



# AZ-305T00A

## Designing Microsoft Azure Infrastructure Solutions



# Design a network infrastructure solution



# Learning Objectives

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

## AZ-305: Design Infrastructure Solutions (30-35%)

### Design network solutions

- Recommend a connectivity solution that connects Azure resources to the internet
- Recommend a connectivity solution that connects Azure resources to on-premises networks
- Recommend a solution to optimize network performance
- 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.



Layers

Compute

Perimeter

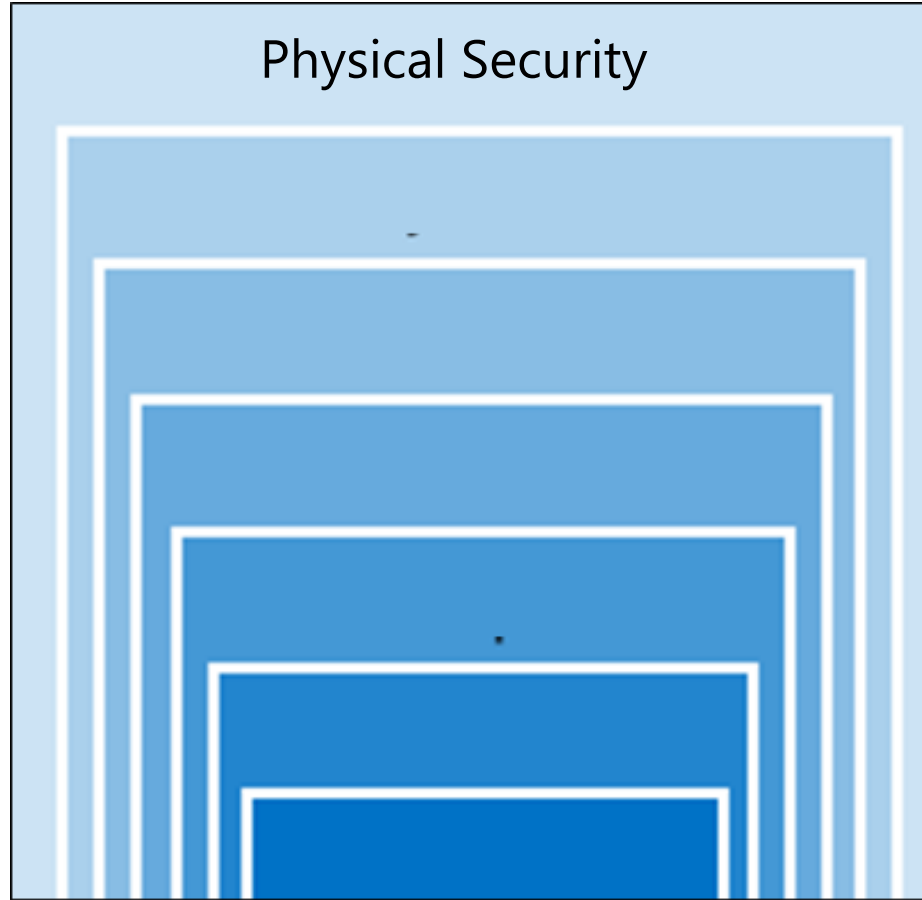
Identity & Access













Application

Data

Physical Security

Network



-  Application Security Groups
-  Azure Firewall
-  Network Security Groups
-  Conditional Access
-  Datacenter security
-  Container security
-  DDoS
-  Azure Information Protection
-  Defender for Cloud Storage
-  Privileged Identity Management
-  Azure Key Vault
-  Host security

# Gather Network Requirements

## Plan Virtual Networks and subnets – design considerations

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

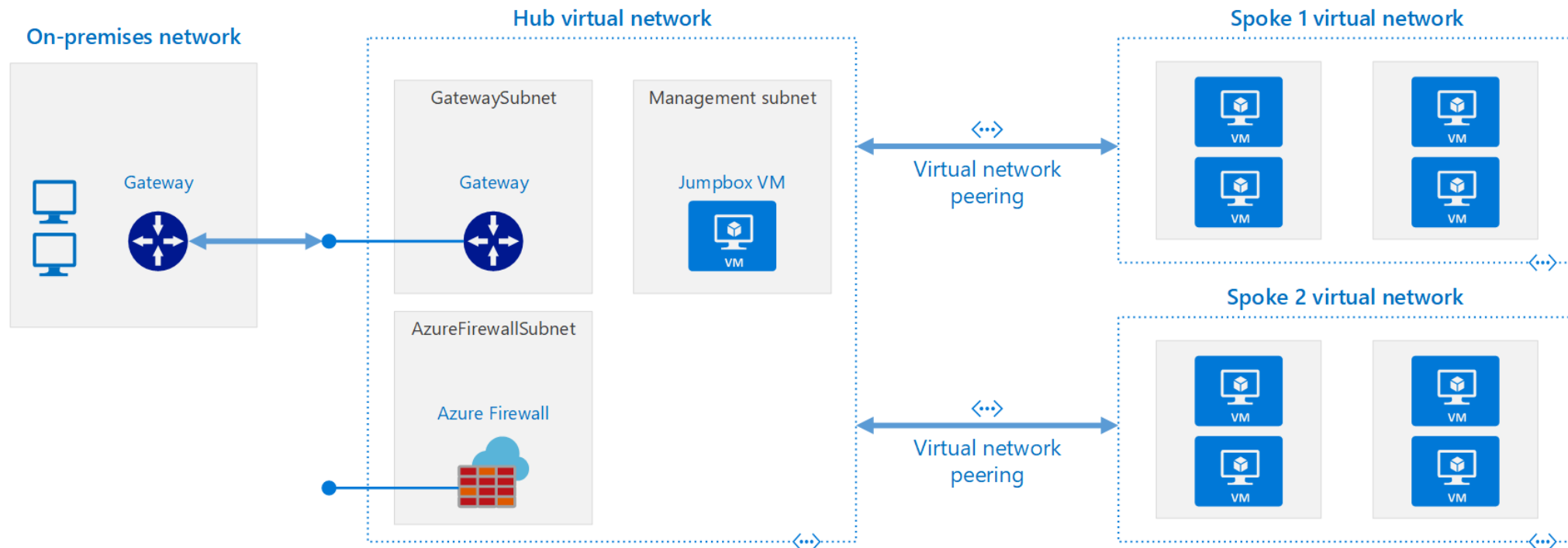


# Design for Azure network connectivity services



# 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.





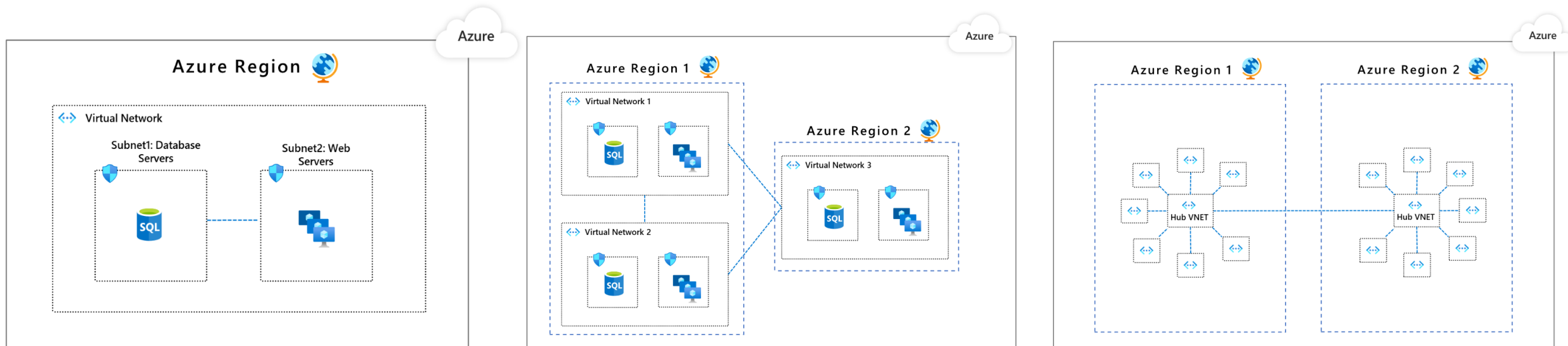
# Design network topology

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

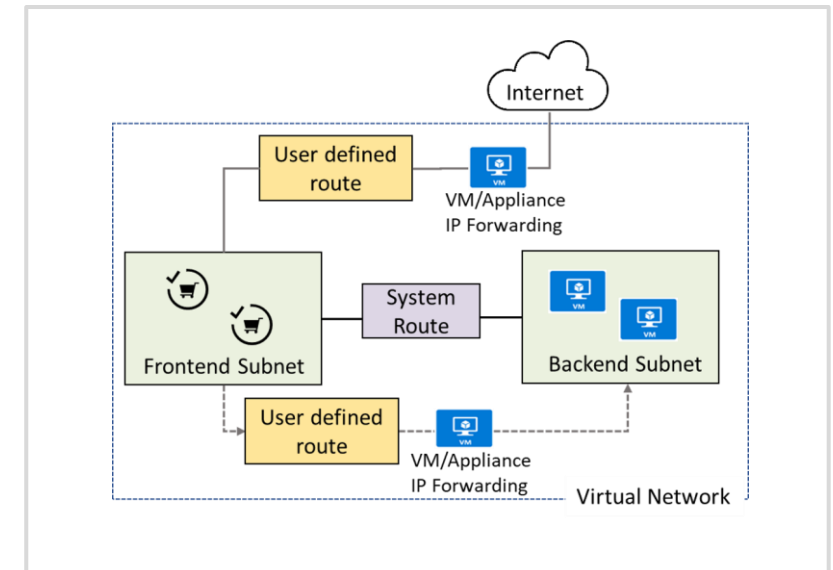
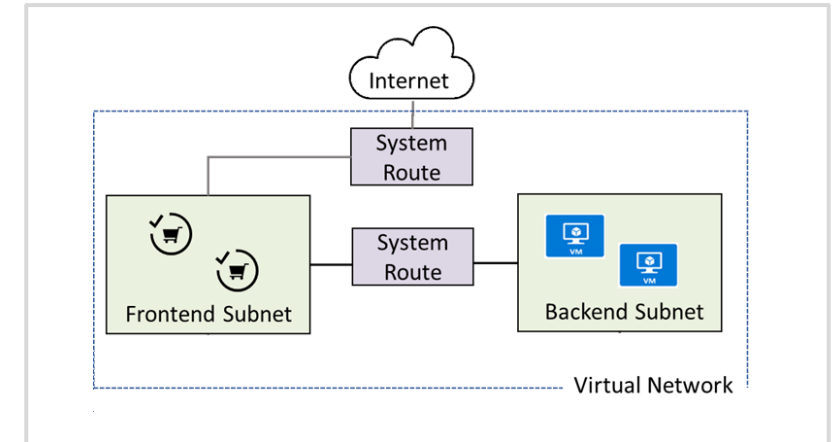


# Design Routing

- 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 on-premises connectivity to Azure virtual networks



# VPN connection

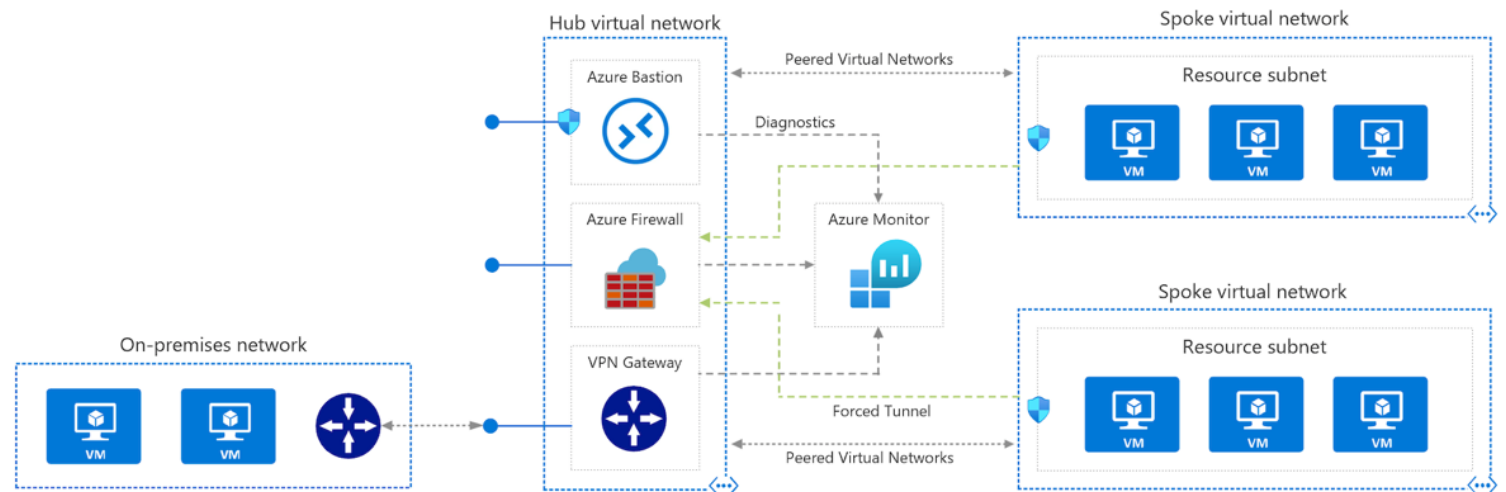
A VPN gateway is a type of virtual network gateway that sends encrypted traffic between an Azure virtual network and an on-premises location.

## 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

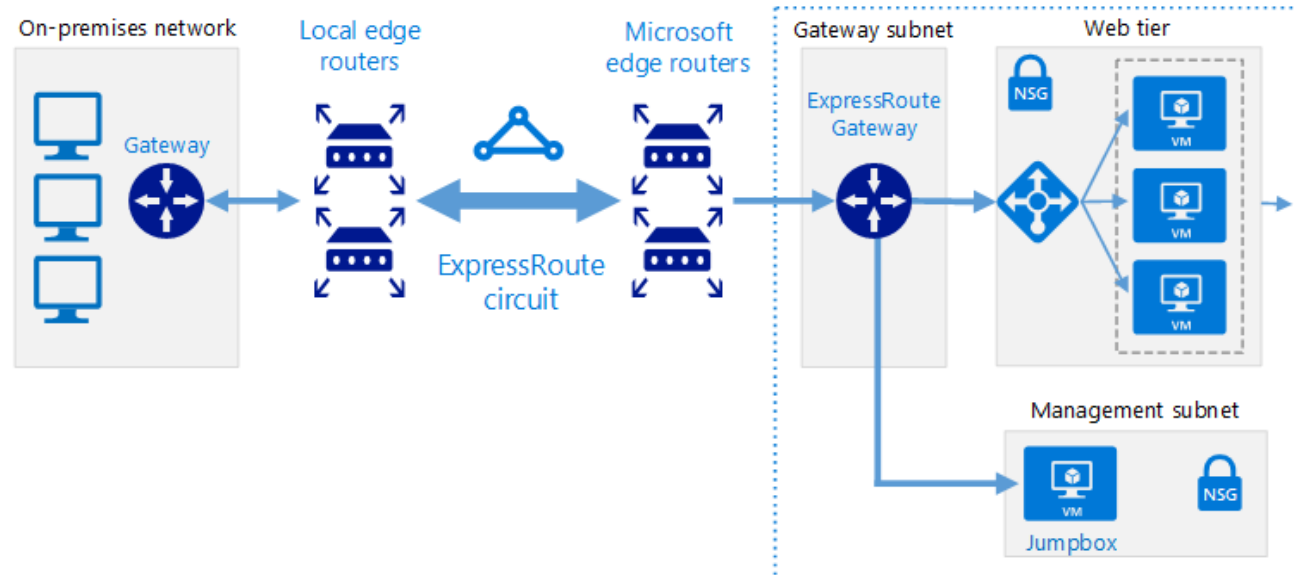
ExpressRoute connections use a private, dedicated connection through a third-party connectivity provider. This connection is private.

## 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

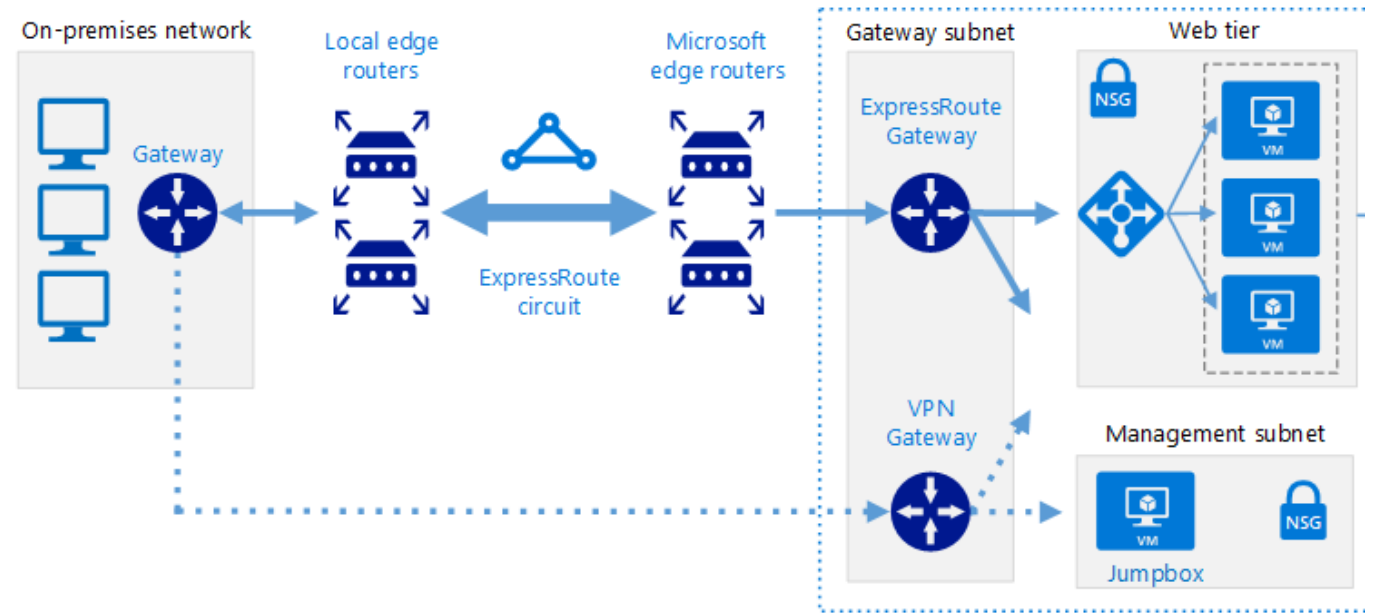
This options combines the previous two, using ExpressRoute in normal conditions, but failing over to a VPN connection if there is a loss of connectivity in the ExpressRoute circuit.

## 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.

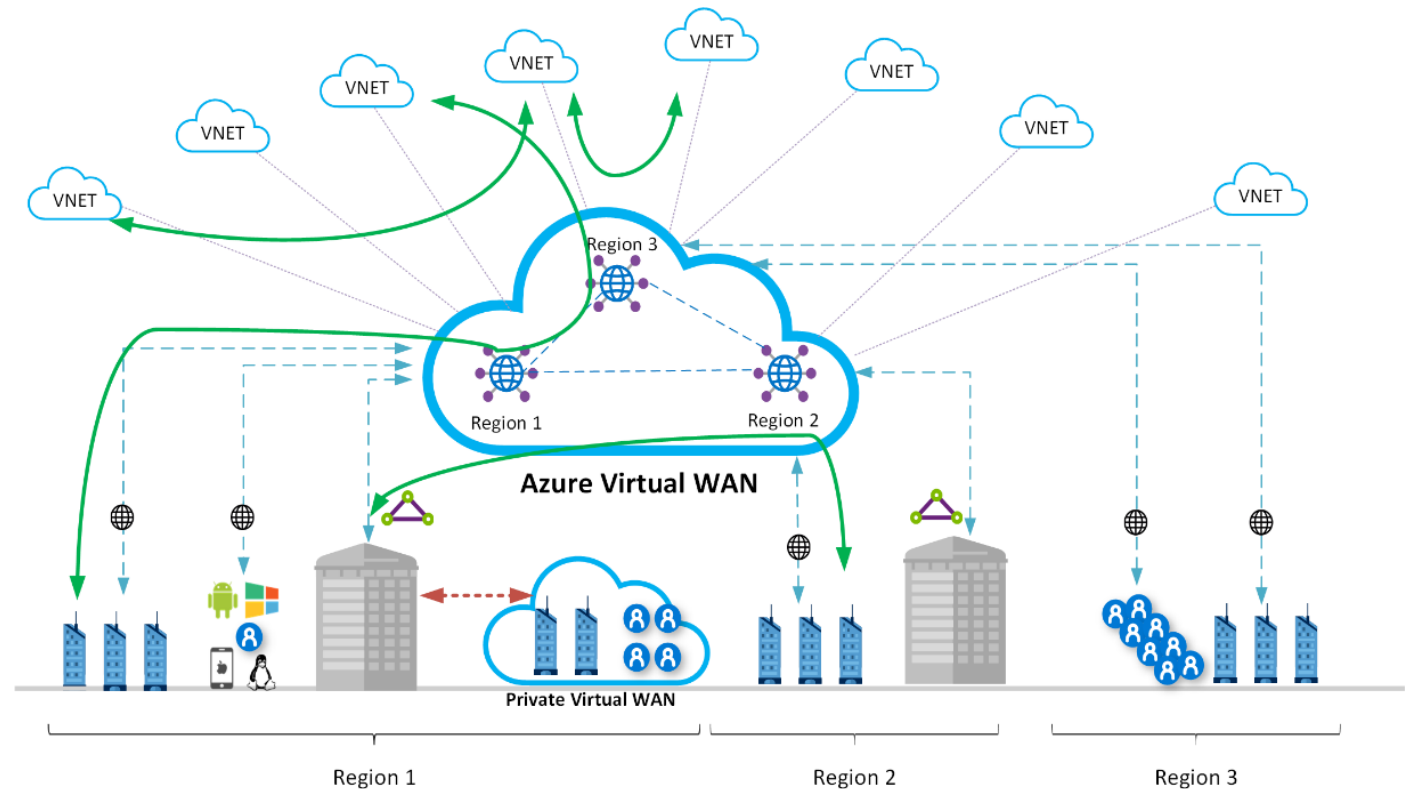




# Azure Virtual WAN

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).

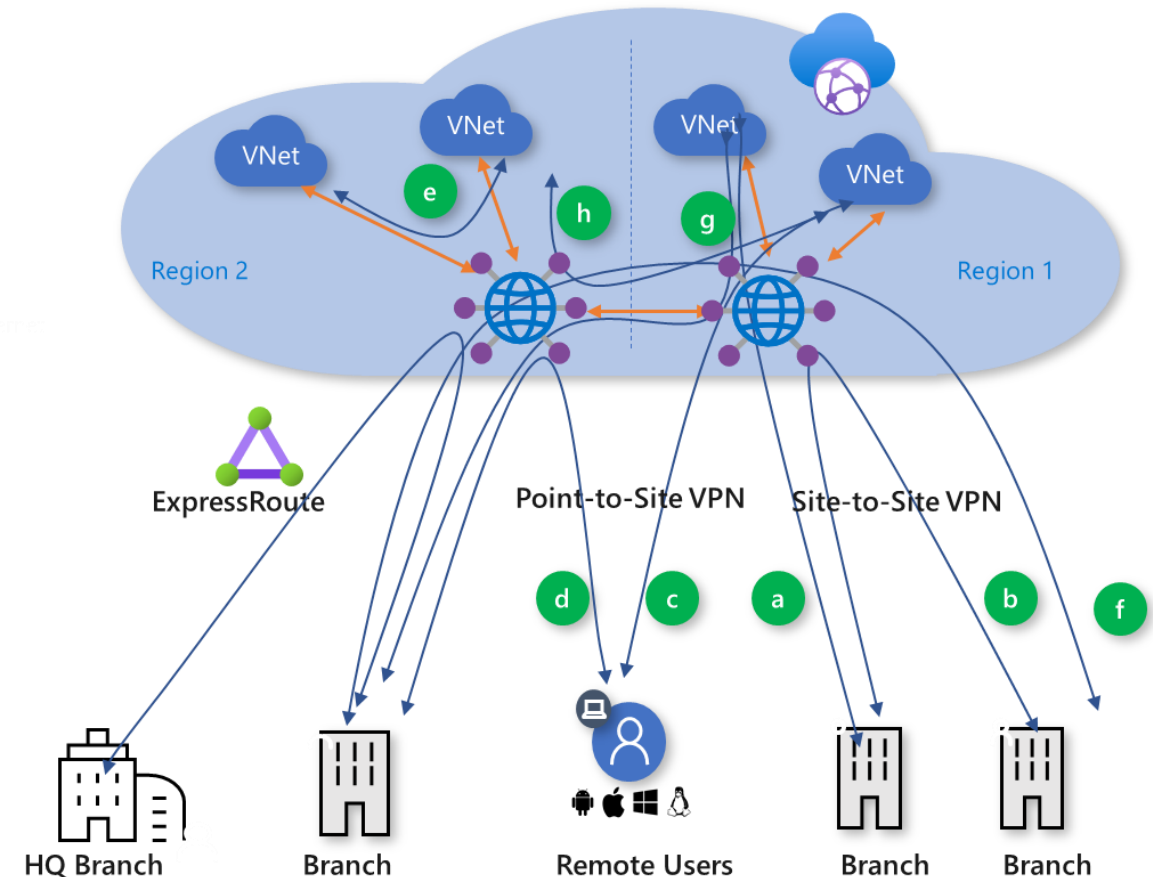


# Global transit network with Virtual WAN

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)



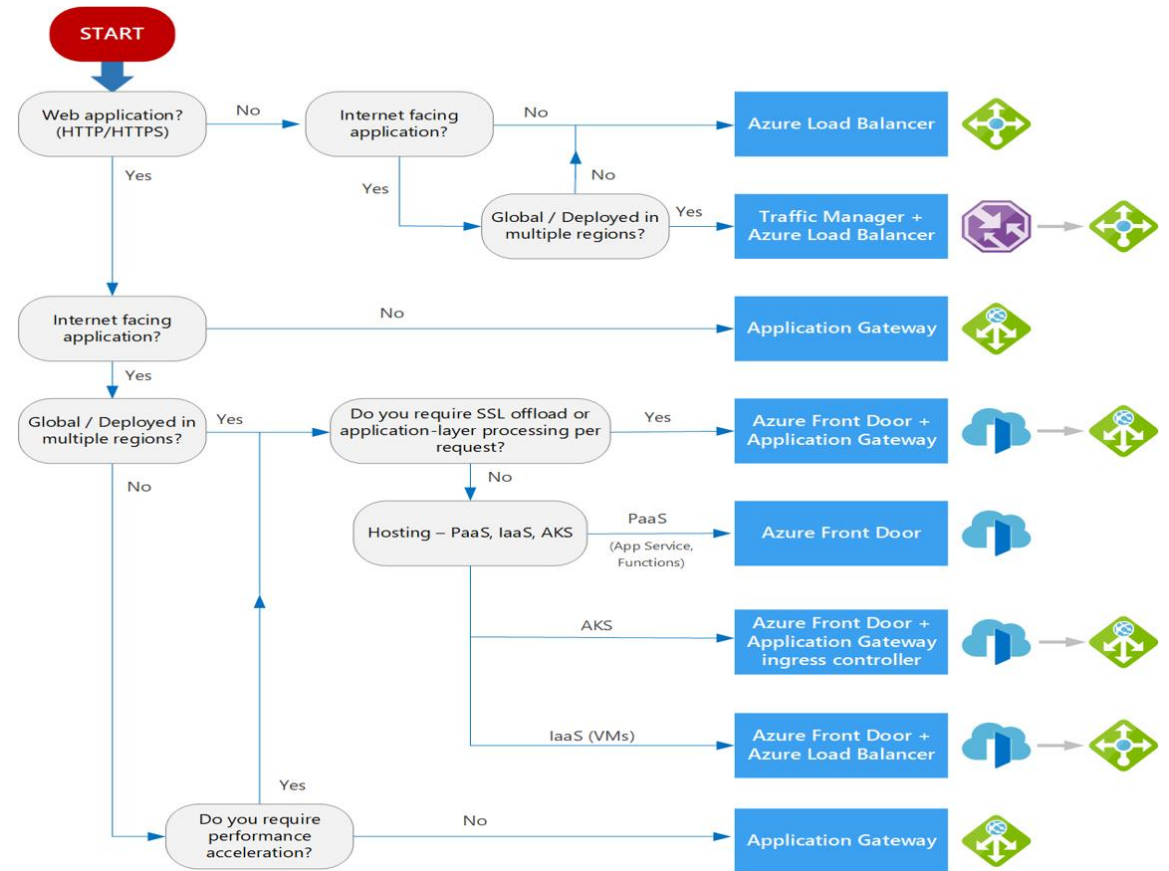
# Design for application delivery services



# Choosing a load balancer solution

Load balancing services to distribute your workloads across multiple computing resources – Azure Front Door, Traffic Manager, Load Balancer, and Application Gateway.

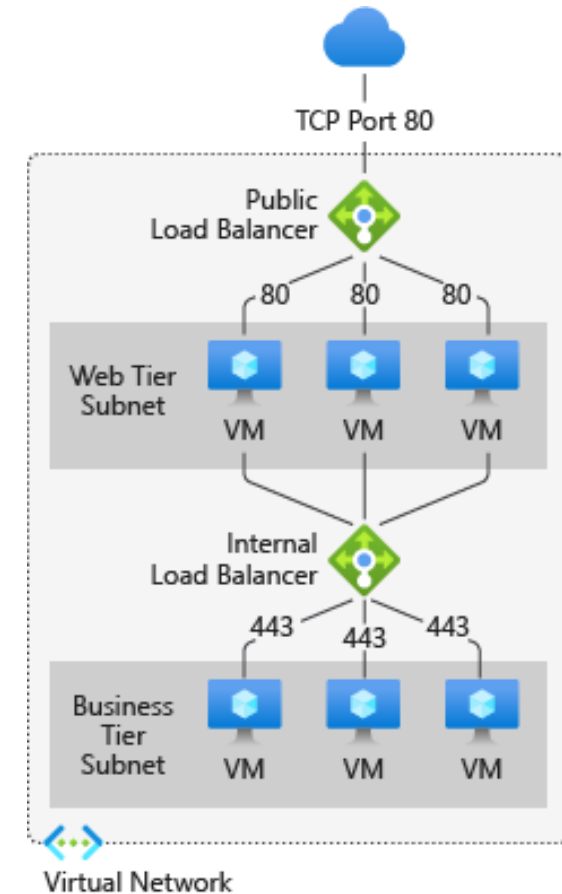
- Traffic type
- Global versus regional
- Availability
- Cost
- Features and limits
- Treat this flowchart as a starting point



# 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

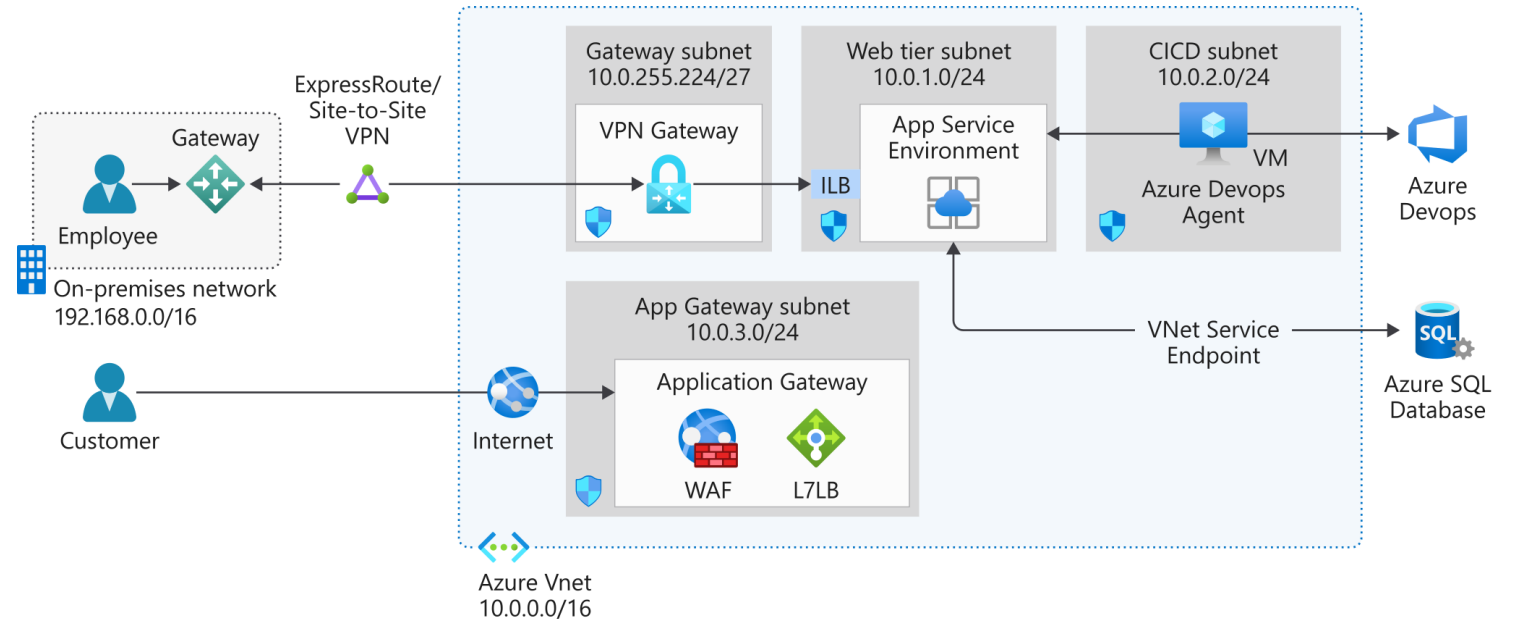


# Application Gateway

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 IaaS
- Regional service



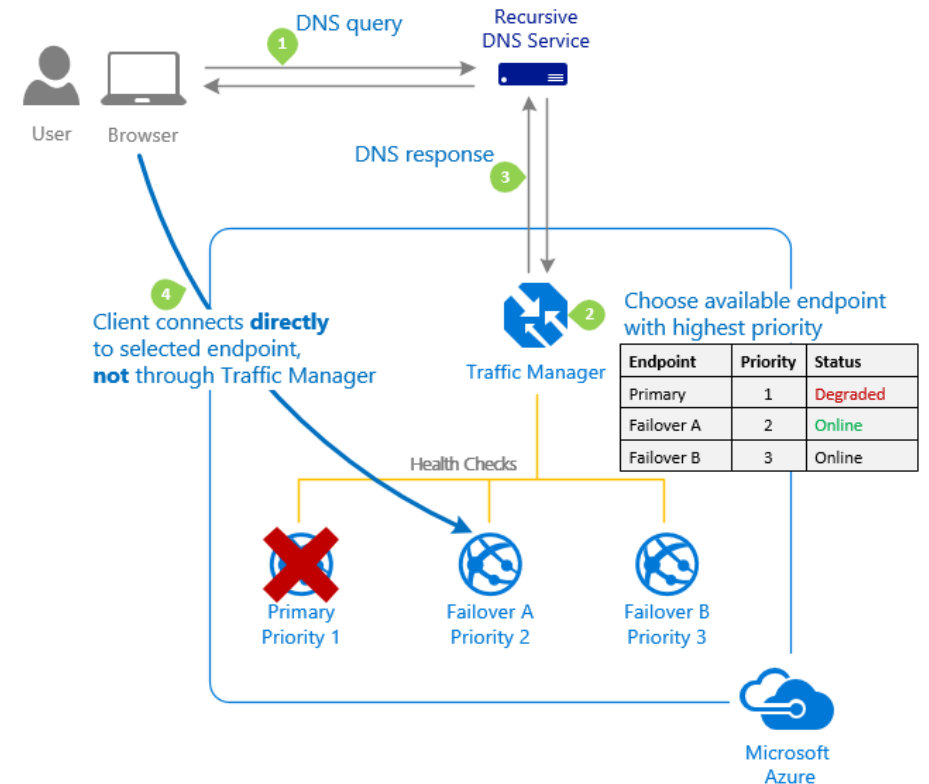


# Traffic Manager

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

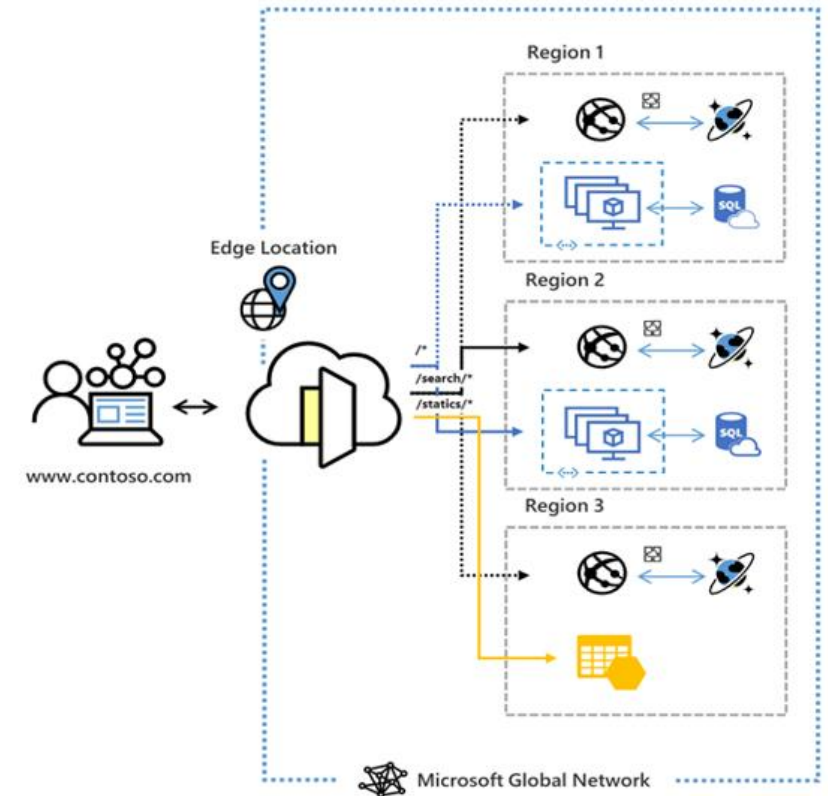


# Azure Front Door Service

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

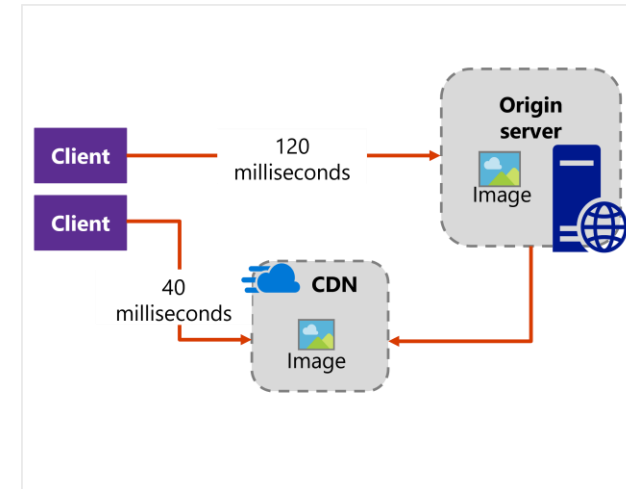


# Content Delivery Network (CDN)

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.



# Design for application protection services



# 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.



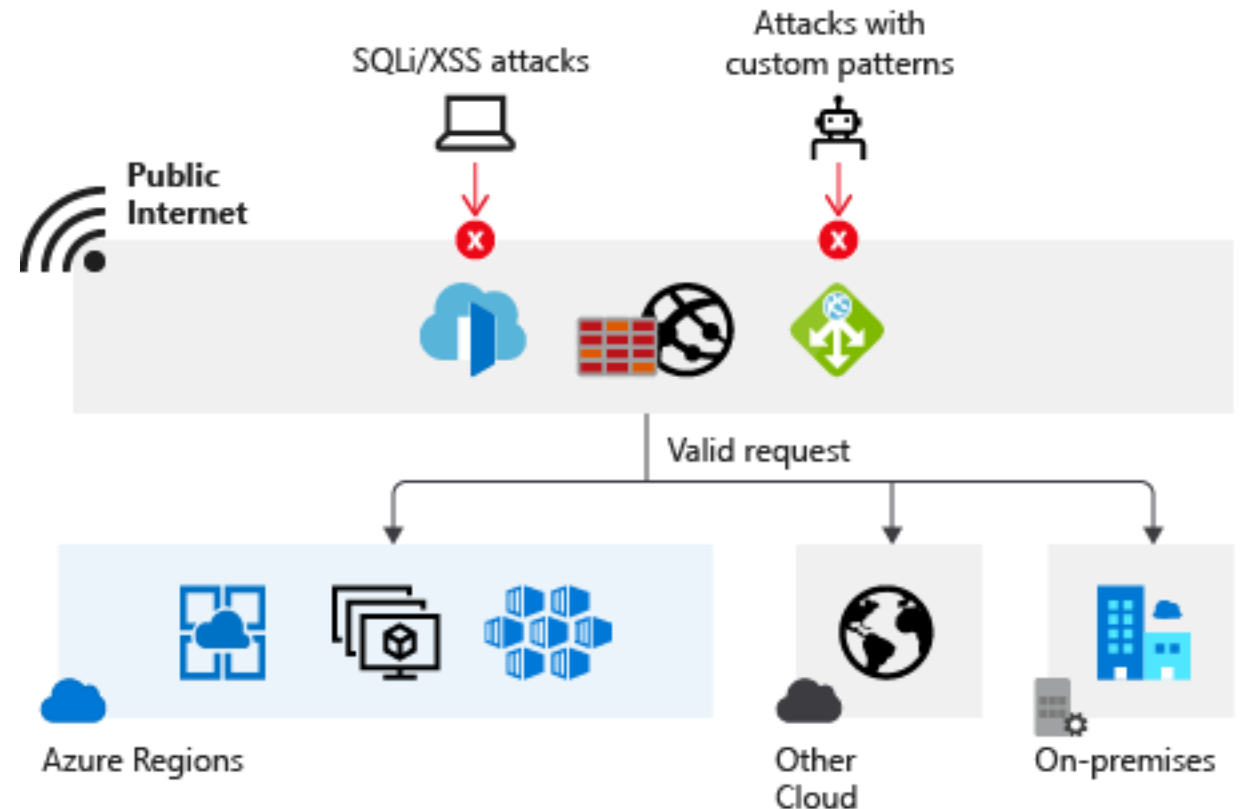
NSGs contain two sets of rules: inbound and outbound. The priority for a rule must be unique within each set.

# 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)



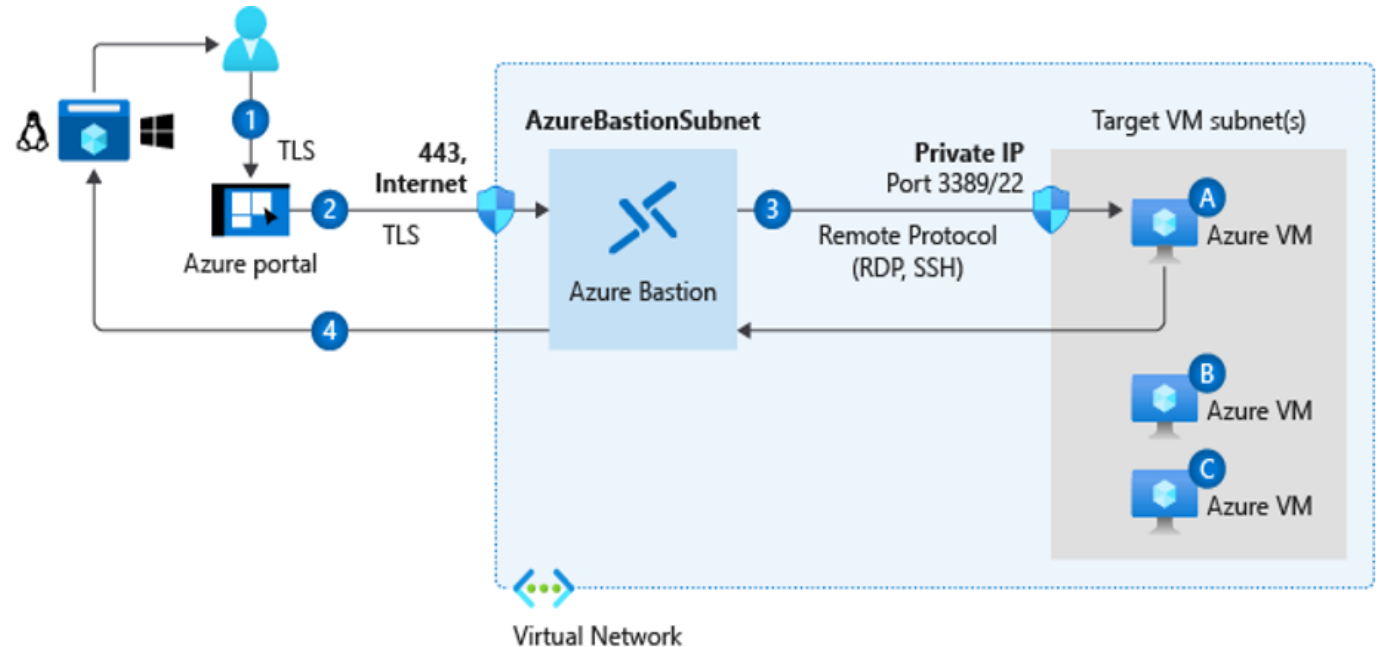


# Azure Bastion

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 need to:

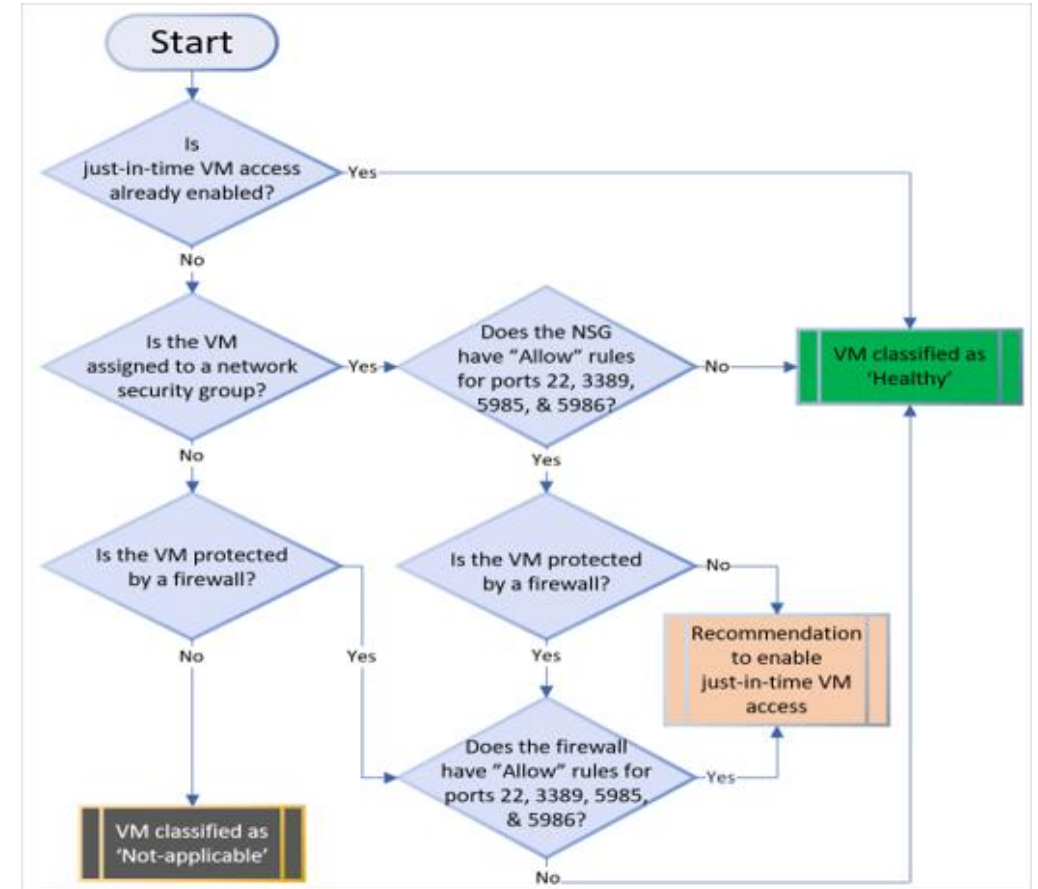
- Secure remote connections from the Azure portal to Azure VMs
- Eliminate exposing RDP and SSH public IP addresses of your Azure VMs
- Access VMs across multiple, peered networks



# Just in Time (JIT) Network Access

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.

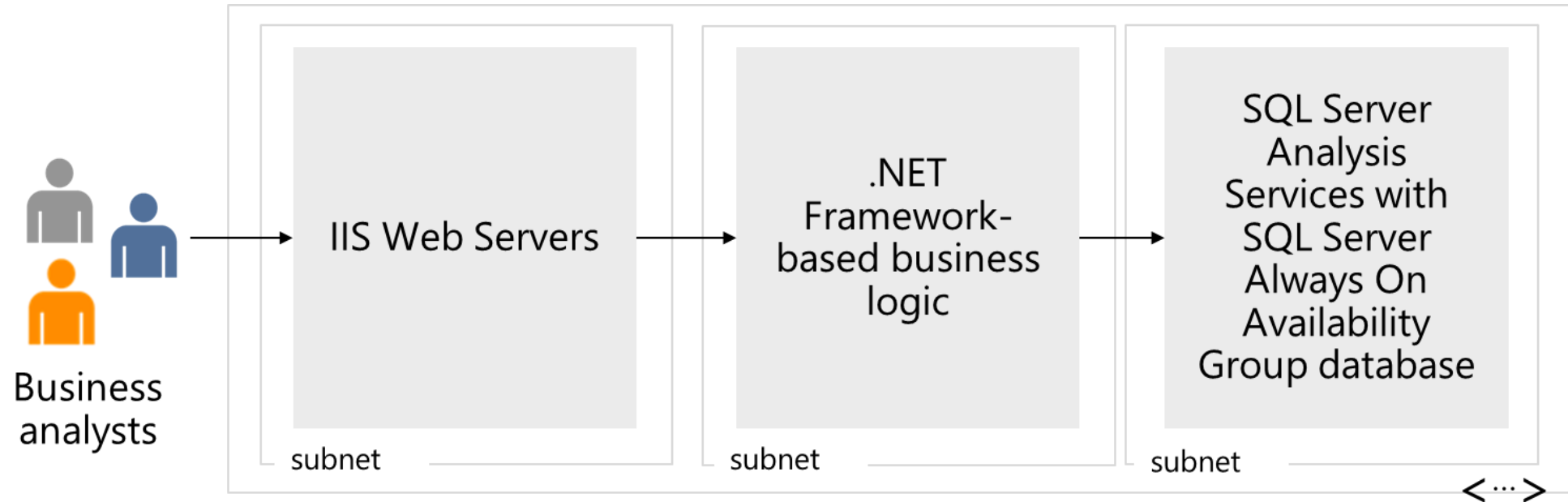
- Supports ports other than 3389 and 22
- Ports are blocked when not in use
- Integrates with NSGs and Azure Firewall



# Case study and review



# Case Study – BI enterprise application

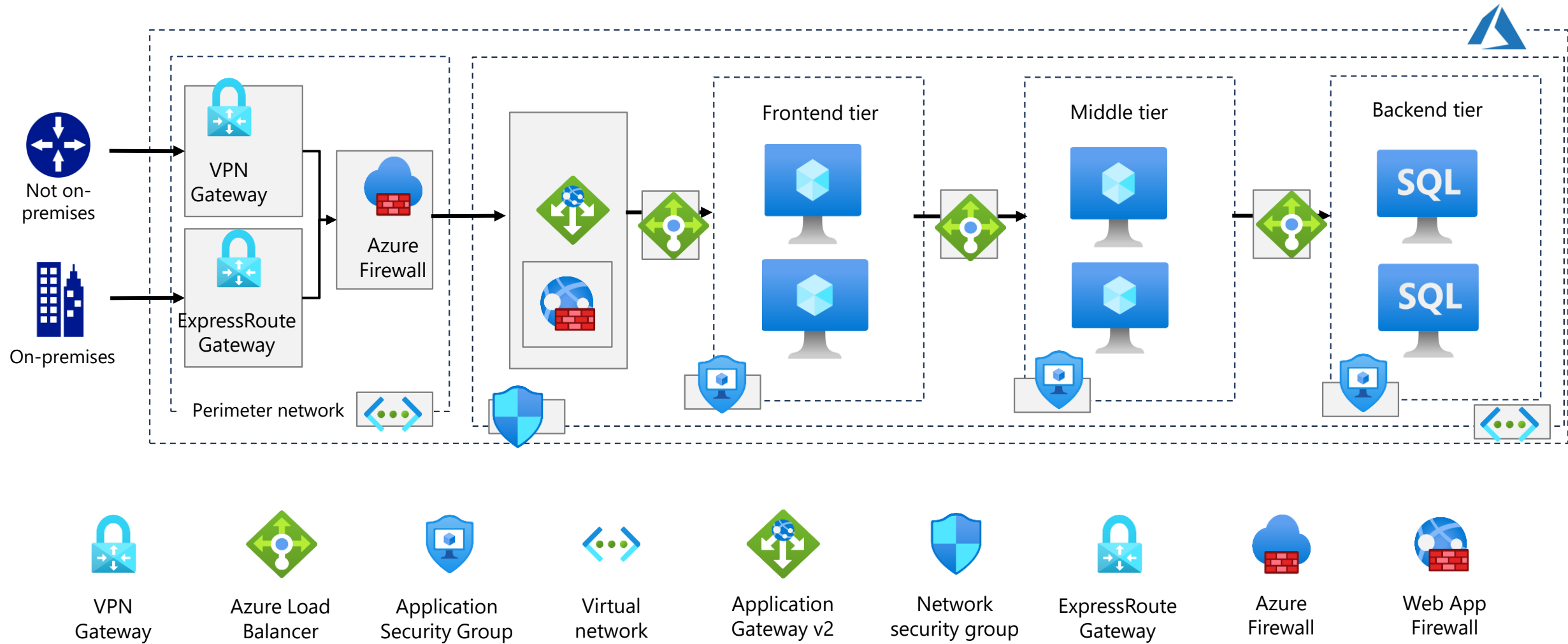


- Heavy demand.
- Servers reach their performance limits during the day.
- Servers sit idle during off hours.

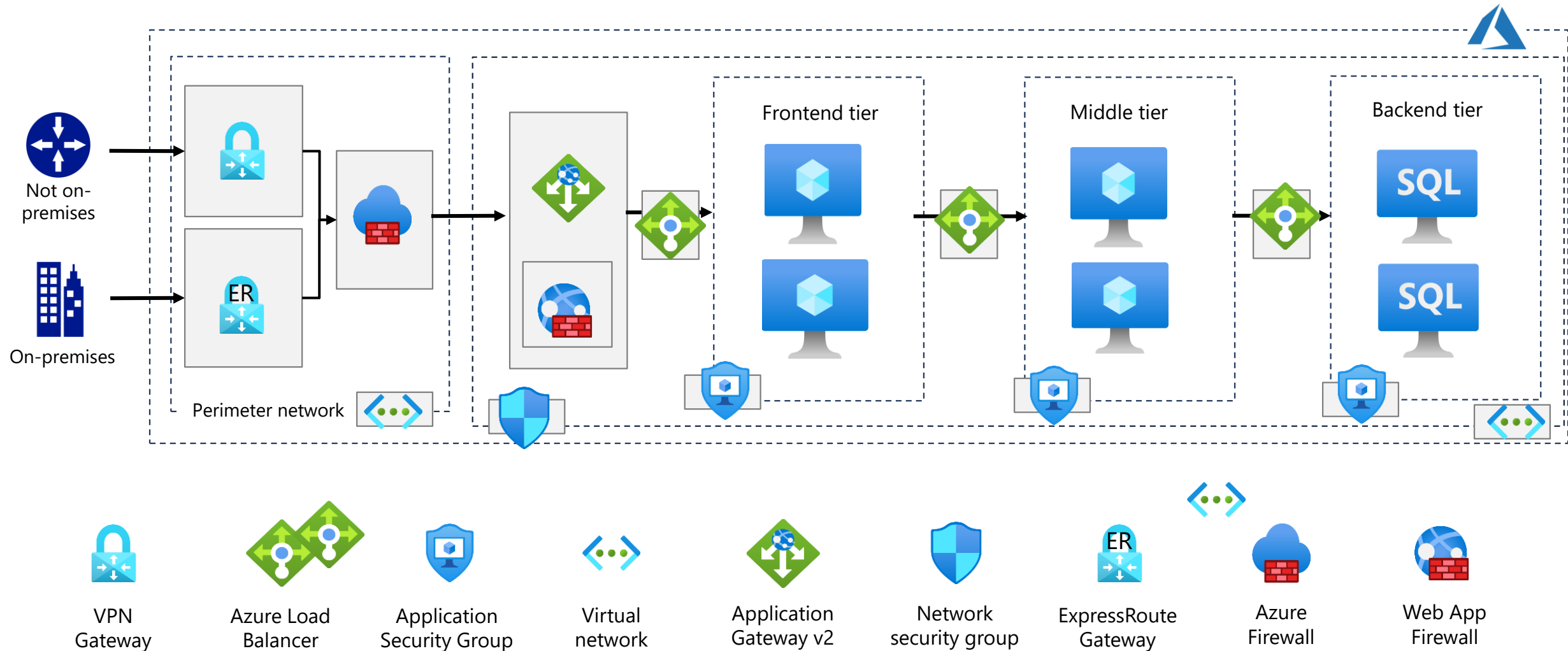
- Rest API call from the front-end tier
- Request demand changes from day to day

- Uses all-flash enterprise SAN storage

# Instructor solution - BI enterprise application

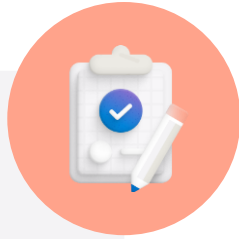


# Completed instructor solution - BI enterprise application





# Learning recap – Network infrastructure solutions



Check your  
knowledge  
questions and  
review

- [AZ-700 Designing and Implementing Microsoft Azure Networking Solutions - Learn | Microsoft Docs](#)
- [Architect network infrastructure in Azure - Learn | Microsoft Docs](#)

Optional exercises:

- [Distribute your services across Azure virtual networks](#)
- [Secure and isolate access using network security groups](#)

# Instructor resources (hidden)



# End of presentation

