Contents

[Public-IP 2](#_Toc502347636)

[Network Security Groups(NSG) 3](#_Toc502347637)

# **Public-IP**

MSFT Azure Resource Type  Microsoft.Network/publicIPAddresses

A public IP address is a **dynamic or static IP** address that you can assign to virtual machines, load balancers, and virtual network gateways to communicate with the Internet. Your public IP addresses are associated with your Azure subscription, and can be moved freely between Azure resources. The address of **dynamic public IP** address may change when dissociated and moved between resources, or when the associated resource is shutdown or deleted. You can use a **static public IP** address to ensure that the assigned address remains the same, even if the associated resource is shutdown or deleted

***Significant Properties***:

* Address Type – Dynamic v/s Static
* DNS Label – Name stored in Azure DNS servers (optional)
* Address Version - IPv4 v/s IPv6 IP addresses. Currently IPV6 addresses can be assigned to Load Balancers

***Our Implementation/Example***:

We will include a **dynamic public IP address** and this will be assigned to a Virtual Machine. This will allow us to connect and login to the VM using RDP.

RDP is only allowed from outside of the Virtual Network for VM’s which have a public IP address assigned to them.

Usage of a static public IP address is more common for VM’s which would host services like Domain Controllers and DNS.

# **Network Security Groups(NSG)**

MSFT Azure Resource Type  Microsoft.Network/networkSecurityGroups

A network security group is a layer of security that acts as a **virtual firewall** for controlling traffic in and out of virtual machines (via network interfaces) and subnets. It contains a set of security rules that **allow or deny** inboundand outbound traffic using the following **5-tuple**: protocol, source IP address range, source port range, destination IP address range, and destination port range. A network security group can be associated to multiple network interfaces and subnets, but each network interface or subnet can be associated to only one network security group.

Security rules are evaluated in priority-order, starting with the lowest number rule, to determine whether traffic is allowed in or out of the network interfaces or subnets associated with the network security group. A network security group has separate ***inbound and outbound rules***, and each rule can allow or deny traffic. Each network security group has a set of default security rules, which allows all traffic within a virtual network and outbound traffic to the internet. There is also a rule to allow traffic originating from Azure's load balancer probe. All other traffic is automatically denied. These default rules can be overriden by specifying rules with a lower priority number.

***Significant Properties***:

* Inbound Security Rules – (Allow/Deny)
* Outbound Security Rules – (Allow/Deny)

***Our Implementation/Example***:

We will include a **3 NSG’s** as part of the implementation and this will be assigned as below.

1. Default NSG – illustrates the default set of rules added by Azure
2. RDP NSG – Add an additional inbound rule to allow traffic for RDP. This will be assigned at a VM Nic level
3. Web traffic NSG – Add inbound rules to allow http/https web traffic. This will be assigned at the subnet level