1. Virtual Network (VNet)

Think of a Virtual Network (VNet) as your own private space in the cloud where you can place your resources (like virtual machines, databases, etc.). It's like creating a virtual version of a traditional network you'd have in an office, but it's all in the cloud.

Why is it important?

A VNet allows your resources to securely communicate with each other, the internet, and even on-premises networks (like your office network).

What can you do with it?

You can control things like IP addresses, routing, and security rules to make sure your resources are safe and can talk to each other properly.

2. Subnet

A subnet is a smaller section of a Virtual Network. Think of it like dividing a big office into smaller rooms or departments. Each subnet can have its own set of rules and resources.

Why use subnets?

Subnets help you organize your resources and apply different security or routing rules to different groups. For example:

- You might have one subnet for web servers that need to be accessible from the internet.
- Another subnet for databases that should only be accessible from within the network.

3. CIDR (Classless Inter-Domain Routing)

CIDR is a way to define the range of IP addresses that your Virtual Network and subnets can use. It looks something like this: 10.0.0.0/16.

What does it mean?

The /16 part tells you how many IP addresses are available in that range. The smaller the number after the /, the more IP addresses you have.

Example: 10.0.0.0/16 means you have a lot of IPs (65,536 to be exact).

Example: 10.0.0.0/24 means you have fewer IPs (256).

Why is it important?

CIDR helps you plan how many IP addresses you need for your network and subnets without wasting them.

4. Network Security Groups (NSGs)

A Network Security Group (NSG) is like a firewall for your Virtual Network or subnets. It controls the traffic that is allowed to flow in and out of your network.

What does it do?

- You can create rules to allow or block traffic based on:
- Source IP address (where the traffic is coming from).
- Destination IP address (where the traffic is going).
- Port (e.g., HTTP traffic uses port 80, HTTPS uses port 443).

Why is it important?

NSGs help you secure your resources by only allowing the traffic you want and blocking everything else.

Here are some additional key points about Virtual Networks in Azure:

Peering: You can connect two Virtual Networks together using VNet peering. This allows resources in different VNets to communicate securely as if they were in the same network.

Public and Private IPs:

Public IPs are used for resources that need to be accessible from the internet (like a website).

Private IPs are used for internal communication within your VNet.

VPN Gateway: If you want to connect your on-premises network (like your office) to your Azure Virtual Network, you can use a VPN Gateway. It creates a secure tunnel between the two.

Service Endpoints: These allow you to securely connect your VNet to Azure services (like Azure Storage or SQL Database) without exposing them to the public internet.

Azure Firewall:

For more advanced security, you can use Azure Firewall, which is a managed firewall service to protect your VNet.

Quickstart: Use the Azure portal to create a virtual network - Azure Virtual Network | Microsoft Learn