CSCI 5902 - Fall 23 - Azure Tutorial

Designed under guidance of Dr. Lu Yang

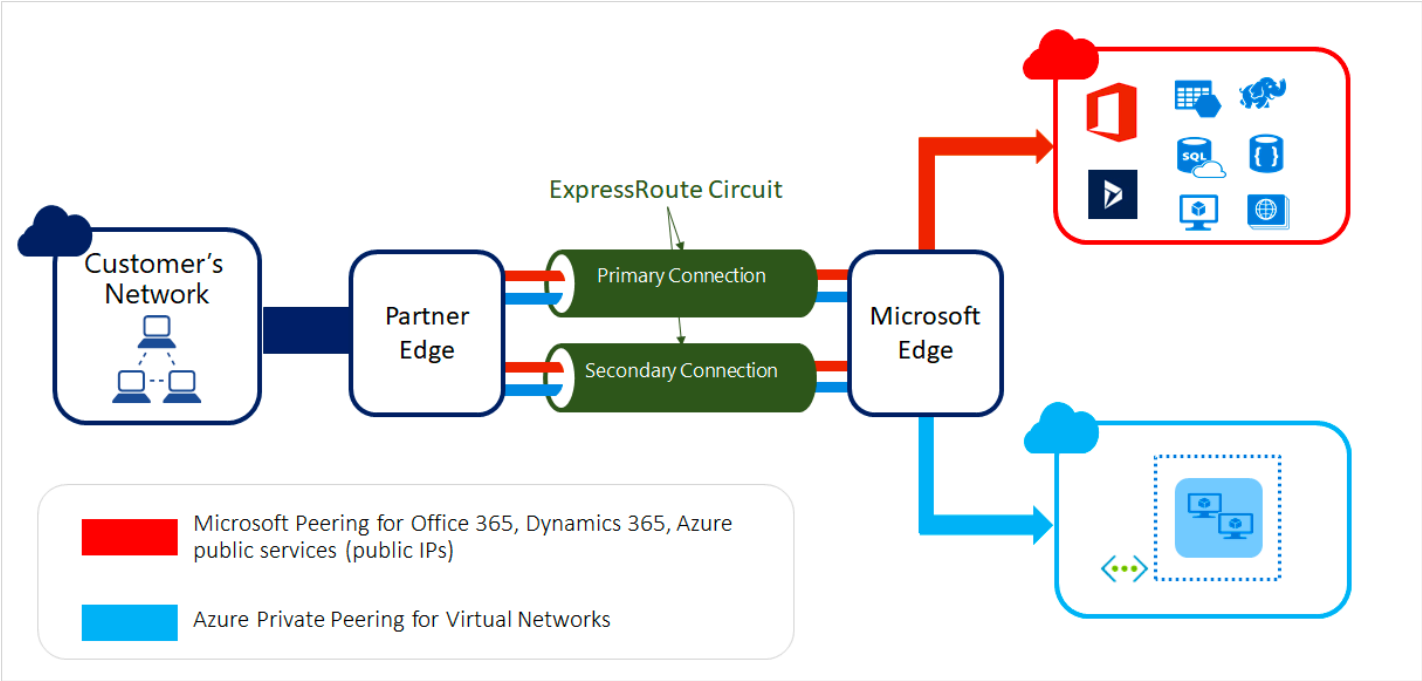
Harmit Narula

Recap

Virtual Network(VNet)

- Azure VNet is the fundamental building block of your private network in Azure.
- A VNet can be used to :
    - Communicate between Azure resources
    - Communicate to other VNets
    - Communicate to internet
    - Communicate with hybrid/on-premise networks
- Network Security Group - Contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources.

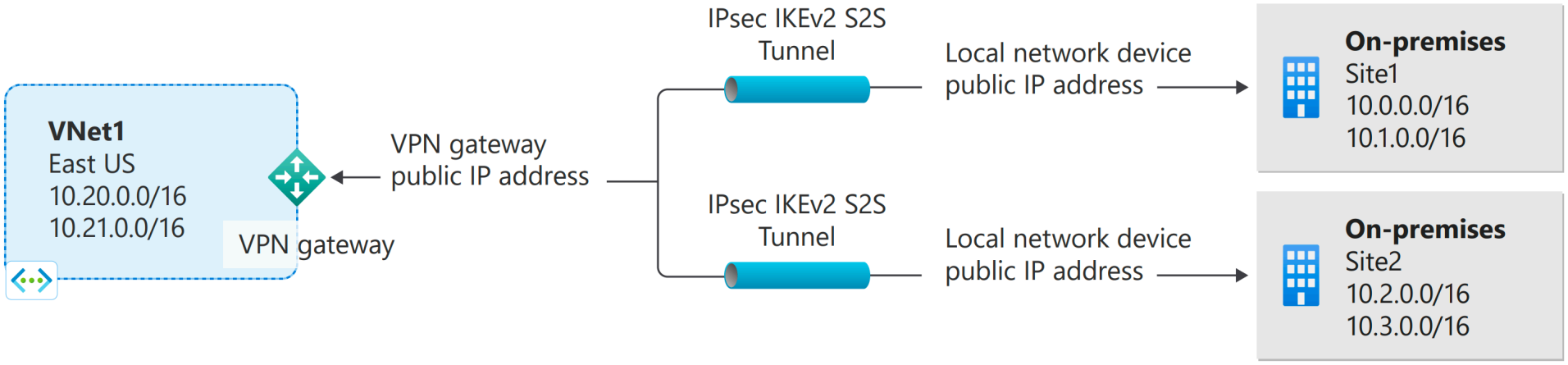
Azure ExpressRoute



Source [1]

Azure VPN Gateway

- VPN Gateway helps you create encrypted cross-premises connections to your virtual network from on-premises locations.
- Can also be used to create encrypted connections between VNets.



Source [1]

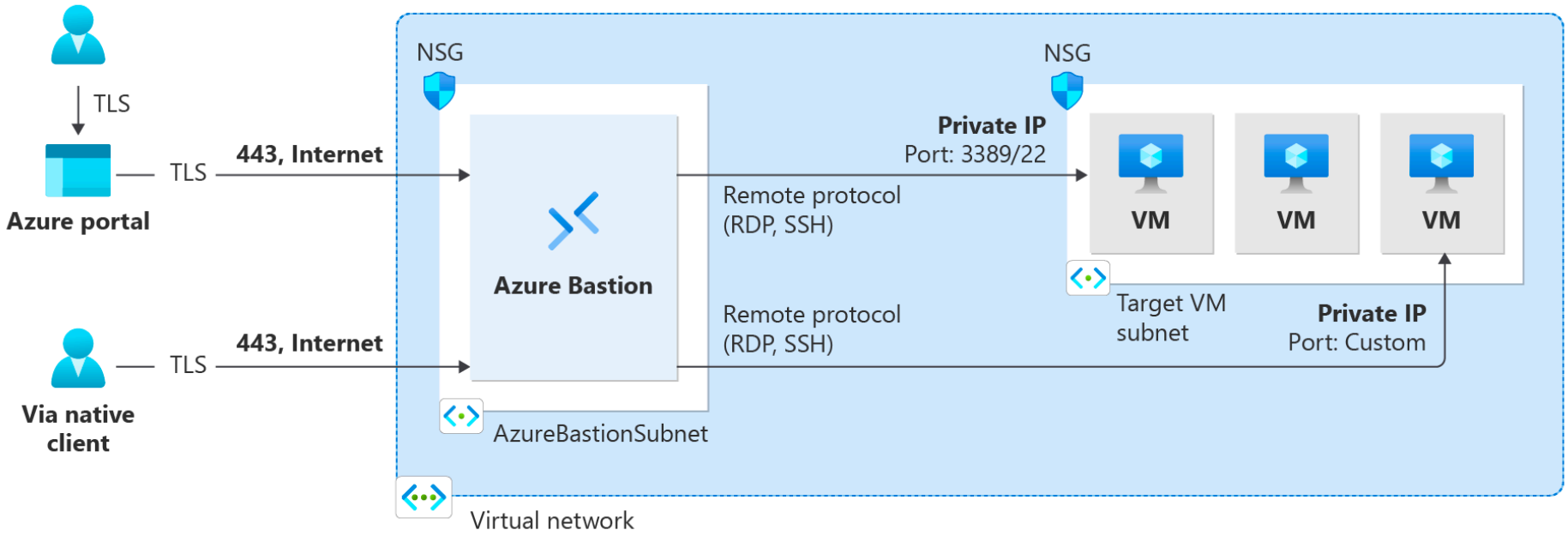
T7 - Azure Network Services

Azure DNS

- Azure DNS provides DNS hosting and resolution using the Microsoft Azure infrastructure.
- Azure DNS consists of three services:
  - Azure Public DNS
  - Azure Private DNS
  - Azure Private DNS Resolver

Azure Bastion

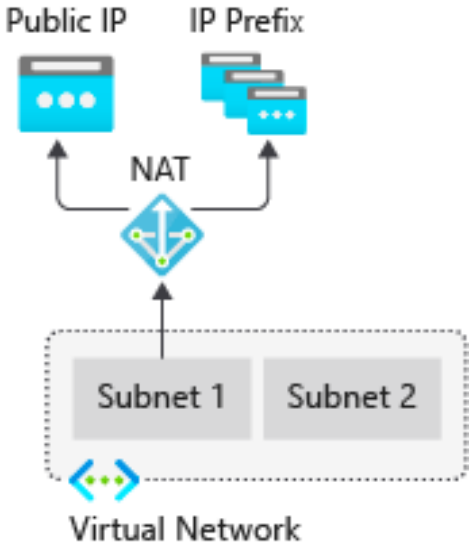
- Azure Bastion service is a fully platform-managed PaaS service which can be deployed inside virtual network.
- It provides secure and seamless RDP/SSH connectivity to the virtual machines directly from the Azure portal over TLS.



Source [1]

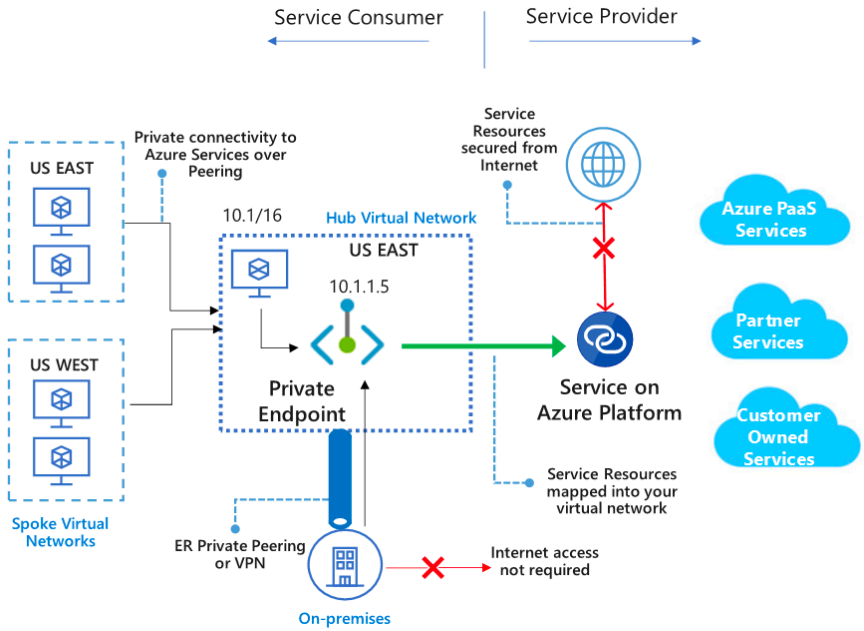
NAT Gateway

- Azure NAT Gateway is a fully managed and highly resilient Network Address Translation (NAT) service.
- Azure NAT Gateway allows all instances in a private subnet connect outbound to the internet while remaining fully private.



Azure Private Link

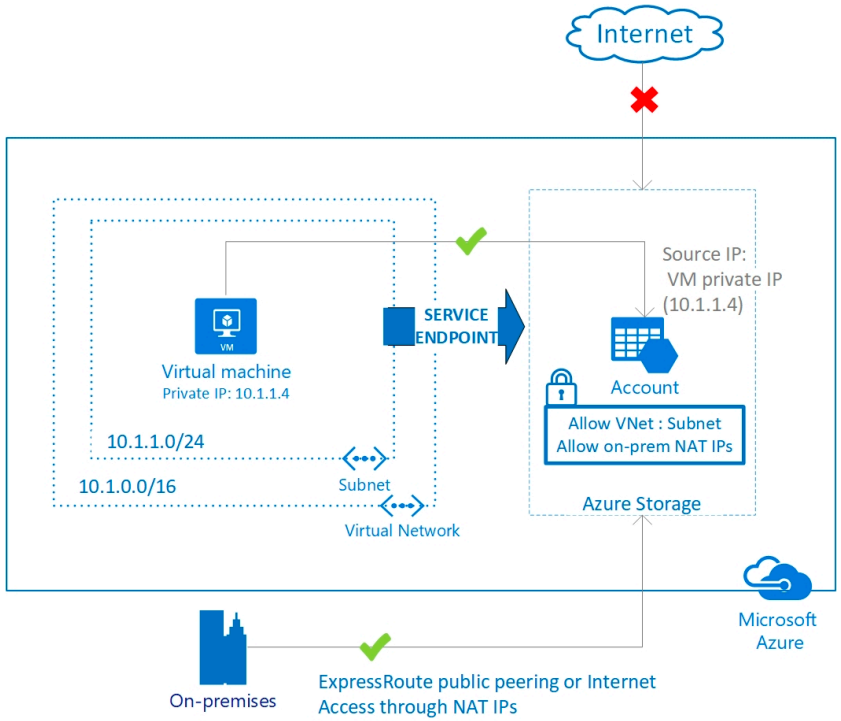
- Azure Private Link enables you to access Azure PaaS Services like Azure Storage and SQL Database and Azure hosted customer-owned/partner services over a private endpoint in your virtual network.
- Traffic between your virtual network and the service travels through the Microsoft backbone network.



Source [1]

Azure Service Endpoints

- Service endpoints extend your virtual network private address space and the identity of your VNet to the Azure services, over a direct connection.

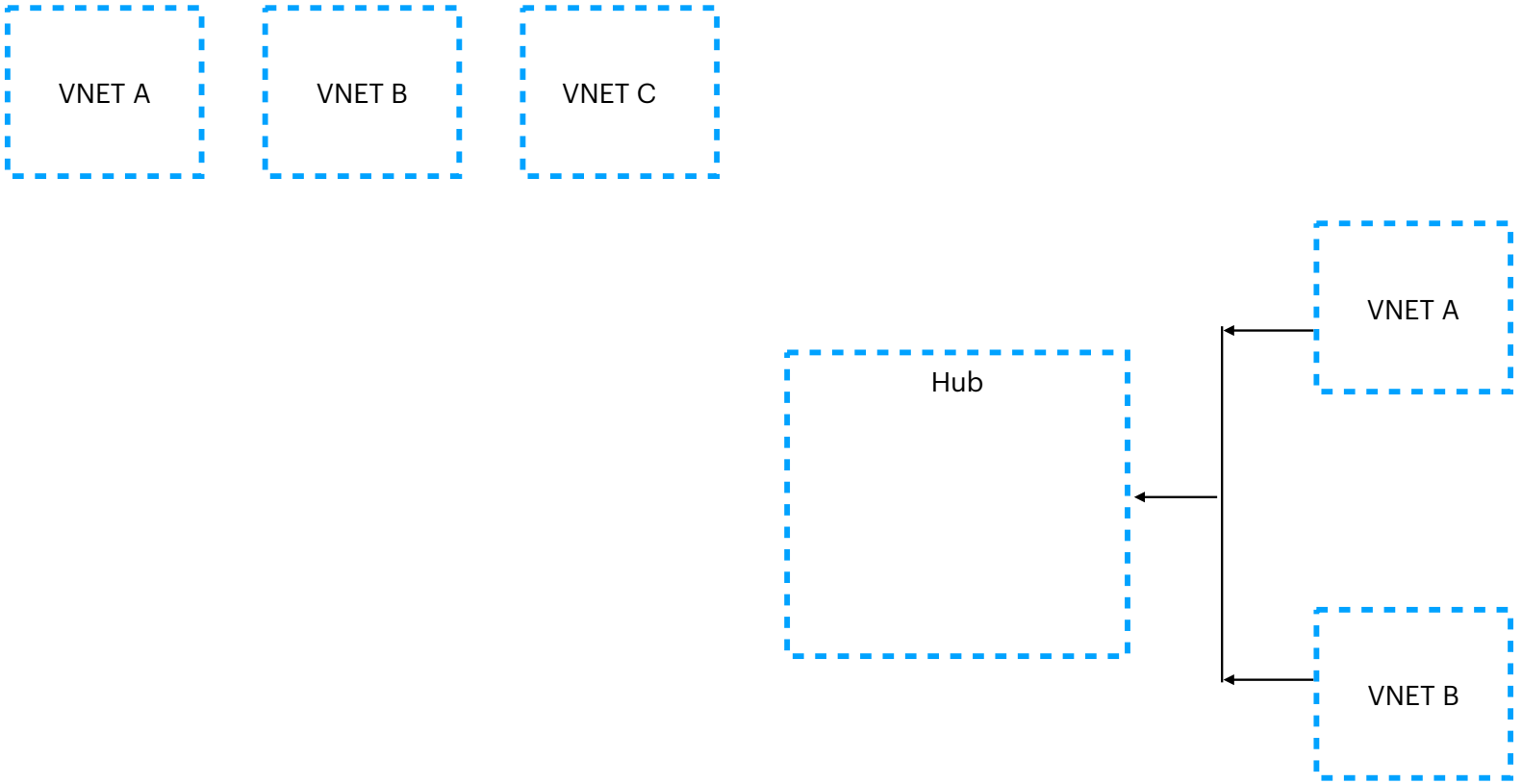


Source [1]

How different VNets interact with each other?

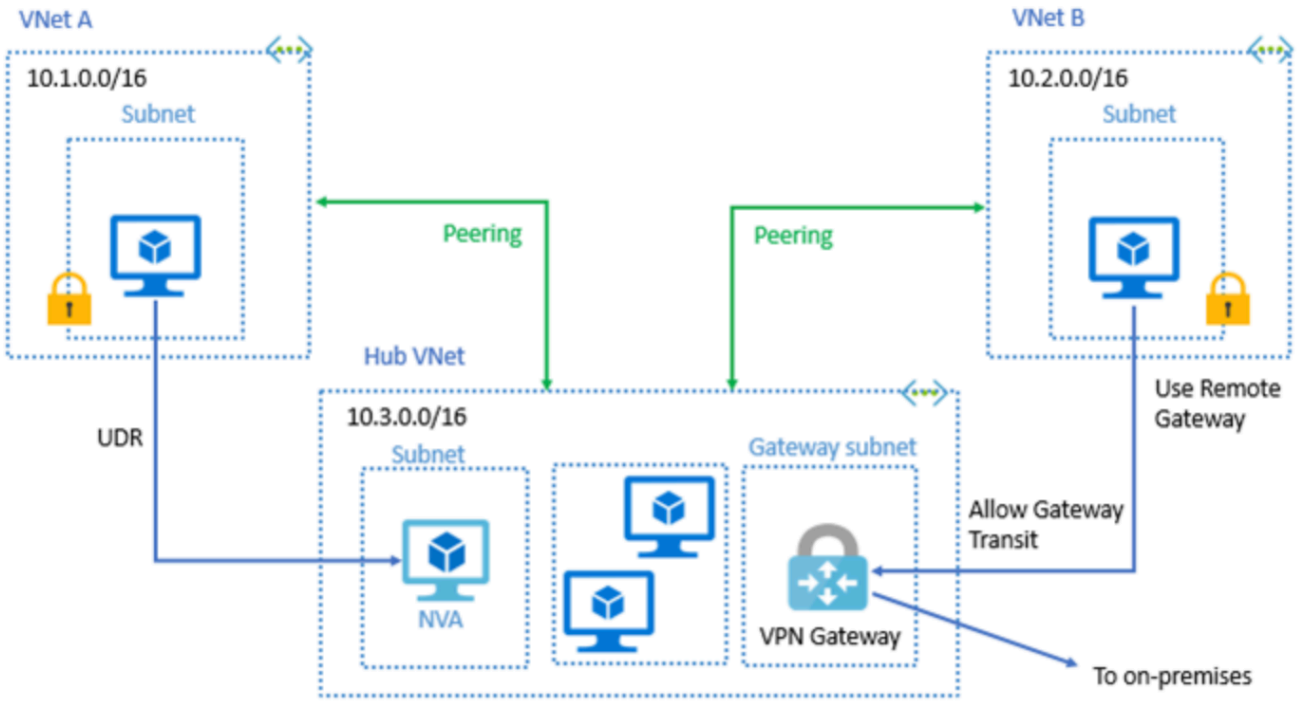
VNet Peering

- A virtual network peering allows connection between two or more VNets.
- The traffic between peered VNets flow over MS backbone network.
- Azure supports 2 types of peering:
  - Virtual network Peering: Same region
  - Global VNet Peering: Across regions
- The network latency between resources in peered VNets in the same regions is same as that of single VNet.
- VNet peering is non-transitive.

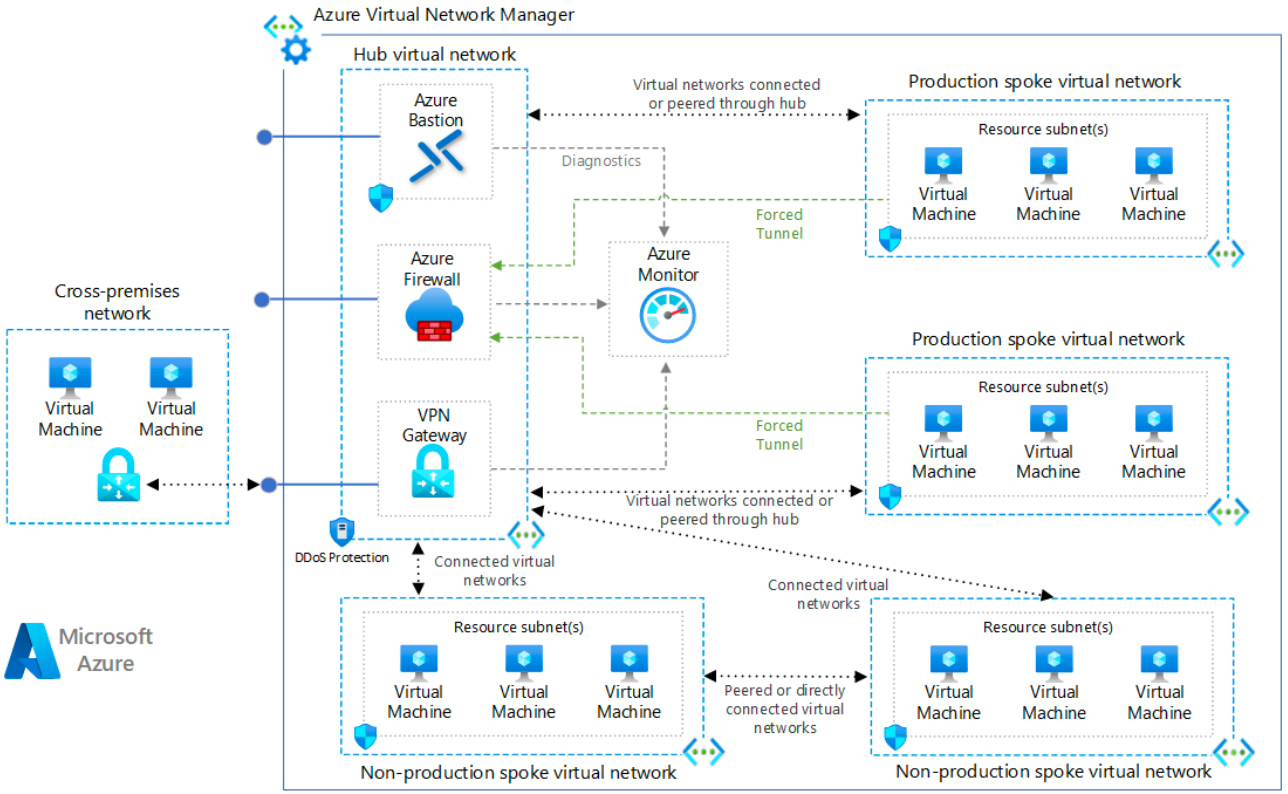

VNET A
VNET B
VNET C
Hub
VNET A
VNET B

Service Chaining

- Virtual network peering enables the next hop in a user-defined route to be the IP address of a virtual machine in the peered virtual network or a VPN gateway.
- Service chaining enables you to direct traffic from one virtual network to a virtual appliance, or virtual network gateway, in a peered virtual network, through user-defined routes


VNet A
10.1.0.0/16
Subnet
Peering
Peering
VNet B
10.2.0.0/16
Subnet
Hub VNet
10.3.0.0/16
Subnet
Gateway subnet
UDR
NVA
VPN Gateway
Allow Gateway Transit
Use Remote Gateway
To on-premises

Hub & Spoke Reference Architecture



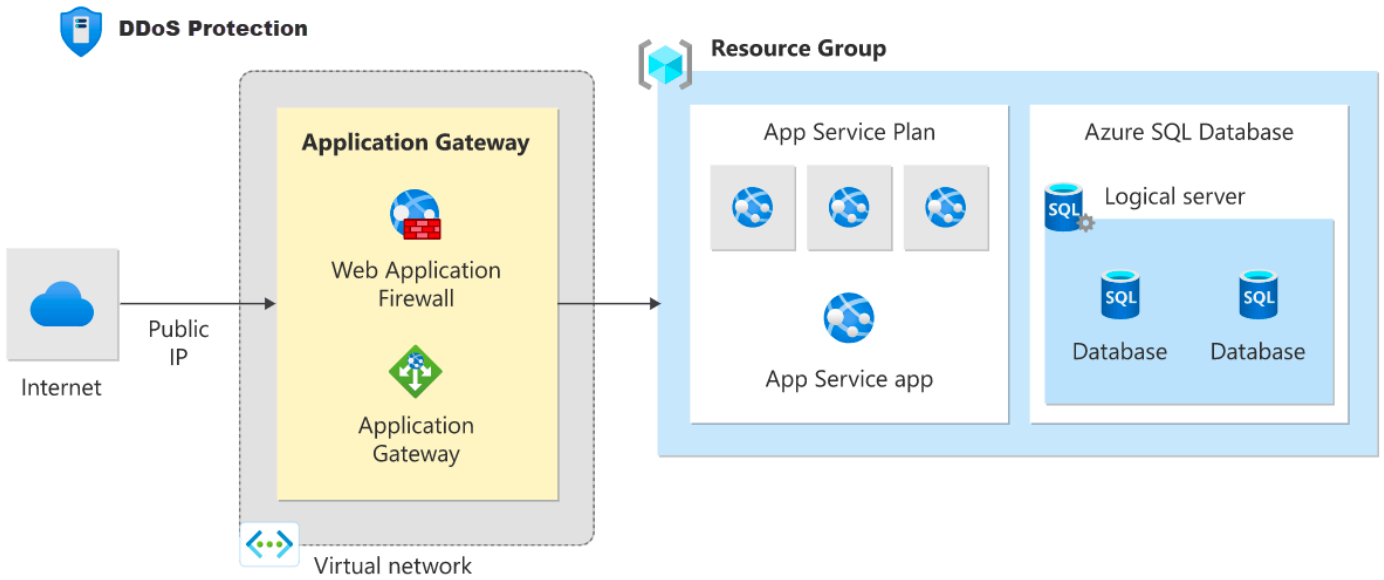
Source : [2]

We are moving to cloud what's the biggest availability and security concern?

DDoS Attacks

Azure DDoS

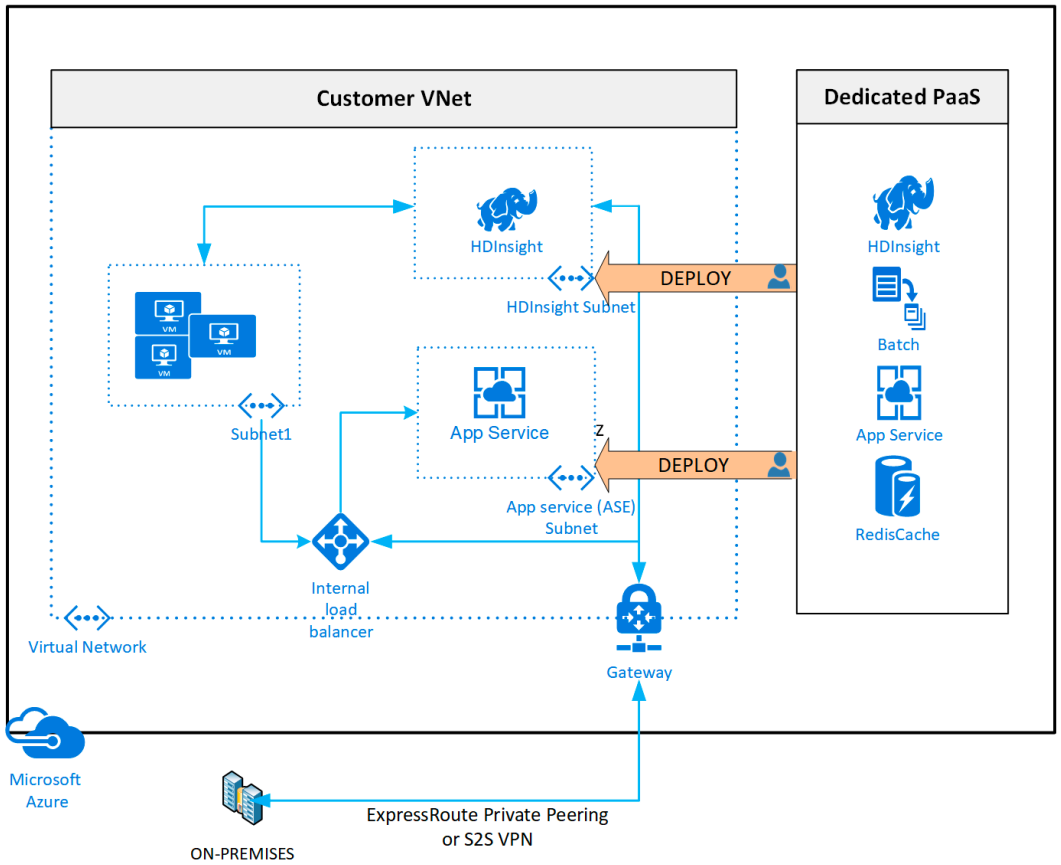
- A DDoS attack attempts to exhaust an application's resources, making the application unavailable to legitimate users. DDoS attacks can be targeted at any endpoint that is publicly reachable through the internet.



Source: [3]

Network isolatoion for Azure Resources

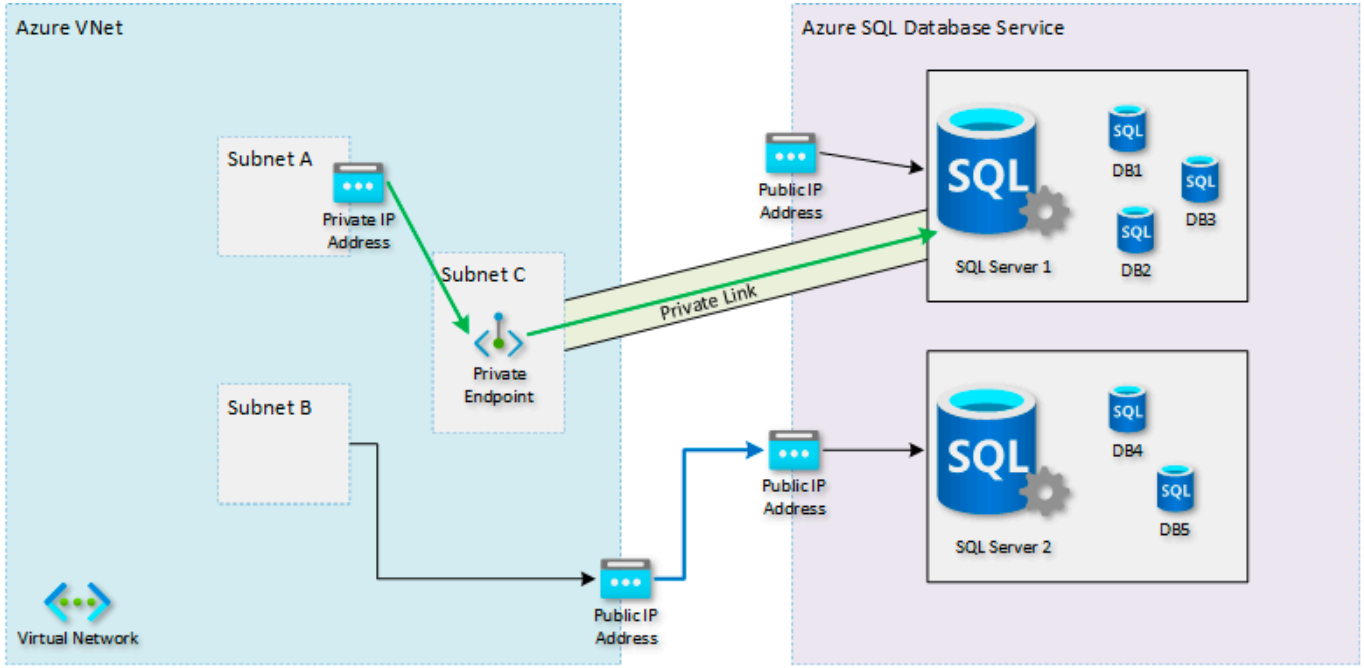
- Deploying dedicated instances of the service into a virtual network



Source: [4]

Network isolatoion for Azure Resources

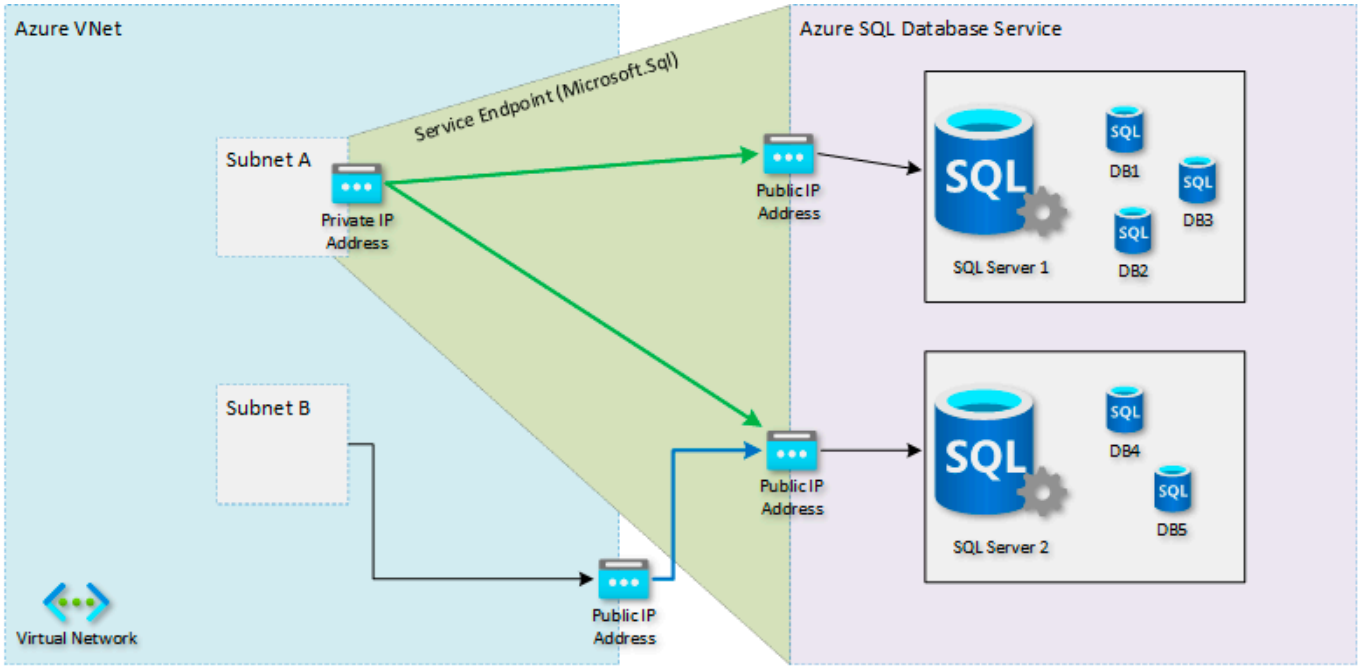
- Private Link and Private Endpoints



Source: [4]

Network isolatoion for Azure Resources

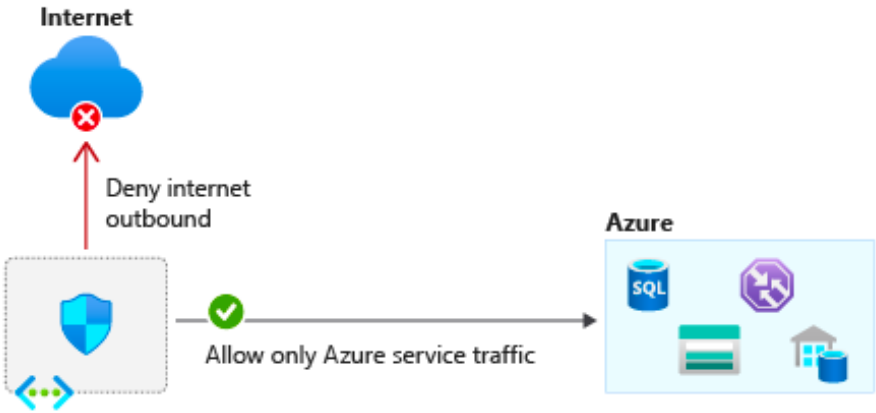
- Service Endpoints



Source: [4]

Network isolatoion for Azure Resources

- Service Tags

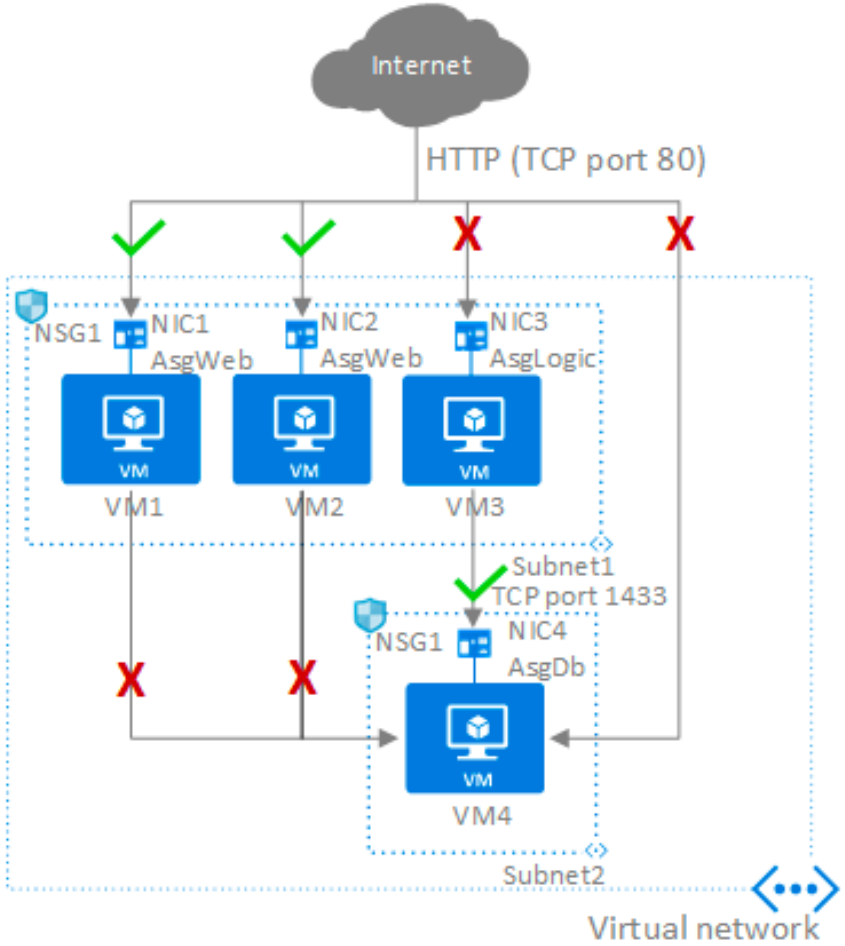


Service Tags in a network security group					
Action	Name	Source	Destination	Destination service tag	Protocol
Allow	AllowStorage	VirtualNetwork	Service Tag	**Storage**	Any
Allow	AllowSQL	VirtualNetwork	Service Tag	**Sql.EastUS**	Any
Deny	DenyAllOutBound	Any	Any	Any	Any

Source: [4]

Imagine a situation where you have 2 tier architecture and you are changing to 3 tier architecture. Now only business tier can access your DBs. How will this impact the network setup?

Applictaion Security Groups



Source: [5]

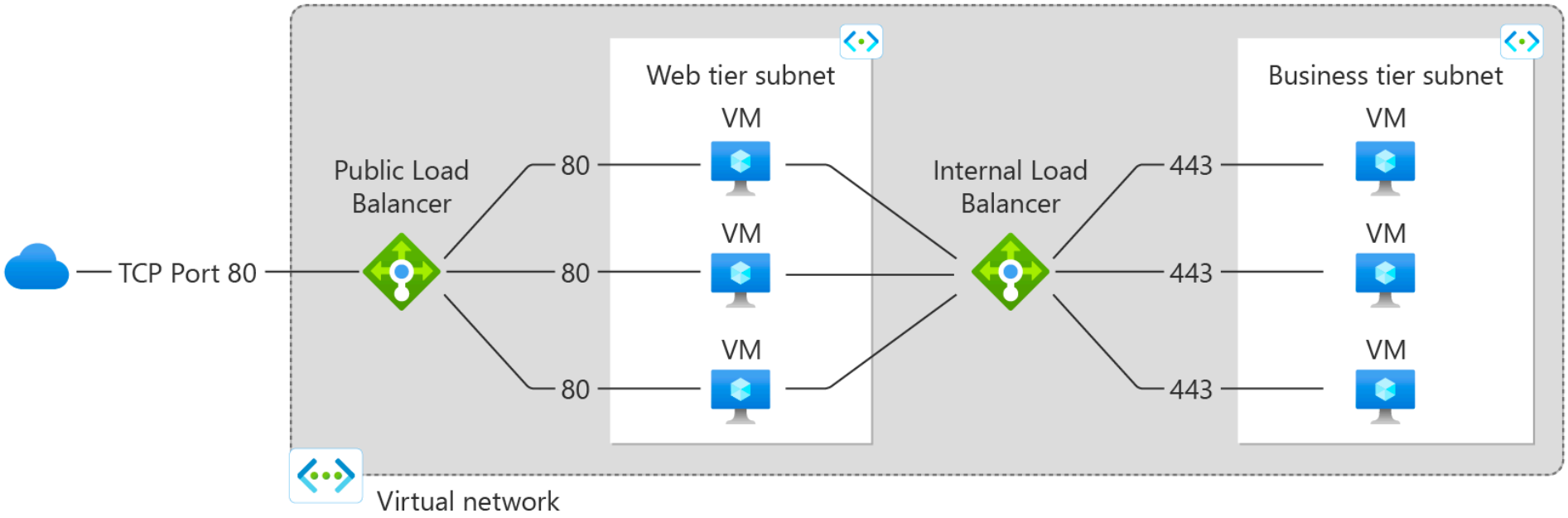
We saw multiple ways to keep application highly available like Scale sets, Availability sets, multi AZ dedeployments etc.

How does it work?

Load Balancer

Azure Load Balancer

- *Load balancing* refers to efficiently distributing incoming network traffic across a group of backend servers or resources.
- Azure Load Balancer operates at layer 4 of the Open Systems Interconnection (OSI) model.
- Two types:
  - Public Load Balancer
  - Internal/Private Load Balancer


Web tier subnet
Business tier subnet
VM
VM
VM
VM
VM
VM
Public Load Balancer
Internal Load Balancer
TCP Port 80
80
80
80
443
443
443
Virtual network

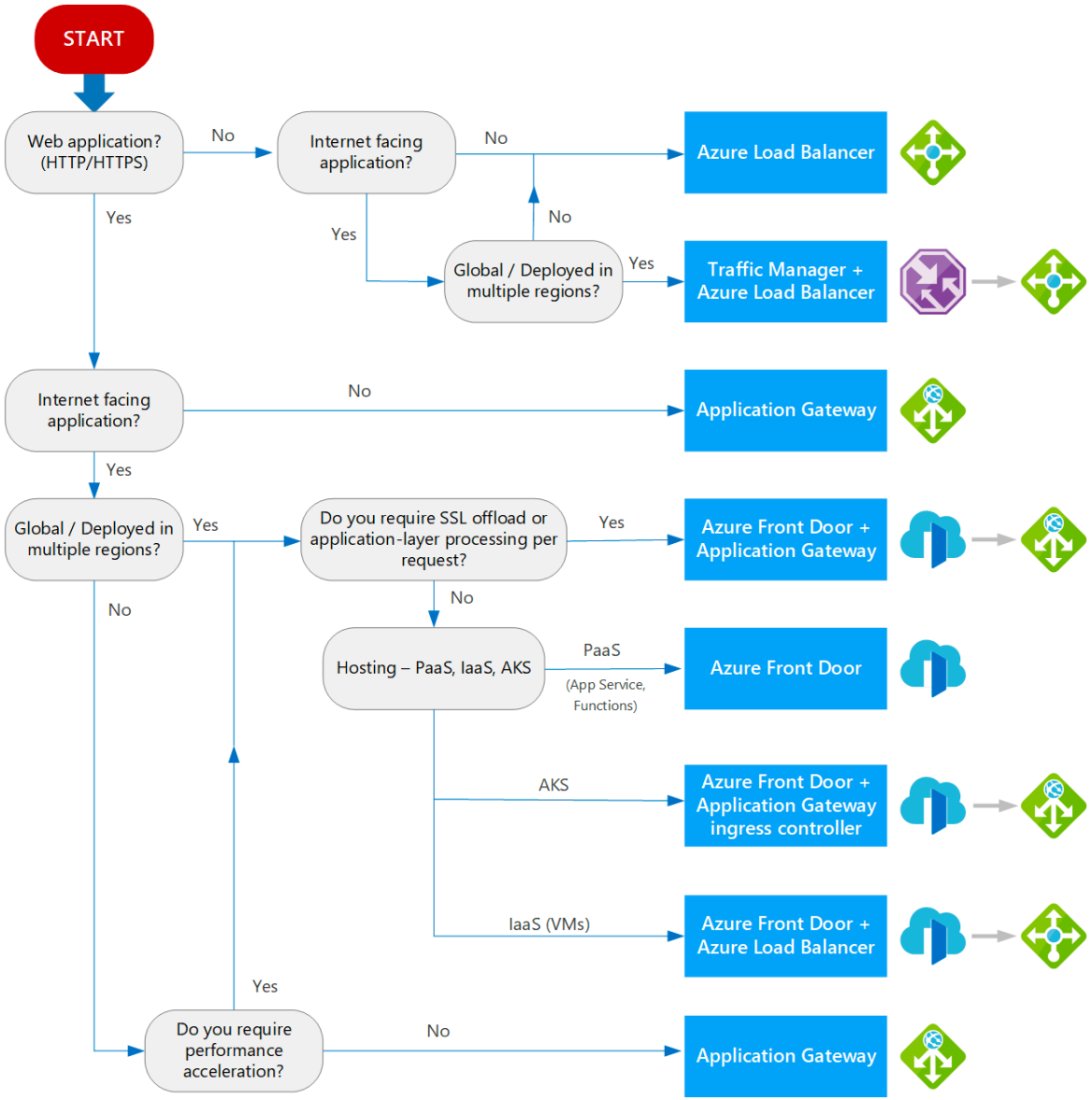
Source: [6]

How can we work with global load balancing?

Load Balancing in Azure

- Azure Front Door: It is an application delivery network that provides global load balancing and site acceleration service for web applications. It offers Layer 7 capabilities for your application like SSL offload, path-based routing, fast failover, and caching to improve performance and high availability of your applications.
- Traffic Manager: It is a DNS-based traffic load balancer that enables you to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness.
- Application Gateway: It provides application delivery controller as a service, offering various Layer 7 load-balancing capabilities. Use it to optimize web farm productivity by offloading CPU-intensive SSL termination to the gateway. App GW is regional service.

Decision Tree



Source: [7]

It’s a wrap

References

[1] https://learn.microsoft.com/en-us/azure/networking/fundamentals/networking-overview

[2] https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?toc=%2Fazure%2Fvirtual-network%2Ftoc.json&tabs=cli

[3] https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview

[4] https://learn.microsoft.com/en-us/azure/virtual-network/vnet-integration-for-azure-services

[5] https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups

[6] https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-overview

[7] https://learn.microsoft.com/en-us/azure/architecture/guide/technology-choices/load-balancing-overview#decision-tree-for-load-balancing-in-azure