Azure Bastion Host

Azure **Bastion** is a **fully managed service** by Microsoft Azure that provides **secure and seamless Remote Desktop Protocol (RDP)** and **Secure Shell (SSH)** access to virtual machines (VMs) without exposing them to the **public internet**.

◆ Why Use Azure Bastion?

1. **Enhanced Security** – No need to expose VMs to the public internet with open RDP/SSH ports.
2. **No Public IP Required** – You can access VMs using their **private IP address**.
3. **Fully Managed** – Microsoft takes care of updates, scaling, and maintenance.
4. **Seamless Access** – Directly access VMs from the **Azure Portal** via the **browser** (without needing an RDP/SSH client).
5. **Protection Against Brute Force Attacks** – Reduces attack vectors by eliminating the need for public-facing RDP/SSH.

◆ How Azure Bastion Works

1. Deploy **Azure Bastion** inside an **Azure Virtual Network (VNet)**.
2. Connect to your **VMs securely** via Azure Portal using a **web-based RDP/SSH session**.
3. No **public IP address** is required for your VMs.
4. Uses **TLS encryption** for communication.

◆ Steps to Deploy Azure Bastion

1. **Create a Virtual Network (VNet)**
    - Ensure your VNet has a dedicated **AzureBastionSubnet** with a subnet mask of at least /26.
2. **Deploy Azure Bastion**
    - Go to **Azure Portal** → Search for **Bastion** → Click **Create**.
    - Select your **Resource Group** and **VNet**.
    - Create a new or use an existing **Public IP** (used only for the Bastion service, not for VMs).
    - Click **Review + Create**.
3. **Access VMs via Bastion**
    - Go to **Virtual Machines** in the **Azure Portal**.
    - Select the VM you want to connect to.
    - Click **Connect → Bastion**.
    - Enter credentials and click **Connect**.

◆ Azure Bastion Pricing

- Pricing is based on:
    - **Instance size** (Standard or Basic).
    - **Hours used** (per hour cost).
    - **Outbound data transfer** (varies by region).

For updated pricing, check: Azure Bastion Pricing

🔹 When to Use Azure Bastion?

✅ If you need **secure access** to VMs **without exposing RDP/SSH ports**.

✅ If you want **easy browser-based** access to VMs **without a VPN**.

✅ If you need a **fully managed** solution with **minimal maintenance**.