

AZ-305T00A

Designing Microsoft
Azure Infrastructure
Solutions

Design a network infrastructure solution

<https://learn.microsoft.com/training/modules/design-network-solutions/>

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

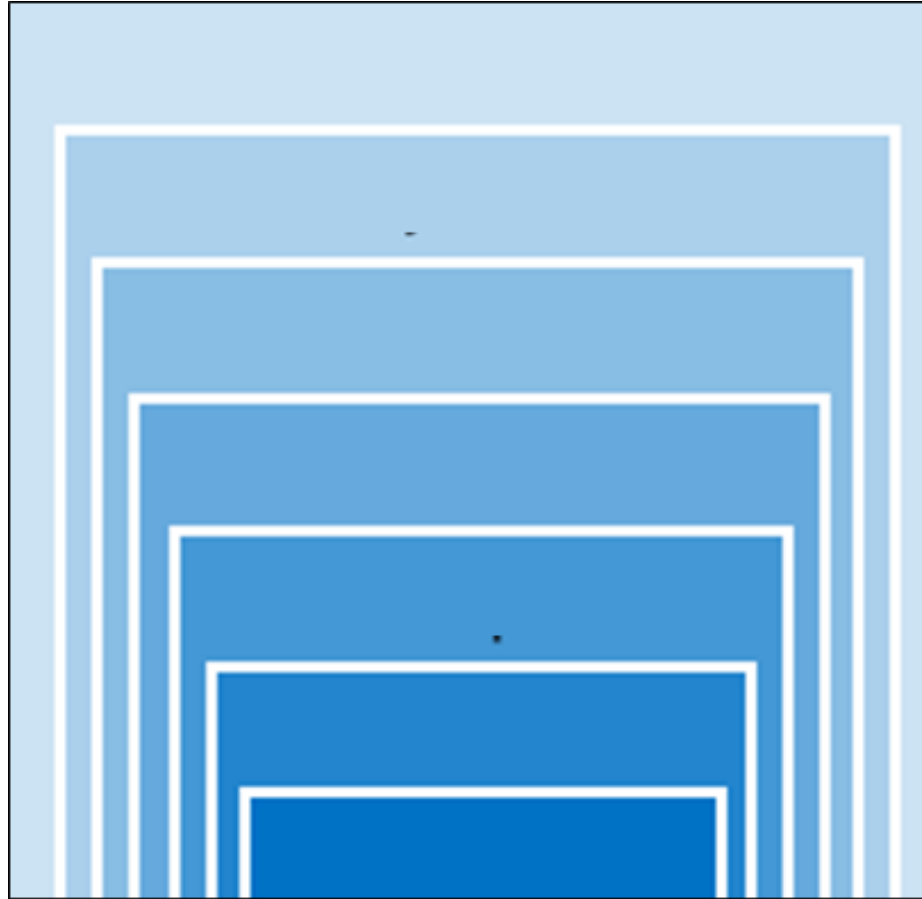
Identity & Access













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



Things to know about network requirements

As you plan your networking solution, there are several requirements you need to consider.


- **Naming:** Define a naming convention that you can use consistently when naming resources to make it easier to manage several network resources over time.
- **Regions:** Determine the Azure regions for your resources according to the physical locations of the consumers of your resources. A virtual network is scoped to a single region/location. However, multiple virtual networks from different regions can be connected together by using Virtual Network peering.
- **Subscriptions:** Plan out how many Azure subscriptions are required to meet your workload requirements, considering you can implement multiple virtual networks within each Azure subscription and Azure region.
- **IP addresses:** Specify a custom private IP address space by using public and private (RFC 1918) addresses. Azure assigns resources in a virtual network a private IP address from the address space that you assign.
- **Segmentation:** Segment your virtual networks with subnets based on workload and security requirements.
- **Filtering:** Define your network security and traffic filtering strategy for your workloads.



Things to consider when defining workload requirements

There are many considerations to review as you plan your network according to the workload requirements for Tailwind Traders.

- **Consider segmentation options for your virtual networks.** Each subnet must have a unique address range, specified in CIDR format, within the address space of the virtual network. The address range can't overlap with other subnets in the virtual network.
 - **Subnets segmented based on application layer.** The following table shows how to segment a virtual network with an address space of 10.245.16.0/20 into subnets based on a three-tiered application.

 Expand table

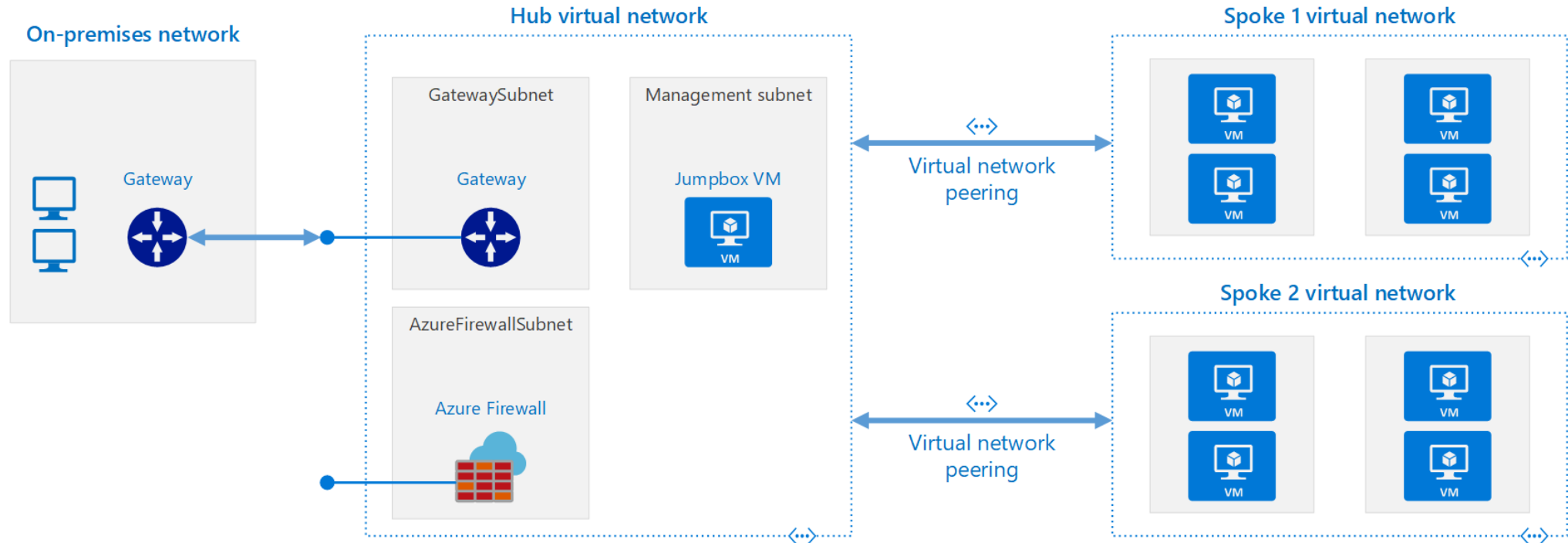
Subnet	CIDR	Addresses	Usage
DEV-FE-EUS2	10.245.16.0/22	1019	Front-end or web-tier virtual machines
DEV-APP-EUS2	10.245.20.0/22	1019	Application-tier virtual machines
DEV-DB-EUS2	10.245.24.0/23	507	Database virtual machines

- **Consider required interfaces and IP addresses.** Identify how many network interfaces and private IP addresses you require in your virtual network. There are limits to the number of network interfaces and private IP addresses that you can have within a virtual network.
- **Consider network security groups.** You can filter network traffic to and from resources in a virtual network by using network security groups and network virtual appliances. You can control how Azure routes traffic from subnets.
- **Consider network traffic routing.** Azure routes network traffic between all subnets in a virtual network, by default. You can override some of Azure's system routes with custom routes.

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.



Three common networking patterns for organizing workloads in Azure:

- Single virtual network
- Multiple virtual networks with peering
- Multiple virtual networks in a hub-spoke topology

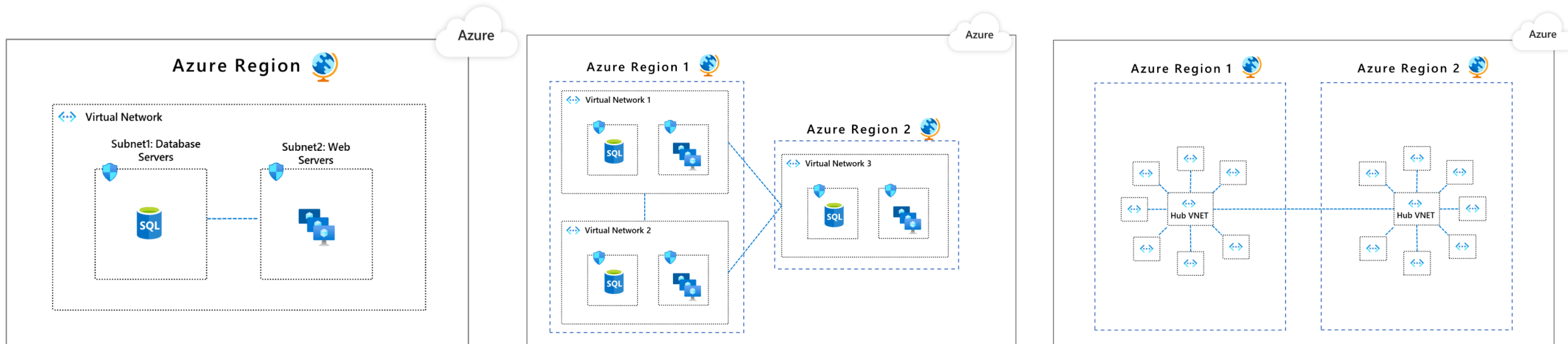
Design network topology

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



The following table compares capabilities of the three networking patterns. Review the details, and think about which patterns are applicable to the network topology for Tailwind Traders.

 Expand table

Compare	Single virtual network	Multiple networks with peering	Multiple networks in hub-spoke topology
Connectivity/Routing (how segments communicate)	System routing provides default connectivity to any workload in any subnet.	System routing provides default connectivity to any workload in any subnet.	No default connectivity between spoke virtual networks. A layer 3 router (such as Azure Firewall) in the hub virtual network is required to enable connectivity.
Network-level traffic filtering	Traffic is allowed by default. NSG can be used for filtering.	Traffic is allowed by default. NSG can be used for filtering.	Traffic between spoke virtual networks is denied by default. Azure Firewall configuration can enable selected traffic, such as <code>windowsupdate.com</code> .
Centralized logging	NSG logs for the virtual network.	Aggregate NSG logs across all virtual networks.	Azure Firewall logs to Azure Monitor all accepted/denied traffic sent via a hub.
Unintended open public endpoints	DevOps can accidentally open a public endpoint via incorrect NSG rules.	DevOps can accidentally open a public endpoint via incorrect NSG rules.	An accidentally opened public endpoint in a spoke virtual network won't enable access. The return packet is dropped via stateful firewall (asymmetric routing).
Application level protection	NSG provides network layer support only.	NSG provides network layer support only.	Azure Firewall supports FQDN filtering for HTTP/S and MSSQL for outbound traffic and across virtual networks.

Design Outbound Connectivity

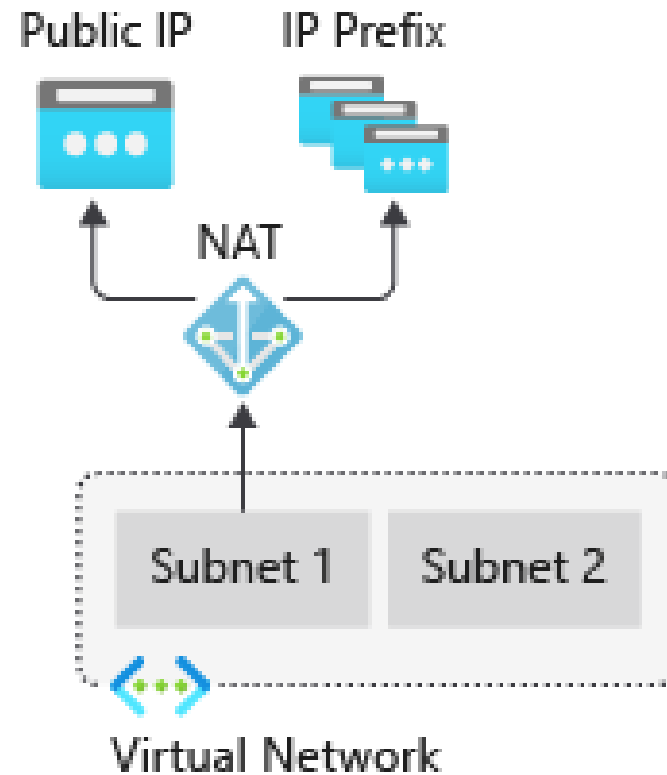
Virtual Network NAT (network address translation) simplifies outbound-only Internet connectivity for virtual networks. When configured on a subnet, all outbound connectivity uses your specified static public IP addresses. NAT is fully managed and highly resilient.

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

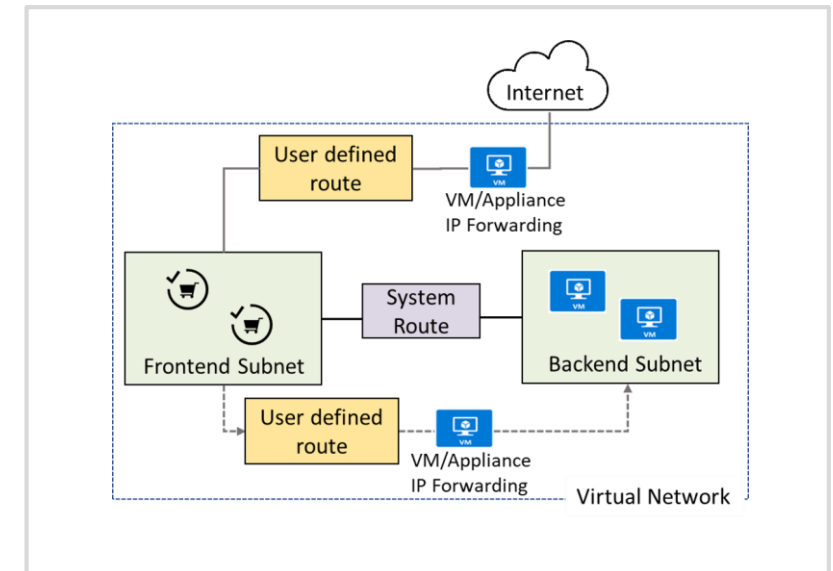
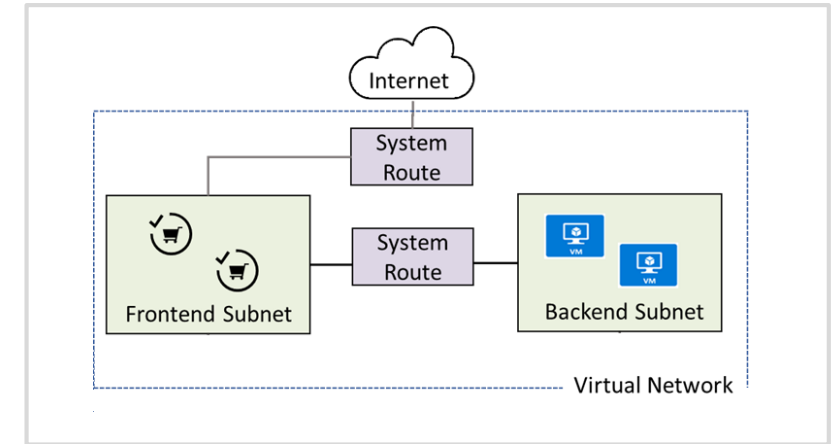


Design Routing

- 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



Things to know about routing tables and routes

Let's take a closer look at the characteristics of routing tables and the route types.

- **System routes:** When you create a virtual network for the first time without defining any subnets, Azure creates system route entries in the routing table. System routes are defined for a specific location when they're created. System routes can't be modified after they're created, but you can override these routes by configuring UDRs.
- **User-defined routes (custom):** When you create one or multiple subnets inside a virtual network, Azure creates default entries in the routing table to enable communication between these subnets within a virtual network. These routes can be modified by using static routes, which are stored as UDRs in Azure. UDRs are also called *custom routes*. You create UDRs in Azure to override Azure's default system routes, or to add more routes to a subnet's route table.
- **Routes from other virtual networks:** When you create a virtual network peering between two virtual networks, a route is added for each address range within the address space of each peered virtual network.
- **Border Gateway Protocol routes:** If your on-premises network gateway exchanges BGP routes with an Azure Virtual Network gateway, a route is added for each route propagated from the on-premises network gateway. These routes appear in the routing table as BGP routes.
- **Service endpoint routes:** The public IP addresses for certain services are added to the route table by Azure when you enable a service endpoint to the service. Service endpoints are enabled for individual subnets within a virtual network. When you enable a service endpoint, a route is only added to the route table for the subnet that belongs to this service. Azure manages the addresses in the route table automatically when the addresses change.
- **Routing order:** When you have competing entries in a routing table, Azure selects the next hop based on the longest prefix match similar to traditional routers. If there are multiple next hop entries with the same address prefix, Azure selects routes in a specific order: UDRs, then BGP routes, and then system routes.



Things to consider when using routing tables and routes

There are many networking scenarios where defining and overriding routes can be an advantage. Review the following suggestions and consider the routes required to support the Tailwind Traders solution.

- **Consider system routes.** Define system routes for specific locations and scenarios that you don't expect to modify.
 - Route traffic between virtual machines in the same virtual network or between peered virtual networks
 - Support communication between virtual machines by using a virtual network-to-network VPN
 - Enable site-to-site communication through Azure ExpressRoute or an Azure VPN gateway
- **Consider user defined routes.** Create custom UDRs to override Azure's default system routes, or to add more routes to a subnet's route table.
 - Enable filtering of internet traffic by using Azure Firewall or forced tunneling
 - Flow traffic between subnets through an NVA
 - Define routes to specify how packets should be routed in a virtual network
 - Define routes that control network traffic and specify the next hop in the traffic flow
- **Consider overriding routes.** Plan for route overrides to control traffic flow.
 - Flow through NVA: [Configure route tables to force traffic between subnets to flow through an NVA](#)
 - Forced tunneling: [Force all internet-bound traffic through an NVA, or on-premises, through an Azure VPN gateway](#)

Design for on-premises
connectivity to Azure virtual
networks

VPN connection

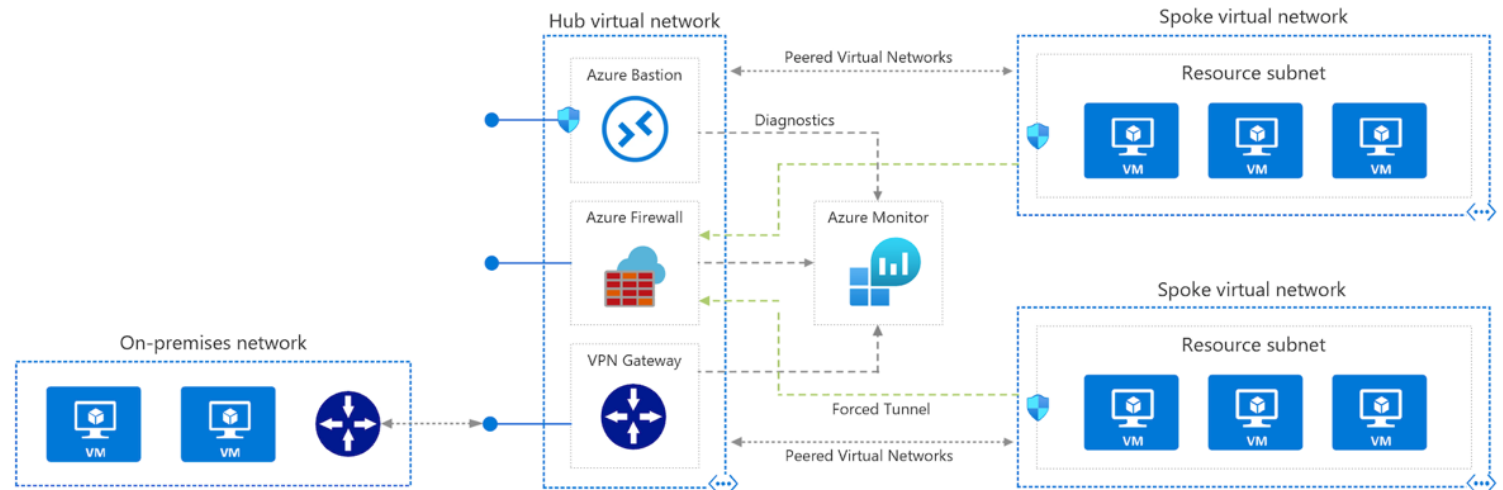
A VPN gateway is a type of virtual network gateway that sends encrypted traffic between an Azure virtual network and an on-premises location.

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

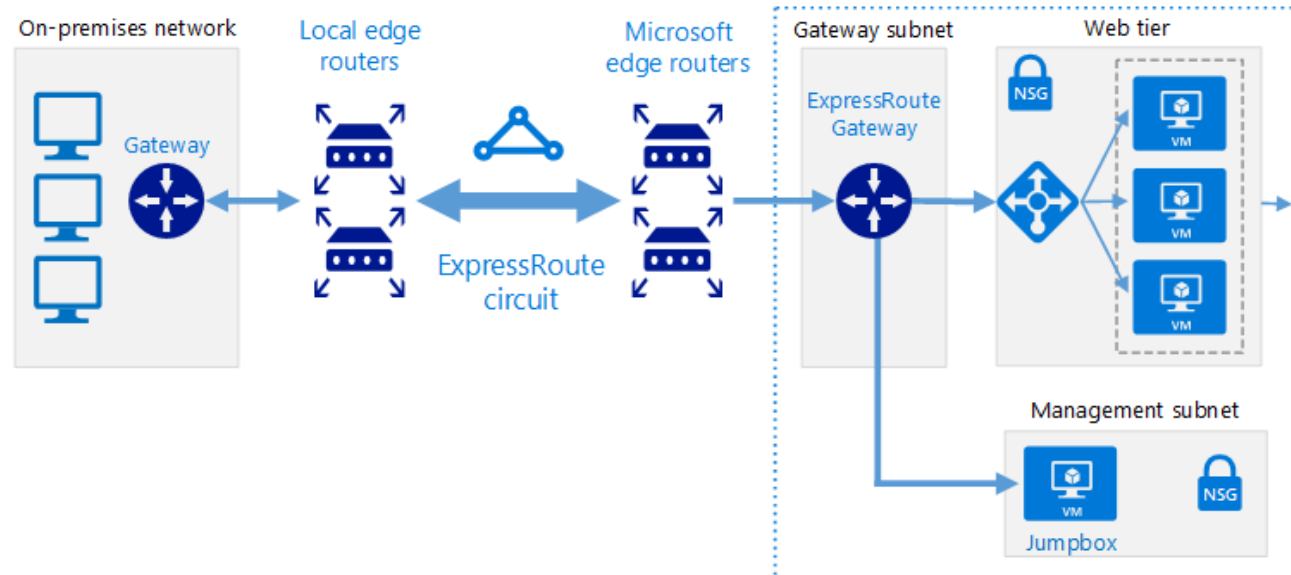
ExpressRoute connections use a private, dedicated connection through a third-party connectivity provider. This connection is private.

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

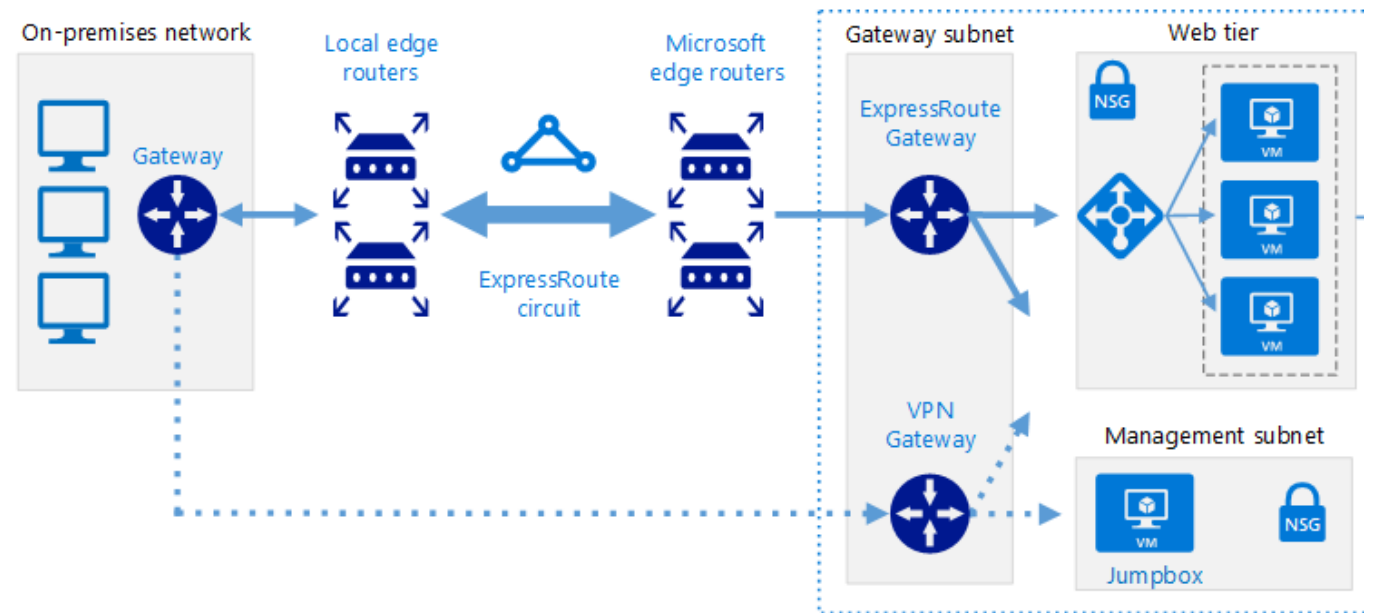
This options combines the previous two, using ExpressRoute in normal conditions, but failing over to a VPN connection if there is a loss of connectivity in the ExpressRoute circuit.

Benefits

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

Challenges

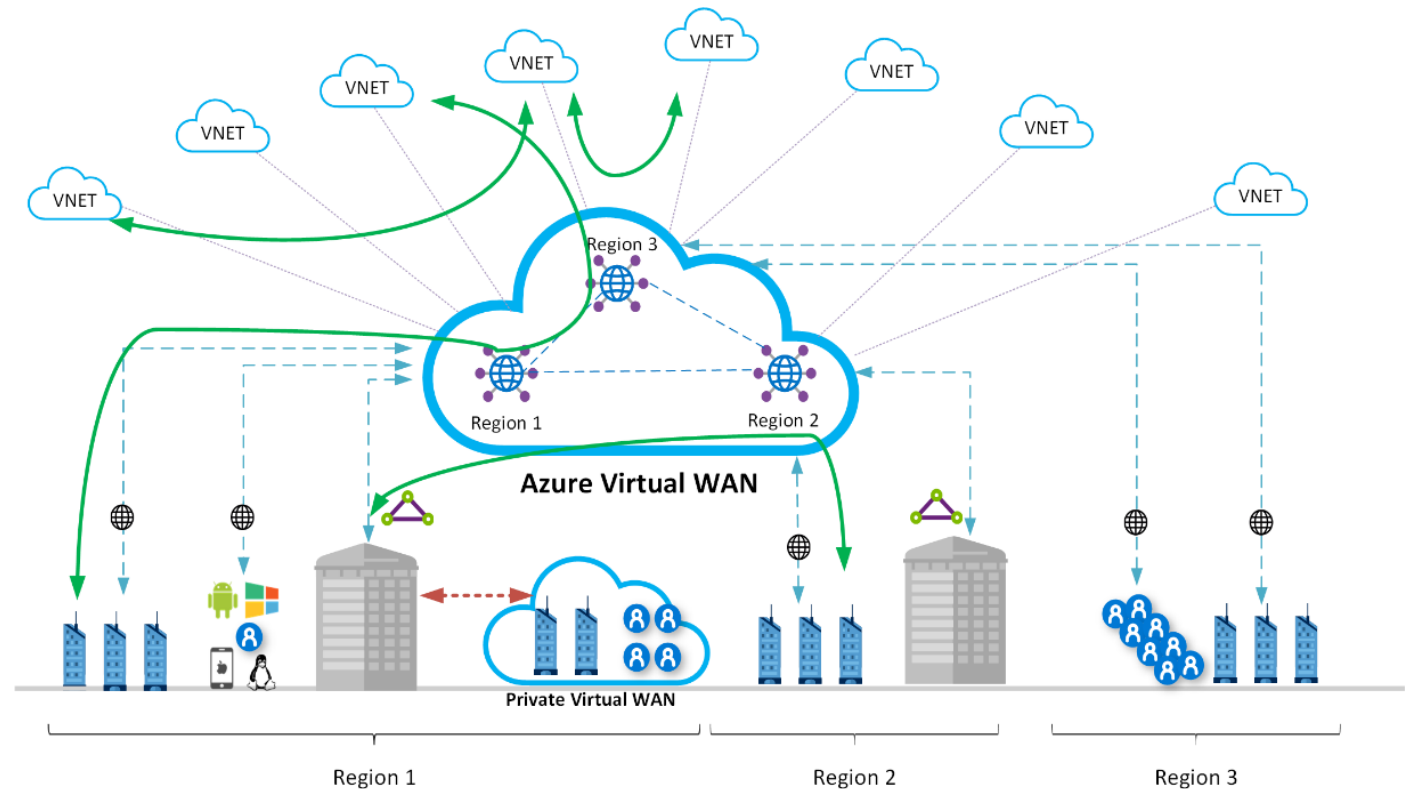
- Complex to configure. You need to set up both a VPN connection and an ExpressRoute circuit.
- Requires redundant hardware (VPN appliances), and a redundant Azure VPN Gateway connection for which you pay charges.



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).

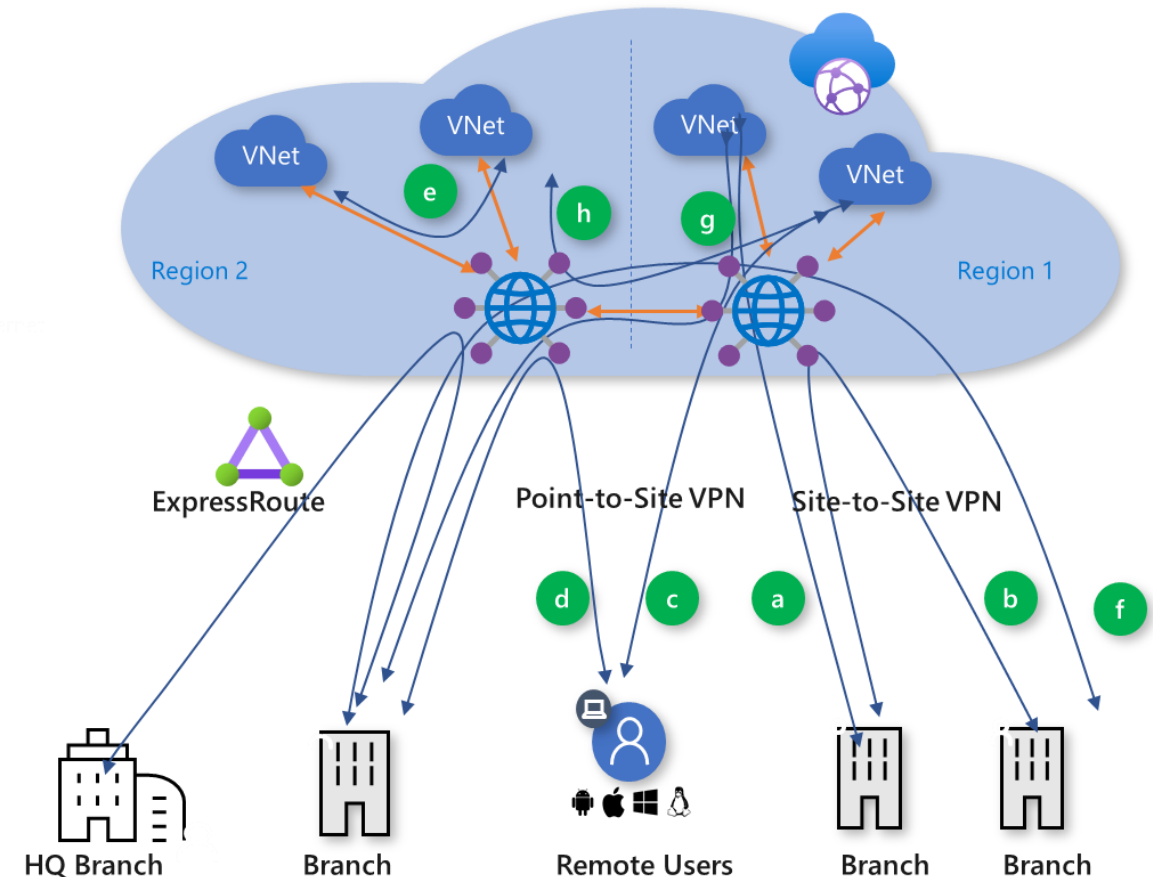


Global transit network with Virtual WAN

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)



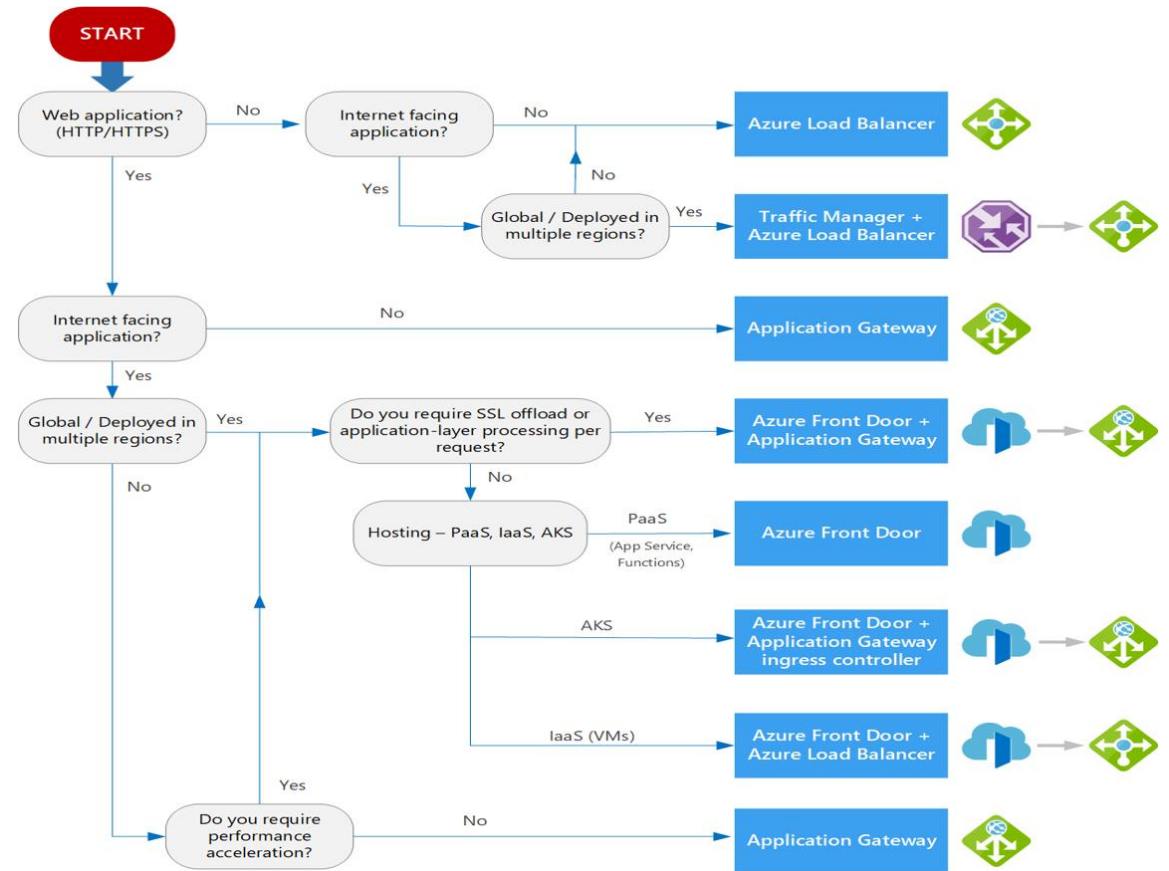
Compare	Azure VPN Gateway	Azure ExpressRoute	ExpressRoute + VPN failover	Azure Virtual WAN + hub-spoke
Benefits	<ul style="list-style-type: none"> - Simple to configure - High bandwidth available (up to 10 Gbps depending on VPN Gateway SKU) 	<ul style="list-style-type: none"> - High bandwidth available (up to 10 Gbps depending on connectivity provider) - Supports dynamic scaling of bandwidth to help reduce costs during periods of lower demand (not supported by all connectivity providers) - Enables direct organizational access to national clouds (depends on connectivity provider) 	<ul style="list-style-type: none"> - High availability if ExpressRoute circuit fails (fallback connection on lower bandwidth network) 	<ul style="list-style-type: none"> - Reduced operational overhead by replacing existing hubs with fully managed service - Cost savings by using managed service, which removes need for NVA - Improved security via centrally managed secured hubs with Azure Firewall and Virtual WAN - Separates concerns between central IT (SecOps, InfraOps) and workloads (DevOps)
Challenges	<ul style="list-style-type: none"> - Requires on-premises VPN device 	<ul style="list-style-type: none"> - Can be complex to set up - Requires working with third-party connectivity provider - Provider responsible for provisioning network connection - Requires high-bandwidth routers on-premises 	<ul style="list-style-type: none"> - Complex to configure - Must set up both VPN connection and ExpressRoute circuit - Requires redundant hardware (VPN appliances) - Requires redundant Azure VPN Gateway connection for which you pay charges 	<p>Note: Azure Virtual WAN is designed to reduce previously listed connectivity challenges.</p>
Scenarios	<p><i>Hybrid apps with light traffic between on-premises hardware and the cloud</i></p> <p><i>Able to trade slightly extended latency for flexibility and processing power of the cloud</i></p>	<p><i>Hybrid apps running large-scale, mission-critical workloads that require high degree of scalability</i></p>	<p><i>Hybrid apps that require higher bandwidth of ExpressRoute and highly available network connectivity</i></p>	<p><i>Connectivity among workloads requires central control and access to shared services</i></p> <p><i>Enterprise requires central control over security aspects like a firewall and segregated management for workloads in each spoke</i></p>

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



Choose an application delivery service

3 minutes

Azure offers several load-balancing services for distributing your workloads across multiple computing resources. As you review the options, there are several factors to consider in your planning.

Things to know about load balancing

Azure load-balancing services can be categorized along two dimensions:

- Global or Regional
- HTTP(S) or non-HTTP(S)

In the Azure portal, the **Help me choose** default tab highlights other configuration characteristics:

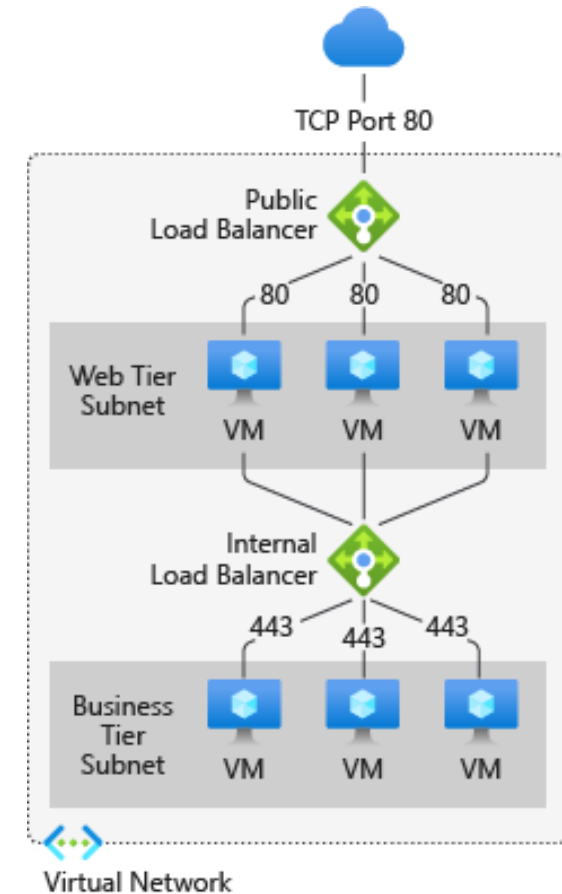
- **Traffic type:** Are you designing a web (HTTP/HTTPS) application? Is the app public facing or is it private?
- **Global versus regional:** Do you need to load balance virtual machines or containers within a virtual network, or load balance scale unit/deployments across regions, or both?
- **Availability:** Does the service [SLA](#) meet your requirements?
- **Cost:** Have you outlined your cost expectations? You can review the [Azure pricing](#) options. In addition to the cost of the service itself, consider the operations cost for managing a solution built on that service.
- **Features and limits:** What are the overall limitations of each service? You can review the [service limits](#).

Load Balancer

What is Azure 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

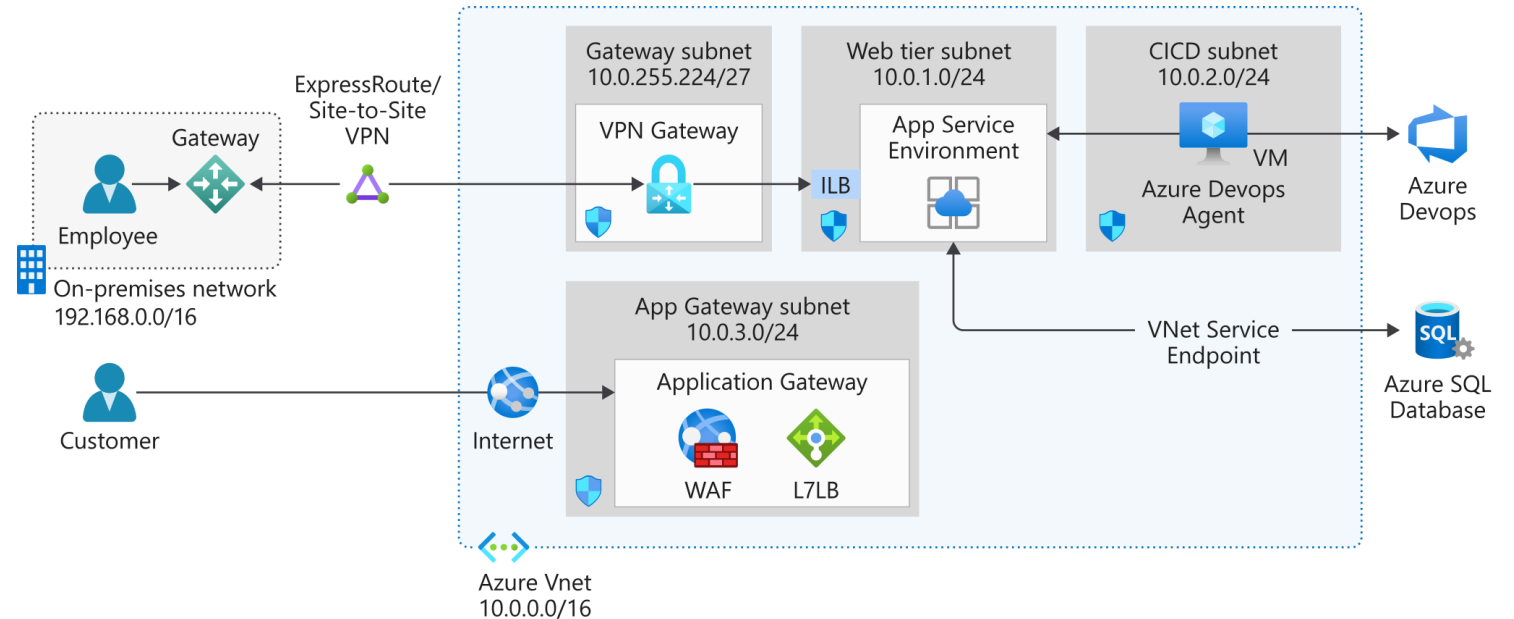


Application Gateway

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



Azure Application Gateway

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications. Application Gateway is an Application Delivery Controller (ADC) as a service, offering various layer 7 load-balancing capabilities for your applications. There are two primary methods of routing traffic: path-based routing and multiple-site routing.

Business scenarios

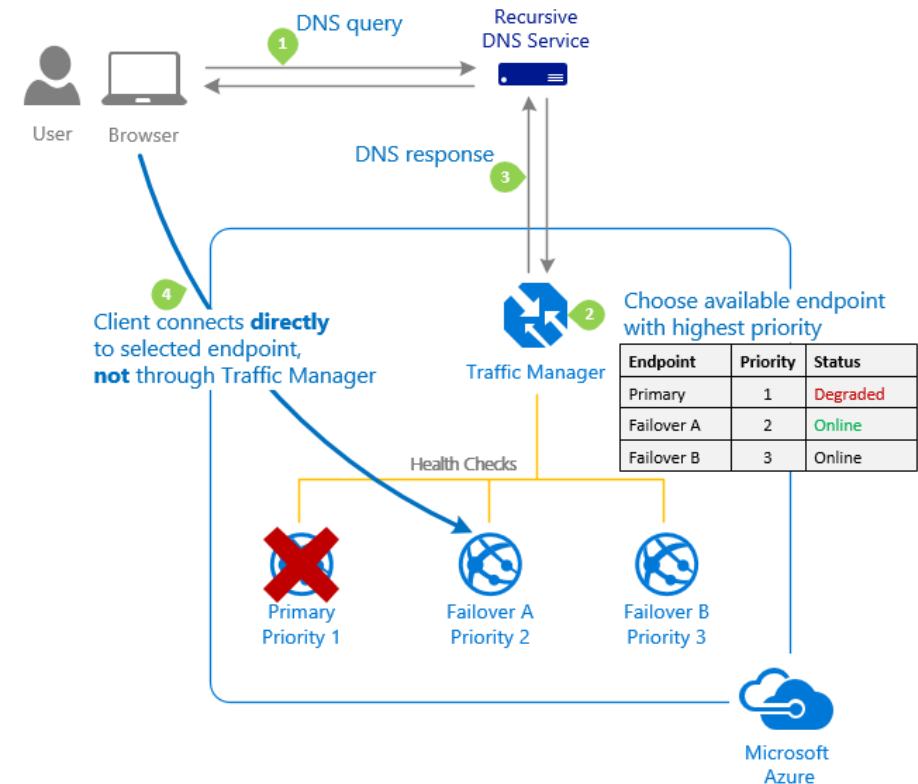
- Path-based routing: Send requests with different URL paths to a different pool of back-end servers
- Multiple-site routing: Support tenants with virtual machines or other resources that host a web application

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 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, while providing high availability and responsiveness. Traffic Manager provides a range of traffic-routing methods to distribute traffic such as priority, weighted, performance, geographic, multi-value, and subnet.

Business scenarios

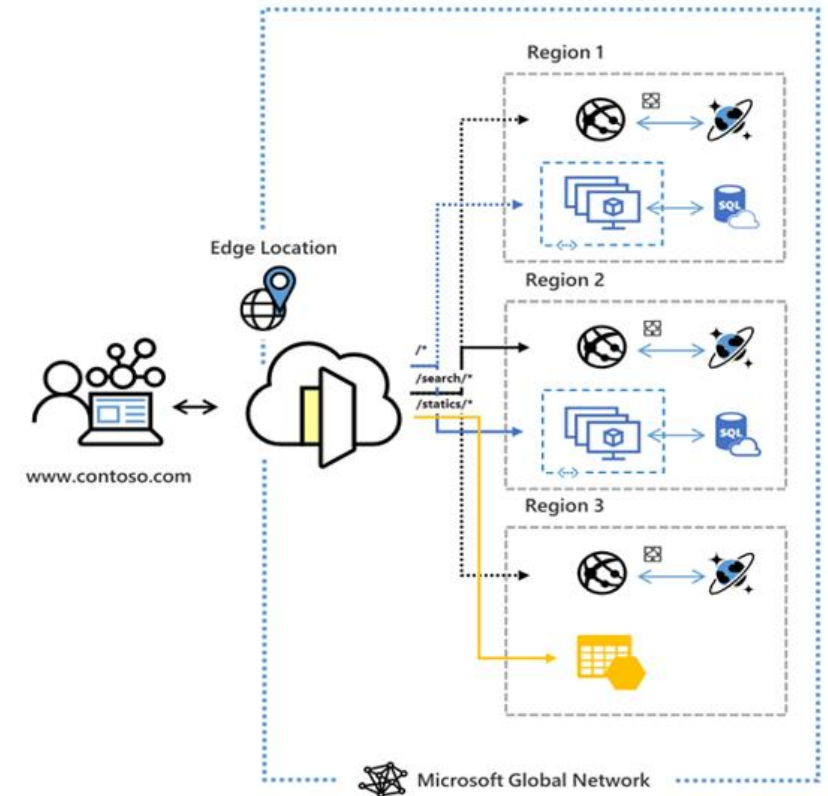
- Increase application availability
- Improve application performance
- Combine hybrid applications
- Distribute traffic for complex deployments

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



Azure Front Door

Azure Front Door lets you define, manage, and monitor the global routing for your web traffic by optimizing for best performance and instant global failover for high availability. With Front Door, you can transform your global (multi-region) consumer and enterprise applications into robust, high-performance personalized modern applications, APIs, and content that reaches a global audience with Azure.

Business scenarios

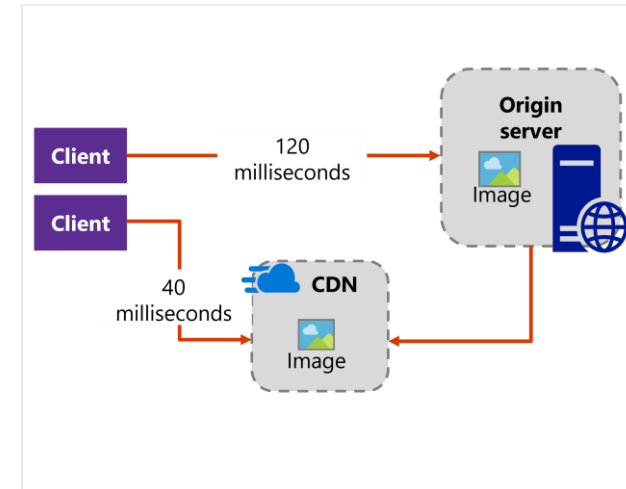
- Low latency: Ensure requests are sent to the lowest latency backends
- Priority: Support primary and secondary backends
- Weighted: Distribute traffic by using weight coefficients
- Affinity: Ensure requests from the same end user are sent to the same backend
- Support WAF and CDN integration for HTTP(S) traffic

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.



Azure Content Delivery Network

Azure Content Delivery Network offers a global solution for rapidly delivering high-bandwidth content to users. Content Delivery Network lets you cache your content at strategically placed physical nodes across the world.

Business scenarios

- Implement point-of-presence locations that are close to large clusters of users
- Reduce latency, both the transmission delay and the number of router hops
- Support Microsoft, Akamai, and Verizon content delivery networks
- Use custom domains, file compression, caching, and geo-filtering

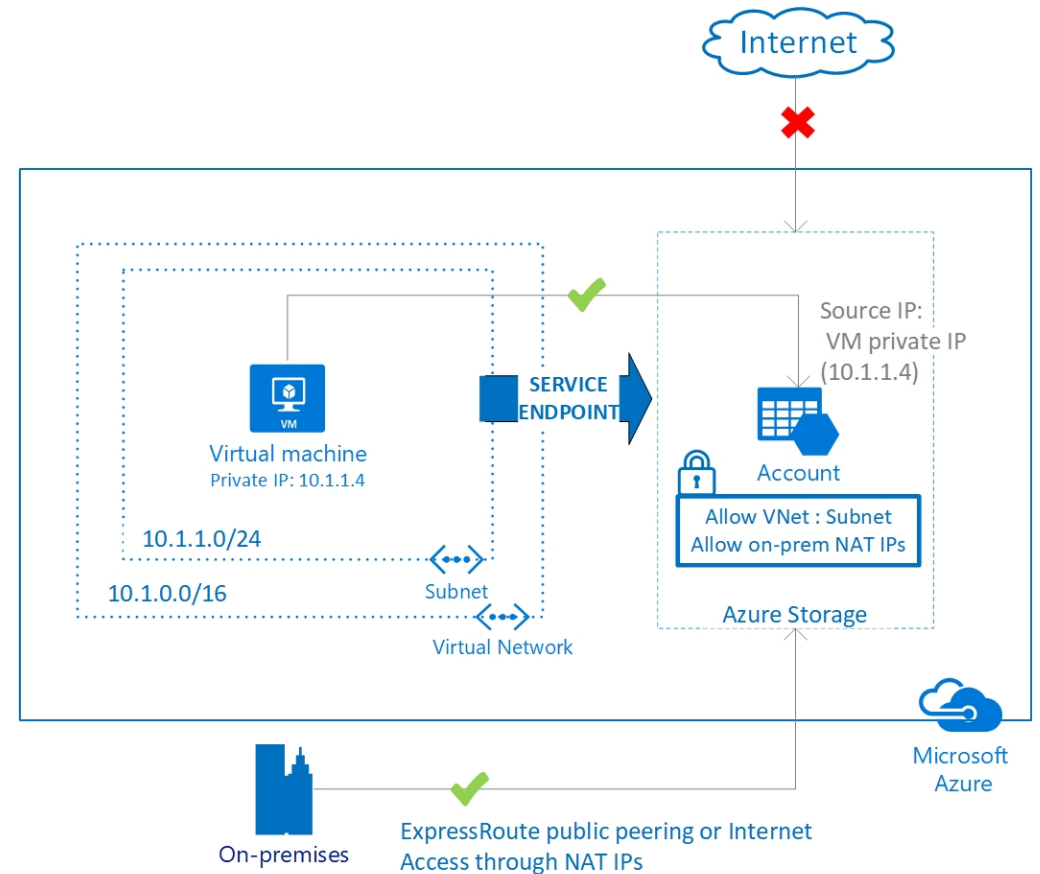
Design for application
protection services

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 Virtual Network - Service endpoints

Azure Virtual Network service endpoints extend your virtual network private address space and the identity of your virtual network to the Azure services over a direct connection. You can use endpoints to secure your critical Azure service resources to have access to only your virtual networks. Traffic from your virtual network to the Azure service always remains on the Microsoft Azure backbone network. Service endpoints are easy to set up and have less management overhead than other strategies.

Business scenarios

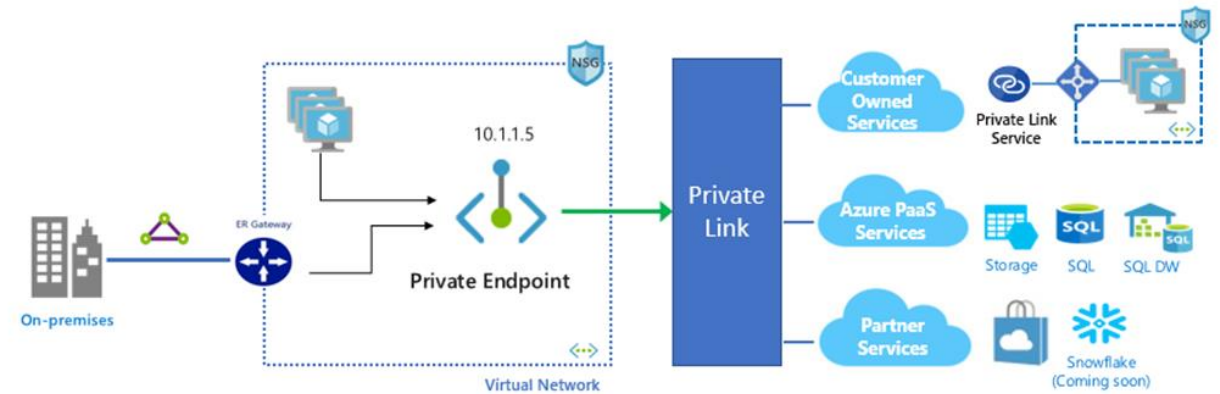
- Secure your critical Azure service resources to only your virtual networks
- Increase security for your Azure service resources
- Implement optimal routing for Azure service traffic from your virtual network

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



Azure Private Link

Azure Private Link enables you to access Azure PaaS services (such as 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. You can create your own private link service in your virtual network and deliver it to your customers. Private Link is used to access PaaS services, such as Azure Storage, Azure SQL, App Services, and more.

Business scenarios

- Enable private connectivity to services on Azure
- Integrate with on-premises and peered networks
- Restrict traffic to the Microsoft network with no public internet access

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 virtual network security groups

You can filter network traffic to and from Azure resources in an Azure virtual network with [Azure network security group \(NSGs\)](#). You can use a network virtual appliance (NVA) such as Azure Firewall or firewalls from other vendors.

An NSG contains a list of access control list (ACL) rules that allow or deny network traffic to subnets, network interface cards (NICs), or both. NSGs can be associated with either subnets or individual NICs connected to a subnet. When an NSG is associated with a subnet, the ACL rules apply to all the virtual machines in that subnet.

NSGs contain two sets of rules: inbound and outbound. The priority for a rule must be unique within each set. Each rule has properties of protocol, source and destination port ranges, address prefixes, direction of traffic, priority, and access type. All NSGs contain a set of default rules. The default rules can't be deleted, but because they're assigned the lowest priority, you can override them with custom rules.

Business scenarios

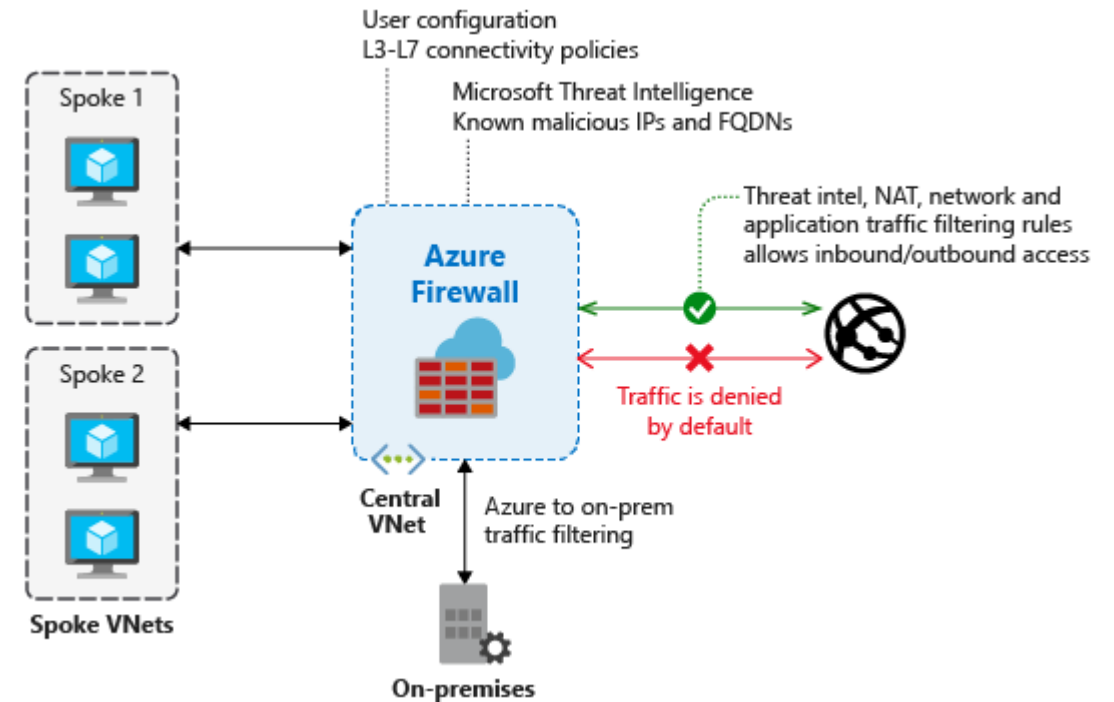
- Control how Azure routes traffic from subnets
- Limit the users in an organization who can work with resources in virtual networks
- Restrict traffic to an individual NIC by associating an NSG directly to a NIC
- Combine NSGs with JIT access to restrict access to your virtual machine management ports

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.



Azure Firewall

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It's a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. Azure Firewall uses a static public IP address for your virtual network resources, which allows outside firewalls to identify traffic originating from your virtual network. Azure Firewall provides inbound protection for non-HTTP/S protocols (such as RDP, SSH, and FTP), outbound network-level protection for all ports and protocols, and application-level protection for outbound HTTP/S.

Business scenarios

- Implement centralized creation, enforcement, and logging of application and network connectivity policies
- Apply connectivity policies across subscriptions and virtual networks
- Combine Azure Firewall rules with just in time (JIT) access to restrict access to your virtual machine management ports

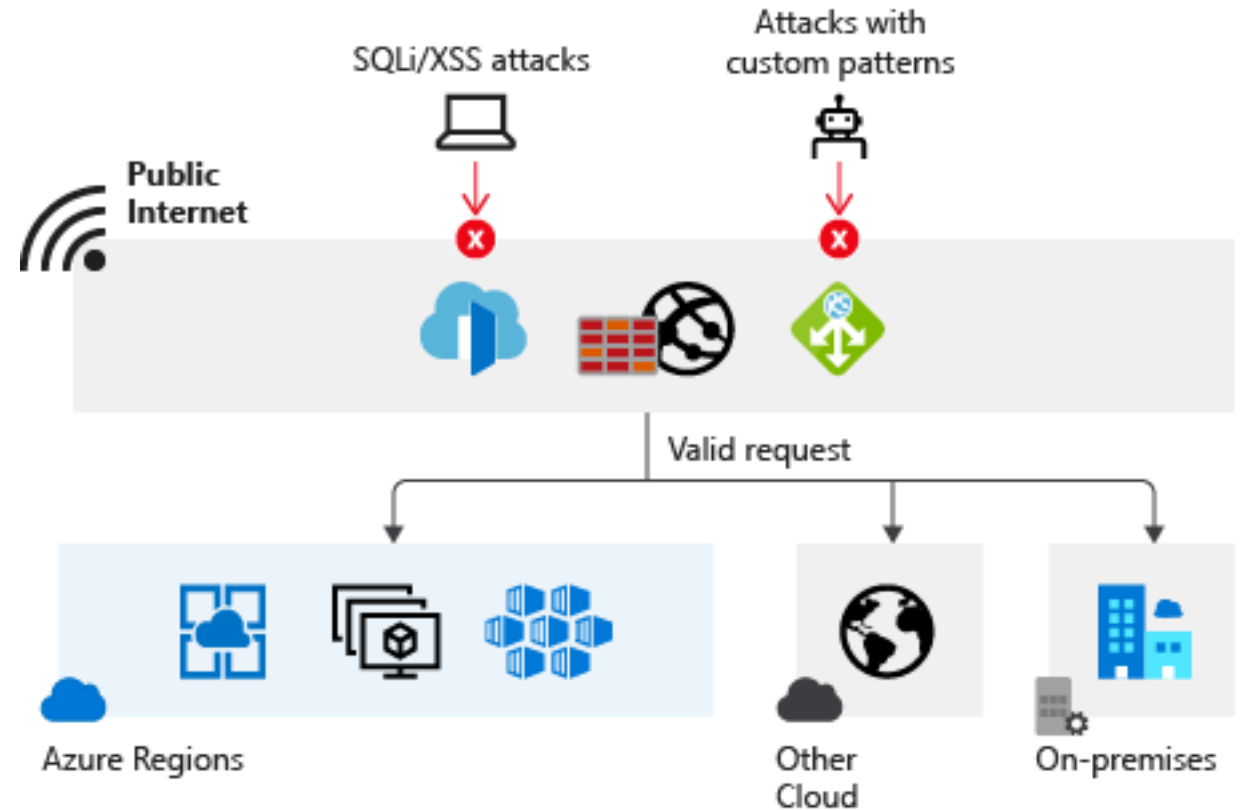


Web Application Firewall

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 Web Application Firewall

Azure Web Application Firewall provides protection to your web applications from common web exploits and vulnerabilities such as SQL injection, and cross-site scripting. Web Application Firewall provides out of box protection from OWASP top 10 vulnerabilities via managed rules. Configure customer-managed rules for extra protection based on source IP range and request attributes (headers, cookies, form data fields, query string parameters). Preventing similar attacks in your application code can be challenging. The process can require rigorous maintenance, patching, and monitoring at multiple layers of the application topology. A centralized web application firewall helps to simplify security management. A web application firewall gives application administrators better assurance of protection against threats and intrusions.

Business scenarios

- React faster to security threats by centrally patching known vulnerabilities instead of securing individual web apps
- Deploy Web Application Firewall with Application Gateway, Front Door, and Content Delivery Network

DDoS Protection

Azure DDoS 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.

Feature	DDoS IP Protection	DDoS Network Protection
Active traffic monitoring & always on detection	●	●
Automatic attack mitigation	●	●
Metrics & alerts	●	●
Mitigation reports	●	●
Mitigation flow logs	●	●
Mitigation policies tuned to customers application	●	●
Integration with Firewall Manager	●	●
Microsoft Sentinel data connector and workbook	●	●
Protection of resources across subscriptions in a tenant	●	●
Public IP Standard SKU protection	●	●
Public IP Basic SKU protection		●
DDoS rapid response support		●
Cost protection		●
WAF discount		●
Price	Per protected IP	Per 100 protected IP addresses



Azure DDoS Protection (distributed denial of service protection)

Azure DDoS 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. Additionally, customers who use Azure DDoS Protection have access to DDoS Rapid Response support to engage DDoS experts during an active attack.

Business scenarios

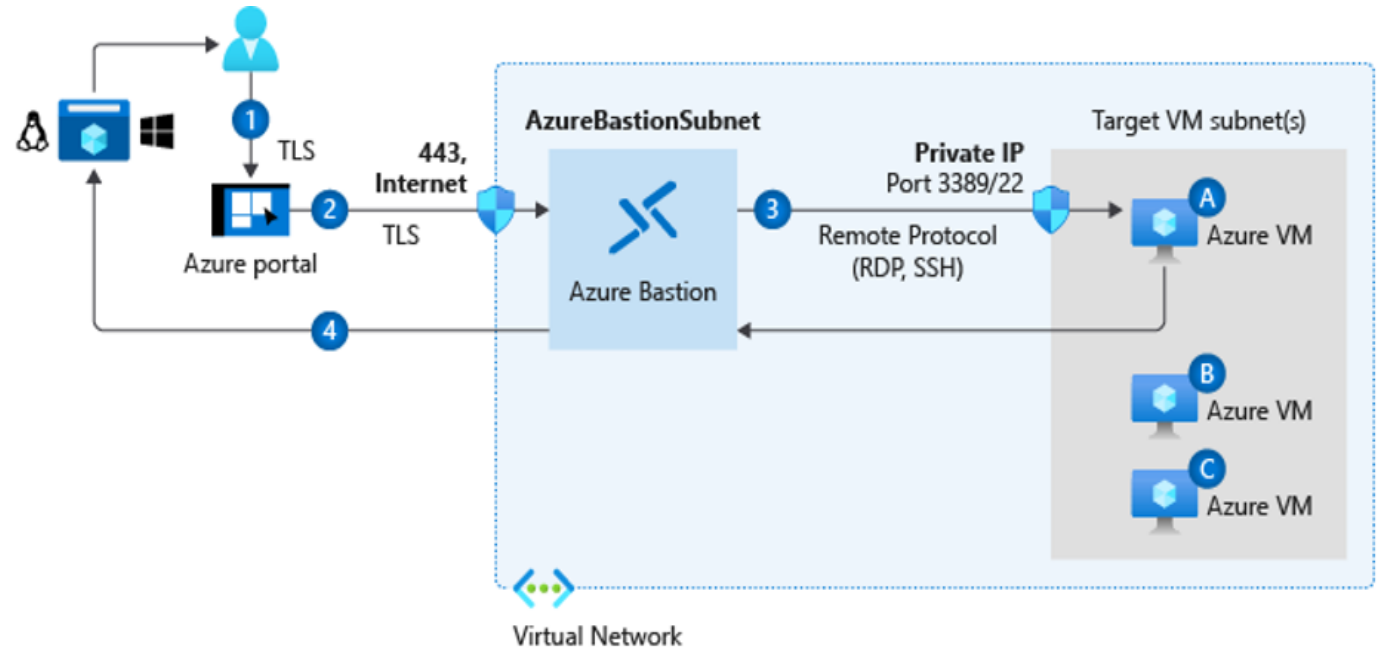
- Implement always-on traffic monitoring, adaptive tuning, and mitigation scale
- Access multi-layered protection, including attack analytics, metrics, and alerting
- Receive support from the DDoS rapid response team

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



Azure Bastion

Azure Bastion is a fully platform-managed PaaS service that you implement inside your virtual network. Azure Bastion provides secure and seamless RDP/SSH connectivity to your virtual machines directly in the Azure portal over TLS. Azure Bastion helps protect against port scanning. RDP ports, SSH ports, and public IP addresses aren't publicly exposed for your virtual machines.

When you connect via Azure Bastion, your virtual machines don't need a public IP address. Traffic initiated from Azure Bastion to target virtual machines stays within the virtual network or between peered virtual networks.

Azure Bastion sits at the perimeter of your virtual network and helps protect against zero-day exploits. You don't need to worry about hardening each of the virtual machines in your virtual network. The Azure platform keeps Azure Bastion up to date.

There's no need to apply NSGs to the Azure Bastion subnet because it's hardened internally. For more security, you can configure NSGs to allow only remote connections to the target virtual machines from the Azure Bastion host.

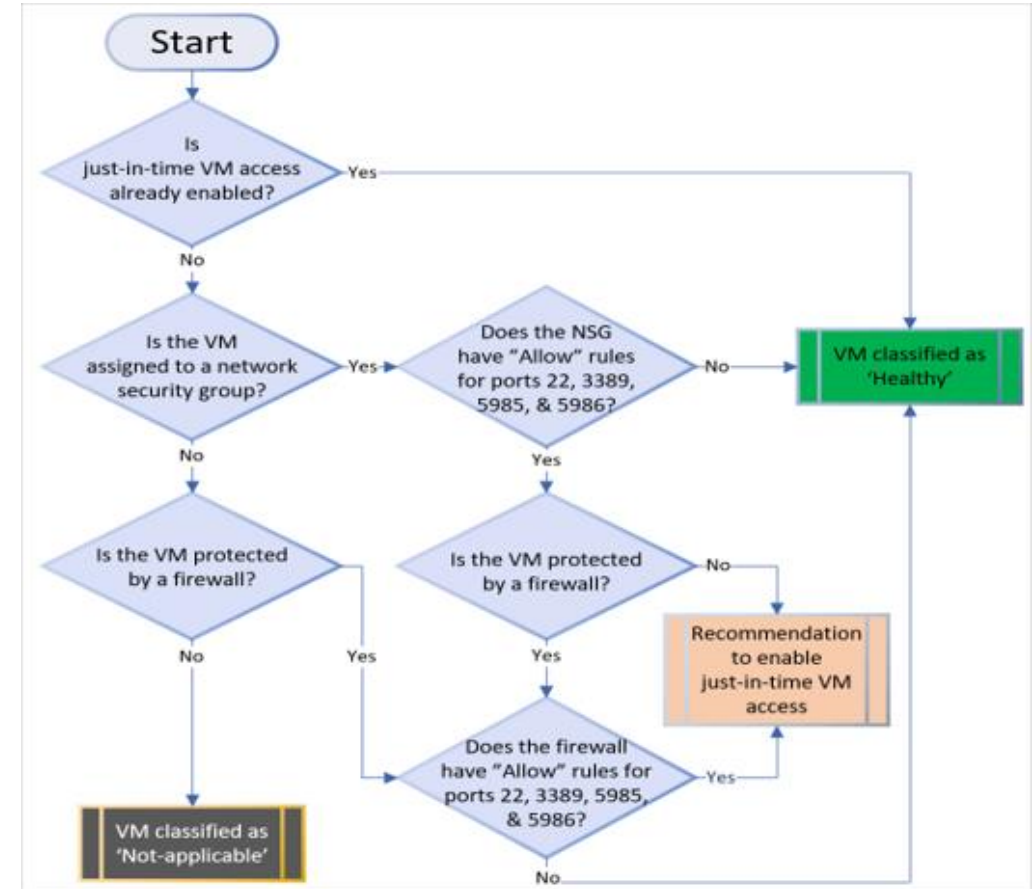
Business scenarios

- Secure remote connections from the Azure portal to Azure virtual machines
- Eliminate exposing RDP ports, SSH ports, or public IP addresses for your internal virtual machines
- Integrate with native security appliances for an Azure virtual network, like Azure Firewall
- Monitor and manage remote connections.

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



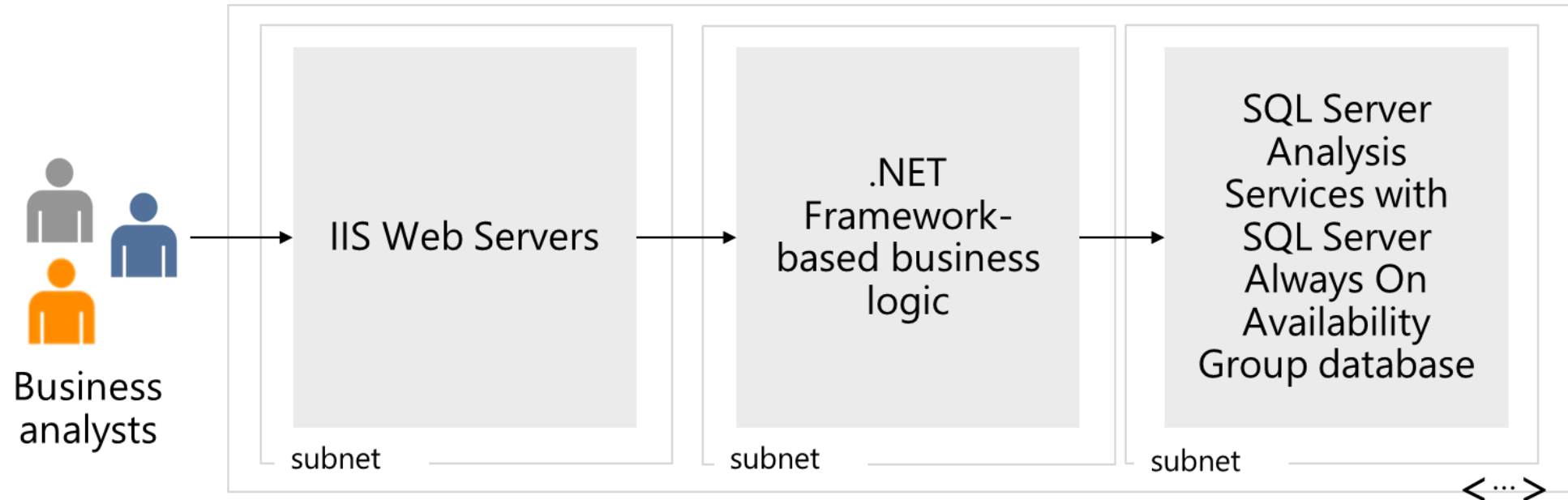
Things to know about JIT network access

JIT network access lets you lock down inbound traffic to your virtual machines. You can implement JIT to reduce exposure to attacks while providing easy access to connect to your virtual machines when needed.

- When you enable JIT virtual machine access, you select the ports on the virtual machines to which inbound traffic is blocked. This configuration ensures "deny all inbound traffic" rules exist for your selected ports in the NSG and [Azure Firewall rules](#). These rules restrict access to your Azure virtual machine's management ports and defend them from attack.
- If other rules already exist for the selected ports, the existing rules take priority over the new "deny all inbound traffic" rules. If there are no existing rules on the selected ports, the new rules take top priority in the NSG and Azure Firewall.
- When a user requests access to a virtual machine, Security Center checks if the user has [Azure role-based access control \(Azure RBAC\)](#) permissions for that virtual machine. If the request is approved, NSGs and Azure Firewall allow inbound traffic to the selected ports from the relevant IP address (or range) for the amount of time specified. After the time has expired, the NSGs are returned to their previous states. Connections that are already established aren't interrupted.

Case study and review

Case Study – BI enterprise application

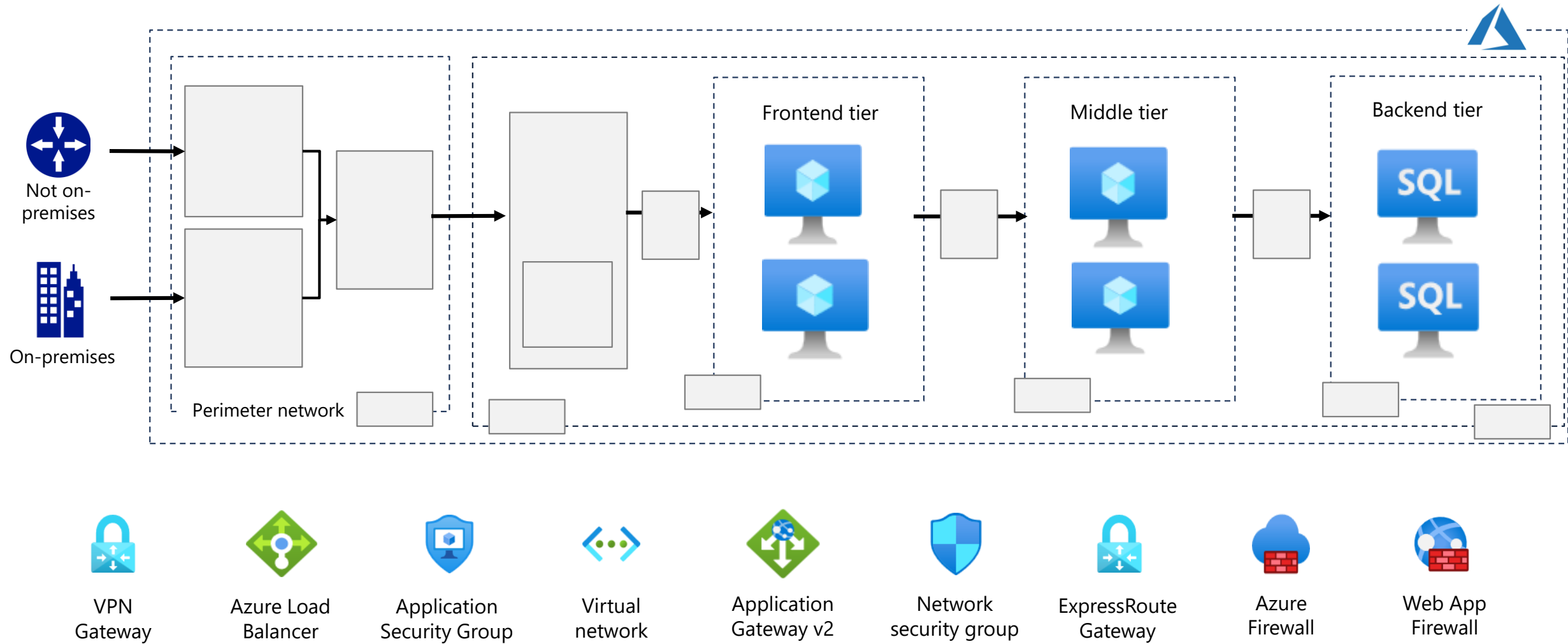


- Heavy demand.
- Servers reach their performance limits during the day.
- Servers sit idle during off hours.

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

- Uses all-flash enterprise SAN storage

Solution - BI enterprise application



Completed solution - BI enterprise application

