AZURE NETWORKING

Dr. Shridhar G. Domanal

Azure Networking

The networking services in Azure provide a variety of networking capabilities that can be used together or separately.

- **Connectivity services**: Connect Azure resources and on-premises resources using any or a combination of these networking services in Azure - Virtual Network (VNet), Virtual WAN, ExpressRoute, VPN Gateway, Virtual network NAT Gateway, Azure DNS, Peering service, and Azure Bastion.

- **Application protection services**: Protect your applications using any or a combination of these networking services in Azure - Private Link, DDoS protection, Firewall, Network Security Groups, Web Application Firewall, and Virtual Network Endpoints.

- **Application delivery services**: Deliver applications in the Azure network using any or a combination of these networking services in Azure - Content Delivery Network (CDN), Azure Front Door Service, Traffic Manager, Application Gateway, Internet Analyzer, and Load Balancer.

- **Network monitoring**: Monitor your network resources using any or a combination of these networking services in Azure - Network Watcher, ExpressRoute Monitor, Azure Monitor, or VNet Terminal Access Point (TAP).

Connectivity Services

This section describes services that provide connectivity between Azure resources, connectivity from an on-premises network to Azure resources, and branch to branch connectivity in Azure - Virtual Network (VNet), Virtual WAN, ExpressRoute, VPN Gateway, Virtual network NAT Gateway, Azure DNS, Azure Peering service, and Azure Bastion.

Service	Why use?	Scenarios
Virtual network	Enables Azure resources to securely communicate with each other, the internet, and on-premises networks.	Filter network traffic Route network traffic Restrict network access to resources Connect virtual networks
ExpressRoute	Extends your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider.	Create and modify an ExpressRoute circuit Create and modify peering for an ExpressRoute circuit Link a VNet to an ExpressRoute circuit Configure and manage route filters for ExpressRoute circuits
VPN Gateway	Sends encrypted traffic between an Azure virtual network and an on-premises location over the public Internet.	Site-to-site-connections VNet-to-VNet connections Point-to-site connections
Virtual WAN	Optimizes and automates branch connectivity to, and through, Azure. Azure regions serve as hubs that you can choose to connect your branches to.	Site-to-site connections, ExpressRoute connections

Connectivity Services

Azure DNS	Hosts DNS domains that provide name resolution by using Microsoft Azure infrastructure.	Host your domain in Azure DNS Create DNS records for a web app Create an alias record for Traffic Manager Create an alias record for public IP Address Create an alias record for zone resource record
Azure Bastion	Configure secure and seamless RDP/SSH connectivity to your virtual machines directly in the Azure portal over TLS. When you connect via Azure Bastion, your virtual machines do not need a public IP address	Create an Azure Bastion host Connect using SSH to a Linux VM Connect using RDP to a Windows VM
Virtual network NAT Gateway	Create a NAT gateway to provide outbound connectivity for a virtual machine.	Create a NAT Gateway
Azure Peering Service (Preview)	Collaborate with service providers for optimal and reliable routing to the Microsoft cloud over the public network.	Register Azure Peering Service

Virtual Network

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. You can use a VNets to:

Communicate between Azure resources: You can deploy VMs, and several other types of Azure resources to a virtual network, such as Azure App Service Environments, the Azure Kubernetes Service (AKS), and Azure Virtual Machine Scale Sets. To view a complete list of Azure resources that you can deploy into a virtual network, see Virtual network service integration.

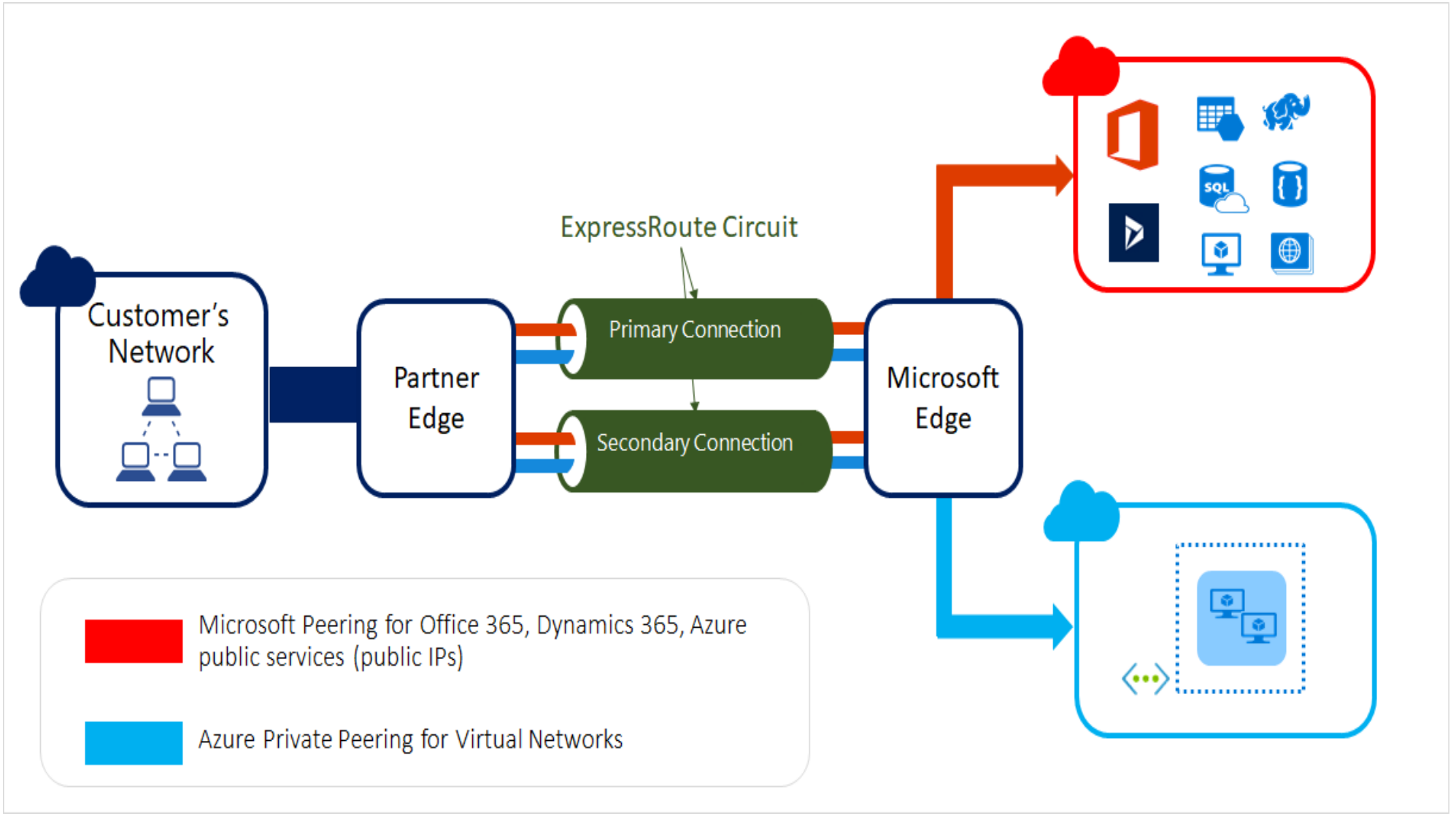
Communicate between each other: You can connect virtual networks to each other, enabling resources in either virtual network to communicate with each other, using virtual network peering. The virtual networks you connect can be in the same, or different, Azure regions

Communicate to the internet: All resources in a VNet can communicate outbound to the internet, by default. You can communicate inbound to a resource by assigning a public IP address or a public Load Balancer. You can also use Public IP addresses or public Load Balancer to manage your outbound connections.

Communicate with on-premises networks: You can connect your on-premises computers and networks to a virtual network using VPN Gateway or ExpressRoute.

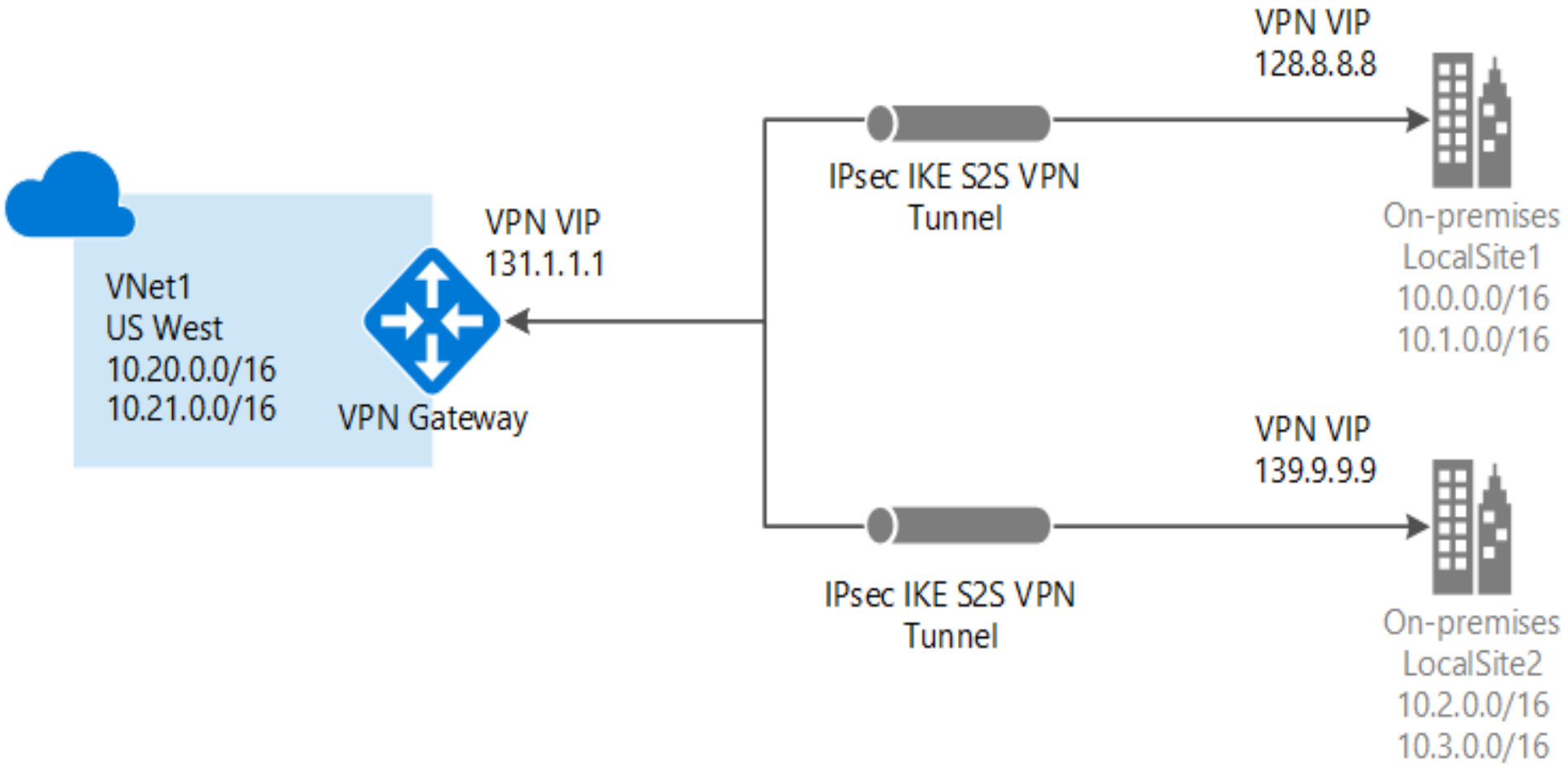
Express Route

ExpressRoute enables you to extend your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider. This connection is private. Traffic does not go over the internet. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure, Office 365, and Dynamics 365.



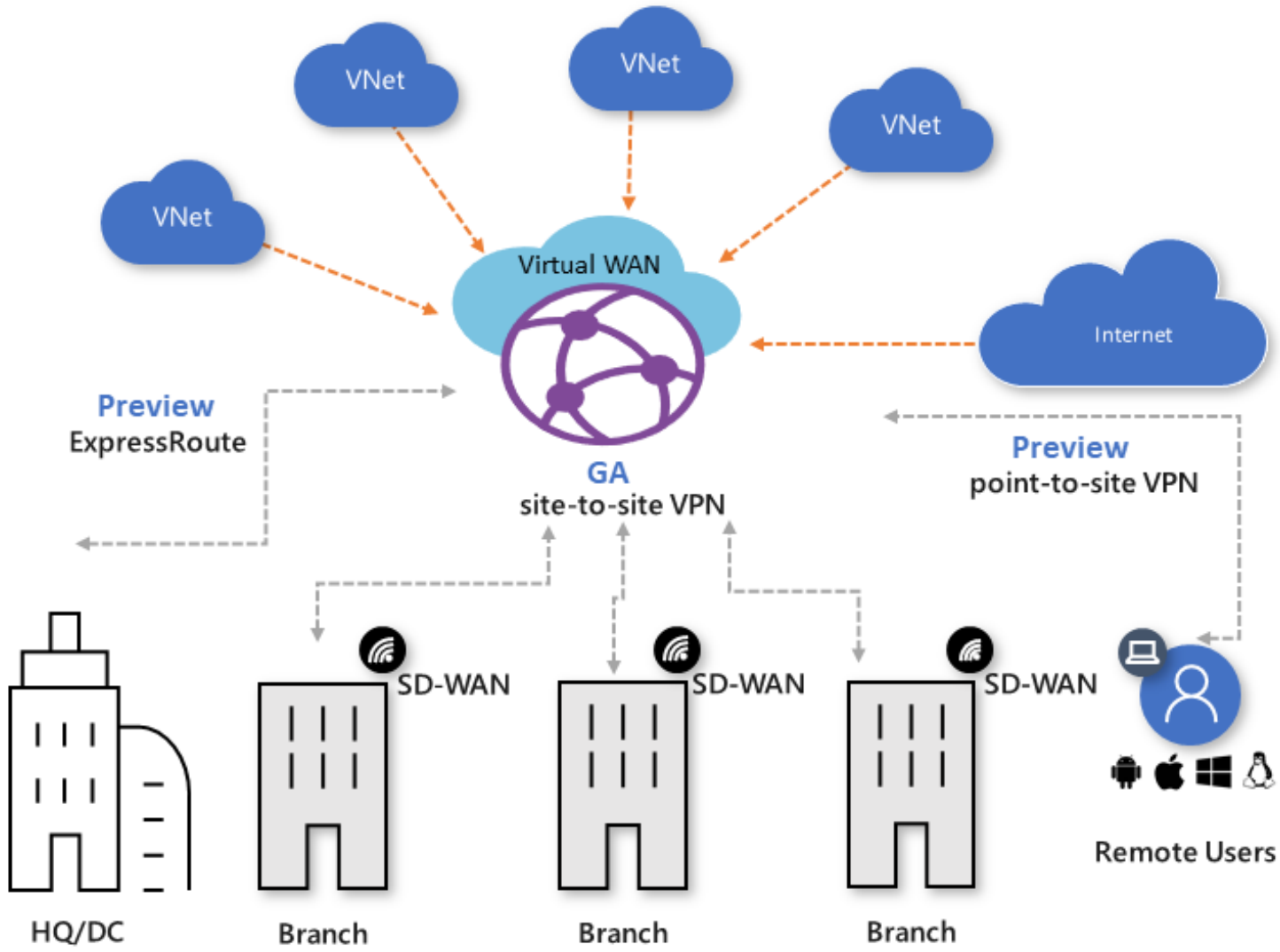
VPN Gateway

VPN Gateway helps you create encrypted cross-premises connections to your virtual network from on-premises locations, or create encrypted connections between VNets. There are different configurations available for VPN Gateway connections, such as, site-to-site, point-to-site, or VNet to VNet. The following diagram illustrates multiple site-to-site VPN connections to the same virtual network.



VPN WAN

Azure Virtual WAN is a networking service that provides optimized and automated branch connectivity to, and through, Azure. Azure regions serve as hubs that you can choose to connect your branches to. You can leverage the Azure backbone to also connect branches and enjoy branch-to-VNet connectivity. Azure Virtual WAN brings together many Azure cloud connectivity services such as site-to-site VPN, ExpressRoute, point-to-site user VPN into a single operational interface. Connectivity to Azure VNets is established by using virtual network connections.

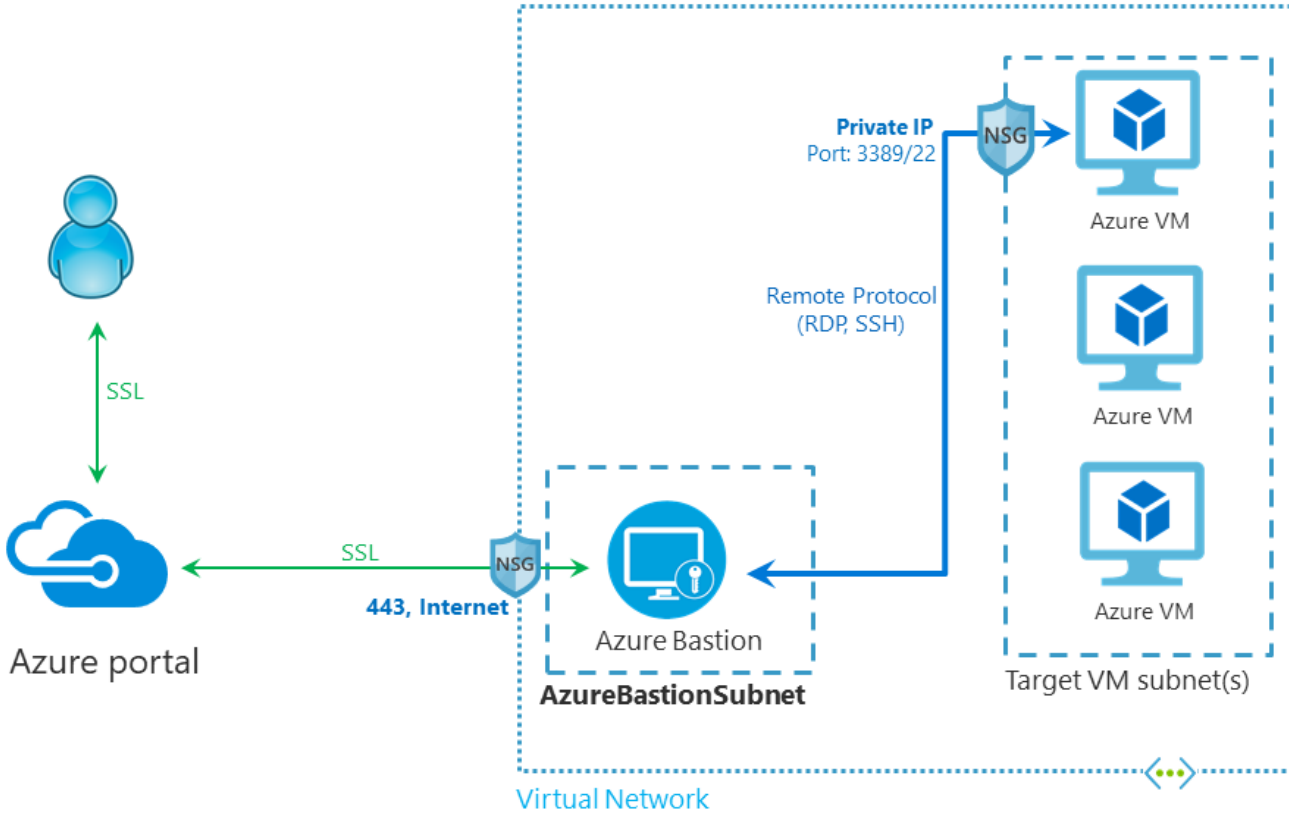


Azure DNS

Azure DNS is a hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure. By hosting your domains in Azure, you can manage your DNS records by using the same credentials, APIs, tools, and billing as your other Azure services.

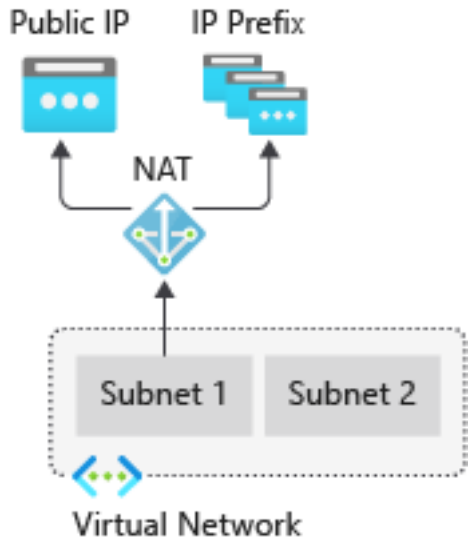
Azure Bastion

- The Azure Bastion service is a new fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly in the Azure portal over TLS. When you connect via Azure Bastion, your virtual machines do not need a public IP address



Virtual Network NAT Gateway

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. Outbound connectivity is possible without load balancer or public IP addresses directly attached to virtual machines



Azure Peering Service

Azure Peering service enhances customer connectivity to Microsoft cloud services such as Office 365, Dynamics 365, software as a service (SaaS) services, Azure, or any Microsoft services accessible via the public internet.

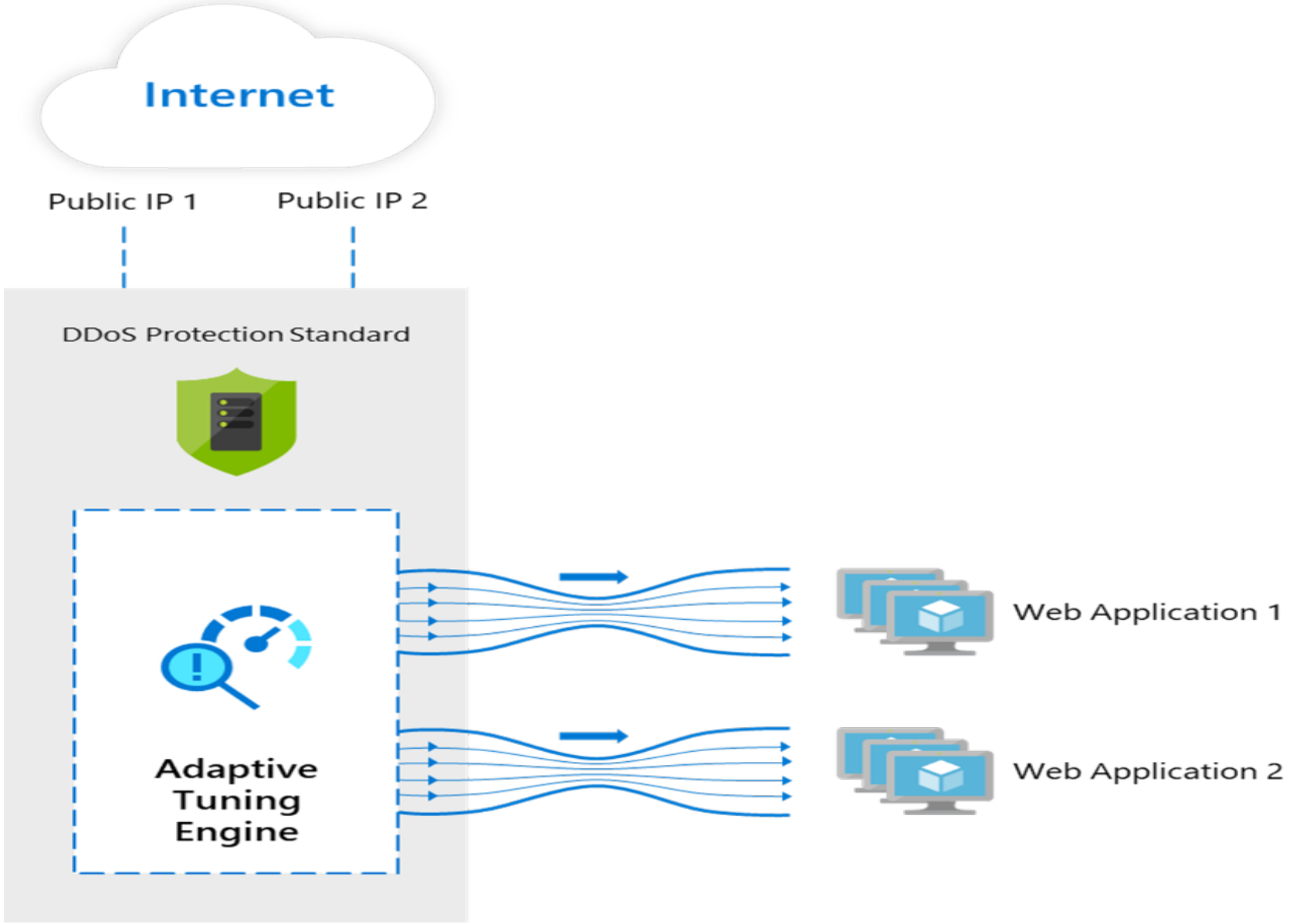
Application Protection Services

This section describes networking services in Azure that help protect your network resources - Protect your applications using any or a combination of these networking services in Azure - Private Link, DDoS protection, Firewall, Network Security Groups, Web Application Firewall, and Virtual Network Endpoints.

Service	Why use?	Scenario
DDoS protection	High availability for your applications with protection from excess IP traffic charges	Manage Azure DDoS Protection
Web Application Firewall	Azure WAF with Application Gateway provides regional protection to entities in public and private address space Azure WAF with Front Door provides protection at the network edge to public endpoints.	Configure bot protection rules Configure custom response code Configure IP restriction rules Configure rate limit rule
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.	Deploy an Azure Firewall in a Vnet - Deploy an Azure Firewall in a hybrid network Filter inbound traffic with Azure Firewall DNAT
Network security groups	Full granular distributed end node control at VM/subnet for all network traffic flows	Filter network traffic using network security groups
Virtual network service endpoints	Enables you to limit network access to some Azure service resources to a virtual network subnet	Restrict network access to PaaS resources
Private Link	Enables you 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.	Create a private endpoint Create a Private Link service

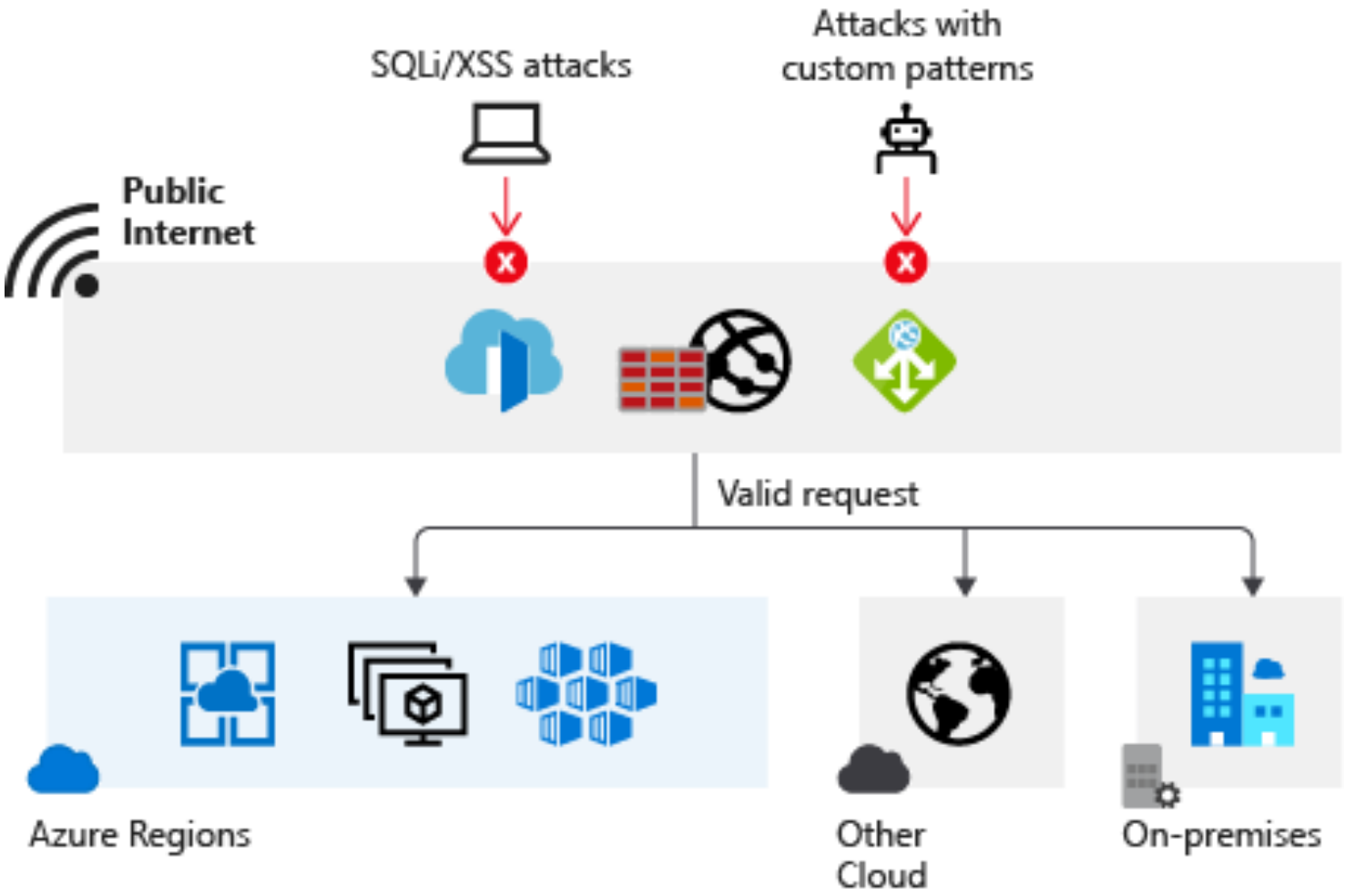
DDoS Protection

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



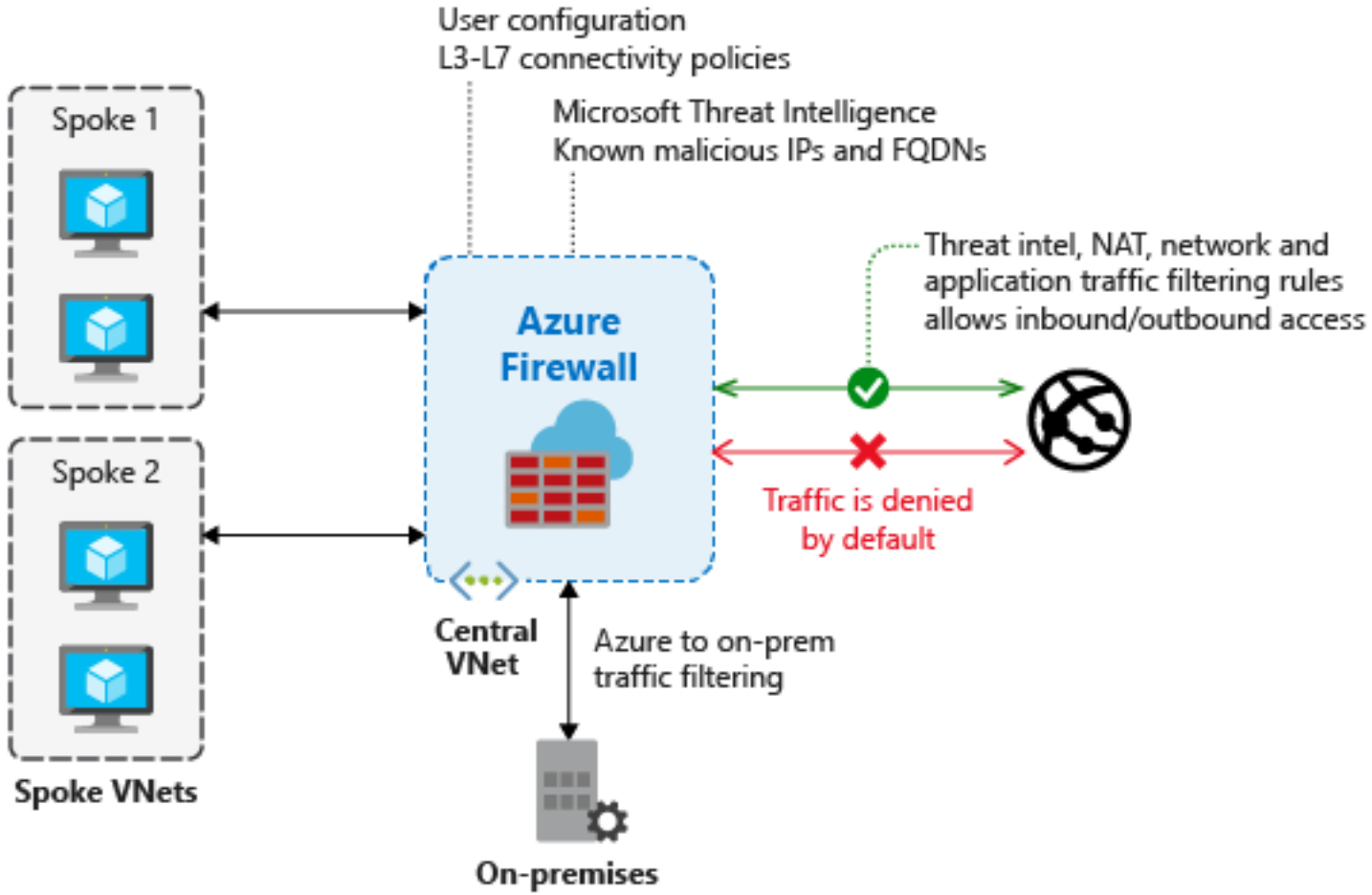
Web Application Firewall (WAF)

Azure Web Application Firewall (WAF) provides protection to your web applications from common web exploits and vulnerabilities such as SQL injection, and cross site scripting. Additionally customers can also configure custom rules, which are customer managed rules to provide additional protection based on source IP range, and request attributes such as headers, cookies, form data fields or query string parameters.



Azure Firewall

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. Using Azure Firewall, you can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network.

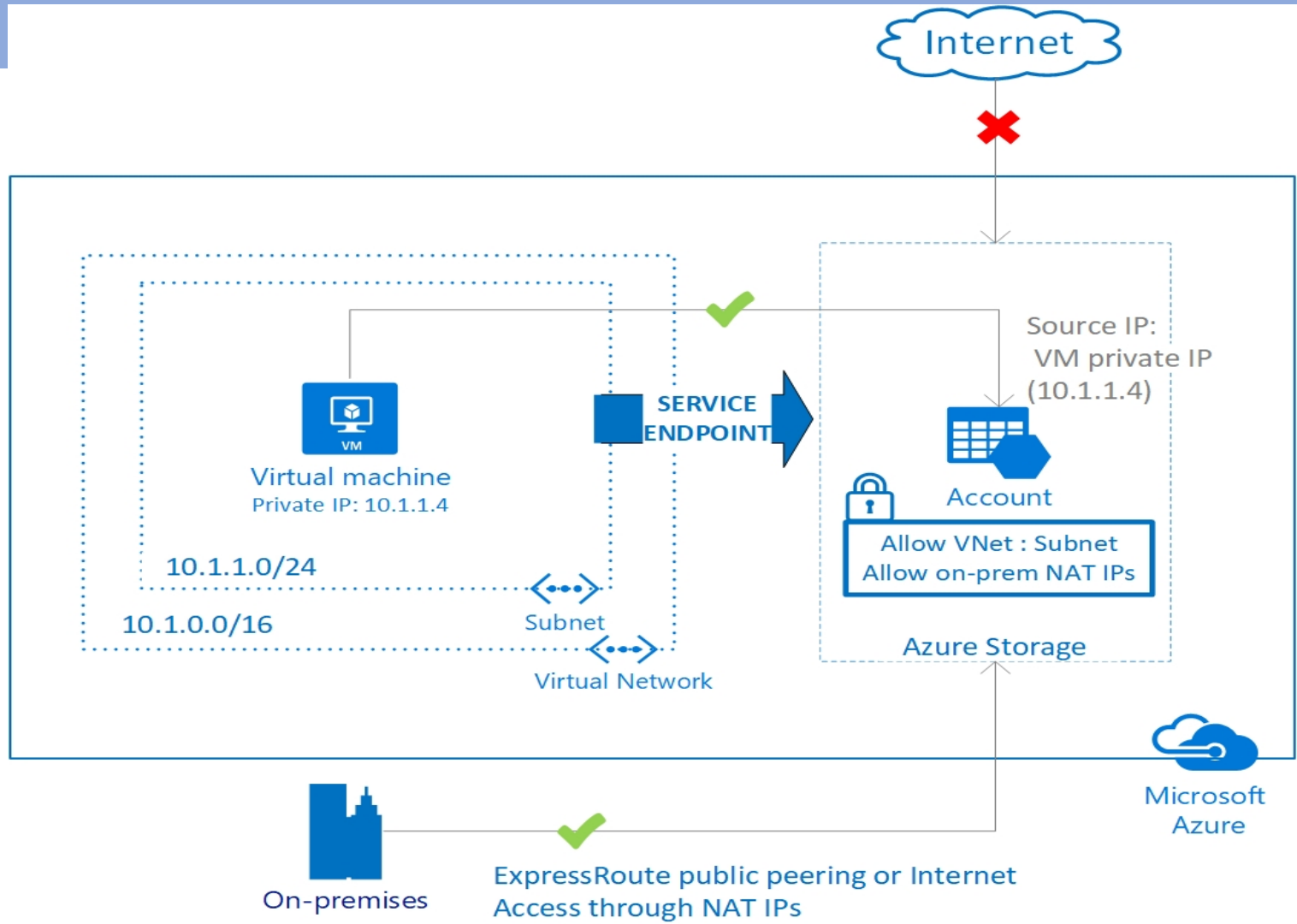


Network Security Groups

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

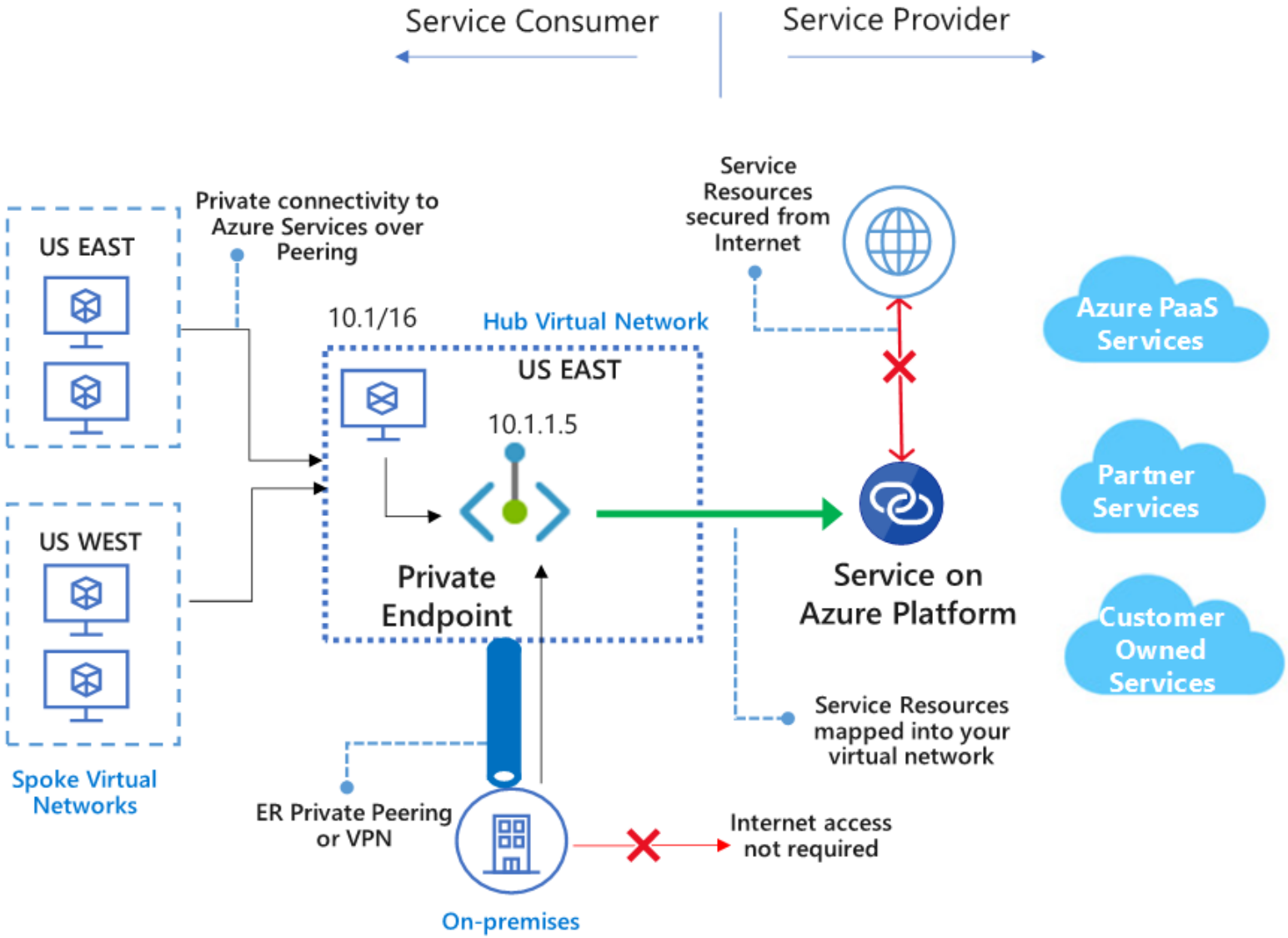
Service Endpoints

Virtual Network (VNet) service endpoints extend your virtual network private address space and the identity of your VNet to the Azure services, over a direct connection. Endpoints allow you to secure your critical Azure service resources to only your virtual networks. Traffic from your VNet to the Azure service always remains on the Microsoft Azure backbone 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. 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.



Application Delivery Services

This section describes networking services in Azure that help deliver applications - Content Delivery Network, Azure Front Door Service, Traffic Manager, Load Balancer, and Application Gateway.

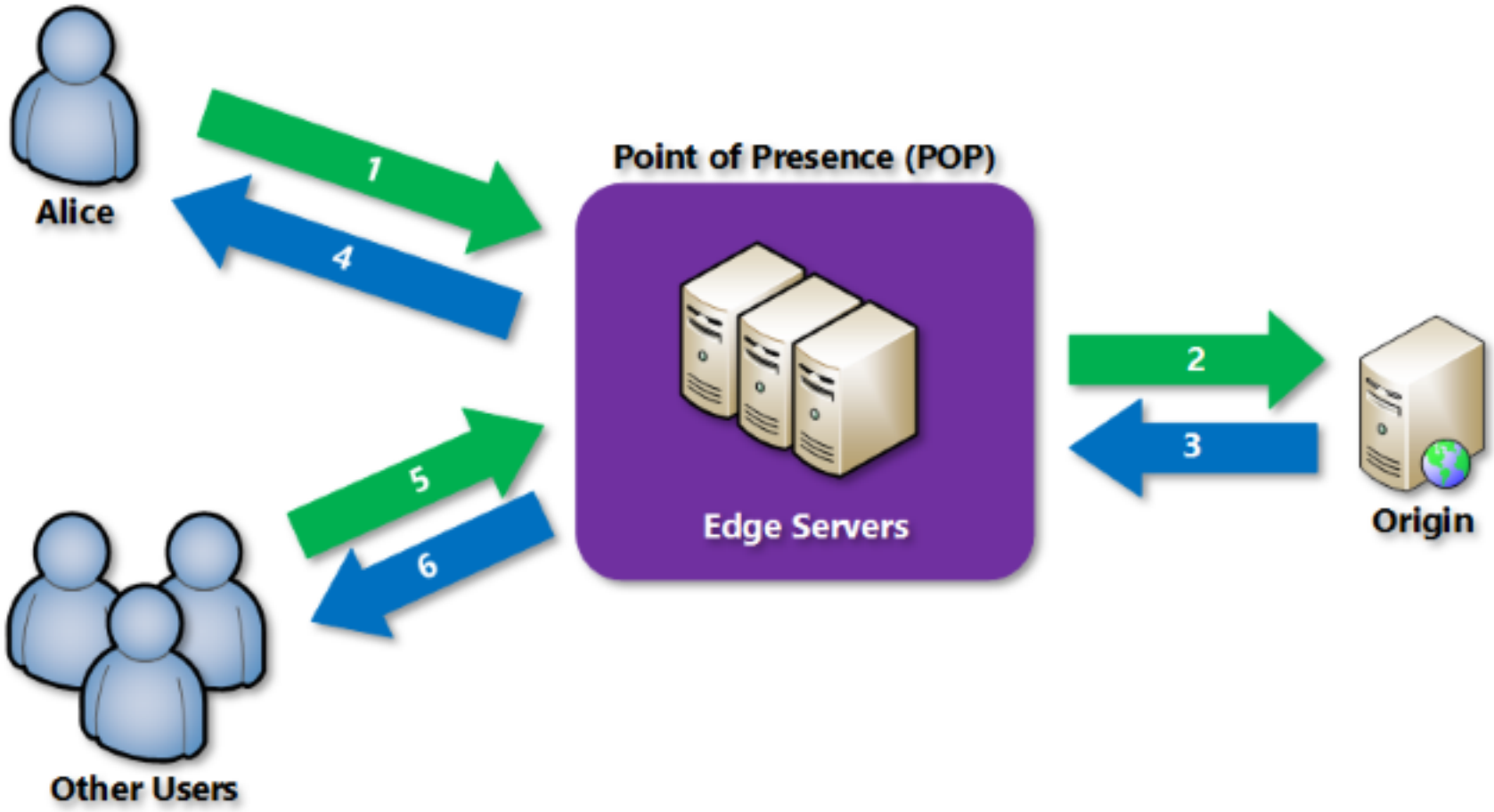
Service	Why use?	Scenario
Content Delivery Network	Delivers high-bandwidth content to users. CDNs store cached content on edge servers in point-of-presence (POP) locations that are close to end users, to minimize latency	Add CDN to a web app - Access storage blobs using an Azure CDN custom domain over HTTPS Add a custom domain to your Azure CDN endpoint Configure HTTPS on an Azure CDN custom domain
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.	Add a custom domain to your Azure Front Door Service Configure HTTPS on a Front Door custom domain Set up geo-filtering Web Application Firewall policy
Traffic Manager	Distributes traffic based on DNS to services across global Azure regions, while providing high availability and responsiveness	Route traffic for low latency Route traffic to a priority endpoint Control traffic with weighted endpoints Route traffic based on geographic location of the endpoint Route traffic based on user's subnet

Application Delivery Services

Load Balancer	Provides regional load-balancing by routing traffic across availability zones and into your VNets. Provides internal load-balancing by routing traffic across and between your resources to build your regional application.	Load balance internet traffic to VMs Load-balance traffic across VMs inside a virtual network Port forward traffic to a specific port on specific VMs Configure load balancing and outbound rules
Application Gateway	Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications.	Direct web traffic with Azure Application Gateway Tutorial: Configure an application gateway with TLS termination using the Azure portal Create an application gateway with URL path-based redirection

Content Delivery Networks

Azure Content Delivery Network (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

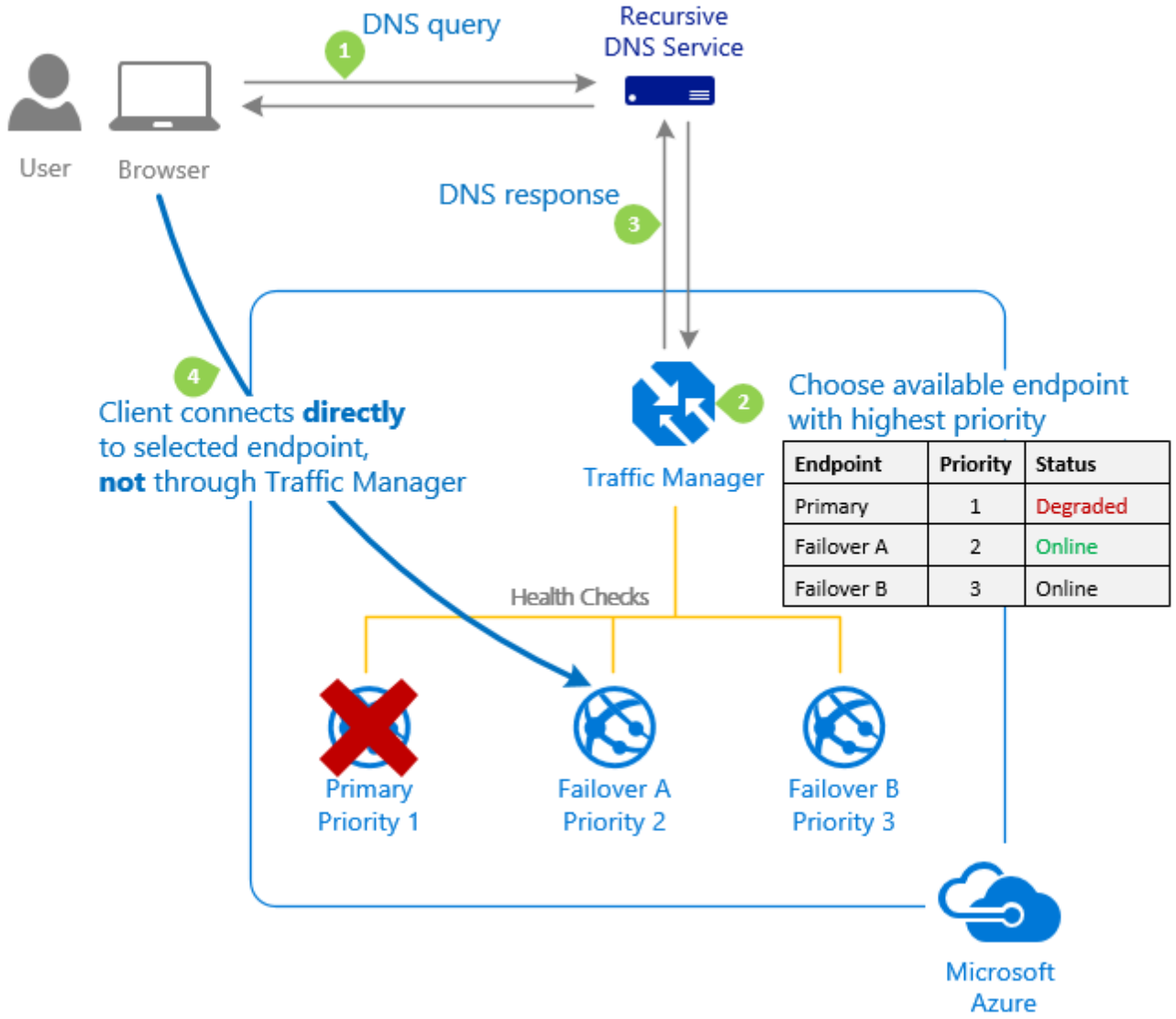


Azure Front Door Service

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. 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 reach a global audience with Azure.

Traffic Manager

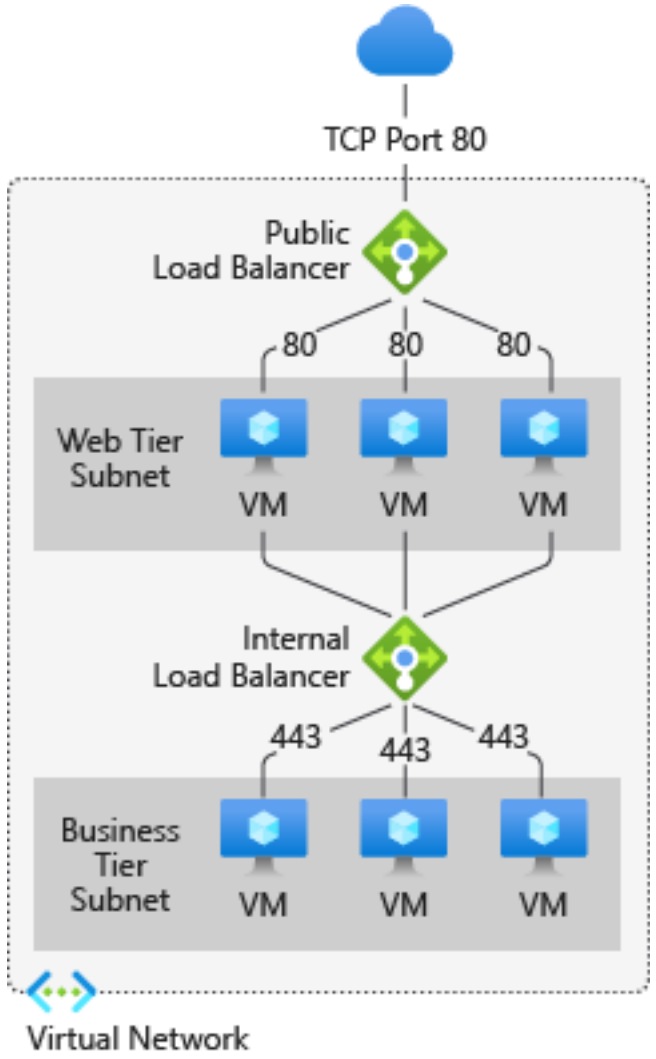
Azure Traffic Manager is a DNS-based traffic load balancer that enables you to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness. Traffic Manager provides a range of traffic-routing methods to distribute traffic such as priority,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



Load Balancer

The Azure Load Balancer provides high-performance, low-latency Layer 4 load-balancing for all UDP and TCP protocols. It manages inbound and outbound connections. You can configure public and internal load-balanced endpoints. You can define rules to map inbound connections to back-end pool destinations by using TCP and HTTP health-probing options to manage service availability

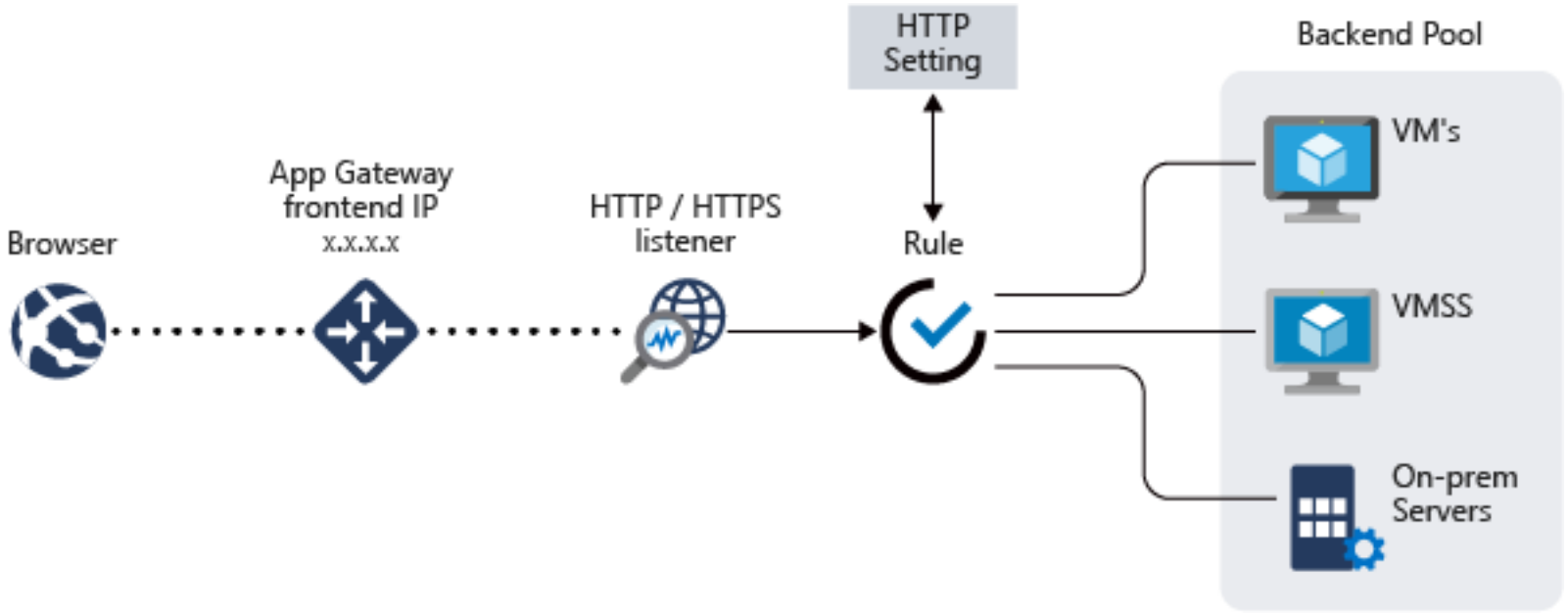
The following picture shows an Internet-facing multi-tier application that utilizes both external and internal load balancers



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

The following diagram shows url path-based routing with Application Gateway.



Network Monitoring Services

This section describes networking services in Azure that help monitor your network resources - Network Watcher, ExpressRoute Monitor, Azure Monitor, and Virtual Network TAP.

Service	Why use?	Scenario
Network Watcher	Helps monitor and troubleshoot connectivity issues, helps diagnose VPN, NSG, and routing issues, capture packets on your VM, automates triggering diagnostics tools using Azure Functions and Logic Apps	Diagnose VM traffic filter problem Diagnose VM routing problem Monitor communications between VMs Diagnose communication problems between networks Log network traffic to and from a VM
ExpressRoute Monitor	Provides real-time monitoring of network performance, availability, and utilization, helps with auto-discovery of network topology, provides faster fault isolation, detects transient network issues, helps analyze historical network performance characteristics, supports multi-subscription	Configure Network Performance Monitor for ExpressRoute ExpressRoute monitoring, metrics, and alerts
Azure Monitor	Helps you understand how your applications are performing and proactively identifies issues affecting them and the resources they depend on.	Traffic Manager metrics and alerts Azure monitor diagnostics for Standard Load Balancer Monitor Azure Firewall logs and metrics Azure web application firewall monitoring and logging
Virtual Network TAP	Provides continuous streaming of virtual machine network traffic to packet collector, enables network and application performance management solutions and security analytics tools	Create a VNet TAP resource

Azure Monitor

Azure Monitor maximizes the availability and performance of your applications by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments. It helps you understand how your applications are performing and proactively identifies issues affecting them and the resources they depend on

Virtual Network TAP

Azure virtual network TAP (Terminal Access Point) allows you to continuously stream your virtual machine network traffic to a network packet collector or analytics tool. The collector or analytics tool is provided by a network virtual appliance partner.

The following picture shows how virtual network TAP works