Cloud Networking

TEKsystems Global Services

WORKFORCE DEVELOPMENT

PARTICIPANT GUIDE

Content Usage Parameters

Content refers to material including instructor guides, student guides, lab guides, lab or hands-on activities, computer programs, etc. designed for use in a training program

1

Content is subject to copyright protection

2

Content may only be leveraged by students enrolled in the training program

3

Students agree not to reproduce, make derivative works of, distribute, publicly perform and publicly display content in any form or medium outside of the training program

4

Content is intended as reference material only to supplement the instructor-led training

LOGISTICS

Class Hours:

- Instructor will set class start and end times.
- There will be regular breaks in class.

Telecommunication:

- Turn off or set electronic devices to silent (not vibrate)
- Reading or attending to devices can be distracting to other students
- Try to delay until breaks or after class

Miscellaneous:

- Courseware
- Bathroom
- Fire drills

HI!

Jason Smith

Cloud Consultant with a Linux sysadmin background. Focused on cloud-native technologies: automation, containers & orchestration

Expertise

- Cloud
- Automation
- CICD
- Docker
- Kubernetes

INTRODUCE YOURSELF

Time to introduce yourself:

- Name you prefer
- Your professional background
- Current responsibilities
- Familiarity with Cloud
- Expectations and goals for class

INTRODUCTION TO CLOUD NETWORKING & VNET FUNDAMENTALS

OBJECTIVES

Define Cloud Networking in Azure: Grasp the core concepts and benefits specific to Azure.

Design and Implement Azure VNets: Understand the principles and steps for creating virtual networks.

Manage IP Addressing and Subnets: Configure IP address spaces and effective subnetting strategies.

Configure Azure Routes: Implement User-Defined Routes (UDRs) for custom traffic flow.

Utilize Azure NAT Gateway: Understand and deploy NAT Gateway for scalable outbound connectivity.

Correlate On-Premises to Azure Networking: Identify similarities and differences in network design and operation.

WHAT IS CLOUD NETWORKING

Virtualization of Network Hardware: Cloud networking abstracts physical network components into software-defined entities.

On-Demand Provisioning: Resources like virtual networks, load balancers, and firewalls are provisioned instantly via API.

Global Reach & Scalability: Easily extend your network across regions and scale resources up or down as needed.

Pay-as-you-go Model: Consume network services as utilities, paying only for what you use, reducing CapEx.

Managed Services: Cloud providers handle underlying infrastructure, patches, and maintenance, reducing operational burden.

KEY CHARACTERISTICS

Integrated Security

Security services are built into the platform.

Software-Defined Networking

Centralized control plane manages network behavior, abstracting hardware.

Isolation and Multi-Tenancy

Securely separates customer networks while sharing underlying physical infrastructure.

Network as Code

Infrastructure definition and deployment are automated using scripts and templates.

Elasticity and Agility

Networks can grow or shrink dynamically, adapting to changing application demands.

AZURE NETWORKING PHILOSOPHY

Hybrid Connectivity Focus

Secure by Design

Global Infrastructure, Local Control

Software-Defined Core

Foundation on Virtual Networks (VNETs)

AZURE NETWORKING CORE COMPONENTS

Network foundation

- Bastions
- Custom IP Prefixes
- DNS private resolvers
- DNS zones
- NAT gateways
- Network interfaces
- Network managers
- Private DNS zones
- Private Link
- Public IP addresses
- Public IP Prefixes
- Route tables
- Virtual networks ★

Hybrid connectivity

- Communications Gateways
- Connections
- ExpressRoute circuits
- ExpressRoute traffic collectors
- Local network gateways
- Mobile Networks
- Peering Services
- Peerings
- Virtual network gateways
- Virtual WANs

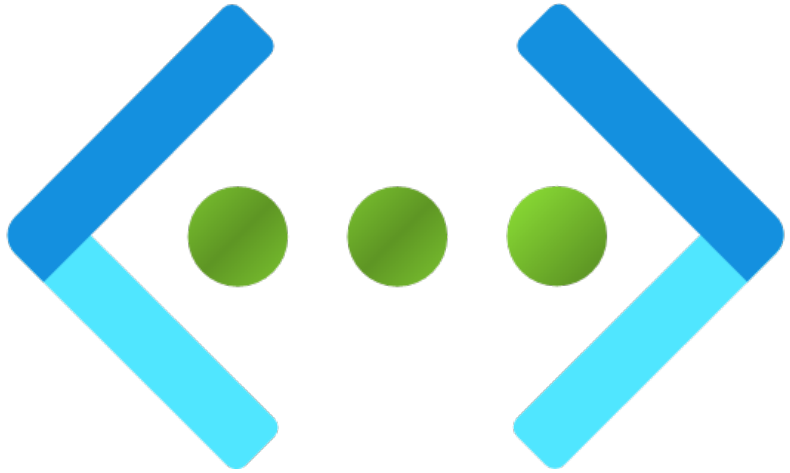
Network security

- DDoS protection plans
- Firewalls
- IP Groups
- Network security groups
- Network Security Perimeters PREVIEW
- Web Application Firewall policies (WAF)

Load balancing

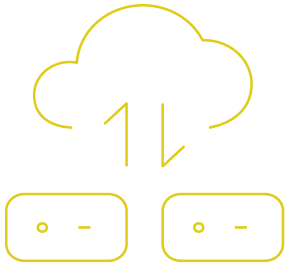
- Application gateways
- Load balancers ★

INTRODUCTION TO AZURE VNETS – THE FOUNDATION



- **Isolated Private Cloud:** VNets provide an isolated, logical network in the Azure cloud, dedicated to your subscription.
- **Custom IP Address Space:** Define your own private IP address ranges using CIDR notation, e.g., 10.0.0.0/16.
- **Segmentation with Subnets:** Break down your VNet into smaller, manageable subnets for different applications or tiers.
- **Secure by Default:** Traffic within a VNet is isolated; external access is only permitted via explicit configuration.
- **Bridge to On-Premises:** Establish secure connections (VPN Gateway or ExpressRoute) between your VNet and on-premises networks.

VNET CAPABILITIES AND FEATURES

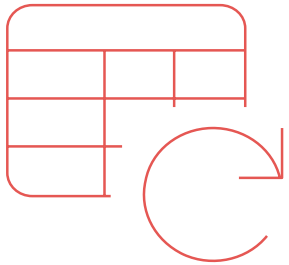


Resource Deployment

Deploy virtual machines and other services into VNets.

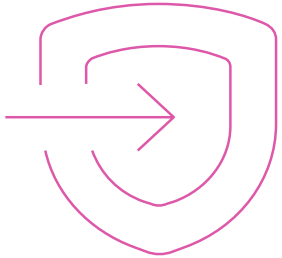
Network Security Groups

Apply inbound/outbound rules to filter network traffic.



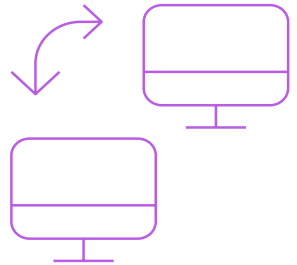
Route Tables

Control traffic patterns by overriding default system routes.



Service Endpoints

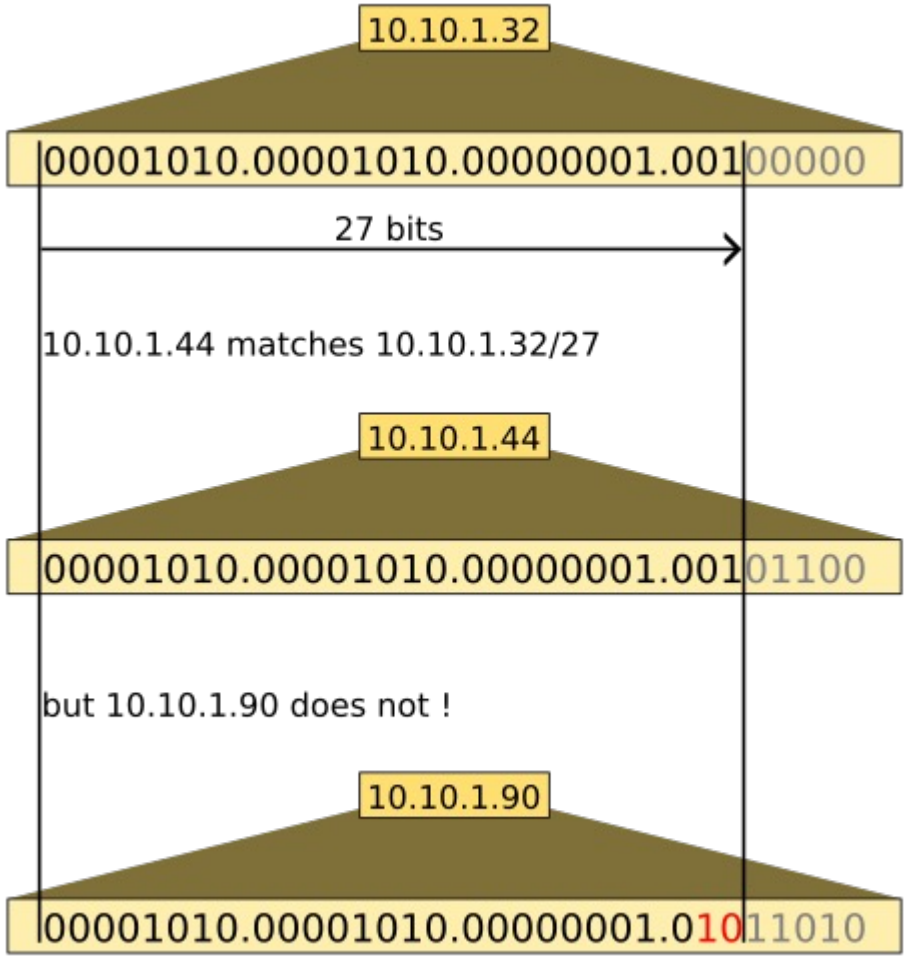
Securely connect to Azure PaaS services using private IPs.



VNet Peering

Connect VNets for seamless communication between networks.

VNET IP ADDRESSING – CIDR BLOCKS



https://upload.wikimedia.org/wikipedia/commons/thumb/7/7b/IP_Address_Match.svg/500px-IP_Address_Match.svg.png

Classless Inter-Domain Routing (CIDR): VNets are defined by a private IP address range in CIDR format (e.g., 10.0.0.0/16).

RFC 1918 Private IP Ranges: Use ranges like 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16 for internal networks.

Non-Overlapping Addresses: Ensure your VNet CIDR block does not overlap with any on-premises network or peered VNet CIDR blocks.

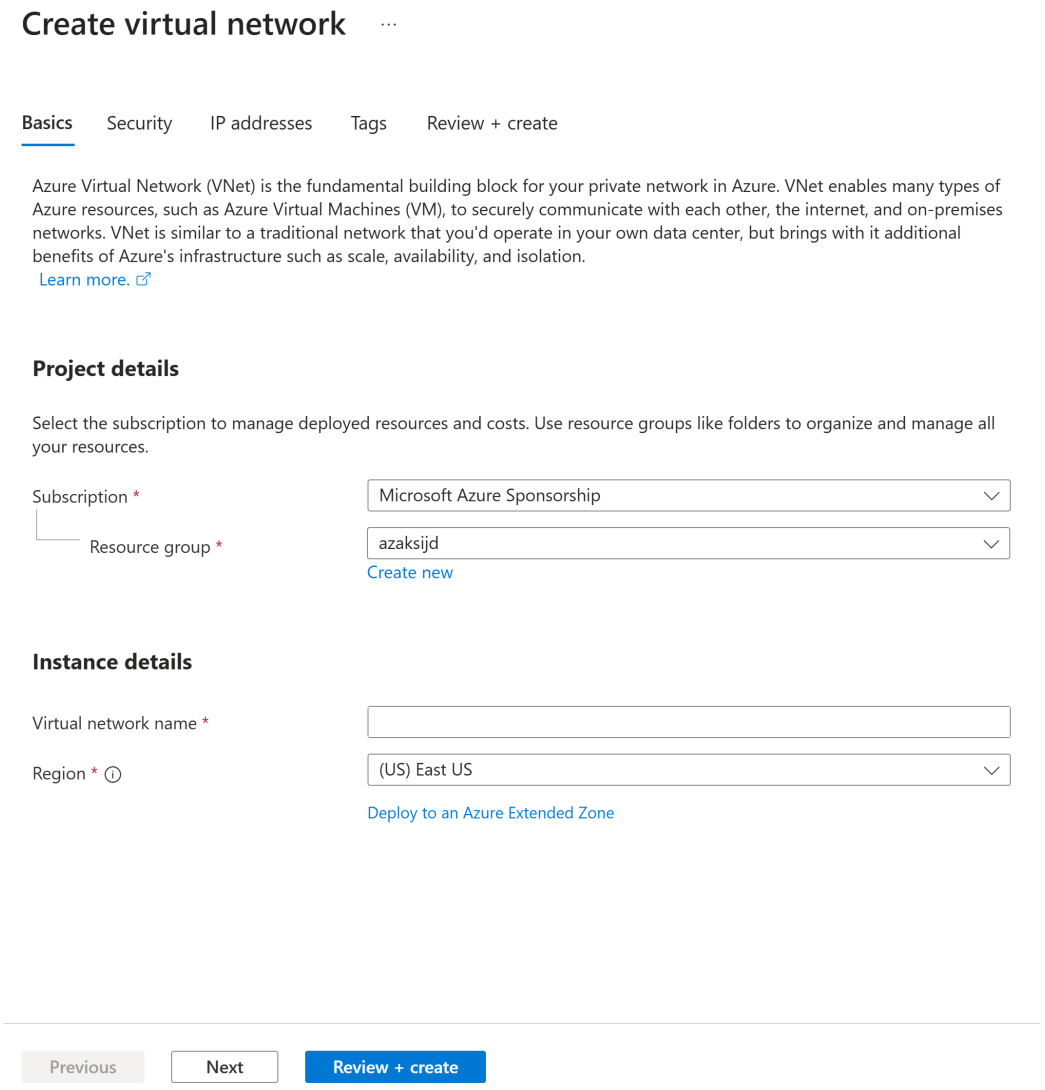
Future Growth Planning: Allocate a larger IP address space than immediately needed to accommodate future expansion.

Minimum VNet Size: A VNet must have at least a /29 CIDR block, though /24 or larger is more common for production.

VNET PLANNING

- **Address Space Alignment:** Align your VNet IP ranges with your corporate IP address management (IPAM) scheme.
- **Reserve Room for Growth:** Always allocate larger VNet address spaces than initially required, considering future services and peering.
- **Non-Overlapping Rule:** Strictly enforce non-overlapping IP address spaces across all VNets and on-premises networks.
- **Documentation:** Maintain clear documentation of VNet CIDR blocks, subnets, and their purposes.
- **Regional Design:** Consider whether a single VNet per region or multiple VNets per region (peered) suits your architecture.

LAB 1: CREATING AN AZURE VIRTUAL NETWORK



Azure Portal Navigation: Walkthrough of locating the Virtual Networks service in the Azure portal.

Basic Configuration: Define the VNet name, resource group, region, and initial address space.

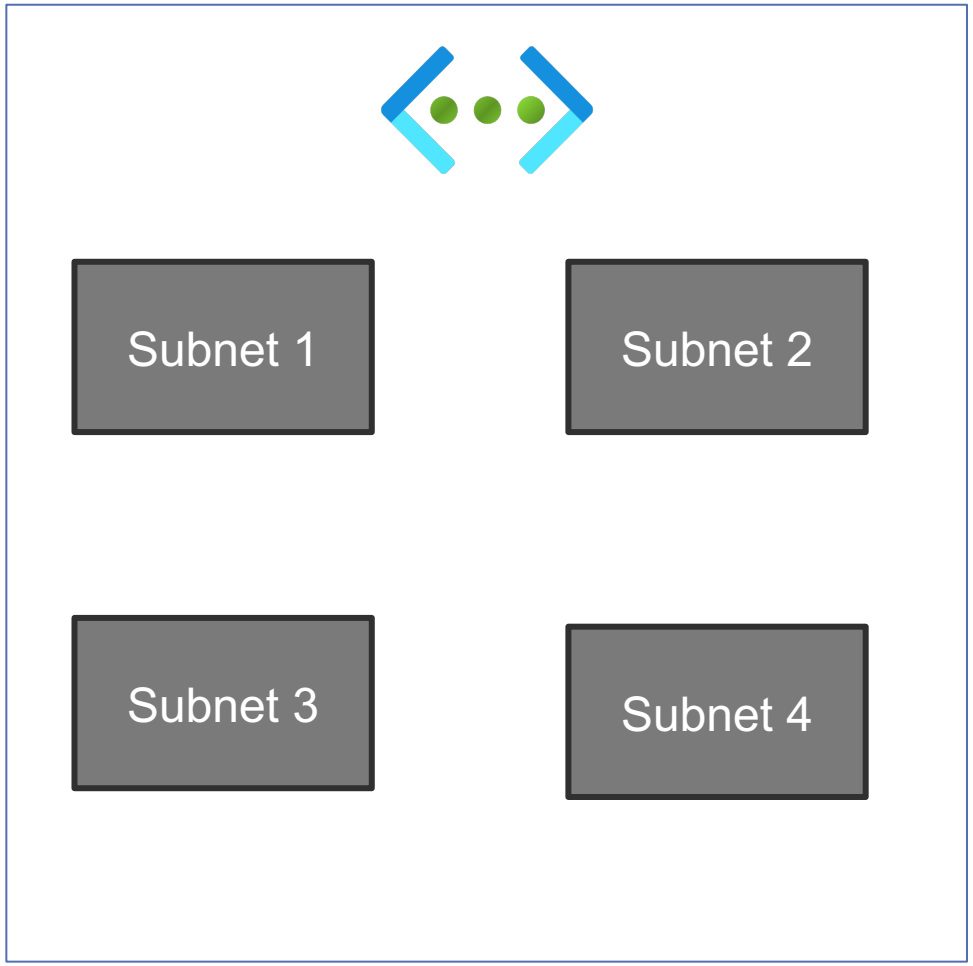
Adding Address Spaces: Add multiple, non-contiguous CIDR blocks to a VNet (if needed).

Initial Subnet Creation: Create a default subnet within the new VNet during creation.

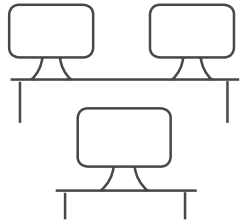
Review and Create: Final validation of settings before deployment.

AZURE SUBNETS- DIVIDING THE VNET

- **Logical Segmentation:** Subnets divide a VNet's IP address space into smaller, manageable segments.
- **Resource Isolation:** Resources within different subnets can be logically isolated for security or organizational purposes.
- **Service Delegation:** Certain Azure services (e.g., Azure Firewall, Application Gateway) require dedicated subnets.
- **Network Security Groups (NSGs):** NSGs are typically associated with subnets to filter traffic for all resources within it.
- **Routing Scope:** Subnets define the boundary for routing and network policy application.

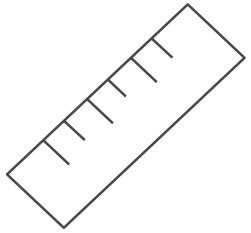


SUBNET ALLOCATION AND USAGE



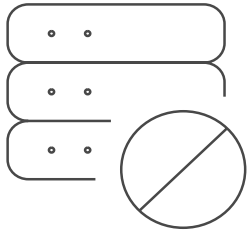
Contiguous IP Range

Subnets must have a contiguous IP address range that is a subset of the VNet's address space.



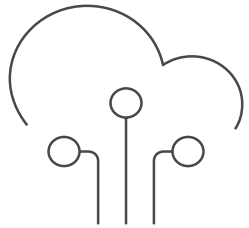
Minimum Size

The smallest subnet you can create in Azure is a /29, allowing for 8 IP addresses.



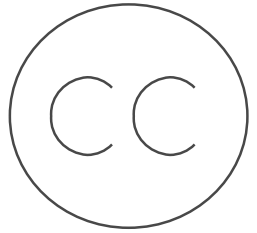
Reserved IP Addresses

Azure reserves 5 IP addresses within each subnet for internal use, including the first four and the last address.



Service-Specific Subnets

Plan dedicated subnets for Azure PaaS services that require network injection.



Naming Conventions

Implement clear and consistent naming conventions for your subnets to aid management.

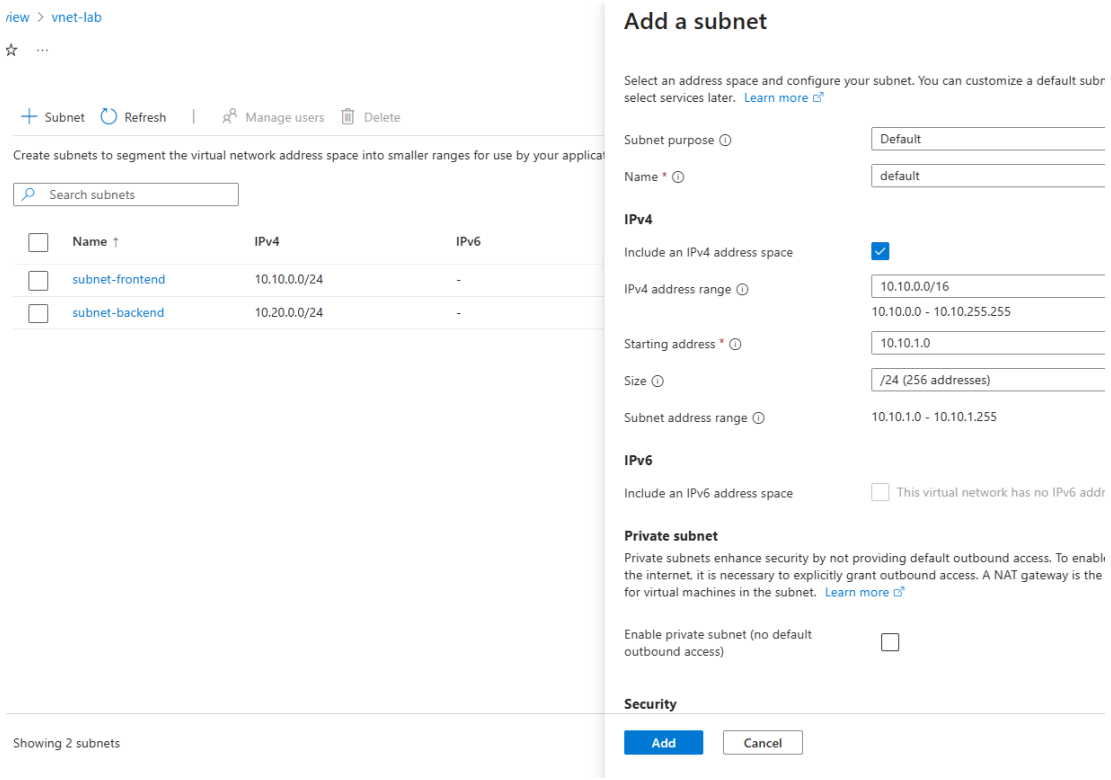
SUBNET DESIGN CONSIDERATIONS

- **Application Tiers:** Create separate subnets for different application tiers (e.g., web, application, database).
- **Security Boundaries:** Use subnets to enforce strong security boundaries with NSGs.
- **Scalability:** Ensure subnets are large enough to accommodate future growth of resources within them.
- **Service Requirements:** Identify and pre-plan subnets for specific Azure services that require delegation.
- **Network Flow:** Design subnets to optimize network traffic flow and minimize inter-subnet communication overhead.

RESERVED IP ADDRESSES IN SUBNETS

- Network Address
- Default Gateway
- Azure DNS IP (1st)
- Azure DNS IP (2nd)
- Broadcast address

LAB 2: CREATING SUBNETS IN AN EXISTING VNET



Accessing VNet Settings: Navigating to an existing VNet's subnets blade in the Azure portal.

Adding a New Subnet: Defining the subnet name and its contiguous address range.

Service Delegation: Demonstrating how to delegate a subnet to a specific Azure service (e.g., Azure Firewall).

Review and Save: Confirming the subnet configuration before creation.

Viewing Usable IPs: Highlighting how the portal displays the number of usable IPs after Azure's reservations.

PUBLIC VS PRIVATE IP ADDRESSES

Private IP Addresses: Assigned to resources within a VNet for internal communication, not directly reachable from the internet.

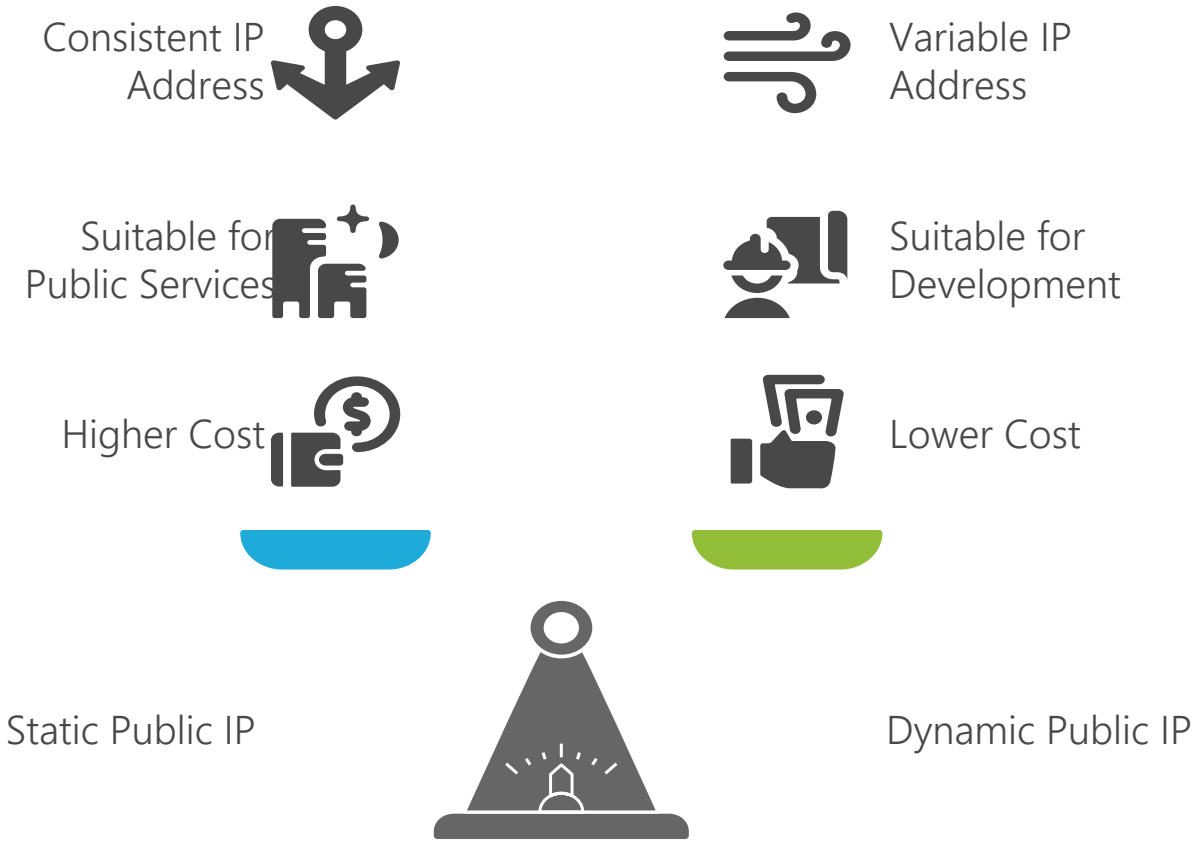
Public IP Addresses (PIP): Assigned to resources that need internet-facing connectivity, globally unique and routable.

Network Address Translation (NAT): Azure uses NAT to translate private IPs to public IPs for outbound internet access.

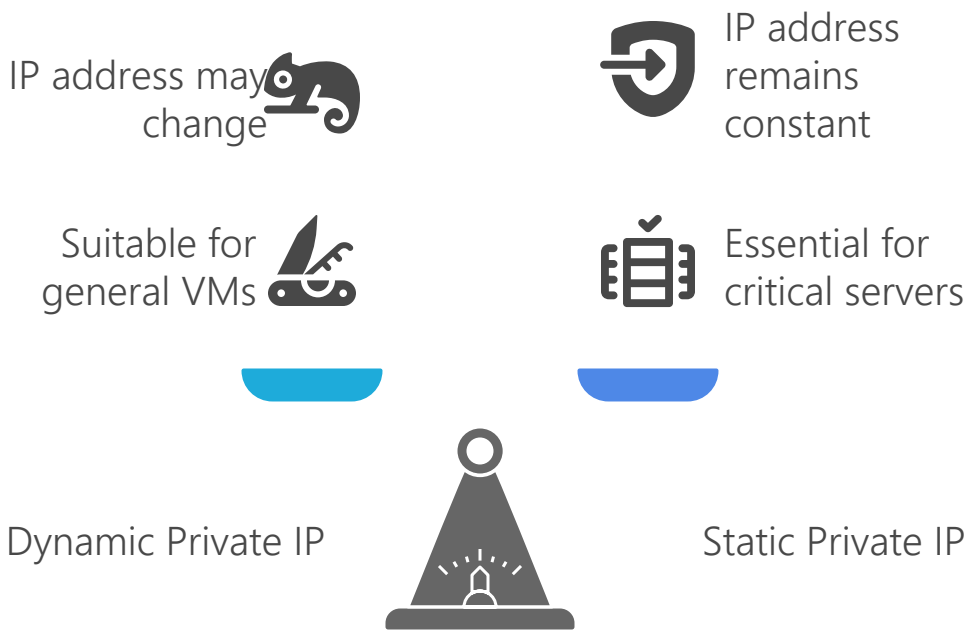
Internal Communication: Most Azure resources communicate using private IP addresses within VNets or peered VNets.

External Access: Public IPs are essential for web servers, public load balancers, or VPN gateways requiring internet exposure.

PUBLIC IP ADDRESSES – STATIC VS. DYNAMIC



PRIVATE IP ADDRESSES – STATIC VS. DYNAMIC ASSIGNMENT



IP ADDRESS ALLOCATION METHODS

Network Interface (NIC) Level: Both public and private IP addresses are primarily associated with a VM's Network Interface.

Primary vs. Secondary IP: Each NIC has a primary private IP, and you can add secondary private IPs.

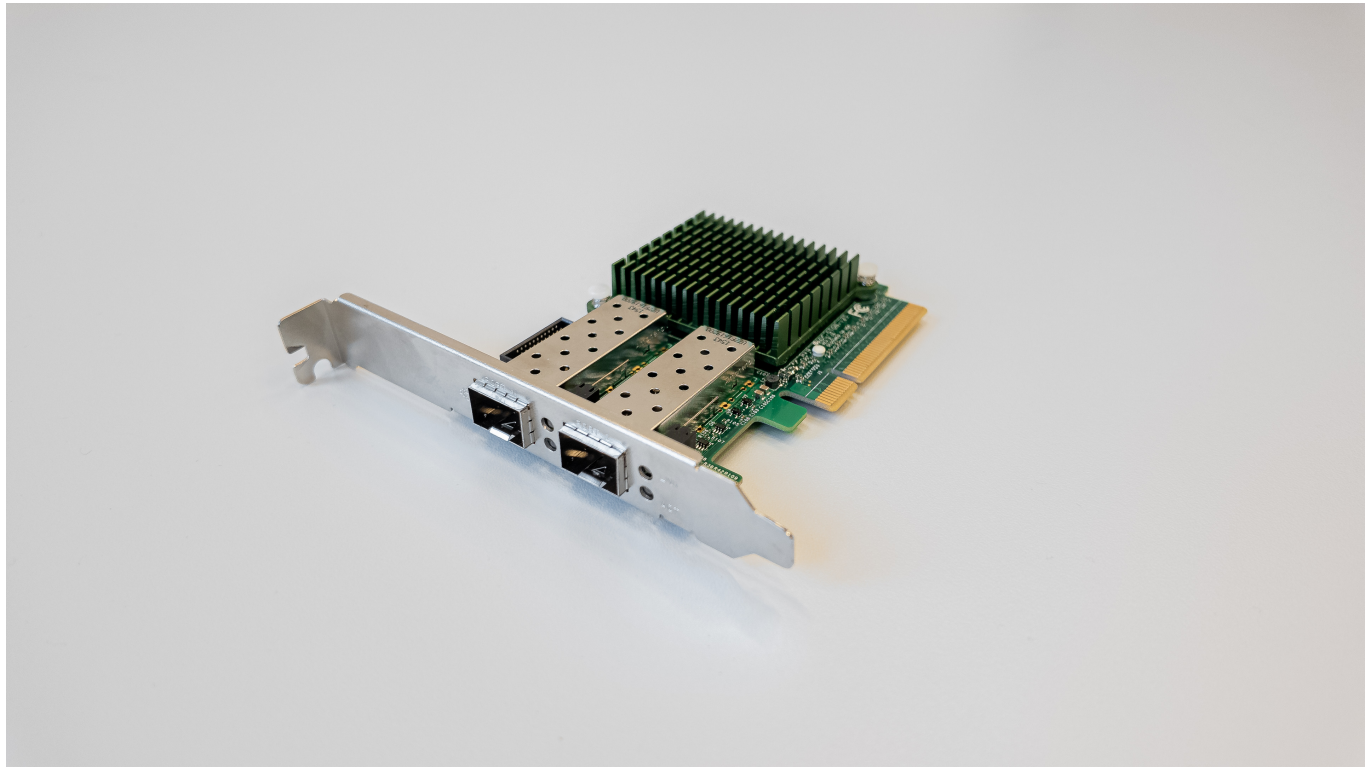
Multiple NICs per VM: A VM can have multiple NICs, each with its own IP configurations.

IP Configuration Object: IP addresses are represented as 'IP configurations' within the NIC resource.

Azure Services with Direct IP: Some Azure services, like Load Balancers, Application Gateways, also have IP addresses directly associated with them.

NETWORK INTERFACES (NICS)

- **VM Connectivity:** A Network Interface Card (NIC) connects an Azure Virtual Machine to a Virtual Network.
- **Essential Component:** Every Azure VM requires at least one NIC to communicate with other resources.
- **IP Configuration:** Each NIC holds one or more IP configurations, defining its private and optional public IP addresses.
- **NSG Association:** NICs can be directly associated with a Network Security Group for granular security rules.
- **Multiple NICs:** VMs can support multiple NICs, allowing for complex network topologies or management/data plane separation.



AZURE ROUTES – SYSTEM ROUTES

Understanding how traffic flows in Azure starts with System Routes. Azure's network fabric provides automatic routing for many common communication patterns.

UNDERSTANDING DEFAULT SYSTEM ROUTES

0.0.0.0/0 (Internet): Default route for all traffic not explicitly covered by other routes, points to Azure's internet gateway.

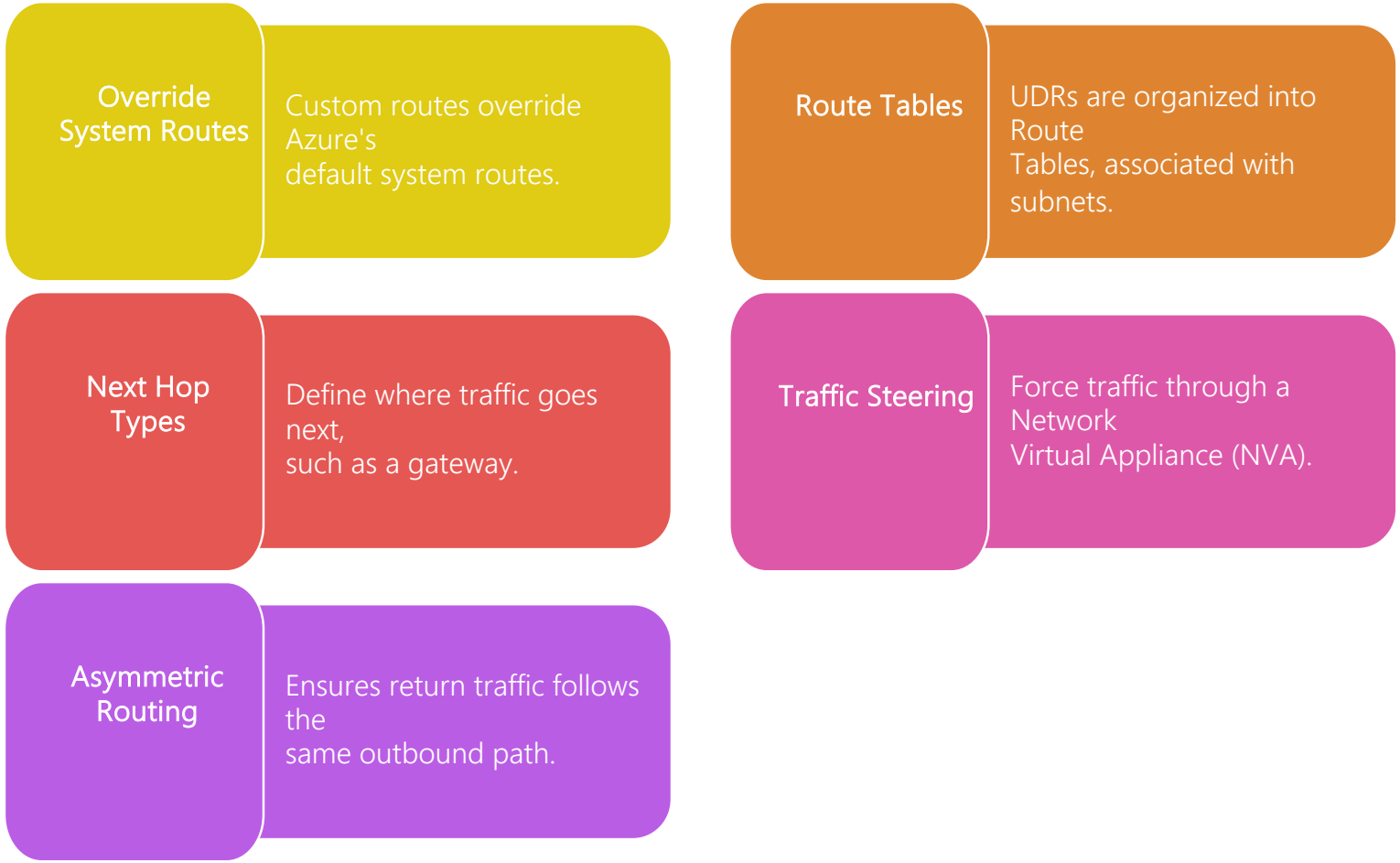
VNet Address Space: Route to direct traffic within the same VNet's address space to the local VNet gateway.

Peered VNet Address Spaces: Routes are automatically added for peered VNets once peering is established.

Virtual Network Gateway: If a VPN Gateway or ExpressRoute is configured, a route to the on-premises network is automatically added.

No Explicit Configuration: These system routes are managed by Azure and do not require user configuration.

USER DEFINED ROUTES



UDR NEXT HOP TYPES

Virtual Appliance: Directs traffic to a private IP address of a network virtual appliance (NVA) within the VNet.

Virtual Network Gateway: Directs traffic to an Azure VPN Gateway or ExpressRoute Gateway for on-premises connectivity.

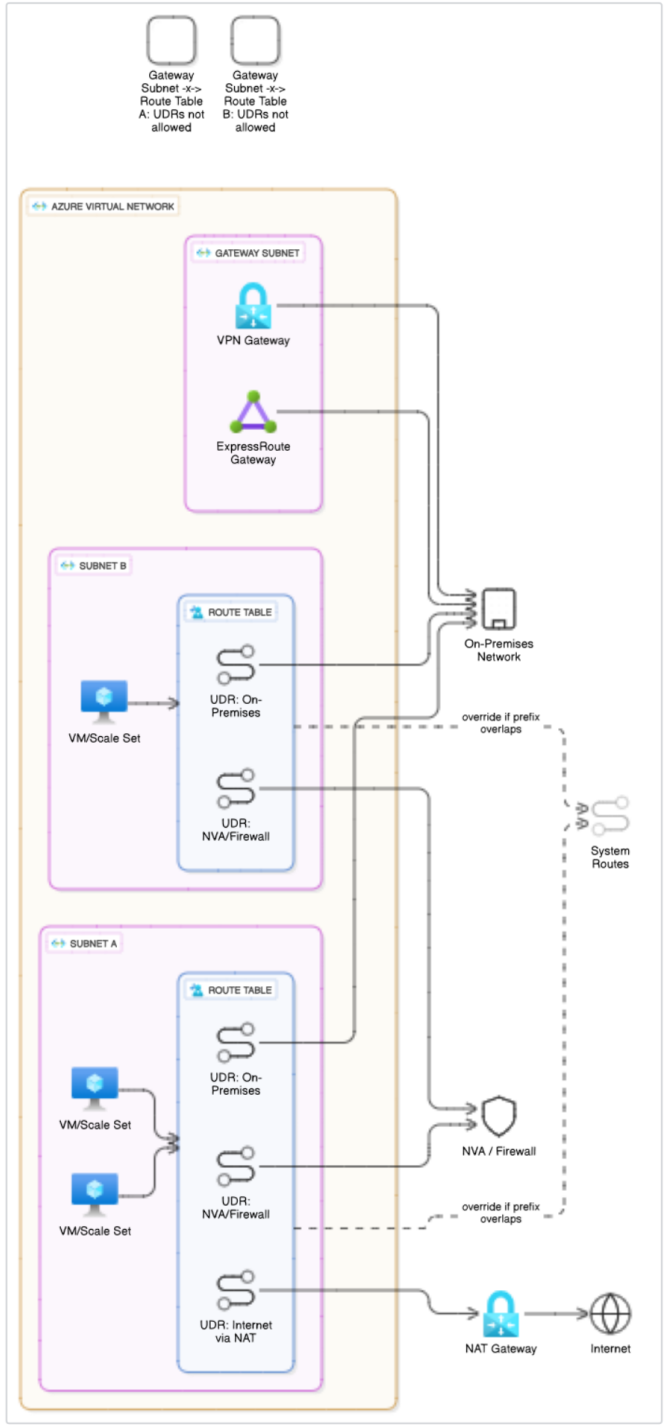
VNet Peering: Directs traffic to a peered VNet, used when custom routing is needed across peered networks.

Internet: Directs traffic to the internet, overriding the default Azure internet route for specific prefixes.

None: Blackholes traffic, dropping packets for the specified address prefix, preventing it from reaching its destination.

APPLYING UDRS TO SUBNETS

- **Subnet-Specific Application:** Route Tables containing UDRs are associated with individual subnets.
- **Effective Routes:** The most specific route always wins; UDRs override system routes for overlapping prefixes.
- **No Multiple Route Tables:** A single subnet can only be associated with one Route Table at a time.
- **Impact on All Resources:** All resources within a subnet associated with a Route Table will adhere to its UDRs.
- **Gateway Subnet Exception:** UDRs cannot be applied to the Gateway Subnet (where VPN/ExpressRoute gateways reside).



ROUTE TABLE ASSOCIATION BEST PRACTICES

- **Centralized Control:** Consolidate UDRs into a few well-defined Route Tables rather than many small ones.
- **Per-Subnet Needs:** Design route tables based on the specific routing requirements of each subnet.
- **Audit and Monitor:** Regularly audit effective routes for your network interfaces to ensure traffic flows as expected.
- **Security Zones:** Use UDRs to enforce traffic inspection by routing all outbound/inbound traffic through a firewall subnet.
- **Hybrid Connectivity:** Ensure UDRs correctly direct traffic between Azure and on-premises via your VPN Gateway/ExpressRoute.

LAB 3: IMPLEMENTING USER-DEFINED ROUTES

Creating a Route Table: Steps to provision a new Route Table resource in Azure.

Adding UDRs: Demonstrating how to add specific routes, defining destination prefix and next hop type.

Associating with a Subnet: Linking the newly created Route Table to a target subnet.

Verifying Effective Routes: Using the 'Effective routes' blade on a VM's NIC to confirm UDR application.

Traffic Flow Testing: Brief overview of how to test if traffic is now correctly flowing via the UDR.

AZURE NAT GATEWAY – OUTBOUND CONNECTIVITY

Azure NAT Gateway is a fully managed, highly resilient service that provides Network Address Translation.

WHY USE AZURE NAT GATEWAY

Simplified Outbound Connectivity: Centralized and simplified management of outbound internet access for multiple VMs or containers.

Improved Security: Eliminates the need for individual public IPs on VMs, reducing attack surface.

Predictable Public IPs: Provides static public IP addresses for outbound traffic, useful for whitelisting by external services.

Eliminates SNAT Port Exhaustion: Addresses a common issue with traditional load balancers by providing abundant SNAT ports.

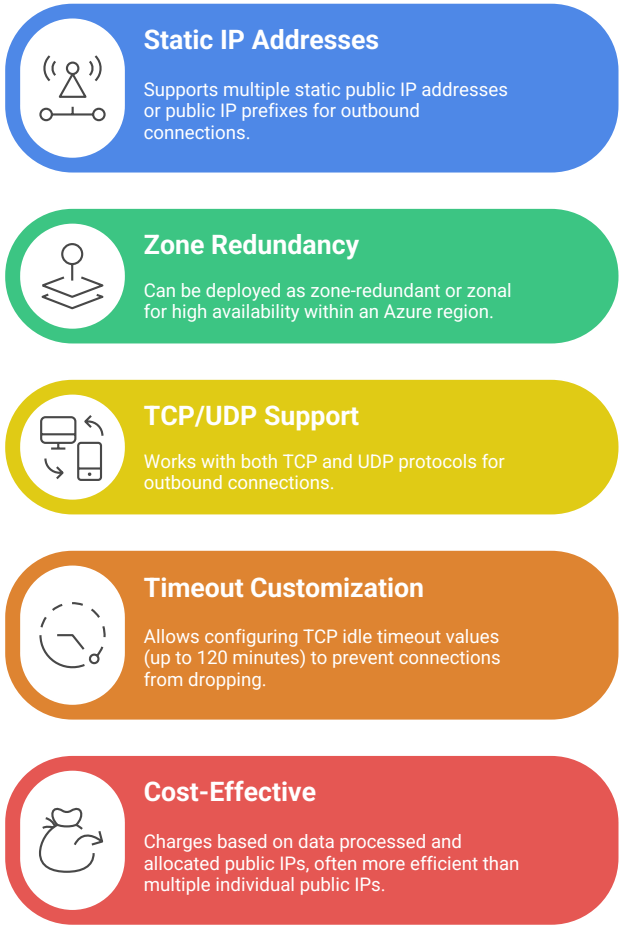
Enhanced Reliability: Managed service with built-in high availability and resilience, no single point of failure.

NAT GATEWAY FEATURES AND BENEFITS

Azure NAT Gateway offers several compelling features and benefits.

It supports not just single static public IP addresses but also entire public IP prefixes for your outbound traffic, giving you flexibility.

For high availability, it can be deployed as zone-redundant, spanning multiple Azure Availability Zones, or as zonal, pinned to a specific zone.



NAT GATEWAY DESIGN CONSIDERATIONS

Subnet Scope: A NAT Gateway should be associated with specific subnets; a subnet can only have one NAT Gateway.

Public IP Prefix: Consider using a public IP prefix for your NAT Gateway for easier IP management and whitelisting.

Avoid Overlap: Ensure NAT Gateway doesn't conflict with other outbound methods like load balancer rules or VM public IPs.

Regional Deployment: Deploy NAT Gateway in the same region as the VNet it serves for optimal performance.

No Inbound Rules: Remember NAT Gateway is for outbound only; pair it with NSGs or load balancers for inbound access.

NAT GATEWAY VS. PUBLIC IP ON VM

Public IP on VM: Direct inbound and outbound connectivity; limited SNAT ports per VM.

Public IP on VM: Direct inbound and outbound connectivity; limited SNAT ports per VM.

NAT Gateway: Outbound-only; massive shared SNAT port pool across subnet resources.

NAT Gateway: No inbound mapping; typically paired with Load Balancers/Application Gateways for inbound.

Security: Public IP on VM increases individual VM exposure; NAT Gateway centralizes and limits exposure.

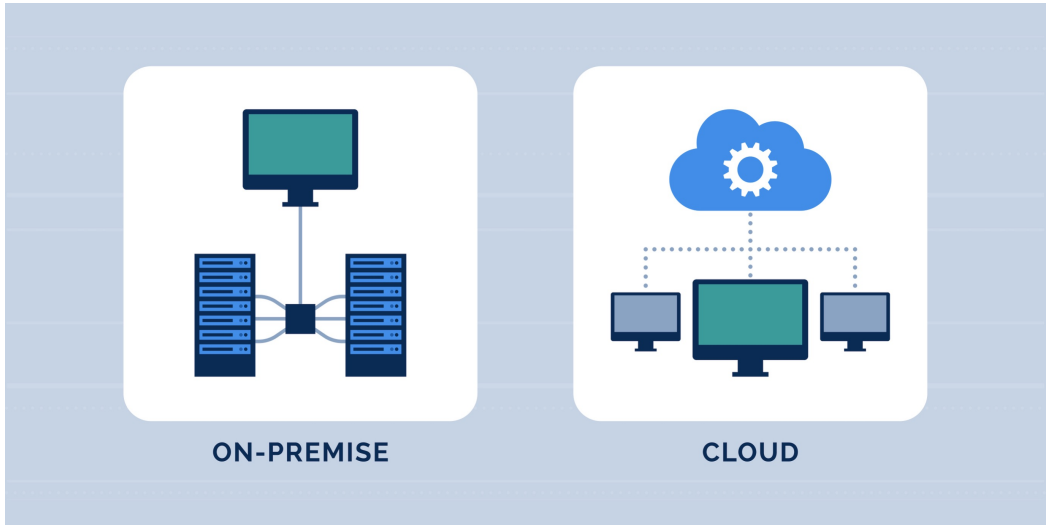
Scalability: Public IP on VM scales outbound capacity per VM; NAT Gateway scales across entire subnets.

Management: Individual management for each VM's public IP; centralized management for subnet outbound.

LAB 4: DEPLOYING AZURE NAT GATEWAY

- **Creating a NAT Gateway Resource:** Walkthrough of provisioning the NAT Gateway in the portal.
- **Attaching Public IP Address/Prefix:** Associating a static public IP or a public IP prefix to the NAT Gateway.
- **Selecting Subnets:** Linking the NAT Gateway to the desired subnets for outbound routing.
- **Configuring Idle Timeout:** Adjusting the TCP idle timeout value for long-lived connections.
- **Verifying Outbound IP:** Demonstrating how to confirm that VMs in the associated subnet are now using the NAT Gateway's public IP for outbound.

ON-PREMISES NETWORKING VS. AZURE NETWORKING



Hardware vs. Software: On-prem relies on physical hardware; Azure is entirely software-defined networking (SDN).

CapEx vs. OpEx: On-prem is capital expenditure; Azure shifts to operational expenditure (pay-as-you-go).

Fixed vs. Elastic Capacity: On-prem requires over-provisioning; Azure offers dynamic, on-demand scalability.

Manual vs. Automated Deployment: On-prem often manual; Azure enables Infrastructure as Code (IaC) and automation.

Direct Access vs. API Driven: On-prem allows direct hardware access; Azure is managed purely via APIs/portal.

NETWORK INFRASTRUCTURE MANAGEMENT

On-Premises:

- **Procurement & Installation:** You handle purchasing, racking, and cabling network devices.
- **Configuration & Maintenance:** Manual configuration of devices, patching, and lifecycle management.
- **Troubleshooting Hardware:** Diagnosing physical failures and replacing faulty components.
- **Capacity Planning:** Forecasting long-term needs and investing in hardware years in advance.
- **Power & Cooling:** Responsible for environmental factors of your network hardware.

Azure:

- **Abstracted Infrastructure:** Azure manages the underlying physical network infrastructure.
- **API-Driven Configuration:** Network components configured programmatically via Azure Portal, CLI, PowerShell, or IaC.
- **Service Health:** Azure monitors and alerts on network service health; no hardware troubleshooting for you.
- **On-Demand Scaling:** Network capacity scales dynamically without user intervention for underlying infrastructure.
- **Global Footprint:** Leverage Azure's global network backbone without building it yourself.

IP ADDRESS MANAGEMENT

On-Premises:

- **Manual IPAM:** Often relies on spreadsheets or dedicated IPAM software for address allocation.
- **DHCP/Static Assignment:** Mix of dynamic (DHCP) and manual static IP assignments.
- **DNS Integration:** Manual integration of DNS records with IP changes.
- **Physical Constraints:** IP ranges often tied to physical locations or VLANs.
- **Auditing Complexity:** Tracking IP usage and availability can be complex

Azure:

- **VNet/Subnet Allocation:** Azure automatically manages IP allocation within defined VNet and subnet ranges.
- **Dynamic/Static Options:** Choice of dynamic or static assignment at the NIC level.
- **Azure DNS Integration:** Seamless integration with Azure DNS for both public and private zones.
- **Logical Boundaries:** IP ranges are defined by logical VNets and subnets, not physical location.
- **Azure Tools:** Azure Portal, CLI, PowerShell, Azure Resource Graph for auditing IP usage.

CONNECTIVITY OPTIONS

On-Premises:

- **Site-to-Site VPN:** Connects networks over the internet, often using dedicated VPN appliances.
- **Direct Connect/MPLS:** Private, dedicated lines for highly secure and performant connections (e.g., MPLS).
- **Router Configuration:** Manual configuration of routers and firewalls for inter-site connectivity.
- **Limited Bandwidth:** Internet-based VPNs can be limited by internet connection speeds.
- **Cost of Hardware:** Upfront cost for VPN appliances and potentially leased lines.

Azure:

- **Azure VPN Gateway:** Managed service for site-to-site (IPsec), point-to-site (OpenVPN/IKEv2), and VNet-to-VNet VPN.
- **Azure ExpressRoute:** Dedicated, private, high-bandwidth connection from your premises to Azure's network backbone.
- **Managed Service:** Azure handles the underlying infrastructure for VPN Gateway and ExpressRoute circuits.
- **Scalable Bandwidth:** VPN Gateway supports various throughputs; ExpressRoute offers up to 100 Gbps.
- **Consumption-Based:** Pay for VPN Gateway instance and ExpressRoute circuit based on usage and speed.

CONNECTIVITY OPTIONS

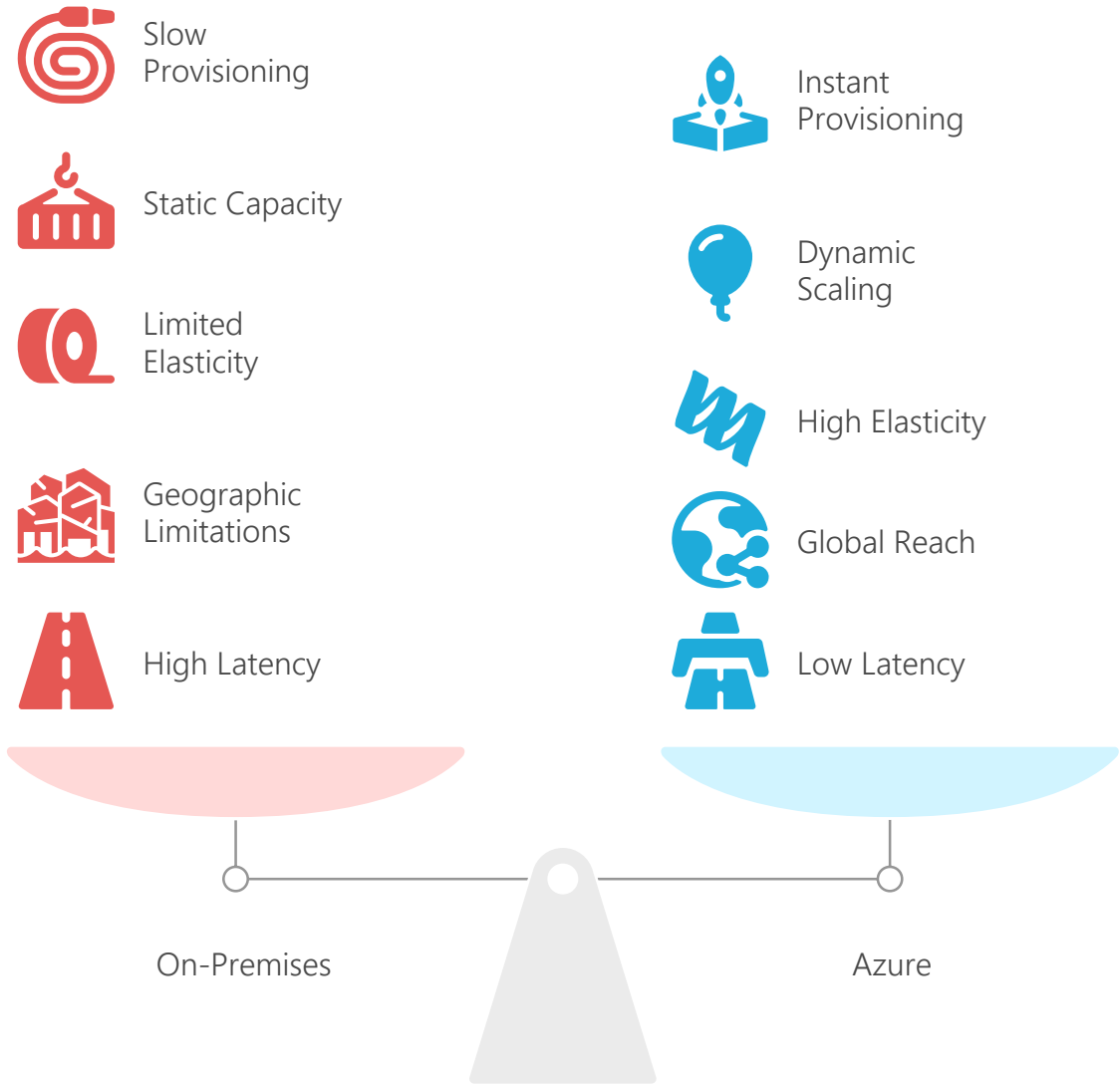
On-Premises:

- **Perimeter-Focused:** Heavily relies on a strong perimeter firewall and physical security.
- **Manual Configuration:** Security policies typically configured manually on individual devices.
- **Patching Responsibility:** You are responsible for patching OS, firmware, and security software.
- **Limited Threat Intelligence:** Rely on in-house or third-party tools for threat detection.
- **Physical Security:** Your responsibility to secure the data center physically.

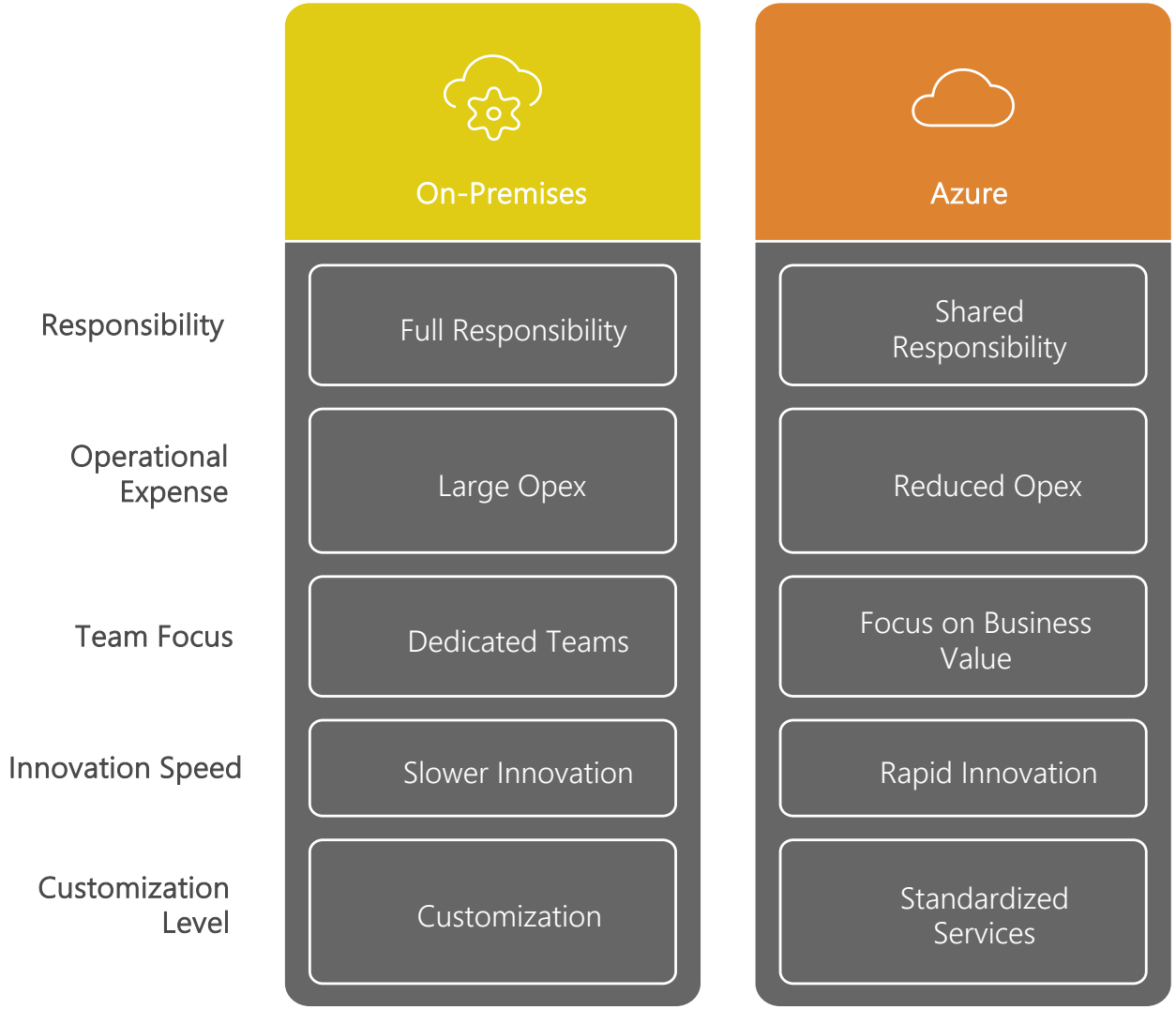
Azure:

- **Defense-in-Depth:** Multi-layered security built into the platform, from physical to application layer.
- **Policy-Driven:** Security policies (NSGs, Azure Firewall, Azure Policy) defined as code and centrally managed.
- **Shared Responsibility Model:** Azure manages platform security; you manage security of your data and applications.
- **Integrated Threat Intelligence:** Leverages Microsoft's global threat intelligence via Azure Security Center, Azure DDoS Protection.
- **Physical Security:** Azure handles physical data center security.

SCALABILITY AND AGILITY



OPERATIONAL MODELS



POP QUIZ:

A network engineer needs to connect an Azure Virtual Machine (VM) to an existing Azure Virtual Network (VNet). Which Azure networking component is essential for this VM to communicate within the VNet?

A. Azure Load Balancer
B. Azure Network Security Group (NSG)
C. Azure Network Interface (NIC)
D. Azure Public IP Address

POP QUIZ:

A network engineer needs to connect an Azure Virtual Machine (VM) to an existing Azure Virtual Network (VNet). Which Azure networking component is essential for this VM to communicate within the VNet?

A. Azure Load Balancer
B. Azure Network Security Group (NSG)
C. Azure Network Interface (NIC)
D. Azure Public IP Address

POP QUIZ:

You are designing an Azure Virtual Network (VNet) for a new application. You plan to use the address space 10.0.0.0/16. You then create a subnet named 'AppSubnet' with the address range 10.0.1.0/24. How many usable IP addresses will be available in the 'AppSubnet' for your virtual machines?

A. 256
B. 251
C. 254
D. 253

POP QUIZ:

You are designing an Azure Virtual Network (VNet) for a new application. You plan to use the address space 10.0.0.0/16. You then create a subnet named 'AppSubnet' with the address range 10.0.1.0/24. How many usable IP addresses will be available in the 'AppSubnet' for your virtual machines?

A. 256
B. 251
C. 254
D. 253

POP QUIZ:

Your Azure Virtual Machine (VM) in SubnetA needs to send all its outbound internet traffic through a Network Virtual Appliance (NVA) located in SubnetB within the same Virtual Network. Which Azure networking component should you use to achieve this traffic steering?

A. Network Security Group (NSG)
B. Application Security Group (ASG)
C. User-Defined Route (UDR)
D. Azure NAT Gateway

POP QUIZ:

Your Azure Virtual Machine (VM) in SubnetA needs to send all its outbound internet traffic through a Network Virtual Appliance (NVA) located in SubnetB within the same Virtual Network. Which Azure networking component should you use to achieve this traffic steering?

A. Network Security Group (NSG)
B. Application Security Group (ASG)
C. User-Defined Route (UDR)
D. Azure NAT Gateway

CLOUD NETWORKING SECURITY

OBJECTIVES

- **Implement Azure RBAC for Network Resources:** Assign appropriate permissions for network management.
- **Configure Network Security Groups (NSGs):** Create and apply rules for granular traffic filtering.
- **Leverage Application Security Groups (ASGs):** Simplify and scale NSG rule management using logical groupings.
- **Deploy and Manage Azure Firewall:** Understand its capabilities for centralized network security.
- **Secure PaaS Connectivity:** Implement Service Endpoints and Private Link for private access to Azure services.
- **Understand DDoS Protection:** Recognize the importance and types of DDoS protection in Azure.

AZURE ROLE-BASED ACCESS CONTROL (RBAC)

Granular Permissions: Control who can create, modify, or delete specific Azure network resources.

Built-in Roles: Leverage predefined roles like "Network Contributor," "Network Reader," and "Classic Network Contributor."

Custom Roles: Create tailored roles for specific network administration tasks if built-in roles don't suffice.

Least Privilege Principle: Assign only the necessary permissions required to perform a specific task.

Scope of Assignment: Apply RBAC assignments at different scopes: subscription, resource group, or individual resource.

BUILT-IN NETWORK RBAC ROLES

- **Network Contributor:** Manages network resources but not access to them. Ideal for network administrators.
- **Network Reader:** Can view all network resources but cannot make any changes. Useful for auditing or monitoring roles.
- **Contributor:** Can manage everything except access to Azure resources. Includes network resource management.
- **Owner:** Can manage everything, including access to resources. Full control, typically limited to very few.
- **Virtual Machine Contributor:** Allows managing virtual machines, including their network interfaces.

MANAGED IDENTITIES FOR AZURE RESOURCES

This feature provides Azure services with an automatically managed identity in Azure Active Directory, eliminating the need for developers to manage credentials like connection strings or API keys directly in their code.

There are two types: a **System-Assigned Identity** is tied directly to the lifecycle of a specific Azure resource, like a Virtual Machine or a Logic App.

A **User-Assigned Identity** is a standalone Azure resource that can be created once and then assigned to multiple Azure resources.

- Managed by Azure
- Easily revoked
- Auto-rotated
- No credentials!

LAB 5: ASSIGNING NETWORK RBAC ROLE

- **Accessing IAM Blade:** Navigating to the Access Control (IAM) blade of a Network Resource Group or VNet.
- **Adding Role Assignment:** Demonstrating how to add a new role assignment.
- **Selecting Role:** Choosing a built-in role like "Network Contributor" or "Network Reader."
- **Assigning to User/Group/Managed Identity:** Selecting the security principal (user, group, or managed identity).
- **Verifying Permissions:** Briefly showing how assigned permissions affect resource management.

NETWORK SECURITY GROUPS – THE FUNDAMENTAL FIREWALL

Layer 4 Filtering: NSGs filter network traffic at the IP address and port level (Layer 4 of OSI model).

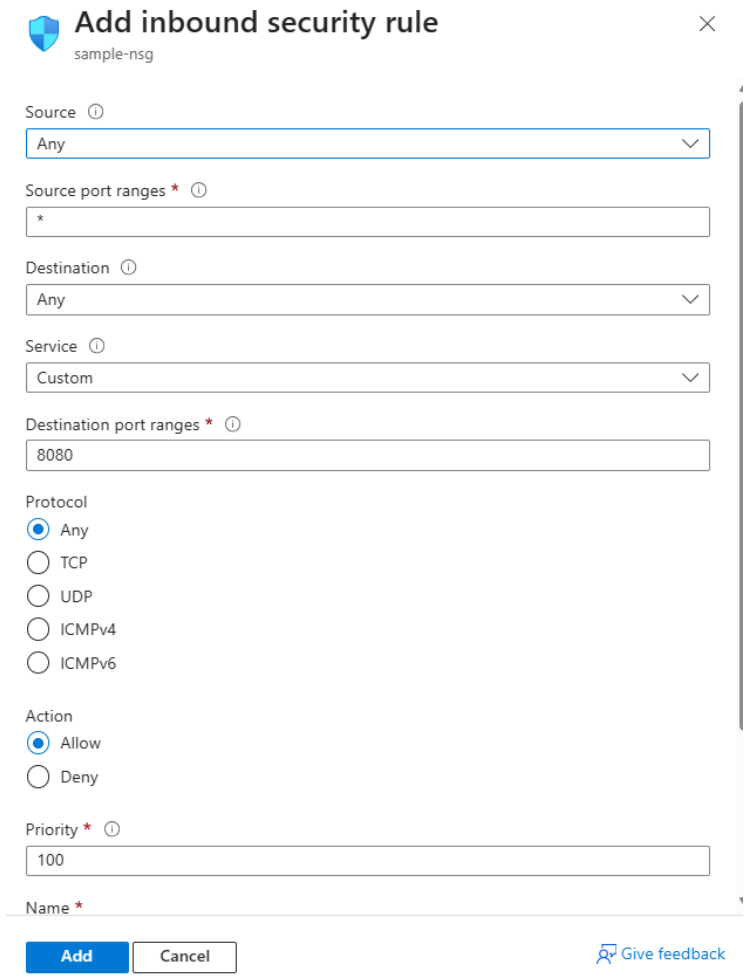
Inbound and Outbound Rules: Define rules for both incoming and outgoing traffic.

Priority-Based Evaluation: Rules are processed in numerical order by priority (lowest number = highest priority).

Allow/Deny Actions: Each rule specifies whether to 'Allow' or 'Deny' traffic.

Stateful Inspection: NSGs are stateful, meaning return traffic for an allowed outbound connection is automatically permitted.

NSG RULE COMPONENTS



Name: A unique name for the NSG rule within its group.

Priority: A number (100-4096) determining the order of rule evaluation; lower numbers are higher priority.

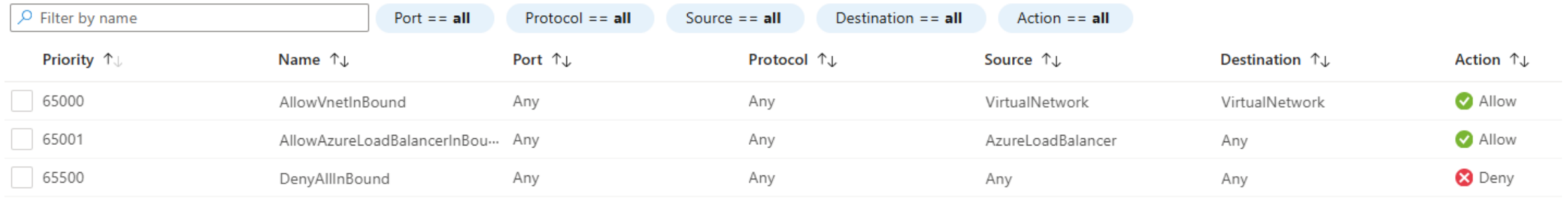
Source/Destination: IP addresses, CIDR blocks, Service Tags, or Application Security Groups.

Source/Destination Port Ranges: Specific ports (e.g., 80, 443) or port ranges (e.g., 20-22).

Protocol: TCP, UDP, ICMP, or Any.

Action: Allow or Deny.

DEFAULT NSG RULES



Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBou···	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

InboundDefault:

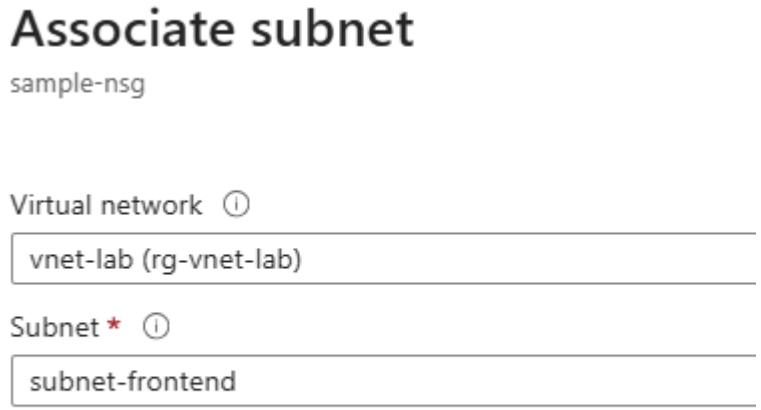
AllowVNetInbound (Priority 65000): Allows traffic within the VNet.
AllowAzureLoadBalancerInbound (Priority 65001): Allows traffic from Azure Load Balancer.
DenyAllInbound (Priority 65500): Denies all other inbound traffic.

OutboundDefault:

AllowVNetOutBound (Priority 65000): Allows traffic within the VNet.
AllowInternetOutBound (Priority 65001): Allows all outbound internet traffic.
DenyAllOutbound (Priority 65500): Denies all other outbound traffic.

NSG ASSOCIATION SCOPE

- **Subnet Association:** Apply an NSG to an entire subnet; rules affect all resources within that subnet.
- **NIC Association:** Apply an NSG directly to a Virtual Machine's Network Interface Card (NIC); rules affect only that specific NIC.
- **Combined Effect:** When both subnet and NIC NSGs are applied, both sets of rules are evaluated.
- **Order of Evaluation (Inbound):** Inbound traffic evaluates Subnet NSG first, then NIC NSG.
- **Order of Evaluation (Outbound):** Outbound traffic evaluates NIC NSG first, then Subnet NSG.
- **Effective Security Rules:** Use the 'Effective Security Rules' blade on a NIC to see the combined rules in effect.



NSG BEST PRACTICES

Granular Rules: Define rules that are as specific as possible (e.g., specific port and IP) to reduce attack surface.

Least Privilege: Only open ports and protocols that are absolutely necessary for communication.

Subnet-level First: Apply NSGs at the subnet level where possible for broader control and consistency.

Application Security Groups (ASGs): Use ASGs to simplify rule management for groups of VMs (covered next).

Audit and Log: Enable NSG flow logs to monitor traffic and review security effectiveness.

APPLICATION SECURITY GROUPS

To simplify NSG rule management, especially in larger or more dynamic environments, Azure introduced Application Security Groups, or ASGs.

ASGs allow you to logically group Virtual Machines by their application workload.

ASG EXAMPLE SCENARIO

Scenario: Allow WebServers to talk to AppServers on port 8080.
Without ASG: Requires individual IP addresses of each WebServer and AppServer in rules, cumbersome to maintain.
With ASG:

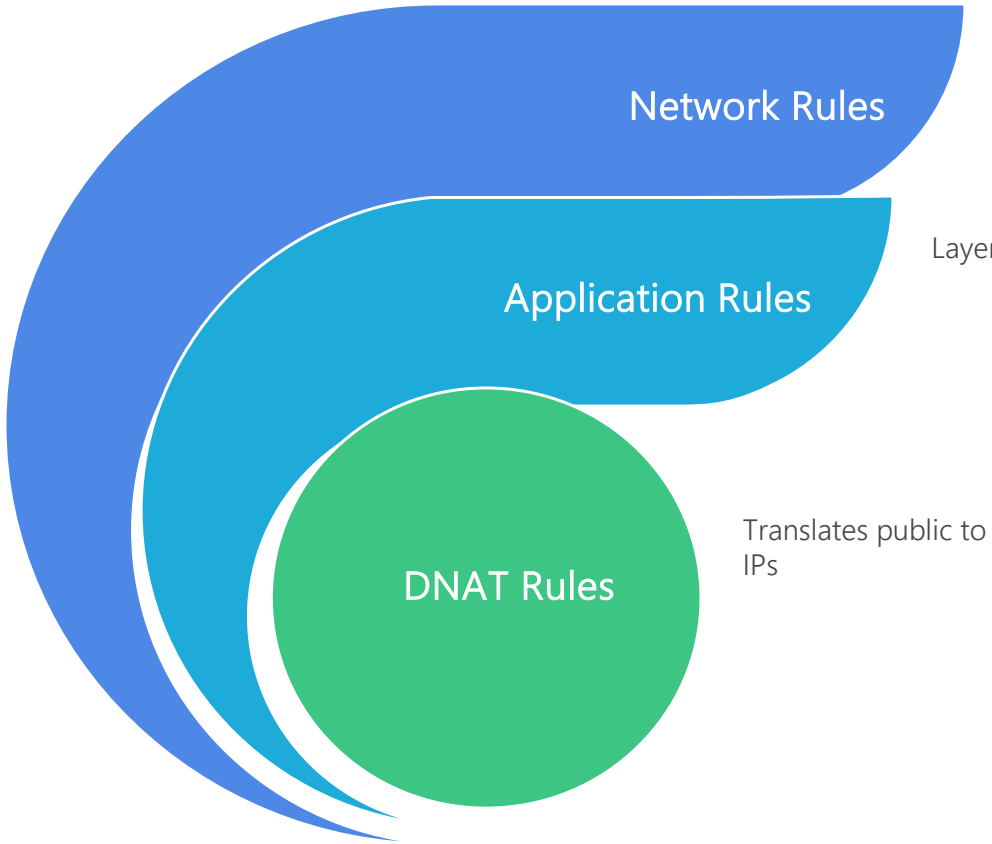
- Create WebServersASG.
- Create AppServersASG.
- Create NSG Rule:
  - Source: WebServersASG
  - Destination: AppServersASG
  - Destination Port: 8080
  - Action: Allow

Benefit: Add or remove VMs from respective ASGs without touching the NSG rule.

AZURE FIREWALL – CENTRALIZED NETWORK SECURITY

For centralized, enterprise-grade network security, Azure Firewall is your go-to service. It's a fully managed, stateful firewall as a service, specifically designed for cloud environments.

AZURE FIREWALL RULE TYPES



Layer 3/4 filtering for all traffic

Layer 7 filtering for web apps

Translates public to private IPs

AZURE FIREWALL DEPLOYMENT MODES

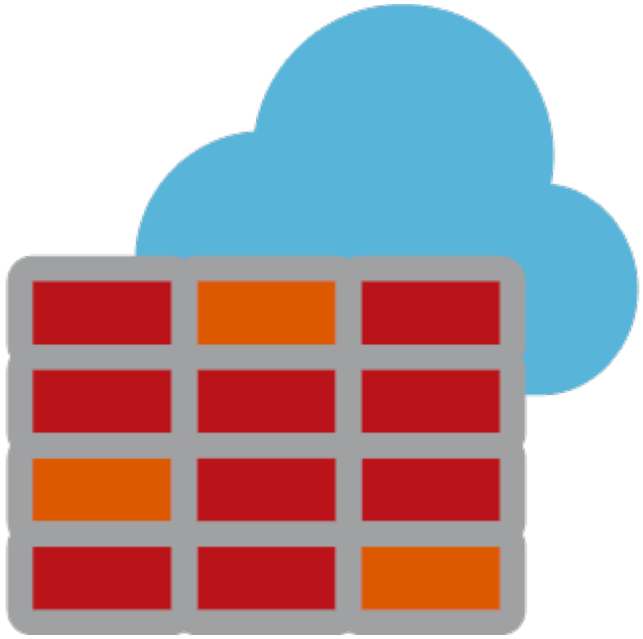
Centralized Deployment (Hub-Spoke):

Firewall deployed in a central "hub" VNet.
Spoke VNets (where workloads reside) are peered to the hub.
UDRs in spoke VNets force all traffic (internet, on-prem, VNet-to-VNet) through the firewall.
Benefits: Centralized security management, reduced cost, consistent policy.

Distributed Deployment (Per-VNet):

Firewall deployed in each workload VNet.
Benefits: Isolated security policies, potentially simpler routing for smaller environments.
Drawbacks: Higher cost, more complex management for many VNets.

AZURE FIREWALL FEATURES



- **Threat Intelligence-based Filtering:** Automatically blocks traffic from known malicious IP addresses and domains.
- **SNAT Support:** All outbound traffic processed by the firewall gets translated to its public IP.
- **Forced Tunneling:** Can force all internet-bound traffic to an on-premises firewall via VPN Gateway/ExpressRoute.
- **Azure Monitor Integration:** Logs all traffic and threat alerts to Azure Monitor for analytics and alerting.
- **Availability Zones Support:** Deploy across multiple Availability Zones for enhanced resilience.
- **Web Categories:** Filter outbound access to websites based on categories (e.g., gambling, social media).

LAB 6: DEPLOYING AZURE FIREWALL

Creating Azure Firewall: Steps to provision the Azure Firewall resource in a dedicated subnet.

Configuring IP Configuration: Assigning a public IP to the firewall.

Creating Network Rules: Defining rules for Layer 3/4 traffic filtering (e.g., allowing specific ports).

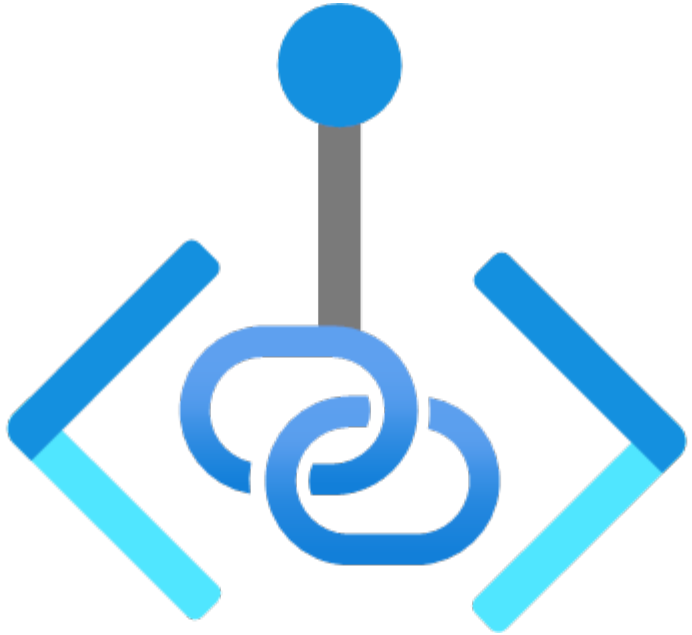
Creating Application Rules: Defining rules for Layer 7 FQDN-based filtering (e.g., allowing specific websites).

Implementing UDRs: Configuring User-Defined Routes in spoke subnets to route traffic through the firewall.

Testing Traffic Flow: Demonstrating inbound/outbound connectivity through the firewall.

AZURE SERVICE ENDPOINTS

Azure Service Endpoints are a powerful feature that extends your VNet's private address space to Azure PaaS services over the Azure backbone.



HOW SERVICE ENDPOINTS WORK

- **Subnet Configuration:** You enable a service endpoint for a specific Azure service on a subnet.
- **Route Overwrite:** Azure's system routes are overwritten to direct traffic to the PaaS service's private endpoint.
- **Source IP:** The source IP address of the traffic to the PaaS service becomes the VNet's private IP.
- **Service Network Access:** The PaaS service then only accepts traffic from the enabled VNet/subnet.
- **No VNet Gateway:** Does not use your VNet gateway for PaaS service communication.

SERVICE ENDPOINTS BEST PRACTICES

Enable on Necessary Subnets: Only enable service endpoints on subnets that absolutely require access to the PaaS service.

Combine with NSGs: Use NSGs with Service Tags to further restrict outbound access to only the necessary PaaS service.

Test Connectivity: Always test connectivity after enabling to ensure traffic flows as expected.

Consider Private Link: For more complex scenarios or cross-subscription access, evaluate Azure Private Link.

Audit and Monitor: Monitor VNet flow logs to verify that PaaS traffic is correctly using the service endpoint.

AZURE PRIVATE LINK

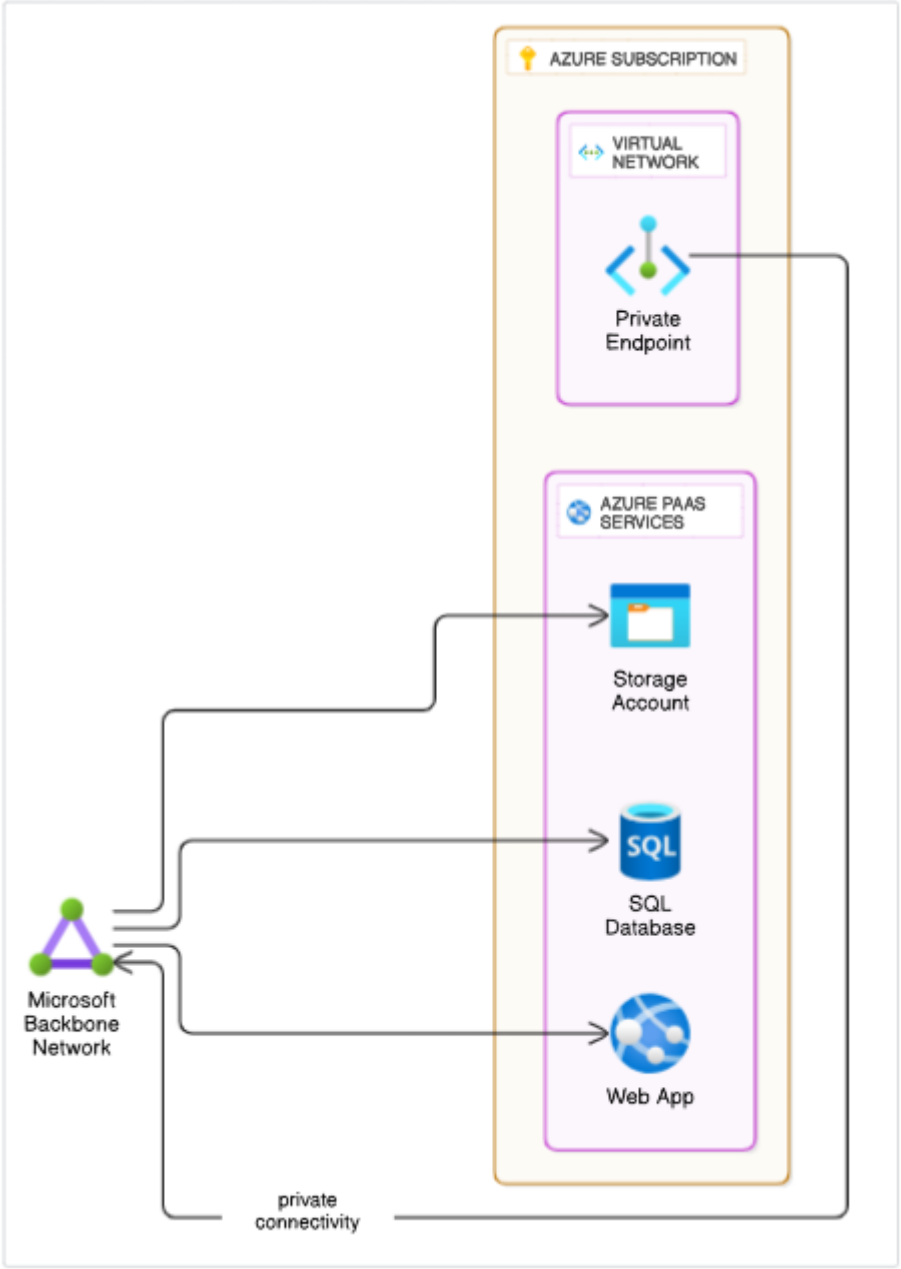
Private Connectivity via Private Endpoint: Provides private connectivity to Azure PaaS services, your own services, and partner services via a Private Endpoint.

No Public Internet Exposure: All traffic remains entirely on the Microsoft backbone network, never traversing the public internet.

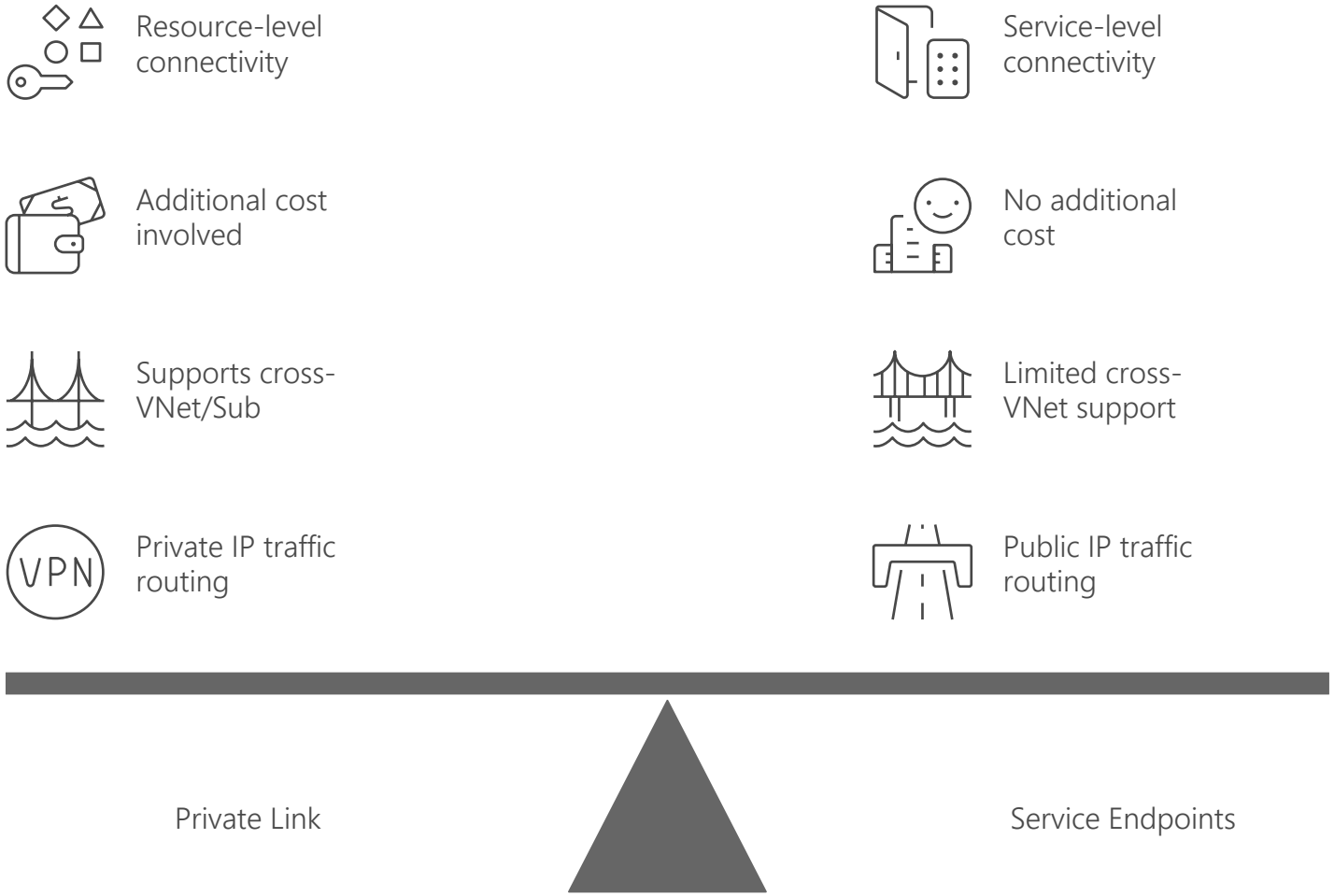
Centralized Access: Access multiple PaaS resources from a single VNet via Private Endpoints.

Cross-Subscription/Tenant: Supports connectivity across different Azure subscriptions and Azure Active Directory tenants.

DNS Integration: Requires proper DNS resolution (Azure Private DNS Zones) for private endpoints.



PRIVATE LINK VS. SERVICE ENDPOINTS



AZURE DDOS PROTECTION

This service provides always-on traffic monitoring for your public IP addresses, constantly looking for signs of Distributed Denial of Service attacks.

When an attack is detected, it automatically mitigates volumetric, protocol, and resource layer attacks.

Azure offers two tiers of DDoS protection: 'Basic' and 'Standard.'

AZURE DDOS PROTECTION STANDARD FEATURES

- **Adaptive Tuning:** Learns your application's normal traffic patterns to detect and mitigate attacks more effectively.
- **Attack Analytics & Metrics:** Provides detailed reports and metrics on DDoS attacks through Azure Monitor.
- **Attack Alerts:** Configurable alerts for when an attack is detected, during mitigation, and when it ceases.
- **WAF Integration:** Seamlessly integrates with Azure Application Gateway WAF or third-party WAFs for application layer protection.
- **DDoS Rapid Response Support:** Access to Microsoft's DDoS Rapid Response (DRR) team for expert support during active attacks.
- **Cost Guarantee:** Standard tier offers a credit guarantee for resource consumption during a verified DDoS attack.

POP QUIZ:

You have an Azure Virtual Machine (VM) running a web application. You need to restrict inbound HTTP (port 80) and HTTPS (port 443) traffic to this VM only from your corporate on-premises IP range (203.0.113.0/24). All other inbound traffic must be denied. Which Azure networking security component is most appropriate for this task?

A. Azure Firewall
B. Azure Load Balancer
C. Network Security Group (NSG)
D. Azure DDoS Protection

POP QUIZ:

You have an Azure Virtual Machine (VM) running a web application. You need to restrict inbound HTTP (port 80) and HTTPS (port 443) traffic to this VM only from your corporate on-premises IP range (203.0.113.0/24). All other inbound traffic must be denied. Which Azure networking security component is most appropriate for this task?

A. Azure Firewall
B. Azure Load Balancer
C. Network Security Group (NSG)
D. Azure DDoS Protection

POP QUIZ:

Your application team regularly deploys new Virtual Machines (VMs) to a subnet. You need to ensure that these new VMs can communicate with a specific set of backend database VMs on port 1433 (SQL Server) without manually updating Network Security Group (NSG) rules every time a VM is added or removed. What should you use to simplify this management?

A. User-Defined Routes (UDRs)
B. Azure Firewall Application Rules
C. Application Security Groups (ASGs)
D. Azure Private Link

POP QUIZ:

Your application team regularly deploys new Virtual Machines (VMs) to a subnet. You need to ensure that these new VMs can communicate with a specific set of backend database VMs on port 1433 (SQL Server) without manually updating Network Security Group (NSG) rules every time a VM is added or removed. What should you use to simplify this management?

A. User-Defined Routes (UDRs)
B. Azure Firewall Application Rules
C. Application Security Groups (ASGs)
D. Azure Private Link

POP QUIZ:

Your company requires an even higher level of security and network isolation for critical Azure PaaS services (e.g., Azure SQL Database, Azure Key Vault). You need to expose these services via a private IP address within your VNet, support cross-subscription connectivity, and ensure all traffic remains exclusively on the Microsoft backbone, without requiring public IP reachability for the PaaS service itself. Which Azure service should you implement?
A. Azure Service Endpoints
B. Azure Private Link
C. Network Security Groups (NSGs)
D. Azure Front Door

POP QUIZ:

Your company requires an even higher level of security and network isolation for critical Azure PaaS services (e.g., Azure SQL Database, Azure Key Vault). You need to expose these services via a private IP address within your VNet, support cross-subscription connectivity, and ensure all traffic remains exclusively on the Microsoft backbone, without requiring public IP reachability for the PaaS service itself. Which Azure service should you implement?

A. Azure Service Endpoints
B. Azure Private Link
C. Network Security Groups (NSGs)
D. Azure Front Door

AZURE LOAD BALANCING SOLUTIONS

LEARNING OBJECTIVES

- **Compare Load Balancing Approaches:** Differentiate between on-premises and Azure load balancing strategies.
- **Implement Azure Load Balancer:** Configure for high availability and basic traffic distribution (L4).
- **Utilize Azure Application Gateway:** Deploy for Layer 7 load balancing, SSL offloading, and WAF capabilities.
- **Deploy Azure Front Door:** Understand its role in global traffic management and content delivery (L7).
- **Configure Session Persistence:** Implement sticky sessions for stateful applications.
- **Secure Web Apps with HTTPS:** Leverage SSL/TLS offloading and end-to-end encryption.
- **Apply Path-based Routing:** Direct traffic based on URL paths with Application Gateway and Front Door.

ON-PREMISES VS. CLOUD LOAD BALANCING

Characteristic	On-Premises	Azure Cloud
Hardware	Hardware-Based	Software-Defined
Sizing	Manual Sizing	Elastic Scale
Configuration	Manual Configuration	API-Driven
Scale	Limited Scale	Global Reach
Resilience	Single Point of Failure	Built-in HA/Resilience

LOAD BALANCING PUBLIC FACING APPLICATIONS

- **Internet-Facing Frontend:** Public IP address assigned to the load balancer for external access.
- **High Availability:** Distributes traffic across multiple backend instances (VMs, containers) for fault tolerance.
- **Scalability:** Allows adding or removing backend instances without affecting the public endpoint.
- **Health Probes:** Continuously monitors the health of backend instances to ensure traffic is sent only to healthy ones.
- **Security:** Integrate with NSGs and WAFs to protect public-facing applications from malicious traffic.

LOAD BALANCING INTERNAL SERVICES

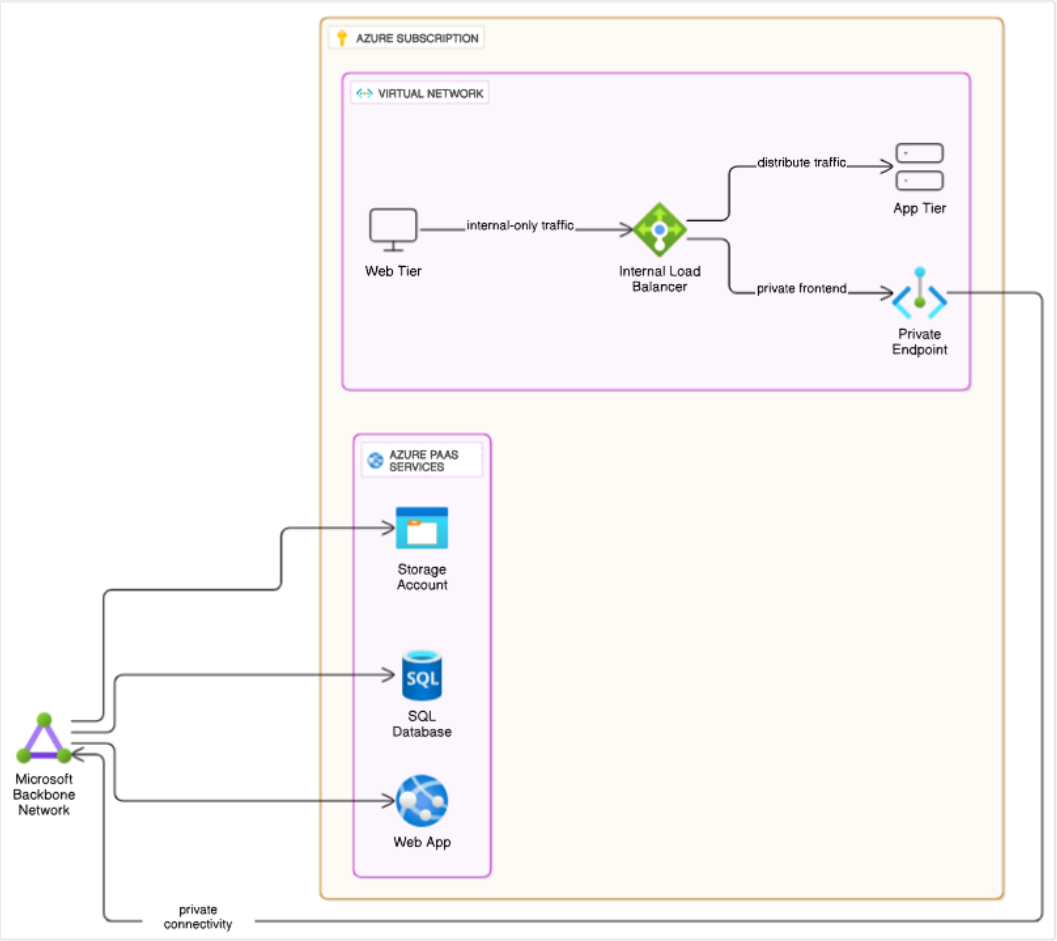
Private IP Frontend: Load balancer uses a private IP address for internal VNet access only.

Internal Application Connectivity: Distributes traffic for internal-only applications or API services.

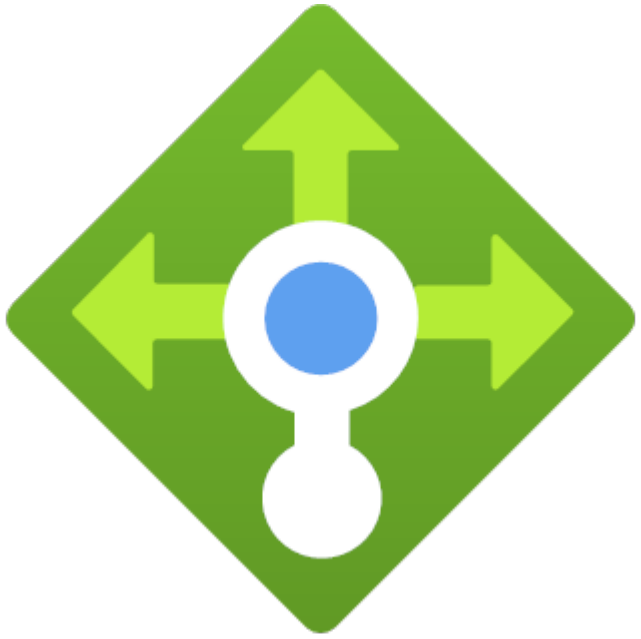
Service Chaining: Used to balance traffic between different tiers of a multi-tier application (e.g., web to app).

No Internet Exposure: Ensures that internal services are never directly exposed to the public internet.

VNet Integration: Seamlessly integrates with VNet subnets for private service discovery.



AZURE LOAD BALANCER – LAYER 4



Core Load Balancing: Distributes network traffic at the Transport Layer (Layer 4 - TCP/UDP).

High Performance, Low Latency: Provides ultra-low latency and high throughput for all TCP/UDP applications.

Health Probes: Monitors the health of backend instances using TCP, HTTP, or HTTPS probes.

Load Balancing Rules: Define how incoming traffic on a frontend IP and port is mapped to backend pool instances.

SNAT (Source Network Address Translation): For outbound connections to the internet from backend VMs (Basic LB limited, Standard LB better).

AZURE LOAD BALANCER TIERS

Basic Load Balancer:

SKU: Basic
Features: Limited features, no Availability Zone support, instance-level public IPs.
Scale: Limited scale for backend pools (up to 300 instances).
Availability: Single Availability Zone (if deployed zonally) or regional.
Security: Closed by default (NSG required to open).
Recommended: For dev/test, small-scale.

Standard Load Balancer:

SKU: Standard
Features: Richer feature set, Availability Zone support, public IP prefixes.
Scale: Scales up to 1000 instances in backend pools.
Availability: Zone-redundant or zonal.
Security: Secure by default (NSG required to open).
Recommended: For production, critical workloads.

LOAD BALANCING RULES & HEALTH PROBES

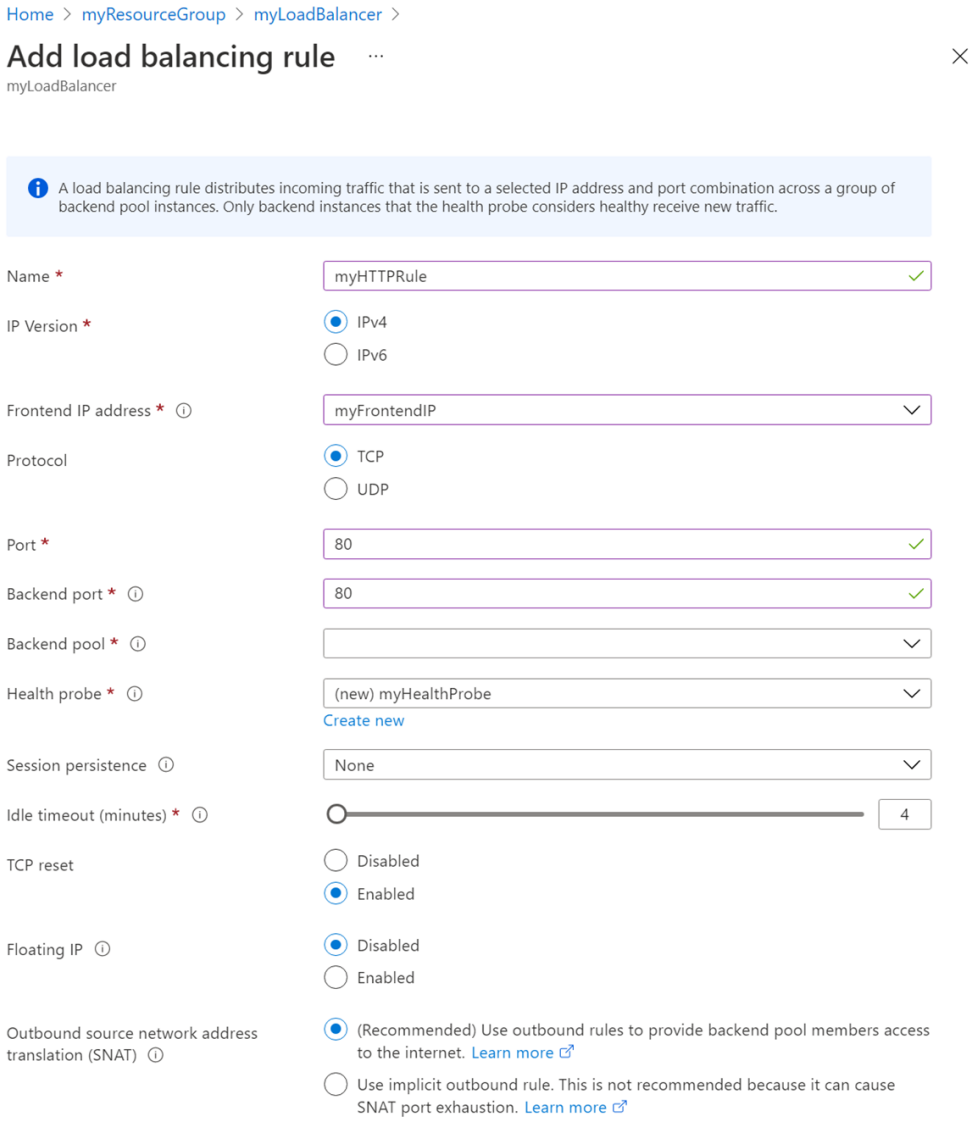
Frontend IP Configuration: The public or private IP address that receives incoming traffic.

Backend Pool: The group of VMs or instances that will receive the load-balanced traffic.

Load Balancing Rule: Maps the frontend IP/port to a backend pool, defining the distribution logic (e.g., 5-tuple hash).

Health Probe: Defines how the load balancer checks the health and availability of instances in the backend pool.

Probe Protocols: Supports TCP, HTTP, and HTTPS probes to various paths/ports.



AZURE APPLICATION GATEWAY – LAYER 7

Web Traffic Load Balancer (L7): Specifically designed for web applications, operating at Layer 7 (HTTP/HTTPS).

URL-based Routing: Supports routing traffic based on URL paths, host headers, or other HTTP attributes.

SSL/TLS Termination: Can offload SSL/TLS encryption, reducing load on backend servers.

Web Application Firewall (WAF): Integrated WAF protects web applications from common web vulnerabilities (OWASP Top 10).

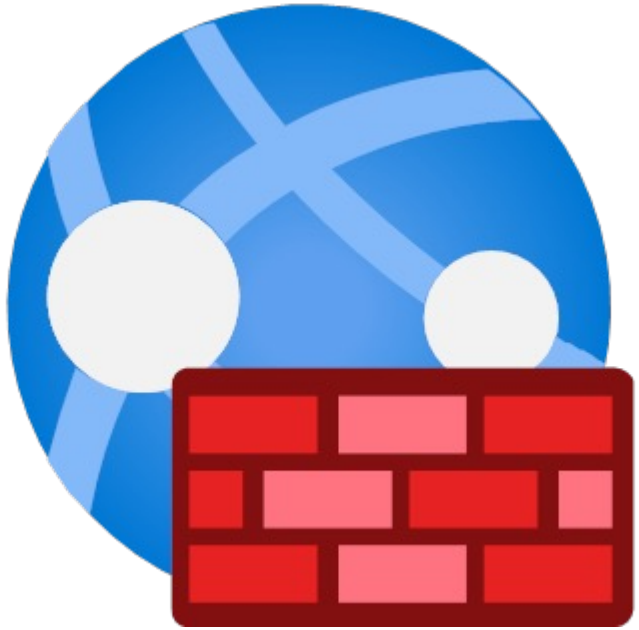
Sticky Sessions (Session Affinity): Ensures requests from the same user are sent to the same backend server.

APPLICATION GATEWAY COMPONENTS

- **Frontend IP Configuration:** The public or private IP address that receives HTTP/HTTPS traffic.
- **Listeners:** Defines the IP address, port, and protocol (HTTP/HTTPS) on which the Application Gateway listens for incoming requests.
- **HTTP Settings:** Configures how requests are routed to backend servers, including port, protocol, and cookie-based affinity.
- **Backend Pools:** Group of backend servers (VMs, VM scale sets, App Services, public IPs) that serve the content.
- **Routing Rules (Request Routing Rules):** Ties listeners to backend pools based on path, host header, or basic rules.

APPLICATION GATEWAY WAF (WEB APPLICATION FIREWALL)

The WAF protects your web applications against common web vulnerabilities, primarily those defined by the OWASP Top 10 list, such as SQL injection and cross-site scripting.



LOAD BALANCING PUBLIC FACING APPS

- **Public IP Frontend:** Application Gateway's frontend is usually a public IP address for internet accessibility.
- **SSL/TLS Termination:** Handles HTTPS traffic, decrypting at the gateway and sending unencrypted (or re-encrypted) to backend.
- **WAF Protection:** Provides a crucial first line of defense against web attacks before traffic reaches your servers.
- **Path-based Routing:** Directs different URL paths (e.g., /images, /api) to different backend pools or services.
- **Custom Domains:** Supports multiple custom domain names and SSL certificates for multi-site hosting.

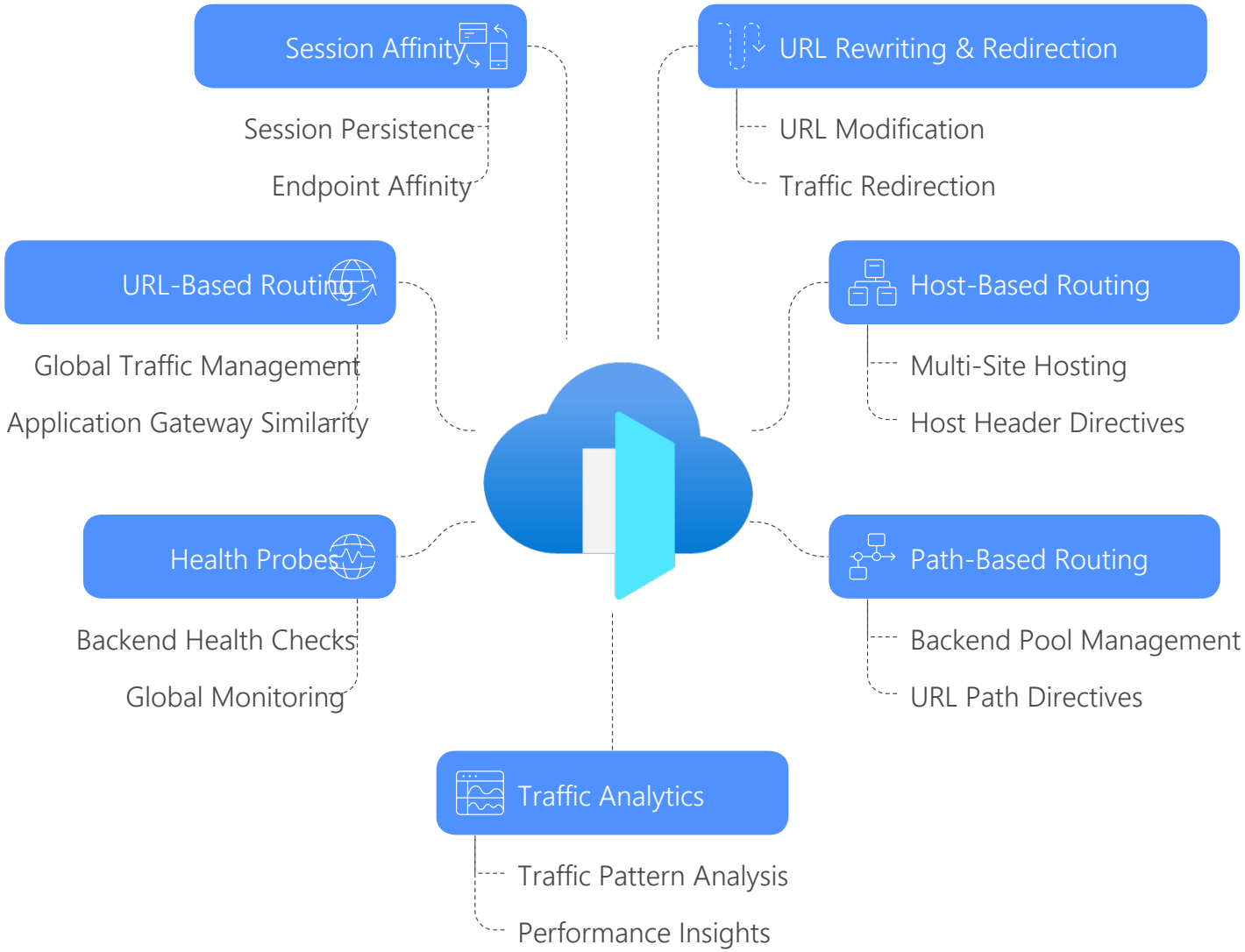
LOAD BALANCING PRIVATE FACING APPS

- **Private IP Frontend:** Application Gateway uses a private IP for internal-only web applications or APIs.
- **Internal Service Mesh:** Can act as a central entry point for internal microservices within a VNet.
- **Secure Tier-to-Tier Communication:** Enables secure communication between application tiers without public exposure.
- **No WAF on Internal Traffic:** While WAF is a core feature, it's typically less relevant for internal traffic (though technically possible).
- **Integrated with Private DNS:** Use Azure Private DNS zones for seamless internal name resolution.

AZURE FRONT DOOR – GLOBAL LAYER 7

Azure Front Door is a powerful service for global Layer 7 load balancing. It distributes web traffic across multiple Azure regions or even external, non-Azure endpoints. Front Door uses the Anycast protocol, which routes client requests to the geographically closest and lowest-latency backend, significantly improving user experience.

FRONT DOOR FEATURES & CAPABILITIES



FRONT DOOR PREMIUM VS. STANDARD

Standard Tier:

Features: Basic CDN, dynamic site acceleration, WAF, Private Link integration.
Pricing: Simpler pricing model based on data transfer and HTTP/HTTPS requests.
Use Cases: General web acceleration, basic WAF, simple global load balancing.

Premium Tier:

Features: All Standard features PLUS private link support for Azure PaaS, Microsoft Threat Intelligence, deeper monitoring.
Pricing: Higher cost, more complex pricing structure.
Use Cases: Enterprise-grade security, highly sensitive applications, advanced analytics, Private Link to origin.

WHEN TO USE FRONT DOOR VS. APP GATEWAY

Front Door:

- **Global Applications:** When users are distributed geographically and require lowest latency.
- **Multi-Region DR/HA:** For active-active or active-passive deployments across multiple Azure regions.
- **CDN & WAF at Edge:** When caching static/dynamic content and WAF protection are needed closest to users.
- **Anycast Advantage:** Benefits from Anycast for optimal routing.

Application Gateway:

- **Regional Applications:** When users are primarily in a single Azure region.
- **VM/VNet based Apps:** For applications deployed within a specific VNet.
- **Internal Load Balancing (L7):** For internal-only web applications or APIs within a VNet.
- **WAF for Regional Apps:** When WAF protection is needed for a regional application.

STICKY SESSIONS & IDLE TIMEOUTS

Sticky Sessions, also known as Session Affinity, ensure that all subsequent requests from a particular client are consistently directed to the same backend server.

Idle Timeouts define the maximum duration a connection can remain inactive without any data transfer before the load balancer closes it.

CONFIGURING STICKY SESSIONS

HTTP Setting Configuration: Cookie-based affinity is enabled within the HTTP Setting of the Application Gateway.

Cookie Name: Can use a default ApplicationGatewayAffinity cookie or a custom one.

Use Cases: Required for applications that store user session state directly on the backend server.

Impact on Scalability: Can impact backend server utilization if one server handles too many persistent sessions.

Stateless Design: Best practice to design applications as stateless to avoid dependency on sticky sessions.

CONFIGURING IDLE TIMEOUTS

Load Balancing Rule Property: Idle timeout is configured as a property of the Load Balancing Rule.

Default Value: The default idle timeout for Azure Load Balancer (Standard) is 4 minutes.

Maximum Value: Can be configured up to 30 minutes for Standard Load Balancer.

Impact on Long-lived Connections: Important for applications with infrequent data exchange (e.g., chat applications, IoT).

Keep-alives: Backend applications should send TCP keep-alives within the timeout period to maintain connections

SECURING WEB APPLICATIONS WITH HTTPS

HTTPS ensures encryption in transit, protecting your data from eavesdropping and tampering as it travels between the client and the server.

This requires SSL/TLS certificates, which are X.509 digital certificates issued by a trusted Certificate Authority.

SSL/TLS OFFLOADING WITH APPLICATION GATEWAY

Benefits: Reduces CPU load on backend servers, simplifies certificate management on VMs.

How it Works: Application Gateway receives encrypted HTTPS traffic, decrypts it, and forwards unencrypted (HTTP) or re-encrypted (HTTPS) to backend.

End-to-End SSL: Option to re-encrypt traffic from Application Gateway to backend servers for full encryption.

Certificate Management: Upload SSL certificates (PFX format) directly to Application Gateway.

Client Certificate Authentication: Application Gateway can also perform client certificate authentication.

PATH BASED ROUTING

APPLICATION GATEWAY

URL Path Segments: Directs traffic to different backend pools based on specific URL path segments.
Multi-Site Hosting: Enables routing for different sites hosted on the same Application Gateway (e.g., www.site1.com, www.site2.com).
Microservices Routing: Route requests for different microservices (e.g., /api/users, /api/products) to dedicated backend services.
Default Backend Pool: Specifies a default backend pool for requests not matching any path-based rule.
URL Rewrite: Can rewrite the URL before forwarding to the backend, enabling cleaner backend URLs.

AZURE FRONT DOOR

Global Scale: Path-based routing applied globally across different regions and backend endpoints.
Closest Backend Routing: Combines path-based logic with Front Door's Anycast routing to send traffic to the optimal backend.
Origin Groups: Define groups of backends (origins) for different application components.
Routing Rules: Connect frontend domains to origin groups based on path patterns.
Content Type Delivery: Deliver specific content types (e.g., images, videos) from optimized backend storage.

POP QUIZ:

You are designing a highly available, internet-facing application in Azure that requires protection against common web vulnerabilities (OWASP Top 10) and needs to offload SSL/TLS encryption from your backend web servers. The application is deployed in a single Azure region. Which Azure load balancing service is most suitable for this scenario?

A. Azure Load Balancer (Standard)
B. Azure Front Door
C. Azure Application Gateway
D. Azure Traffic Manager

POP QUIZ:

You are designing a highly available, internet-facing application in Azure that requires protection against common web vulnerabilities (OWASP Top 10) and needs to offload SSL/TLS encryption from your backend web servers. The application is deployed in a single Azure region. Which Azure load balancing service is most suitable for this scenario?

A. Azure Load Balancer (Standard)
B. Azure Front Door
C. Azure Application Gateway
D. Azure Traffic Manager

POP QUIZ:

You have a set of stateful web application backend servers in Azure. You need to ensure that once a client establishes a session with a particular backend server, all subsequent requests from that same client are consistently routed to the *same* server to maintain session state. Which feature should you enable on your Layer 7 load balancer?

A. Path-based routing
B. Health probes
C. Session affinity (sticky sessions)
D. URL redirection

POP QUIZ:

You have a set of stateful web application backend servers in Azure. You need to ensure that once a client establishes a session with a particular backend server, all subsequent requests from that same client are consistently routed to the *same* server to maintain session state. Which feature should you enable on your Layer 7 load balancer?

A. Path-based routing
B. Health probes
C. Session affinity (sticky sessions)
D. URL redirection

POP QUIZ:

Your company is deploying a new global e-commerce application that needs to deliver content with the lowest possible latency to users worldwide. The application backend is hosted in multiple Azure regions (East US, West Europe, Southeast Asia). You also want an integrated Web Application Firewall (WAF) at the edge. Which Azure service combination is the best fit?

A. Azure Load Balancer (Standard) + Azure CDN
B. Azure Application Gateway + Azure Traffic Manager
C. Azure Front Door + Azure CDN (Premium)
D. Azure Front Door (Standard or Premium)

POP QUIZ:

Your company is deploying a new global e-commerce application that needs to deliver content with the lowest possible latency to users worldwide. The application backend is hosted in multiple Azure regions (East US, West Europe, Southeast Asia). You also want an integrated Web Application Firewall (WAF) at the edge. Which Azure service combination is the best fit?

A. Azure Load Balancer (Standard) + Azure CDN
B. Azure Application Gateway + Azure Traffic Manager
C. Azure Front Door + Azure CDN (Premium)
D. Azure Front Door (Standard or Premium)

INDIVIDUAL KEY TAKEAWAYS

Write down three key insights from today's session.

Highlight how these take aways influence your work.

Q&A AND OPEN DISCUSSION


THANK
YOU