Demystifying Azure Networking for Developers

VAIBHAV GUJRAL

Agenda

- Azure Regions and data centers
- Virtual Networks
- VPN Gateways
- NSGs and ASGs
- Load Balancing Options

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

Americas | Europe | Asia Pacific | Middle East and Africa | Azure Government | Azure China

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

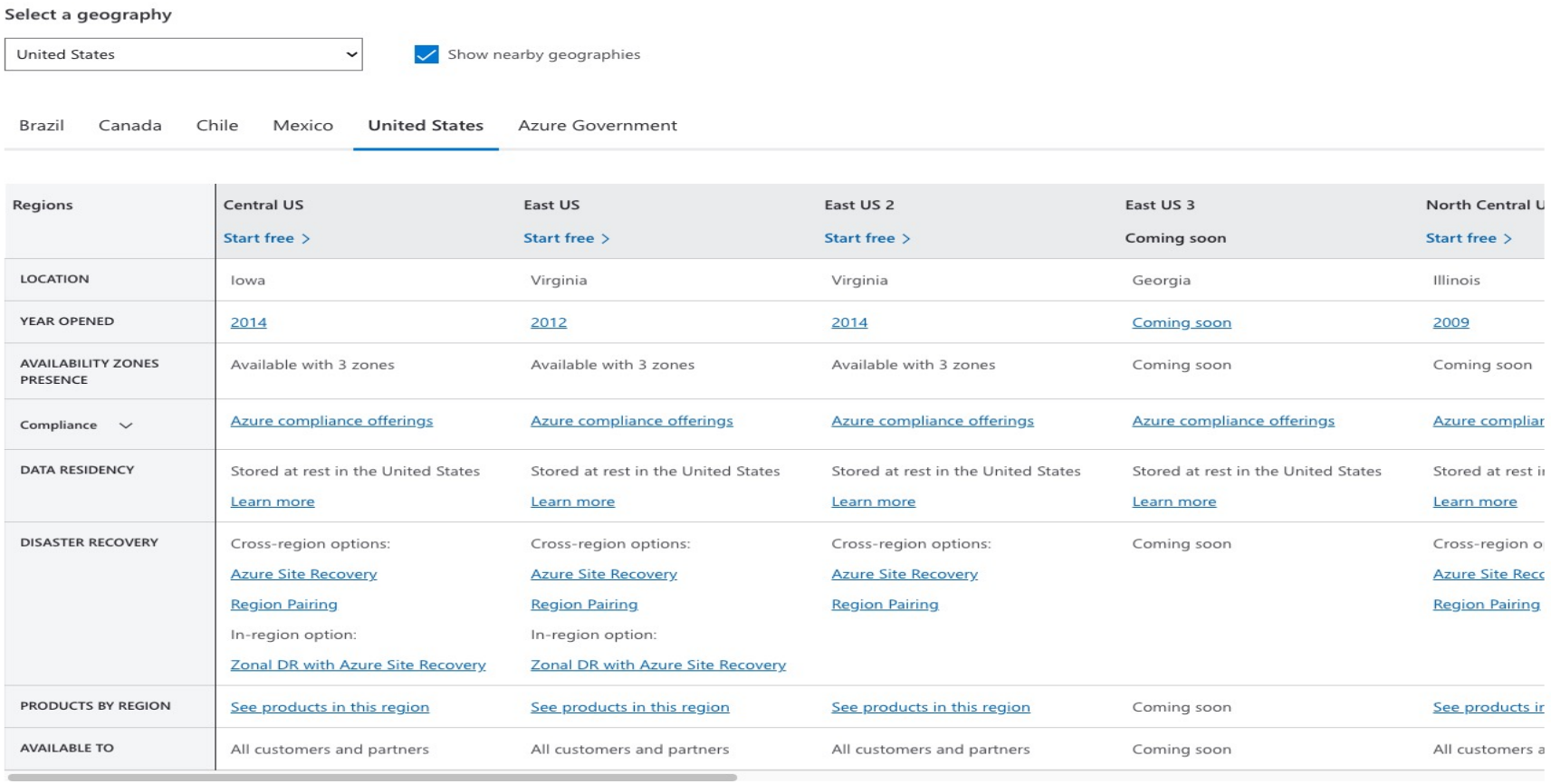
Americas | **Europe** | Asia Pacific | Middle East and Africa | Azure Government | Azure China

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)

Americas | Europe | **Asia Pacific** | Middle East and Africa | Azure Government | Azure China

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

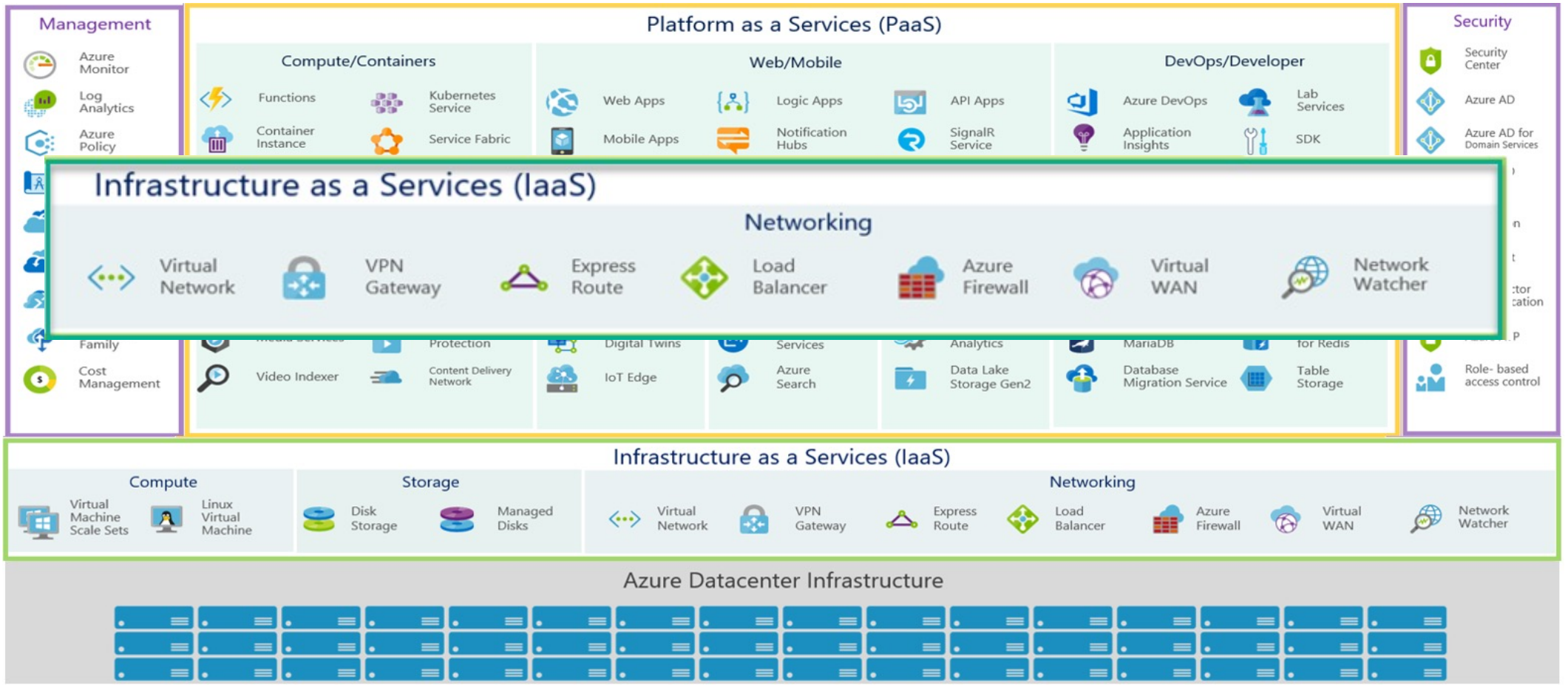
Global Presence



Regions	Central US Start free >	East US Start free >	East US 2 Start free >	East US 3 Coming soon	North Central U Start free >
LOCATION	Iowa	Virginia	Virginia	Georgia	Illinois
YEAR OPENED	2014	2012	2014	Coming soon	2009
AVAILABILITY ZONES PRESENCE	Available with 3 zones	Available with 3 zones	Available with 3 zones	Coming soon	Coming soon
Compliance	Azure compliance offerings	Azure compliance offerings	Azure compliance offerings	Azure compliance offerings	Azure compliar
DATA RESIDENCY	Stored at rest in the United States Learn more	Stored at rest in the United States Learn more	Stored at rest in the United States Learn more	Stored at rest in the United States Learn more	Stored at rest i Learn more
DISASTER RECOVERY	Cross-region options: Azure Site Recovery Region Pairing In-region option: Zonal DR with Azure Site Recovery	Cross-region options: Azure Site Recovery Region Pairing In-region option: Zonal DR with Azure Site Recovery	Cross-region options: Azure Site Recovery Region Pairing	Coming soon	Cross-region o Azure Site Recc Region Pairing
PRODUCTS BY REGION	See products in this region	See products in this region	See products in this region	Coming soon	See products ir
AVAILABLE TO	All customers and partners	All customers and partners	All customers and partners	Coming soon	All customers a

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

Azure Services



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

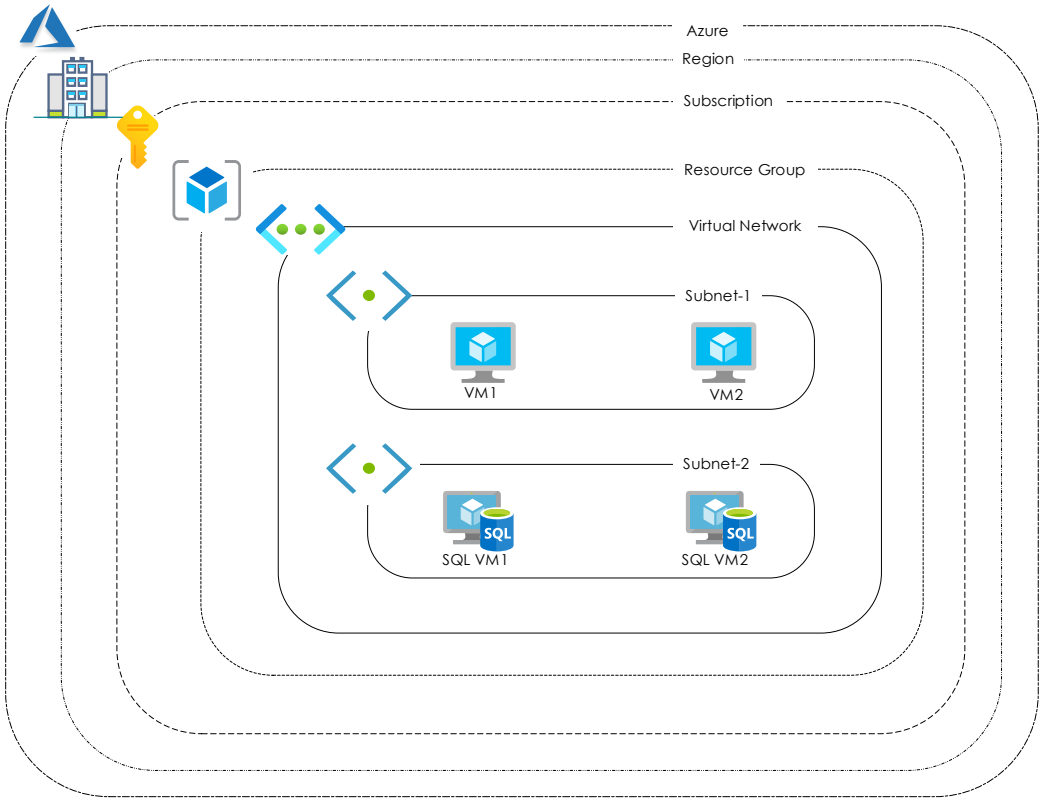
VNet is scoped to a single region and subscription

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

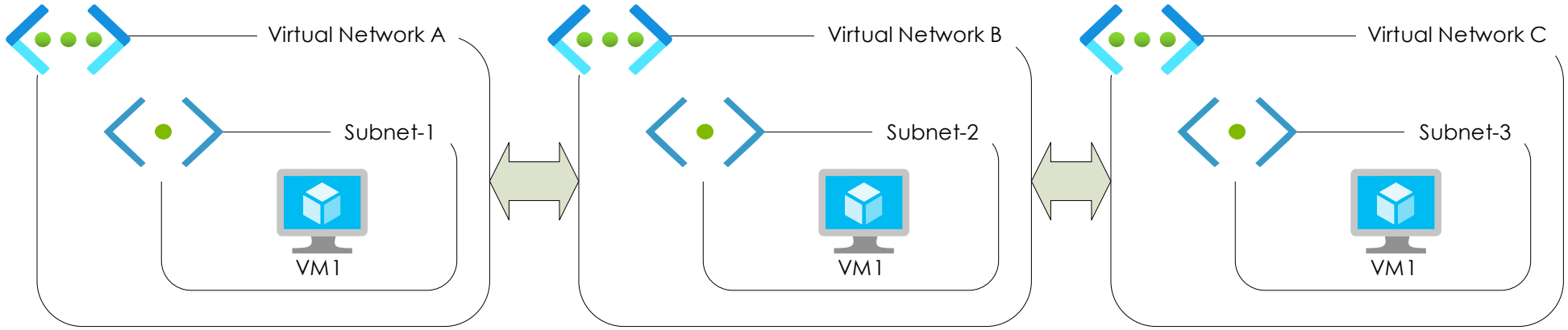
VNet Peering

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



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:

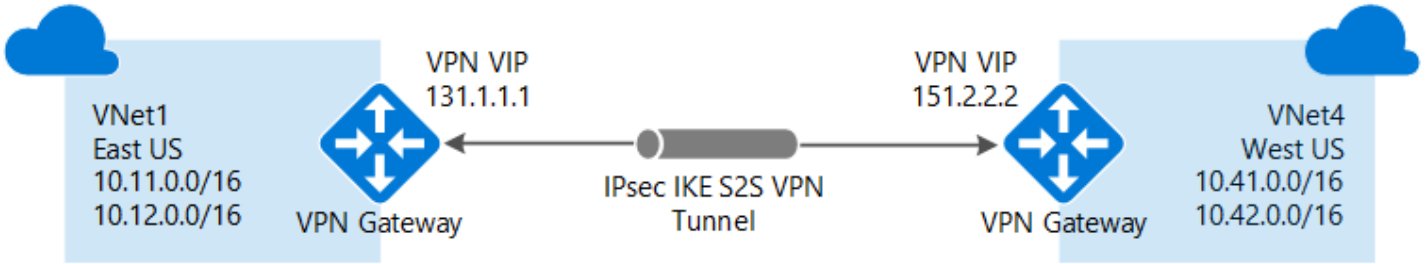
Each VPN can have only one VPN gateway, whereas a VPN gateway can have multiple connections.

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

VPN Gateway

Connectivity options through VPN Gateway:

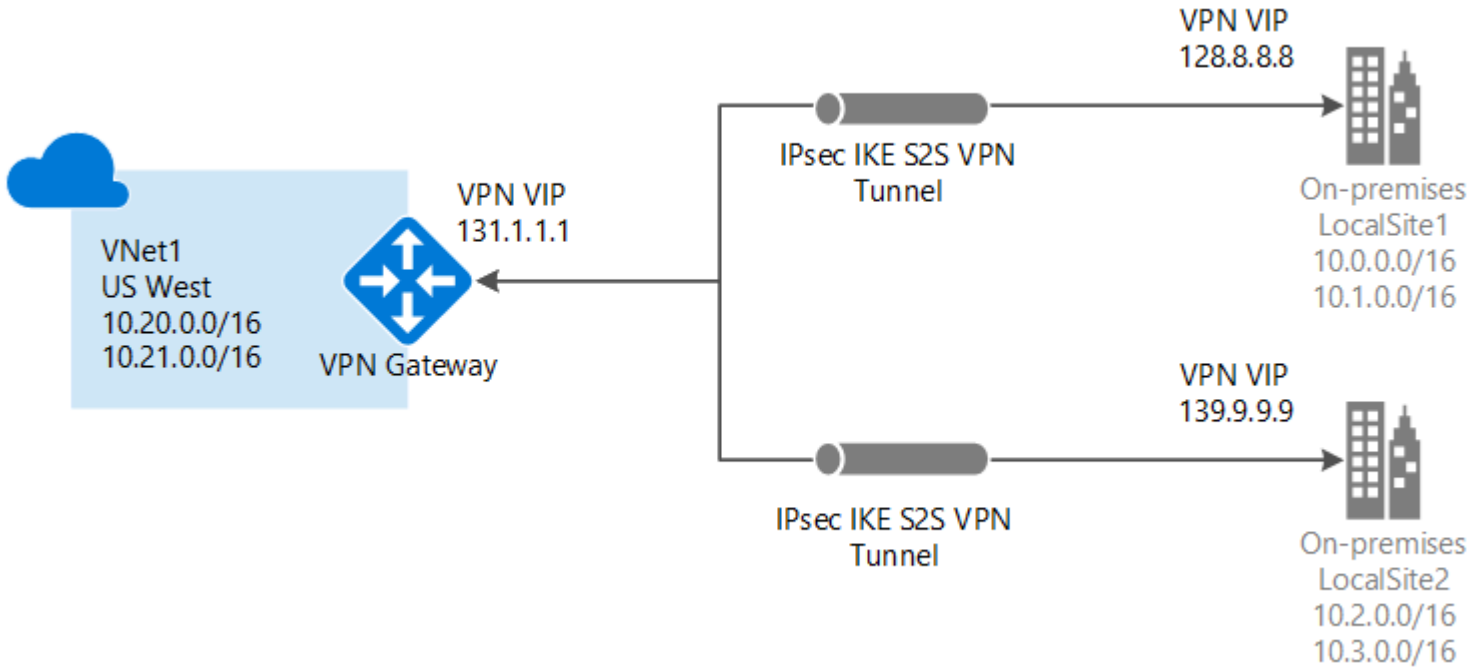
1. VNet-to-VNet: an IPsec/IKE VPN tunnel connection between that VPN gateway and another VPN gateway. The VNets can be:
   - in the same or different regions
   - in the same or different subscriptions
   - in the same or different deployment models



VPN Gateway

Connectivity options through VPN Gateway:

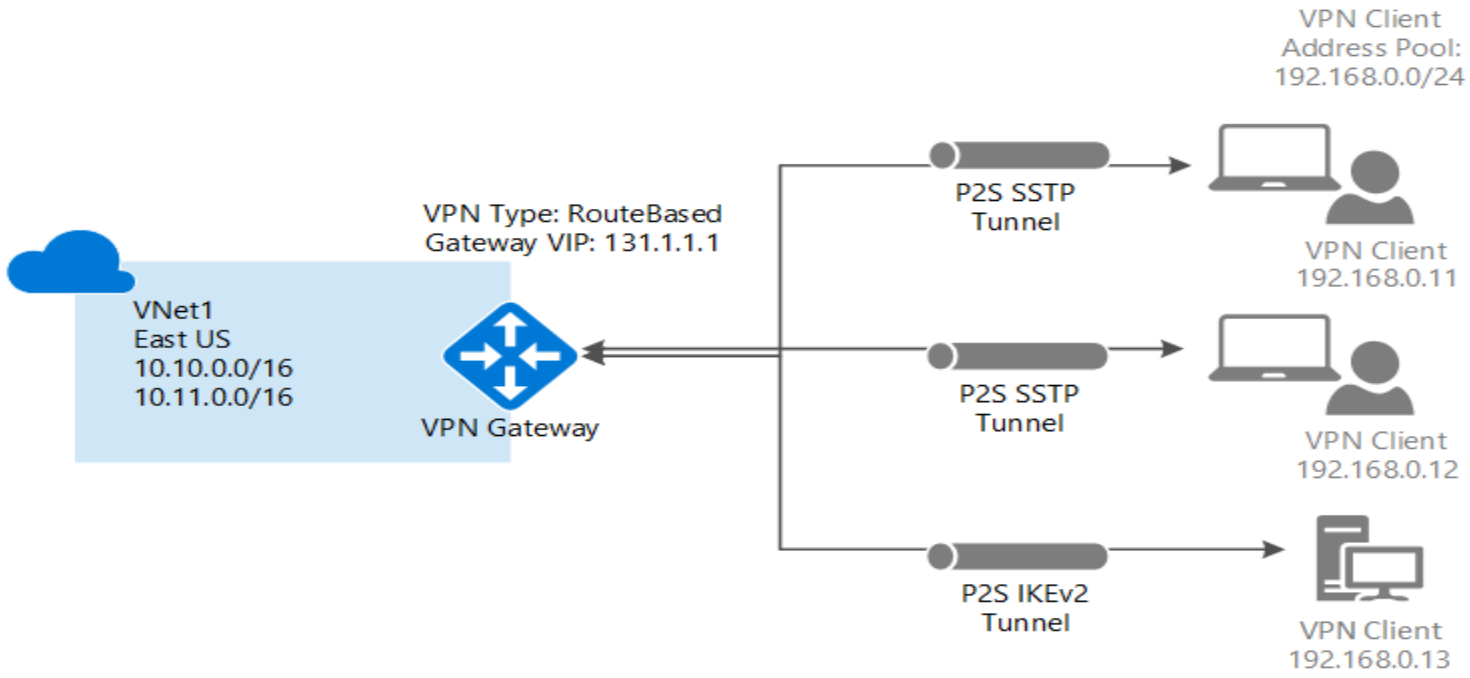
2. Site-to-Site: a cross-premises IPsec/IKE VPN tunnel connection between the VPN gateway and an on-premises VPN device.



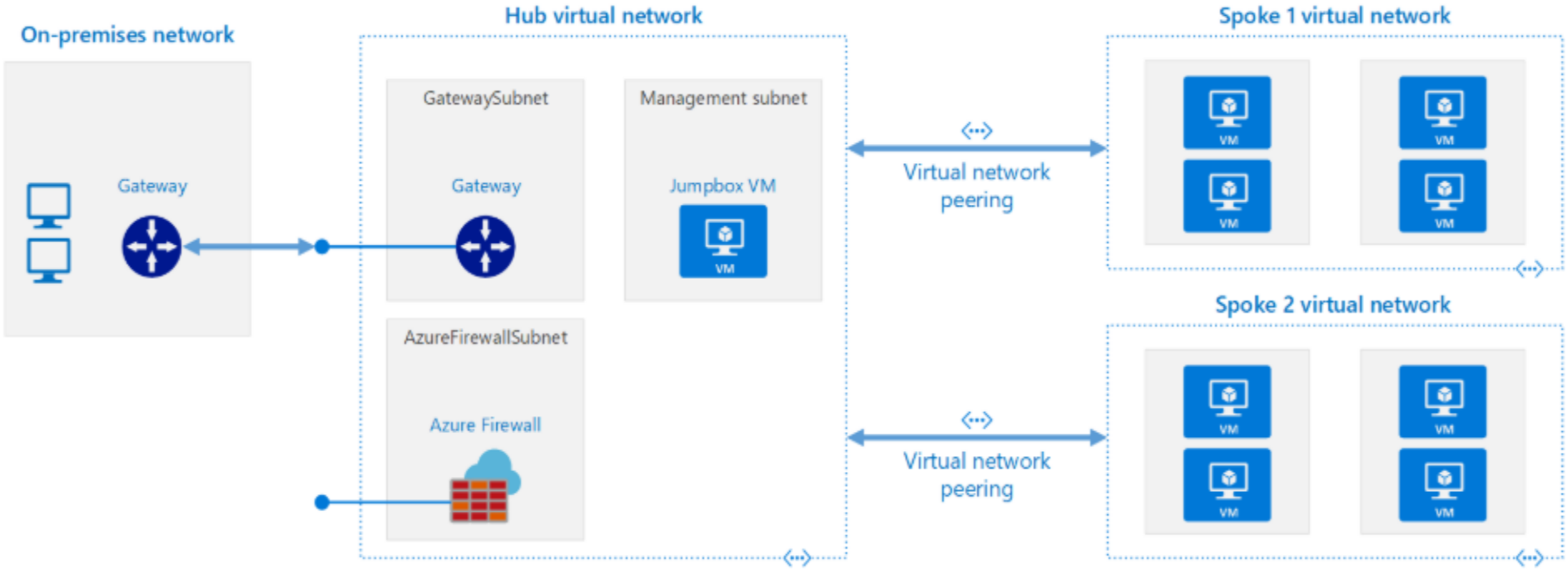
VPN Gateway

Connectivity options through VPN Gateway:

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



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:

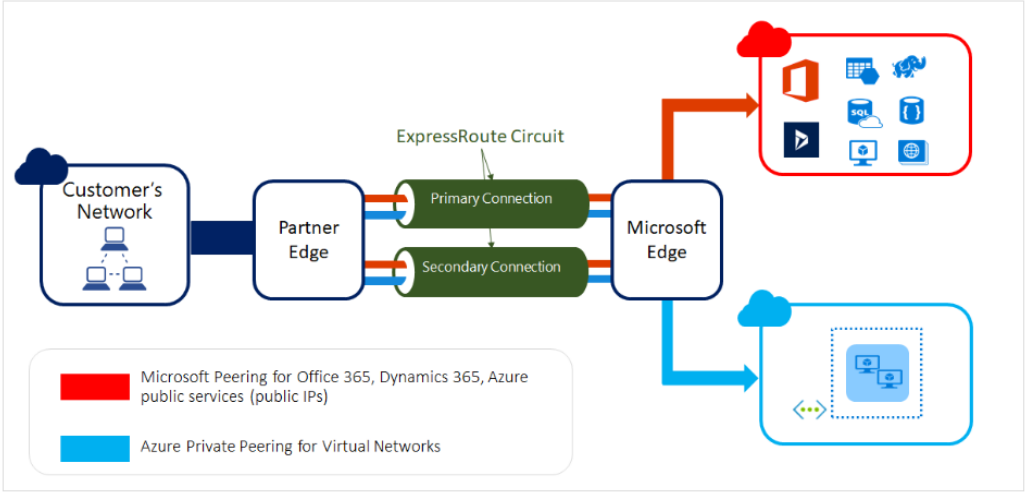
50 Mbps	100 Mbps
200 Mbps	500 Mbps
1 Gbps	10 Gbps

Two pricing models:

1. Metered
2. Unmetered

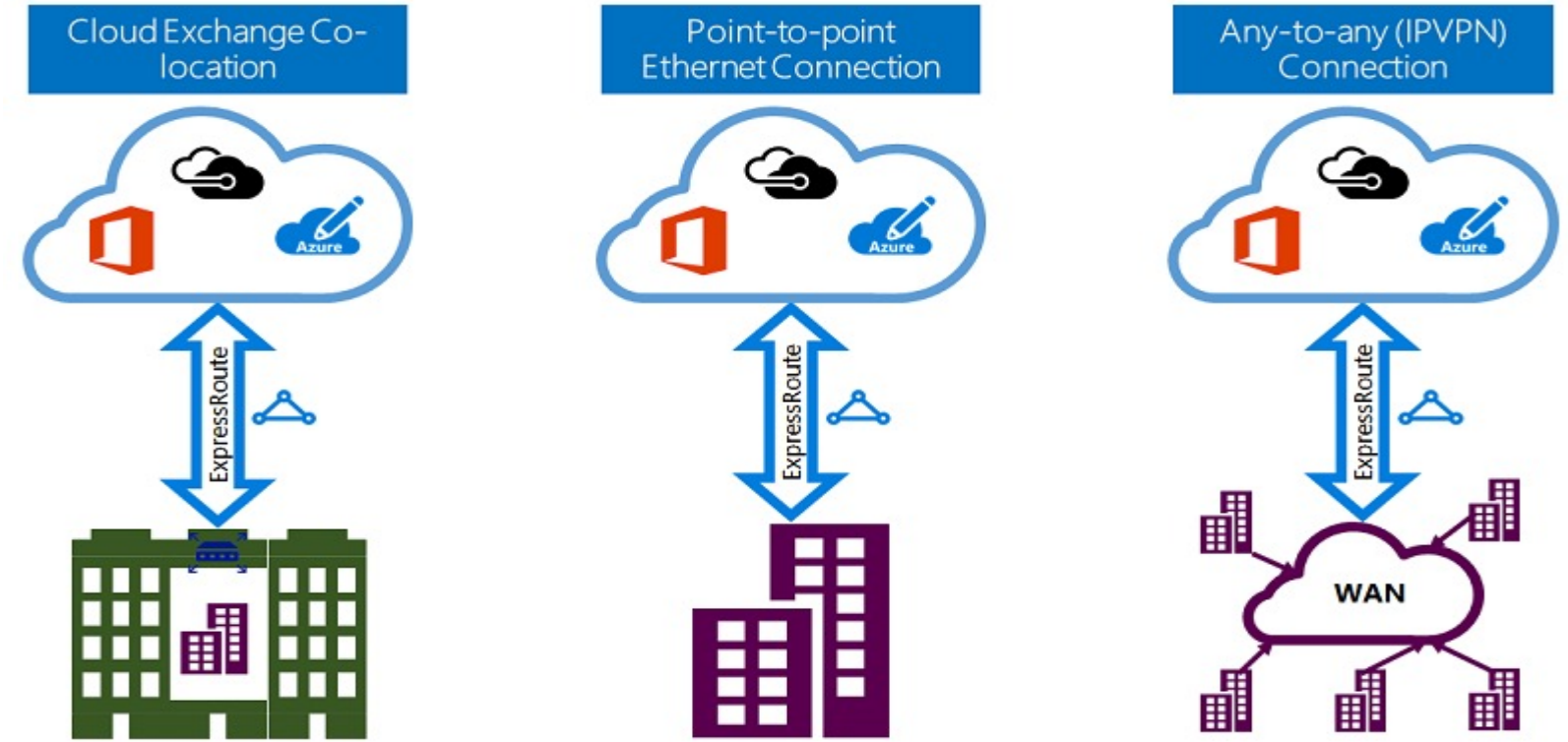
Express Route Direct

Express Route Global Reach



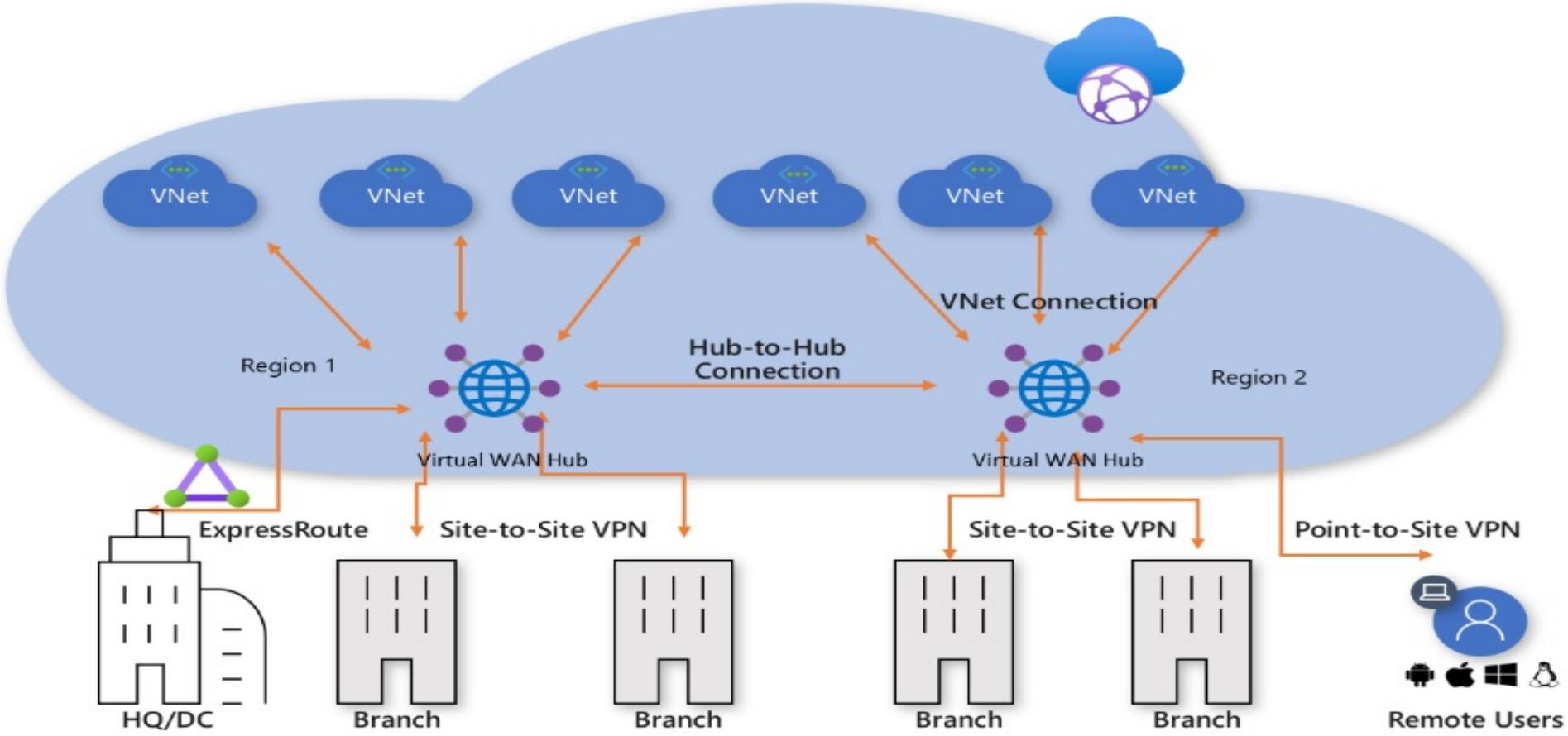
Express Routes

Three different connectivity models:



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

Virtual WAN

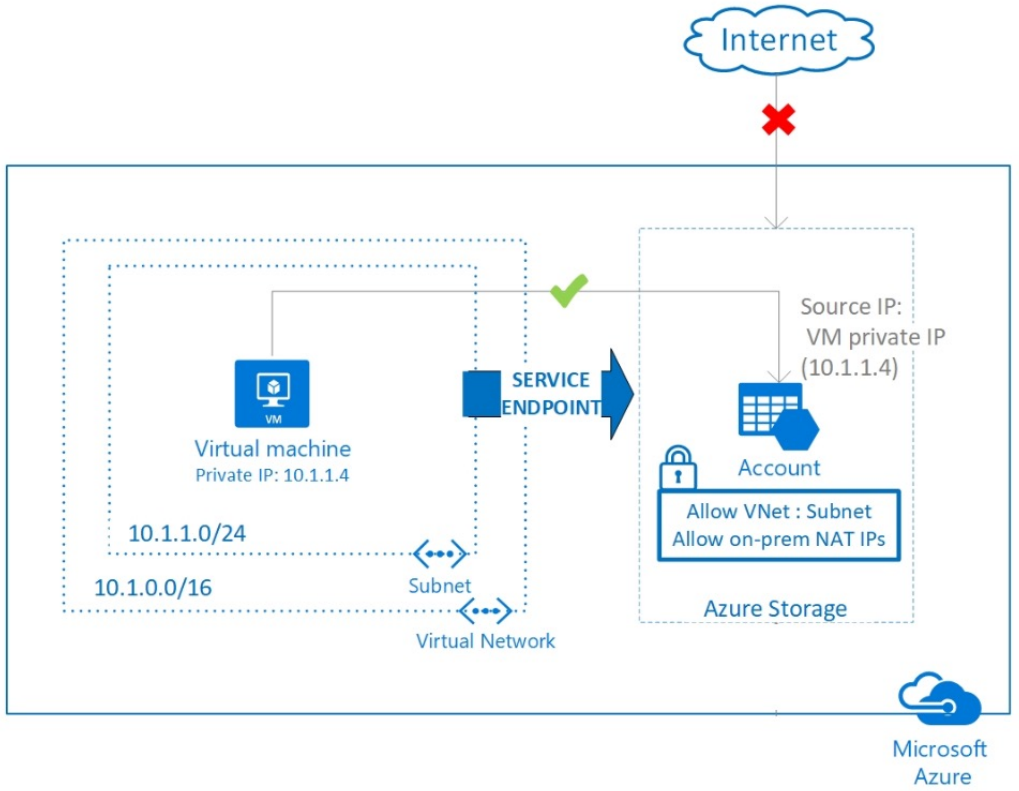

VNet
VNet
VNet
VNet
VNet
VNet
VNet Connection
Region 1
Hub-to-Hub
Connection
Region 2
Virtual WAN Hub
Virtual WAN Hub
ExpressRoute
Site-to-Site VPN
Site-to-Site VPN
Point-to-Site VPN
HQ/DC
Branch
Branch
Branch
Branch
Remote Users

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

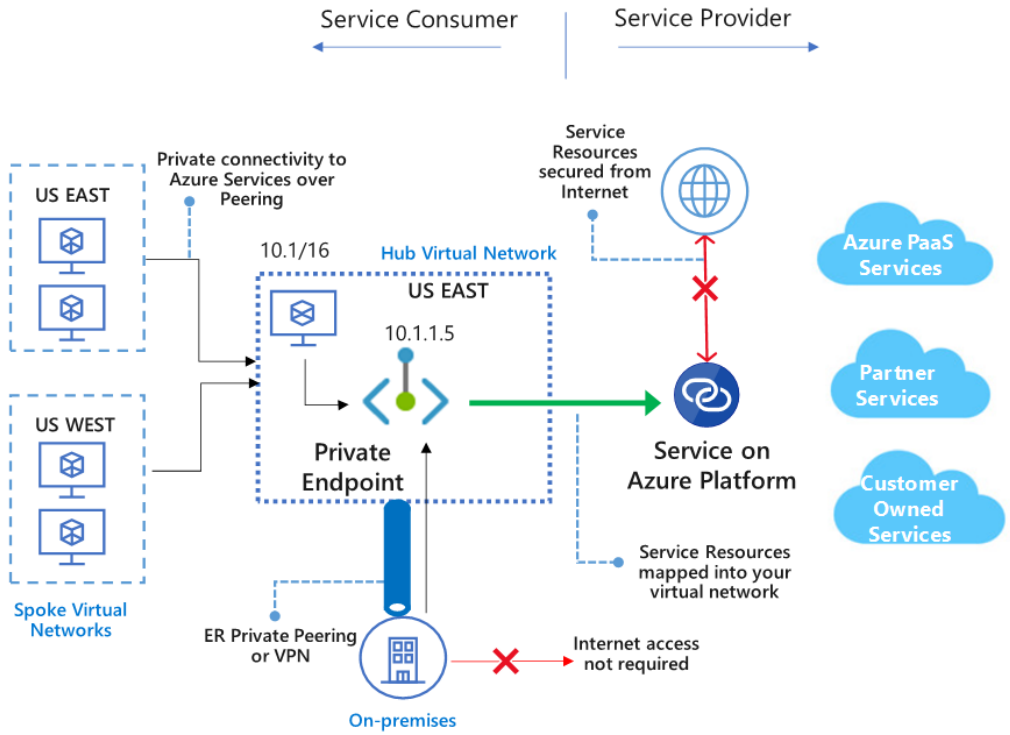


Private Links / Endpoints

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.

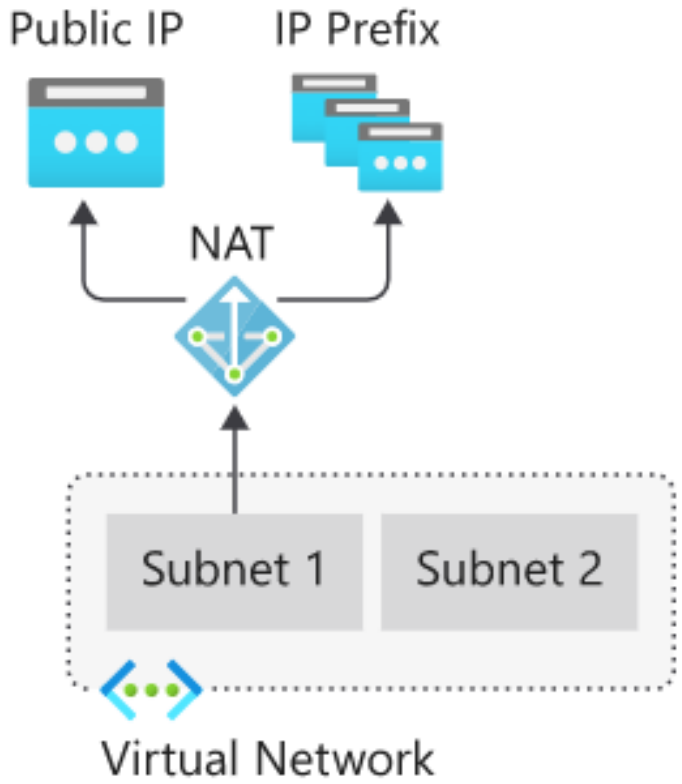


Virtual Network NAT

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

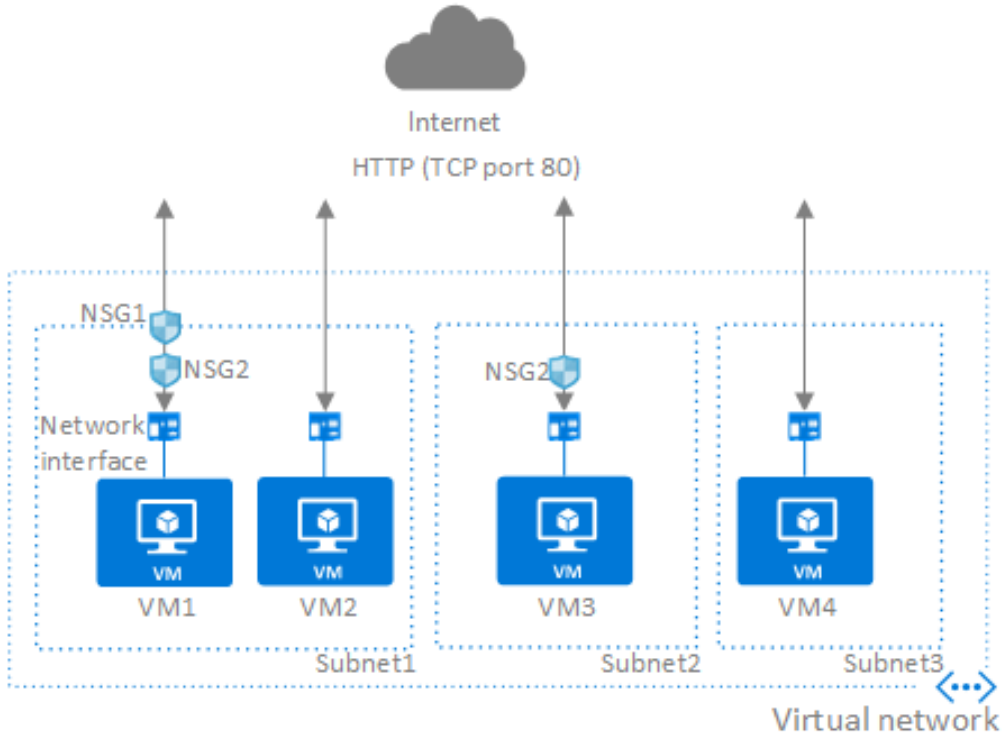
Filter network traffic to and from Azure resources in an Azure virtual network

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.

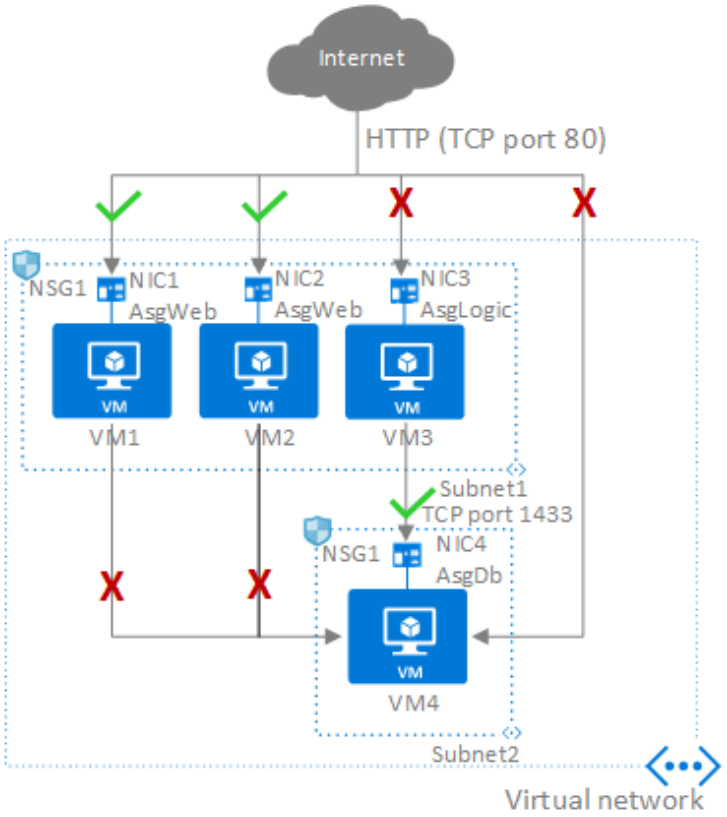


Application Security Groups

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.

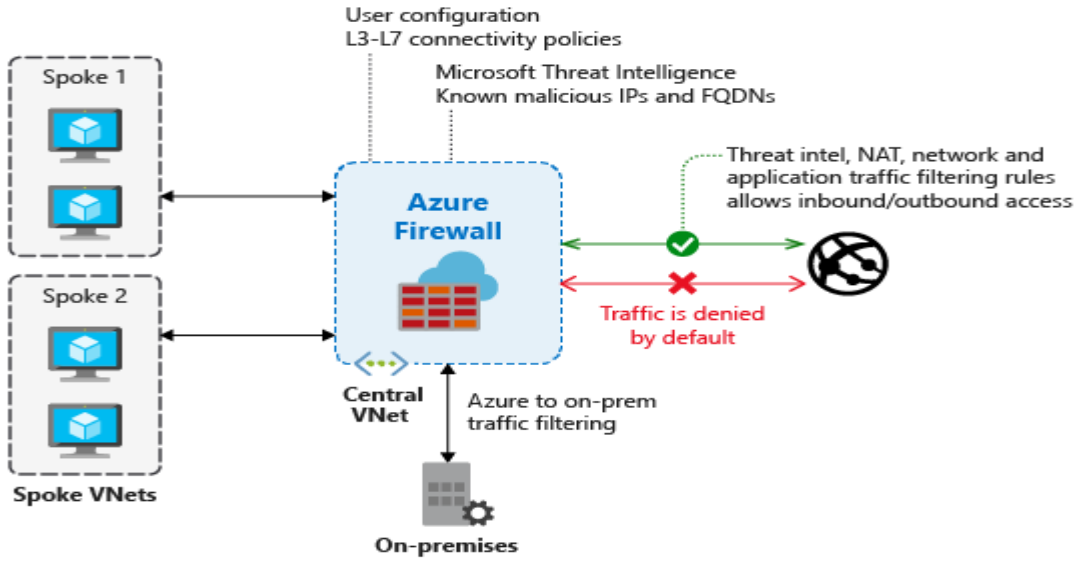


Azure Firewall

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.



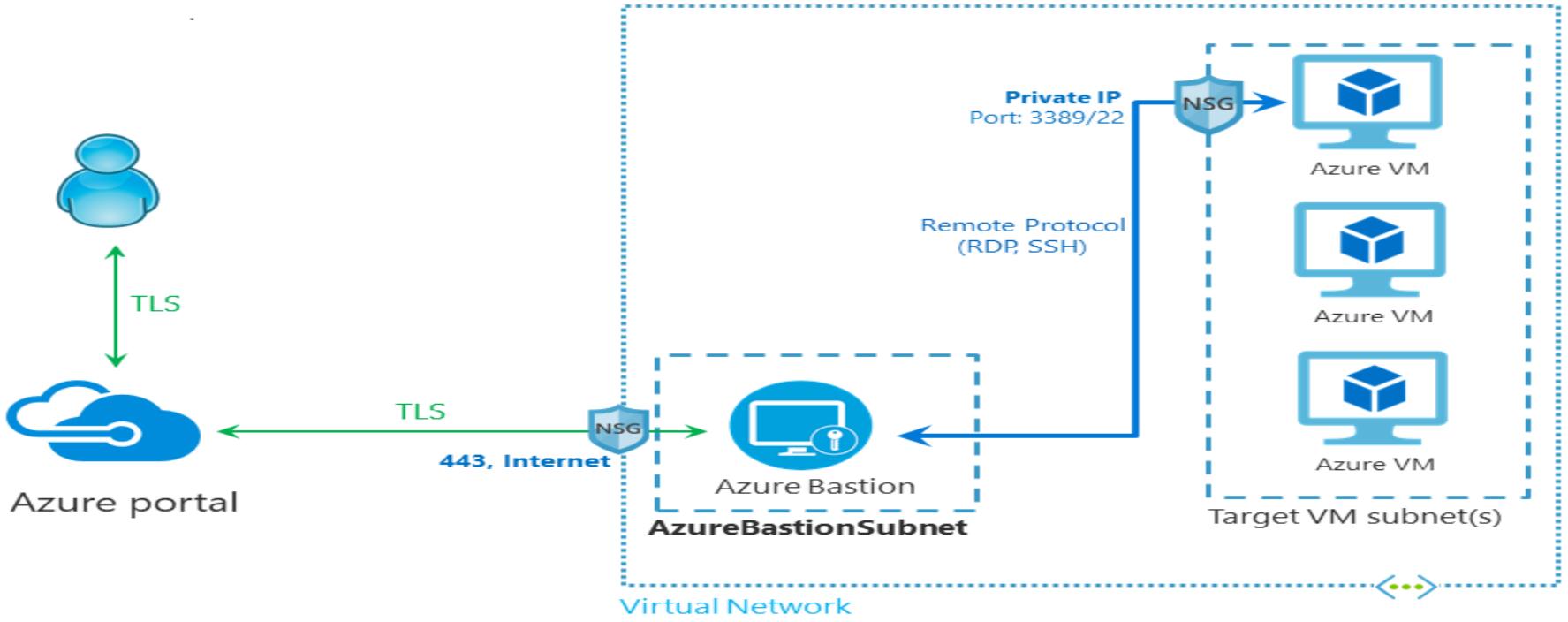
Azure DDoS protection

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

Azure Bastion

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



Load Balancing

Azure Load Balancer

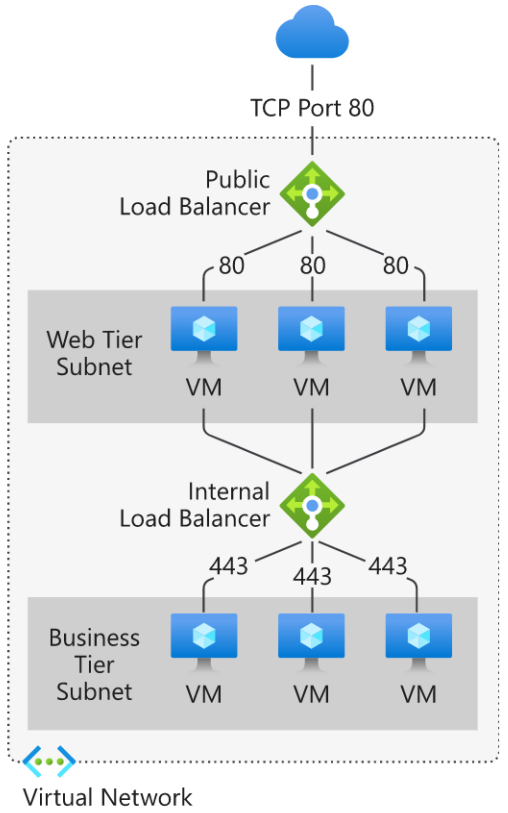
Azure Load Balancer is Layer 4 load balancer.

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.

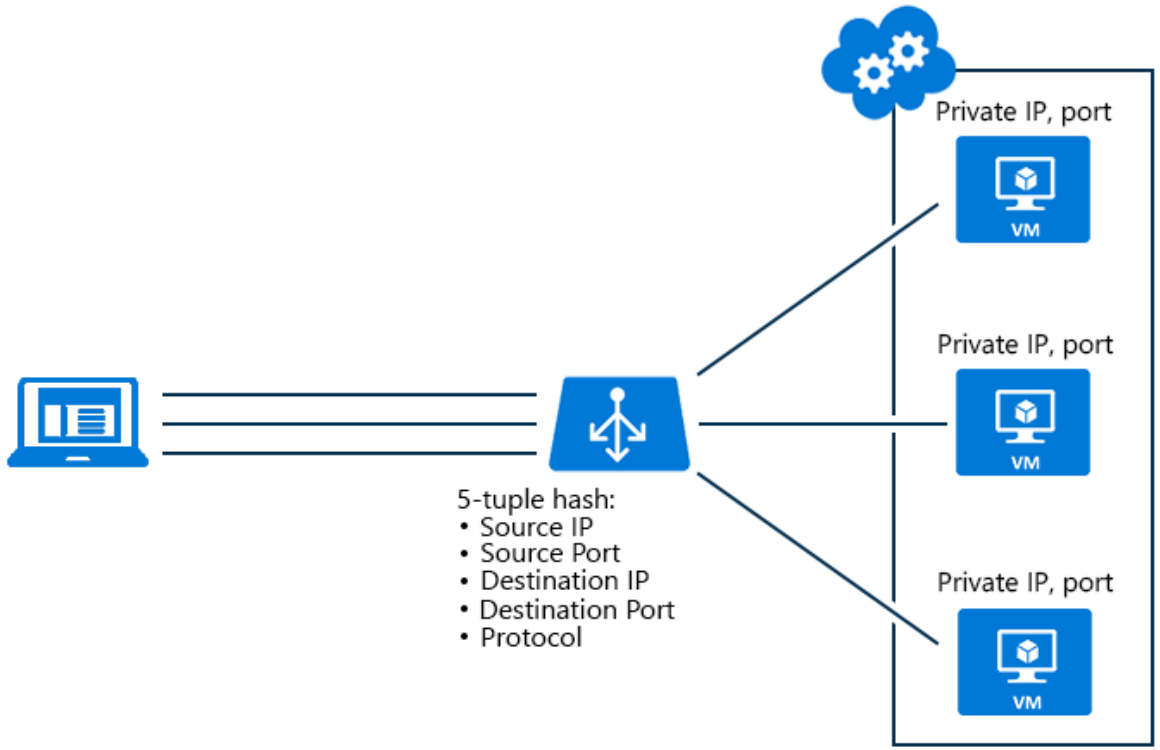


Azure Load Balancer

Source IP affinity mode.

The hash includes

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



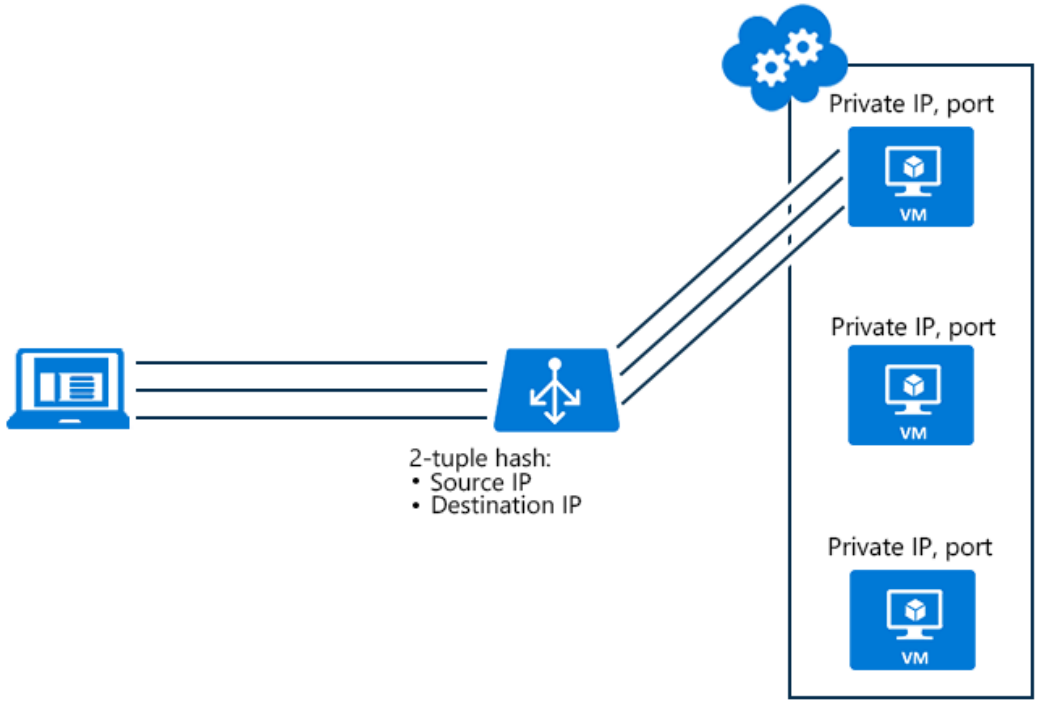
Azure Load Balancer

Source IP Affinity Mode allows sending connections from the same client computer to the same server. It uses a two or three-tuple hash.

Two tuple includes –

- Source IP
- Destination IP

Three tuple also includes protocol type



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.

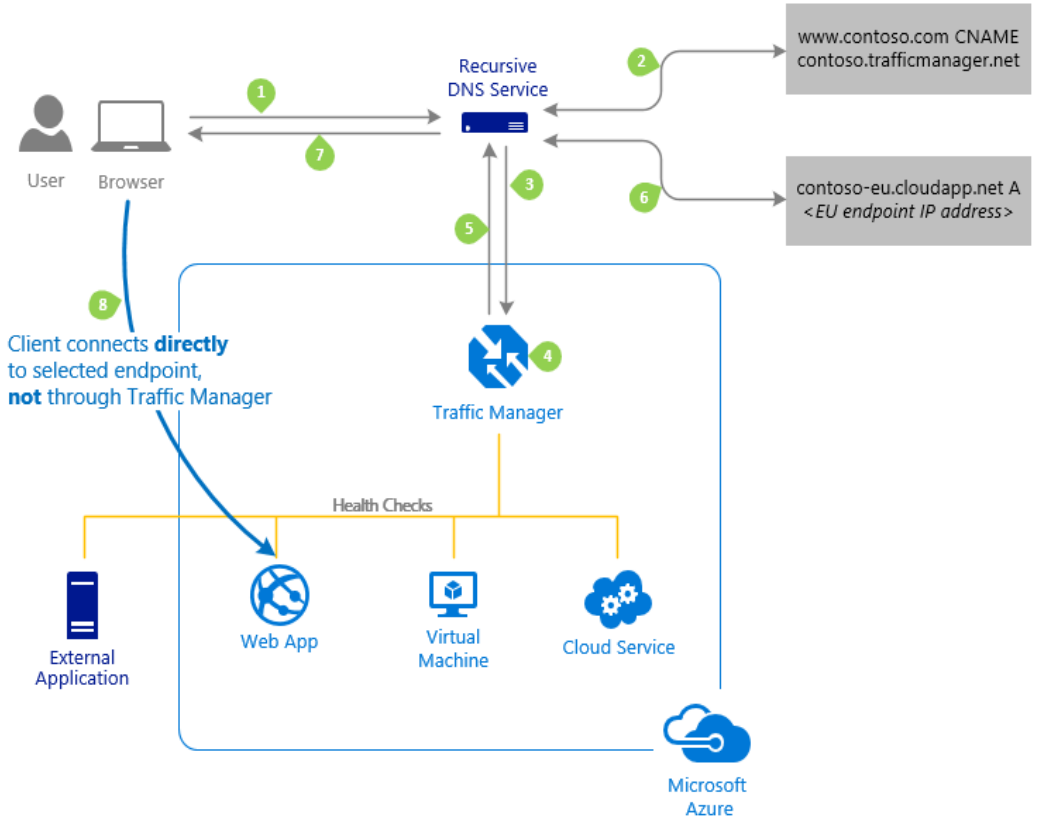
Azure Traffic Manager

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

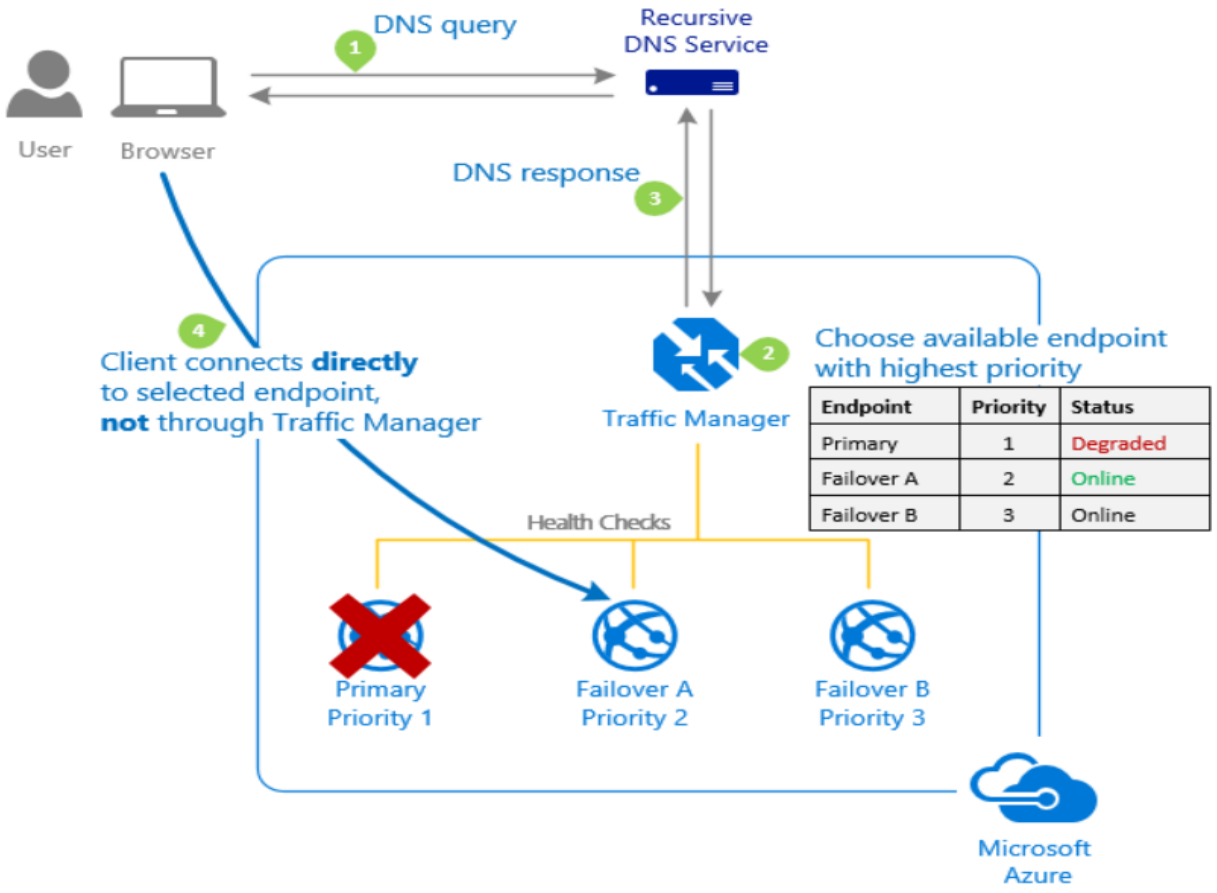
Supports different traffic routing methods including priority, weighted, performance, geographic, multi-value and subnet.

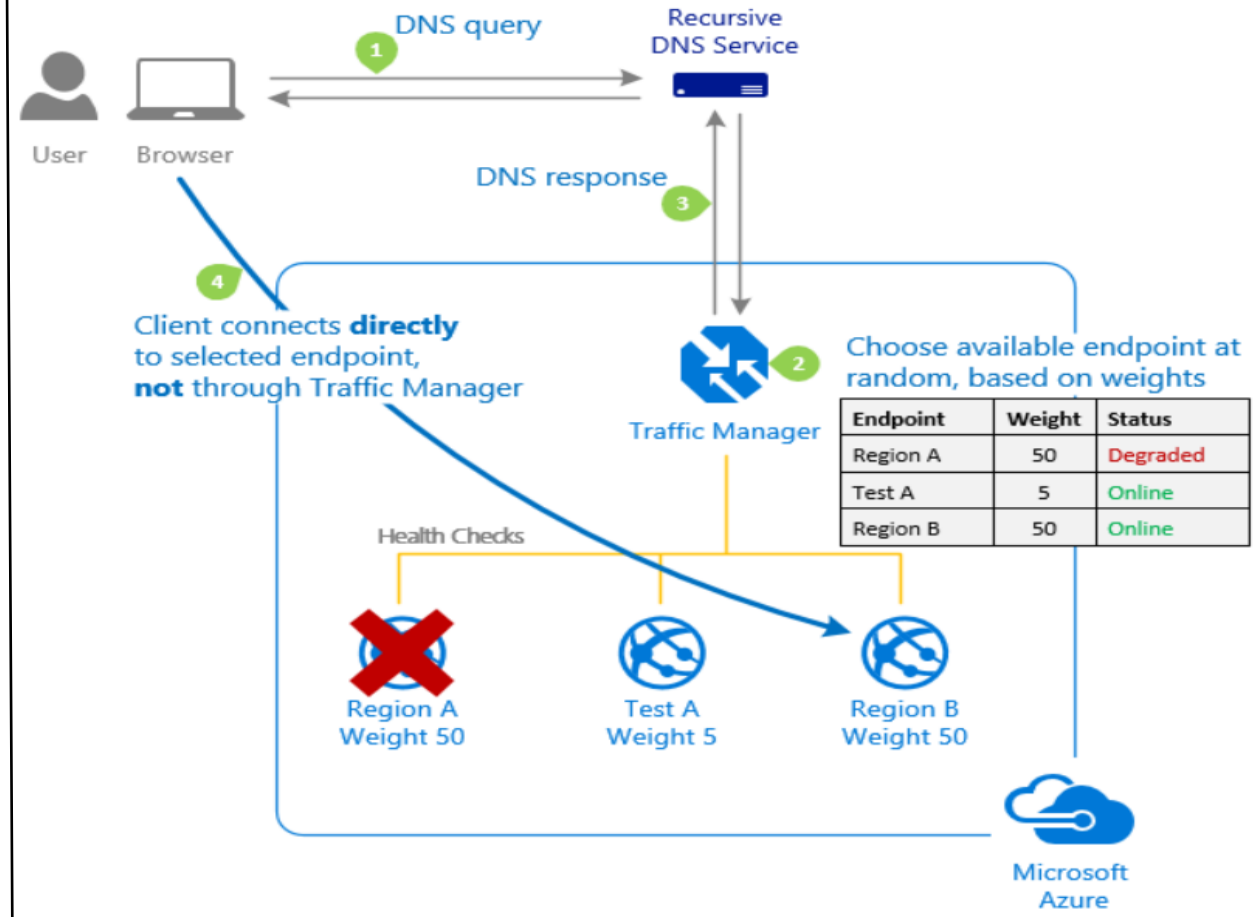
Traffic Manager also monitors the endpoint health continuously and failover automatically when endpoints fail.

Use for routing incoming traffic for high performance and availability



Azure Traffic Manager





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

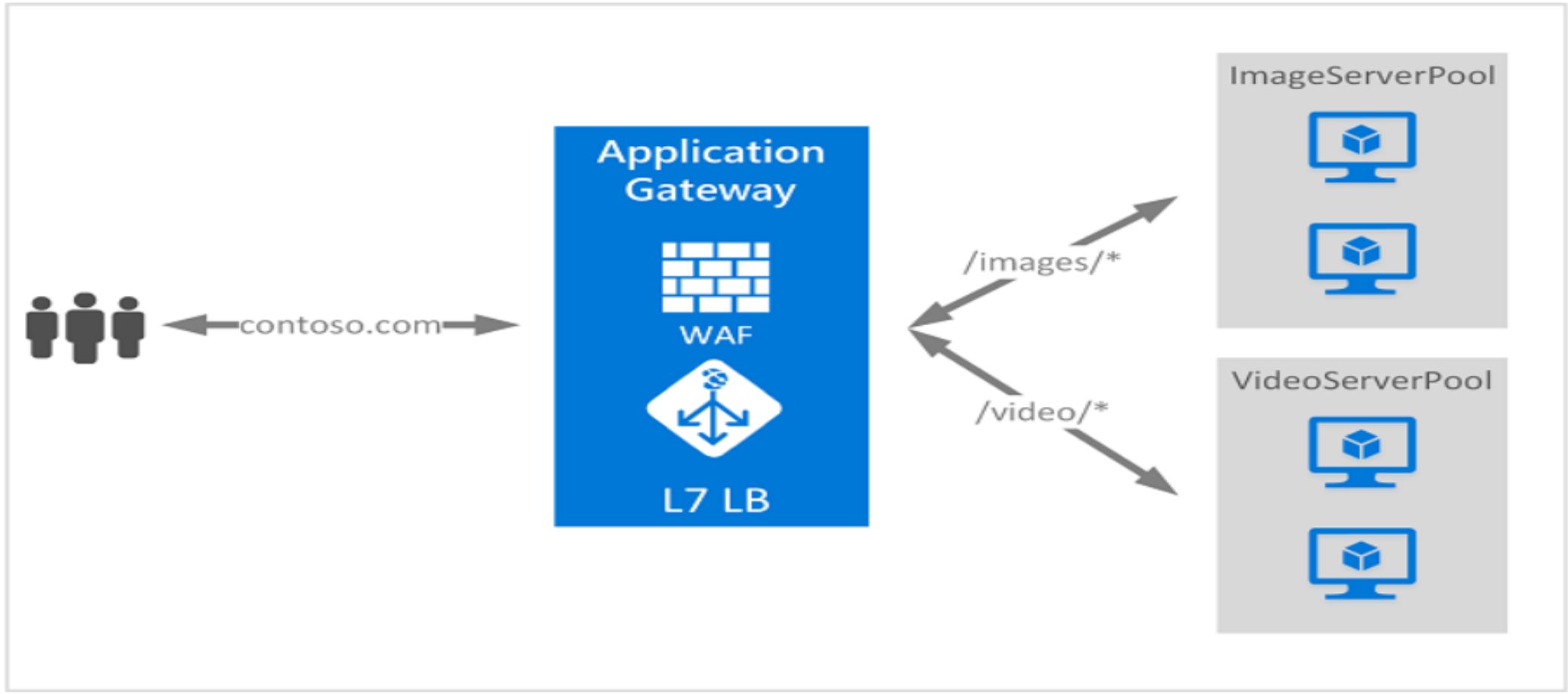
Azure Application Gateway

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

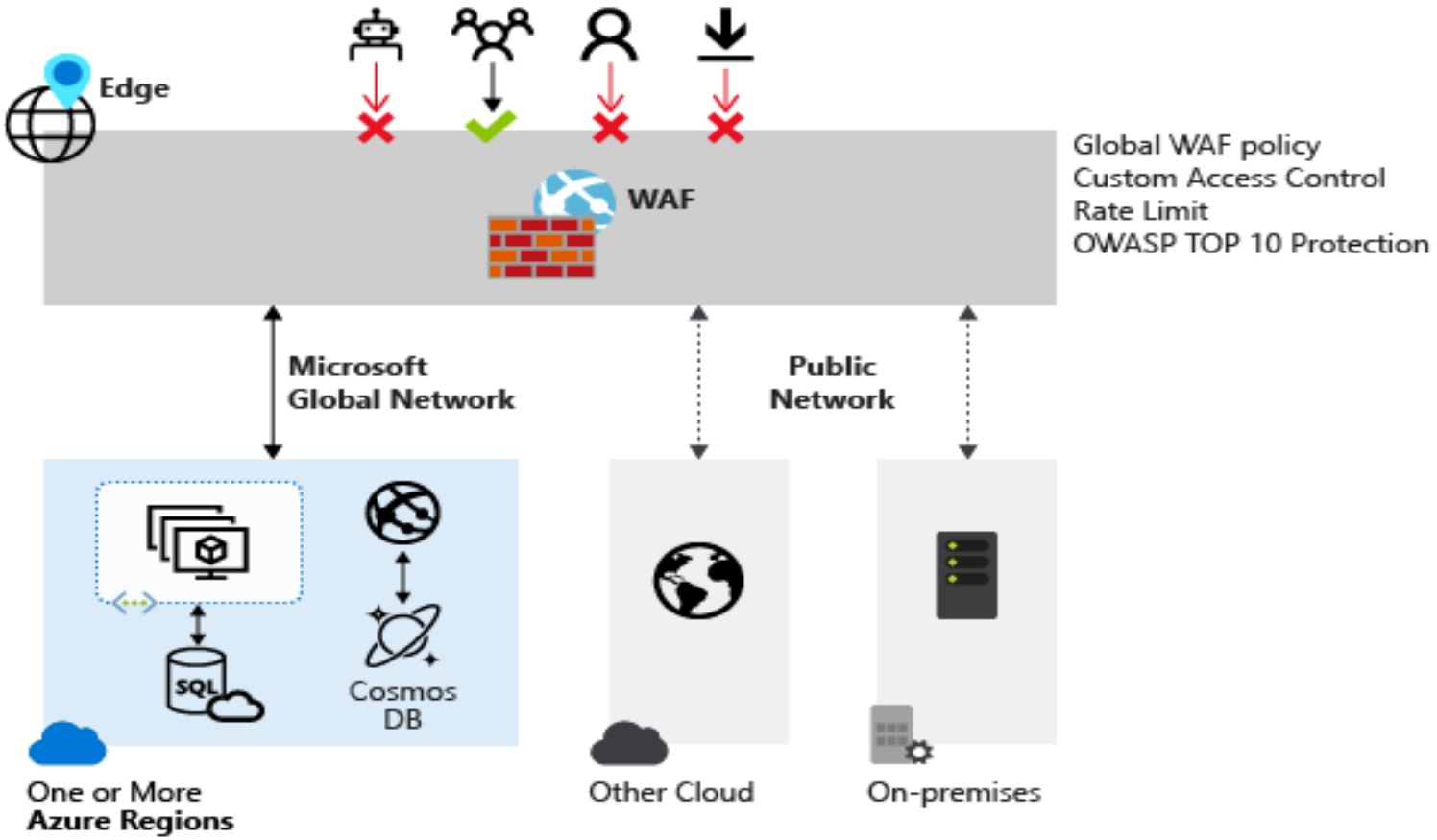
Features:

- 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



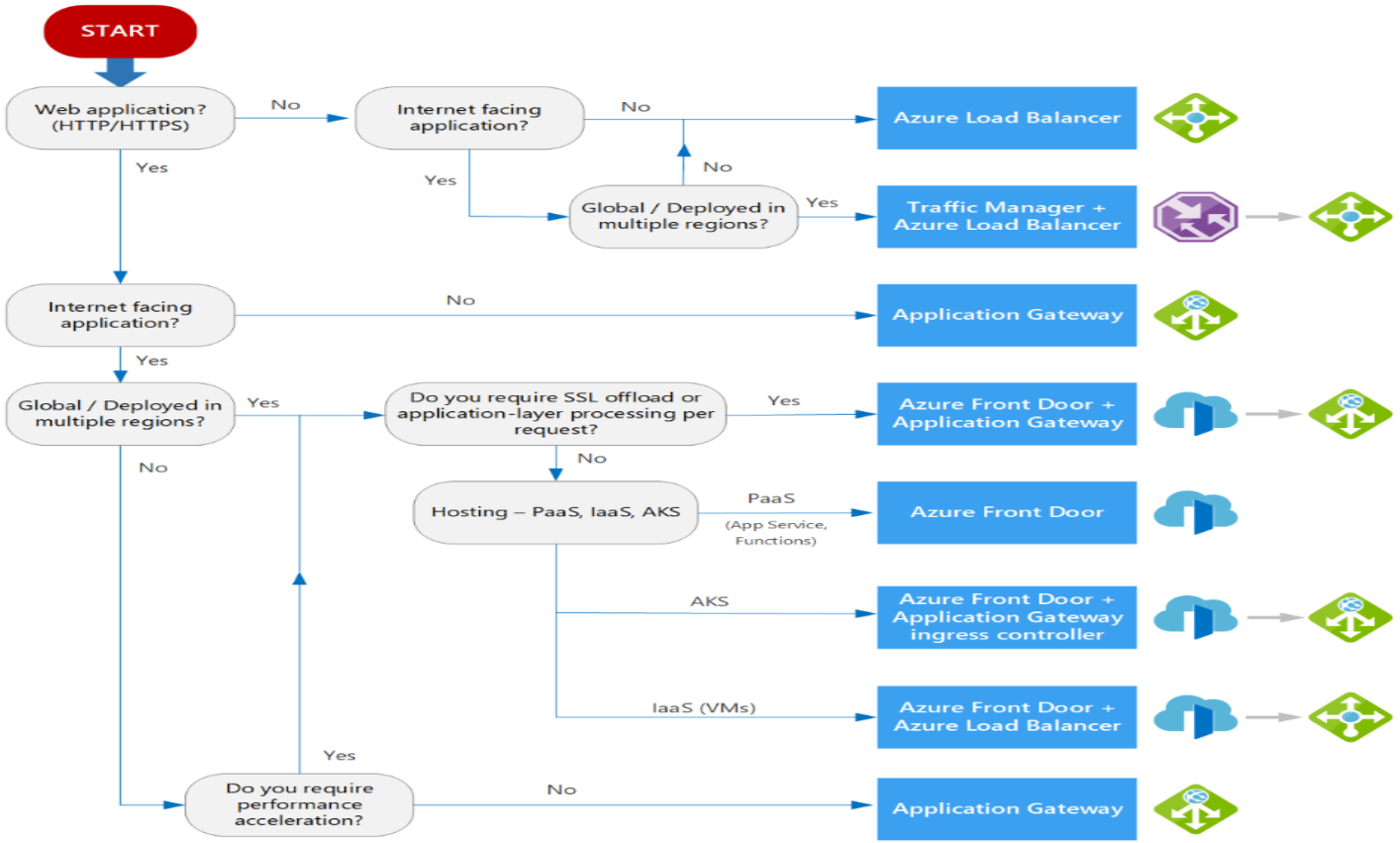
Azure Web Application Firewall



What to use when?

Service	Global/regional	Recommended traffic
Azure Front Door	Global	HTTP(S)
Traffic Manager	Global	non-HTTP(S)
Application Gateway	Regional	HTTP(S)
Azure Load Balancer	Regional	non-HTTP(S)

What to use when?

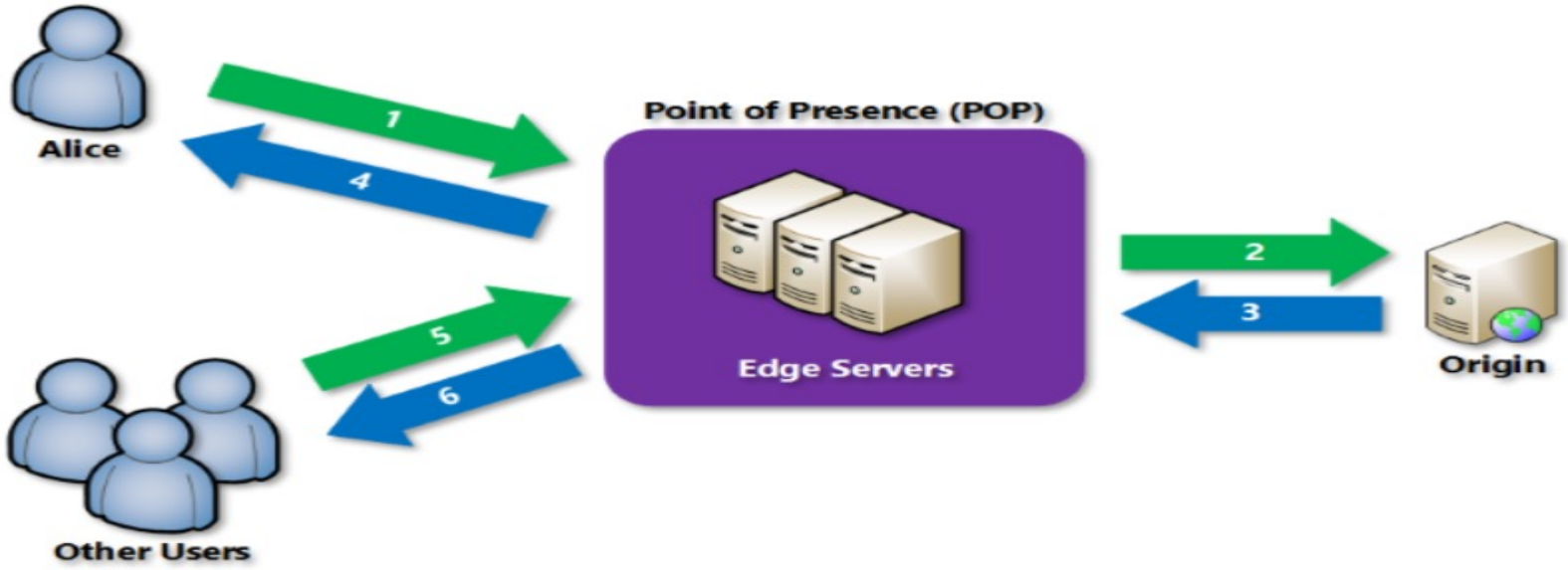


https://docs.microsoft.com/en-us/azure/architecture/guide/technology-choices/load-balancing-overview

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.



Further Learning

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

About me

Director, Global Microsoft Cloud CoE at Capgemini

4x Microsoft Azure MVP since 2020

Leader, Omaha Azure User Group(https://omahaazure.org)

15+ cloud certifications and counting…

https://vaibhavgujral.com

@vaibhavgujral_

https://www.linkedin.com/in/vaibhavgujral/

https://www.youtube.com/c/VaibhavGujral

vaibhav@vaibhavgujral.com

LinkedIn

Twitter

Email

Slides


Q&A


thank
you