Azure Virtual Network (VNet)

An **Azure Virtual Network (VNet)** is a fundamental networking resource in Azure that enables secure communication between Azure resources, on-premises networks, and the internet. It is similar to a traditional network in a data center but with added cloud capabilities.

Key Features of Azure VNet

✅ **Isolation & Segmentation** – Each VNet is isolated, ensuring secure communication within defined boundaries.
✅ **Subnetting** – Divide a VNet into multiple subnets for better traffic management.
✅ **Hybrid Connectivity** – Connect on-premises networks using VPN Gateway, ExpressRoute, or Azure Virtual WAN.
✅ **Network Security** – Use **Network Security Groups (NSGs)** and **Azure Firewall** for access control.
✅ **Load Balancing** – Use Azure Load Balancer and Application Gateway for traffic distribution.
✅ **Private Access to Azure Services** – Use **Private Link** to securely connect to Azure services without public internet exposure.

How to Create a Virtual Network in Azure

Using Azure Portal:

1. **Sign in** to Azure Portal.
2. Go to **"Create a resource"** > Search for **"Virtual Network"** > Click **Create**.

3. **Set up Basic Settings**
    - Select **Subscription** and **Resource Group**.
    - Enter **Name** and **Region** for your VNet.
4. **Add Subnets**
    - Define **Address Space** (e.g., 10.0.0.0/16).
    - Create subnets (e.g., 10.0.1.0/24 for VMs, 10.0.2.0/24 for databases).
5. **Configure Security & Networking Options**
    - Enable **DDoS Protection** and **Firewall (optional)**.
    - Attach **Network Security Groups (NSGs)** for traffic control.
6. **Review & Create** – Validate settings and deploy the VNet.

Common Use Cases

- **Hosting applications securely** (VMs, databases, web apps).
- **Hybrid cloud solutions** (connect Azure with on-prem).
- **Multi-tier architectures** (using subnets for web, app, and DB layers).
- **Big data and analytics** (connect data pipelines securely).

Subnet in Azure Virtual Network (VNet)

A **subnet** in Azure is a smaller segment of an **Azure Virtual Network (VNet)** that helps organize and manage network resources. Subnets allow you to separate services logically and control traffic flow with security policies.

Key Features of Azure Subnets

✅ **IP Address Allocation** – Each subnet gets a range of private IPs from the VNet.
✅ **Network Segmentation** – Separate workloads (e.g., web, app, and database tiers).
✅ **Security Control** – Apply **Network Security Groups (NSGs)** to restrict access.
✅ **Route Control** – Use **User-Defined Routes (UDRs)** to manage traffic flow.
✅ **Integration with Azure Services** – Connect VMs, App Services, Azure Kubernetes Service (AKS), etc.

How to Create a Subnet in Azure

1️⃣ Using Azure Portal

1. **Go to Azure Portal** – portal.azure.com
2. Navigate to **Virtual Networks** and select your **VNet**.
3. Click **"Subnets"** > **"Add Subnet"**.
4. **Enter Subnet Details**:

- **Name**: Example – WebSubnet
- **Address range (CIDR)**: Example – 10.0.1.0/24
- **Network Security Group (NSG)**: (Optional) Assign an NSG.
- **Route Table**: (Optional) Assign a custom route table.

5. Click **"Save"** to create the subnet.

Subnet Best Practices

Use Multiple Subnets for Workload Separation (e.g., WebSubnet, AppSubnet, DBSubnet).

Assign NSGs to Subnets for security (e.g., allow only required ports).

Plan IP Ranges Carefully – Ensure subnets don't overlap.

Use Route Tables for Traffic Control – Define custom routes if needed.

Consider Private Endpoints – To securely connect Azure services within the subnet.

Example Subnet Setup for a Web Application

Subnet Name	CIDR Range	Purpose
WebSubnet	10.0.1.0/24	Hosts Web Servers (VMs, App Services)
AppSubnet	10.0.2.0/24	Runs Application Layer (APIs, Services)

DBSubnet	10.0.3.0/24	Holds Databases (SQL, CosmosDB, etc.)