**Azure Network Security and Protection Services**

**1. Azure DDoS Network Protection**

**What is it?**

Azure DDoS Protection defends your applications and services from **Distributed Denial of Service (DDoS) attacks**, which attempt to overwhelm your network with traffic.

**Tiers:**

* **Basic** – Enabled by default for every Azure service; provides global Azure-level protection.
* **Standard** – Offers **enhanced protection** with:
  + Real-time telemetry
  + Alerting and mitigation reports
  + Cost protection against scaled attacks

**Key Features:**

* Automatic attack detection and mitigation
* Integration with Azure Monitor for logging and alerts
* Application-layer protection when combined with Azure Web Application Firewall (WAF)
* Cost guarantee during attacks (credit-back for impacted resources)

**Use Case:**

Protect critical services (web apps, APIs, gaming platforms) from traffic floods and volumetric attacks.

**2. Azure Firewall**

**What is it?**

Azure Firewall is a **managed, cloud-native network security service** that protects Azure Virtual Networks (VNets) by **controlling inbound and outbound traffic**.

**Key Features:**

* **Stateful firewall as a service** with built-in high availability
* Supports **FQDN filtering, URL filtering**, and **TLS inspection**
* **Threat intelligence** from Microsoft to block known malicious IPs/domains
* **Network rules**, **application rules**, and **NAT rules** for traffic control
* **Integration with Azure Monitor**, **Sentinel**, and **Microsoft Defender for Cloud**

**Use Case:**

Centralized policy enforcement across workloads, multi-region deployments, and secure hybrid cloud traffic.

**3. Azure Bastion**

**What is it?**

Azure Bastion provides **secure and seamless RDP and SSH access** to Azure Virtual Machines **without exposing them to the public internet**.

**Key Features:**

* Browser-based RDP/SSH access over SSL
* No public IPs required on VMs
* Integrated with Azure Portal
* Reduces risk of brute-force attacks
* Supports Azure AD-based authentication (preview)

**Use Case:**

Secure VM access in isolated environments or production networks with no public exposure.

**4. Virtual Network Encryption**

**What is it?**

Virtual Network (VNet) Encryption ensures **end-to-end encryption of traffic** between Azure Virtual Machines and subnets using **IPsec encryption**.

**Key Options:**

* **Encryption-in-transit within Azure**:
  + Some traffic is automatically encrypted (e.g., between storage and compute)
  + **Private Link** and **TLS** can help secure connections between services
* **VNet-to-VNet encryption:**
  + Use **VPN Gateway** with IPsec/IKE tunnels to encrypt communication between VNets.
* **Confidential computing**:
  + Use **confidential VMs** to encrypt data in use.

**Use Case:**

Secure inter-subnet or inter-VNet communication in sensitive workloads, compliance-driven environments, or multi-region deployments.