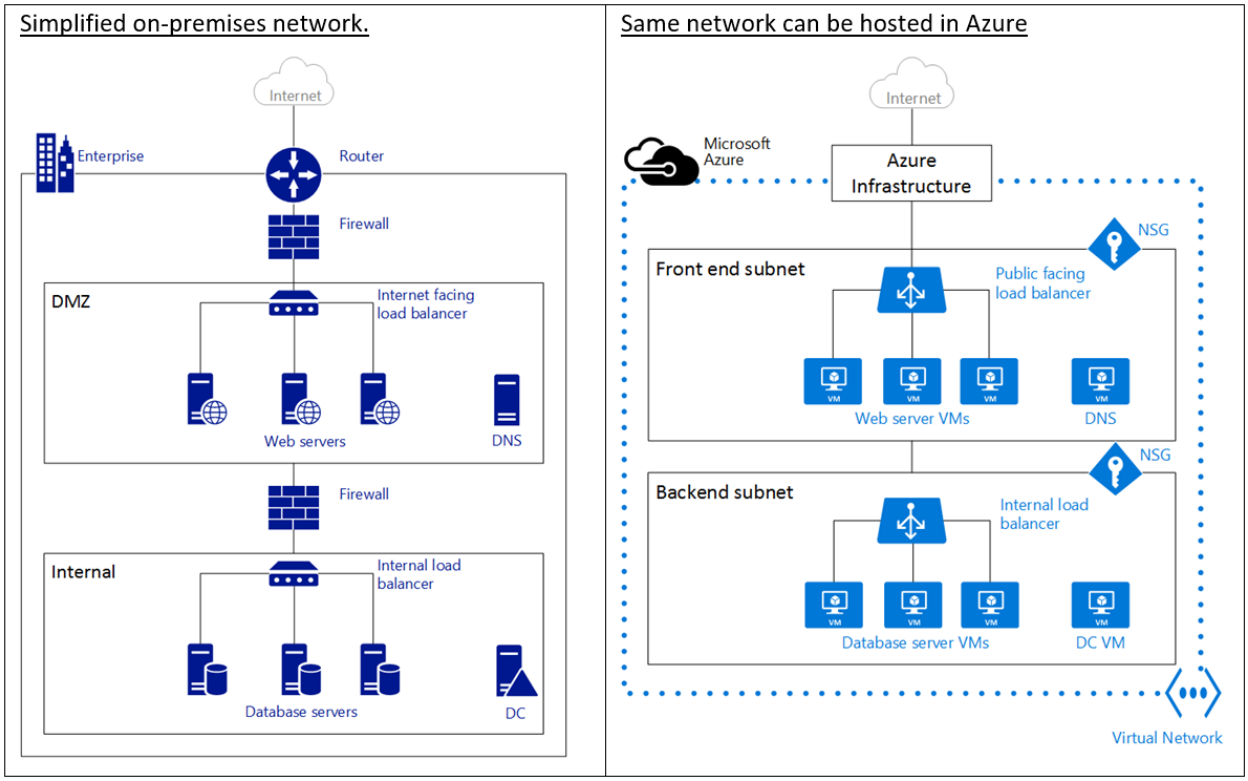
Overview of Azure Networking

- An Azure virtual network (VNet) is a representation of your own network in the cloud.
- It is **a logical isolation** of the Azure cloud dedicated to your subscription. You can fully control the IP address blocks, DNS settings, security policies, and route tables within this network.
- You can also further segment your VNet into **subnets** and launch Azure virtual machines (VMs).
- You can connect the virtual network to your on-premises network using one of the connectivity options available in Azure. In essence, you can expand your network to Azure, with complete control on IP address blocks with the benefit of enterprise scale Azure provides.



*In computer **networks**, a **DMZ** (**demilitarized zone**) is a physical or logical **sub-network** that separates an internal local area **network** (LAN) from other untrusted **networks**, usually the Internet. Notice how the Azure infrastructure takes on the role of the router, allowing access from your VNet to the public Internet without the need of any configuration.

Firewalls can be substituted by Network Security Groups (NSGs) applied to each individual subnet. And physical load balancers are substituted by internet facing and internal load balancers in Azure.

Subnet:

- Subnet is a **range of IP addresses** in the VNet, you can divide a VNet into multiple subnets for organization and security.

- VMs deployed to subnets (same or different) within a VNet can communicate with each other without any extra configuration.
- You can also configure route tables and NSGs to a subnet.

Network Interface Card (NIC):

- VMs communicate with other VMs and other resources on the network by using virtual network interface card (NIC). Virtual NICs configure VMs with private and optional public IP address.
- VMs can have more than one NIC for different network configurations.

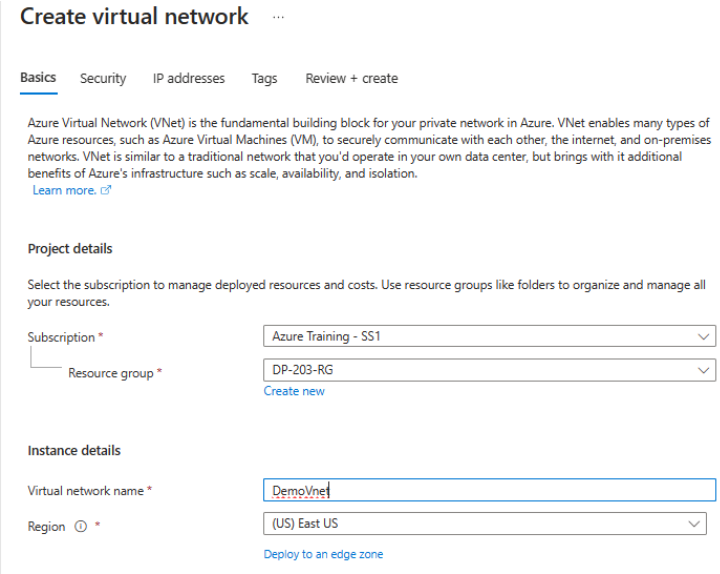
Network Security Group (NSG):

- You can create NSGs to control **inbound and outbound** access to network interfaces (NICs), VMs, and subnets. Each NSG contains one or more rules specifying whether traffic is **approved or denied** based on **source IP address, source port, destination IP address, and destination port.**

Lab 1: **Create Virtual Network and Subnet**

1. **Create Virtual Network (By default namespace is 10.0.0.0/16).If it is not available use(**192.168. 0.0)

Browse Virtual network→+Create→



Next → Next → Observe the default address range and default subnet and delete it.

2. Change the address space if required as (198.168.0.0)

Basics Security IP addresses Tags Review + create

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. Learn more

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. Learn more

Add IPv4 address space

192.168.0.0/16 Delete address space

192.168.0.0 /16 (65,536 addresses)

192.168.0.0 - 192.168.255.255 (65536 addresses)

+ Add a subnet

Subnets	IP address range	Size	NAT gateway

3. Add one subnet.

+ Add a subnet

Add a subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. Learn more

IP address space 192.168.0.0/16

192.168.0.0 - 192.168.255.255 (65536 addresses)

Subnet details

Subnet template Default

Name * FrontEnd

Starting address * 192.168.0.0

Subnet size /24 (256 addresses)

IP address space 192.168.0.0 - 192.168.0.255 (256 addresses)

Security

Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. Learn more

NAT gateway None

Create new

Network security group None

Create new

Route table None

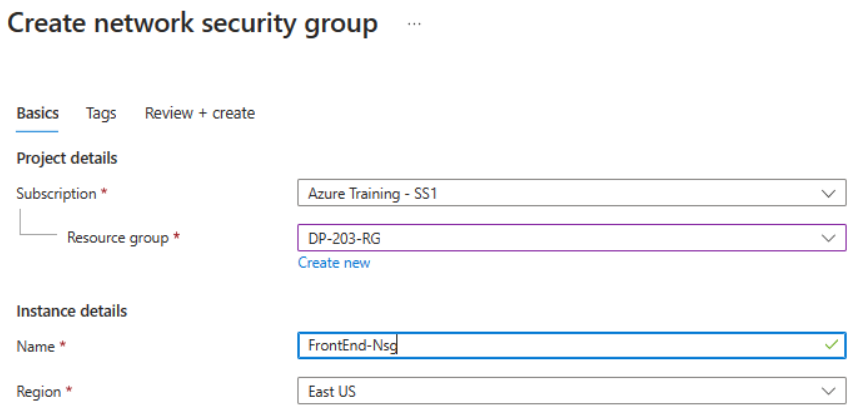
→ Add → Review + Create → Create.

4. Select VNet → Diagram (Under Monitoring)

Lab2: Create Network Security Group (NSG) and associate with FrontEnd Subnet

1. Create **NSG** for Frontend

Browse → Network Security Groups → +Create

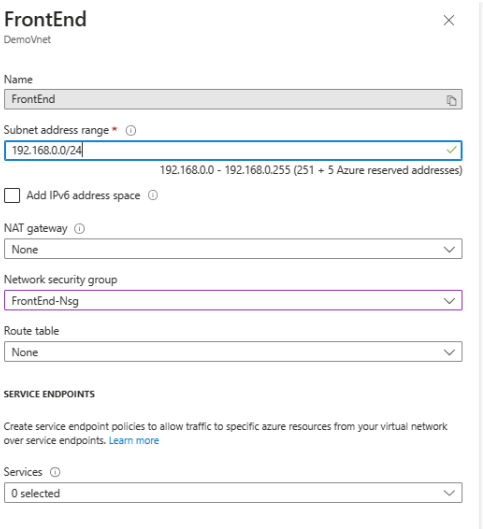


→Review + Create→Create

2. Associate the NSG to the FrontEnd subnet

Select your Vnet(DemoVnet) → Settings → Subnets → FrontEnd →

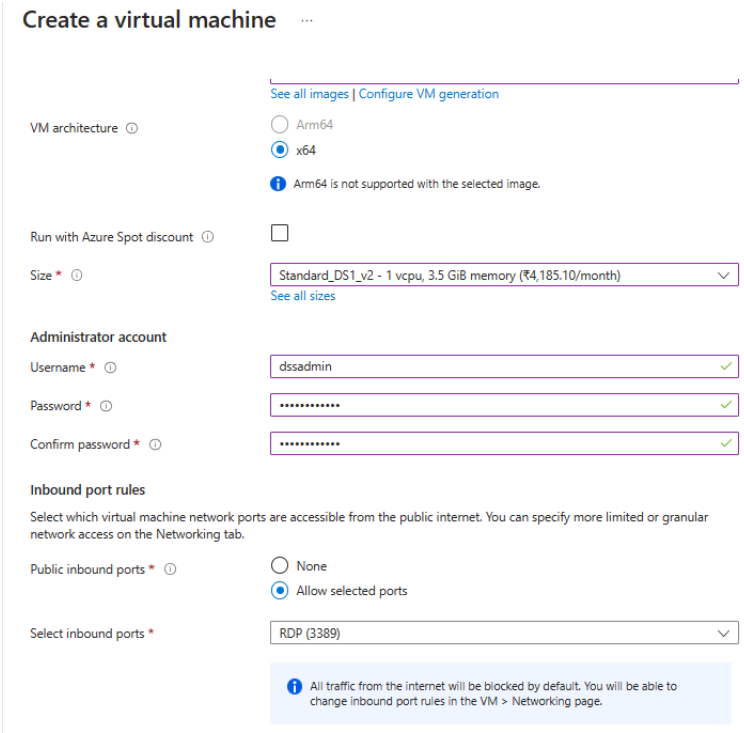
Network security group = **FrontEnd-Nsg**



→Save

Lab3: Create Virtual machine in FrontEnd Subnet and connect to VM

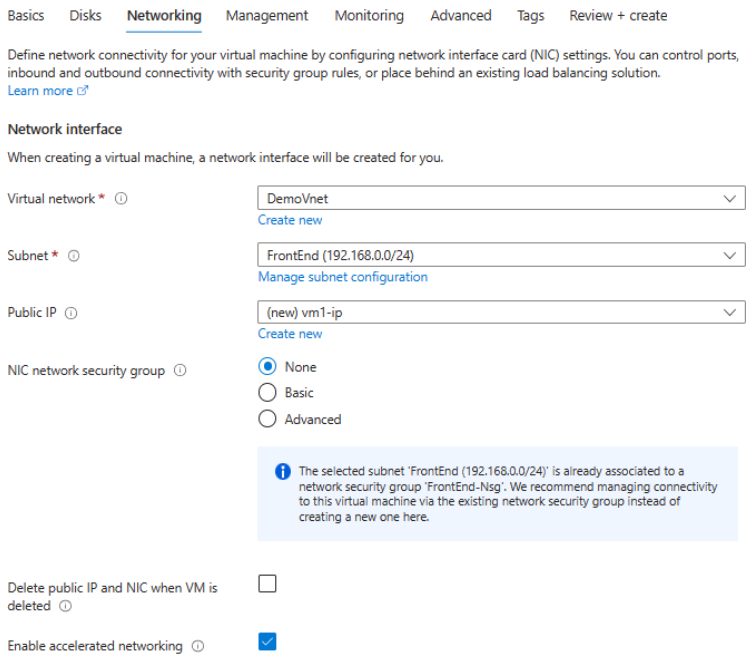
1. Browse → Virtual Machine → +Create → Azure Virtual Machine →



Public inbound ports: None

2. Next → Accept all defaults in Disks tab → Next

3. Go to Networking Tab →



Review + Create → Create

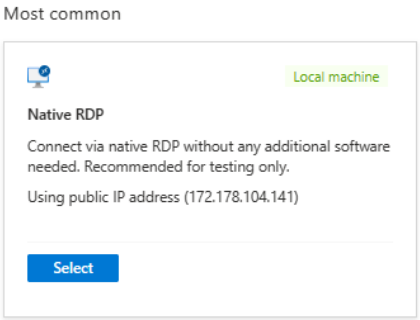
Lab4: Connect to Virtual machine using RDP and Configure Inbound rule for FrontEnd-Nsg

Frontend-nsg. The front end NSG will be applied to the *FrontEnd* subnet, and contain two rules:

a) **rdp-allow**: This rule will allow RDP traffic to the *FrontEnd* subnet.

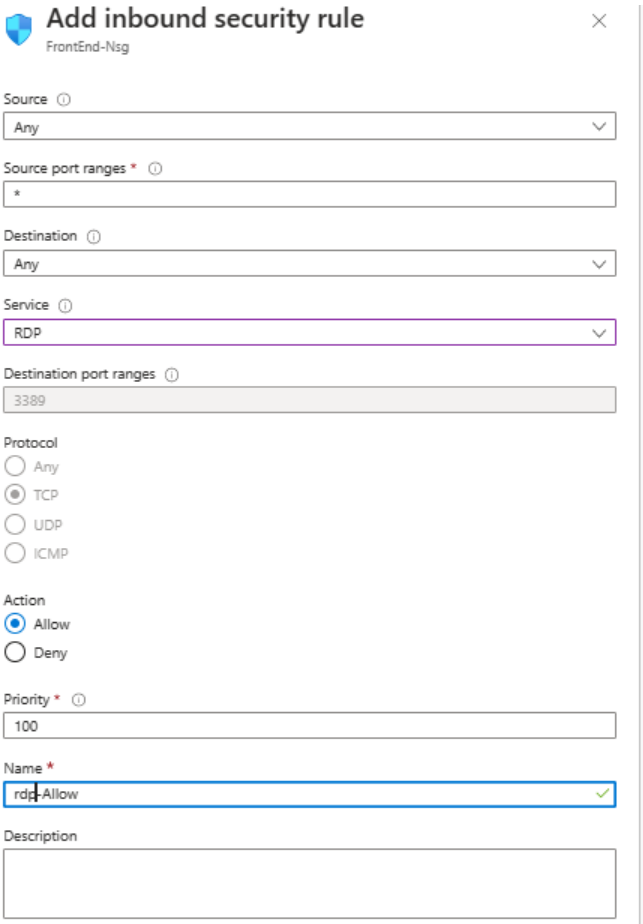
b) **web-allow:** This rule will allow HTTP traffic to the *FrontEnd* subnet.

1. VM1→connect→Native RDP→Select→Download RDP File



2.
3. Observe that you won't be able to connect
4. Configure Security rules for Frontend-Nsg

   Select Frontend-nsg → Settings → **Inbound security rules → +Add**



→Add

5. Try now to connect to Virtual Machine using RDP again and it will be successful.

Lab5: Install IIS on Virtual machine and allow http traffic to VM

1. Connect to VM → Server Manager → Dashboard → Add roles and features → Next → Next → Next →

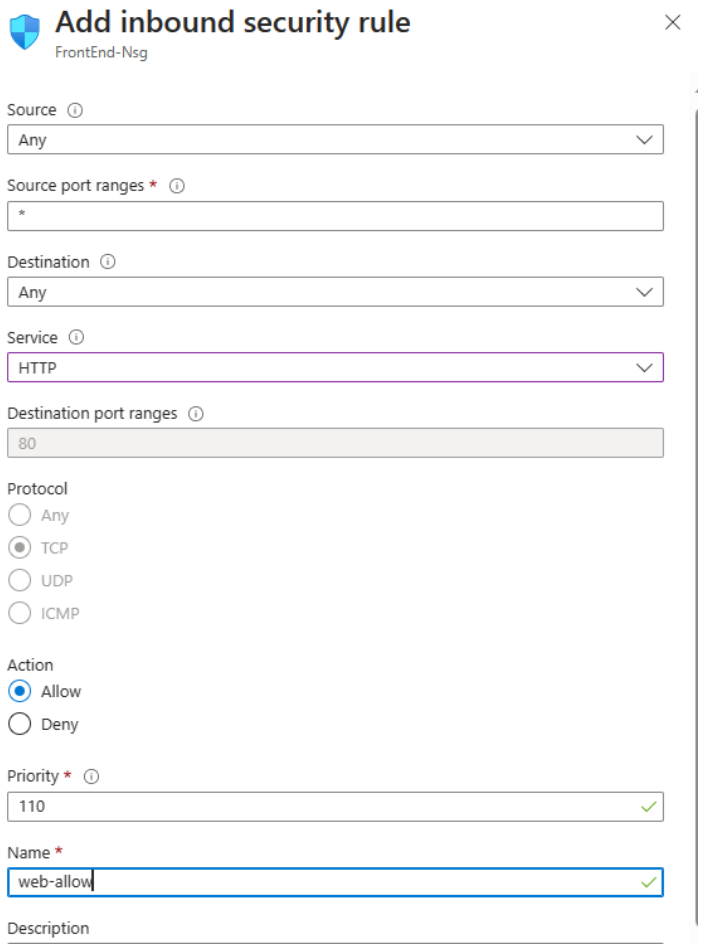
   Select Web server → Add feature→Next → Next → Install.

2. Azure Portal→Your vm→ Overview → Note the Public IP address→ In Browser → visit http://<PublicIPAddressOfVM>

   Observe that you are not able to reach vm using http.

3. Azure Portal → Select FrontEnd-Nsg → Networking → Add Inbound Rule →

Configure Rule to allow http to VM.



→ Add

4. Select VM → Overview → Note the Public IP address
5. In Browser → visit http://<PublicIPAddressOfVM>
6. Note that you get the default page of the website.