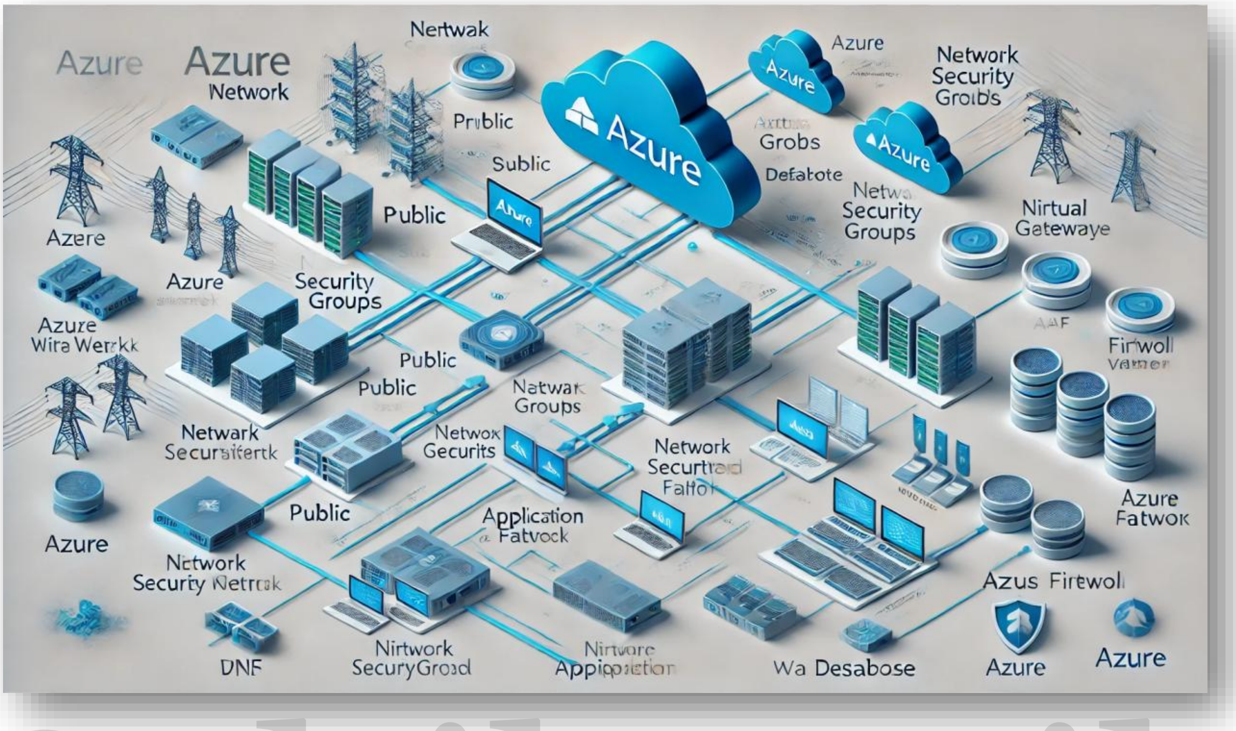
Week-6 | Azure Networking Basic to Advanced



Azure Networking is the backbone of cloud communication, enabling secure and efficient data exchange between resources. A well-architected networking solution in Azure ensures optimized performance, proper access control, and seamless integration between on-premises and cloud environments.

This document covers essential networking concepts, including **Virtual Networks (VNets), Network Security Groups (NSGs), Azure Load Balancer, Azure Firewall, VPN Gateways, Azure DNS, and Web Application Firewall (WAF)**.

---

1. Virtual Networks (VNets) and Subnetting

What is an Azure Virtual Network (VNet)?

An Azure Virtual Network (VNet) is an isolated network environment that allows Azure resources to communicate securely. VNets use **Classless Inter-Domain Routing (CIDR)** to allocate IP addresses and enable segmentation using subnets.

Subnetting in Azure

Subnets help isolate workloads, improve security, and control traffic flow. Common subnet types include:

- **Public Subnet** – Contains web applications accessible via the internet.
- **Private Subnet** – Hosts backend services that interact internally.
- **Database Subnet** – Stores sensitive data, restricting access to specific services.

Azure automatically assigns an internal **Dynamic Host Configuration Protocol (DHCP)** address to all resources within a VNet.

---

2. Security Mechanisms in Azure Networking

Network Security Groups (NSGs)

NSGs control inbound and outbound traffic at the subnet or individual resource level. They define:
✓ **Inbound rules** – Control who can send traffic into the network.
✓ **Outbound rules** – Define what traffic can leave the network.

For example:

- Allow SSH (port 22) only from a specific IP range.
- Allow HTTP (port 80) and HTTPS (port 443) to web servers.
- Deny all other traffic by default for security.

Azure Firewall

Azure Firewall is a cloud-based network security service that protects Azure workloads from unauthorized access. It provides:

- **Stateful packet filtering** – Monitors active connections and blocks malicious traffic.
- **Application FQDN Filtering** – Filters traffic based on fully qualified domain names (FQDN).
- **Threat Intelligence Integration** – Blocks known malicious IPs automatically.

Application Security Groups (ASGs)

ASGs allow you to group VMs logically, making NSG rule management easier.

---

3. Traffic Management and Load Balancing

Azure provides various load-balancing solutions:

Azure Load Balancer (Layer 4)

- Operates at the **transport layer (TCP/UDP)**.
- Distributes traffic across multiple VMs using algorithms like **round-robin** and **least connections**.
- Supports **availability sets** to ensure high availability.
- Handles **both inbound and outbound traffic** balancing.

Azure Application Gateway & Web Application Firewall (WAF) (Layer 7)

Azure Application Gateway is an intelligent load balancer that operates at the **application layer (HTTP/HTTPS)**.

Key Features:

- **Load Balancing** – Routes traffic across backend instances.
- **SSL Termination** – Offloads SSL processing to improve web server performance.
- **Web Application Firewall (WAF)** – Protects against common web vulnerabilities and exploits (e.g., SQL injection, cross-site scripting).
- **URL-Based Routing** – Directs traffic based on specific URL paths.
- **Multi-Site Hosting** – Hosts multiple web applications behind a single gateway.

Traffic Flow Example

When a user visits a website (example.com):

1. **Azure DNS** resolves the domain name to an IP address.
2. **Azure Firewall & NSG** enforce security policies.
3. **Azure Load Balancer or Application Gateway** directs the request to an available backend instance.

---

4. Azure DNS - Domain Name System

Azure DNS provides name resolution using Microsoft's global infrastructure.

Key Features:

- **Domain Hosting** – Hosts domain names and manages DNS records.
- **Integration with Azure Services** – Works with services like **App Service** and **Traffic Manager**.
- **Global Availability** – Ensures low-latency responses worldwide.

How Domain Resolution Works?

1. A user enters example.com in a browser.
2. The request is sent to the **ISP's DNS**.
3. The ISP forwards the query to **Azure DNS**.
4. Azure DNS resolves the domain name to an **IP address** of a Load Balancer or Web App.
5. The request is then processed and directed accordingly.

---

5. Hybrid Networking and Inter-VNet Communication

Azure provides multiple ways to connect different networks securely.

Virtual Network Peering

- **Global VNet Peering** – Connects VNets across different Azure regions.
- **Transitive Routing** – Traffic flows directly between peered VNets, improving performance.

- Low **latency and high-bandwidth** connectivity with no additional hardware required.

VNet Gateway

- Enables secure communication between **on-premises networks and Azure VNets**.
- Supports **Site-to-Site VPN and Point-to-Site VPN**.

Azure VPN Gateway

Azure VPN Gateway provides encrypted site-to-site connectivity between **on-premises networks and Azure VNets**.

Key Features:

- **IPsec/IKE VPN Protocols** – Ensures secure communication.
- **High Availability** – Supports **active-active and active-passive configurations**.
- **BGP Support** – Enables dynamic routing between on-premises networks and Azure.

ExpressRoute

- **Private, high-speed** connection between on-premises data centers and Azure.
- Bypasses the **public internet** for improved security and lower latency.

---

6. Azure Route Tables and Custom Routing

Azure uses **route tables** to control network traffic direction within a VNet.

Default Routing in Azure

By default, Azure provides **system routes** that:

- Allow traffic within the same VNet.
- Enable internet access for public subnets.
- Block unauthorized traffic.

Custom Routes

Users can create **custom route tables** to:

- **Force traffic through a firewall or VPN gateway** for security compliance.
- **Enable communication between peered VNets**.
- **Restrict internet access** for private subnets.

---

7. Best Practices for Azure Networking

✓ **Plan CIDR blocks properly** – Avoid overlapping IP ranges.
✓ **Implement least privilege security** – Use NSGs and ASGs to restrict access.
✓ **Use Azure Firewall** – Protect against unauthorized traffic.
✓ **Leverage load balancing** – Ensure high availability and fault tolerance.
✓ **Monitor and log network activity** – Use **Azure Monitor** and **Network Watcher**.
✓ **Optimize hybrid connectivity** – Use the right method (**VNet Peering, VPN Gateway, or ExpressRoute**).

Conclusion

Azure Networking is a critical component for building scalable, secure, and high-performing cloud architectures. By leveraging **VNets, subnets, security groups, firewalls, load balancing, hybrid connectivity, and DNS services**, organizations can ensure smooth and secure operations.

Understanding these core networking principles helps in designing and managing **secure, resilient, and efficient cloud infrastructures**.