Microsoft

Azure Networking

Scan this QR-code to access **free educational resources, step-by-step learning guides** as well as get practical experience in **Azure Networking!**

https://aka.ms/AA8j3oi

Don’t forget to add **Microsoft Azure as a skill** to your LinkedIn account to stay connected with our developer community!!!

+ Microsoft Azure

We post the latest announcements about **free events for developers** in Ireland on our official Twitter account!

@MSDevIRL

LUNCH
LEARN

Cloud Lunch and Learn Sessions

Vaibhav
Gujral

Demystifying Azure Networking

1st June 2020 at 12 PM Coordinated Universal Time (UTC)

On Teams - https://bit.ly/35Bz3u1

In collaboration with

.NetMafia

CloudFamily

More info on our website: https://bit.ly/2yX21YW

office PNG Designed By 588ku from Pngtree.com

Demystifying Azure Networking

VAIBHAV GUJRAL

About Me

- 14 years of experience across designing and developing enterprise-class applications
- Microsoft Certified Azure Solutions Architect Expert
- Cloud Architect at Kiewit
- Organizer, Omaha Azure User Group
- Speaker | Blogger
- #AzureHeroes Community Hero
- http://www.vaibhavgujral.com
- @vabgujral
- linkedin.com/in/vaibhavgujral/

Microsoft CERTIFIED AZURE SOLUTIONS ARCHITECT EXPERT
Microsoft CERTIFIED AZURE DEVOPS ENGINEER EXPERT
Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE
Microsoft CERTIFIED AZURE ADMINISTRATOR ASSOCIATE
Microsoft CERTIFIED AZURE DEVELOPER ASSOCIATE
Microsoft CERTIFIED AZURE FUNDAMENTALS

Agenda

- Azure Regions and data centers
- Virtual Networks
- VPN Gateways
- Network Filtering
- Routing
- Load Balancing Options
- Network Monitoring

Understanding Azure Regions

Data Centers

A data center is a building or group of buildings used to house physical infrastructure including racks, switches etc.

Regions

A region is a set of datacenters deployed within a latency-defined perimeter and connected through a dedicated regional low-latency network (< 2ms).

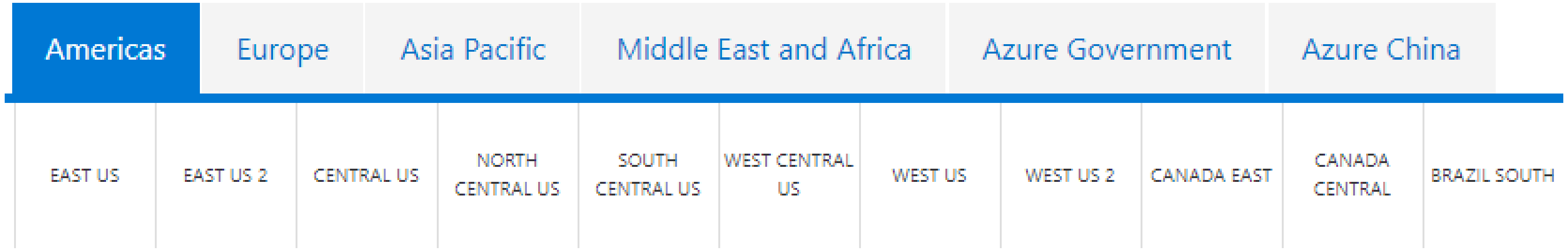
Geographies

A geography is a discrete market, typically containing two or more regions, that preserves data residency and compliance boundaries.

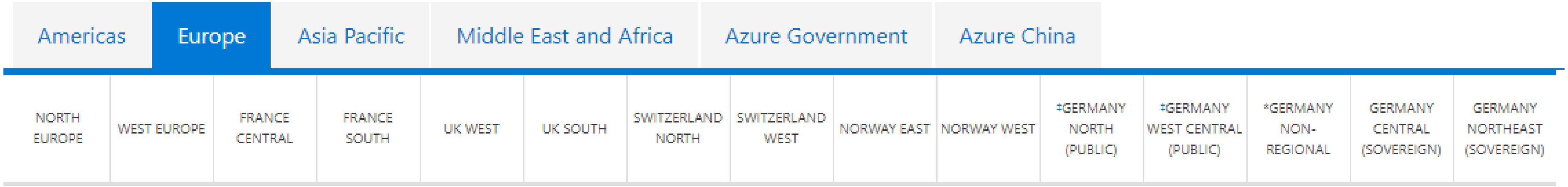
Availability Zones

Availability Zones are physically separate locations within an Azure region. Each Availability Zone is made up of one or more datacenters equipped with independent power, cooling, and networking.

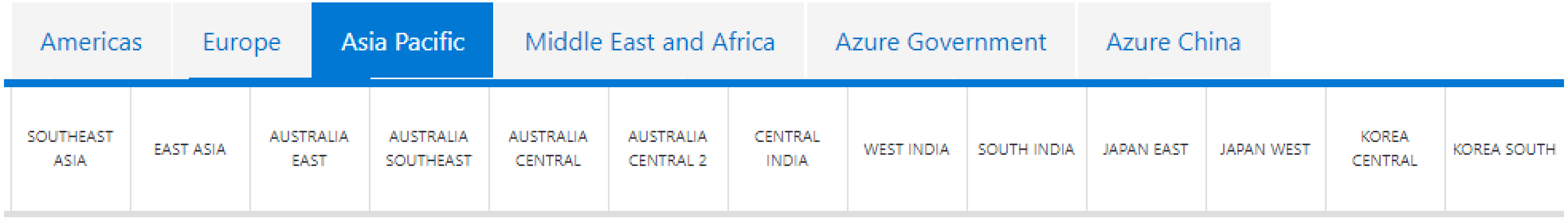
Understanding Azure Regions



EAST US	EAST US 2	CENTRAL US	NORTH CENTRAL US	SOUTH CENTRAL US	WEST CENTRAL US	WEST US	WEST US 2	CANADA EAST	CANADA CENTRAL	BRAZIL SOUTH



NORTH EUROPE	WEST EUROPE	FRANCE CENTRAL	FRANCE SOUTH	UK WEST	UK SOUTH	SWITZERLAND NORTH	SWITZERLAND WEST	NORWAY EAST	NORWAY WEST	‡GERMANY NORTH (PUBLIC)	‡GERMANY WEST CENTRAL (PUBLIC)	*GERMANY NON-REGIONAL	GERMANY CENTRAL (SOVEREIGN)	GERMANY NORTHEAST (SOVEREIGN)

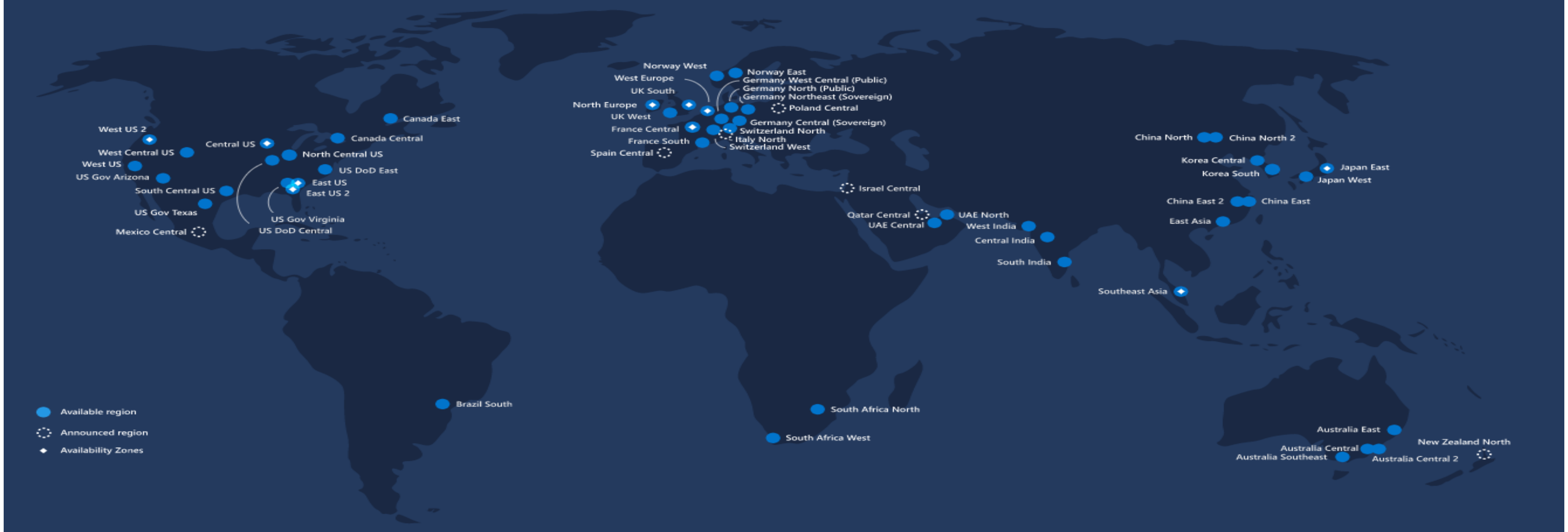


SOUTHEAST ASIA	EAST ASIA	AUSTRALIA EAST	AUSTRALIA SOUTHEAST	AUSTRALIA CENTRAL	AUSTRALIA CENTRAL 2	CENTRAL INDIA	WEST INDIA	SOUTH INDIA	JAPAN EAST	JAPAN WEST	KOREA CENTRAL	KOREA SOUTH

Global Presence

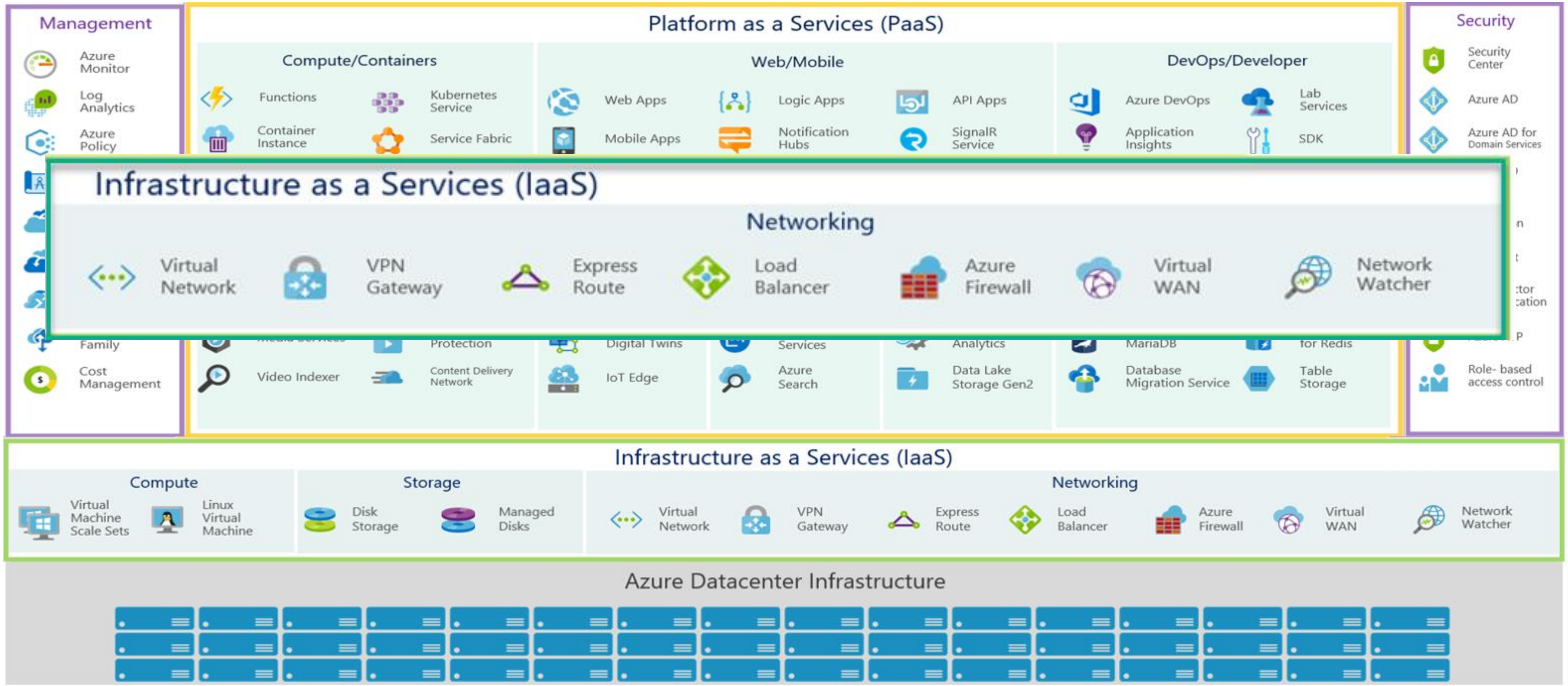
60+ regions worldwide **140** available in 140 countries

https://azure.microsoft.com/en-us/global-infrastructure/



* Three Azure Government Secret region locations undisclosed

Azure Services



Management
Azure Monitor
Log Analytics
Azure Policy
Family
Cost Management

Platform as a Services (PaaS)

Compute/Containers
Functions
Kubernetes Service
Container Instance
Service Fabric
Protection
Video Indexer
Content Delivery Network

Web/Mobile
Web Apps
Logic Apps
API Apps
Mobile Apps
Notification Hubs
SignalR Service
Digital Twins
Services
Analytics
IoT Edge
Azure Search
Data Lake Storage Gen2

DevOps/Developer
Azure DevOps
Lab Services
Application Insights
SDK
MariaDB
for Redis
Database Migration Service
Table Storage

Security
Security Center
Azure AD
Azure AD for Domain Services
Role- based access control

Infrastructure as a Services (IaaS)

Networking
Virtual Network
VPN Gateway
Express Route
Load Balancer
Azure Firewall
Virtual WAN
Network Watcher

Infrastructure as a Services (IaaS)

Compute
Virtual Machine Scale Sets
Linux Virtual Machine

Storage
Disk Storage
Managed Disks

Networking
Virtual Network
VPN Gateway
Express Route
Load Balancer
Azure Firewall
Virtual WAN
Network Watcher

Azure Datacenter Infrastructure

Azure Virtual Network

Azure Virtual Network is the fundamental building block for private network in Azure

Supports RFC 1918 IP address spaces (https://tools.ietf.org/html/rfc1918)

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

You define the IP address ranges for your virtual network using Classless Inter-Domain Routing(CIDR) notation.

- *192.168.100.14/24*
    - 256 IP addresses ($2^{(32-n)}$)
    - 192.168.100.0 – 192.168.100.255

You can have up to 65536 private IP addresses per virtual network

Azure Virtual Network

Use subnets for network segmentation within your virtual network

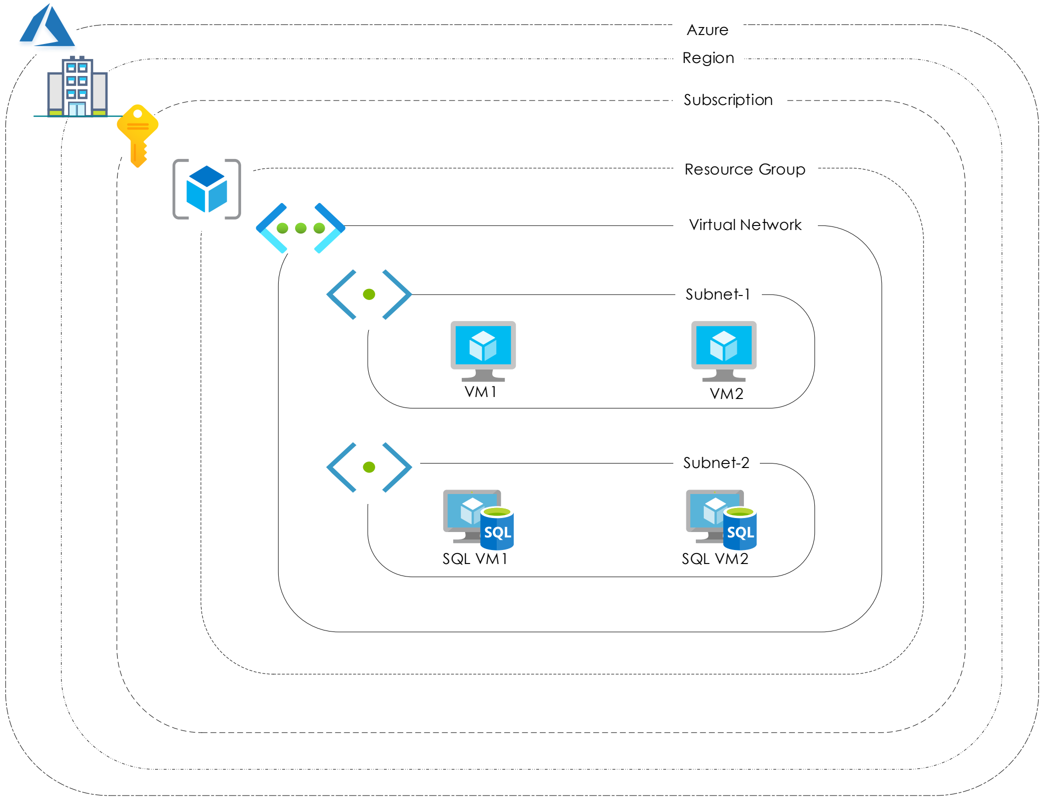
VNet is scoped to a single region and subscription

Avoid overlapping address spaces with other VNets or your on-prem networks

All resources in a VNet can communicate outbound to the internet, by default.

Inbound communication to a resource from internet takes place by assigning a public IP address or a public Load Balancer.

You can also use public IP or public Load Balancer to manage your outbound connections.



Azure Virtual Networks

Best Practices:

1. Avoid non-overlapping address spaces.
2. Ensure subnets don’t cover the entire address space of the VNet. Reserve some address space for the future
3. Better to have fewer large VNets than multiple small VNets to avoid management issues.
4. Secure your VNets with Network Security Groups (NSGs)

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-vnet-plan-design-arm

VPN Gateway

Used to send encrypted traffic between Azure Virtual Networks over the Microsoft network or an Azure virtual network and an on-premises location over the public Internet.

Uses a specific subnet called the gateway subnet in which Virtual machines running gateway services are deployed

Two types:

1. Vpn:
2. ExpressRoute:

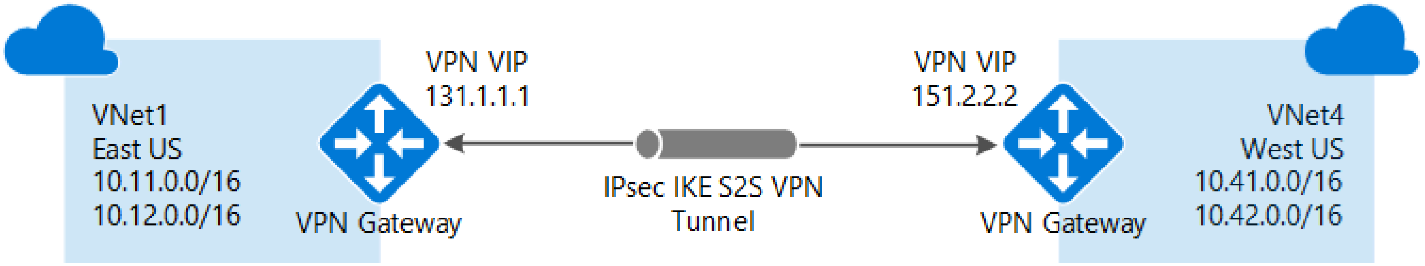
Each VPN can have only one VPN gateway, whereas a VPN gateway can have multiple connections.

A VPN can have one VPN gateway and one express route gateway

VPN Gateway

Connectivity options through VPN Gateway:

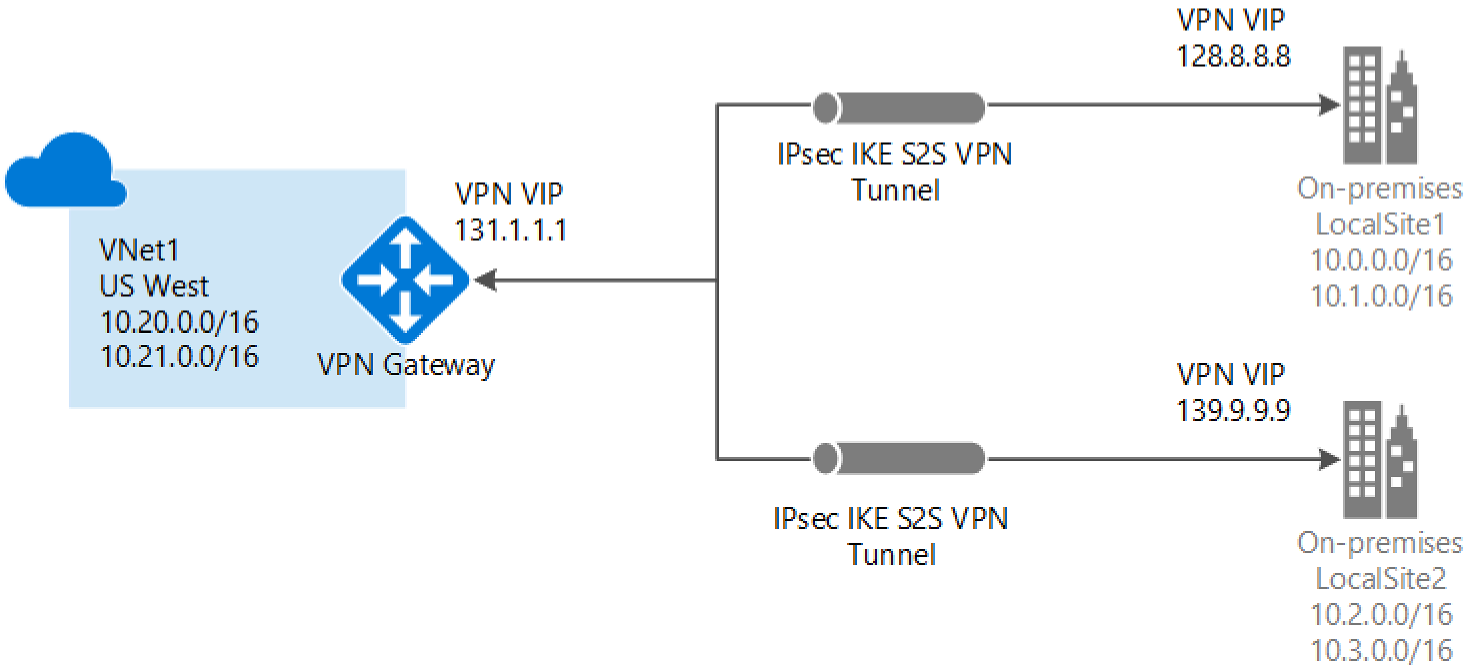
1. VNet-to-VNet: an IPsec/IKE VPN tunnel connection between that VPN gateway and another VPN gateway. The VNets can be:
   - in the same or different regions
   - in the same or different subscriptions
   - in the same or different deployment models



VPN Gateway

Connectivity options through VPN Gateway:

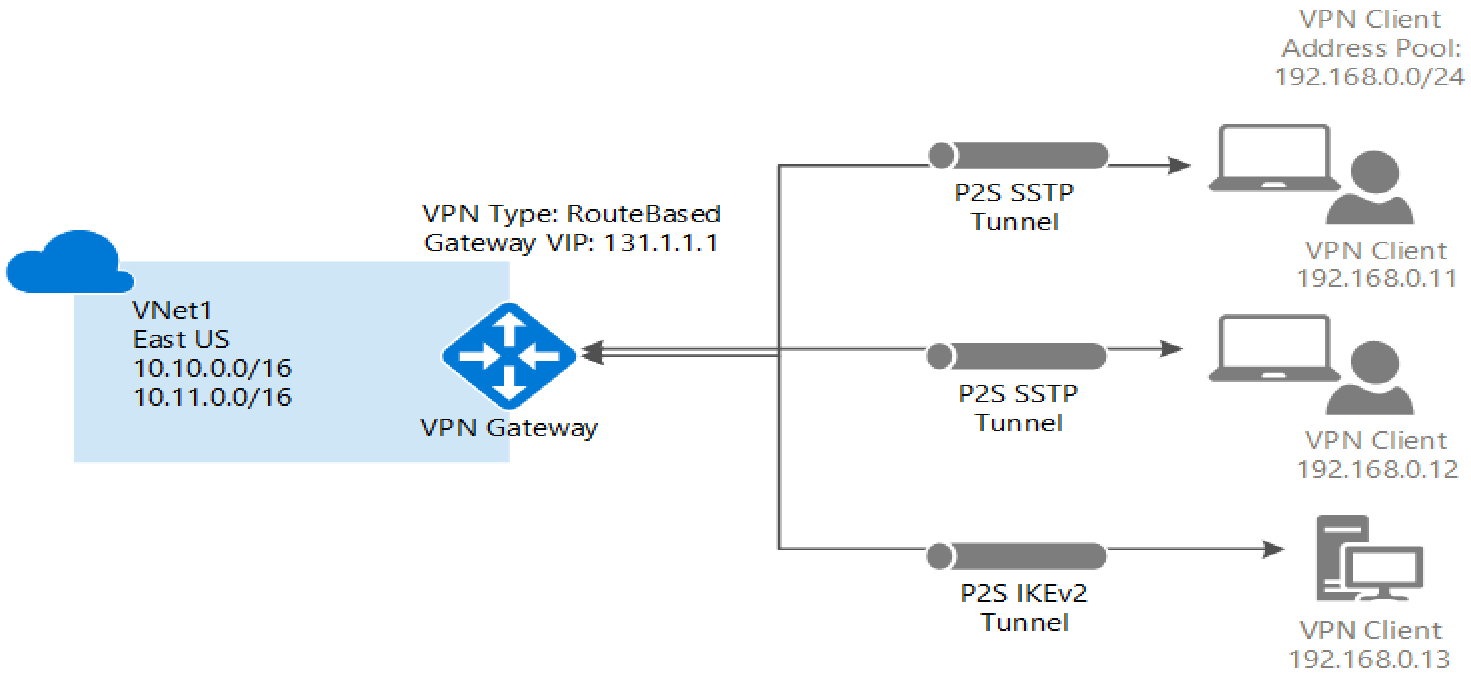
2. Site-to-Site: a cross-premises IPsec/IKE VPN tunnel connection between the VPN gateway and an on-premises VPN device.



VPN Gateway

Connectivity options through VPN Gateway:

3. Point-to-Site: connect virtual network from an individual client computer



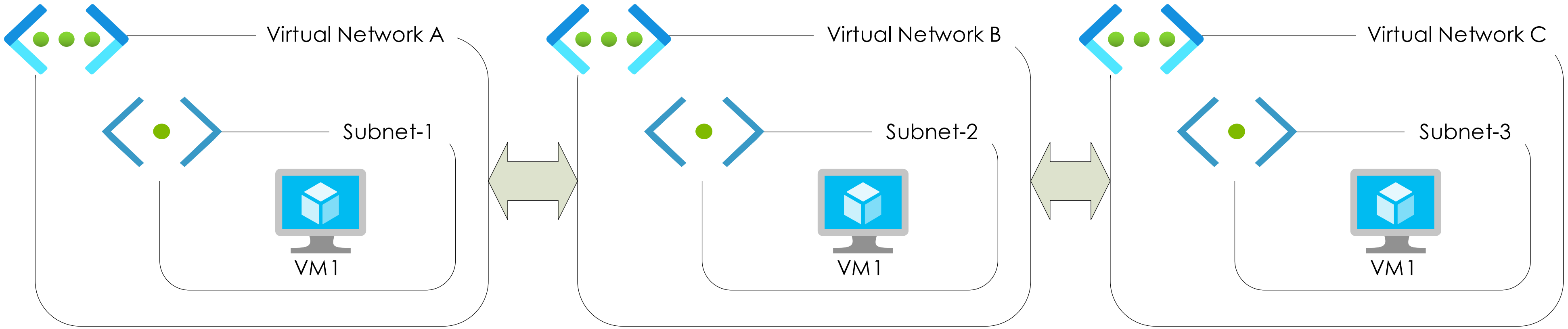
VNet Peering

Connect Virtual Networks without a virtual network gateway

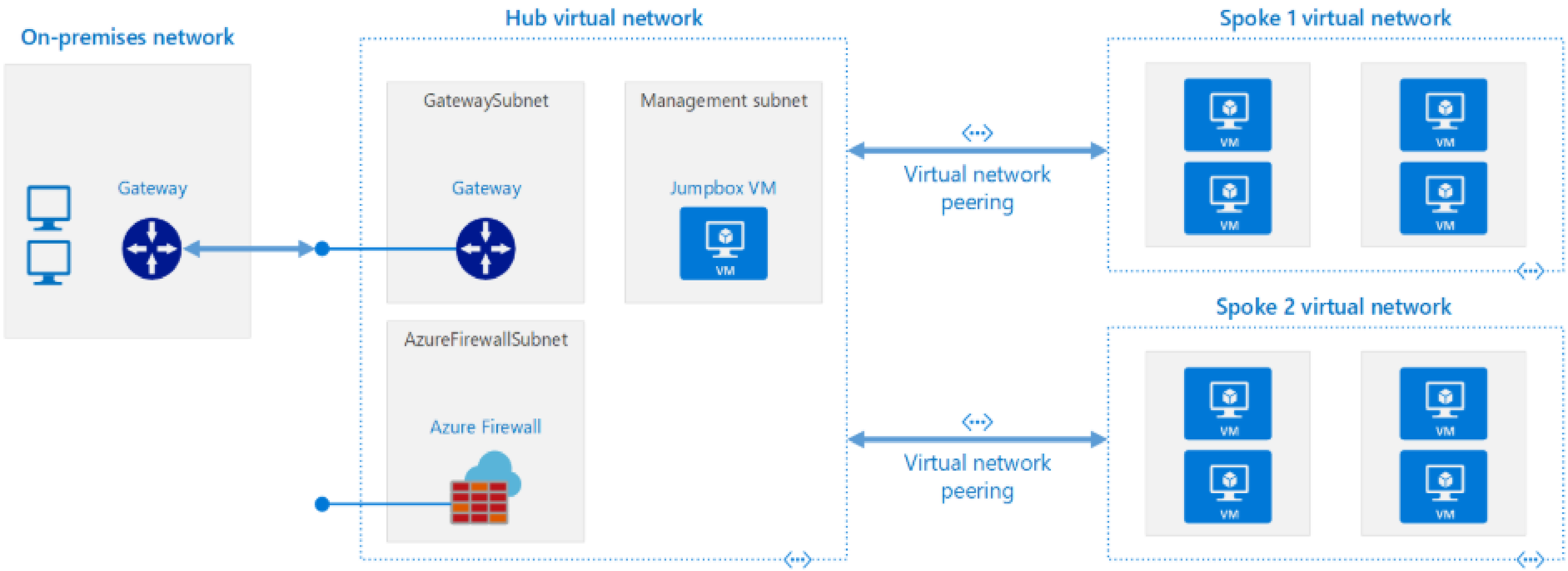
Virtual Network peers appear as one Virtual Network after peering

Two Types of peering:

1. Virtual Network peering: Connect VNets within the same Azure region
2. Global Virtual Network peering: Connect VNets across Azure regions



Hub and Spoke Topology



https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke

Express Routes

Private connection to on-premises networks facilitated by a connectivity provider.

Each circuit has a fixed bandwidth ranging from:

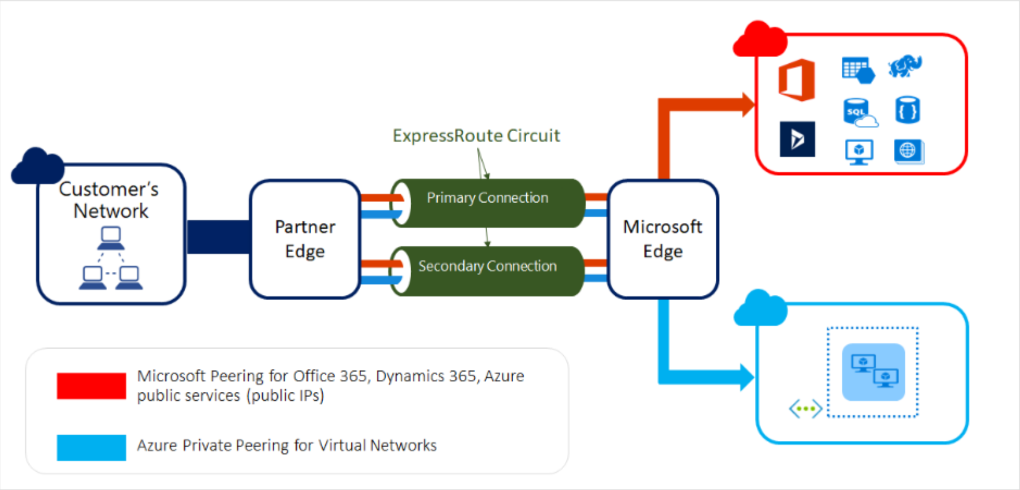
- 50 Mbps
- 100 Mbps
- 200 Mbps
- 500 Mbps
- 1 Gbps
- 10 Gbps

Two pricing models:

1. Metered
2. Unmetered

Express Route Direct

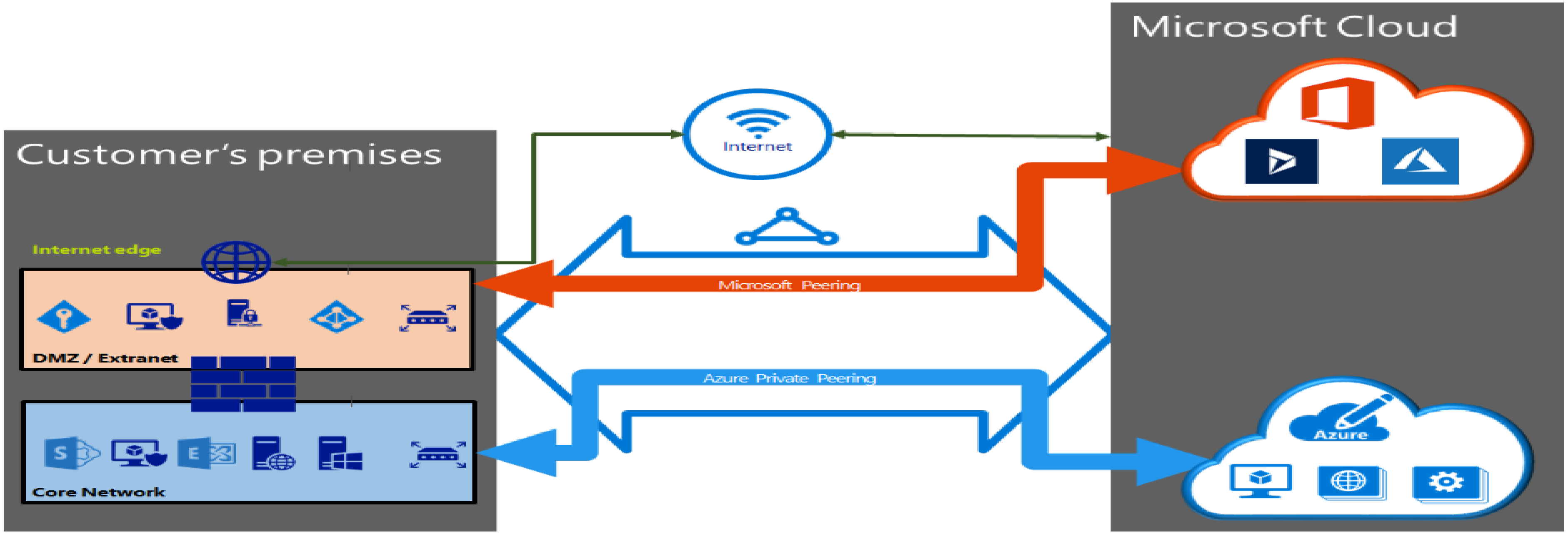
Express Route Global Reach


ExpressRoute Circuit
Customer's Network
Partner Edge
Primary Connection
Secondary Connection
Microsoft Edge
Microsoft Peering for Office 365, Dynamics 365, Azure public services (public IPs)
Azure Private Peering for Virtual Networks

Express Routes

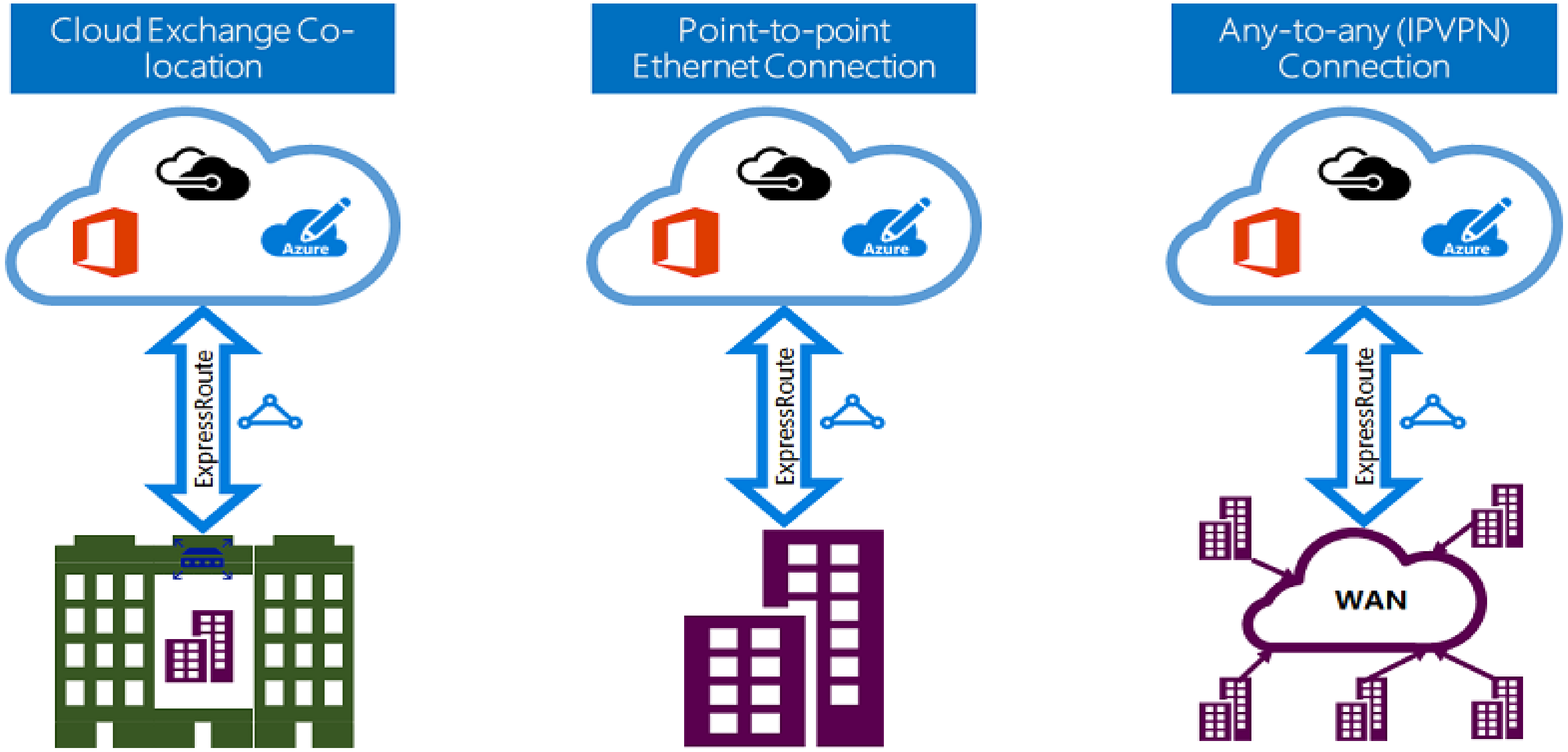
ExpressRoute circuits include two independent peerings*:

1. Private peering
2. Microsoft peering



Express Routes

Three different connectivity models:



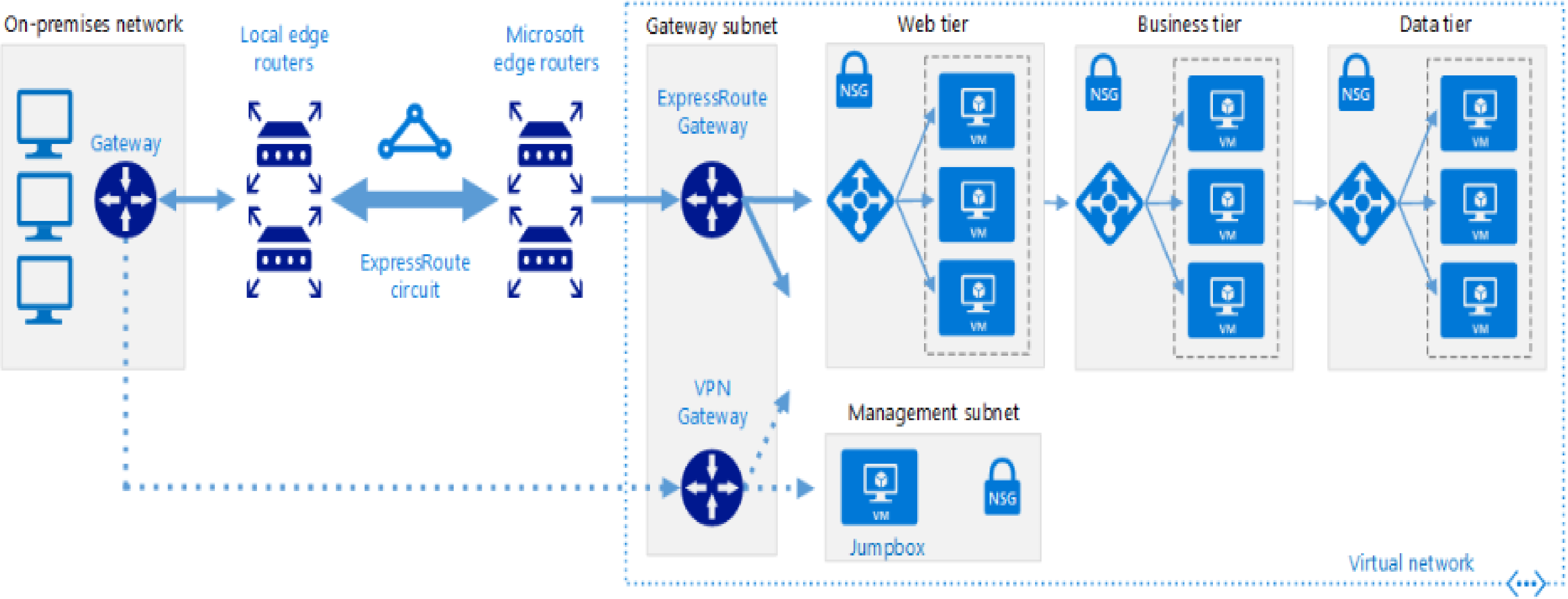
Cloud Exchange Co-location

Point-to-point Ethernet Connection

Any-to-any (IPVPN) Connection

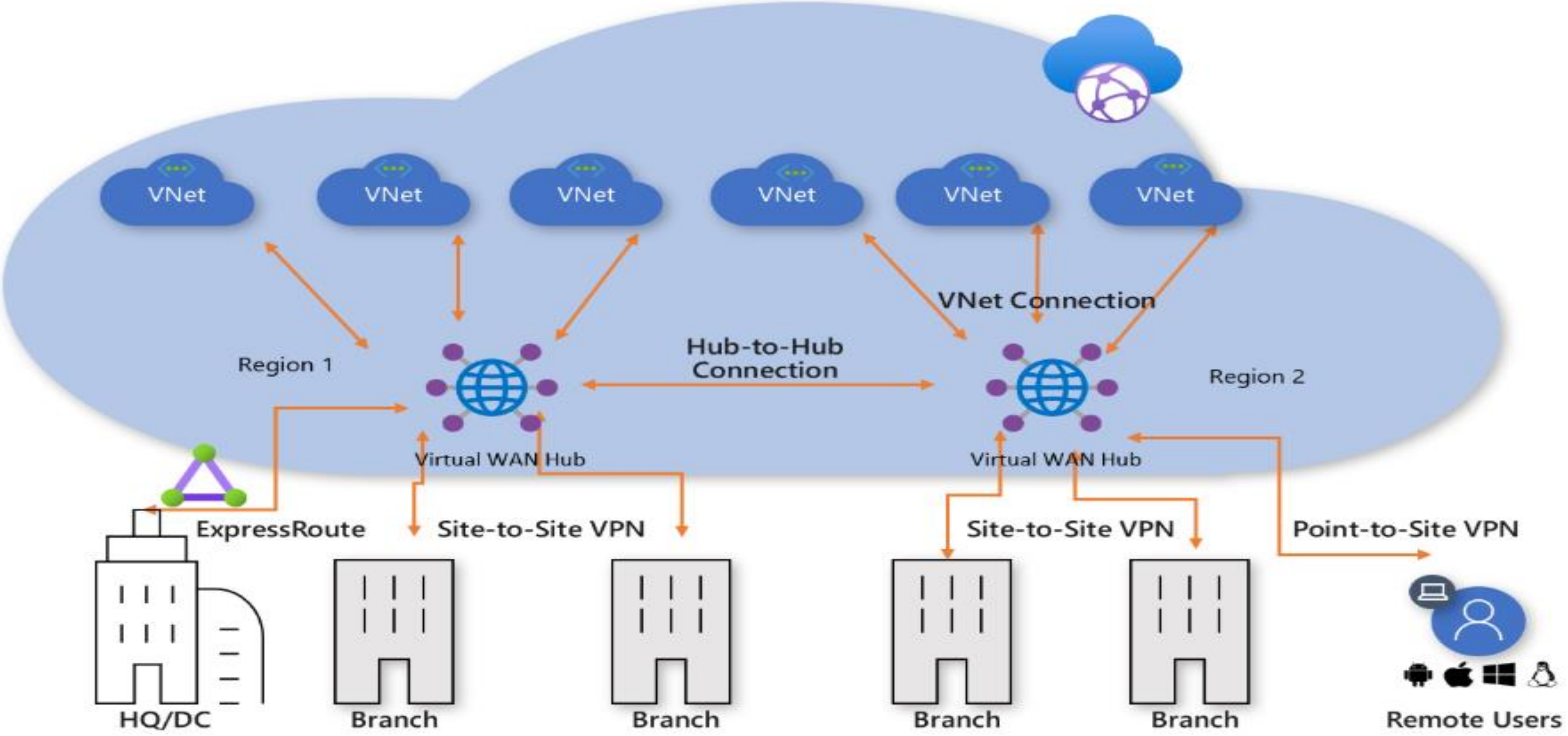
https://docs.microsoft.com/en-us/azure/expressroute/expressroute-locations-providers

ExpressRoute with VPN failover



https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/expressroute-vpn-failover

Virtual WAN

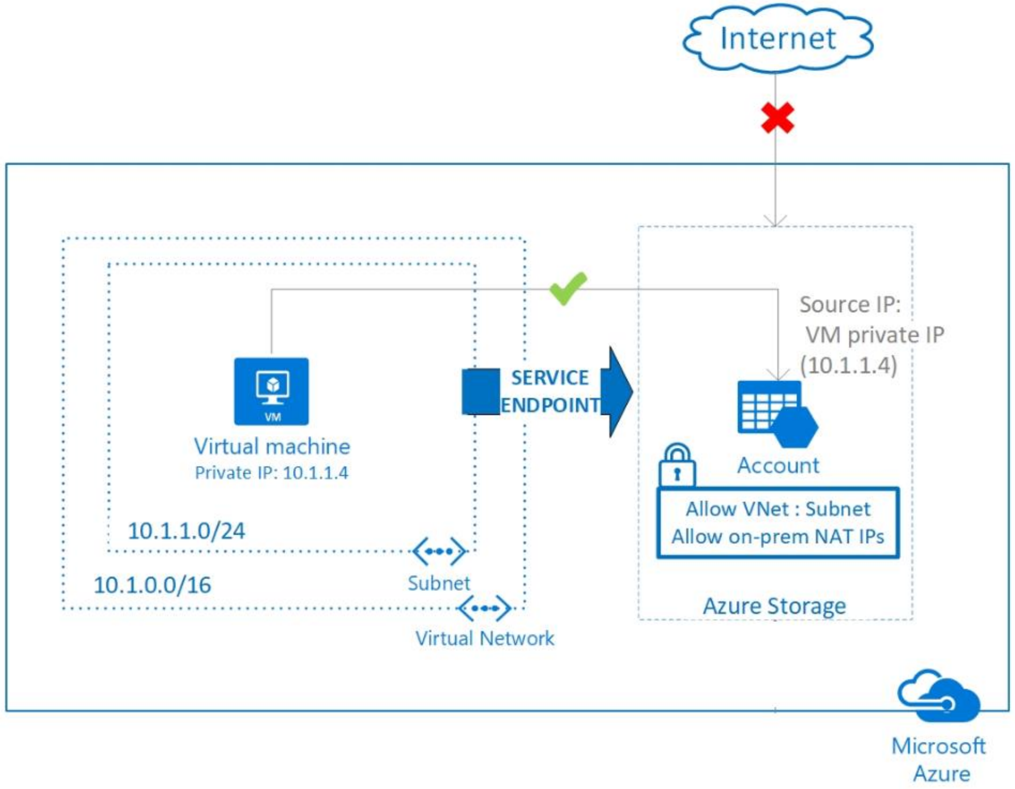

VNet
VNet
VNet
VNet
VNet
VNet
VNet Connection
Region 1
Hub-to-Hub Connection
Region 2
Virtual WAN Hub
Virtual WAN Hub
ExpressRoute
Site-to-Site VPN
Site-to-Site VPN
Point-to-Site VPN
HQ/DC
Branch
Branch
Branch
Branch
Remote Users

Service Endpoints

Secure and direct connectivity to Azure services over an optimized route over the Azure backbone network

Enables private IP addresses in the VNet to reach the endpoint of an Azure service without needing a public IP address on the VNet.

There is no additional cost for using service endpoints

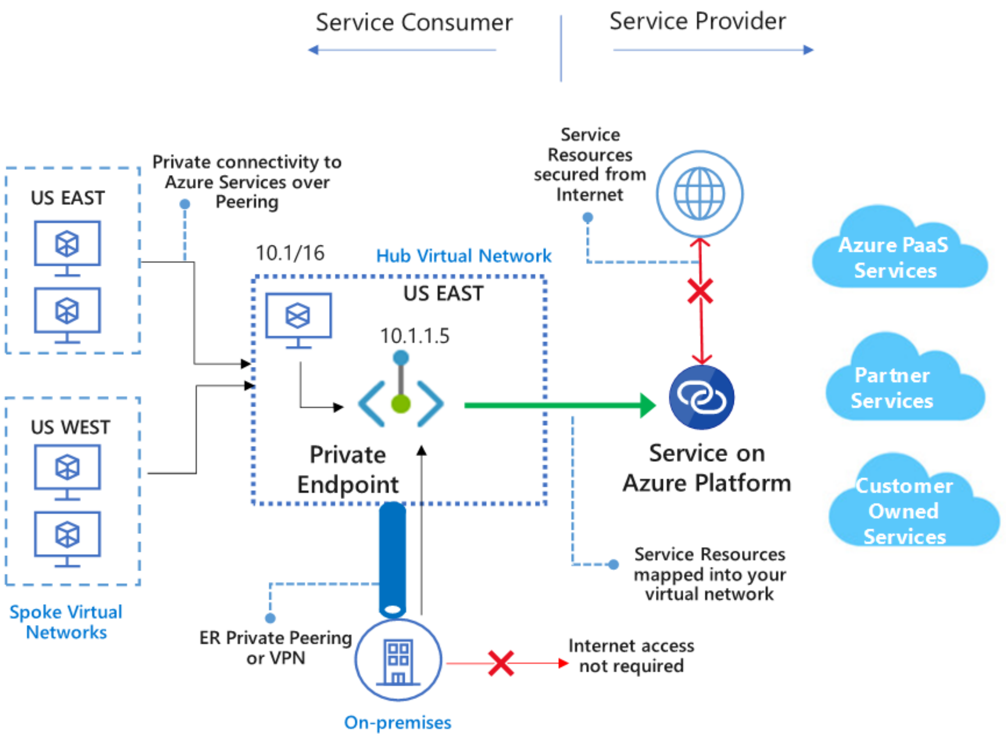


Private Links / Endpoints

Access Azure PaaS Services (for example, Azure Storage and SQL Database) and Azure hosted customer-owned/partner services over a private endpoint in your virtual network.

Traffic between your virtual network and the service travels the Microsoft backbone network.

Exposing your service to the public internet is no longer necessary.

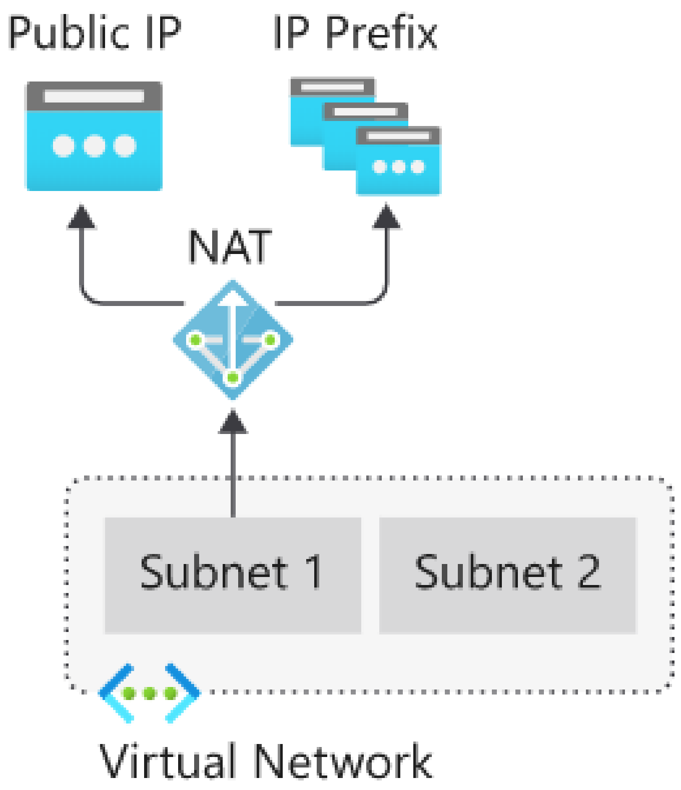

Service Consumer
Service Provider
US EAST
US WEST
Spoke Virtual Networks
Private connectivity to Azure Services over Peering
10.1/16
Hub Virtual Network
US EAST
10.1.1.5
Private Endpoint
Service Resources secured from Internet
Service on Azure Platform
Service Resources mapped into your virtual network
ER Private Peering or VPN
On-premises
Internet access not required
Azure PaaS Services
Partner Services
Customer Owned Services

Virtual Network NAT

Virtual Network NAT (network address translation) simplifies outbound-only Internet connectivity for virtual networks.

When configured on a subnet, all outbound connectivity uses your specified static public IP addresses.

When configured, all UDP and TCP outbound flows from any virtual machine instance within the subnet will use NAT.



Network Security

Network Security Groups

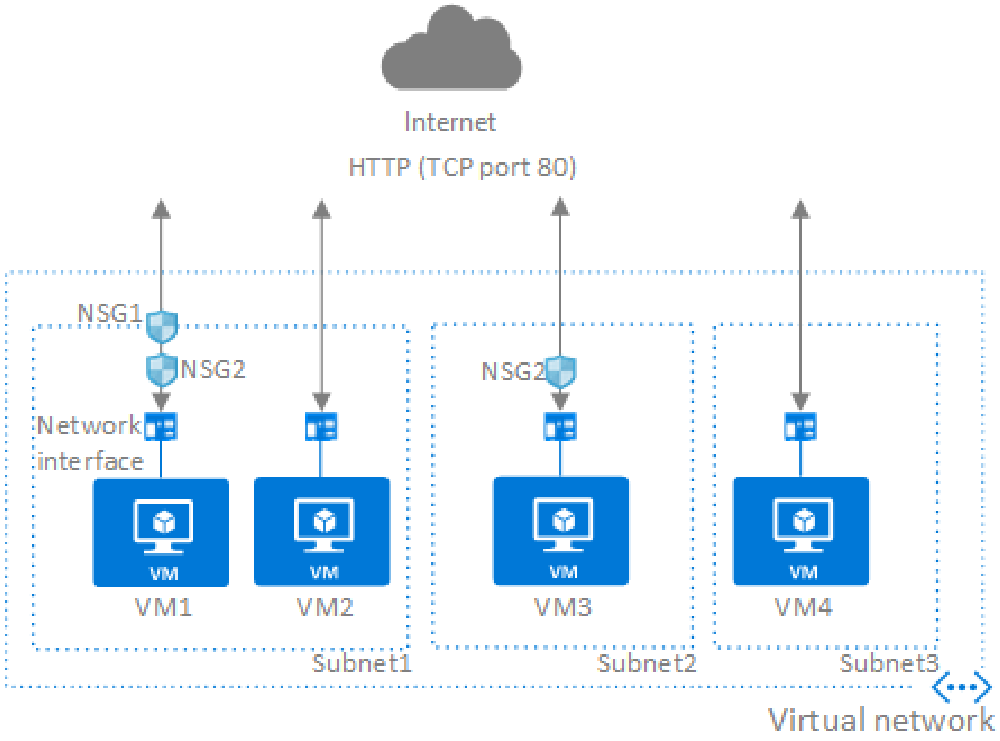
Filter network traffic to and from Azure resources in an Azure virtual network

A network security group contains security rules to allow or deny inbound or outbound network traffic

For each rule, you can specify source and destination, port, and protocol.

Network security group security rules are evaluated by priority using the 5-tuple information (source, source port, destination, destination port, and protocol) to allow or deny the traffic.

Can be applied at NIC or subnet level.

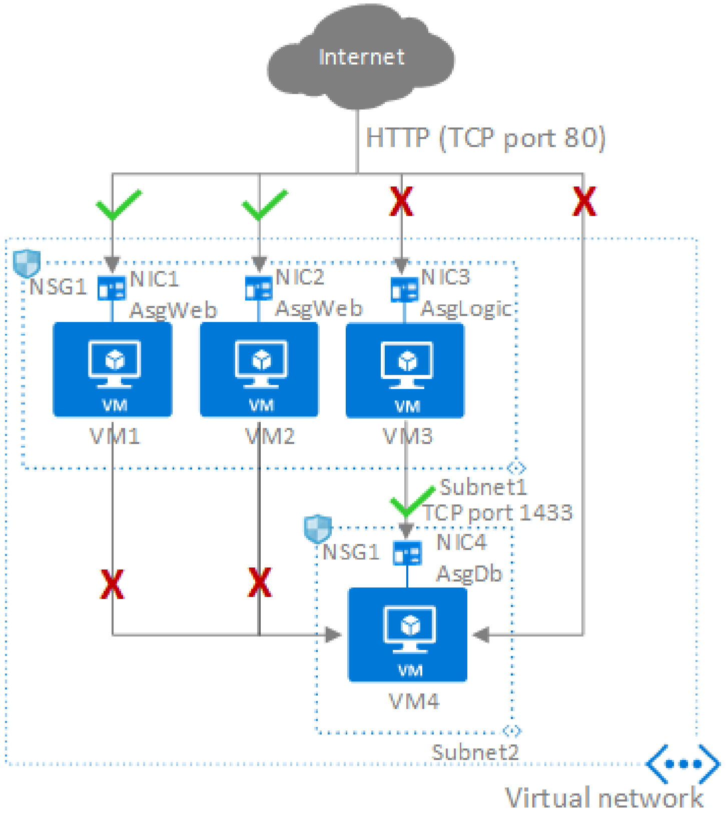


Application Security Groups

Application security groups enable you to configure network security as a natural extension of an application's structure, allowing you to group virtual machines and define network security policies based on those groups.

You can reuse your security policy at scale without manual maintenance of explicit IP addresses.

The platform handles the complexity of explicit IP addresses and multiple rule sets, allowing you to focus on your business logic.

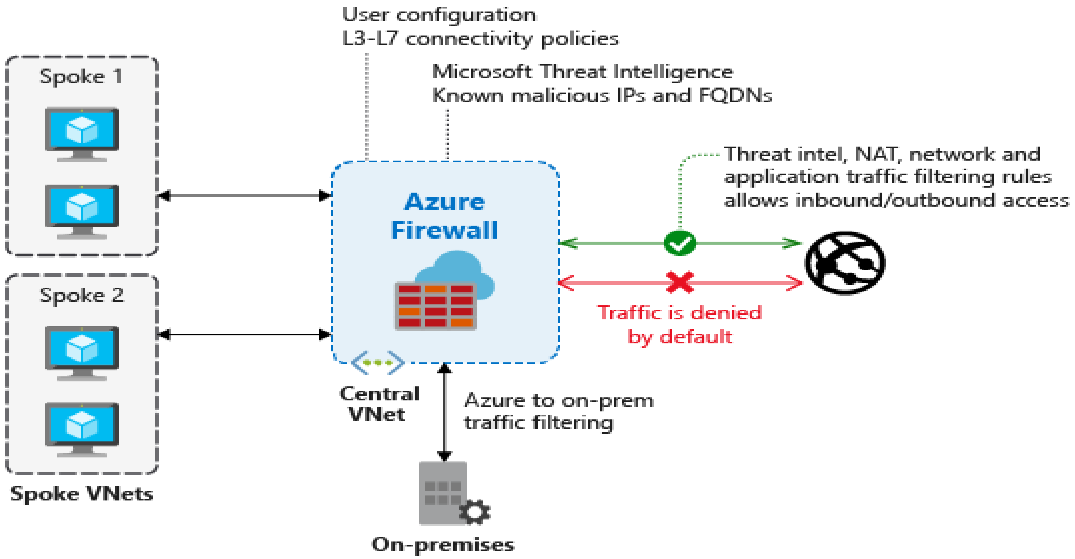


Azure Firewall

Fully managed, cloud-based network security service to protects Azure Virtual Network resources.

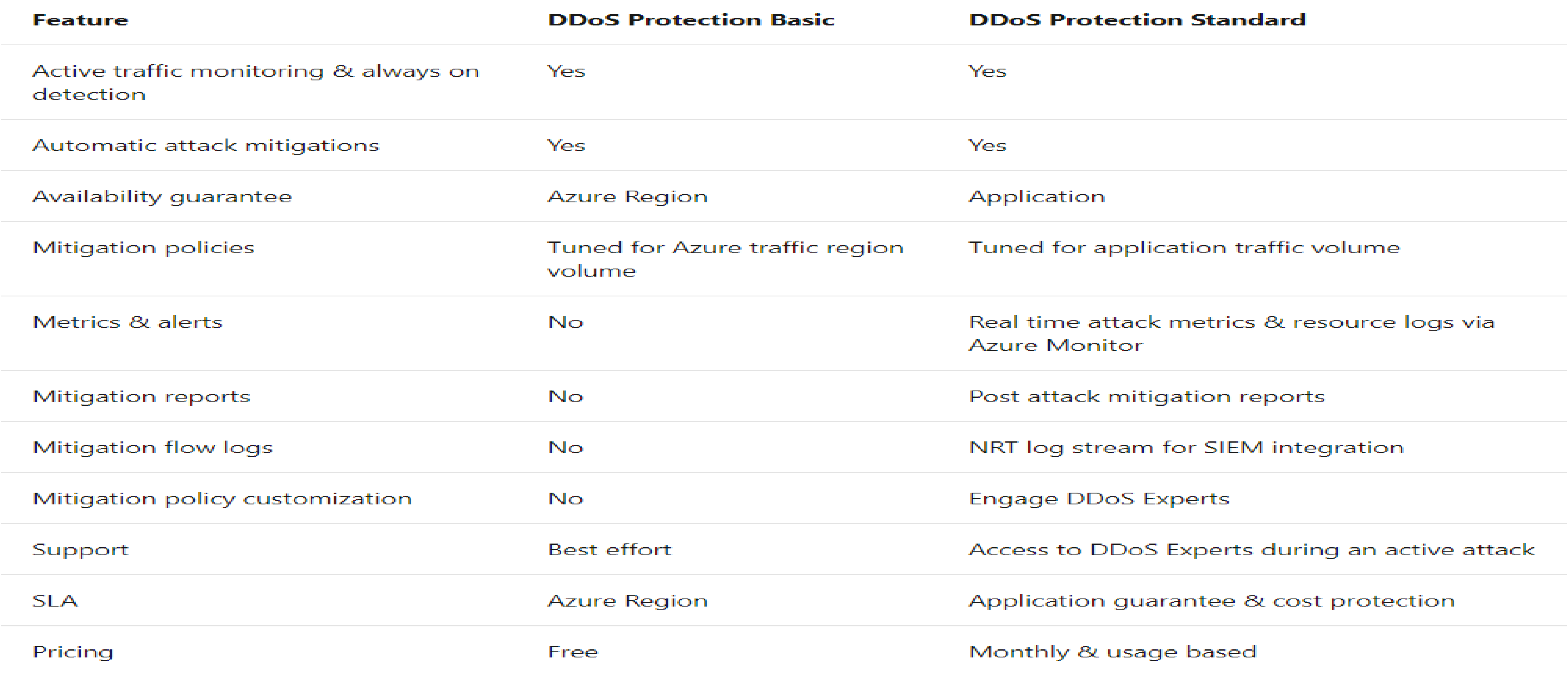
Fully stateful firewall as a service

Built-in high availability and unrestricted cloud scalability.


User configuration
L3-L7 connectivity policies
Microsoft Threat Intelligence
Known malicious IPs and FQDNs
Spoke 1
Spoke 2
Spoke VNets
Azure Firewall
Threat intel, NAT, network and application traffic filtering rules allows inbound/outbound access
Traffic is denied by default
Central VNet
Azure to on-prem traffic filtering
On-premises

Azure DDoS protection

Protect your Azure resources from Distributed Denial of Service (DDoS) attacks.



Feature	DDoS Protection Basic	DDoS Protection Standard
Active traffic monitoring & always on detection	Yes	Yes
Automatic attack mitigations	Yes	Yes
Availability guarantee	Azure Region	Application
Mitigation policies	Tuned for Azure traffic region volume	Tuned for application traffic volume
Metrics & alerts	No	Real time attack metrics & resource logs via Azure Monitor
Mitigation reports	No	Post attack mitigation reports
Mitigation flow logs	No	NRT log stream for SIEM integration
Mitigation policy customization	No	Engage DDoS Experts
Support	Best effort	Access to DDoS Experts during an active attack
SLA	Azure Region	Application guarantee & cost protection
Pricing	Free	Monthly & usage based

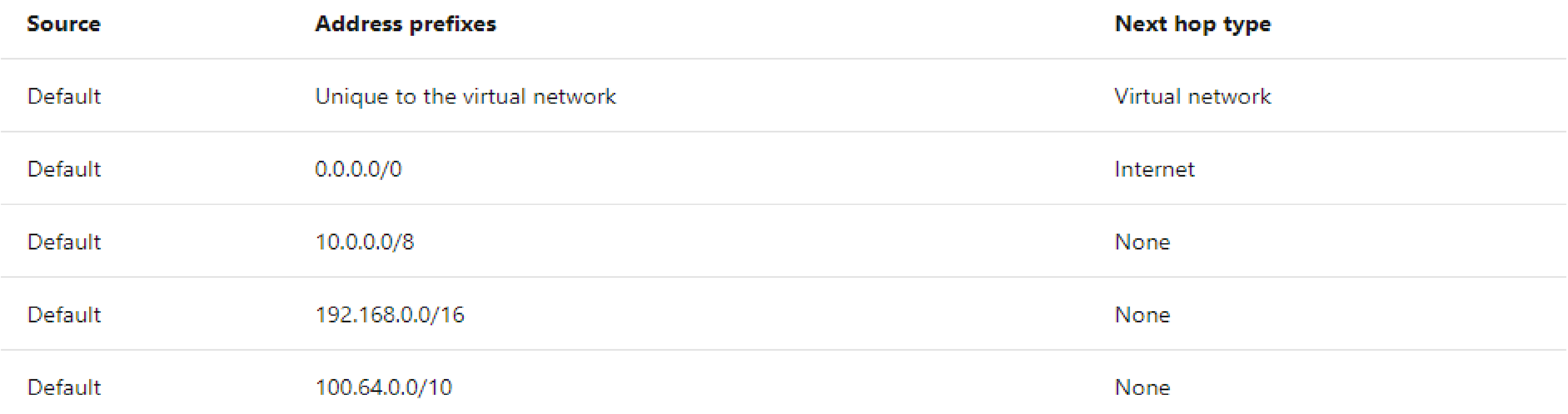
Routing

Routing

A route table is automatically created for each subnet within an Azure virtual network with system default routes already added to the table.

Azure's system default routes can be overridden with custom routes.

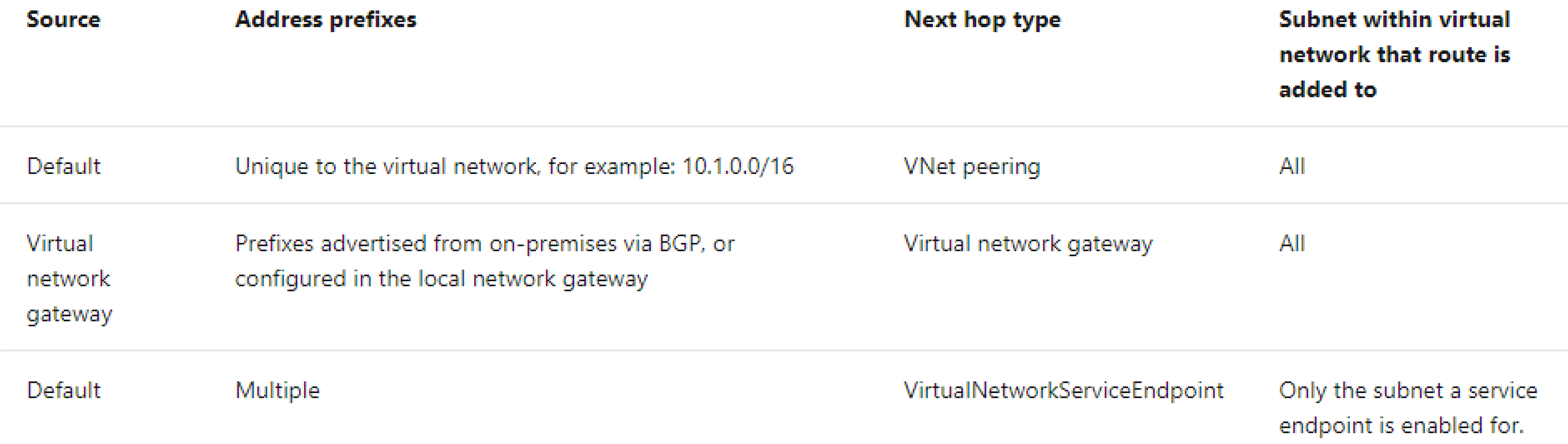
All the outbound traffic from a subnet is routed based on the routes in the subnet's route table.



Source	Address prefixes	Next hop type
Default	Unique to the virtual network	Virtual network
Default	0.0.0.0/0	Internet
Default	10.0.0.0/8	None
Default	192.168.0.0/16	None
Default	100.64.0.0/10	None

Routing

Additional default rules are added to support different Azure Capabilities like VNet Peering and VPN Gateways.



Source	Address prefixes	Next hop type	Subnet within virtual network that route is added to
Default	Unique to the virtual network, for example: 10.1.0.0/16	VNet peering	All
Virtual network gateway	Prefixes advertised from on-premises via BGP, or configured in the local network gateway	Virtual network gateway	All
Default	Multiple	VirtualNetworkServiceEndpoint	Only the subnet a service endpoint is enabled for.

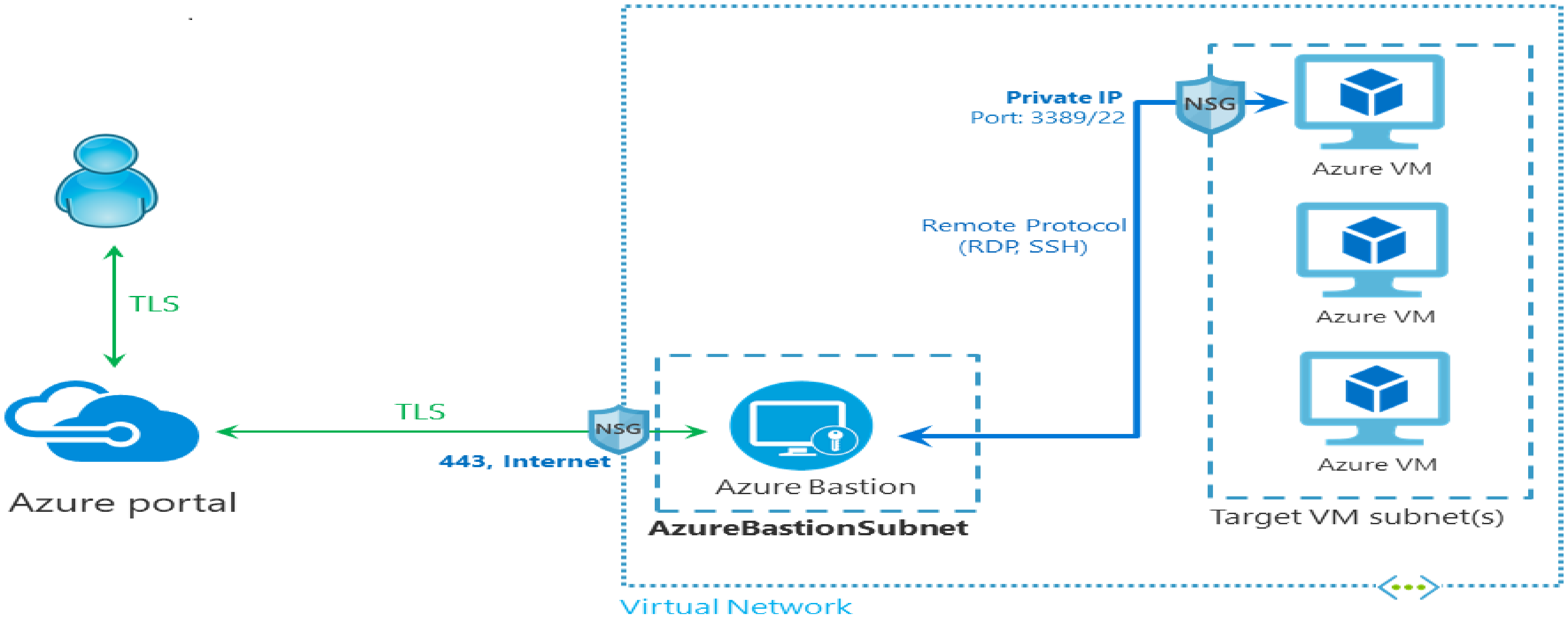
Routing

Custom Routes could be created using

1. User-defined routes to either override Azure's default routes or add additional routes. The following next hop types can be specified when creating a user-defined route:
   - Virtual Appliance
   - Virtual Network Gateway
   - None
   - Virtual Network
   - Internet
2. Border Gateway Protocol (BGP) Routes between your on-prem network gateway and Azure Virtual Network Gateway.
   - Use with VPN gateways of "ExpressRoute" type

Azure Bastion

Secure and seamless RDP/SSH connectivity to your virtual machines directly in the Azure portal over TLS



Load Balancing

Azure Load Balancer

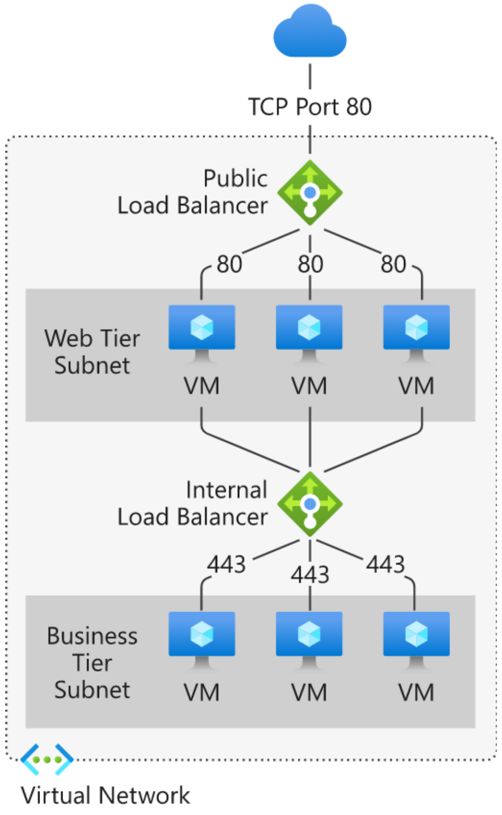
Azure Load Balancer is Layer 4 load balancer.

Evenly distributes inbound network traffic across a group of backend resources or servers.

The backend pool can be Azure virtual machines or instances in a virtual machine scale set.

Two Types:

- Public load balancer: for load balancing internet traffic to your Virtual Machines. Uses a public IP address for front end configuration.
- Internal (or Private) load balancer: for load balancing inside a virtual network. Uses a private IP address for front end configuration.

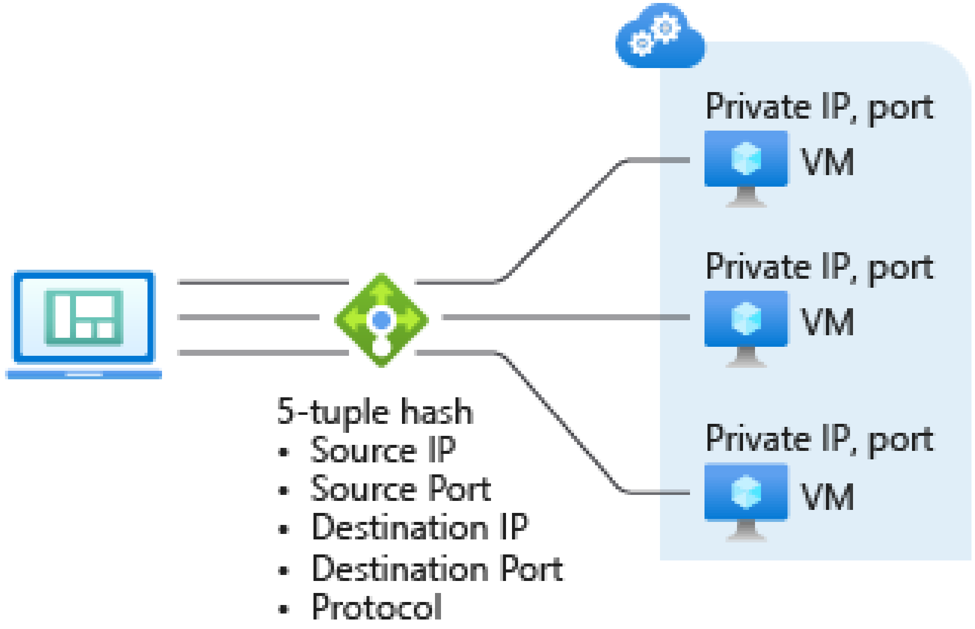


Azure Load Balancer

Load balancer uses a Five-tuple hash.

The hash includes

- Source IP Address
- Source Port
- Destination IP Address
- Destination Port
- IP protocol number to map flows to available server



Azure Load Balancer

Basic load balancer

Up to 300 instances

Health Probes: TCP, HTTP

No SLA

Open to internet by default

Standard load balancer

Up to 1000 instances

Health Probes: TCP, HTTP, HTTPS

99.99% SLA

Supports HA Ports

Secure by Default

Skus are not mutable.

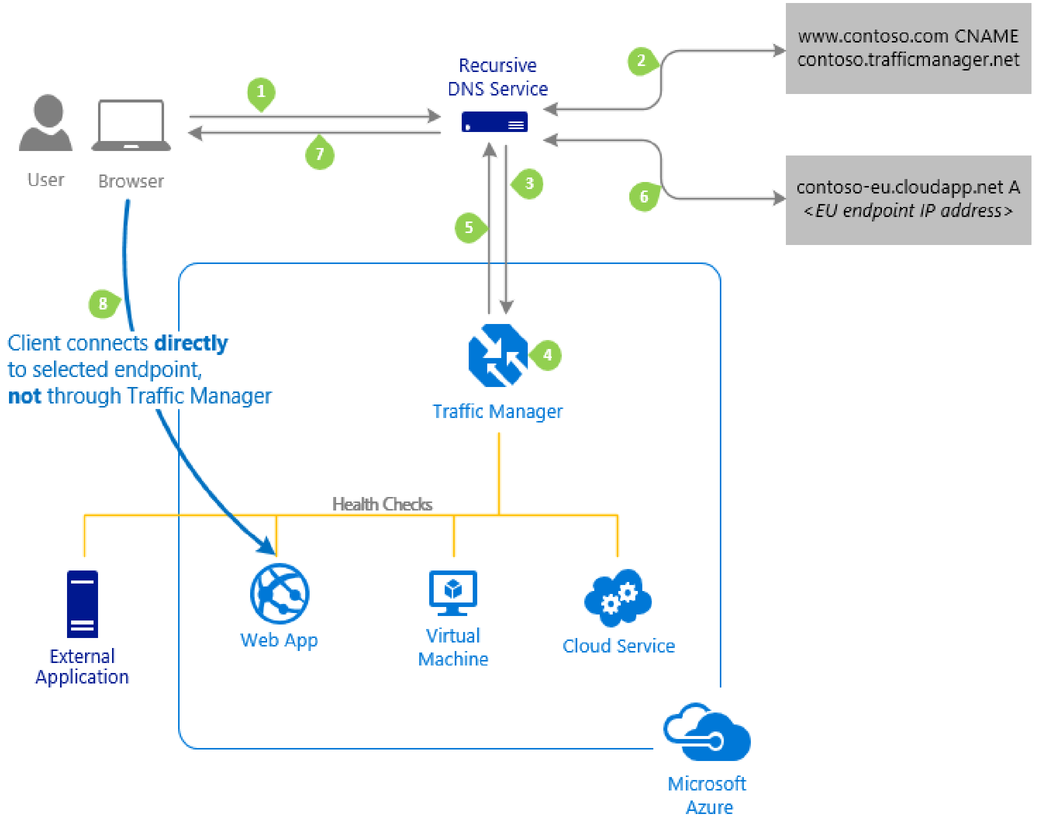
Azure Traffic Manager

DNS-based traffic load balancer that enables you to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness.

Supports different traffic routing methods including priority, weighted, performance, geographic, multi-value and subnet.

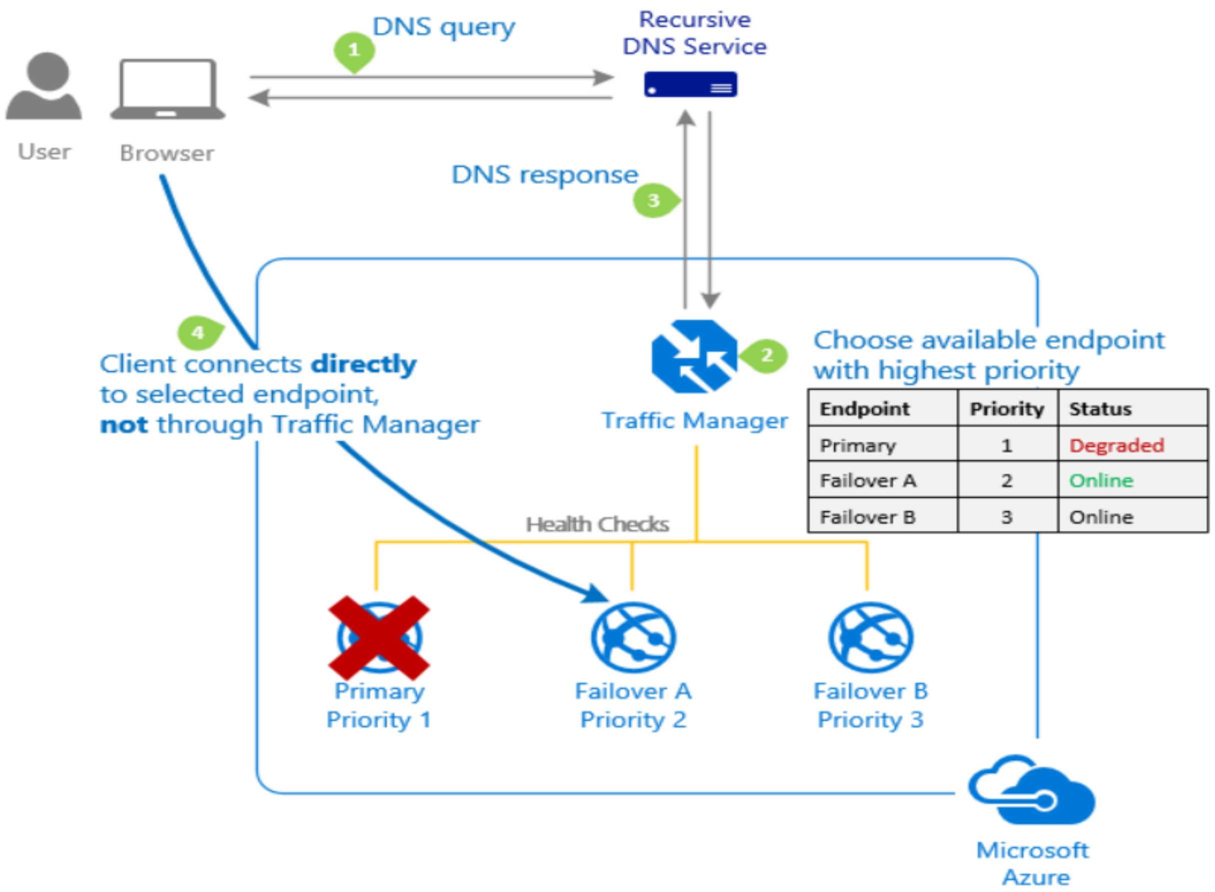
Traffic Manager also monitors the endpoint health continuously and failover automatically when endpoints fail.

Use for routing incoming traffic for high performance and availability

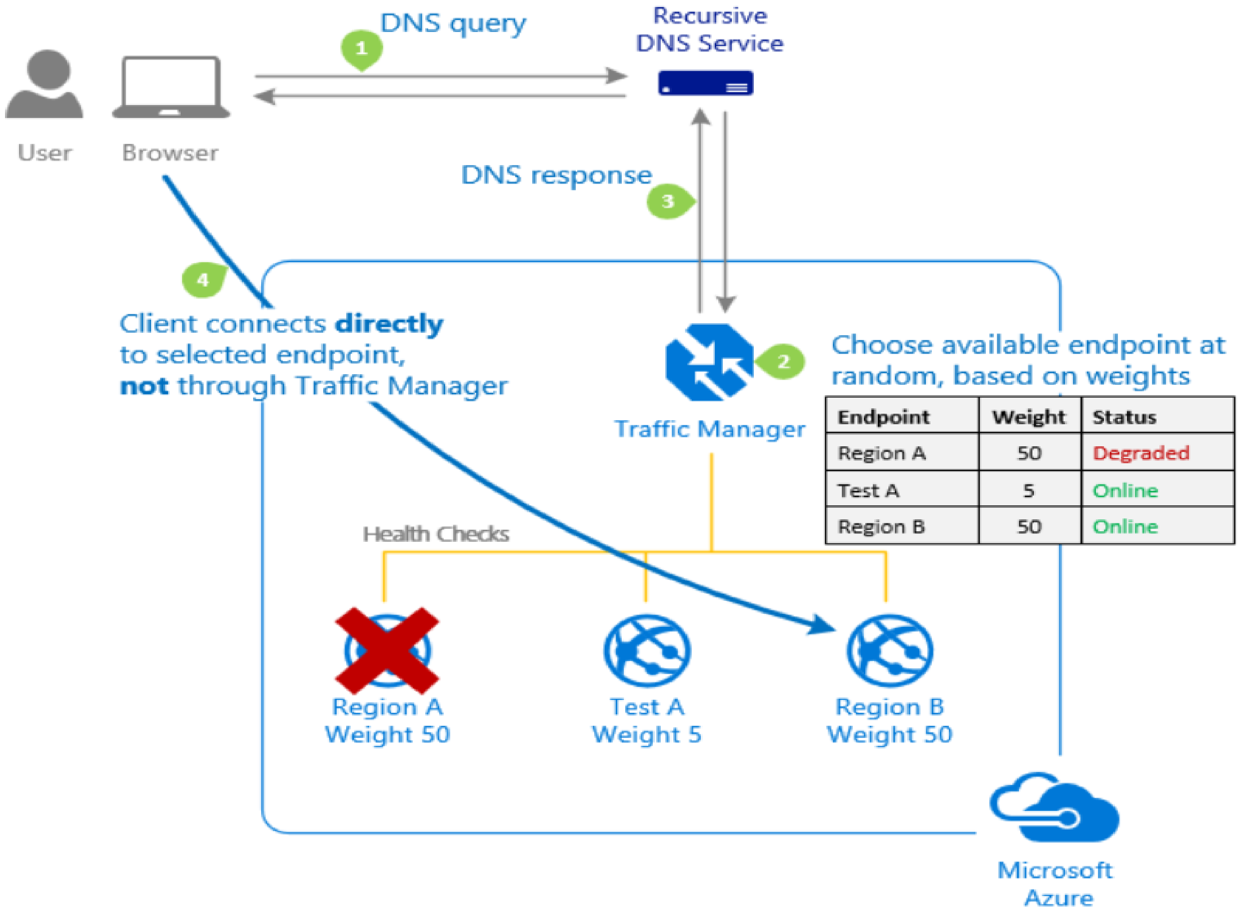


User
Browser
1
7
Recursive DNS Service
2
www.contoso.com CNAME contoso.trafficmanager.net
3
5
6
contoso-eu.cloudapp.net A <EU endpoint IP address>
8
Client connects **directly** to selected endpoint, **not** through Traffic Manager
4
Traffic Manager
Health Checks
External Application
Web App
Virtual Machine
Cloud Service
Microsoft Azure

Azure Traffic Manager



Endpoint	Priority	Status
Primary	1	Degraded
Failover A	2	Online
Failover B	3	Online



Endpoint	Weight	Status
Region A	50	Degraded
Test A	5	Online
Region B	50	Online

Azure Front Door

Azure Front Door is Application Delivery Network (ADN) as a service

It offers layer 7 load-balancing capabilities for your applications with instant failover

Features:

- Dynamic site acceleration (DSA)
- TLS/SSL offloading and end to end TLS,
- Web Application Firewall (WAF) and DDoS Protection
- Cookie-based session affinity
- Url path-based routing
- Free certificates and multiple domain management, and others

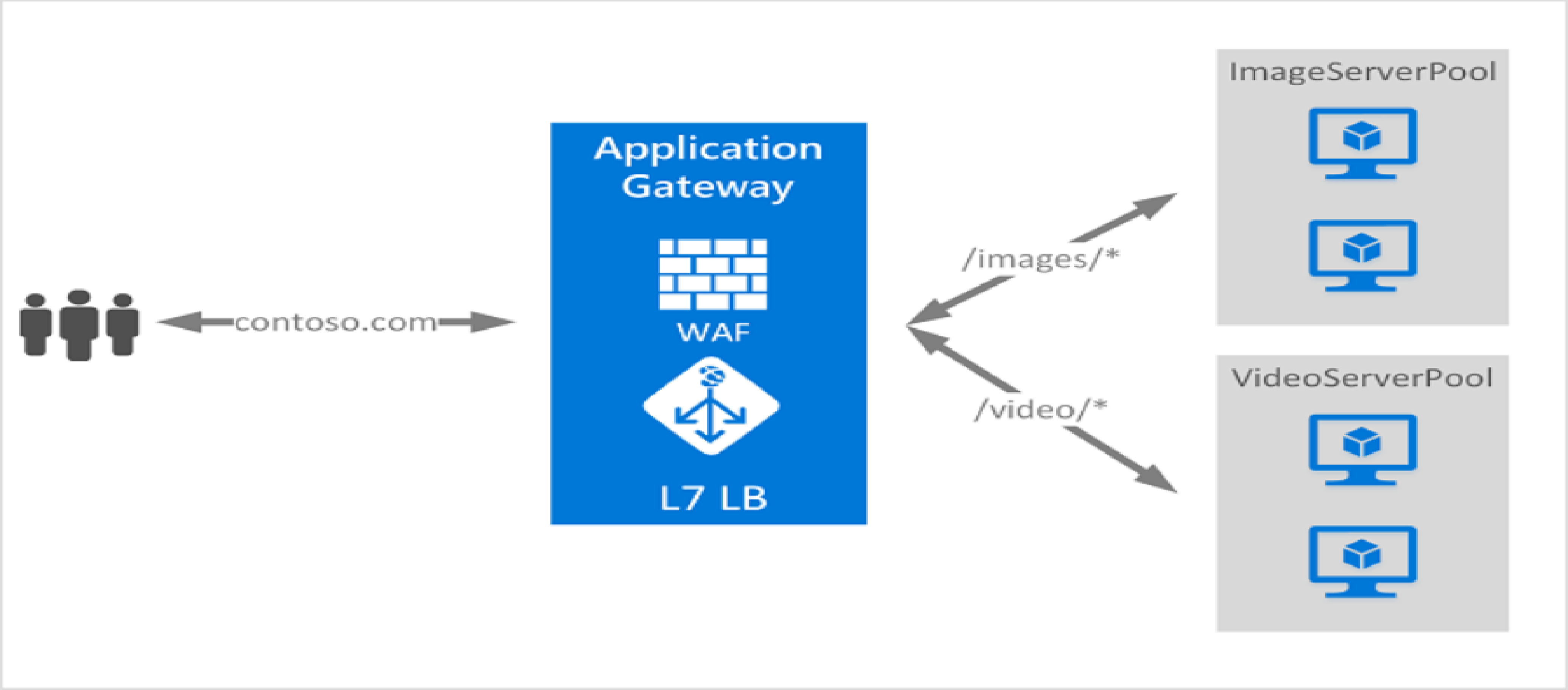
Azure Application Gateway

Azure Application Gateway is a platform-managed, scalable, and highly available application delivery controller as a service and offers a customizable layer 7 load-balancing solution

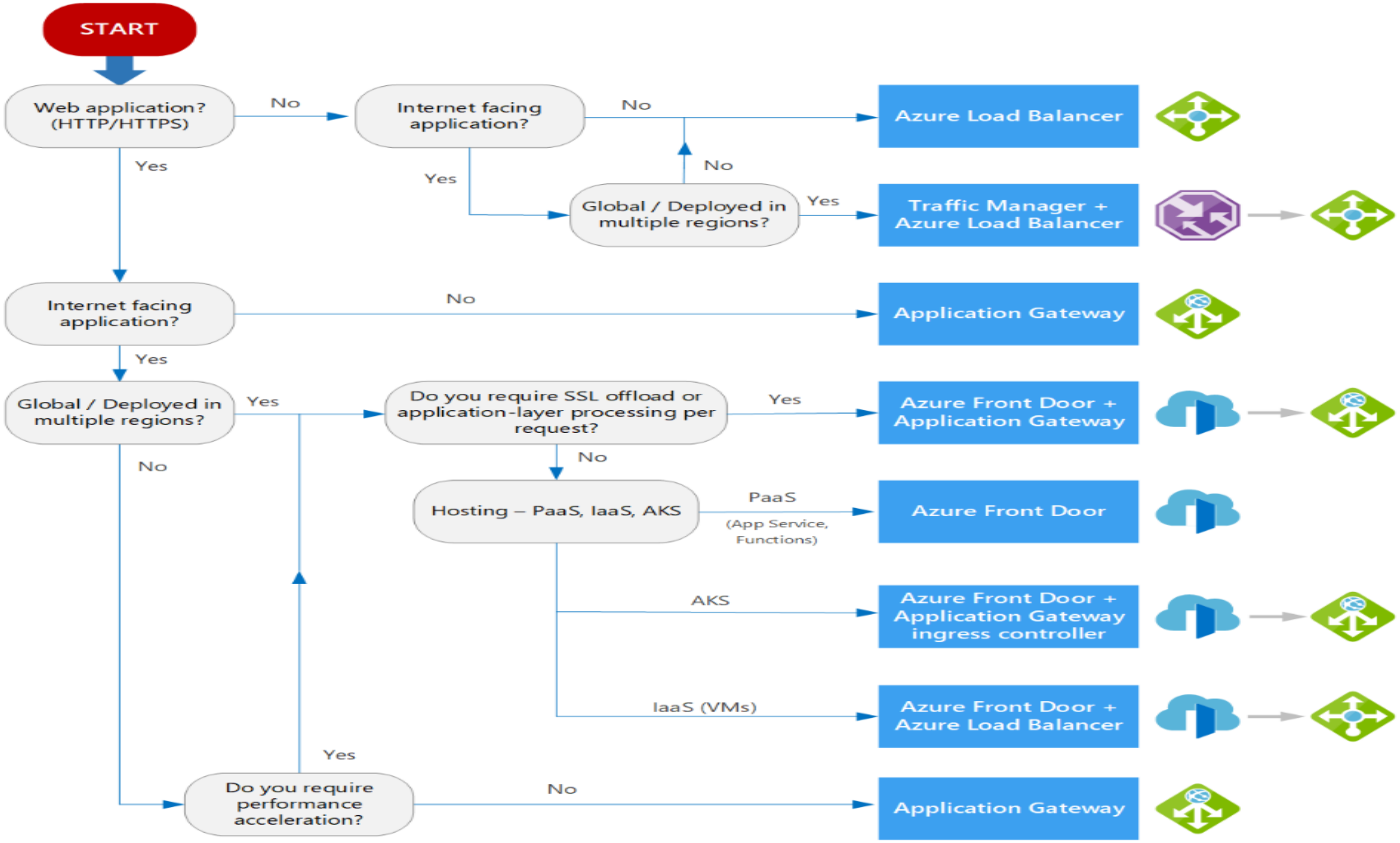
Features:

- 99.95 percent uptime service-level agreement for multi-instance deployments
- Centralized SSL offload and SSL policy
- Support for cookie-based session affinity
- Support for public, private, and hybrid websites
- Integrated web application firewall
- Management through Azure APIs

Azure Application Gateway



What to use when?



START

Web application? (HTTP/HTTPS)

No

Internet facing application?

No

Azure Load Balancer

No

Yes

Global / Deployed in multiple regions?

Yes

Traffic Manager + Azure Load Balancer

Yes

Internet facing application?

No

Application Gateway

Yes

Global / Deployed in multiple regions?

Yes

Do you require SSL offload or application-layer processing per request?

Yes

Azure Front Door + Application Gateway

No

Hosting – PaaS, IaaS, AKS

PaaS (App Service, Functions)

Azure Front Door

AKS

Azure Front Door + Application Gateway ingress controller

IaaS (VMs)

Azure Front Door + Azure Load Balancer

No

Do you require performance acceleration?

Yes

No

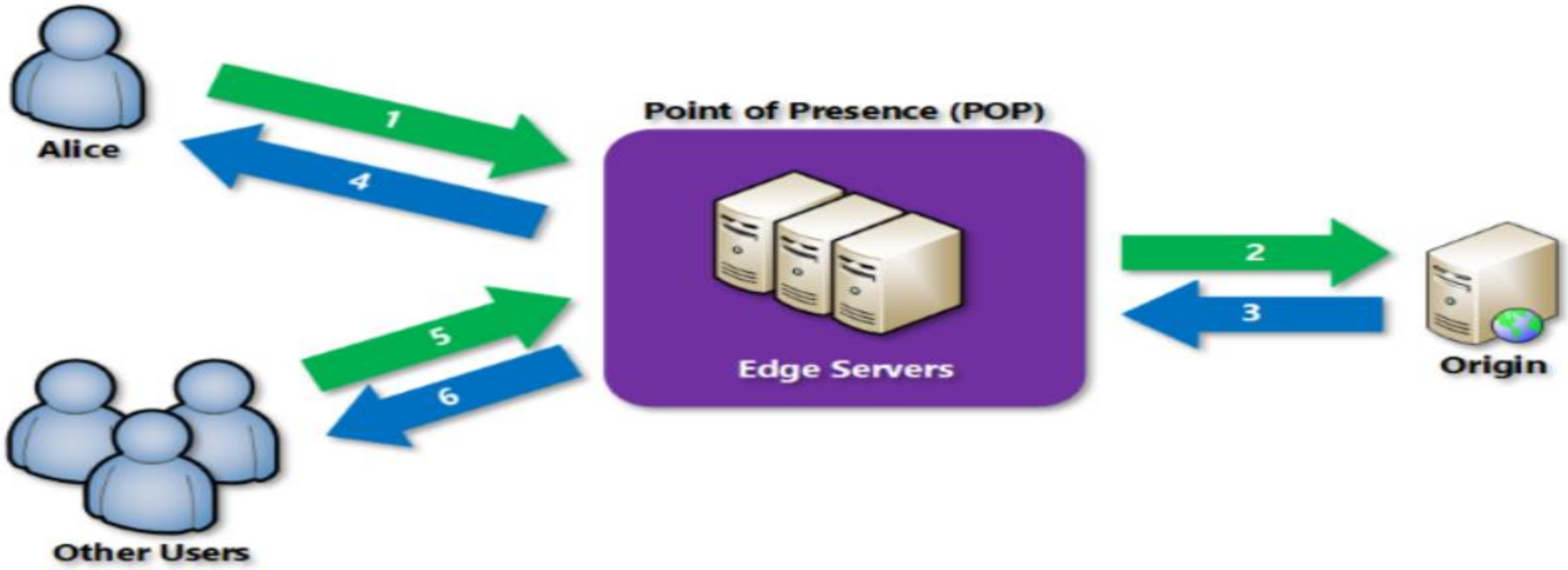
Application Gateway

https://docs.microsoft.com/en-us/azure/architecture/guide/technology-choices/load-balancing-overview

Azure Content Delivery Network

Azure Content Delivery Network is a distributed network of servers that can efficiently deliver web content to users.

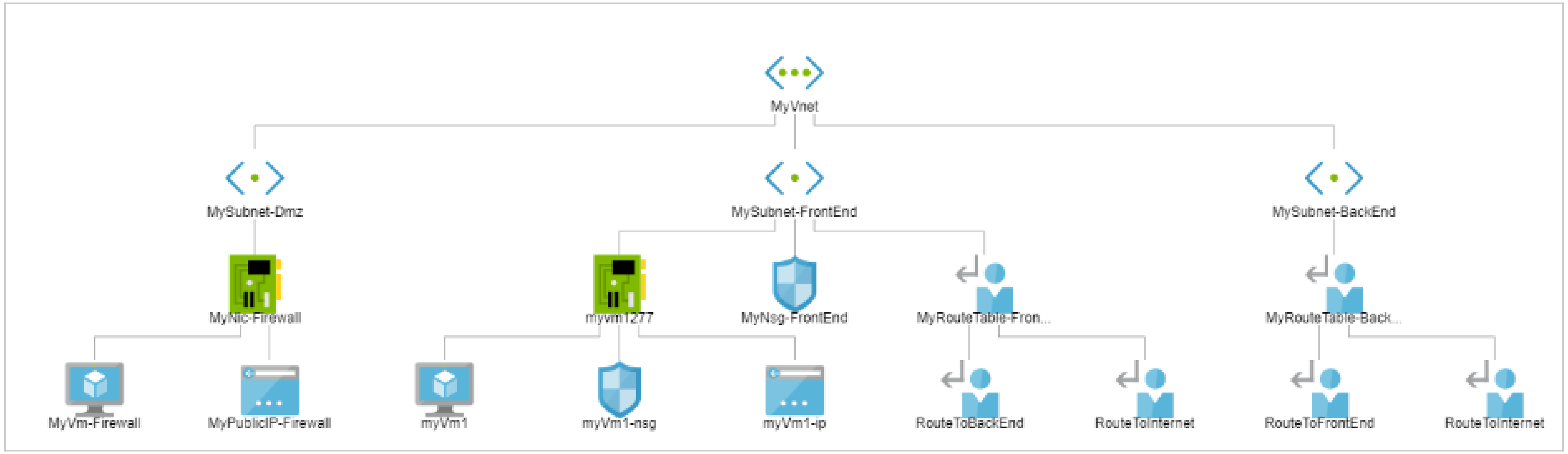
CDNs store cached content on edge servers in point-of-presence (POP) locations that are close to end users, to minimize latency.



Network Monitoring

Azure Network Watcher

Monitor, diagnose, view metrics, and enable or disable logs for resources in an Azure virtual network using Azure Network Watcher.



Network Performance Monitor

Cloud-based hybrid network monitoring solution to monitor network performance between various points in the network infrastructure.

Three broad capabilities:

Performance Monitor: Monitors network connectivity across cloud deployments and on-premises locations, multiple data centers, and branch offices and mission-critical multitier applications or microservices.

Service Connectivity Monitor: monitors the connectivity from your users to the services you care about, determine what infrastructure is in the path, and identify where network bottlenecks occur.

Express Route Monitor: Monitors end-to-end connectivity and performance between your branch offices and Azure, over Azure ExpressRoute.

Resources

1. Azure Architecture Center: https://docs.microsoft.com/en-us/azure/architecture/
2. Microsoft Azure Documentation: https://docs.microsoft.com/en-us/azure
3. Azure Best practices for network security: https://docs.microsoft.com/en-us/azure/security/fundamentals/network-best-practices
4. Microsoft Learn: https://docs.microsoft.com/en-us/learn/
5. Pluralsight + Microsoft – 200+ free courses: https://www.pluralsight.com/partners/microsoft/azure
6. Azure Friday: https://azure.microsoft.com/en-us/resources/videos/azure-friday/
7. Azure Role-based Certifications: https://www.microsoft.com/en-us/learning/certification-overview.aspx

Q&A

Microsoft

Azure Networking

Scan this QR-code to access **free educational resources, step-by-step learning guides** as well as get practical experience in **Azure Networking!**

https://aka.ms/AA8j3oi

Don’t forget to add **Microsoft Azure as a skill** to your LinkedIn account to stay connected with our developer community!!!

+ Microsoft Azure

We post the latest announcements about **free events for developers** in Ireland on our official Twitter account!

@MSDevIRL

thank
you
123RF