Azure Firewall vs Azure Network Security Groups (NSG)

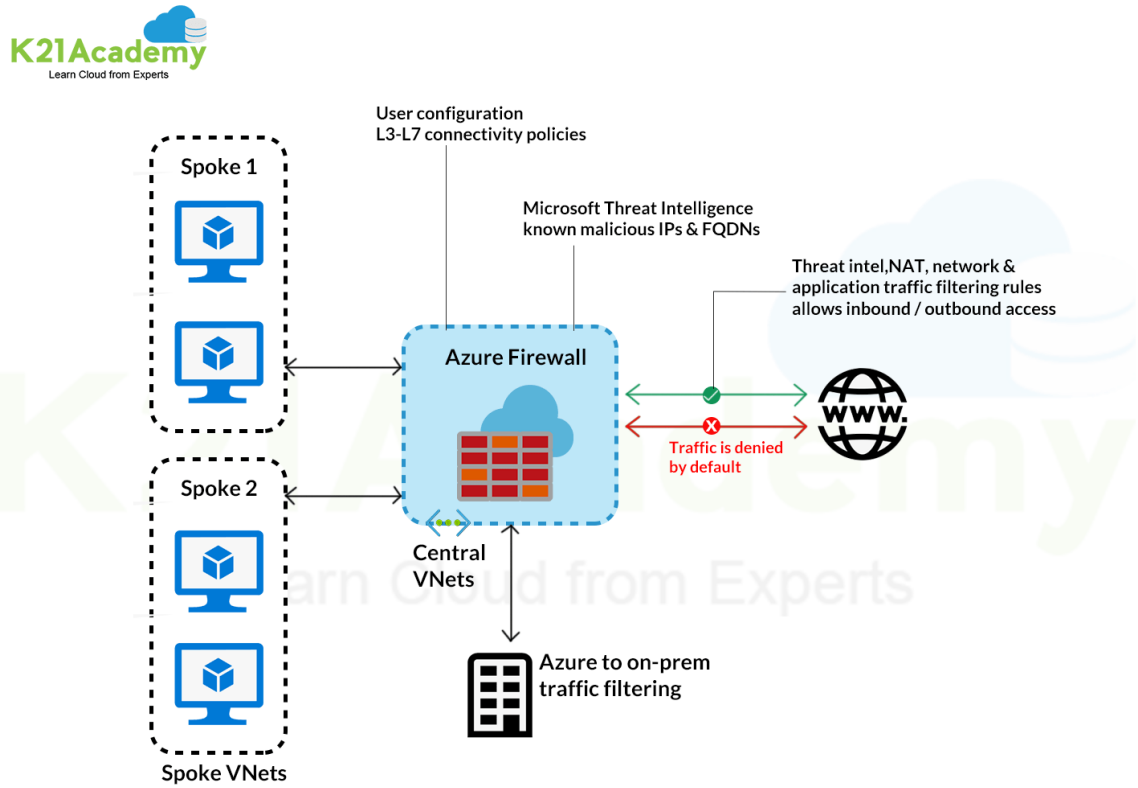
Azure Firewall vs. NSG often creates a lot of delusions. Whenever we need to run any workload on cloud service, it becomes essential to monitor and manage the security measures such as incoming and outgoing traffic that uses your resources. Microsoft Azure provides two security services to track the in and out traffic flows. In this post, I will give you a walk-through of Azure NSG vs Firewall.

What is Azure Firewall?

Azure Firewall is a **fully managed network security service**. It is used to **secure the incoming and outgoing traffic** of content within it. It is an **intelligent system** that automatically detects the workloads in the VNet and protects all resources from malicious traffic. The Azure Firewall is based on layers 4 and 7 of the OSI (Open Systems Interconnection Model) model. It is effortless to implement the Azure Firewall. Users need to set and configure rules like Nat rules, Application rules, and Network rules to apply Firewall.

How does Azure Firewall work?

Azure firewall offers enough features to provide **optimized control** over the in and out network traffic. It **eliminates** the **need** for **Load Balancer** **configuration** because of its high availability. Microsoft Azure ensures **99.99% availability** of its resources due to its availability zone feature. It does not charge anything extra for scalability. You pay only for what you use.

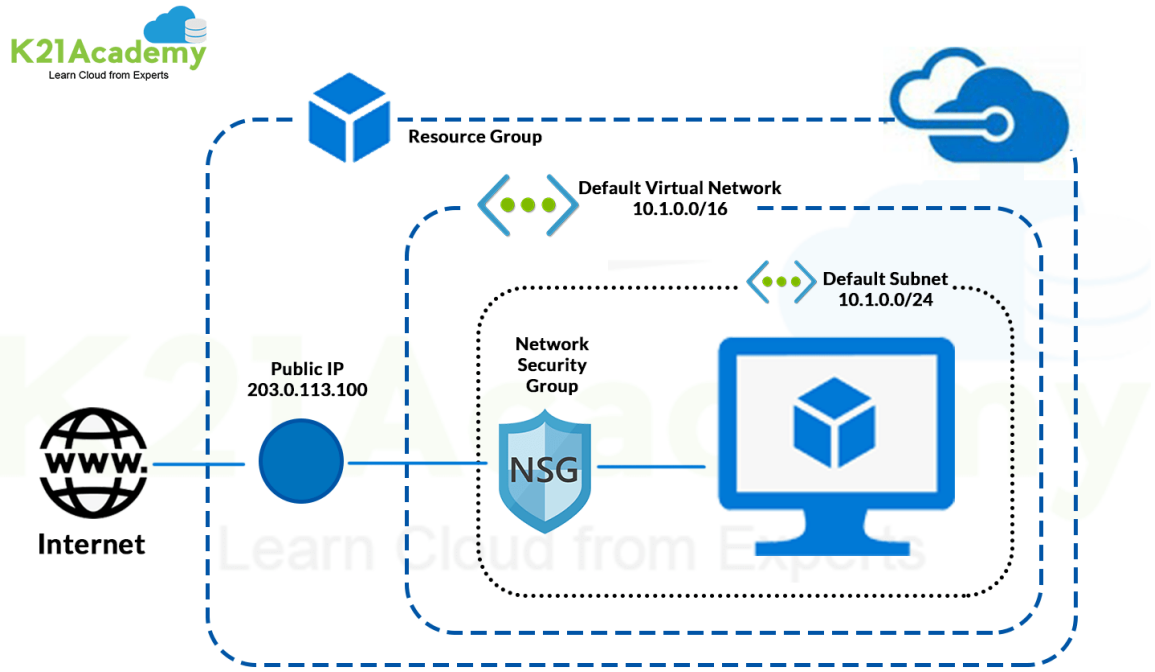


Moreover, it also allows restriction on outbound traffic by specifying the FQDN service. You can create your own defined rules using Azure Firewall to filter networks based on source IP, destination IP, port, and protocol. These rules further show the status as Allow or Deny status. It also enables threat intelligence features that can identify malicious IP addresses and irrelevant traffic.

What is Azure Network Security Groups (NSG)?

Azure Network Security Groups is a **fully managed** offering from Microsoft that helps **refine traffic from and to Azure VNet.** The Azure NSG consists of certain security rules that users can allow or deny at their convenience. Evaluation of these rules is done through a **5-tuple hash**. The 5-tuple hash takes values from the Source port number, IP Addresses, Destination IP address and port number, etc. It allows to associate Network Security Groups with a VNet or a VM network interface very easily, and it works on layers 3 and 4 of the OSI model.

How does Azure Network Security Groups work?



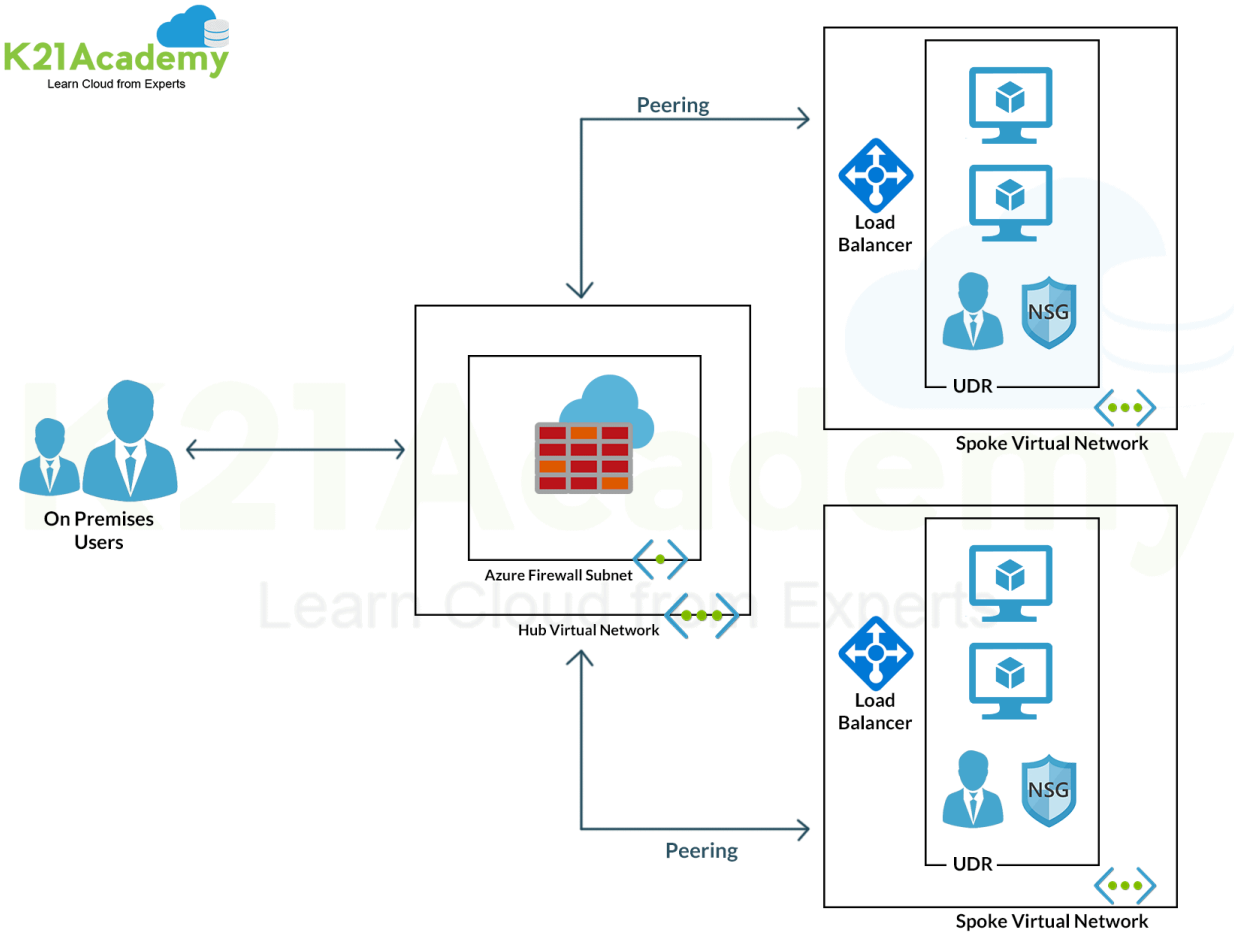
Azure Network Security Group (NSG) is a great solution offered by Microsoft to protect virtual **networks.** Using this, administrators can comfortably organize, filter, direct and limit various network traffic flows. You can **set different inbound and outbound rules** to allow or deny a specific type of traffic to configure Azure Network Security Group. If you want to use Azure Network Security Groups, you need to create it and configure individual rules.

You can define any rules required as per the situation, such as to define whether the traffic flowing through the network is safe and needs to be permitted or not.

Difference between Azure Firewall vs NSG (Azure Network Security Groups)

Let's see how Azure Firewall vs NSG differentiates from each other:

Azure Firewall	Azure Network Security Groups
Azure Firewall is a **robust service** and a fully managed firewall.	Azure Network Security Group is a **basic firewa**
It is loaded with tons of features to **ensure maximum protection** of your resources.	This solution is used to **filter traffic** at the netwo layer.
It can **analyze and filter** L3, L4 traffic, and L7 application traffic.	No such facility is available in Azure NSG.
Azure Firewall provides full support to application **FQDN tags**.	This feature is not available in Azure NSG.
It allows you to **mask the source and destination** network addresses	This feature is missing here.
It offers a **threat intelligence-based filtering** option.	This feature is missing in NSG.



Feature Comparison

Let's compare Azure Firewall and Azure NSG based on their features.

Service Tags:

Service tags act as a **label** that shows a **range of IP addresses** for specific services such as Data Lake, Container Registry, Azure Key Vault, etc. Both Azure Firewall and NSG provide full support to service tags, but users can't customize them as Microsoft manages them.

FQDN Tags

Azure Firewall only **supports FQDN Tags**. They signify a group of fully qualified domain names of Microsoft services such as Windows Update or Azure Backup. FQDN Tags are also managed by Microsoft and cannot be customized.

SNAT

SNAT stands for **Source Network Address Translation** and is supported by Azure Firewall only. This feature lets the Azure Firewall configure with a public IP address that you can use to mask the IP address of Azure resources that are sending out via the Firewall.

DNAT

DNAT stands for **Destination Address Translation**, and Azure Firewall supports this feature to translate incoming traffic to the firewall's public IP address to the private IP addresses of a VNet.

Q1. When should you use the Azure firewall instead of NSG?
Ans: Azure Firewall is a fully managed service that can filter and analyze the traffic of layers 3, 4, and 7 of the OSI model. Azure firewall service eliminates the need for Load Balancer and ensures 99.99% availability for two configured zones.

Q2. Is Azure firewall necessary?
Ans: Azure Firewall provides several security features by default to protect from Denial of Service protection, basic traffic monitoring, access control lists, or Intrusion. Hence, it is recommended to use Azure Firewall.

Q3. What is NSG in Azure?
Ans: NSG stands for Network Security Group. It activates a rule or access control list that allows or denies network traffic to virtual machines. You can associate NSG with either subnets or individual virtual machines.

Q4.Can you turn off the Azure firewall?
Ans: There are allocate and de-allocate methods available, which you can use via Azure PowerShell. Firewall billing stops and starts when you allocate or deallocate the firewall as per your requirement.

Q5. Do I need a firewall in the cloud?
Ans: Yes, you do need a firewall when you are using cloud computing. Cloud security does offer better security, but it is not sufficient for modern-day business needs. If you are constantly accessing the internet for any kind of work, firewall cloud security is much needed.