Cloud Infrastructure Week#6

Emrah Mutlu

January 2024

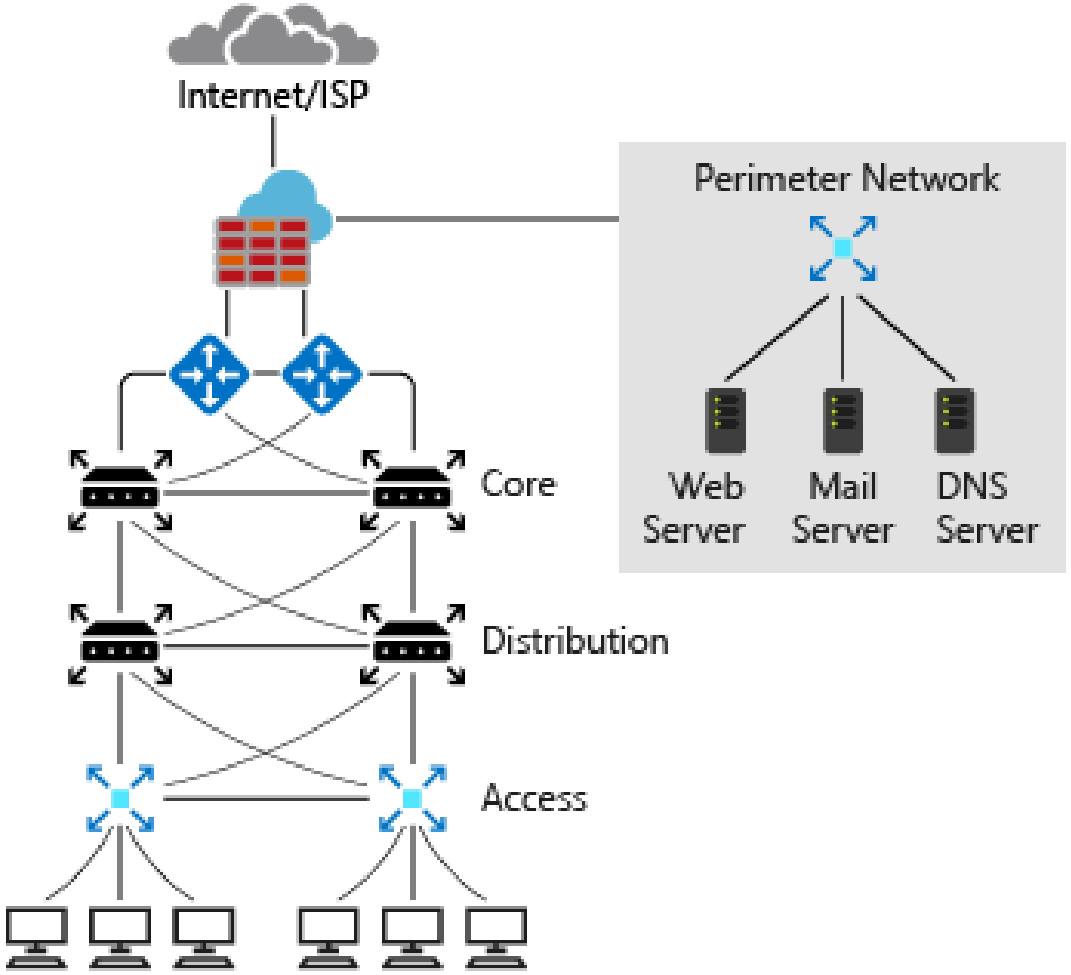
AGENDA – WEEK#6

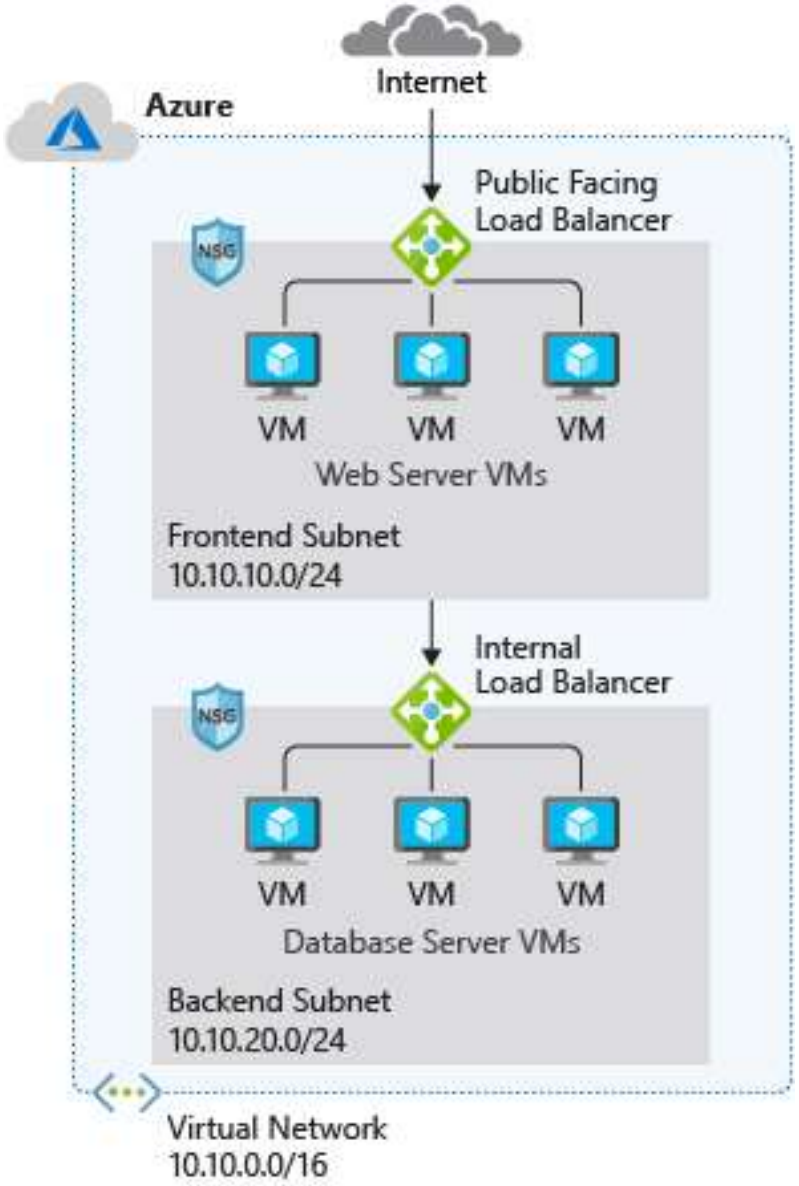
- Cloud Network
  - Differences between traditional network vs. cloud network
  - Virtual Networks and Cloud Network Rules
  - VNET Peering
  - Load Balancer
  - NSG
  - APPGW (Application Gateway) & WAF (Web Application Firewall)
  - NVA (Network Virtual Appliance)
  - Traffic Manager & Front Door & CDN (Content Delivery Network)
  - S2S VPN
  - Express Route
  - Hub & Spoke Topology in Cloud
  - Lab Session

Orion Innovation

Cloud Network

DIFFERENCES BETWEEN THE TRADITIONAL NETWORK VS CLOUD NETWORK



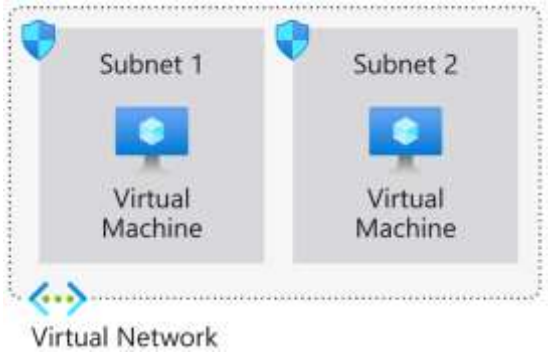


VNET

A virtual network (VNET) is composed of many elements including, but not limited to, network interfaces, load balancers, subnets, network security groups, and public IP addresses. These elements work together and enable secure, reliable network communication between your Azure resources, the internet, and on-premises networks.

Cloud Network Rules:

- Private IP Address Pools:
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16



- The .1, .2, .3, and last IP addresses are not visible or configurable by the Azure customer. These addresses are reserved and used by internal Azure services. Therefore, the number of possible addresses on an Azure subnet is **(2^n)-5**, where n represents the number of host bits.
- The smallest subnet that is supported uses a /29 subnet mask. The largest supported subnet uses a /8 subnet mask.
- By default, all subnets in an Azure virtual network can communicate with each other. However, you can use a network security group to deny communication between subnets.
- There can be no IP address overlap for interconnected networks.

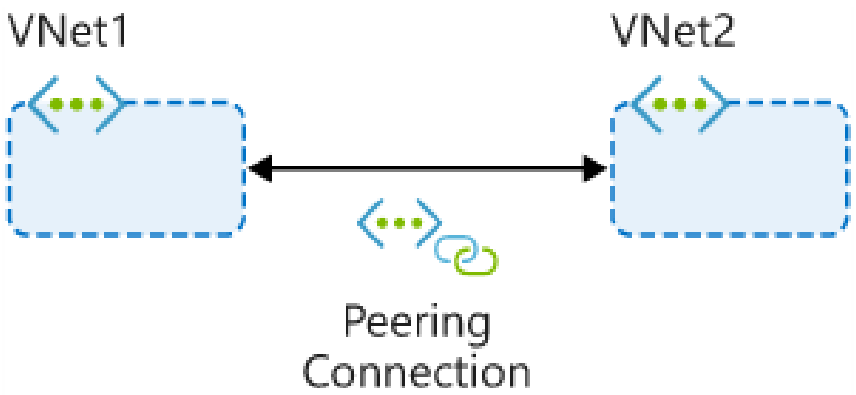
Network Planning:

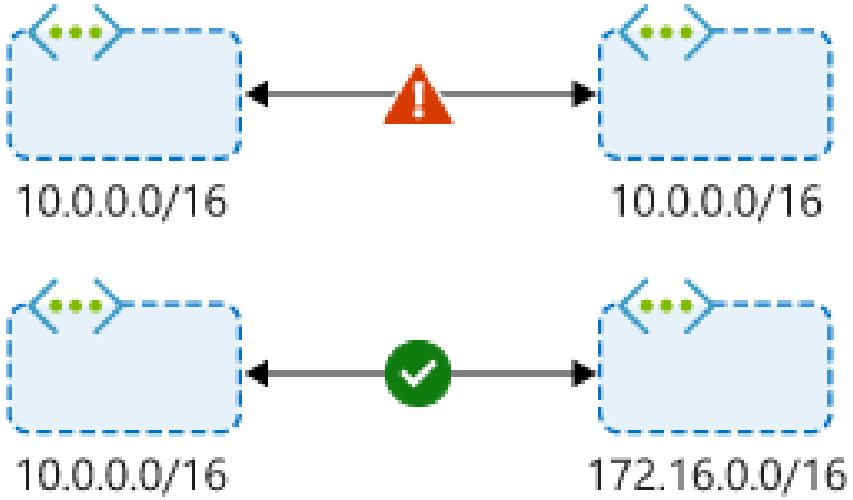
- Based on the services running on the infrastructure, what devices do you need to separate?
- How many subnets do you need?
- How many devices per subnet will you have?
- How many devices are you planning to add to the subnets in future?
- Are all subnets going to be the same size?
- How many subnets do you want or plan to add in future?

Example: https://learn.microsoft.com/en-us/training/modules/design-ip-addressing-for-azure/5-exercise-implement-vnets

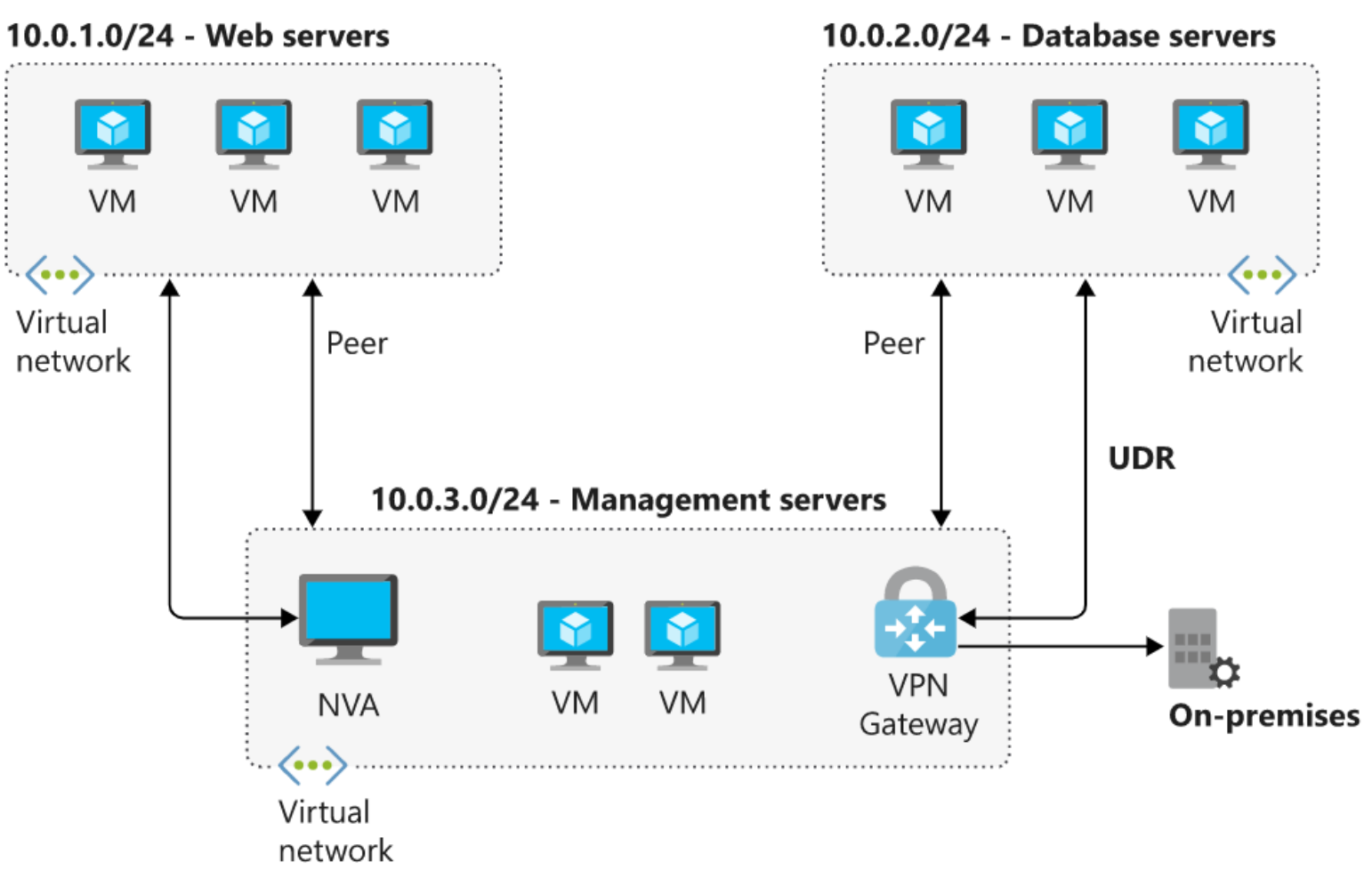
VNET PEERING

- You can use virtual network peering to directly connect Azure virtual networks. When you use peering to connect virtual networks, virtual machines (VMs) in these networks can communicate with each other as if they were in the same network.
- In peered virtual networks, traffic between virtual machines is routed through the Azure network. The traffic uses only private IP addresses. It doesn't rely on internet connectivity, gateways, or encrypted connections. The traffic is always private, and it takes advantage of the high bandwidth and low latency of the Azure backbone network.
- IP address spaces of connected networks within Azure and between Azure and your on-premises system can't overlap. This is also true for peered virtual networks.



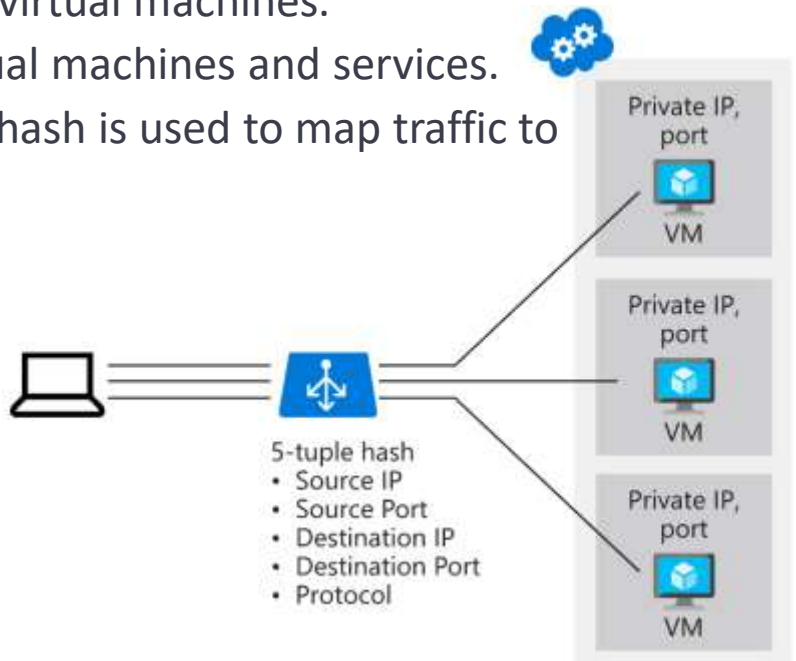


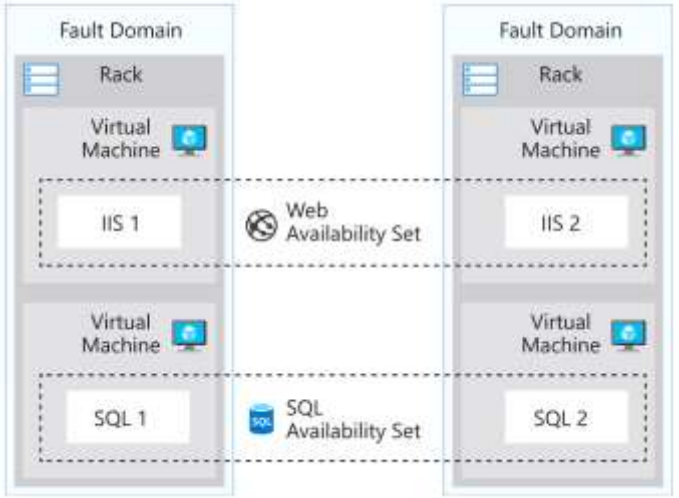
Example: Peering with VNET Peering, UDRs and VPN GWs.

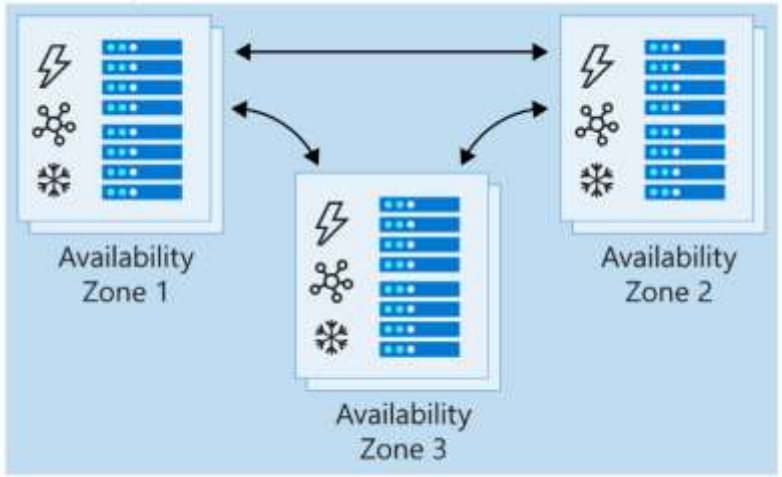


LOAD BALANCER

- Azure Load Balancer is a service you can use to distribute traffic across multiple virtual machines.
- Use Load Balancer to scale applications and create high availability for your virtual machines and services.
- Load balancers use a hash-based distribution algorithm. By default, a five-tuple hash is used to map traffic to available servers. The hash is made from the following elements:
  - **Source IP**: The IP address of the requesting client.
  - **Source port**: The port of the requesting client.
  - **Destination IP**: The destination IP of the request.
  - **Destination port**: The destination port of the request.
  - **Protocol type**: The specified protocol type, TCP or UDP.
- Load balancers support availability sets and availability zones to ensure that virtual machines are always available.

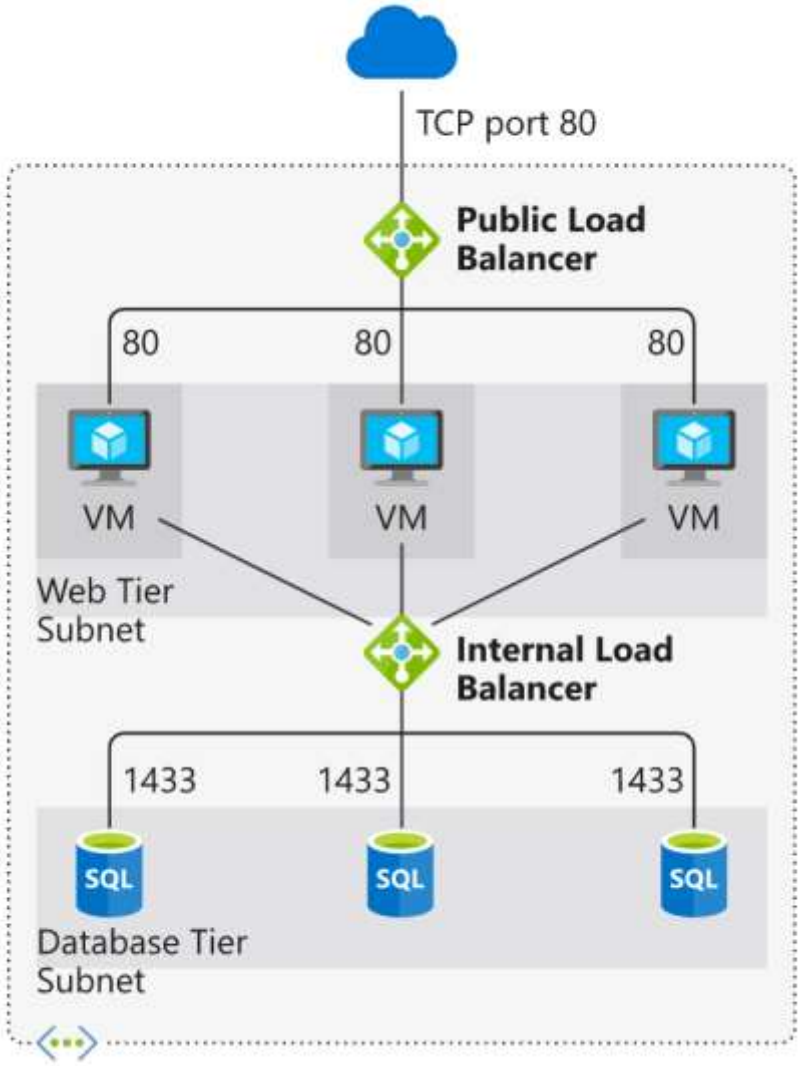






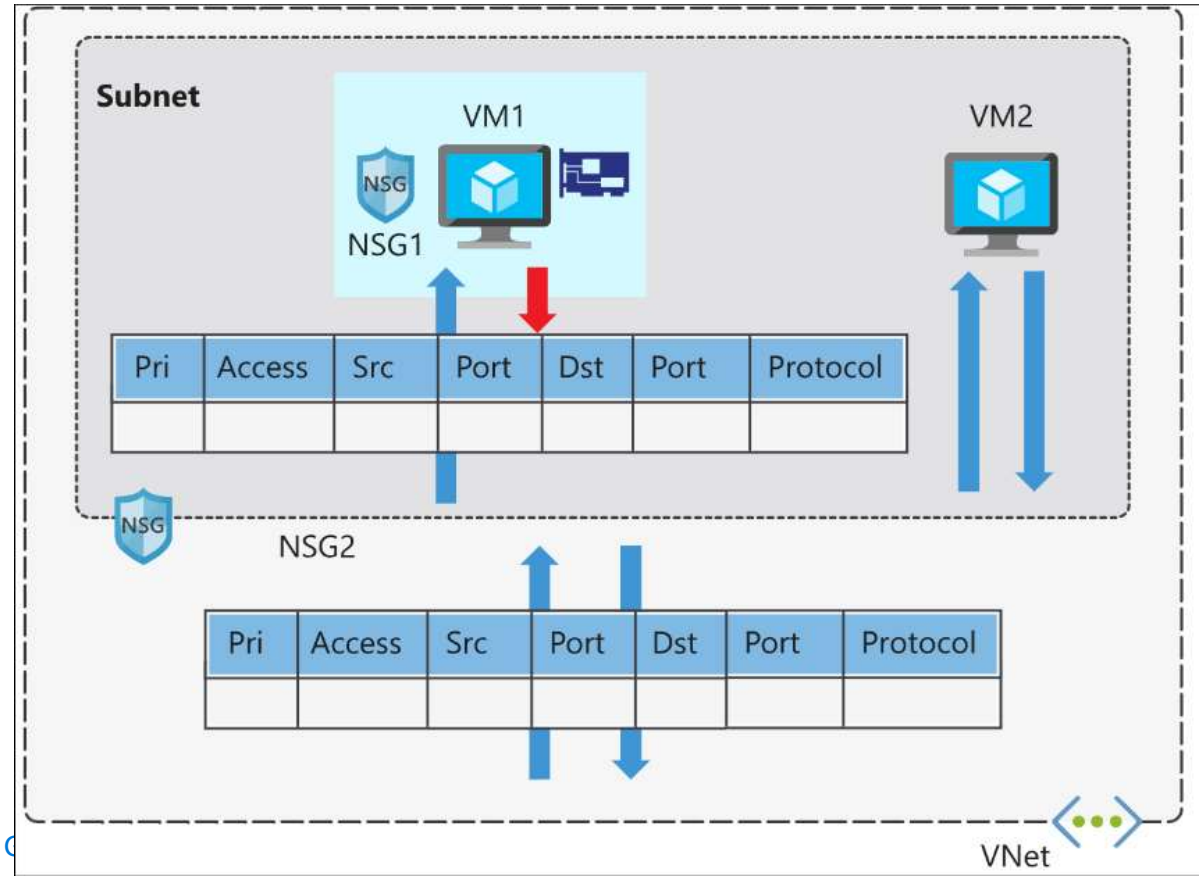
Configuration	Service level agreement (SLA)	Information
Availability set	99.95%	Protection from hardware failures within datacenters
Availability zone	99.99%	Protection from entire datacenter failure

Example: Load balancing the n-tier architected network with ELB & ILB:



NSG

- Network security groups filter network traffic to and from Azure resources. Network security groups contain security rules that you configure to allow or deny inbound and outbound traffic.
- Network security groups are assigned to a network interface or a subnet. When you apply network security groups to both a subnet and a network interface, each network security group is evaluated independently. Inbound traffic is first evaluated by the network security group applied to the subnet, and then by the network security group applied to the network interface. Conversely, outbound traffic from a VM is first evaluated by the network security group applied to the network interface, and then by the network security group applied to the subnet.



Property	Explanation
Name	A unique name within the network security group.
Priority	A number between 100 and 4096.
Source and destination	Any, or an individual IP address, classless inter-domain routing (CIDR) block (10.0.0.0/24, for example), service tag, or app security group.
Protocol	TCP, UDP, or Any.
Direction	Whether the rule applies to inbound, or outbound traffic.
Port range	An individual port or range of ports.
Action	Allow or deny the traffic.

NSG

- Inbound default security rules:

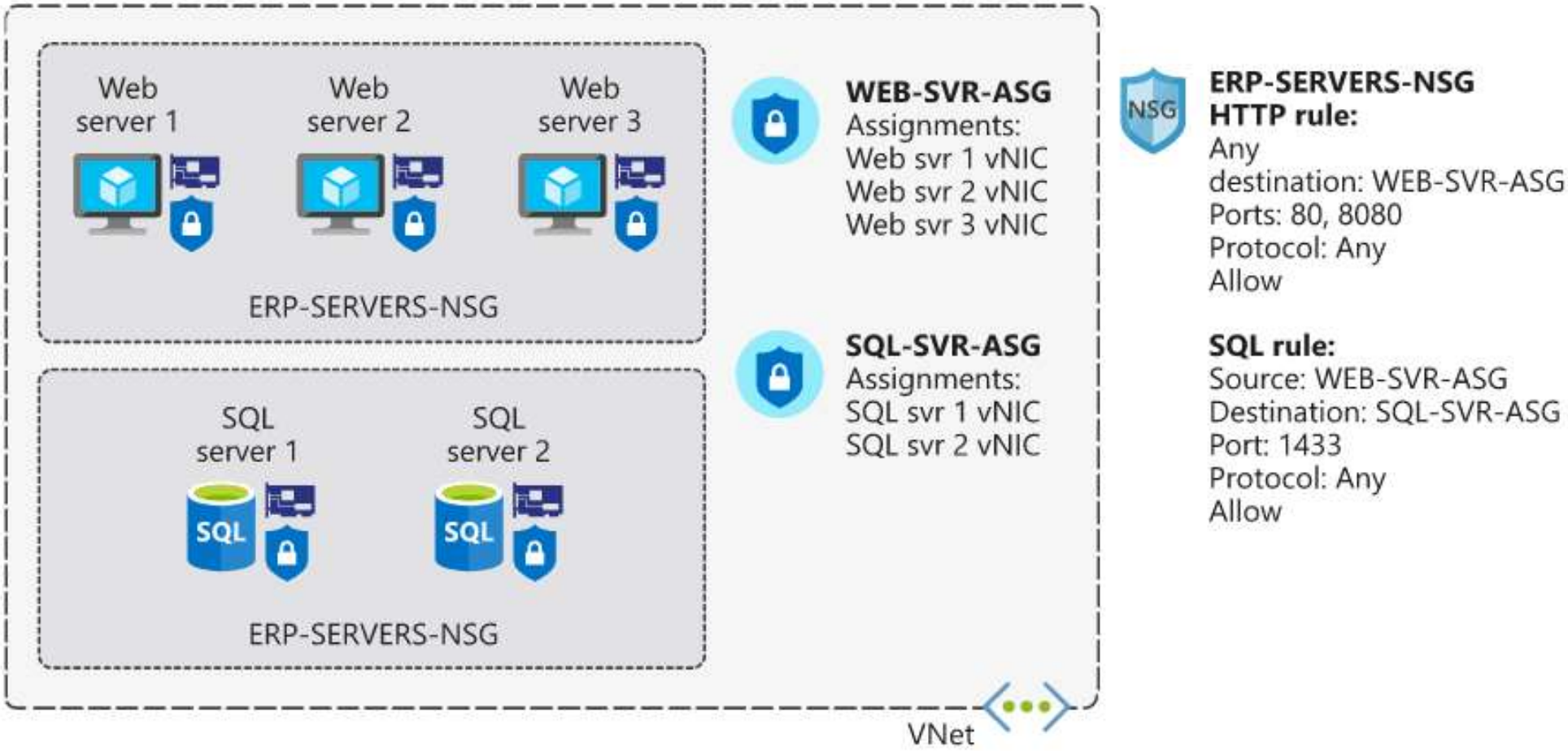
Priority	Rule name	Description
65000	AllowVnetInbound	Allow inbound coming from any VM to any VM within the subnet.
65001	AllowAzureLoadBalancerInbound	Allow traffic from the default load balancer to any VM within the subnet.
65500	DenyAllInBound	Deny traffic from any external source to any of the VMs.

- Outbound default security rules:

Priority	Rule name	Description
65000	AllowVnetOutbound	Allow outbound going from any VM to any VM within the subnet.
65001	AllowInternetOutbound	Allow outbound traffic going to the internet from any VM.
65500	DenyAllOutBound	Deny traffic from any internal VM to a system outside the virtual network.

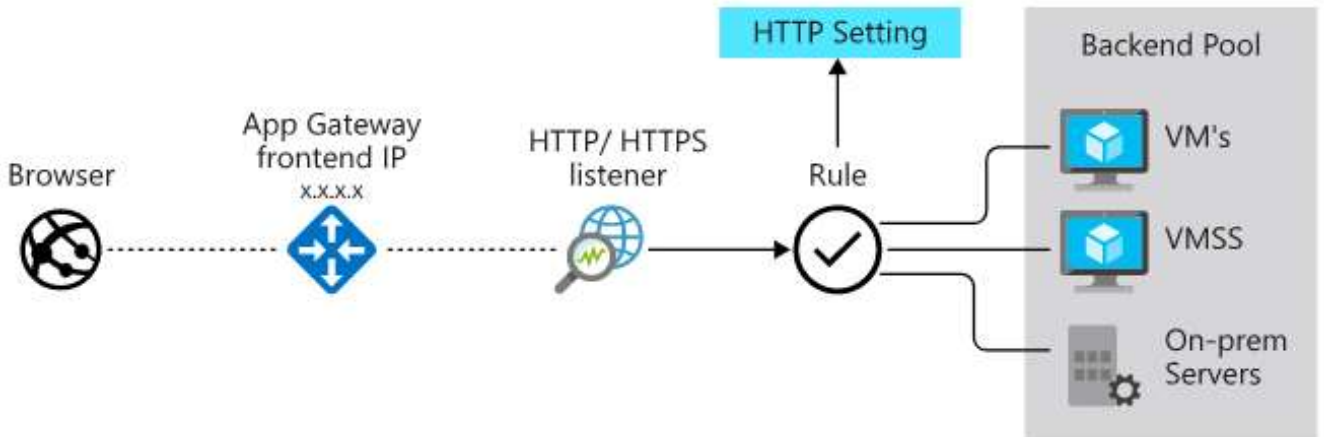
- Service tags:
  - **VirtualNetwork** - Represents all virtual network addresses anywhere in Azure, and in your on-premises network if you're using hybrid connectivity.
  - **AzureLoadBalancer** - Denotes Azure's infrastructure load balancer. The tag translates to the virtual IP address of the host (168.63.129.16) where Azure health probes originate.
  - **Internet** - Represents anything outside the virtual network address that is publicly reachable, including resources that have public IP addresses. One such resource is the Web Apps feature of Azure App Service.
  - **AzureTrafficManager** - Represents the IP address for Azure Traffic Manager.
  - **Storage** - Represents the IP address space for Azure Storage. You can specify whether traffic is allowed or denied. You can also specify if access is allowed only to a specific region, but you can't select individual storage accounts.
  - **SQL** - Represents the address for Azure SQL Database, Azure Database for MySQL, Azure Database for PostgreSQL, and Azure SQL Data Warehouse services. You can specify whether traffic is allowed or denied, and you can limit to a specific region.
  - **AppService** - Represents address prefixes for Azure App Service.

- Example: Securing the n-tier architected network:



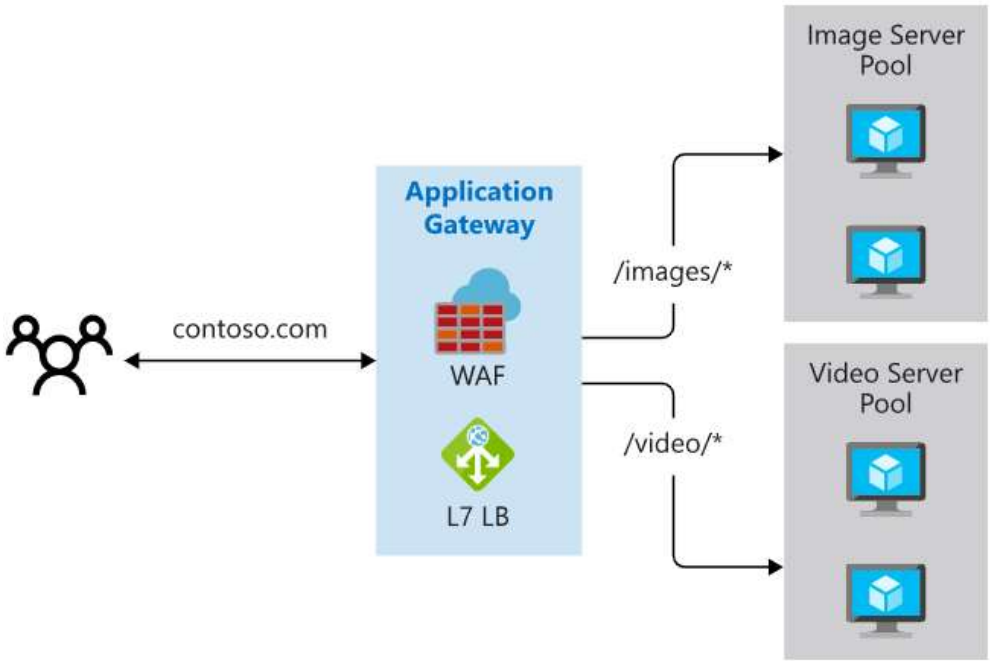
APP GW (APPLICATION GATEWAY)

- Application Gateway manages the requests that client applications can send to a web app.
- Application Gateway routes traffic to a pool of web servers based on the URL of a request. This is known as *application layer routing*. The pool of web servers can be Azure virtual machines, Azure virtual machine scale sets, Azure App Service, and even on-premises servers.

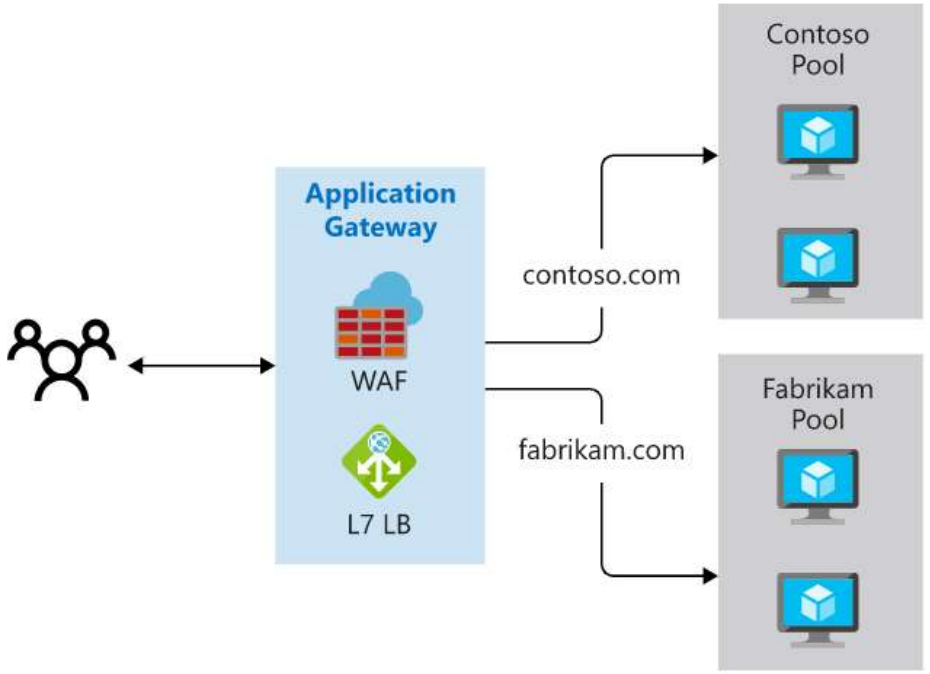


- Load-balancing works with the OSI Layer 7 routing implemented by Application Gateway routing, which means that it load balances requests based on the routing parameters (host names and paths) used by the Application Gateway rules.

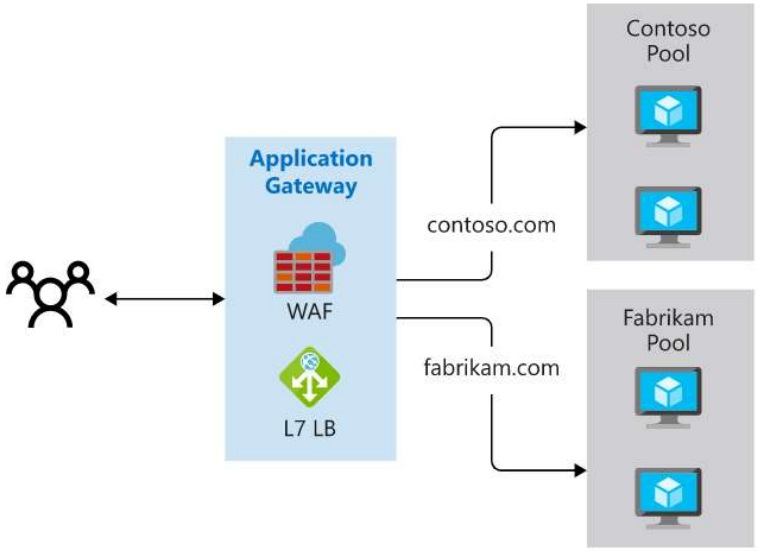
Path-based routing enables you to send requests with different paths in the URL to a different pool of back-end servers. For example, you could direct requests with the path /video/* to a back-end pool containing servers that are optimized to handle video streaming, and direct /images/* requests to a pool of servers that handle image retrieval.



Multiple site hosting enables you to configure more than one web application on the same application gateway instance. In a multi-site configuration, you register multiple DNS names (CNAMEs) for the IP address of the Application Gateway, specifying the name of each site.



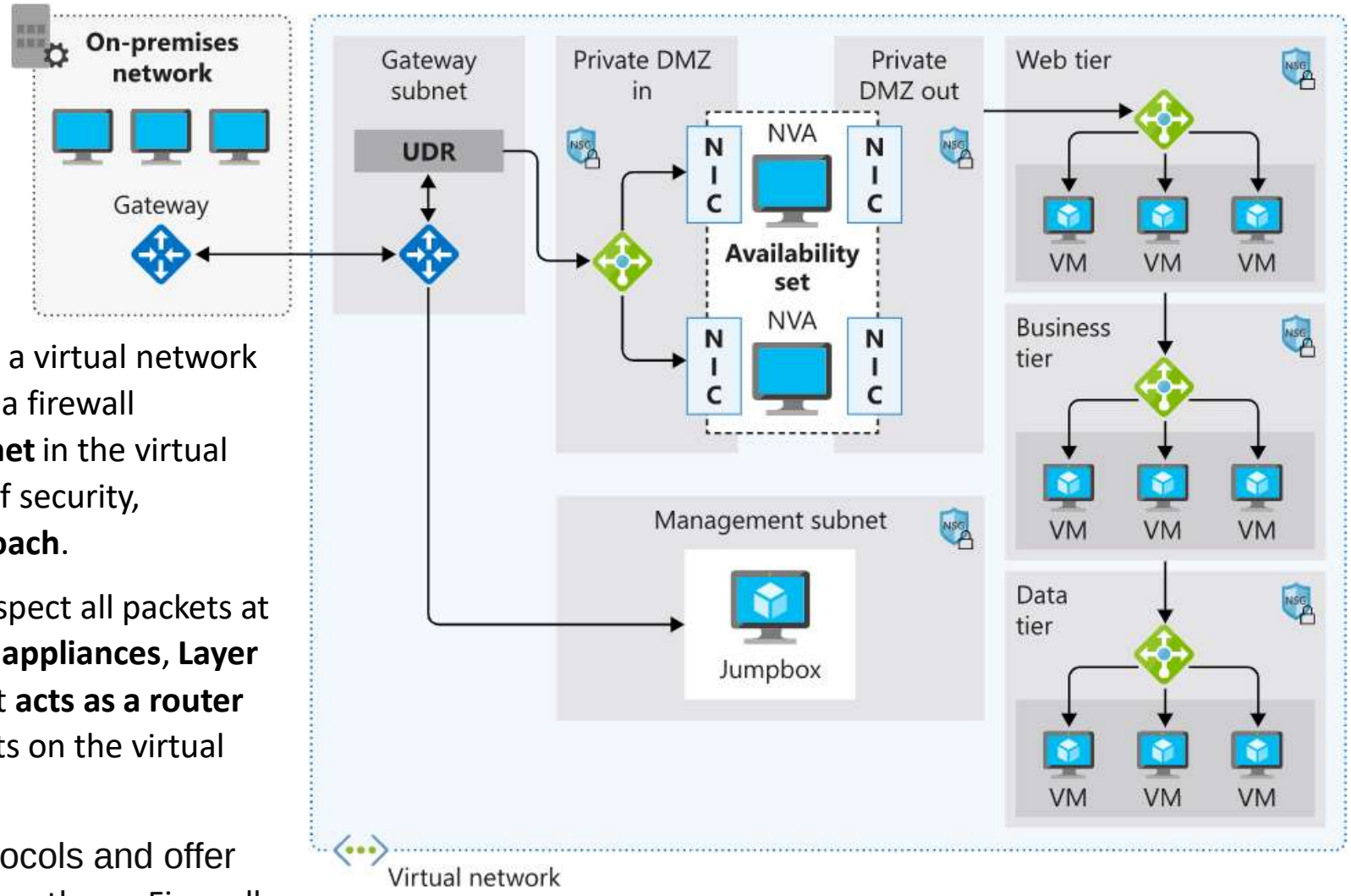
- **The *web application firewall* (WAF)** is an optional component that handles incoming requests before they reach a listener. The web application firewall checks each request for many common threats, based on the *Open Web Application Security Project* (OWASP):
  - SQL-injection
  - Cross-site scripting
  - Command injection
  - HTTP request smuggling
  - HTTP response splitting
  - Remote file inclusion
  - Bots, crawlers, and scanners
  - HTTP protocol violations and anomalies



- **Health probes** are an important part in assisting the load balancer to determine which servers are available for load balancing in a back-end pool. Application Gateway uses a health probe to send a request to a server. If the server returns an HTTP response with a status code between 200 and 399, the server is deemed healthy.

NVA (NETWORK VIRTUAL APPLIANCES)

- A network virtual appliance (NVA) is a virtual appliance that consists of various layers like:
  - a firewall
  - a WAN optimizer
  - application-delivery controllers
  - routers
  - load balancers
  - IDS/IPS
  - proxies



- You can deploy **firewall appliances** into a virtual network in different configurations. You can put a firewall appliance in a **perimeter-network subnet** in the virtual network. Or if you want more control of security, implement a **microsegmentation approach**.
- **Microsegmentation** lets the **firewall** inspect all packets at **OSI Layer 4** and, for **application-aware appliances**, **Layer 7**. When you deploy an **NVA** to Azure, it **acts as a router** that forwards requests between subnets on the virtual network.
- NVAs an handle a wide range of protocols and offer vendor-specific services but costs more than a Firewall.

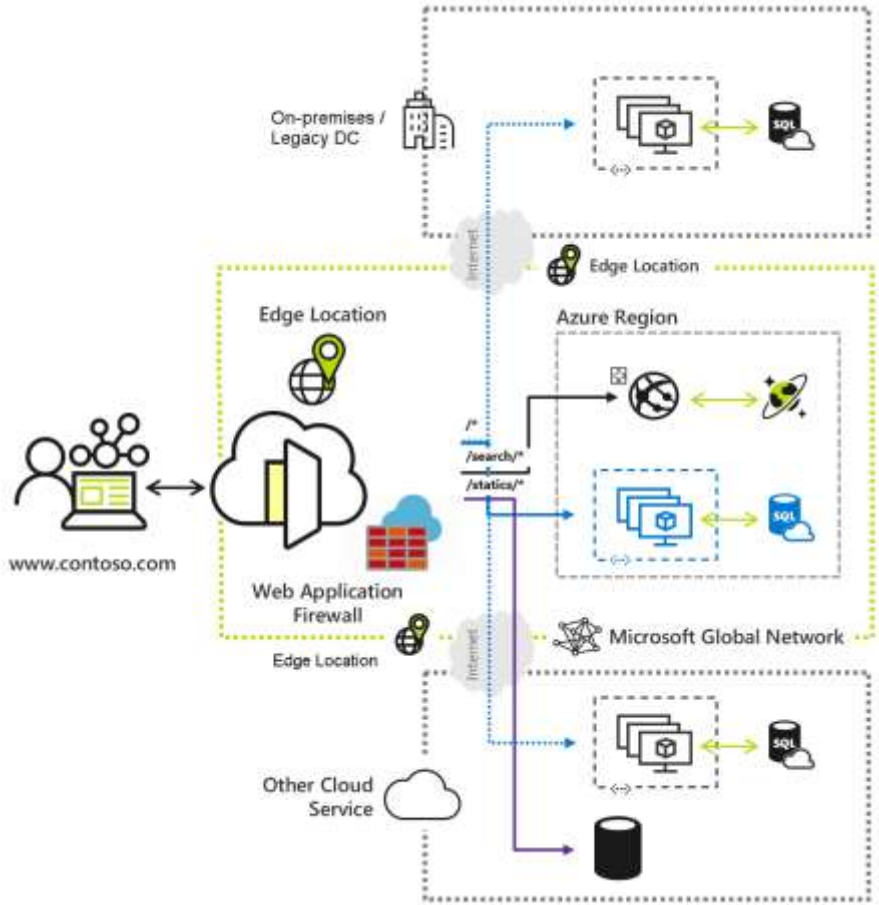
AZURE TRAFFIC MANAGER

- Azure Traffic Manager is a **DNS-based traffic load balancer** that you can use to distribute traffic optimally to services **across Azure regions globally**. You can use Traffic Manager to distribute traffic to different regions while providing high availability, resilience, and responsiveness in your app.

- When a client attempts to connect to a service, first it **resolves the DNS name** of the service as an IP address. The client then connects to that IP address to access the service. Traffic Manager uses DNS to direct clients to a specific service endpoint IP address based on the rules of the traffic routing method that's used. Clients connect directly to the selected endpoint. Traffic Manager isn't a proxy or gateway. Traffic Manager doesn't see the traffic that passes between the clients and the service; it just gives clients the IP address of where they need to go.

AZURE FRONT DOOR

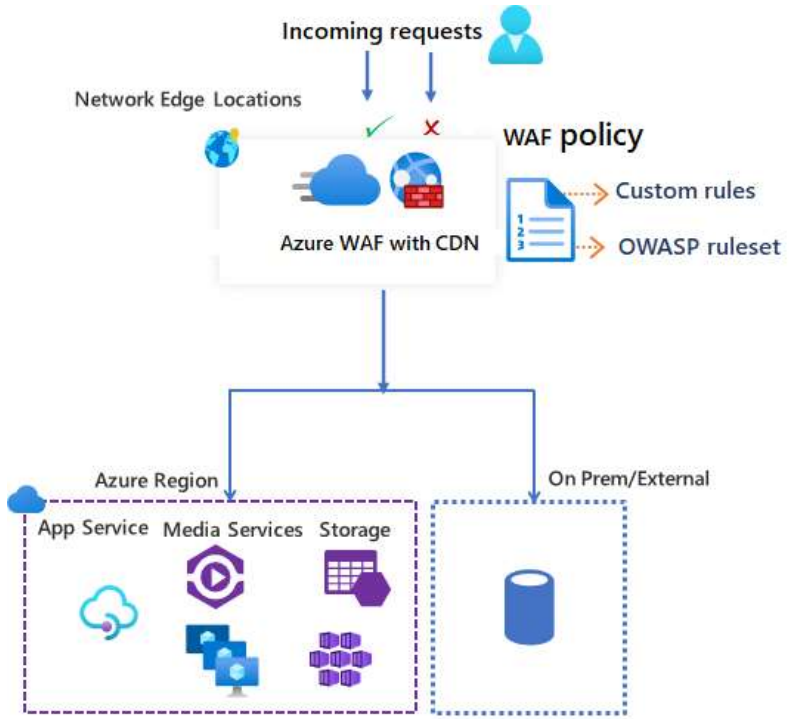
- Like Traffic Manager, Azure Front Door is a global load balancer. Unlike Traffic Manager, it works at the network application layer, Layer 7, and uses HTTP and HTTPS properties to do filtering and routing.
- With Front Door, we can do many types of routing that Traffic Manager doesn't support. For example, we can route traffic based on the browser's country code. Front Door also supports TLS protocol termination. There is, however, an exception. If we want to route traffic for any protocol other than HTTP and HTTPS, we'll have to use Traffic Manager.



AZURE CDN (CONTENT DELIVERY NETWORK)

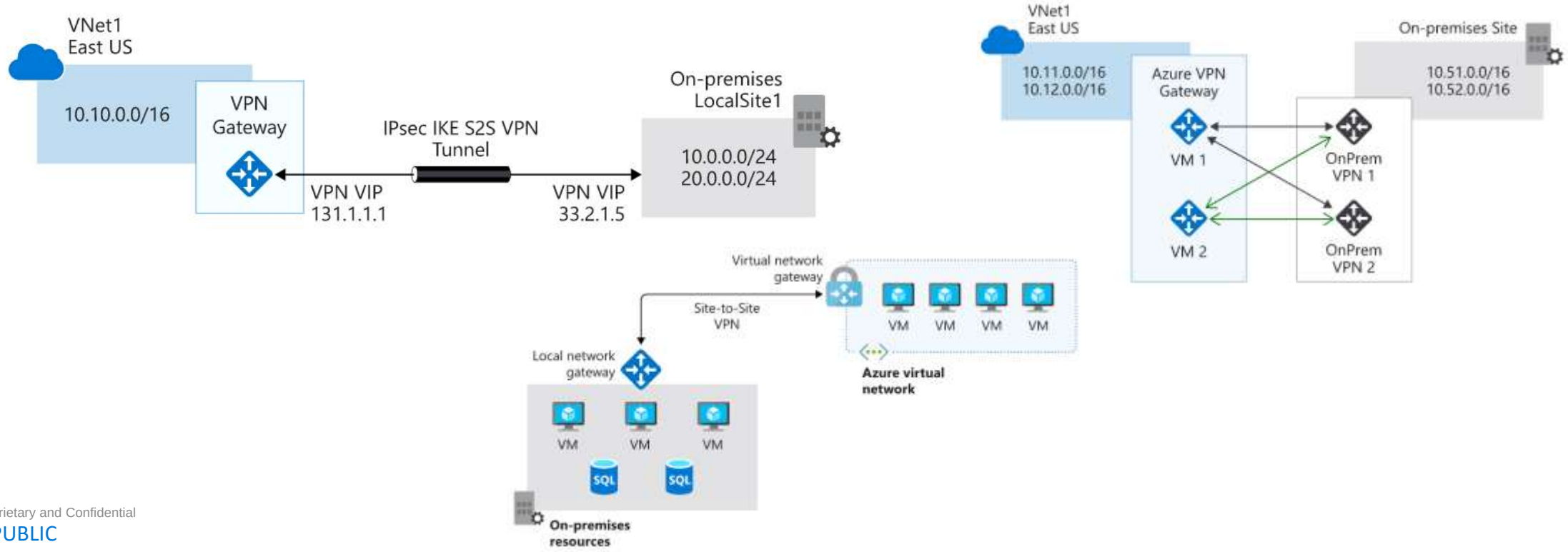
- A content delivery network is a distributed network of servers that can efficiently deliver web content to users. A content delivery network store cached content on edge servers in point of presence (POP) locations that are close to end users, to minimize latency.
- Azure Content Delivery Network offers developers a global solution for rapidly delivering high-bandwidth content to users by caching their content at strategically placed physical nodes across the world. Azure Content Delivery Network can also accelerate dynamic content, which can't get cached, by using various network optimizations using content delivery network POPs. For example, route optimization to bypass Border Gateway Protocol (BGP).

- The benefits of using Azure Content Delivery Network to deliver web site assets include:
  - Better performance and improved user experience for end users, especially when using applications where multiple round-trips requests required by end users to load contents.
  - Large scaling to better handle instantaneous high loads, such as the start of a product launch event.
  - Distribution of user requests and serving of content directly from edge servers so that less traffic gets sent to the origin server.



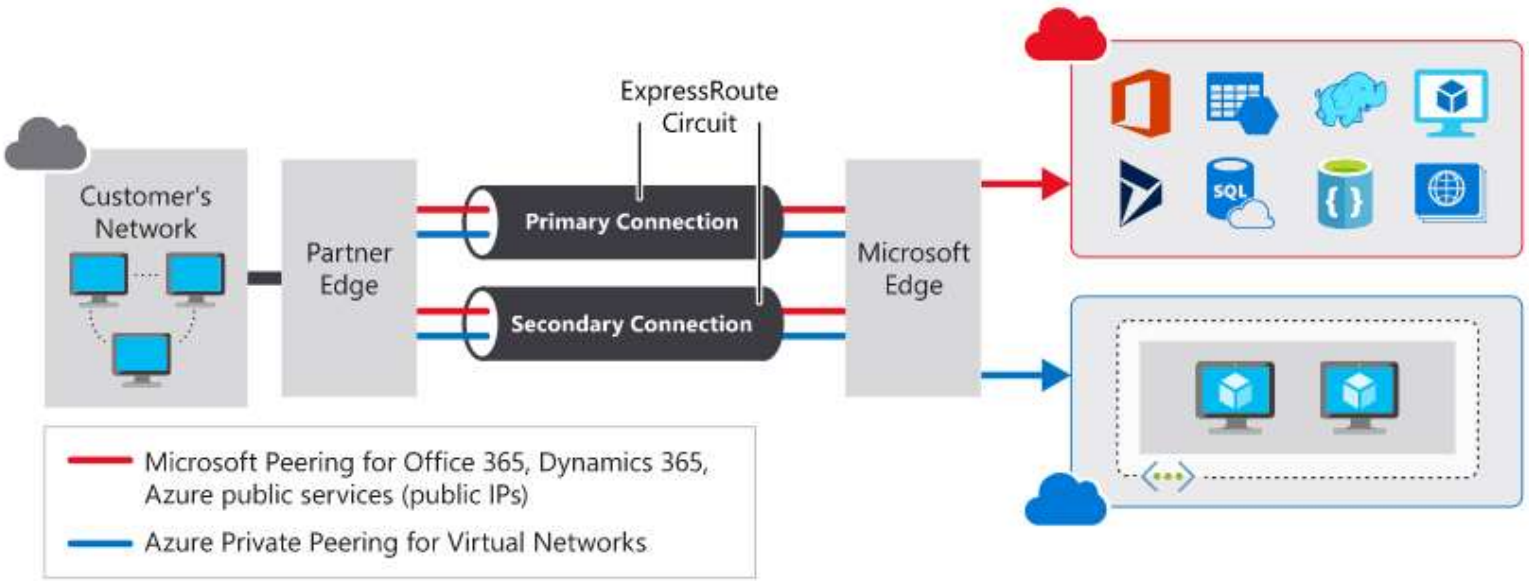
S2S VPN

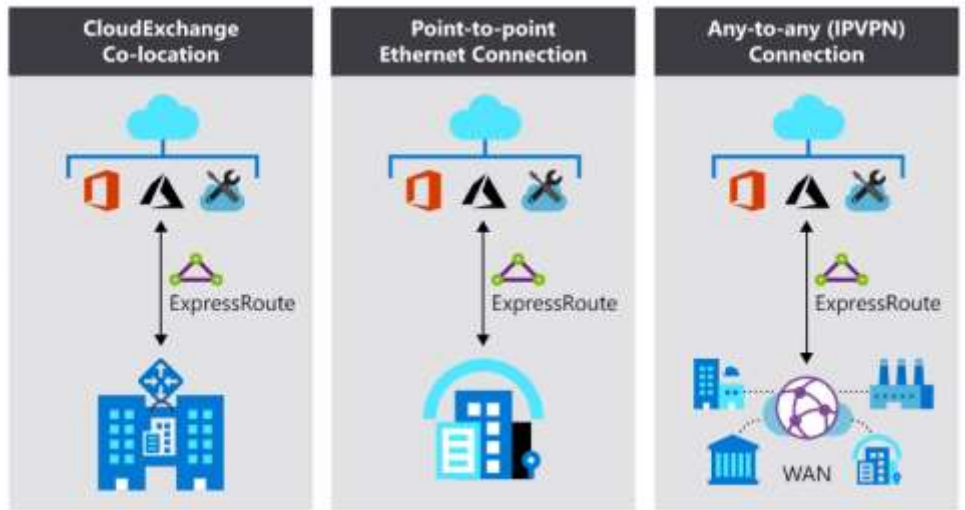
- A VPN gateway is a type of Virtual Network Gateway. VPN gateways are deployed in Azure virtual networks and enable the following connectivity:
  - Connect on-premises datacenters to Azure virtual networks through a site-to-site connection.
  - Connect individual devices to Azure virtual networks through a point-to-site connection.
  - Connect Azure virtual networks to other Azure virtual networks through a network-to-network connection.
- All transferred data is encrypted (IPSec IKE) in a private tunnel as it crosses the internet.
- On-prem site requires a VPN device. Redundancy is maintained with VPN GW pairs.



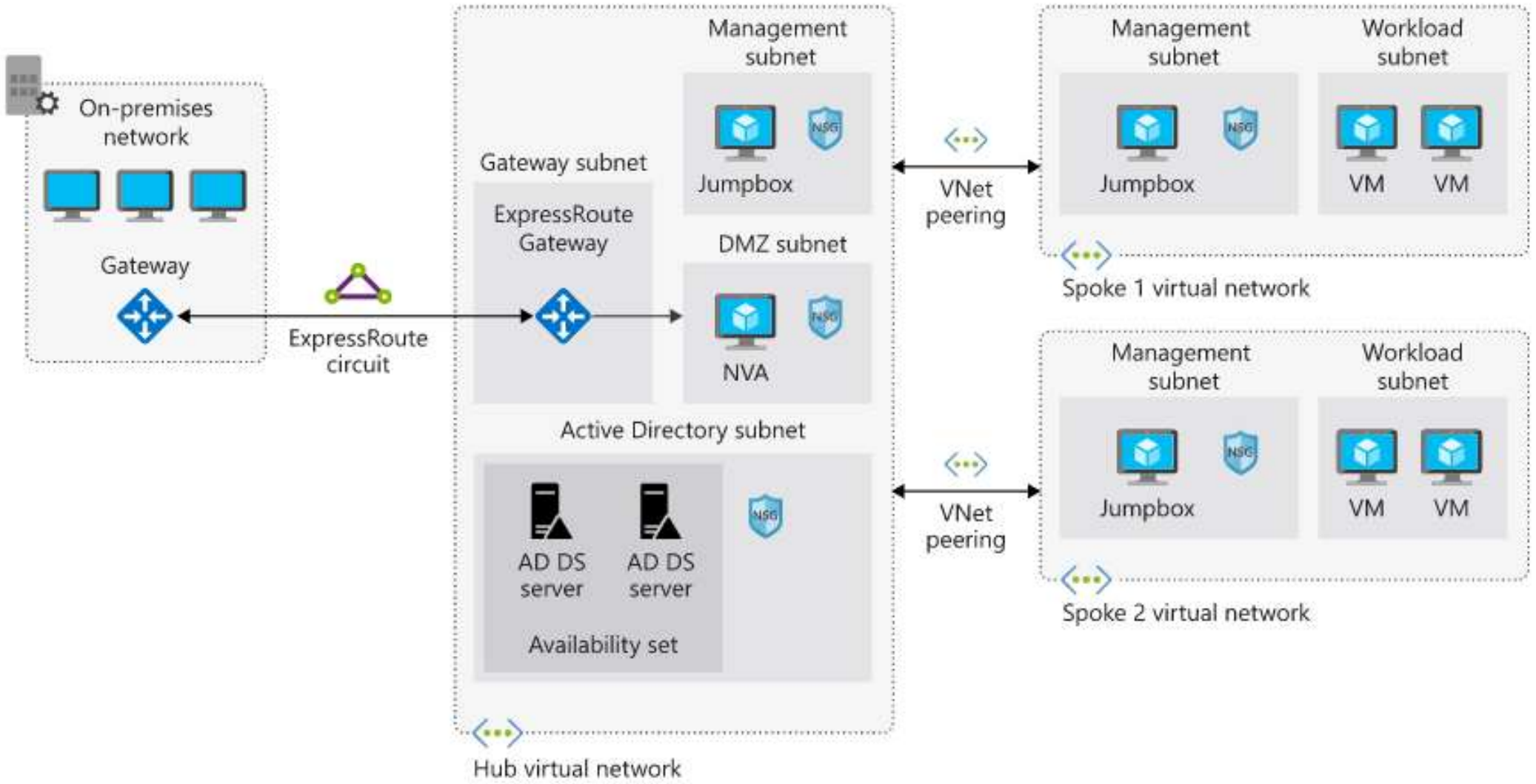
AZURE EXPRESSROUTE

- Azure ExpressRoute lets you seamlessly extend your on-premises networks into the Microsoft cloud.
- This connection between your organization and Azure is dedicated and private.
- Security is enhanced, connections are more reliable, latency is minimal, and throughput is greatly increased. Redundancy is maintained within the circuit.
- Expressroute has 3 types;
  - CloudExchange Co-location: DC is co-located with the Azure ISP vendor. Provides L2/L3 connectivity.
  - P2P Ethernet Connection: DC is located in a separate place. Provides L2/L3 connectivity.
  - IPVPN Connection: Integrate WAN circuit with Azure. Provides L3 connectivity only.

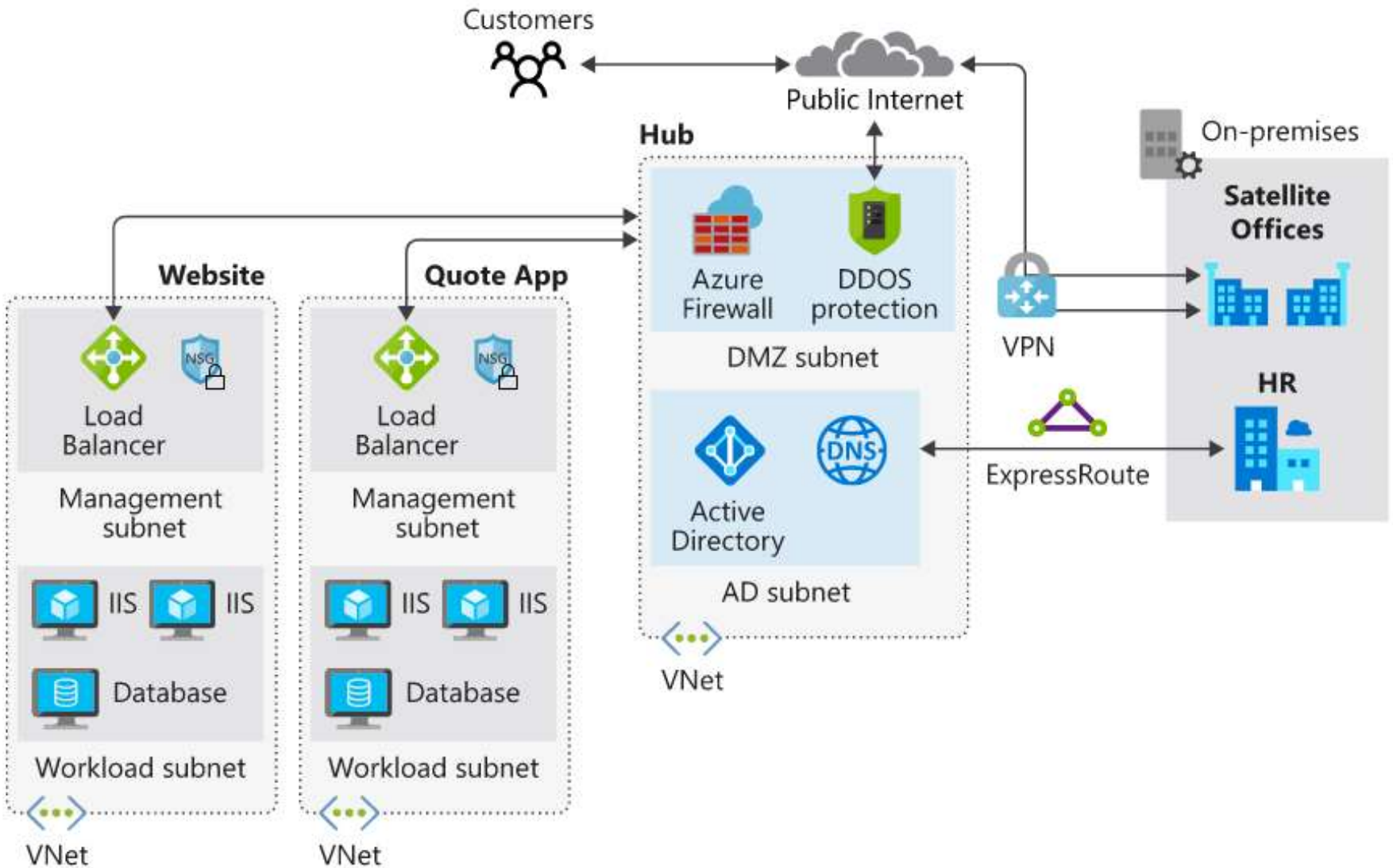




HUB AND SPOKE TOPOLOGY IN CLOUD



HUB AND SPOKE TOPOLOGY IN CLOUD



Orion Innovation

Lab Session

LAB#12: SECURE THE NETWORK WITH NSG

- Follow the instructions:
- https://learn.microsoft.com/en-us/training/modules/secure-and-isolate-with-nsg-and-service-endpoints/3-exercise-network-security-groups

- Follow the instructions:
- https://learn.microsoft.com/en-us/training/modules/integrate-vnets-with-vnet-peering/3-exercise-prepare-vnets-for-peering-using-azure-cli-commands
- https://learn.microsoft.com/en-us/training/modules/integrate-vnets-with-vnet-peering/4-exercise-configure-vnet-peering-connections-using-azure-cli-commands
- https://learn.microsoft.com/en-us/training/modules/integrate-vnets-with-vnet-peering/5-exercise-verify-vnet-peering

LAB#14: LOAD BALANCER

- Follow the instructions:
- https://learn.microsoft.com/en-us/training/modules/improve-app-scalability-resiliency-with-load-balancer/4-exercise-configure-public-load-balancer?pivots=bash

LAB#15: APPGW TEST

- Follow the instructions:
- https://learn.microsoft.com/en-us/training/modules/load-balance-web-traffic-with-application-gateway/3-exercise-create-web-sites
- https://learn.microsoft.com/en-us/training/modules/load-balance-web-traffic-with-application-gateway/5-exercise-create-configure-application-gateway
- https://learn.microsoft.com/en-us/training/modules/load-balance-web-traffic-with-application-gateway/6-exercise-test-application-gateway

LAB#16: NVA TEST

- Follow the instructions:
- https://learn.microsoft.com/en-us/training/modules/control-network-traffic-flow-with-routes/5-exercise-create-nva-vm
- https://learn.microsoft.com/en-us/training/modules/control-network-traffic-flow-with-routes/6-exercise-route-traffic-through-nva

- Compare AWS and Azure’s Network services. Provide a short summary.
- Prepare a network diagram with the following requirements on AWS:
  - Customer has resources on both on-prem and AWS centers.
  - Customer DC needs to be connected via S2S VPN to AWS.
  - AWS has Web Servers and DBs with n-tier architecture.
  - All cloud security systems has to be in place.
  - Media of the Web content is stored in blobs on AWS.
  - Caching of DBs are required to handle high volume of IOPS traffic.
  - Web calls need to be directed to both on-prem and AWS resources to share the load.
  - Auto-scaling is required to handle high traffic period.
  - Design should follow the least cost rule on AWS.

Thank You

orioninc.com