1. **Objective**:

- ✓ Prepare a R&D document on the working of NSG & ASG, Allowing specific IPs to access VMs and Deny Internet using NSG, Public IPs and Types, Static and Dynamic IP, Service tags, Allocate Static IPs to all VM's, Creating a Network Security Group, Creating Public IP, Associating/De-associating Public IP with virtual machine, Creation of Network Interface

2. Introduction

Microsoft Azure, or just **Azure** is the cloud computing platform developed by Microsoft.
It has management, access and development of applications and services to individuals, companies, and governments through its global infrastructure.

Azure Virtual Network is a service that provides the fundamental building block for your private network in Azure. An instance of the service (a virtual network) enables many types of Azure resources to securely communicate with each other, the internet, and on-premises networks. These Azure resources include virtual machines (VMs).

A virtual machine is like a physical computer, but it is actually a digital version of it. Actually, it is not so much different from physical computers because they have also memory, CPU, as well as they have disks to store our data or various files and one more interesting thing is that they can also connect to the internet.

A **virtual network** (VNet) allows you to specify an IP address range for the VNet, add subnets, associate network security groups, and configure route tables.

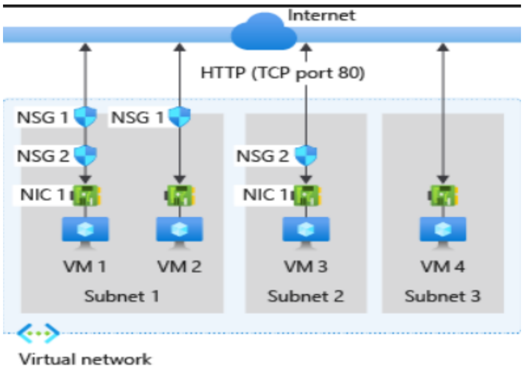
A **subnet** is a range of IP addresses in your VNet. You can launch Azure resources into a specified subnet. Use a **public subnet** for resources that need to connect to the Internet and a **private subnet** for resources that won't be connected to the Internet.

To protect the Azure resources in each subnet, use **network security groups**.

Azure Network security provides custom control over the inbound and outbound traffic to the Azure services. It facilitates with secure cloud network by defining the network security groups with customized rules specifying what protocol, IP address, ports based traffic are allowed to Azure services.

3. Network Security Group

A network security group contains security groups that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.



NSGs allow you to define security rules that filter network traffic based on source IP address, destination IP address, source port, destination port, and protocol. These rules can be applied to subnets, individual VMs, or network interfaces, making NSGs a fundamental tool for securing your Azure network infrastructure.

Inbound Traffic:

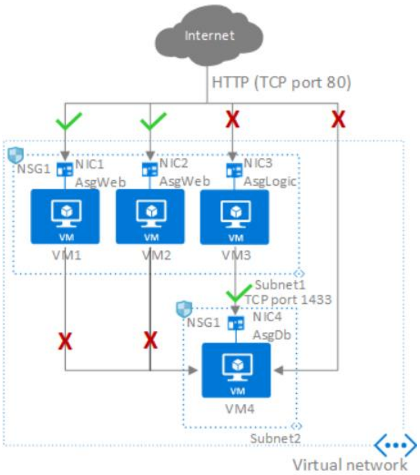
An inbound firewall protect against the network coming from the internet.
For inbound traffic, Azure processes the rules in a network security group associated to a subnet first, if there's one, and then the rules in a network security group associated to the network interface, if there's one.

Outbound Traffic:

An outbound firewall limits the access to the internet from inside.
For outbound traffic, Azure processes the rules in a network security group associated to a network interface first, if there's one, and then the rules in a network security group associated to the subnet, if there's one.

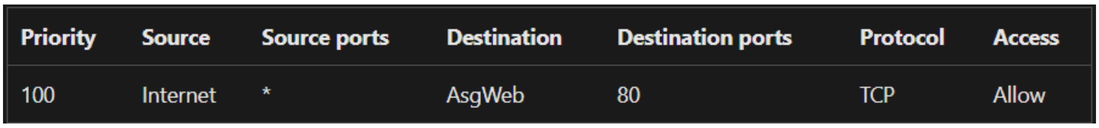
4. Application Security Groups

Application security groups enable you to configure network security as a natural extension of an application's structure, allowing you to group virtual machines and define network security policies based on those groups. You can reuse your security policy at scale without manual maintenance of explicit IP addresses. The platform handles the complexity of explicit IP addresses and multiple rule sets, allowing you to focus on your business logic.



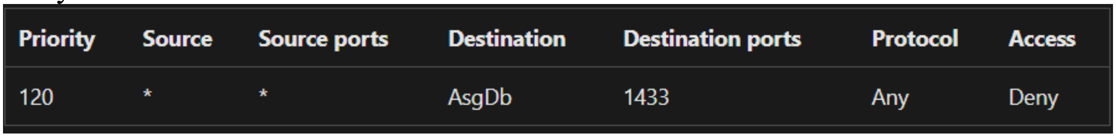
The primary purpose of ASGs is to define network security policies that allow or deny traffic between different tiers or components of an application. By creating ASGs and associating them with your VMs, you can control network traffic flow at a granular level, enabling you to enforce security policies between different application tiers.

Rules in ASG:
Allow-HTTP-Inbound-Internet



Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
100	Internet	*	AsgWeb	80	TCP	Allow

Deny-Database-All



Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
120	*	*	AsgDb	1433	Any	Deny

And many more..

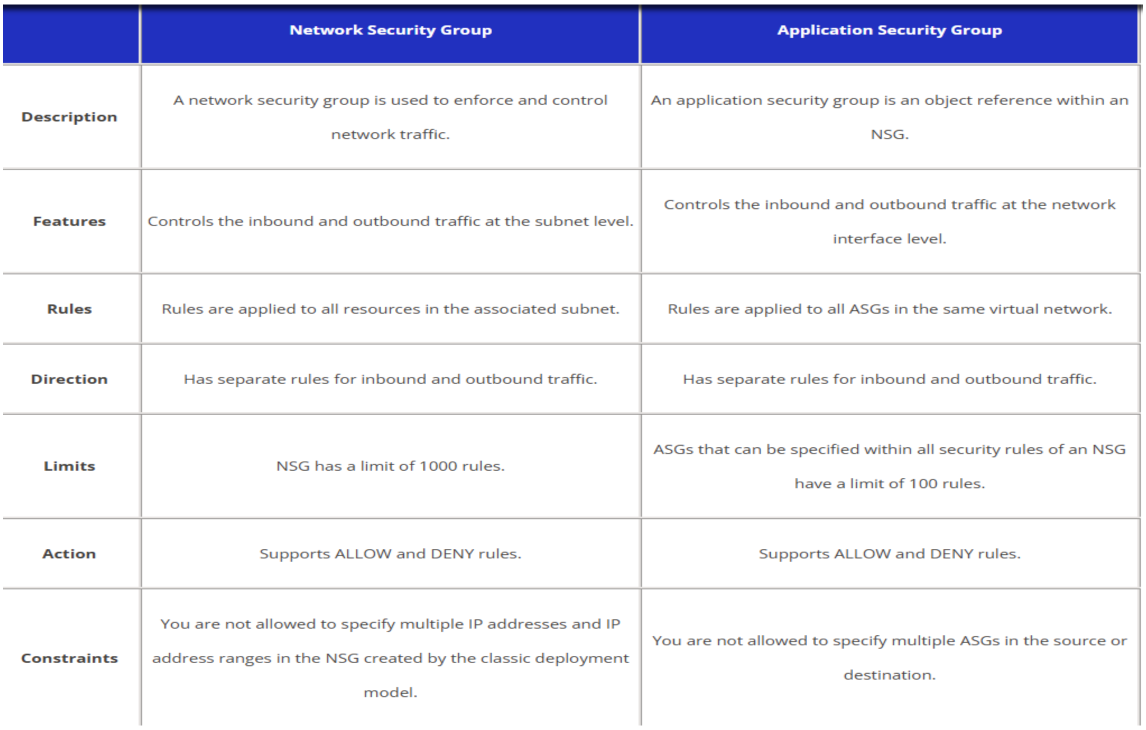
5. Difference between Application Security Group and Network Security Groups

- ✓ **Layer of Operation:** ASGs operate at the transport layer (Layer 4), while NSGs operate at both the network layer (Layer 3) and the transport layer (Layer 4).

- ✓ **Scope:** ASGs are primarily used for managing security between different application tiers, while NSGs focus on network-level security, controlling traffic flow within subnets, between subnets, and between virtual networks.

- ✓ **Granularity:** ASGs offer granular control over network traffic by allowing rules based on source and destination IP addresses and source and destination ports. NSGs provide broader network-level control, including protocol-based filtering

- ✓ **Application vs. Network:** ASGs are tailored for securing application components and enforcing policies specific to application tiers. NSGs, on the other hand, are designed for securing network infrastructure and implementing network-level security policies.



	Network Security Group	Application Security Group
Description	A network security group is used to enforce and control network traffic.	An application security group is an object reference within an NSG.
Features	Controls the inbound and outbound traffic at the subnet level.	Controls the inbound and outbound traffic at the network interface level.
Rules	Rules are applied to all resources in the associated subnet.	Rules are applied to all ASGs in the same virtual network.
Direction	Has separate rules for inbound and outbound traffic.	Has separate rules for inbound and outbound traffic.
Limits	NSG has a limit of 1000 rules.	ASGs that can be specified within all security rules of an NSG have a limit of 100 rules.
Action	Supports ALLOW and DENY rules.	Supports ALLOW and DENY rules.
Constraints	You are not allowed to specify multiple IP addresses and IP address ranges in the NSG created by the classic deployment model.	You are not allowed to specify multiple ASGs in the source or destination.

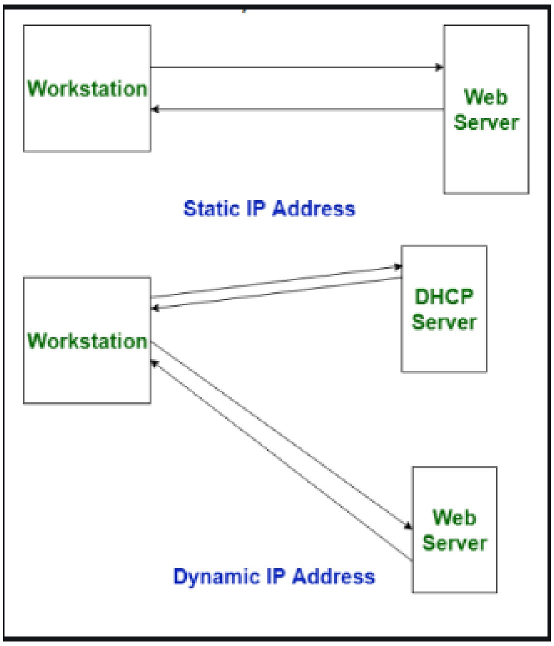
6. Static and Dynamic IP

A Static IP address is a fixed address that is manually assigned to a device for a long period of time. This type of IP address does not dynamically change with time, but will only change through an action done by the user or the network administrator. Assigning Static IP address is common in servers, network devices or any device that has to have a fixed address that can be accessed from a distance.

When Static IPs are Needed

Static IP addresses are especially important in cases where a device has to be quickly found over the internet on a permanent basis.

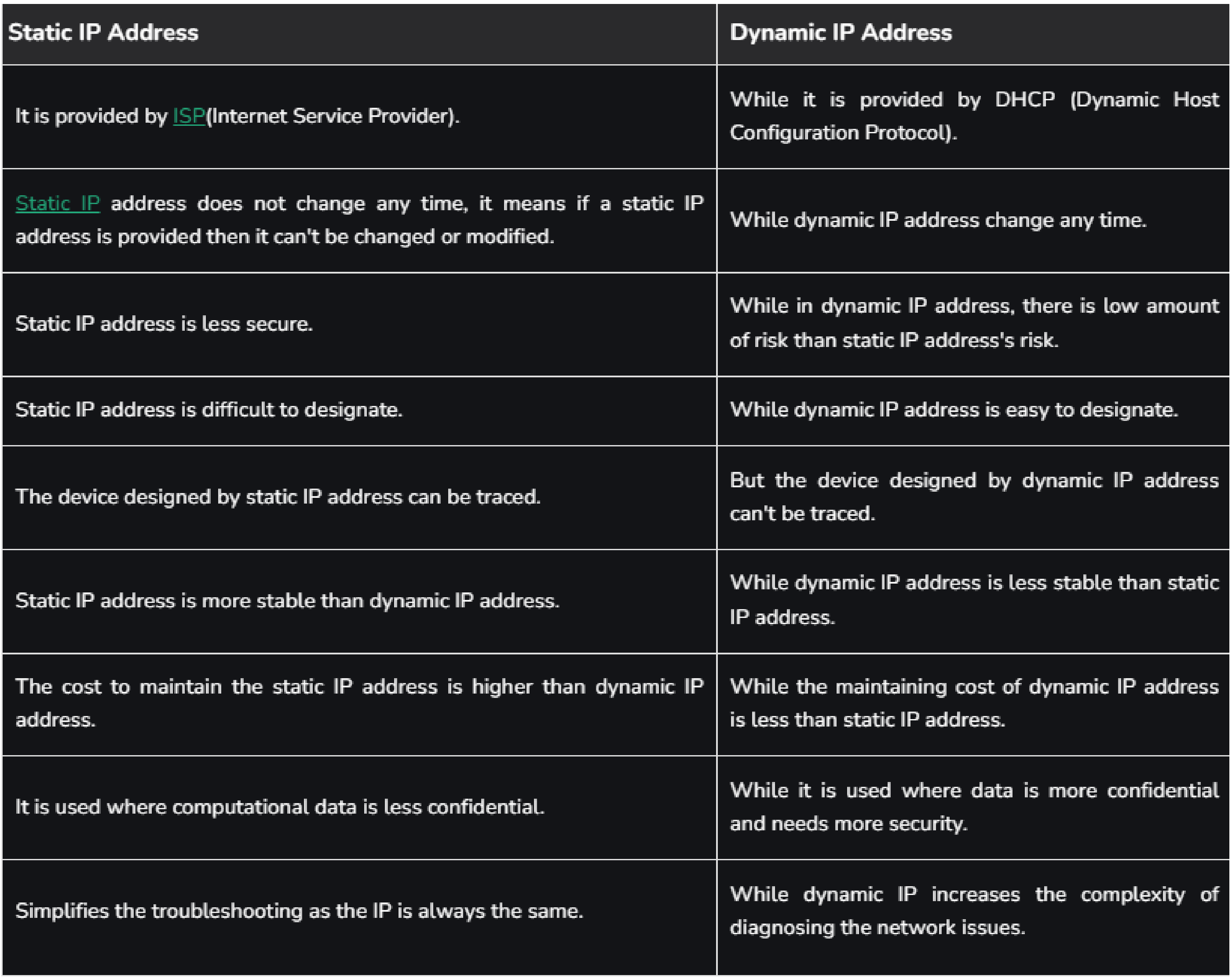
- Web Servers: A website must have one or more static IP addresses to be assigned to the domain always point to the correct server.
- Remote Access: Some of the devices that require a remote connection like the CCTV cameras or a VPN are preferable to be as static as possible.
- Hosting Servers: Game or email servers that are in constant use also need a static IP so that the services running in the background remain undisturbed.
- Secure Communications: Some devices that participate in secure communications might require static IPs to make the link stable and reliable.



A Dynamic IP Addresse is an IP address which is changed from time to time. In contrast to the static IP, an IPv6 address is obtained by DHCP server – (Dynamic Host Configuration Protocol) automatically. In the DHCP, a host receives an available IP address from the DHCP server for some period of time referred to as the lease time and the IP address given to the host may change.

Advantages of Dynamic IP Address

- **More Available and Cheaper**: Since there are more dynamic IPs and they cost less, they are more economical than static ones.
- **Better Security**: Dynamic IPs change each time you connect, making it harder for hackers to target your device.
- **Easy to Use**: You don’t have to worry about managing or setting up the IP, which makes it great for home use or people who aren't tech-savvy.



Static IP Address	Dynamic IP Address
It is provided by ISP(Internet Service Provider).	While it is provided by DHCP (Dynamic Host Configuration Protocol).
Static IP address does not change any time, it means if a static IP address is provided then it can't be changed or modified.	While dynamic IP address change any time.
Static IP address is less secure.	While in dynamic IP address, there is low amount of risk than static IP address's risk.
Static IP address is difficult to designate.	While dynamic IP address is easy to designate.
The device designed by static IP address can be traced.	But the device designed by dynamic IP address can't be traced.
Static IP address is more stable than dynamic IP address.	While dynamic IP address is less stable than static IP address.
The cost to maintain the static IP address is higher than dynamic IP address.	While the maintaining cost of dynamic IP address is less than static IP address.
It is used where computational data is less confidential.	While it is used where data is more confidential and needs more security.
Simplifies the troubleshooting as the IP is always the same.	While dynamic IP increases the complexity of diagnosing the network issues.

7. References:

- https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview
- https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works
- https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups
- https://www.cloudthat.com/resources/blog/difference-between-application-security-groups-asgs-and-network-security-groups-nsgs
- https://tutorialsdojo.com/network-security-group-nsg-vs-application-security-group/
- https://www.geeksforgeeks.org/computer-networks/difference-between-static-and-dynamic-ip-address/