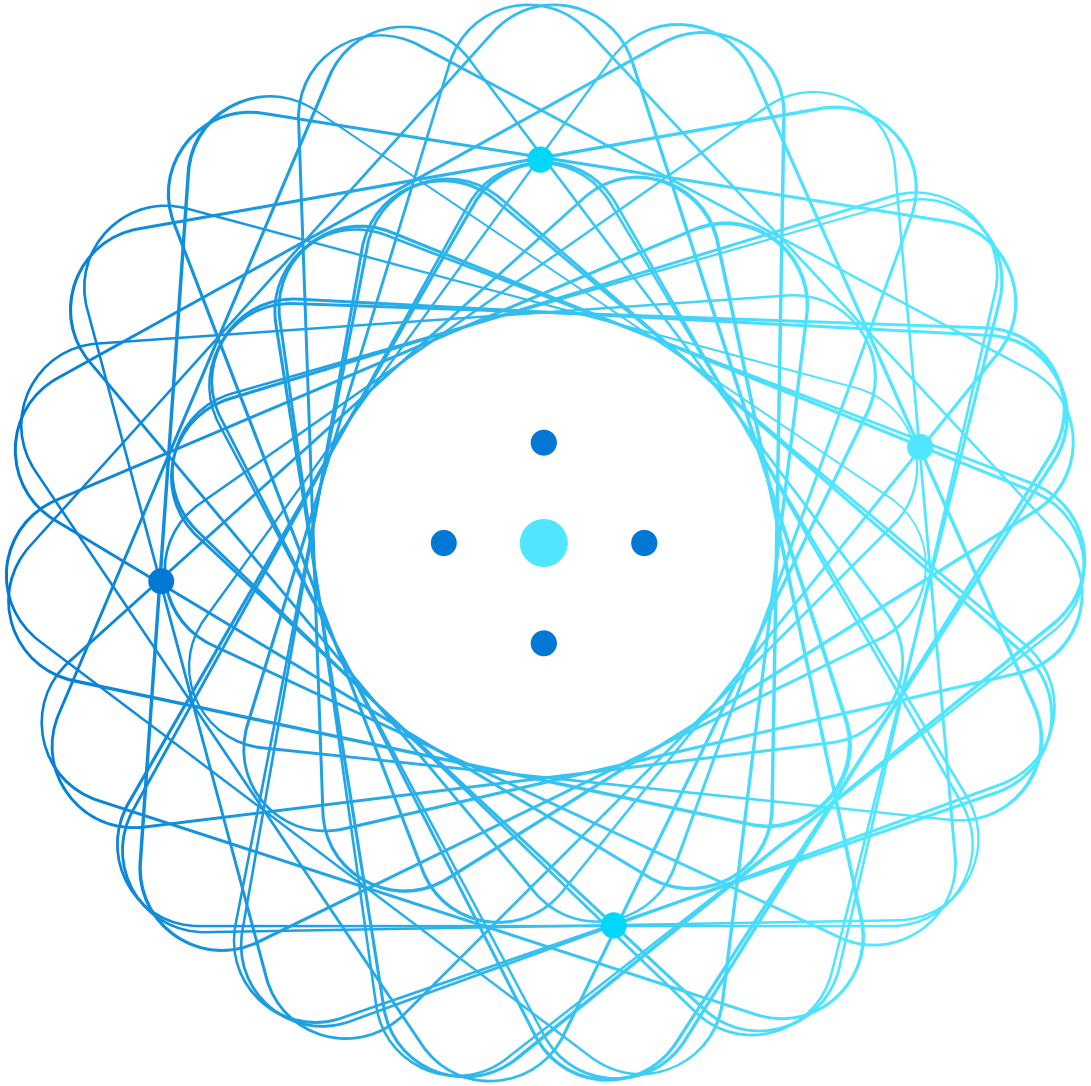
Microsoft Azure

AZ-305

Designing Microsoft Azure Infrastructure Solutions

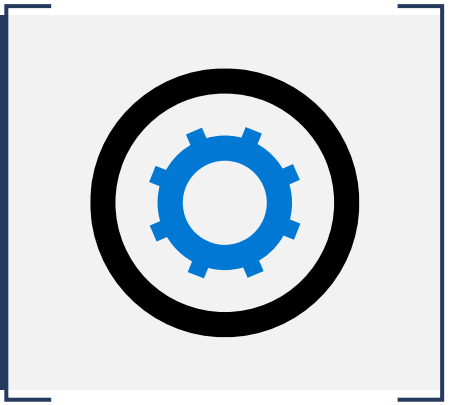


Mark Russinovich

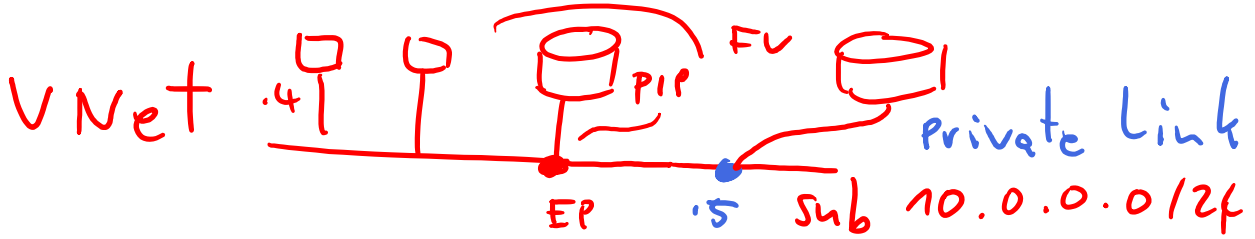
AZ-305 Agenda

Module 01 Design a governance solution
Module 02 Design a compute solution
Module 03 Design a non-relational data storage solution
Module 04 Design a data storage solution for relational data
Module 05 Design a data integration solution
Module 06 Design an application architecture solution
Module 07 Design Authentication and Authorization Solutions
Module 08 Design a solution to log and monitor Azure resources
Module 09 Design a network infrastructure solution
Module 10 Design a business continuity solution
Module 11 Design a migration solution

Design a network infrastructure solution



Introduction



- Recommend a network architecture solution based on workload requirements
- Design for on-premises connectivity to Azure virtual networks
- Design for Azure network connectivity services
- Design for application delivery services
- Design for application protection services

AZ-305: Design Infrastructure Solutions (25-30%)

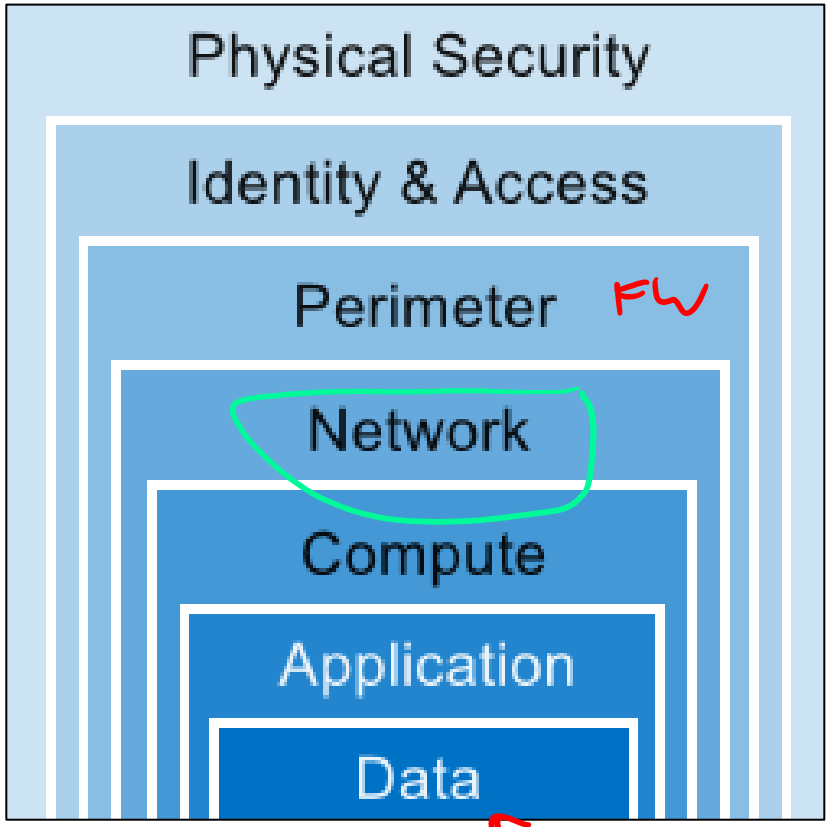
Design network solutions

- Recommend a network architecture solution based on workload requirements
- Recommend a connectivity solution that connects Azure resources to the Internet
- Recommend a connectivity solution that connects Azure resources to on-premises networks
- Optimize network performance for applications
- Recommend a solution to optimize network security
- Recommend a load balancing and routing solution

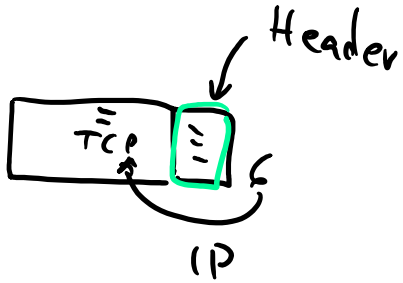
Recommend a network architecture solution based on workload requirements

Defense in Depth (activity)

Provide a layered approach and multiple levels of protection.



- Azure Information Protection
- DDoS Azure Firewall
- Conditional Access
- Network Security Groups
- Microsoft Defender for Cloud for SQL
- Microsoft Defender for Cloud for Storage
- Network Micro-Segmentation
- Host Security
- Privileged Identity Management
- Application Security Groups
- Container Security

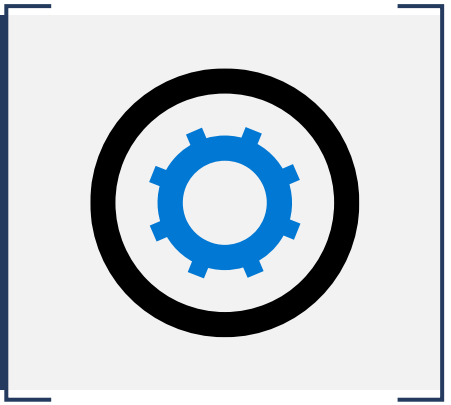


Gather Network Requirements

Plan Virtual Networks and subnets – design considerations

- Naming
- Regions
- Subscriptions
- Segmentation
- Security
- Connectivity
- Permissions
- Policy

Design for on-premises connectivity to Azure virtual networks



VPN connection

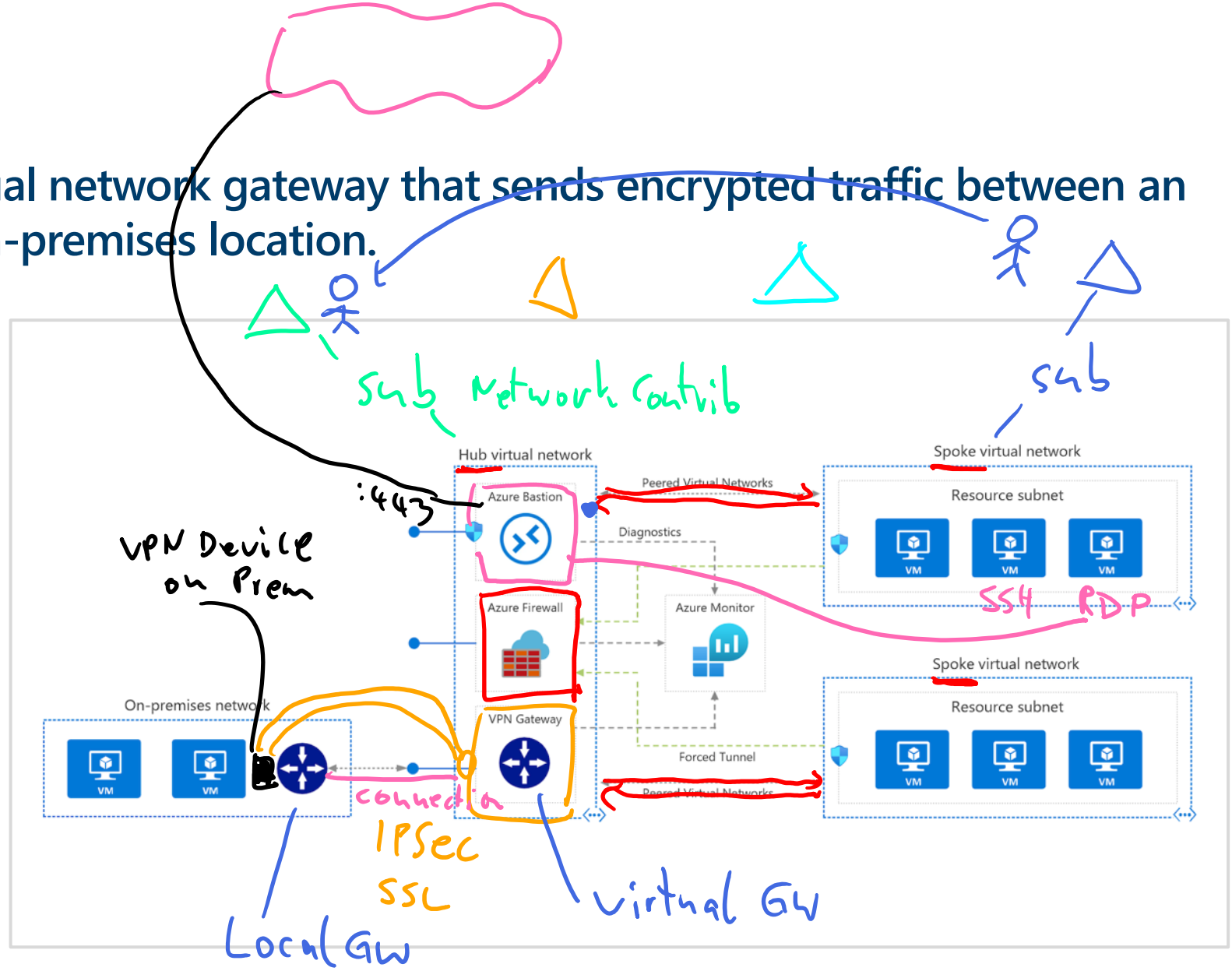
A VPN gateway is a type of virtual network gateway that sends encrypted traffic between an Azure virtual network and an on-premises location.

Benefits

- Simple to configure
- Up to 10 Gbps depending on the VPN Gateway SKU

Challenges

- Requires an on-premises VPN device
- The SLA only covers the VPN gateway, and not your network connection to the gateway or throughput



Azure ExpressRoute and ExpressRoute Direct connection

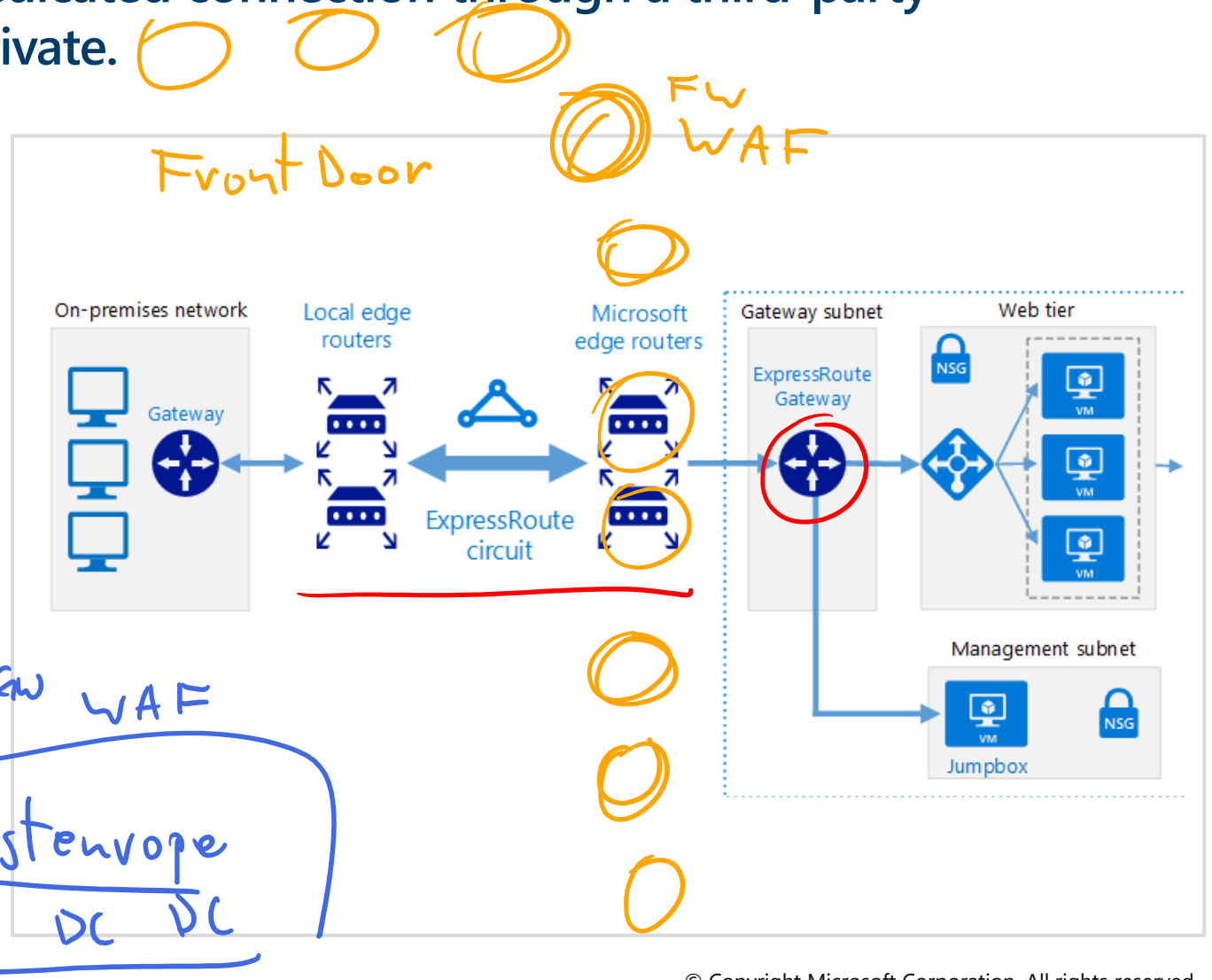
ExpressRoute connections use a private, dedicated connection through a third-party connectivity provider. This connection is private.

Benefits

- Up to 100 Gbps bandwidth - supports dynamic scaling of bandwidth and direct access to national clouds
- Global reach - traffic over private connection
- Up to 99.95% availability SLA across the entire connection.

Challenges

- Can be complex to set up
- working with a third-party connectivity provider
- Requires high-bandwidth routers on-premises



ExpressRoute with VPN failover

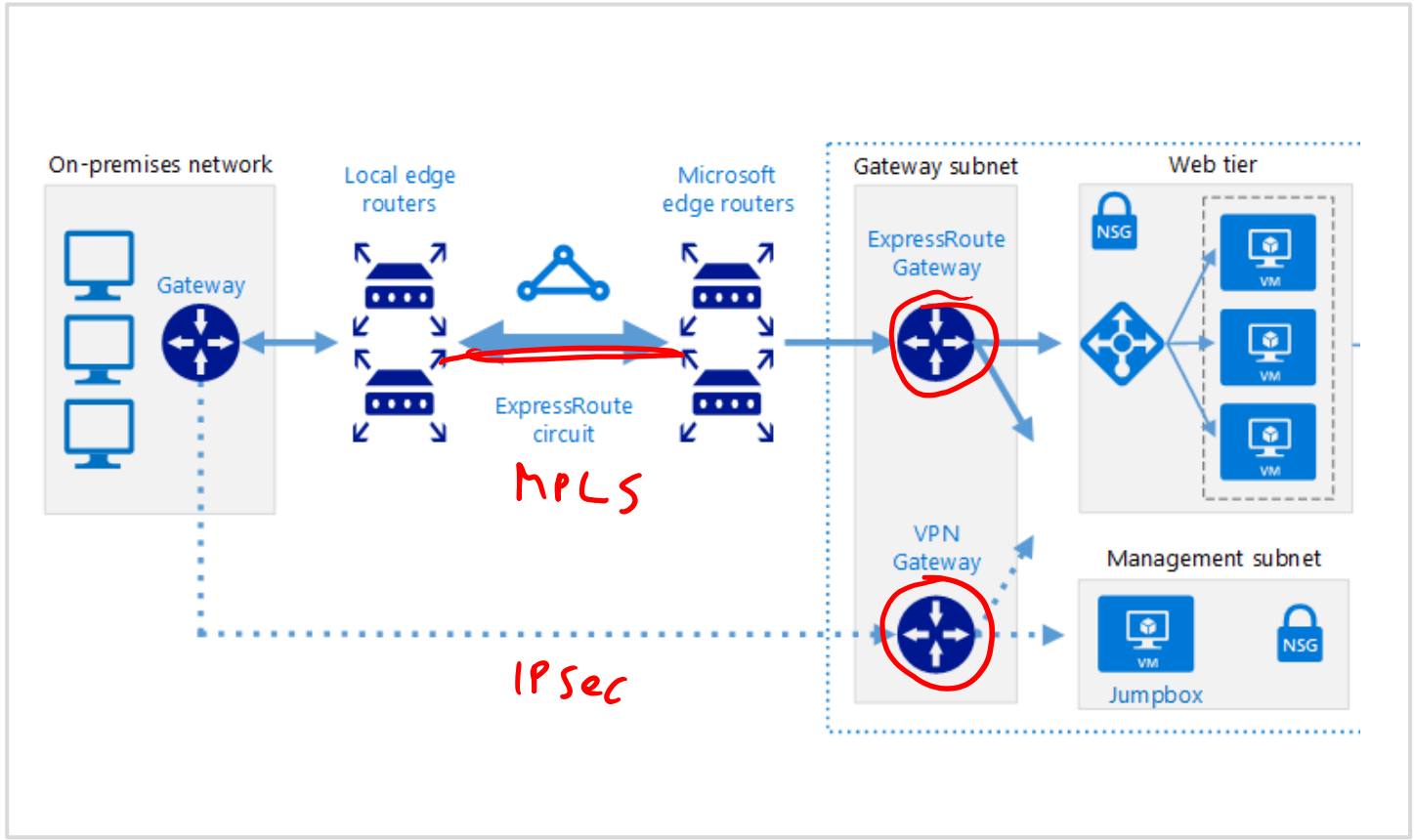
This options combines the previous two, using ExpressRoute in normal conditions, but failing over to a VPN connection if there is a loss of connectivity in the ExpressRoute circuit.

Benefits

- High availability if the ExpressRoute circuit fails, although the fallback connection is on a lower bandwidth network.

Challenges

- Complex to configure. You need to set up both a VPN connection and an ExpressRoute circuit.
- Requires redundant hardware (VPN appliances), and a redundant Azure VPN Gateway connection for which you pay charges.



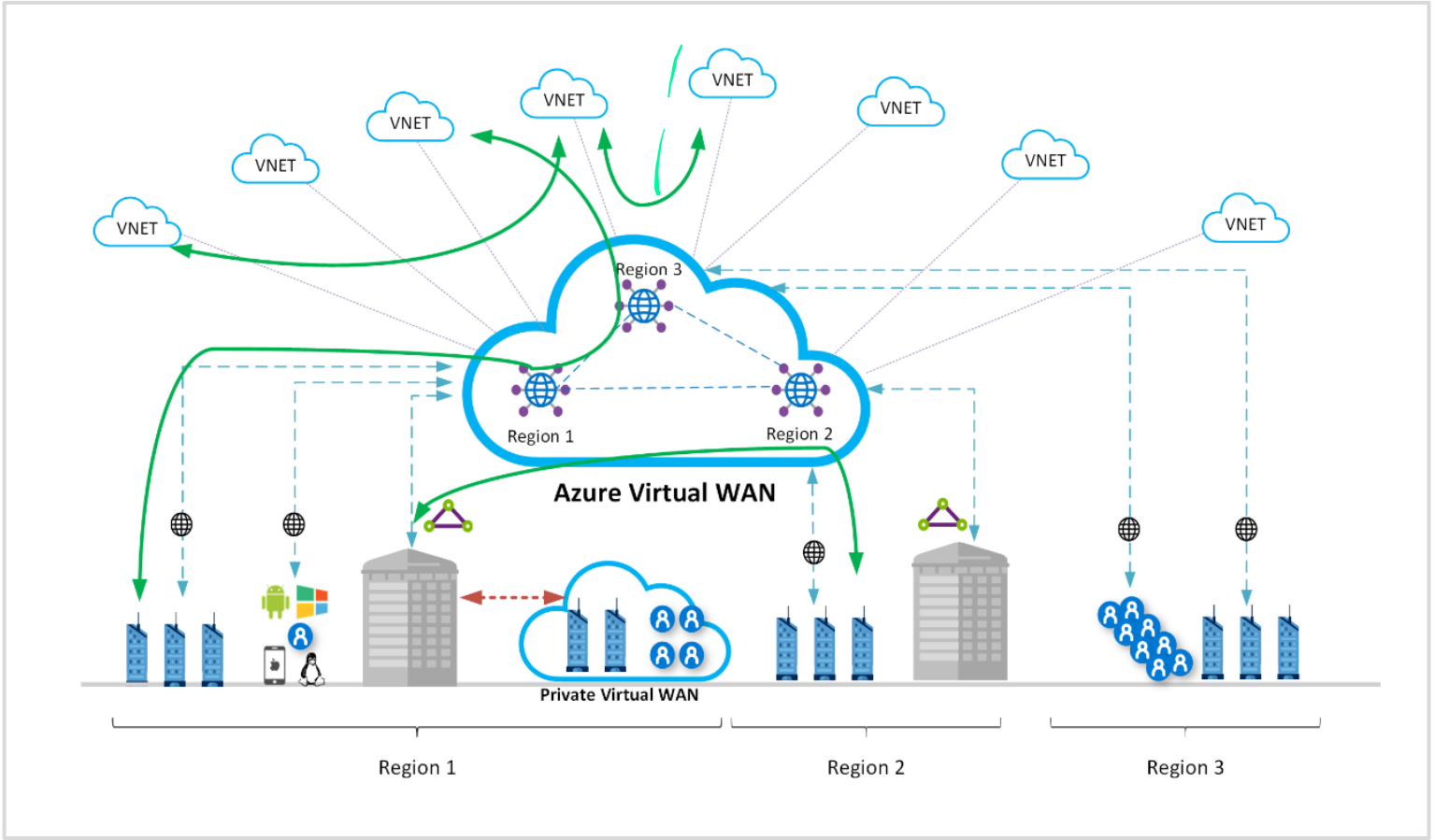
Azure Virtual WAN

VNet Peering VNet

VNet VPN VNet

Azure Virtual WAN is a networking service that brings many networking, security, and routing functionalities together to provide a single operational interface

- Fully managed VWAN service.
- Cost savings by using a managed service and removing the necessity of network virtual appliance.
- Improved security by introducing centrally managed secured Hubs with Azure Firewall and VWAN
- Separation of concerns between central IT (SecOps, InfraOps) and workloads (DevOps).

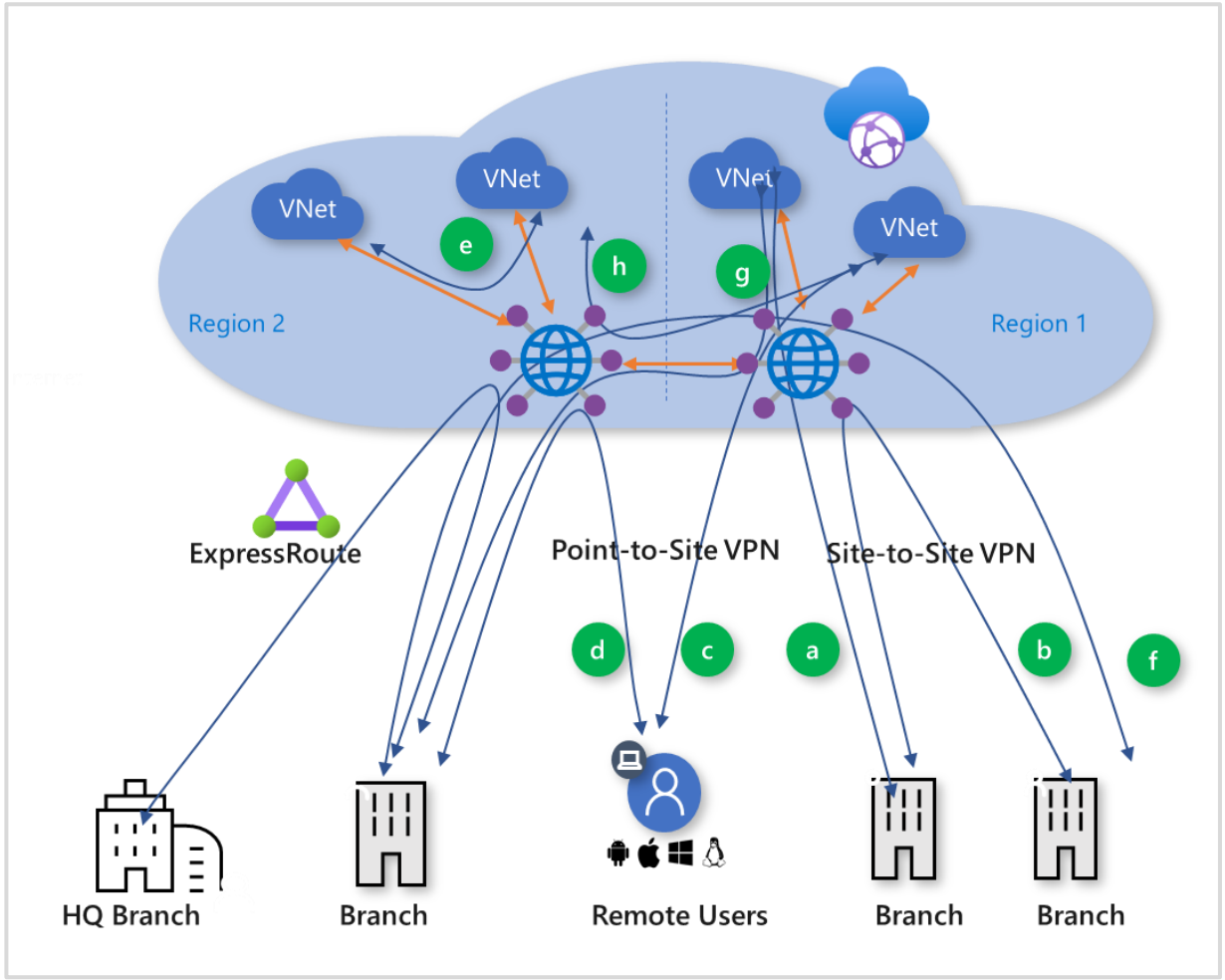


Global transit network with Virtual WAN

Global transit network architecture is being adopted by enterprises to consolidate, connect, and control the cloud-centric modern, global enterprise IT footprint

Azure Virtual WAN supports the following global transit connectivity paths:

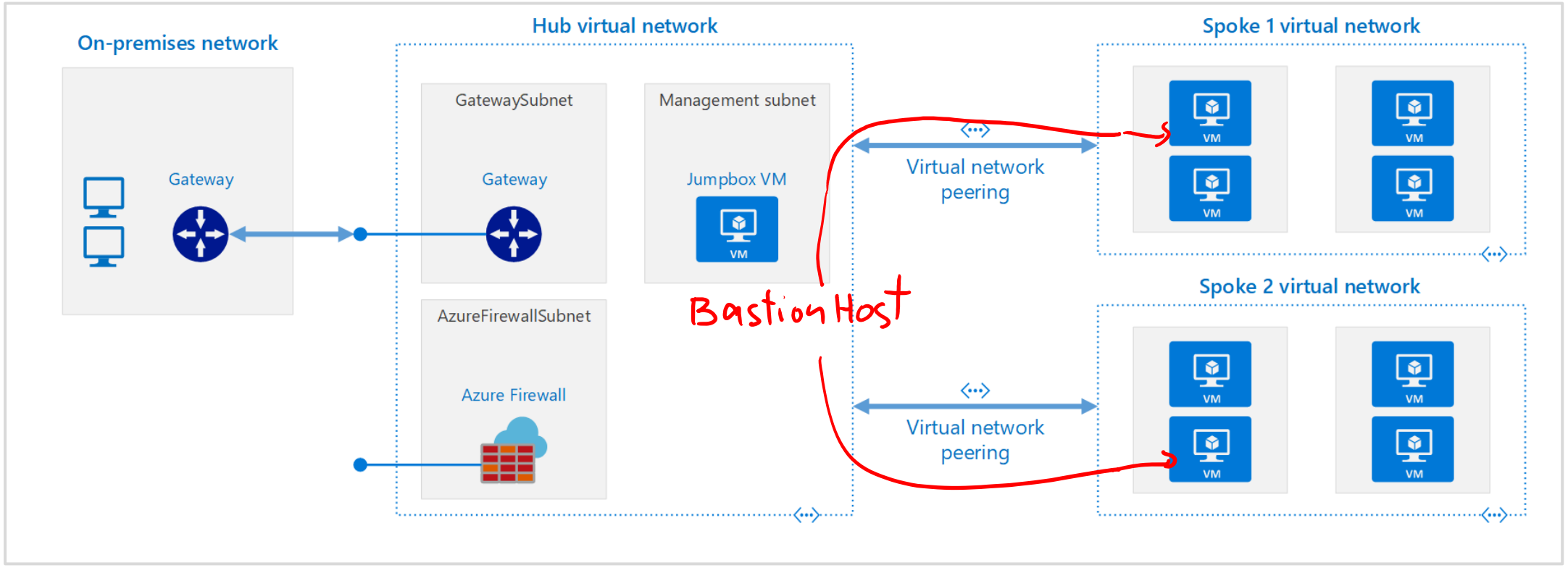
- Branch-to-VNet (a)
- Branch-to-branch (b)
    - ExpressRoute Global Reach and Virtual WAN
- Remote User-to-VNet (c)
- Remote User-to-branch (d)
- VNet-to-VNet (e)
- Branch-to-hub-hub-to-Branch (f)
- Branch-to-hub-hub-to-VNet (g)
- VNet-to-hub-hub-to-VNet (h)



Design for Azure network connectivity services

Design Azure Virtual networks

Azure Virtual Network is the fundamental building block for your private network in Azure. A virtual network is a virtual, isolated portion of the Azure public network. Use VNets to communication between Azure resources, the internet and on-premises networks.



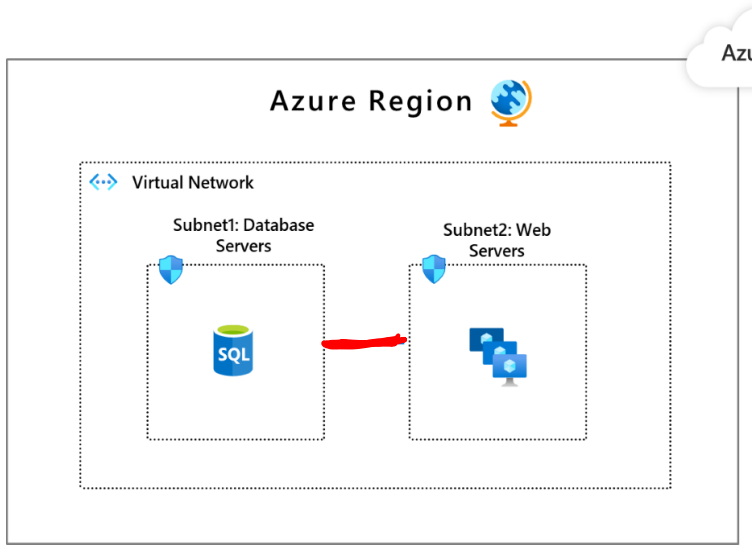
Design network topology

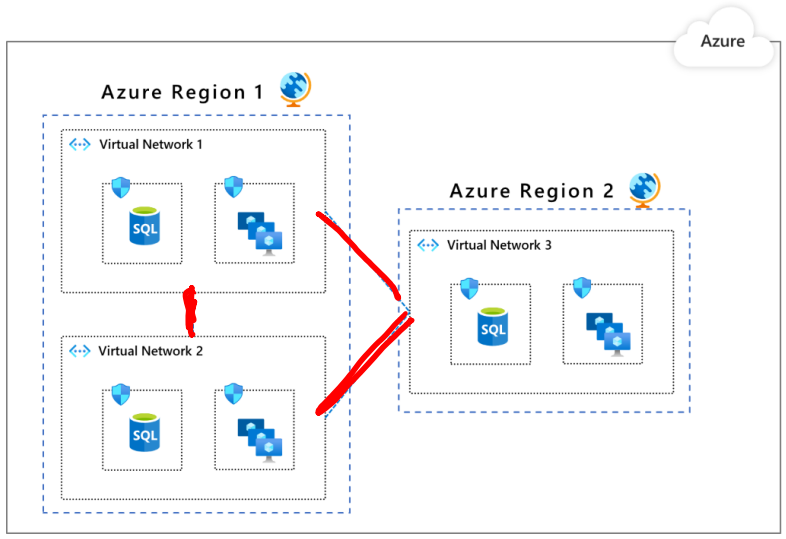
Segmentation is a model in which you take your networking footprint and create software defined perimeters using tools available in Microsoft Azure.

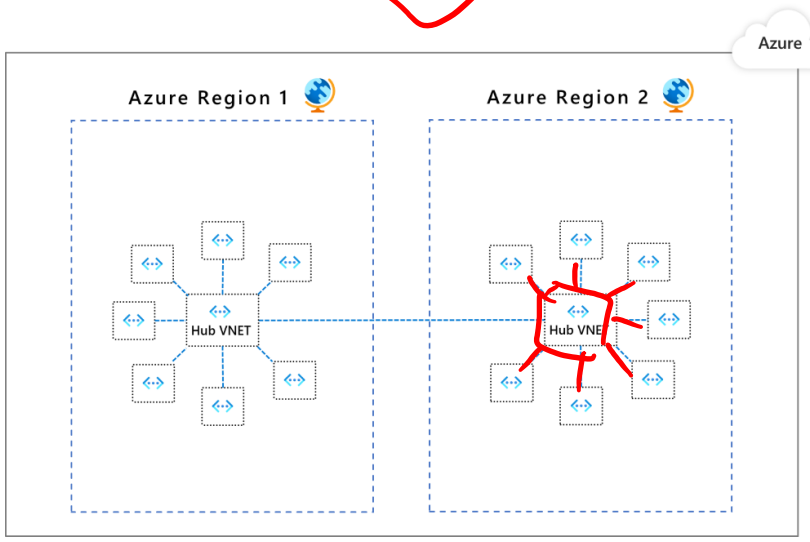
Pattern 1: Single Virtual Network

Pattern 2: Multiple Virtual Networks with peering in between them

Pattern 3: Multiple Virtual Networks in a hub & spoke model

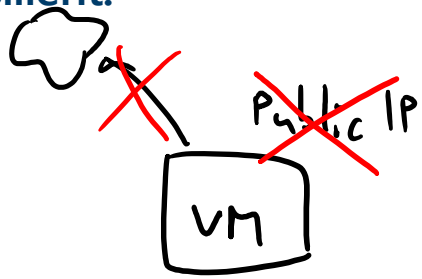






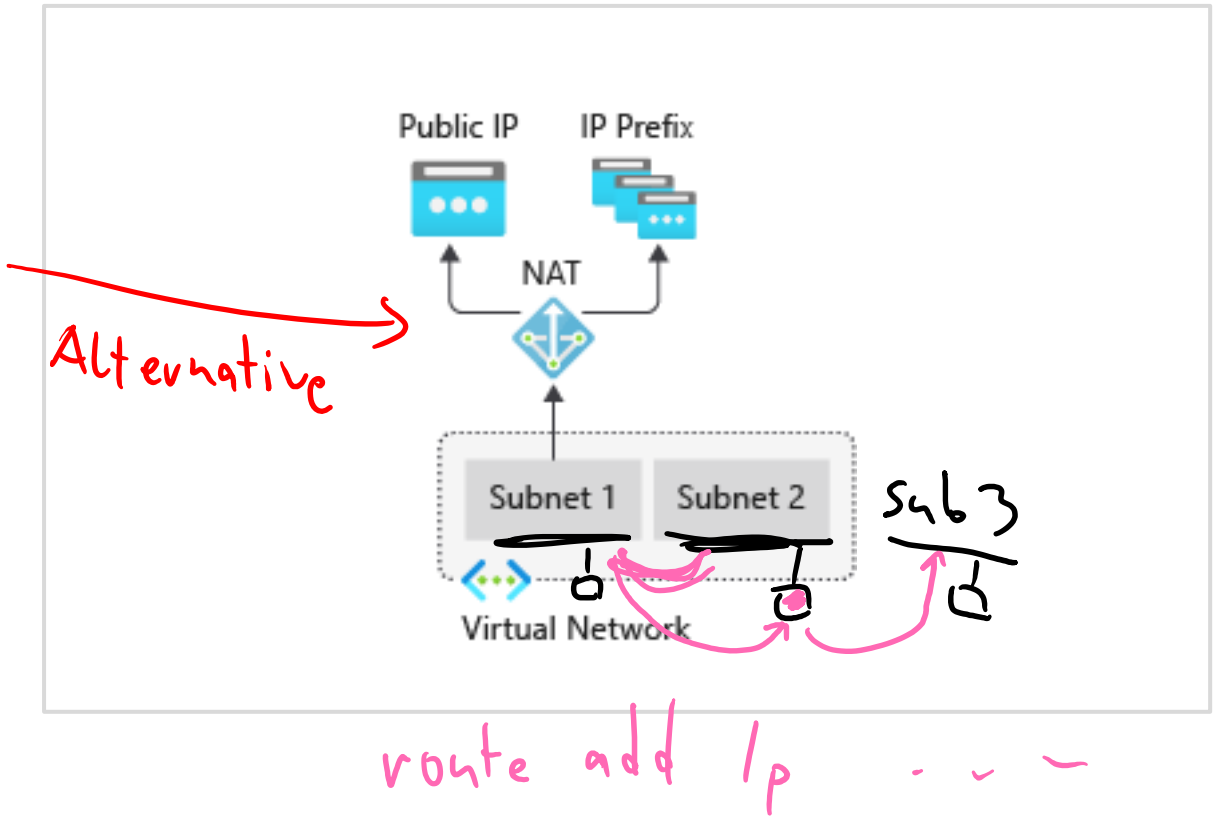
Design Outbound Connectivity

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. NAT is fully managed and highly resilient.



Options include:

- Azure Firewall
- Load balancer
- Virtual Network NAT gateway

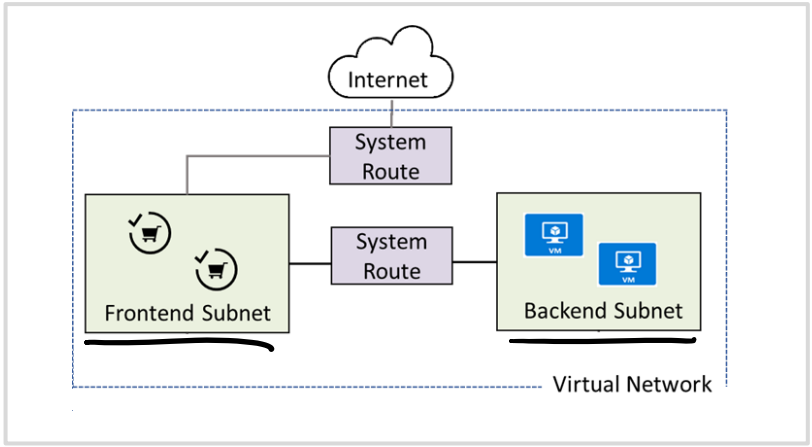


Choose Virtual Network NAT gateway when:

- You need on-demand outbound to internet connectivity without pre-allocation
- You need one or more static public IP addresses for scale
- You need configurable idle timeout
- You need TCP reset for unrecognized connections

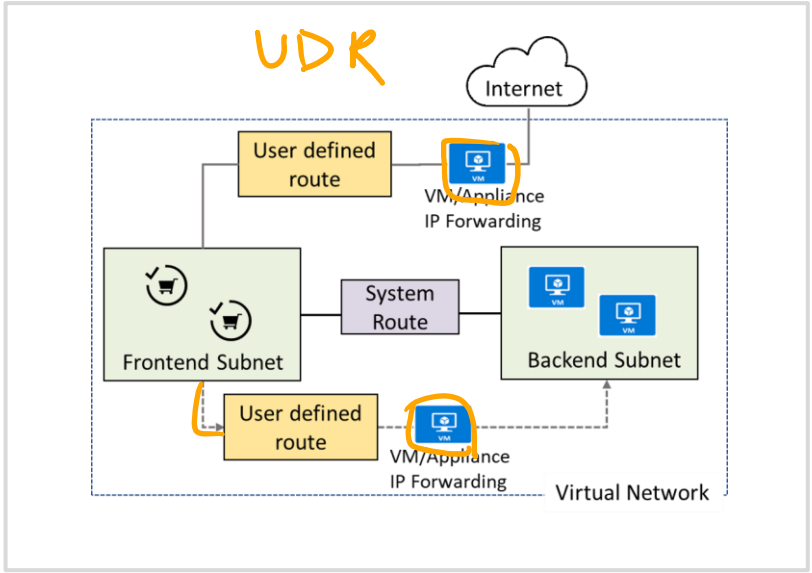
Design Routing

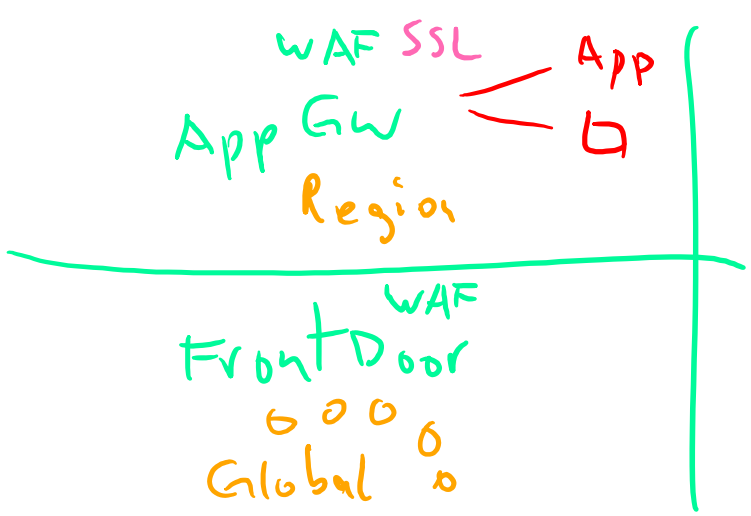
- When you create a virtual network for the first time without defining any subnets, Azure creates routing entries in the routing table.
- When creating subnets inside a virtual network, Azure creates default entries in the routing table to enable communication between subnets within a virtual network.
- When creating a virtual network peering between two virtual networks, a route is added for each address range within the address space of each virtual network for which a peering is created.

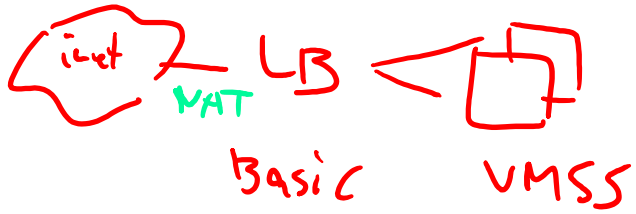


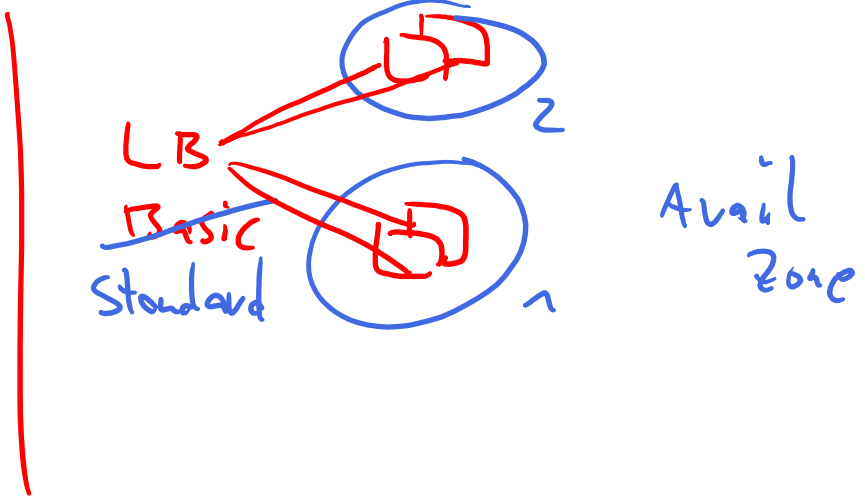
Types and priority of routes:

- User Defined Routes (UDR)
- BGP routes
- System routes

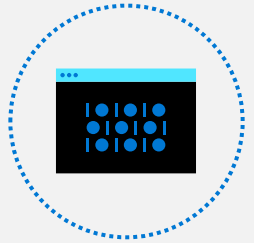








Design for application delivery services

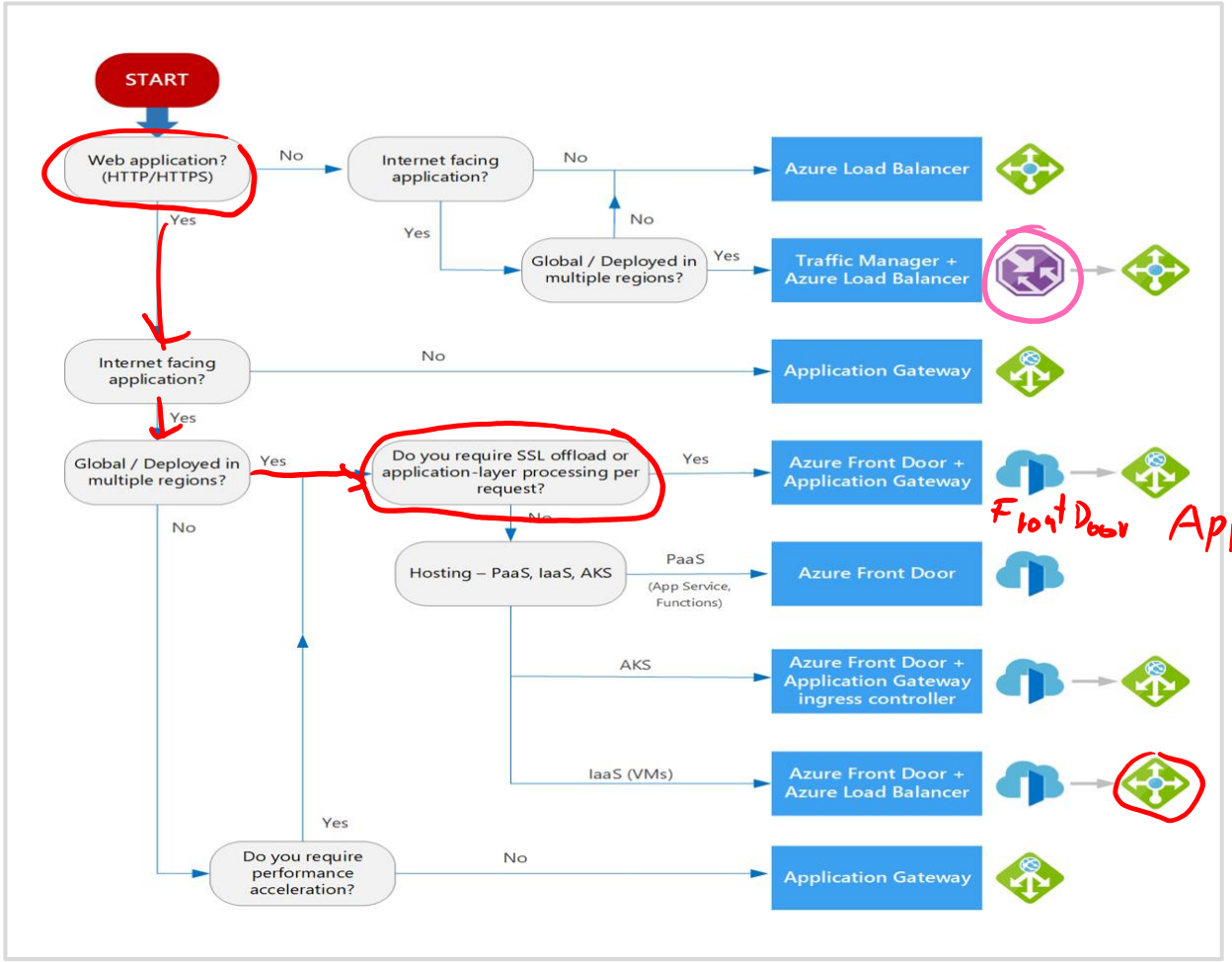


Choosing a load balancer solution

Azure provides various load balancing services that you can use to distribute your workloads across multiple computing resources – Azure Front Door, Traffic Manager, Load Balancer, and Application Gateway.

Decision criteria

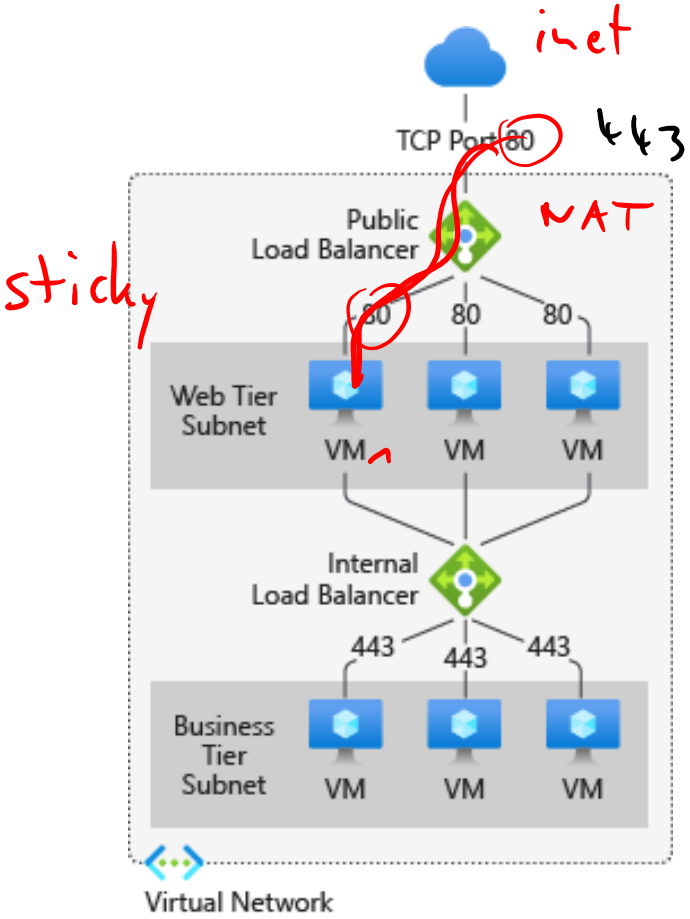
- Traffic type
- Global versus. regional
- Availability
- Cost
- Features and limits
- Treat this flowchart as a starting point



Load Balancer

High-performance, low-latency load-balancing for all UDP and TCP protocols

- Layer 4 load-balancing for all UDP and TCP protocols
- Manages inbound and outbound connections
- Provides public and internal load-balanced endpoints
- Uses rules to map inbound connections to backend destinations
- Health probes manage service availability

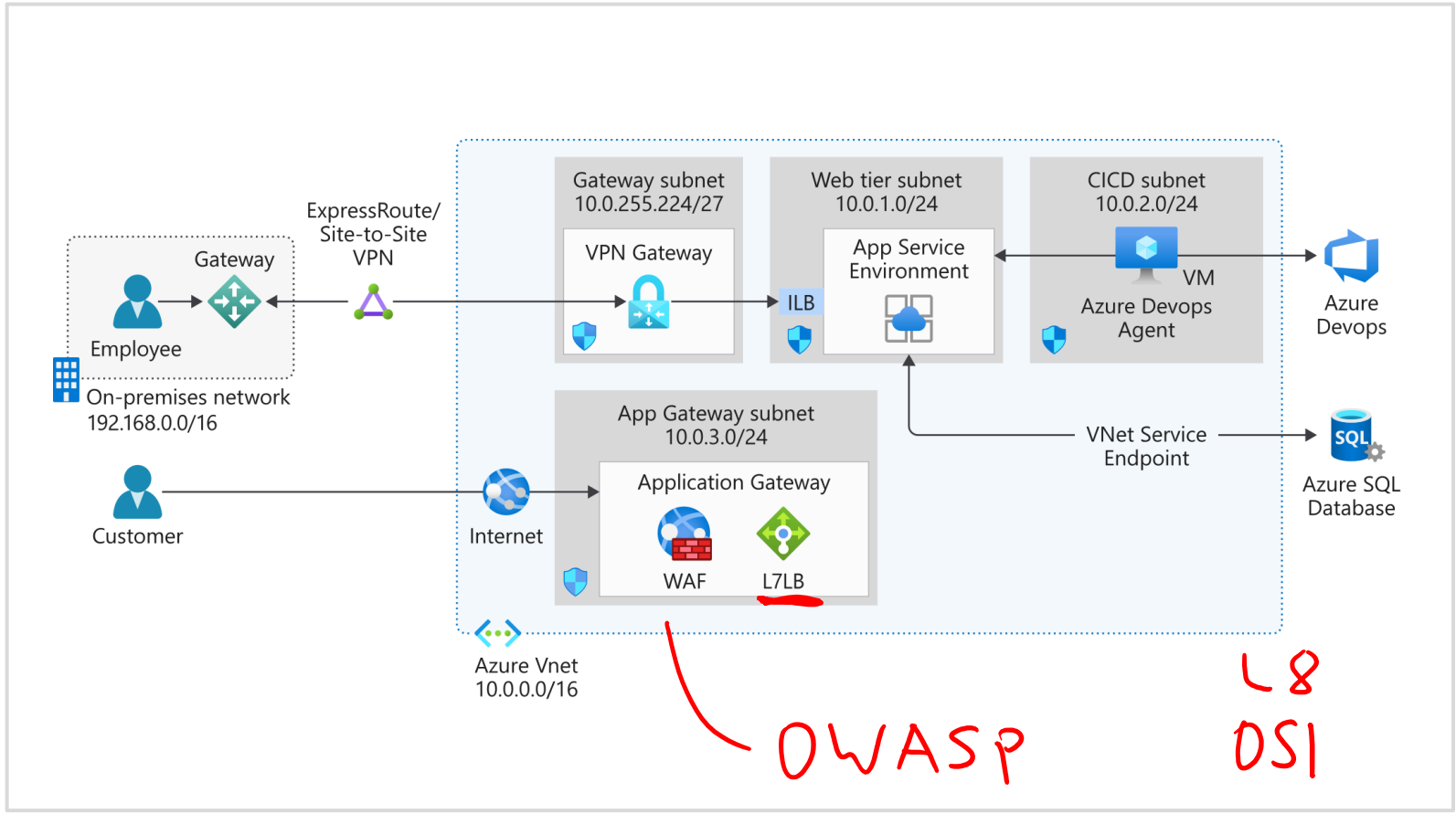


Application Gateway

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications. It is an Application Delivery Controller (ADC) as a service, offering various layer 7 load-balancing capabilities for your applications.

When to use Application Gateway

- Layer 7 - HTTP(s) only
- Supports WAF -stateful inspection
- Traffic routing
- SSL/TLS termination
- Supports PaaS and Ips
- Regional service



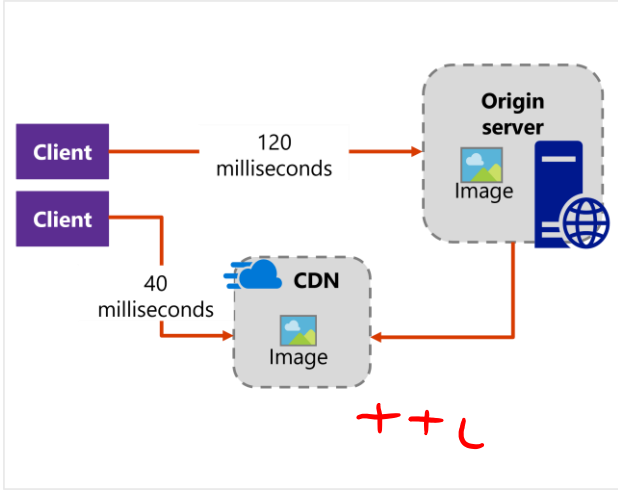
Content Delivery Network (CDN)

Microsoft
Akamai

Azure CDN 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.

When to leverage a CDN:

- You want point-of-presence locations that are close to large clusters of users.
- You want to reduce latency - both the transmission delay and the number of router hops.
- You want custom domains, file compression, caching, and geo-filtering.

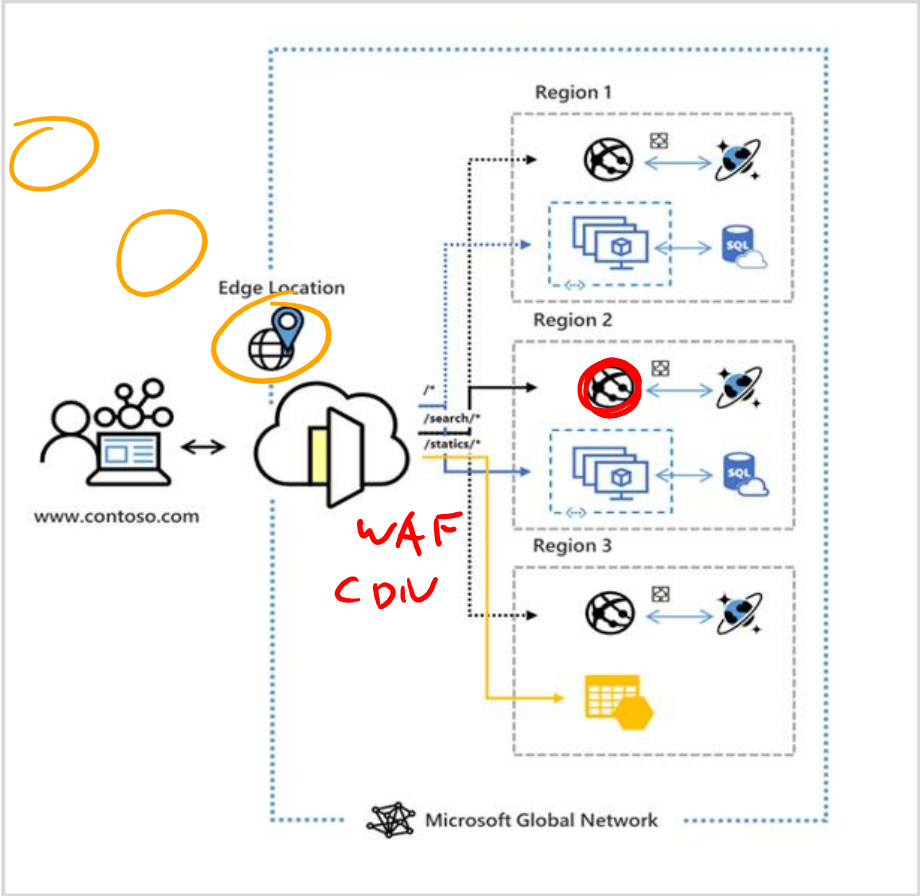


Azure Front Door Service

Azure Front Door Service enables you to define, manage, and monitor the global routing for your web traffic by optimizing for best performance and instant global failover for high availability.

Choose Front Door when:

- You need to ensure that requests are sent to the lowest latency backends (low latency)
- You have primary and secondary backends (priority)
- You want to distribute traffic using weight coefficients (weighted)
- You want to ensure requests from the same end user gets sent to the same backend (affinity)
- Your traffic is HTTP(s) based and you need WAF and/or CDN integration

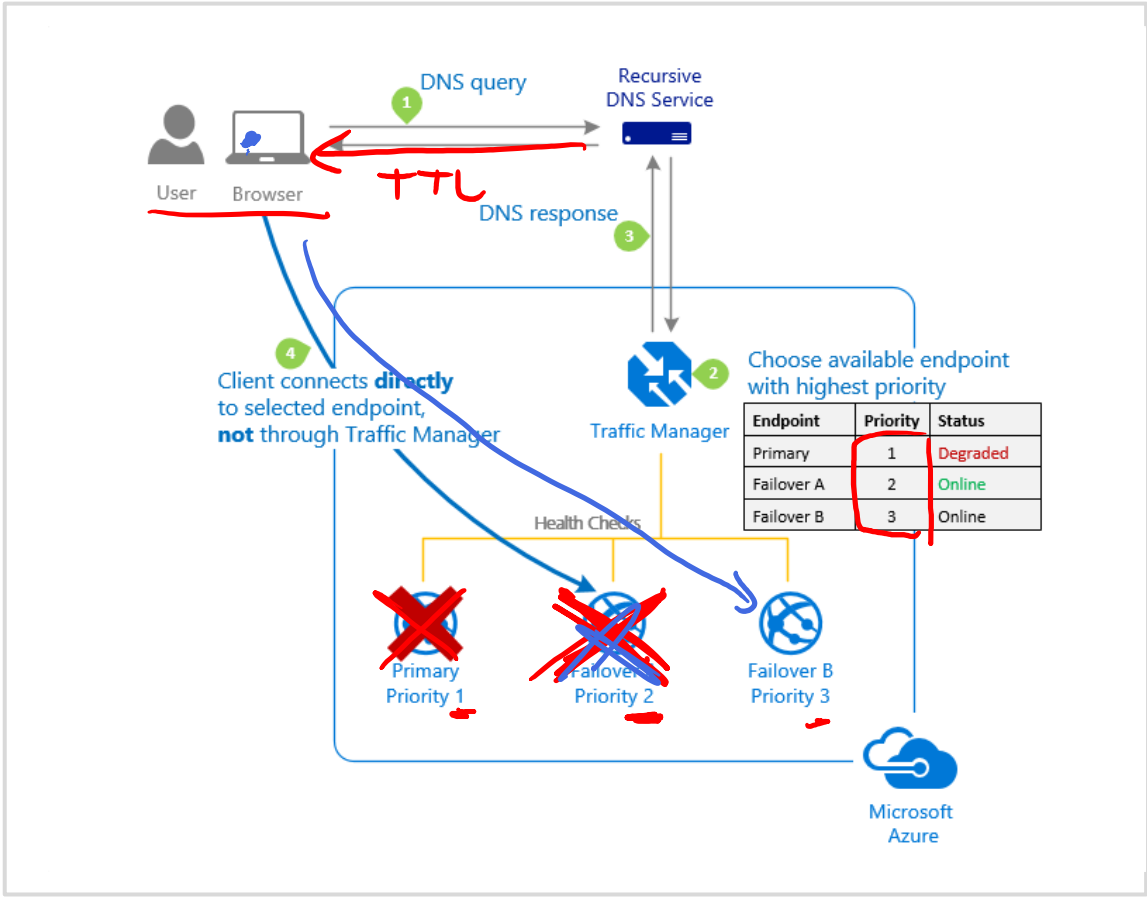


Traffic Manager

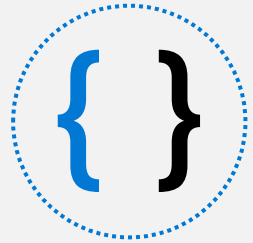
Azure Traffic Manager is a DNS-based traffic load balancer that enables you to distribute traffic optimally to services across global Azure regions. Traffic Manager provides a range of traffic-routing methods to distribute traffic such as priority, weighted, performance, geographic, multi-value, or subnet.

Choose Traffic Manager when you need:

- To increase application availability
- Improve application performance
- Combine hybrid applications
- Distribute traffic for complex deployments



Design for application protection services

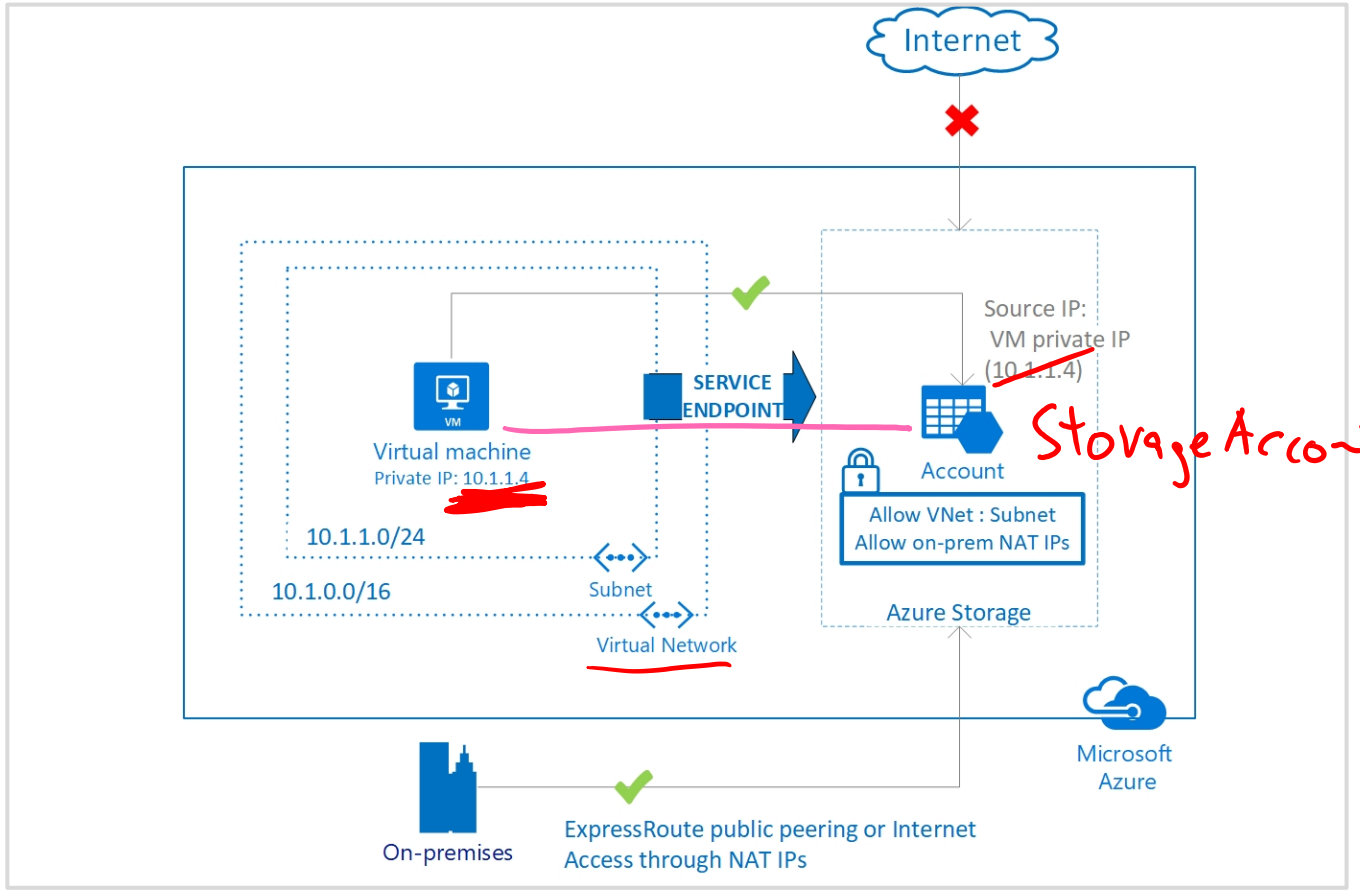


Service endpoints

Virtual Network (VNet) service endpoint provides secure and direct connectivity to Azure services over an optimized route over the Azure backbone network

Key Benefits:

- Improved security for your Azure service resources
- Optimal routing for Azure service traffic from your virtual network
- Simple to set up with less management overhead

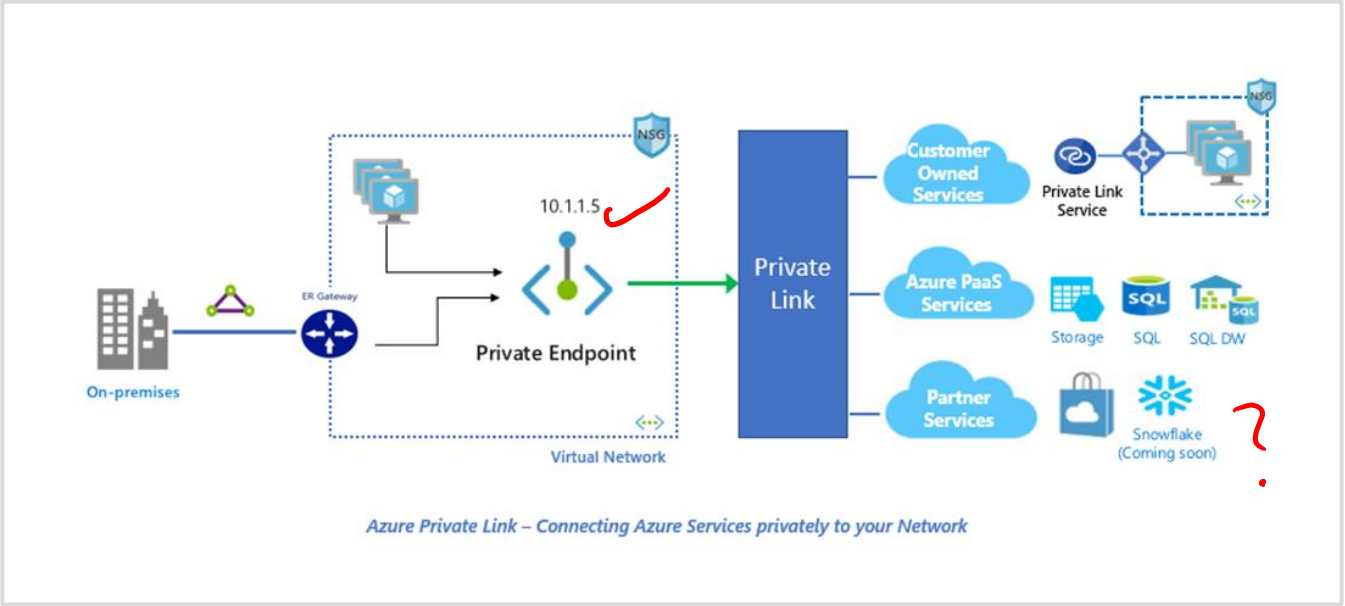


Azure Private Link

Azure Private Link enables you to 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. Private link is used to access PaaS services such as Azure Storage, Azure SQL, App Services and more as illustrated below.

Recommend private link or private endpoints when:

- You need private connectivity to services on Azure
- You need integration with on-premises and peered networks
- You need traffic to remain on Microsoft network, with no public internet access



Azure Private Link – Connecting Azure Services privately to your Network

Network security groups

You can filter network traffic to and from Azure resources in an Azure virtual network with a network security group.

A network security group (NSG) contains a list of Access Control List (ACL) rules that allow or deny network traffic to subnets, NICs, or both.

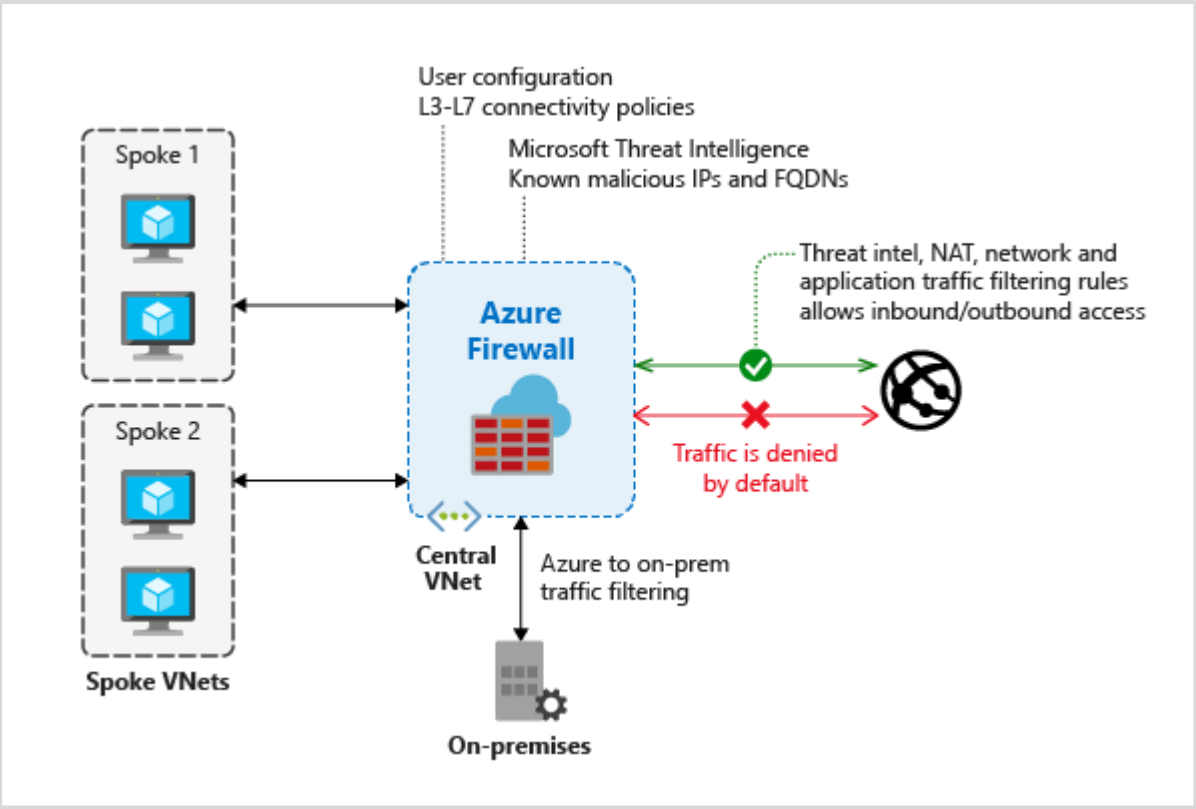
NSGs contain two sets of rules: inbound and outbound. The priority for a rule must be unique within each set.

Azure Firewall

Azure firewall is a cloud-native network security service offering high-availability and scalability. Azure Firewall provides inbound protection for non-HTTP/S protocols (for example, RDP, SSH, FTP), outbound network-level protection for all ports and protocols, and application-level protection for outbound HTTP/S.

Use Azure Firewall to:

- Protect your network against infiltration.
- Implement hierarchical firewall policies.
- Configure spoke-to-spoke connectivity.
- Monitor incoming and outgoing traffic.
- If you require multiple firewalls.

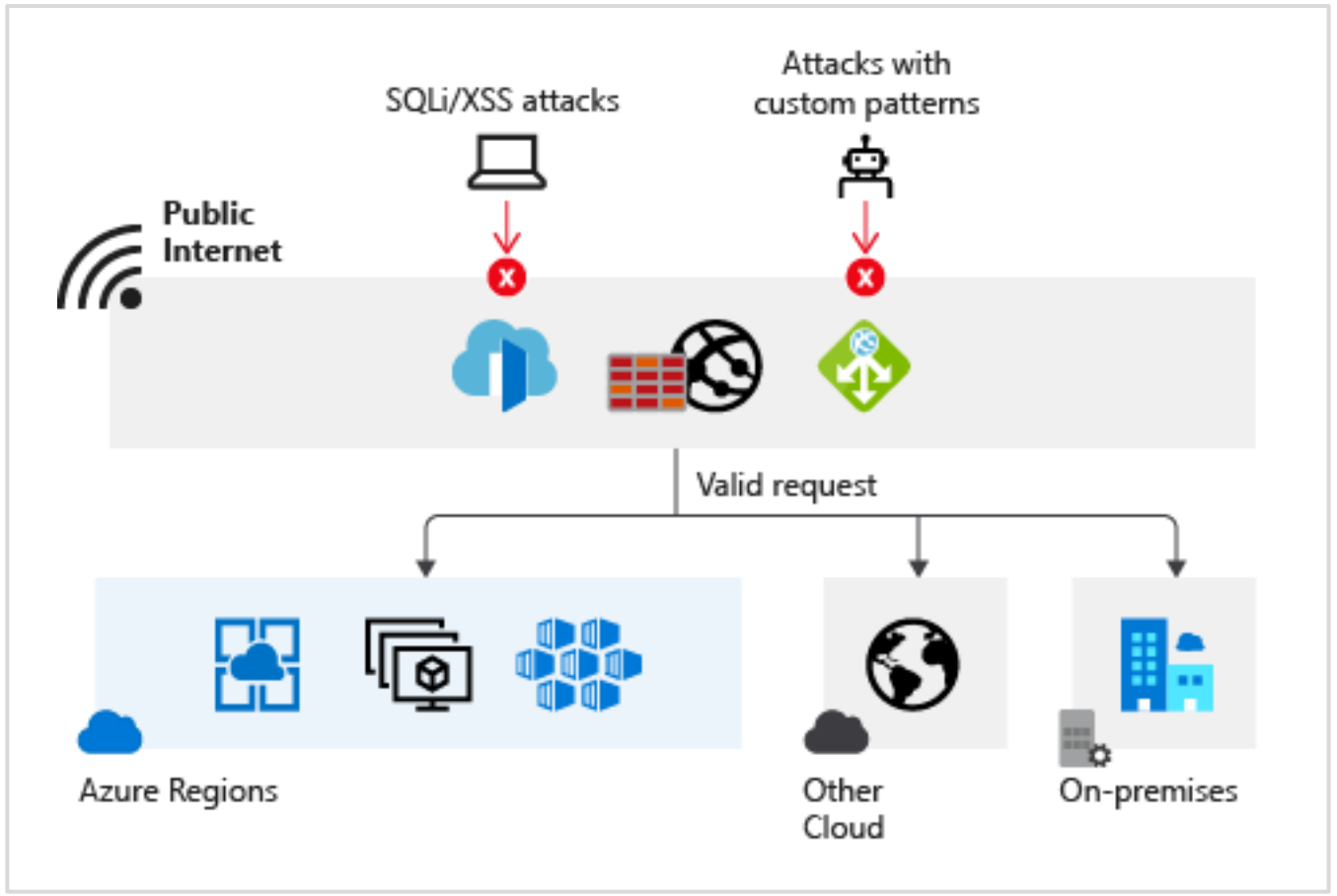


Web Application Firewall

Azure Web Application Firewall (WAF) provides centralized protection to your web applications from common web exploits and vulnerabilities such as SQL injection, and cross site scripting. Azure WAF provides out of box protection from OWASP top 10 vulnerabilities via managed rules.

When to use Web Application firewall:

- To prevent attacks in application code
- Centrally manage security for applications
- Deploy WAF with Azure Application Gateway, Azure Front Door and Azure Content Delivery Network (CDN)



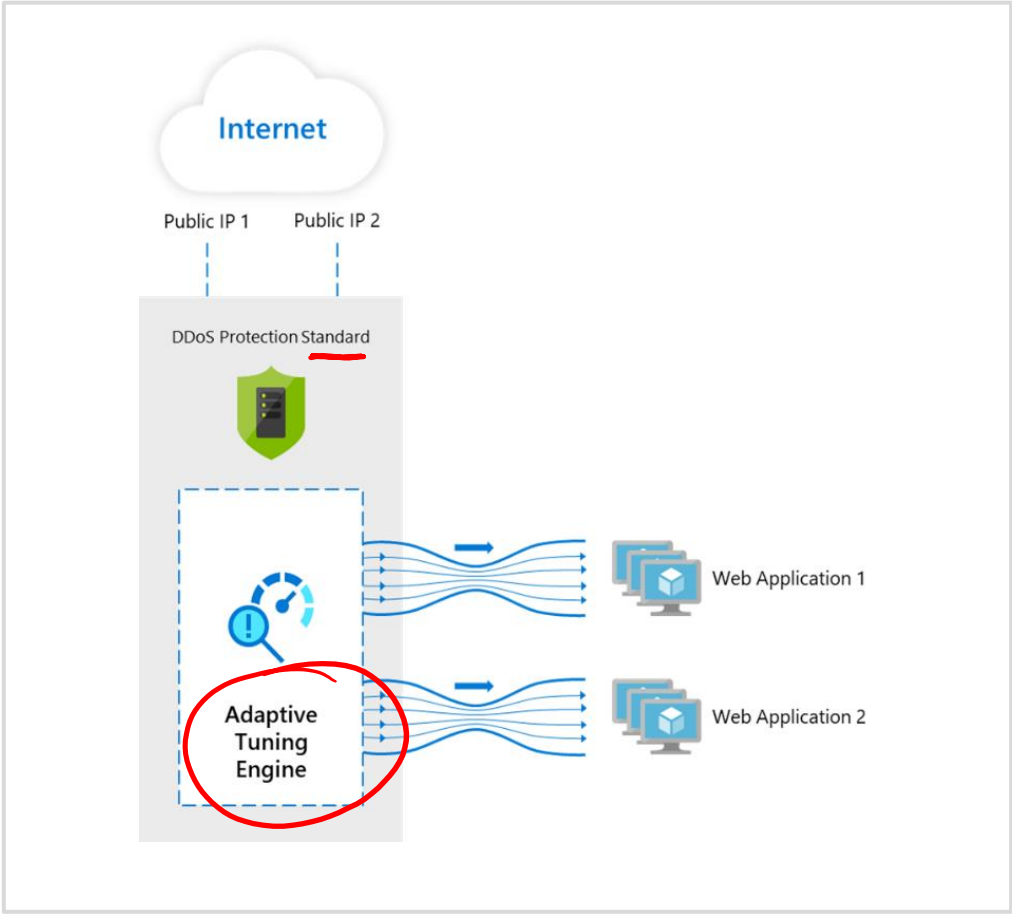
DDoS Protection

Azure DDoS Standard Protection provides countermeasures against the most sophisticated DDoS threats. The service provides enhanced DDoS mitigation capabilities for your application and resources deployed in your virtual networks.

Basic

Use DDoS protection Standard:

- Always-on traffic monitoring
- Adaptive tuning
- Multi-layered protection
- Mitigation scale
- Attack analytics and metrics
- Attack alerting
- DDoS rapid response

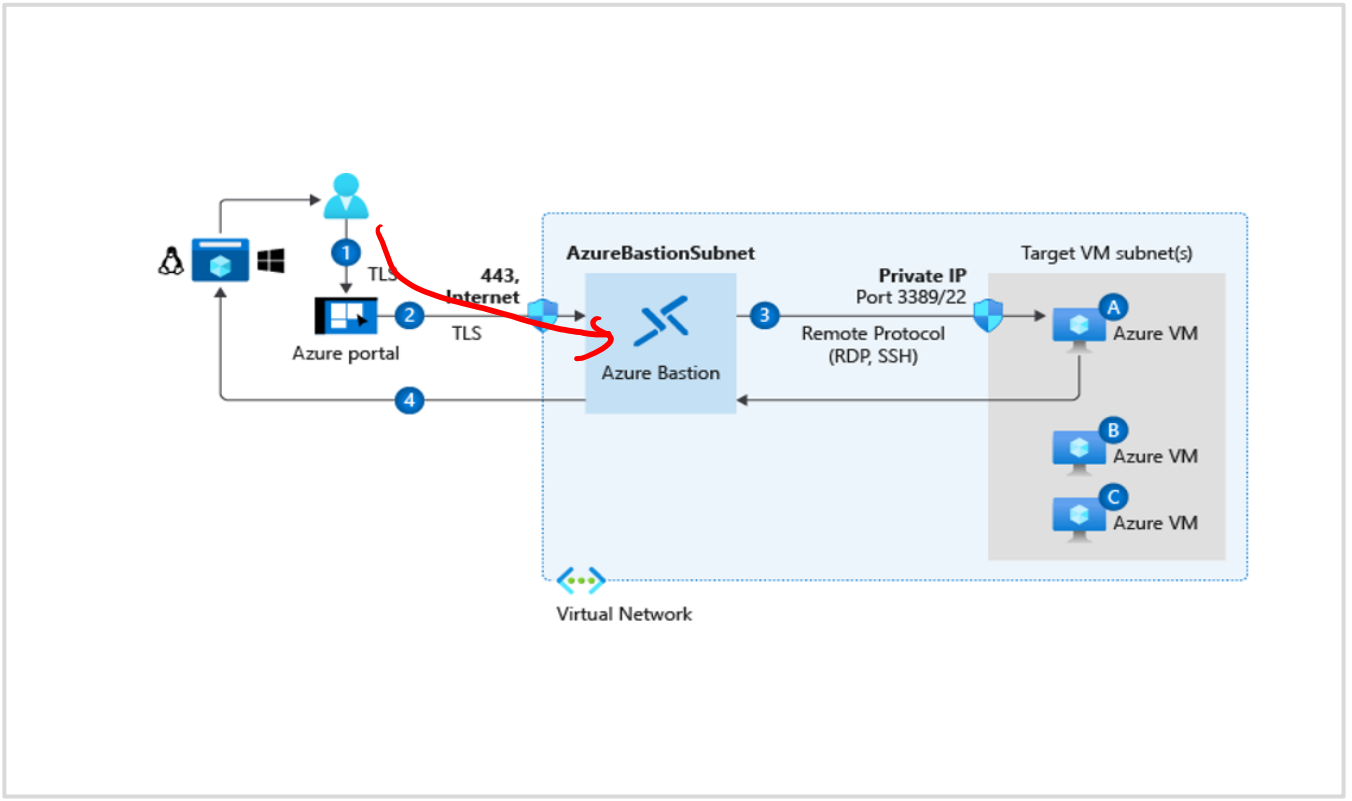


Azure Bastion

The Azure Bastion service is a fully platform-managed PaaS service which provides secure and seamless RDP/SSH connectivity to your virtual machines directly in the Azure portal over TLS.

Recommend Azure Bastion when you n eed to:

- Secure remote connections from the Azure portal to Azure VMs
- Eliminate exposing RDP and SSH public IP addresses of your Azure VMs
- Access VMs across multiple, peered networks



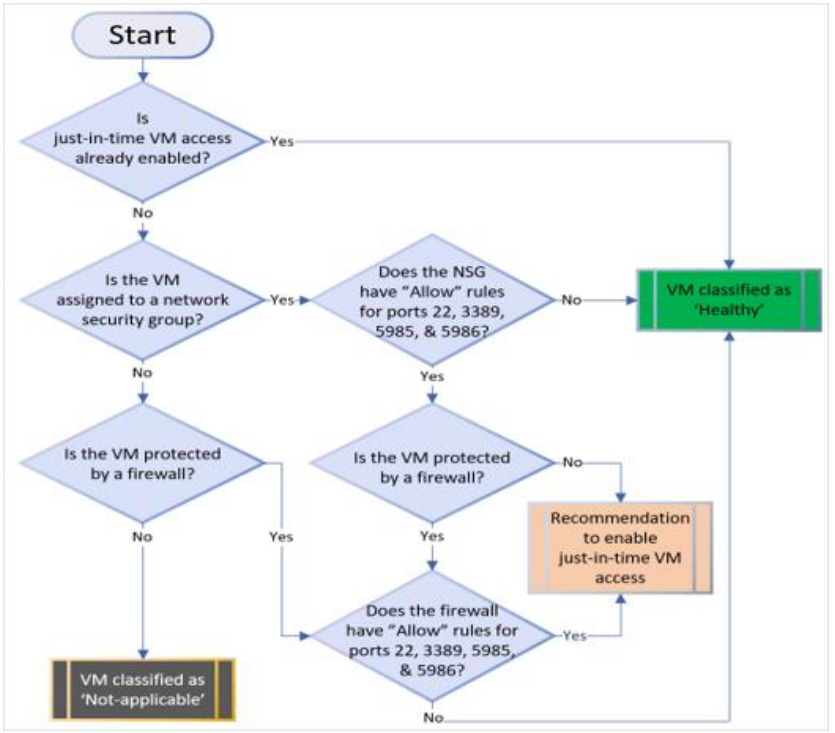
Just in Time (JIT) Network Access

PS
JEA Just Enough Admin
DSC
TLA Three Letter Acronym

With JIT, you can lock down the inbound traffic to your VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.

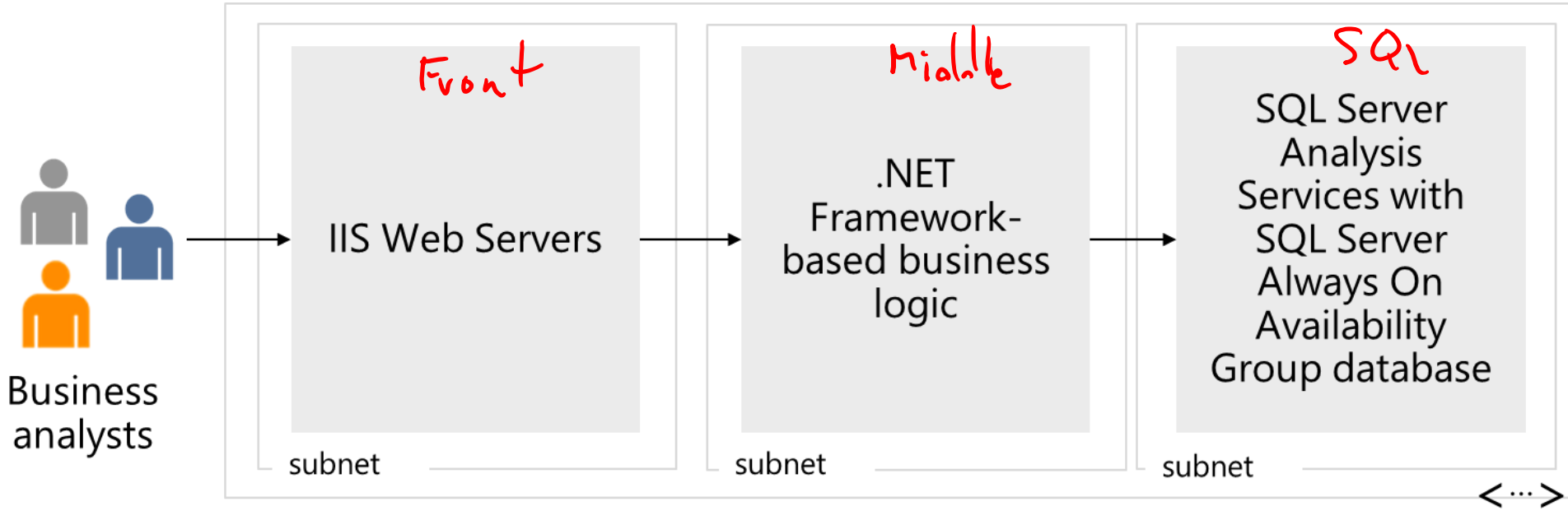
Defender for Cloud (ASC)

- Supports ports other than 3389 and 22
- Ports are blocked when not in use
- Integrates with NSGs and Azure Firewall



Review

Case Study – BI enterprise application

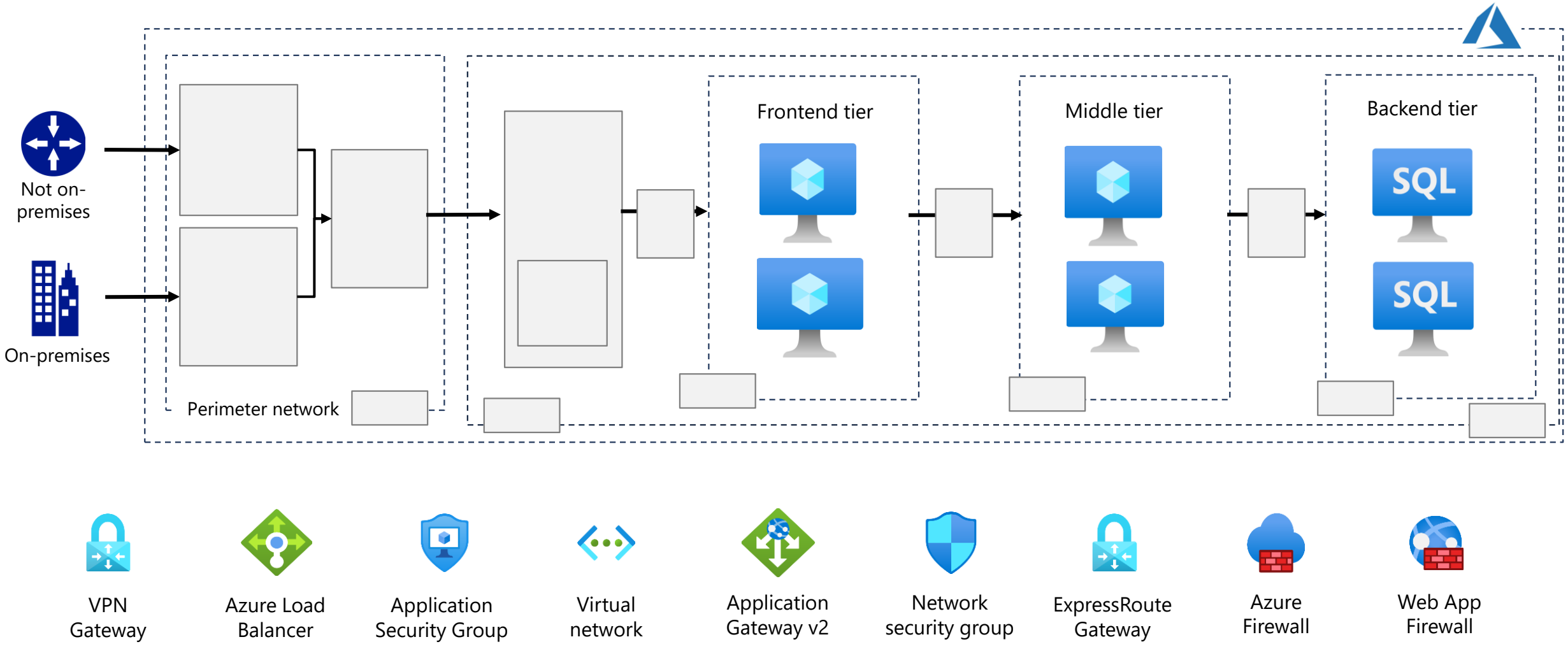


- Heavy demand.
- Servers reach their performance limits during the day.
- Servers sit idle during off hours.

- Rest API call from the front-end tier
- Request demand changes from day to day

- Uses all-flash enterprise SAN storage

Instructor solution - BI enterprise application



VPN Gateway

Azure Load Balancer

Application Security Group

Virtual network

Application Gateway v2

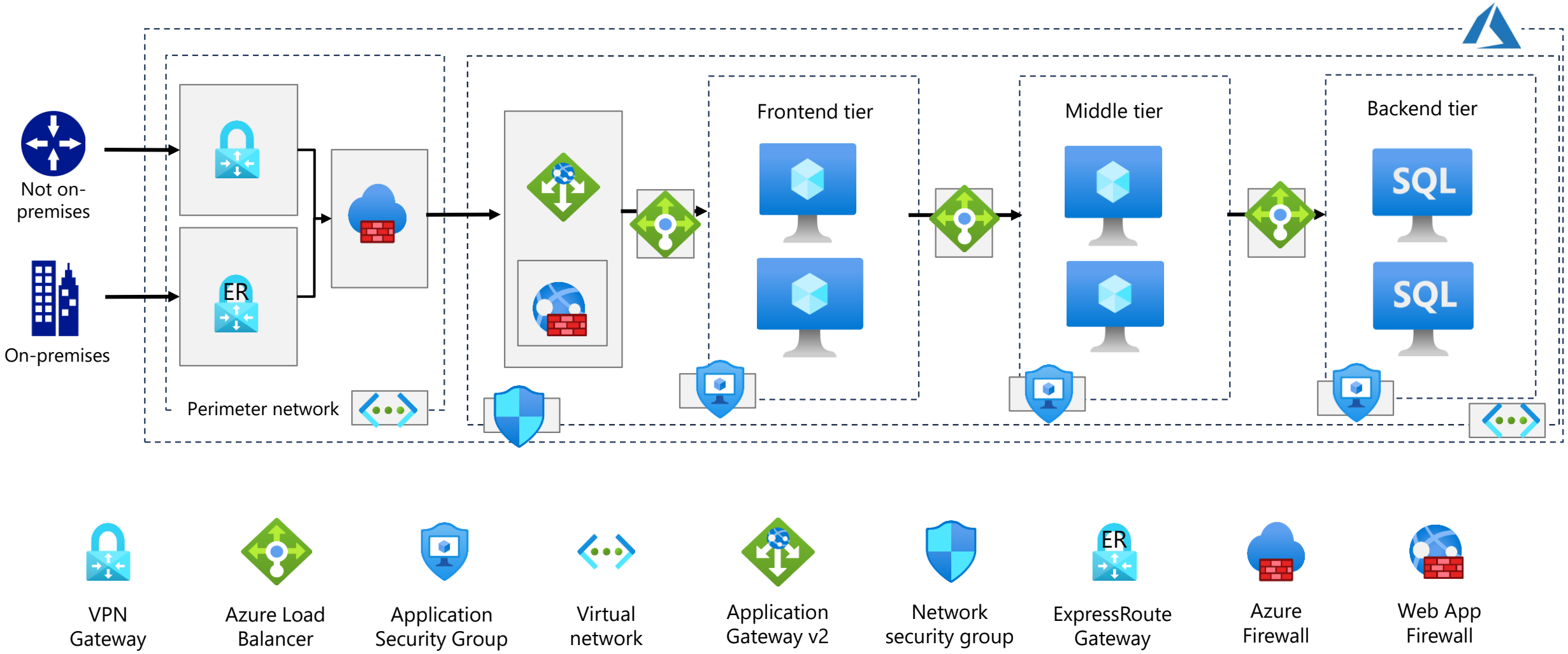
Network security group

ExpressRoute Gateway

Azure Firewall

Web App Firewall

Completed instructor solution - BI enterprise application



VPN Gateway

Azure Load Balancer

Application Security Group

Virtual network

Application Gateway v2

Network security group

ExpressRoute Gateway

Azure Firewall

Web App Firewall

Summary and resources

Check your knowledge

Microsoft Learn Modules (docs.microsoft.com/Learn)

- AZ-700 Designing and Implementing Microsoft Azure Networking Solutions - Learn | Microsoft Docs
- Explore Azure networking services - Learn | Microsoft Docs
- Secure network connectivity on Azure (AZ-900) - Learn | Microsoft Docs
- Architect network infrastructure in Azure - Learn | Microsoft Docs

- Optional hands-on lab - Distribute your services across Azure virtual networks and integrate them by using virtual network peering
- Optional hands-on lab - Secure and isolate access to Azure resources by using network security groups and service endpoints

End of presentation