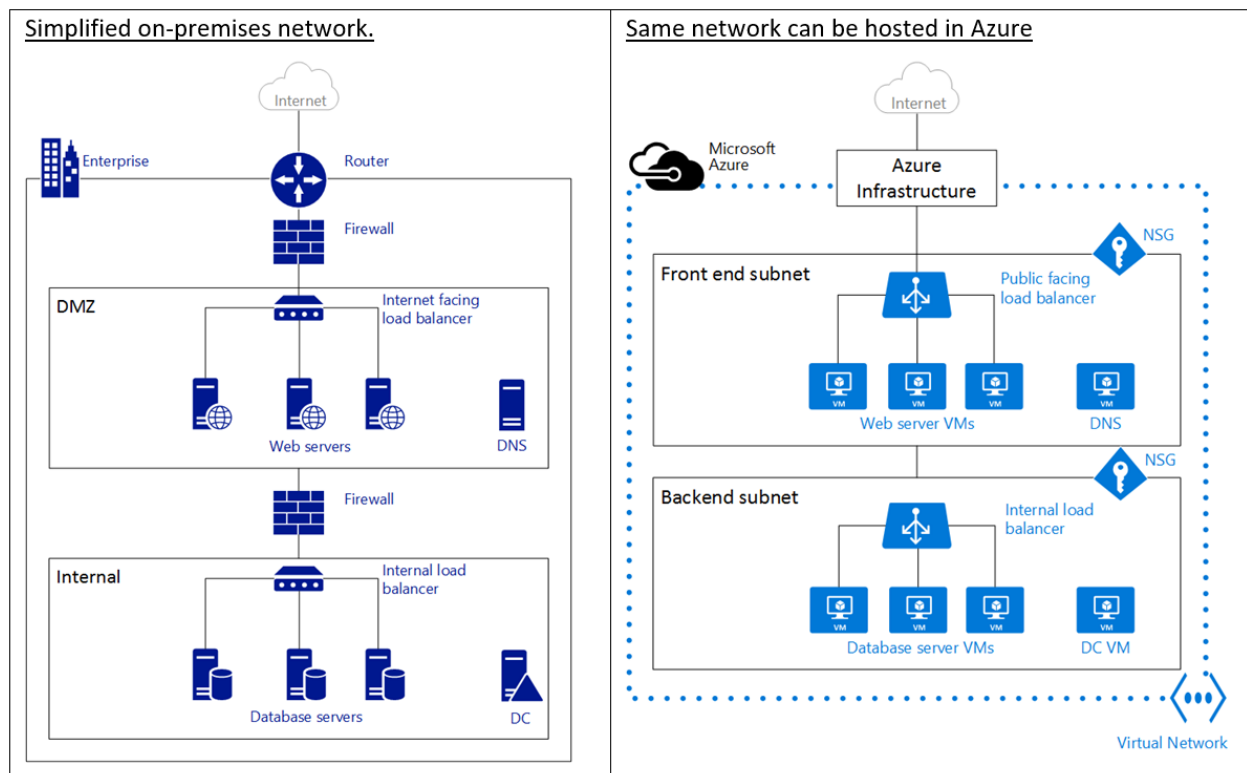


Overview of Azure Networking

- 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 →

Create virtual network

[Basics](#)
[Security](#)
[IP addresses](#)
[Tags](#)
[Review + create](#)

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.

[Learn more.](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Azure Training - SS1

Resource group *

DP-203-RG

[Create new](#)

Instance details

Virtual network name *

DemoVnet

Region ⓘ *

(US) East US

[Deploy to an edge zone](#)

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)

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

Create network security group ...

Basics Tags Review + create

Project details

Subscription * Azure Training - SS1 ▼

Resource group * DP-203-RG ▼
[Create new](#)

Instance details

Name * FrontEnd-Nsg ✓

Region * East US ▼

→Review + Create→Create

2. Associate the NSG to the FrontEnd subnet

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

Network security group = **FrontEnd-Nsg**

FrontEnd ×

DemoVnet

Name FrontEnd 🔍

Subnet address range * 📘
192.168.0.0/24 ✓
192.168.0.0 - 192.168.0.255 (251 + 5 Azure reserved addresses)

☐ Add IPv6 address space 📘

NAT gateway 📘
None ▼

Network security group
FrontEnd-Nsg ▼

Route table
None ▼

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services 📘
0 selected ▼

→Save

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

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

Create a virtual machine ...

[See all images](#) | [Configure VM generation](#)

VM architecture ⓘ

☐ Arm64

☒ x64

i Arm64 is not supported with the selected image.

Run with Azure Spot discount ⓘ ☐

Size * ⓘ Standard_DS1_v2 - 1 vcpu, 3.5 GiB memory (₹4,185.10/month) ▼

[See all sizes](#)

Administrator account

Username * ⓘ dssadmin ✓

Password * ⓘ ***** ✓

Confirm password * ⓘ ***** ✓

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ ☐ None

☒ Allow selected ports

Select inbound ports * RDP (3389) ▼

i All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

Public inbound ports: None

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

3. Go to Networking Tab →

Basics Disks **Networking** Management Monitoring Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * ⓘ DemoVnet ▼

[Create new](#)

Subnet * ⓘ FrontEnd (192.168.0.0/24) ▼

[Manage subnet configuration](#)

Public IP ⓘ (new) vm1-ip ▼

[Create new](#)

NIC network security group ⓘ ☒ None

☐ Basic

☐ Advanced

i The selected subnet 'FrontEnd (192.168.0.0/24)' is already associated to a network security group 'FrontEnd-Nsg'. We recommend managing connectivity to this virtual machine via the existing network security group instead of creating a new one here.

Delete public IP and NIC when VM is deleted ⓘ ☐

Enable accelerated networking ⓘ ☒

Review + Create → Create

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

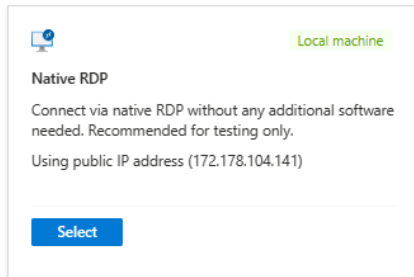
Frontend-nsg. The front end NSG will be applied to the *FrontEnd* subnet, and contain two rules:

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

Most common



- 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 inbound security rule** ×

Source ⓘ
Any ▼

Source port ranges * ⓘ
*

Destination ⓘ
Any ▼

Service ⓘ
RDP ▼

Destination port ranges ⓘ
3389

Protocol
☐ Any
☒ TCP
☐ UDP
☐ ICMP

Action
☒ Allow
☐ Deny

Priority * ⓘ
100

Name *
rdp-Allow ✓

Description

→Add

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

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 inbound security rule ×
FrontEnd-Nsg

Source ⓘ
Any

Source port ranges * ⓘ
*

Destination ⓘ
Any

Service ⓘ
HTTP

Destination port ranges ⓘ
80

Protocol
☐ Any
☒ TCP
☐ UDP
☐ ICMP

Action
☒ Allow
☐ Deny

Priority * ⓘ
110 ✓

Name *
web-allow ✓

Description

→ 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.