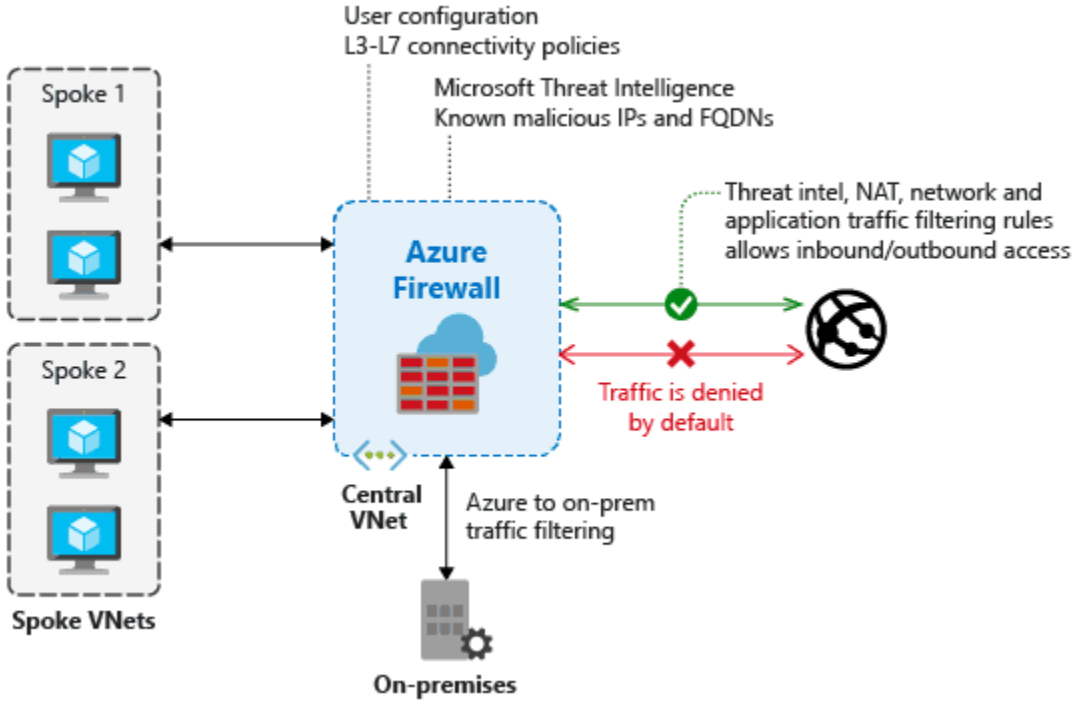
Microsoft Azure Secure Network Connectivity: Firewall, DDOS, & NSG

This blog will cover the **topic 3.1 Azure Secure Network Connectivity** which includes **Firewall**, **DDOS,** and **NSG.**

As with any other cloud service, the protection of the cloud is Microsoft's responsibility, protection in the cloud is your responsibility. Proper knowledge of the following tools and where to use them can immensely reduce security risks to your cloud deployments.

Azure Firewall

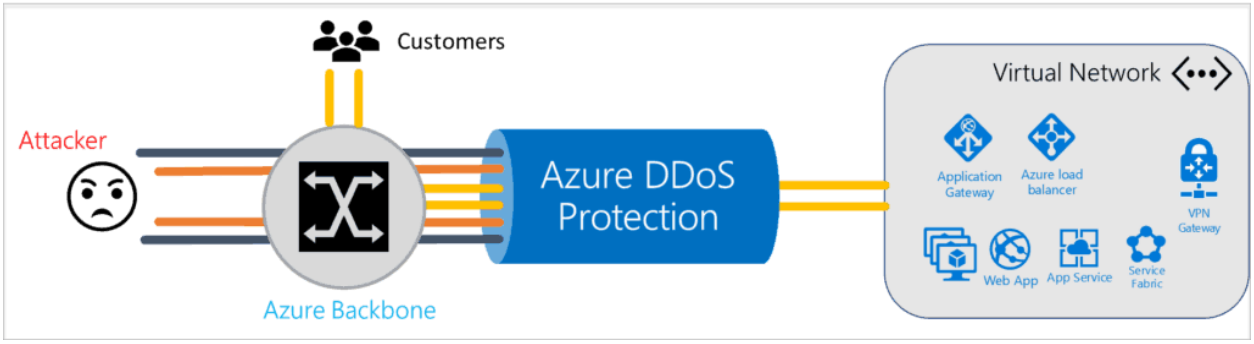
1. The Azure Firewall is a **managed service** that provides **cloud-based network security** for the protection of your Azure virtual network resources.
2. It's a completely **stateful firewall** service that has **high availability** and **near unlimited cloud scalability**.
3. It enables you to centrally create, enforce, and log application and network policies **across subscriptions and virtual networks**.
4. It provides **full-service integration** with Azure Monitor for logging and analytics.
5. The firewall can also be configured with **threat intelligence-based filtering** to block well known malicious traffic automatically using Microsoft updated sources.



Azure DDoS Protection

1. DDoS attacks are targeted at any **service endpoint** that is **publicly reachable** from the internet and try to exhaust an application's resources, resulting in access being **unavailable** to legitimate users.
2. DDoS protection is an **always-on** and **real-time service** and can easily defend against common network-level attacks.

3. It provides the same protection that Microsoft utilizes for its services over **both IPv4 and IPv6** public addresses.
4. **Real-time telemetry** is available via Azure Monitor views during an attack for taking action and logged as well as for analysis at a later stage.



Azure Network Security Groups

1. Azure Network Security groups(NSG's) can be used to **filter network traffic from and to Azure resources** in the Azure Virtual network.
2. NSG contain security rules that enable you to allow or deny outbound traffic from, or inbound traffic to, various types of Azure resources.
3. For existing connections, a flow record is created, Azure resources are **denied or allowed to communicate based on the connection state of the flow record**.
4. A **flow record** allows a Network Security Group to **become stateful.**