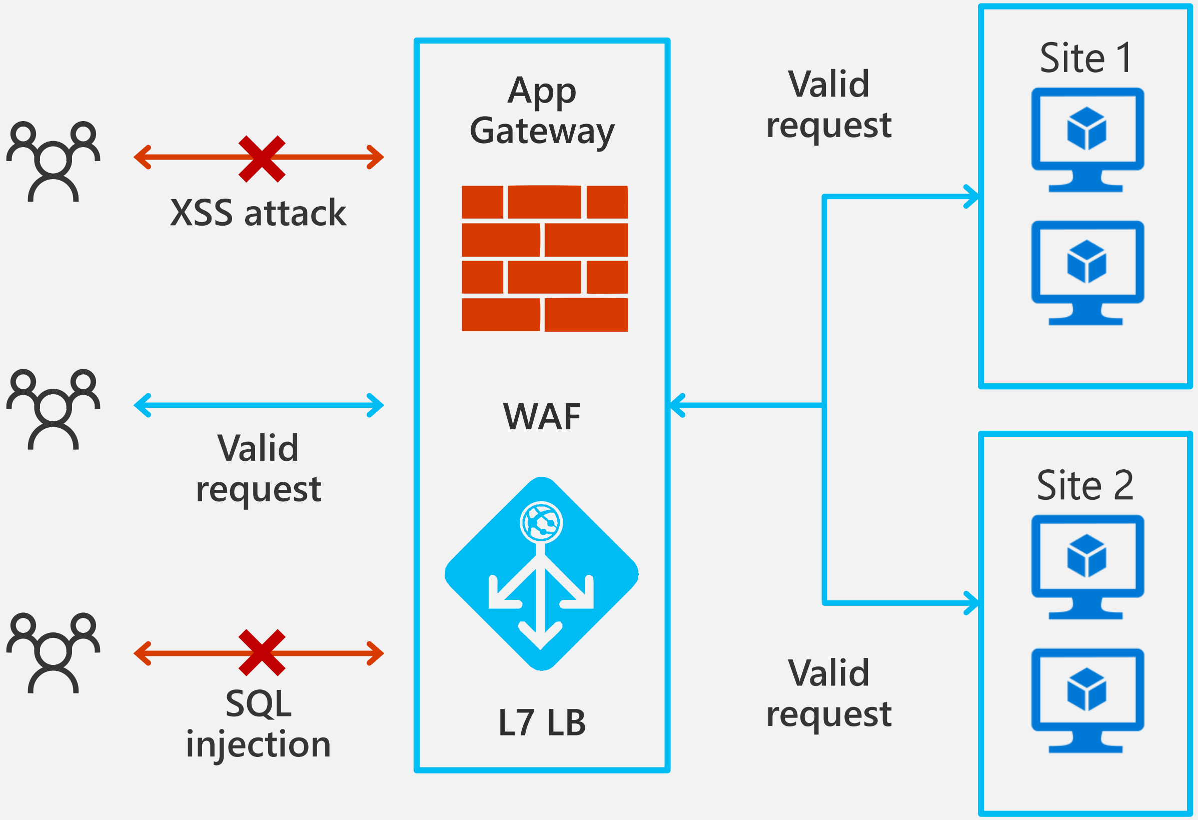
Protecting your application

From the Internet

Within the VNet

Within Azure

Web Application Firewall



Protect your app against prevalent X- Site Scripting and SQL Injection attacks

Blocks threats based on Top 10 OWASP signatures

Integrated with Azure Security Center

Real-time logging with Azure Monitor

Platform managed, scalable and highly available

Protecting your application

From the Internet

Within the VNet

Within Azure

Simplified Security Group Management

Network Security Groups (NSG)

IP based network ACL

Attach: Subnet and NICs

Service Tags

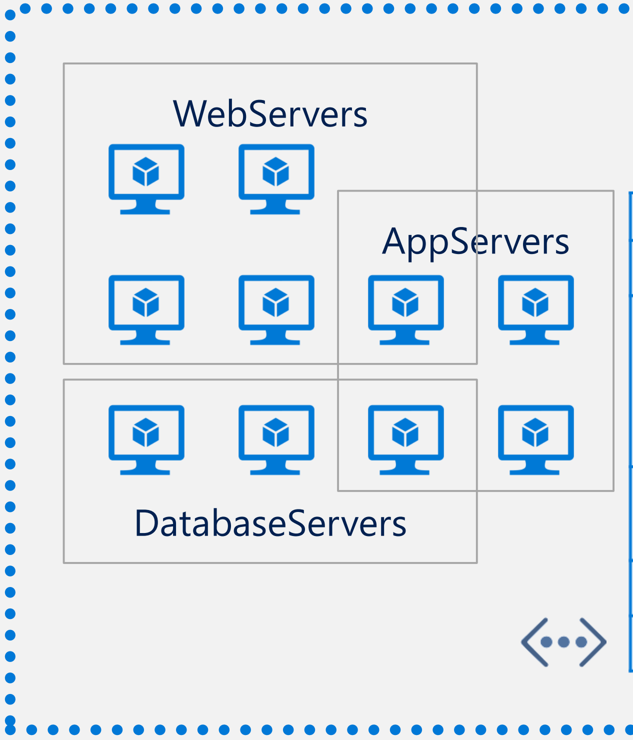
Named monikers for Azure service IPs

SQL, Storage, Traffic Manager supported

Application Security Groups (ASG)

Named monikers for custom grouping of VMs

Natural expression of application security



	Name	Source	Destination	Port
Allow	AllowInternetToWeb	Internet	WebServers	80,8080 (HTTP)
Allow	AllowAppToOnPrem	AppServers	10.10.128.0/22, 10.20.36.0/20, 192.168.65.0/20, 192.168.10.0/24	22, (SSH) 21, (FTP) 3389, (RDP) 3306 (MySQL)
Allow	AllowAppToExternalAPI	AppServers	148.234.0.0/16, 190.22.33.8/30	443 (HTTPS)
Allow	AllowDBServerToStorage	DatabaseServers	Storage	Any
Deny	DenyAll	Any	Any	Any

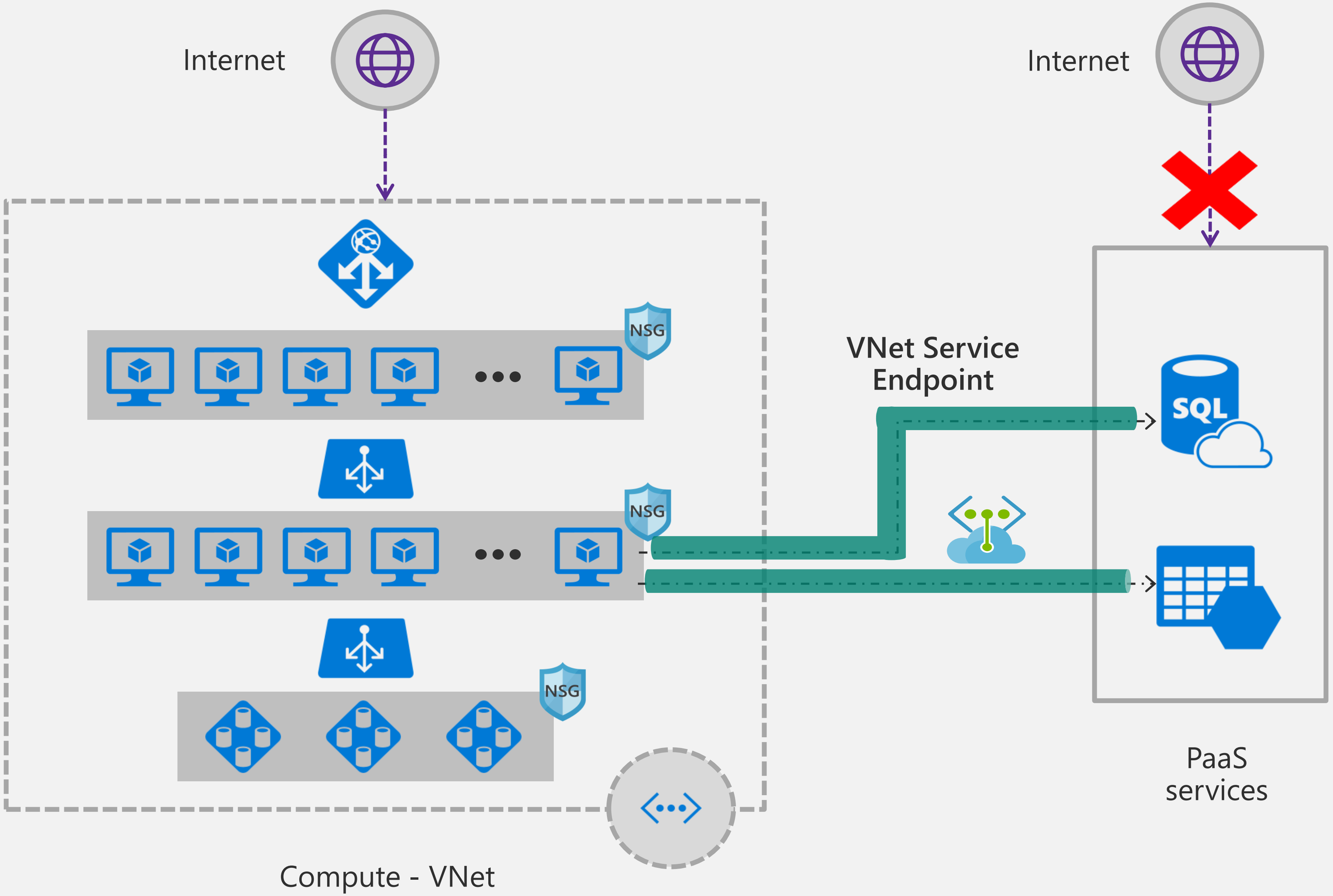
Protecting your application

From the Internet

Within the VNet

Within Azure

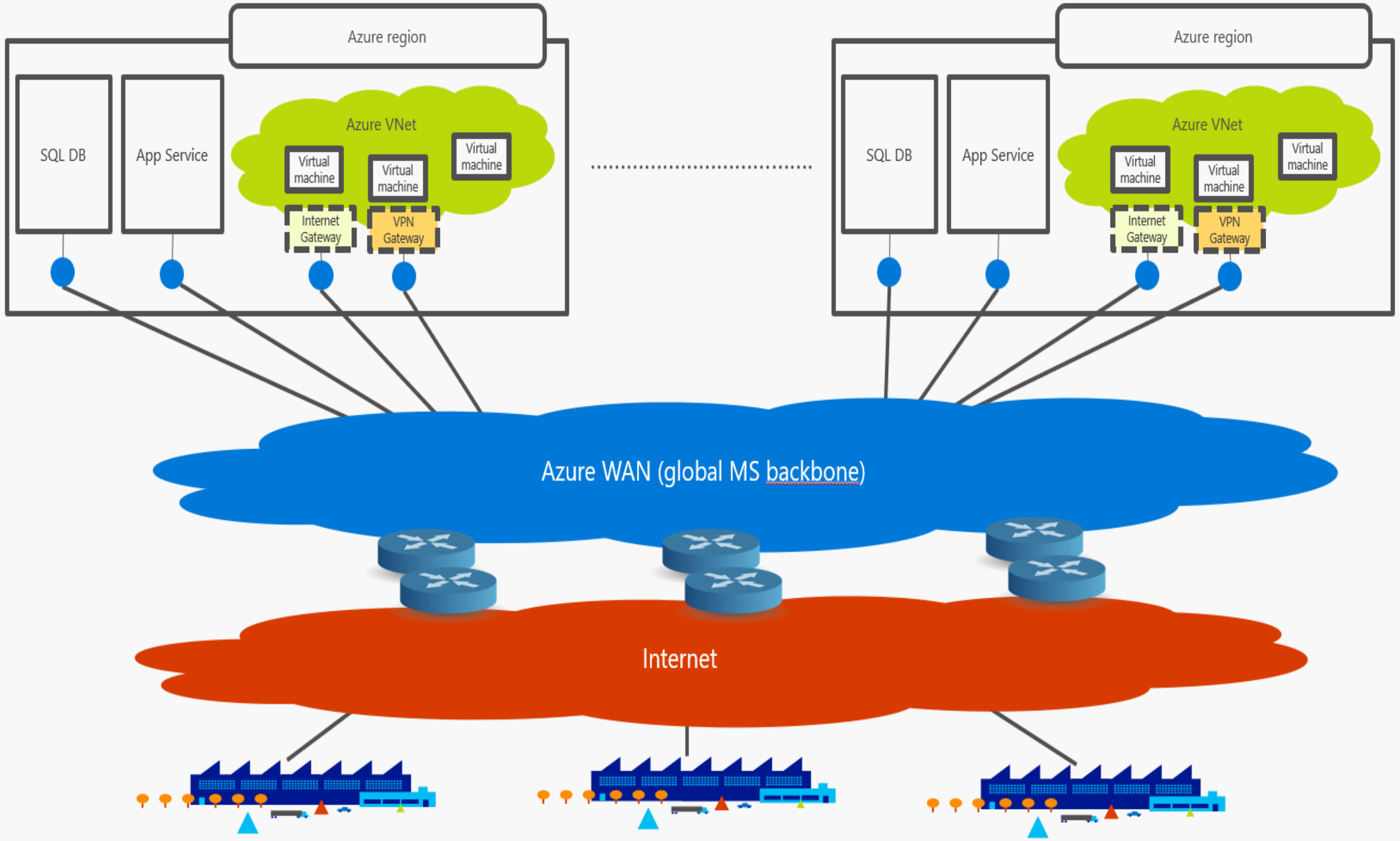
Securing PaaS Services



Expressroute fundamentals

Why Expressroute?

The need for enterprise-grade connectivity

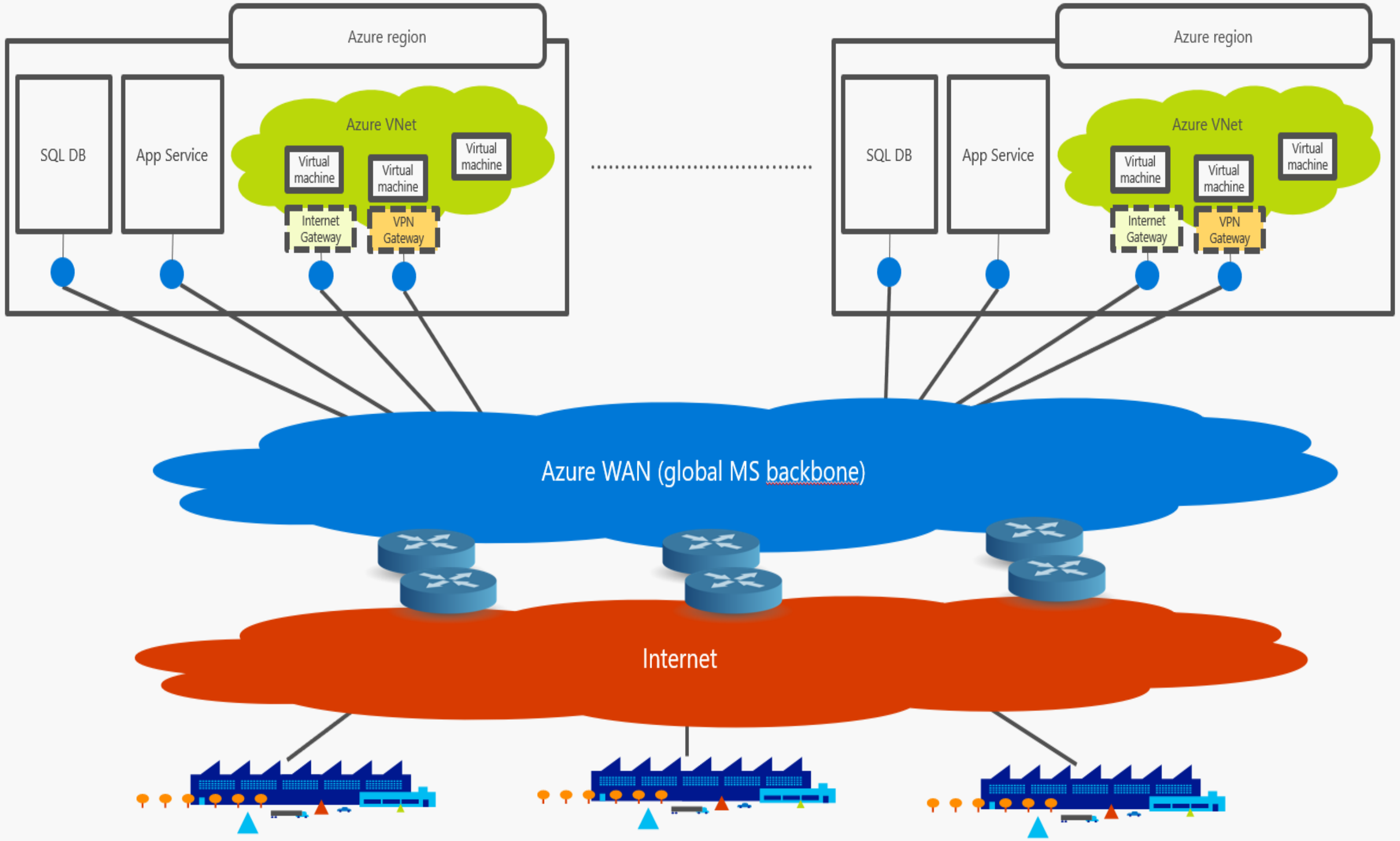


Enterprise-grade network; no congestion due to proactive bandwidth provisioning + aggressive traffic engineering (SWAN)

Private datacenter network, high bandwidth (10, 40, 100 Gb/s)

Why Expressroute?

The need for enterprise-grade connectivity



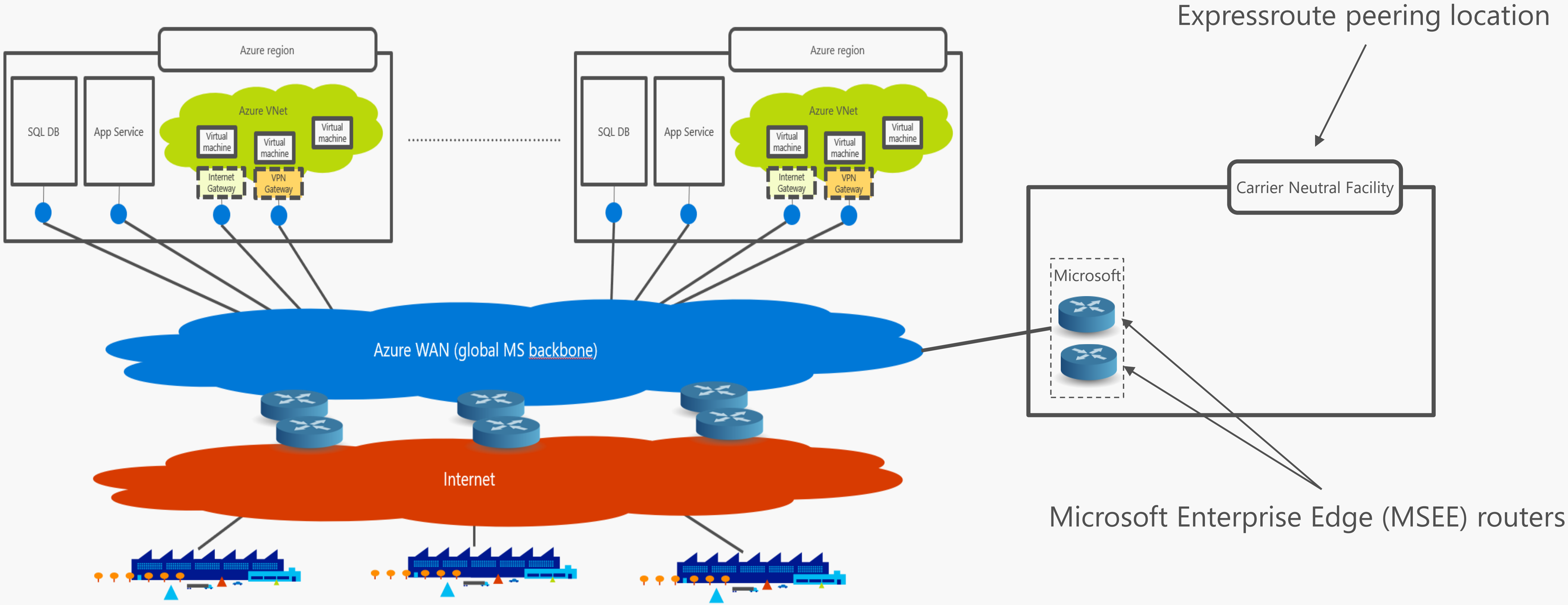
Enterprise-grade network; no congestion due to proactive bandwidth provisioning + aggressive traffic engineering (SWAN)

Best effort service (unpredictable performance) ⚠

Private datacenter network, high bandwidth (10, 40, 100 Gb/s)

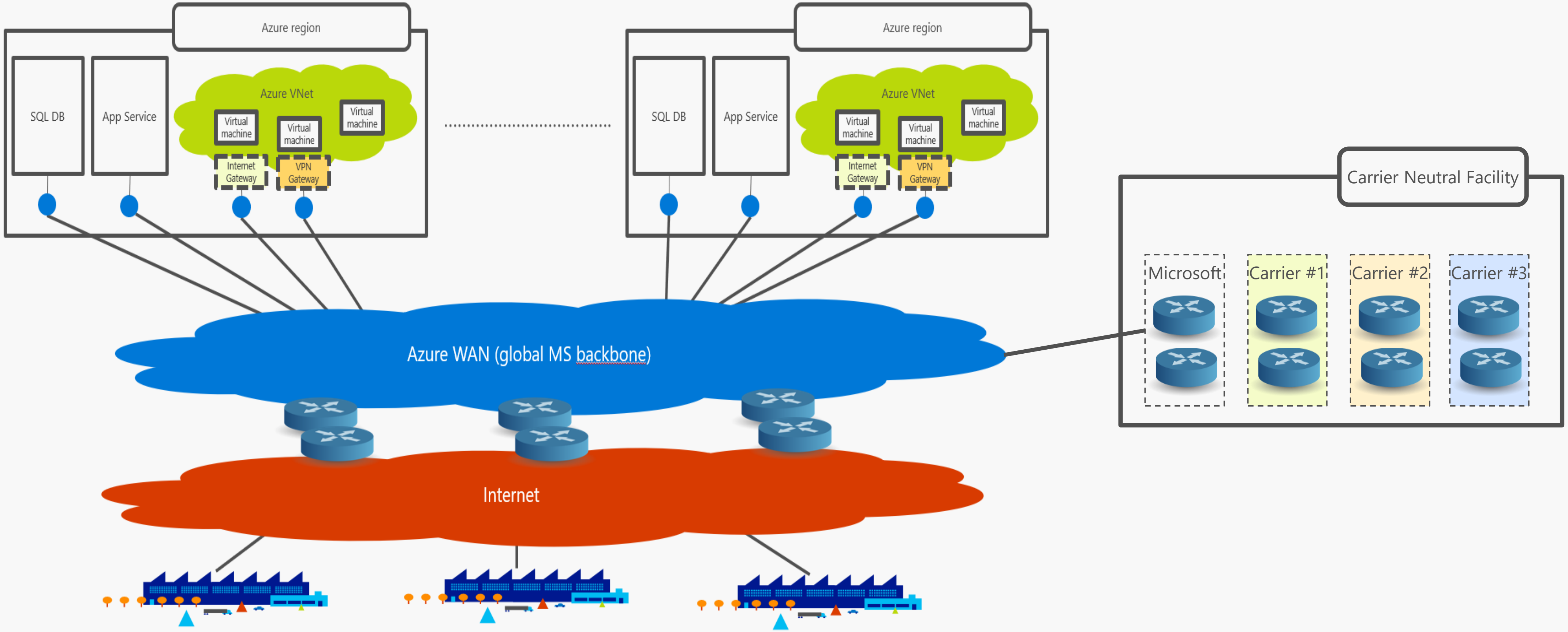
What is Expressroute?

Private connections to the Microsoft backbone



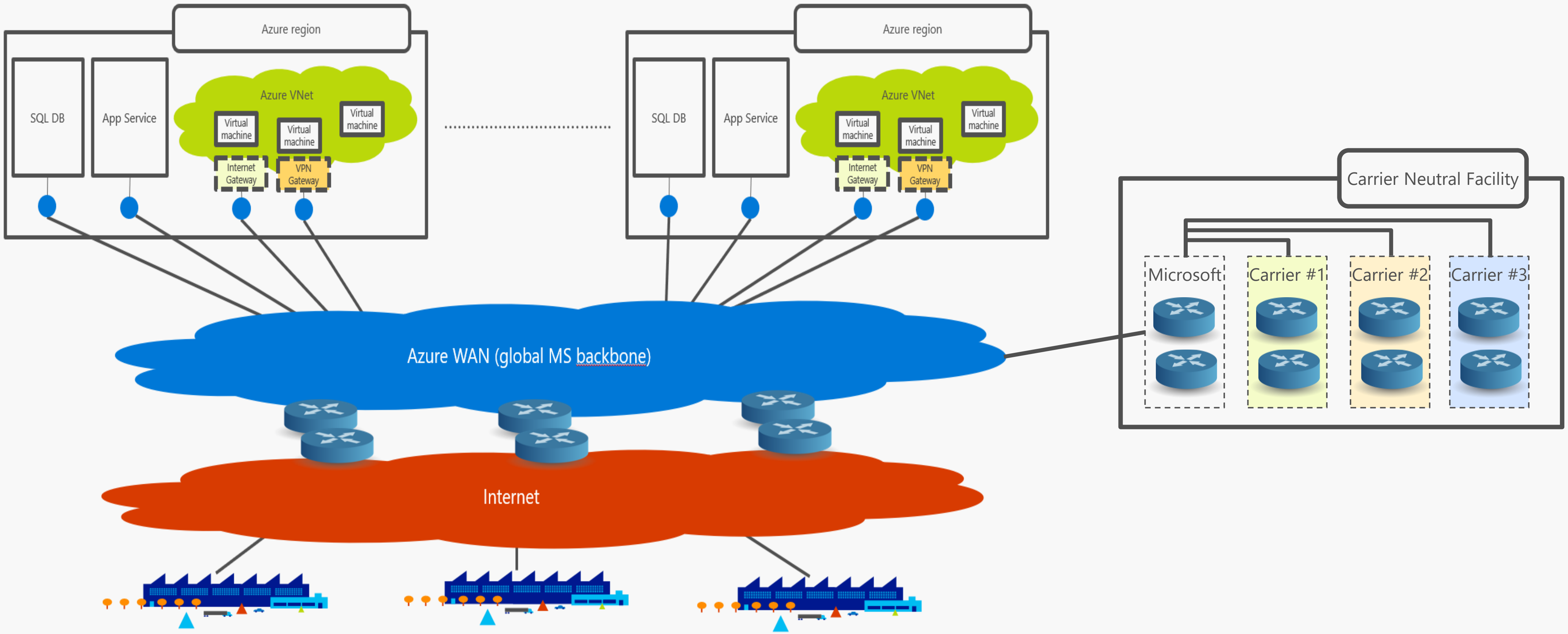
What is Expressroute?

Private connections to the Microsoft backbone



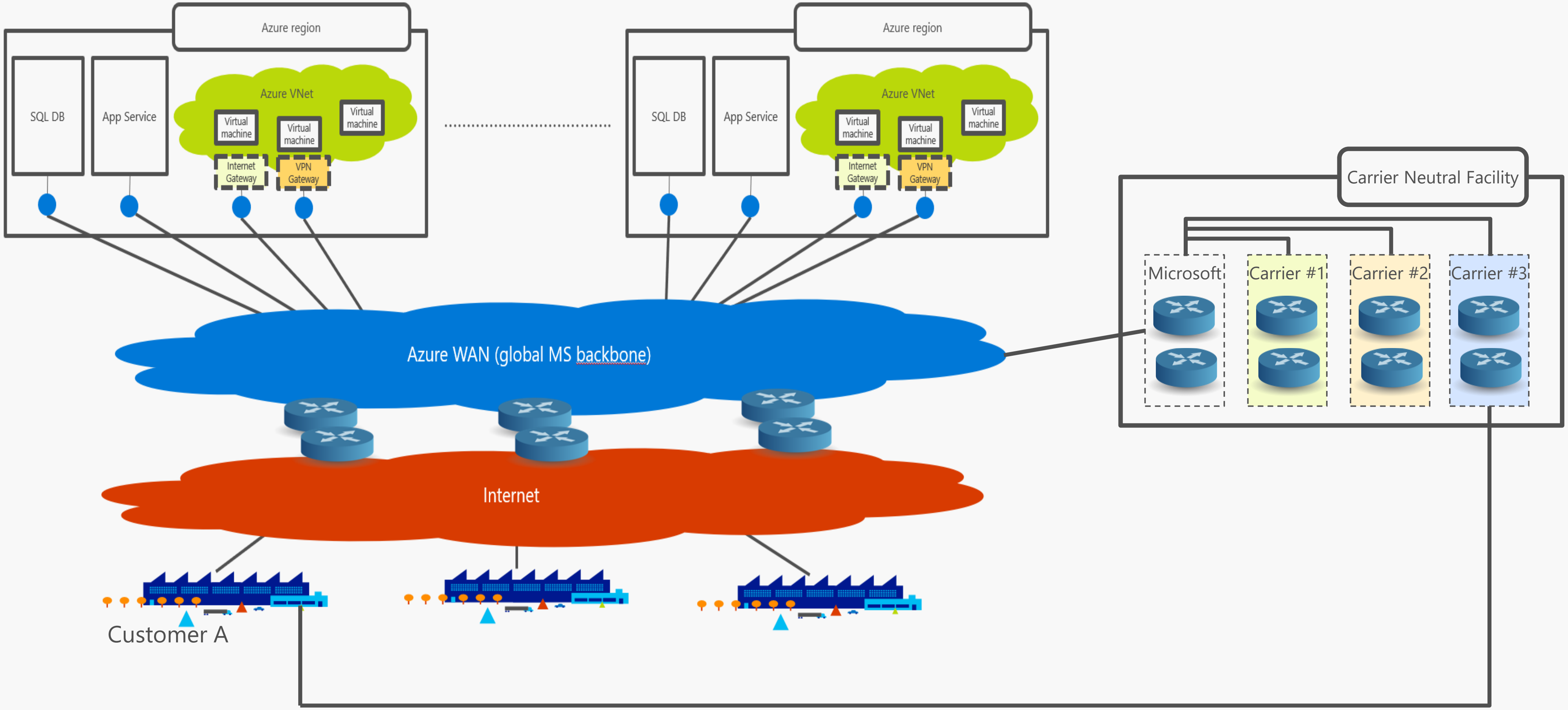
What is Expressroute?

Private connections to the Microsoft backbone



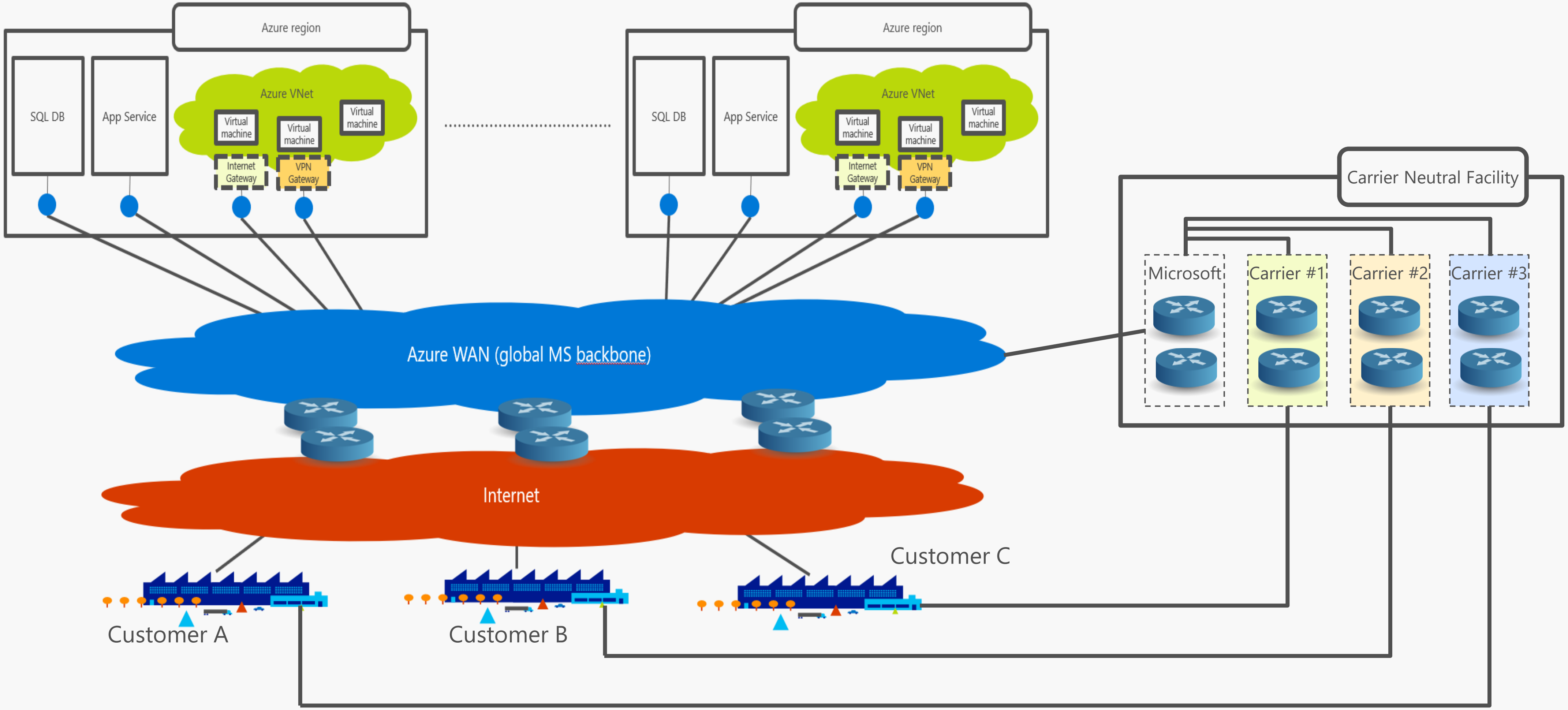
What is Expressroute?

Private connections to the Microsoft backbone



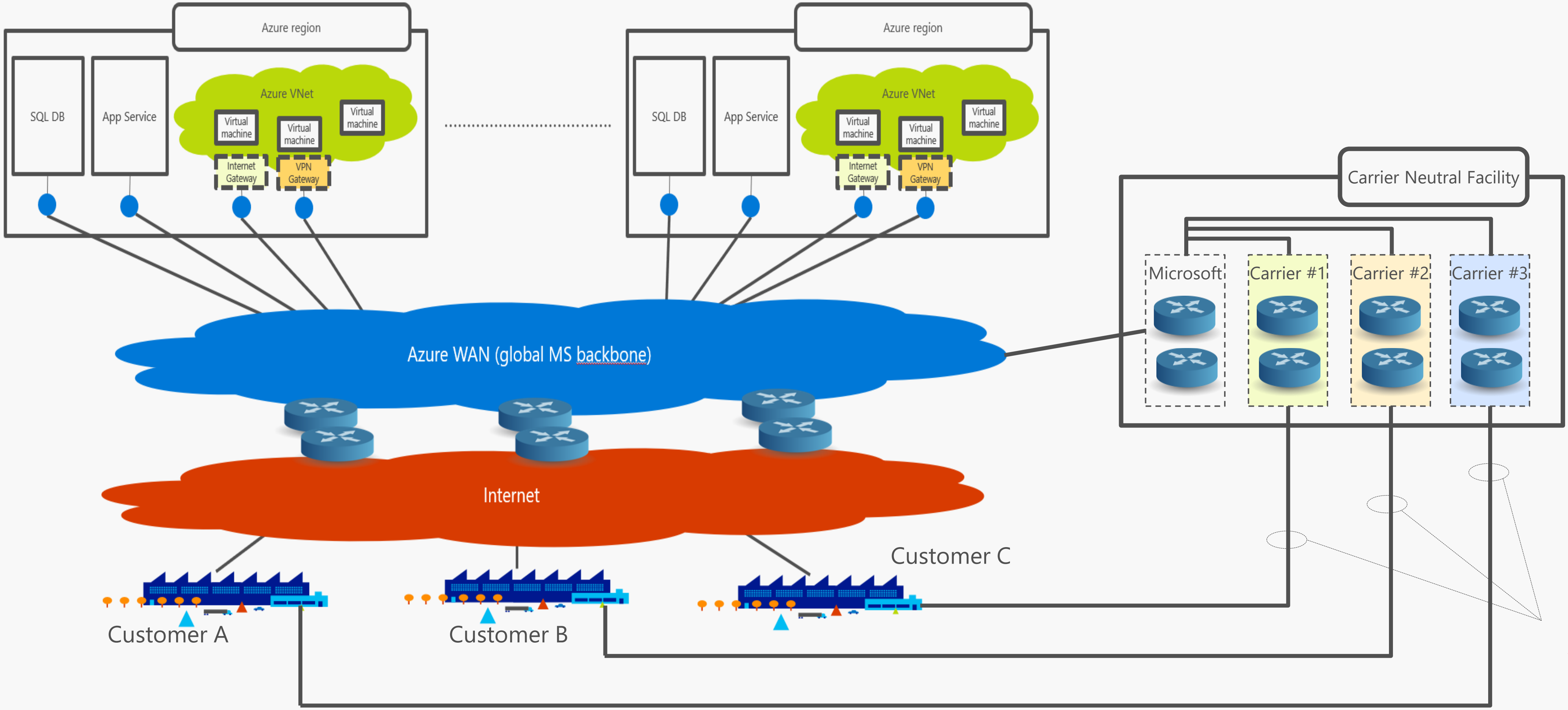
What is Expressroute?

Private connections to the Microsoft backbone



What is Expressroute?

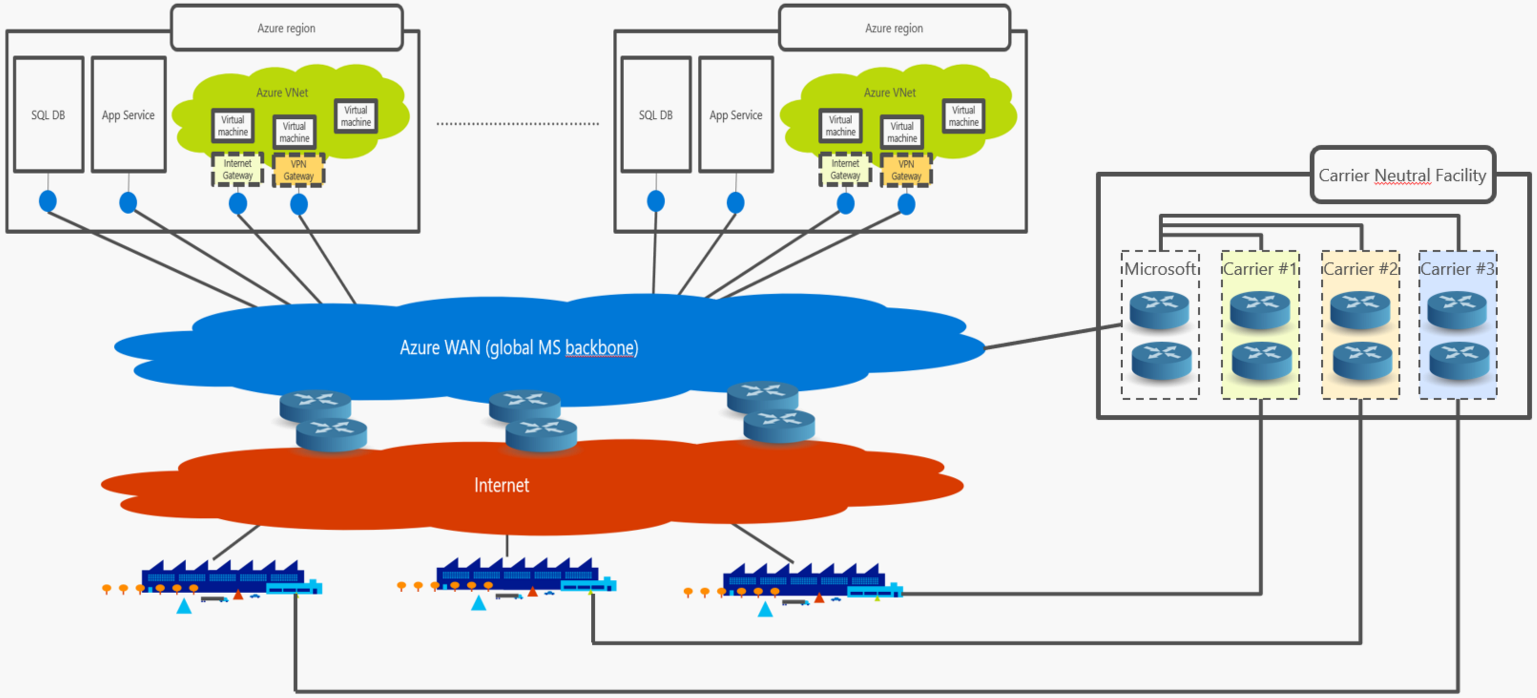
Private connections to the Microsoft backbone



dedicated bandwidth & predictable latency

Why Expressroute?

Value proposition & key benefits



- Expressroute allows customers to peer with the Microsoft network over dedicated links, ***bypassing the public internet***

- Customers get ***dedicated bandwidth*** on Microsoft routers

- Microsoft proactively manages capacity to ensure that bandwidth allocated to customers is always available => ***no congestion***

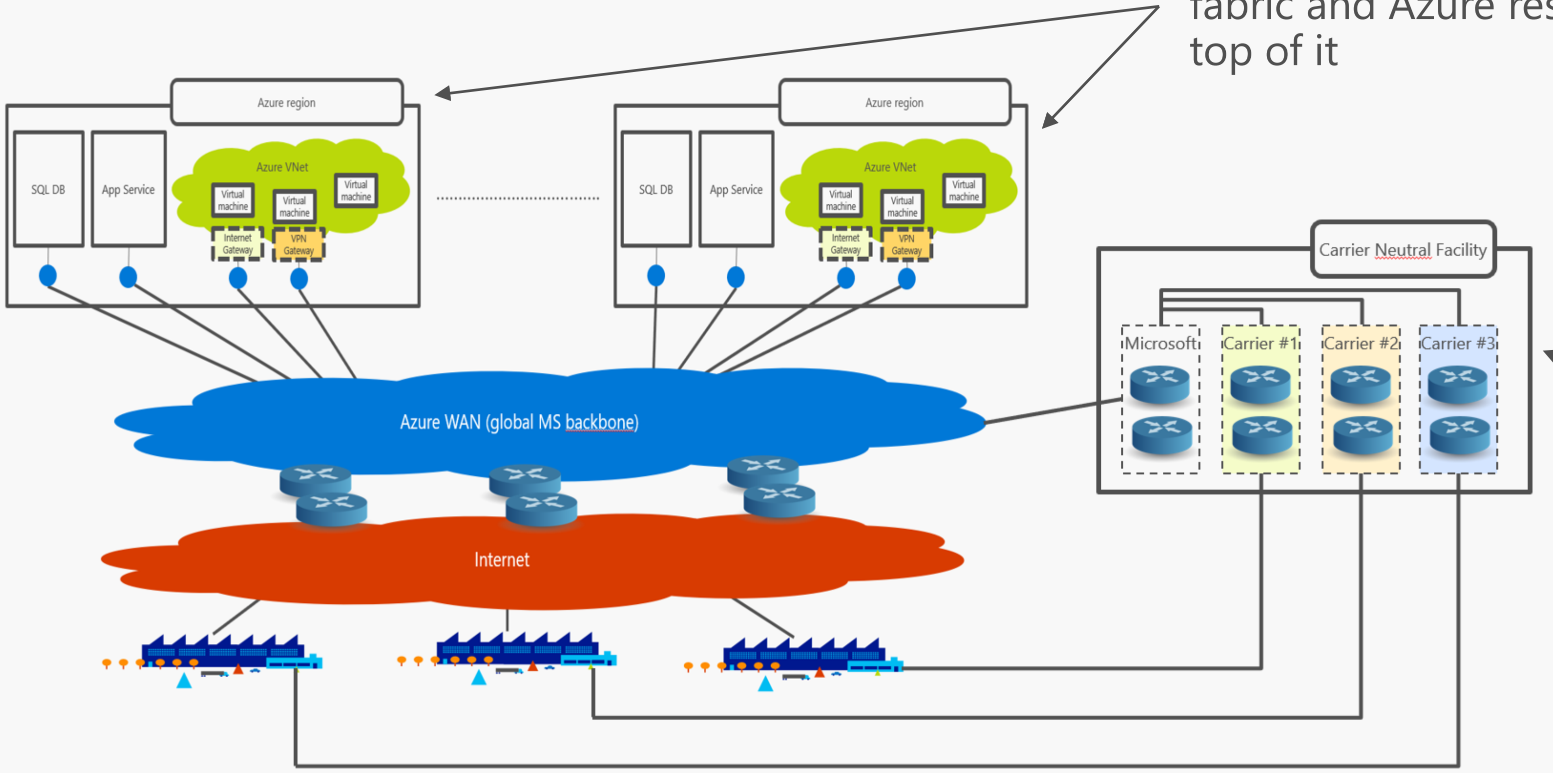
- Without congestion, ***latency and throughput are consistent over time*** and predictable

- Predictable latency is one of the ***key enablers for cloud adoption***

Expressroute key facts

#1: Peering locations are NOT Azure datacenters

Microsoft-managed DCs, hosting the Azure fabric and Azure resources deployed on top of it

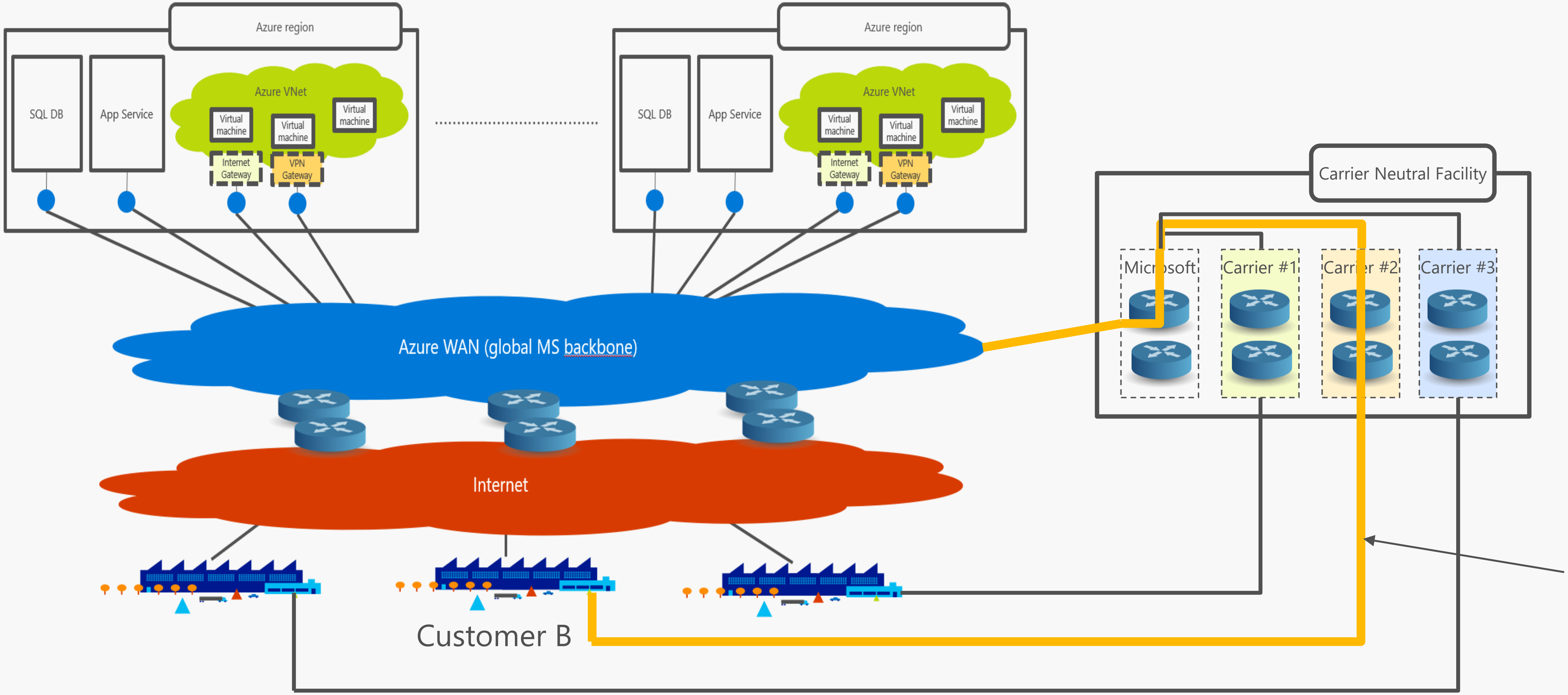


Facility owned & managed by third party

Microsoft is a customer, buys hosting space to deploy its ER routers

Expressroute key facts

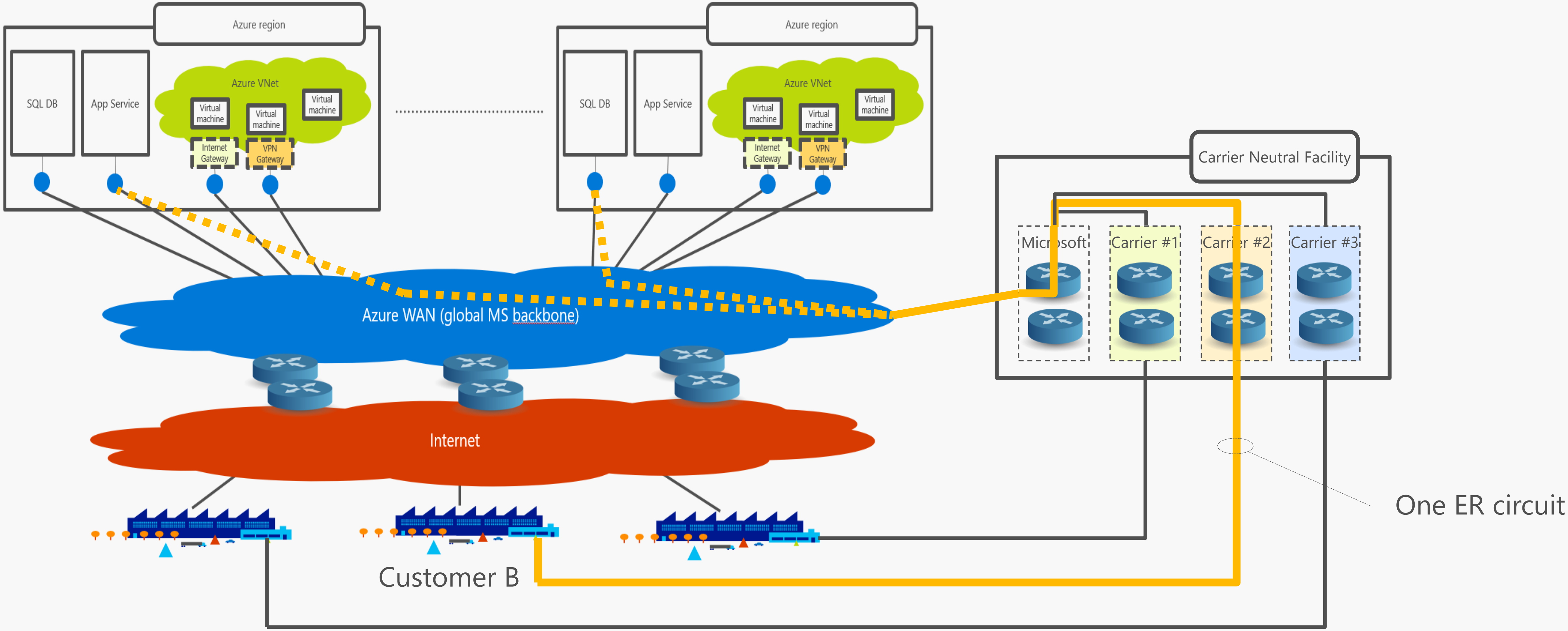
#2: An ER circuit is a connection the Microsoft network, not to a specific Azure region



ER connects Customer B's premises to the Microsoft network

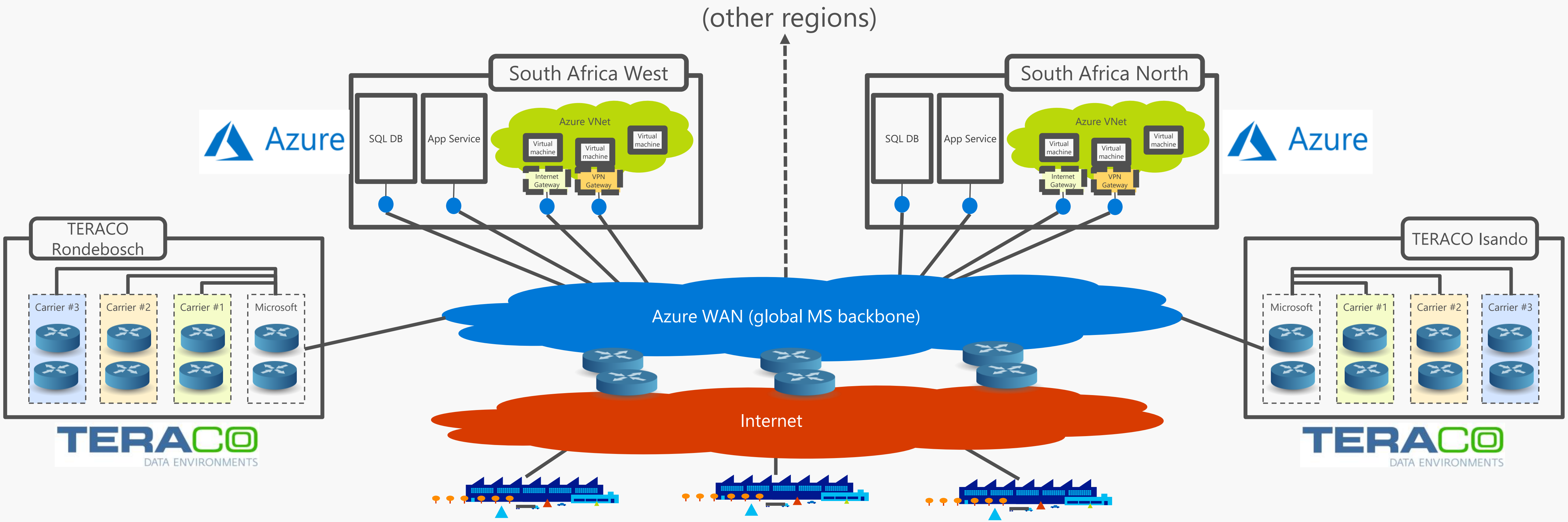
Expressroute key facts

#3: A single ER circuit provides access to resources in multiple Azure regions



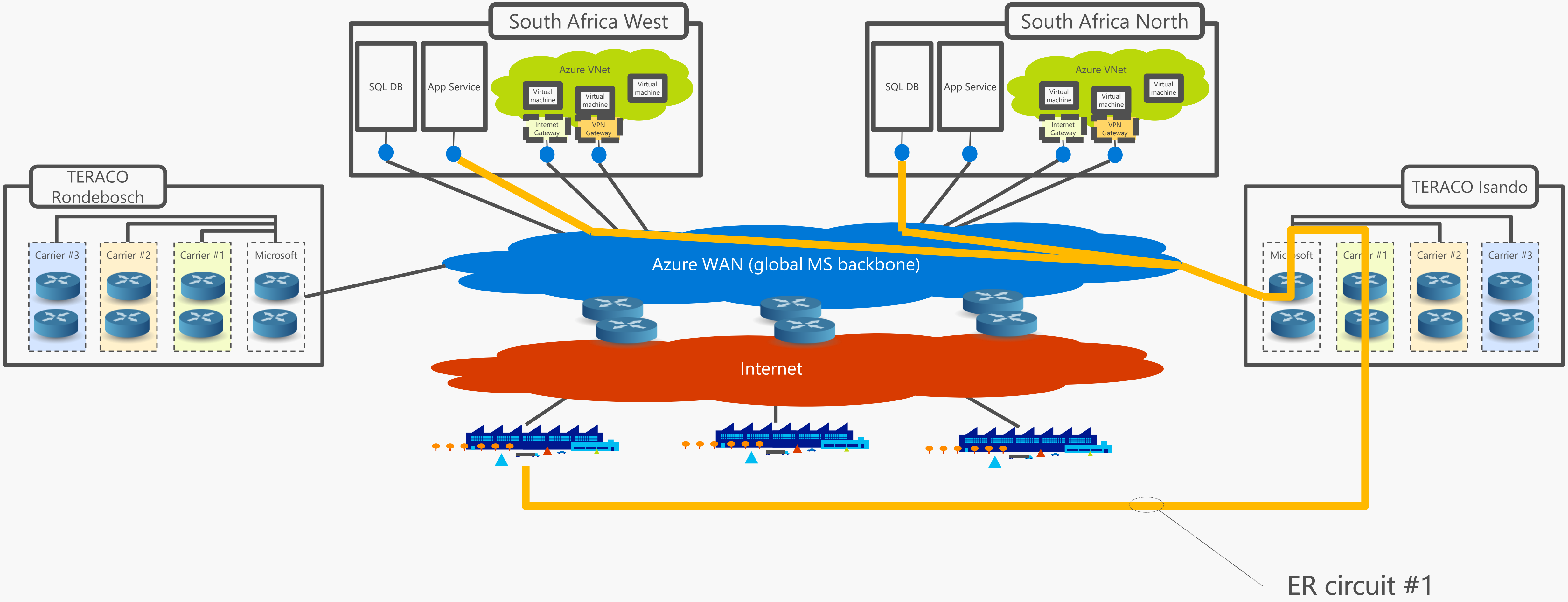
Expressroute in South Africa

Regions and peering locations



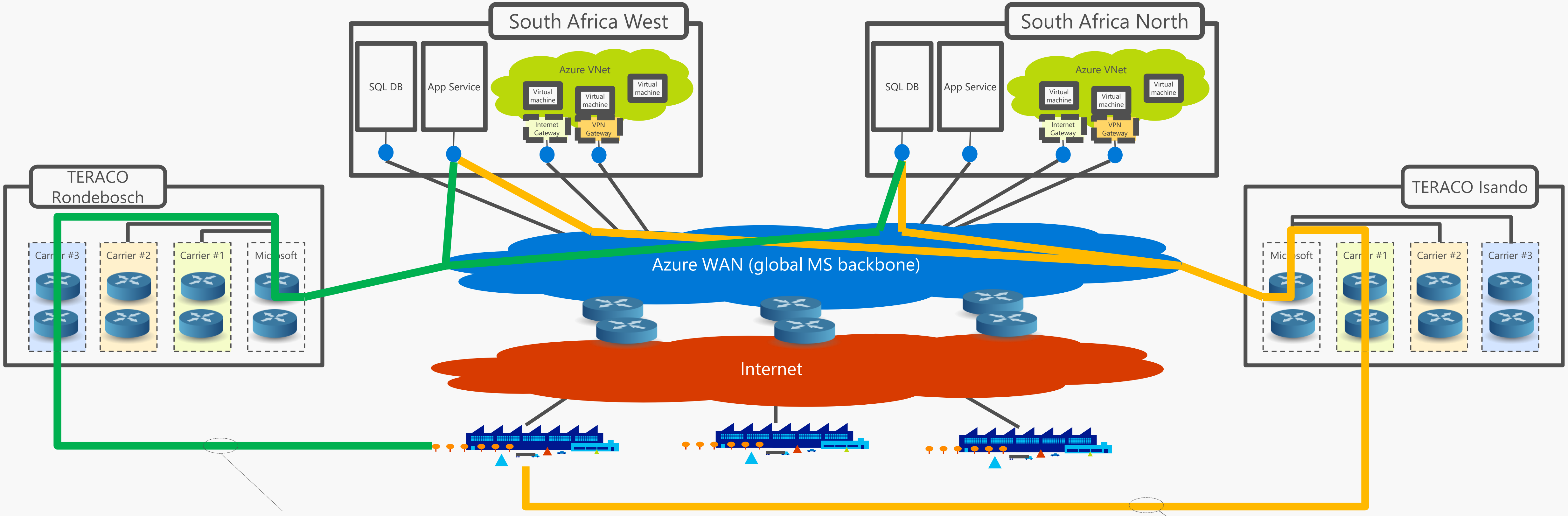
Expressroute in South Africa

Typical disaster-resilient implementation (two ER circuits)



Expressroute in South Africa

Typical disaster-resilient implementation (two ER circuits)



ER circuit #2 (carrier can be different than ER circuit #1)

ER circuit #1

Thank you

Matthew Levy

https://mattchatt.co.za

@skrods

https://www.linkedin.com/in/matthew-levy-170bbb21/