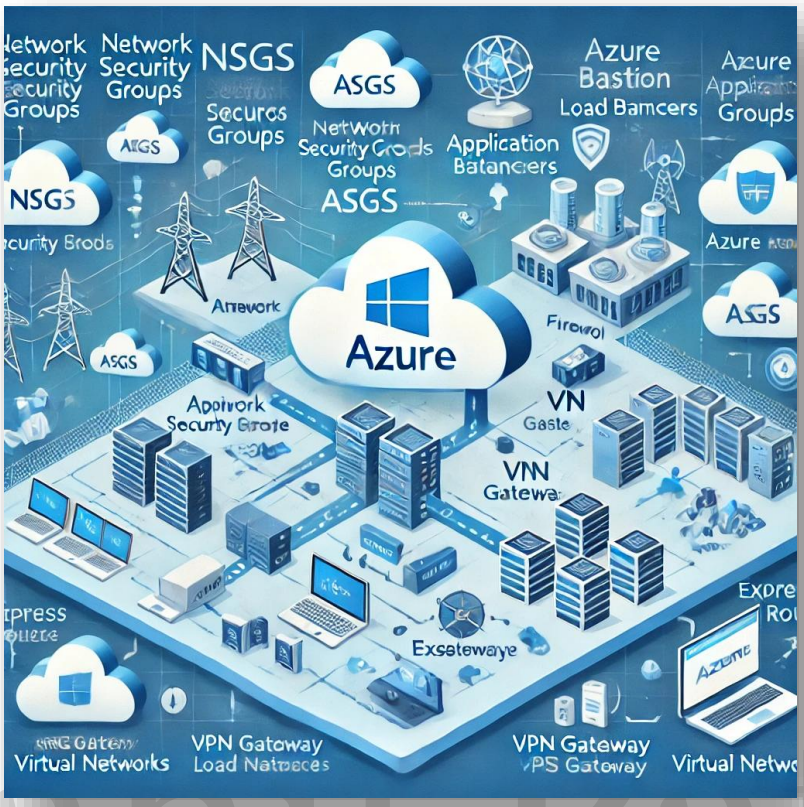
Week-7 |Azure Networking Interview Q&A



1. What is the difference between NSG and ASG?

- **Application Security Groups (ASGs)** group VMs logically to apply security rules efficiently.
- **Network Security Groups (NSGs)** control inbound and outbound network traffic at the subnet or NIC level.
- ASGs are used within NSGs to simplify security management for applications.

---

2. How can you block access to your VM from a subnet?

- By default, traffic is allowed between subnets within the same **Virtual Network (VNet)**.
- A default NSG rule **"AllowVnetInBound"** (priority: **65000**) permits this.
- To block access, create a **Deny rule** with a **lower priority** (e.g., **5000**).

---

3. Are Azure NSGs stateful or stateless?

- NSGs are **stateful**, meaning if an inbound rule allows traffic, an outbound response is automatically allowed.

Example:

If **port 80** is open for incoming HTTP requests, the response is allowed without defining an explicit outbound rule.

---

4. What is the difference between Azure Firewall and NSG?

Feature	Azure Firewall	NSG
Scope	Controls both **inbound** and **outbound** traffic	Controls traffic **within** a VNet and **between** VNets
Functionality	Stateful, provides **Layer 3 to Layer 7 filtering**, threat intelligence, and logging	Stateful, applies security rules at **Layer 4**
Use Case	Protects against malicious threats, inspects packets	Defines **allow/deny rules** for subnets or VM

---

5. What are the advantages of Resource Groups in Azure?

- **Logical Organization** for better resource management.
- **Lifecycle Management** to manage resources efficiently.
- **Tagging** for categorization.
- **RBAC (Role-Based Access Control)** for access control.
- **Cost Management** for tracking expenses.
- **ARM Templates** for automation.
- **Resource Locks** to prevent accidental deletion.

---

6. What is the difference between Azure User Data and Custom Data?

- **Custom Data** is accessible **only during VM creation** and disappears after first boot.
- **User Data** is a persistent version of Custom Data and remains **modifiable and accessible** anytime.

---

7. What is the difference between Azure Application Gateway and Azure Load Balancer?

Feature	Azure Application Gateway	Azure Load Balancer
OSI Layer	Operates at **Layer 7** (Application Layer)	Operates at **Layer 4** (Transport Layer)
Features	**SSL termination, URL-based routing, Web Application Firewall (WAF)**	**IP-based traffic routing**

Feature	Azure Application Gateway	Azure Load Balancer
Use Case	Best for **web traffic distribution**	Best for **general TCP/UDP traffic balancing**

---

8. Explain the traffic flow to an application deployed in the web subnet of an ideal Azure Networking setup.

User Access:

- Users access the application over the internet.
- DNS resolves the domain to a **public IP address**.

Traffic Routing:

- Incoming traffic reaches **Azure Front Door**, **Azure Application Gateway**, or **Azure Load Balancer**.
- These services handle **SSL termination, load balancing, and security filtering**.

Network Security Group (NSG) Enforcement:

- NSGs filter inbound and outbound traffic to allow only necessary access.

Azure Virtual Network (VNet) Components:

- Web servers communicate internally within the **VNet's private subnet**.

Application Processing:

- Web servers process requests and serve the content securely.

---

9. Describe the purpose of Azure Bastion for secure remote access to VMs.

- **Eliminates Public IP Exposure:** Securely connects to VMs without needing public IPs.
- **Reduces Attack Surface:** Prevents direct SSH/RDP access over the internet.
- **RBAC & MFA:** Integrates with **Role-Based Access Control (RBAC)** and **Multi-Factor Authentication (MFA)**.
- **Azure Portal Access:** Provides direct access from the Azure portal.
- **Auditing & Monitoring:** Enables tracking of all login activities.

---

10. What is the difference between Route Table and NSG?

Feature	Route Table	Network Security Group (NSG)
Function	Defines how traffic is routed within a VNet	Defines **allow/deny** network access rules
Scope	Applies to subnets	Applies to subnets or NICs
Use Case	Controls traffic flow between subnets, VNets, or on-premises	Controls **security access** at the network layer

---

Additional Questions for a Deeper Understanding

11. What is Azure Private Endpoint and when is it used?

- **Azure Private Endpoint** allows services to be accessed privately within a **VNet** without exposure to the public internet.
- Used for **securing communication** with **Azure PaaS services** like **Azure Storage, SQL Database, and Web Apps**.

---

12. What is VNet Peering and its advantages?

- **VNet Peering** allows **private communication** between Azure VNets.
- **Low latency & high-speed connectivity** between VNets.
- **No need for VPN gateways** or complex routing.

---

13. What is the difference between VPN Gateway and ExpressRoute?

Feature	VPN Gateway	ExpressRoute
Connectivity	Uses the **public internet**	Uses a **private dedicated connection**
Speed	Supports **up to 10 Gbps**	Supports **higher bandwidths** (50 Gbps+)
Security	Encrypted but **internet-based**	More **secure & reliable** for enterprises

---

14. What is the purpose of Azure DDoS Protection?

- Protects applications from **Distributed Denial of Service (DDoS) attacks**.
- **Monitors & mitigates** attack traffic in real-time.
- **Integrated with Azure VNet** for **automatic threat response**.

---

15. What is the difference between Azure Front Door and Azure Traffic Manager?

Feature	Azure Front Door	Azure Traffic Manager
Function	**Layer 7 load balancing & CDN**	**DNS-based traffic routing**
Security	**Web Application Firewall (WAF)**	**No built-in security features**
Use Case	**Multi-region global apps**	**Geo-routing based on DNS resolution**

---

16. What are the different types of Azure Load Balancers?

1. **Public Load Balancer** – Routes traffic to **internet-facing services**.
2. **Internal Load Balancer** – Distributes traffic within a **private VNet**.
3. **Global Load Balancer** – Manages cross-region **global traffic**.

---

17. What is Azure Virtual WAN?

- **Azure Virtual WAN** simplifies **large-scale networking**.
- Connects **branch offices, VNets, and on-premises** seamlessly.
- Uses **ExpressRoute, VPN, and SD-WAN**.

---

18. How do you implement Zero Trust Security in Azure Networking?

- **Use NSGs & Azure Firewall** for strict access control.
- **Enable Private Endpoints** to keep traffic within VNets.
- **Implement Azure Bastion** to eliminate public VM exposure.
- **Use RBAC & Conditional Access** for identity security.
