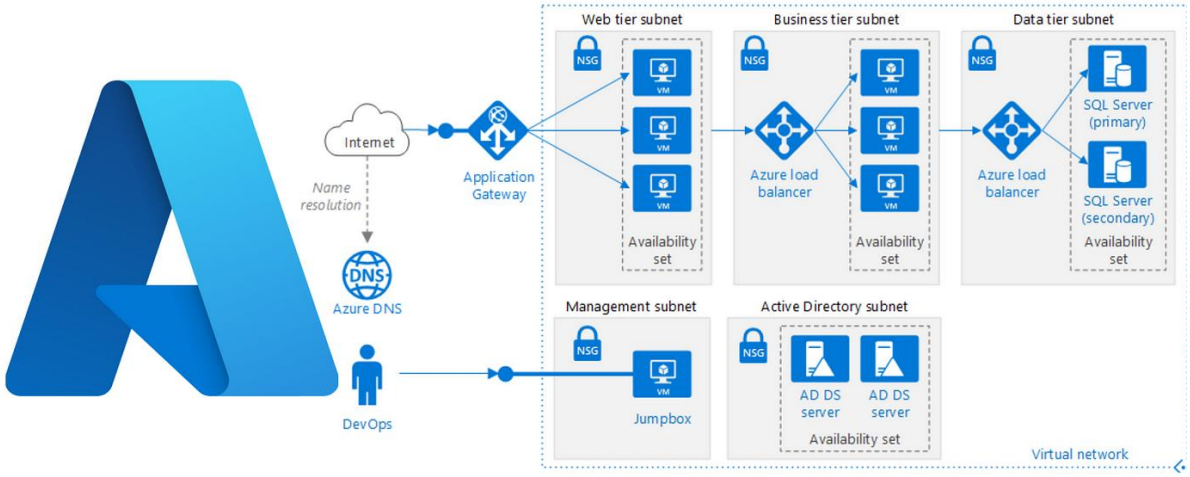
Week-5 | Azure Virtual Network(VNet)

INTRODUCTION TO AZURE VIRTUAL NETWORKS



Introduction

Azure Virtual Network (VNet) is a fundamental networking service in Microsoft Azure that provides **logical isolation** of resources, allowing users to securely connect and manage cloud resources. It acts as a private network within the Azure cloud, enabling communication between Azure resources while maintaining strict control over access and security.

This guide explores **Azure VNets, subnets, security configurations, and best practices** for setting up a secure cloud networking environment.

Understanding Azure Virtual Network (VNet)

What is a Virtual Network?

A Virtual Network (VNet) in Azure is a **logically isolated** network within the cloud that enables secure communication between virtual machines, databases, and other cloud resources. It functions similarly to a traditional on-premises network but with the added benefits of **scalability, flexibility, and cloud-native security features**.

Key Features of VNet

1. **Private Network in Azure** – Provides an isolated environment to host virtual machines, applications, and databases.
2. **Subnetting** – Supports multiple subnets within a VNet for network segmentation.
3. **Security Controls** – Integrates **Network Security Groups (NSG)** and **Azure Service Groups (ASG)** for traffic filtering and access management.
4. **Hybrid Connectivity** – Enables **VPN Gateway** and **ExpressRoute** to connect on-premises networks to Azure.

5. **Traffic Routing** – Uses **User-Defined Routes (UDR)** and built-in Azure routing for traffic management.

Subnetting in Azure Virtual Network

Why Use Subnets?

Subnets allow you to **divide a VNet into smaller, manageable segments**, each dedicated to a specific workload or security requirement. By using subnets, you can:

- **Enhance security** by separating different application layers.
- **Optimize performance** by isolating traffic flows.
- **Improve manageability** by applying security rules at the subnet level.

Common Subnet Types in an Azure VNet

1. **Public Subnet** – Hosts web applications and services that require **internet access**.
2. **Private Subnet** – Hosts internal applications, APIs, and business logic components.
3. **Database Subnet** – Houses databases that should be **isolated from the internet** for security reasons.

Example Subnet Design:

Subnet Name	Purpose	Security Considerations
Public Subnet	Web applications, APIs	Restricted to HTTP/HTTPS access
Private Subnet	Business logic services	Only accessible from internal applications
Database Subnet	Databases (MySQL, PostgreSQL, etc.)	No internet access, only internal connections

---

Security in Azure Virtual Network

Security is a critical aspect of designing a VNet. Azure provides various security mechanisms to **restrict unauthorized access and protect sensitive data**.

1. Network Security Groups (NSG)

NSGs control **inbound and outbound traffic** at both the subnet and virtual machine level. They contain **rules** that define which traffic is allowed or denied based on **source, destination, port, and protocol**.

Example NSG Rules:

Rule Name	Source	Destination	Port	Action
Allow HTTP	Internet	Web Servers	80	Allow
Allow HTTPS	Internet	Web Servers	443	Allow
Deny All	Any	Any	Any	Deny

NSG Best Practices:

- Apply **NSGs at the subnet level** to enforce security policies consistently.
- **Use "Deny All" as the default rule** and allow only necessary traffic.
- Regularly **review NSG rules** to eliminate unused or overly permissive rules.

2. Azure Service Groups (ASG)

Azure Service Groups (ASG) allow you to group multiple virtual machines and apply security rules to the entire group instead of individual VMs.

Benefits of ASG:

- Simplifies security rule management.
- Ensures consistency by applying policies to grouped resources.
- Provides **dynamic updates** when new VMs are added to the group.

Example Use Case:

- An NSG rule can allow all instances in a subnet to access a database.
- An ASG can further **restrict access** so that only a specific group of application servers can connect to the database.

Traffic Routing in Azure Virtual Network

Azure VNets provide built-in routing capabilities, ensuring efficient traffic flow between resources. However, users can define **custom routes** for greater control over network traffic.

1. Default Routing

Azure automatically creates default system routes to handle traffic within a VNet. These include:

- Routes between subnets within the same VNet.
- Routes for internet access if a public IP is assigned.
- Routes to on-premises networks if **VPN Gateway or ExpressRoute** is configured.

2. User-Defined Routes (UDR)

User-Defined Routes allow organizations to override Azure's default routing. **Common use cases include:**

- Forcing all internet-bound traffic through a **firewall or security appliance**.
- Directing traffic through a **network virtual appliance (NVA)** for inspection.
- Ensuring that **database traffic remains within private subnets**.

Example User-Defined Route (UDR) Configuration:

Route Name	Destination	Next Hop Type
Internet Traffic	0.0.0.0/0	Firewall
Private Network	10.1.0.0/16	Virtual Network
Database Traffic	10.2.0.0/24	None (Local Subnet)

Hybrid Networking with Azure VNet

Organizations often need to **extend their on-premises network** to Azure. Azure provides multiple connectivity options for hybrid networking:

1. VPN Gateway

- **Site-to-Site VPN:** Secure connection between an on-premises network and Azure.
- **Point-to-Site VPN:** Individual device connection to an Azure VNet.

2. Azure ExpressRoute

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

3. VNet Peering

- Connects multiple VNets within the same or different Azure regions.
- **Low-latency, high-bandwidth** private network communication.
- Useful for interconnecting **development, testing, and production environments** securely.

Best Practices for Azure Virtual Network (VNet)

1. **Follow the Principle of Least Privilege (PoLP):**
    - Restrict access to only necessary resources using **NSGs and ASGs**.
2. **Use Subnet Segmentation:**
    - Separate public, private, and database workloads into dedicated subnets.
3. **Monitor and Audit Network Traffic:**

- Enable **Azure Monitor, Network Watcher, and Traffic Analytics**.

4. **Implement User-Defined Routes (UDR):**
    - Control routing of network traffic for improved security.
5. **Leverage Hybrid Connectivity Where Needed:**
    - Use **VPN Gateway or ExpressRoute** for secure on-premises connectivity.
6. **Secure Internet-Facing Resources:**
    - Use **Azure Firewall or Application Gateway** for traffic filtering.

Conclusion

Azure Virtual Network (VNet) is an essential service for managing secure and efficient cloud networking. By implementing **subnets, NSGs, ASGs, custom routes, and hybrid networking**, organizations can **optimize security, enhance connectivity, and ensure seamless cloud integration**.

Understanding and properly configuring VNets is critical for **secure, scalable, and well-structured** cloud infrastructure.
