

Portfolio Lab Report By THATO KGOLE
Date: November 2025
Cloud PlatForm: Microsoft Azure

OVERVIEW

This lab demonstrates the configuration and security setup of an Azure Virtual Network environment with multiple subnets, Network Security Groups, and connected Virtual Machines.

The goal was to simulate a real-world enterprise network that securely manages internal communication between application tiers

PROBLEM STATEMENT

In cloud environments, multiple services such as virtual machines, databases, and web applications must communicate efficiently and securely.

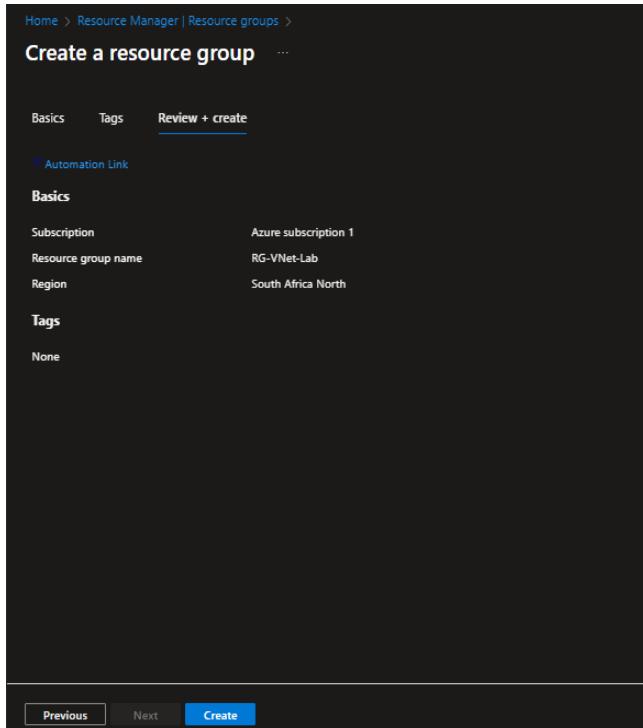
Without proper network design, services may be exposed to public access or experience internal connection failures

This project explores how to design, configure, and secure Azure Virtual Network to ensure controlled internal communication between resources using subnets and security boundaries.

Step 1: Create a Resource Group

This acts as a logical container for all the lab's resources.

In the Azure Portal, navigate to Resource Groups and create one.



Step 2: Create a Virtual Network (VNet)

Go to Networking - Virtual Networks and create a new Vnet.

Define two subnets – Frontend and Backend

Ensure both subnets have non-overlapping IP ranges to prevent routing conflicts.

Home > Network foundation | Virtual networks >

Create virtual network

Validation passed

Basics Security IP addresses Tags Review + create

view automation template

Basics

Subscription	Azure subscription 1
Resource Group	RG-VNet-Lab
Name	VNet-Lab
Region	South Africa North

Security

Azure Bastion	Disabled
Azure Firewall	Disabled
Azure DDoS Network Protection	Disabled

IP addresses

Address space	10.0.0.0/16 (65,536 addresses)
Subnet	Frontend-subnet (10.0.0.0/24) (256 addresses)
Subnet	Backend-subnet (10.0.1.0/24) (256 addresses)

Tags

Previous Next Create Download a template for automation

Step 3: Create Network Security Groups

Create two NSGs - one for each subnet

Frontend-NSG

Backend-NSG

Home > Network foundation | Network security groups >
Create network security group ...

Validation passed

Basics Tags Review + create

Basics

Subscription	Azure subscription 1
Resource group	RG-VNet-Lab
Region	South Africa North
name	NSG-Frontend

Tags

None

Create < Previous Next > Download a template for automation

Home > Network foundation | Network security groups >
Create network security group ...

Validation passed

Basics Tags Review + create

Basics

Subscription	Azure subscription 1
Resource group	RG-VNet-Lab
Region	South Africa North
name	NSG-Backend

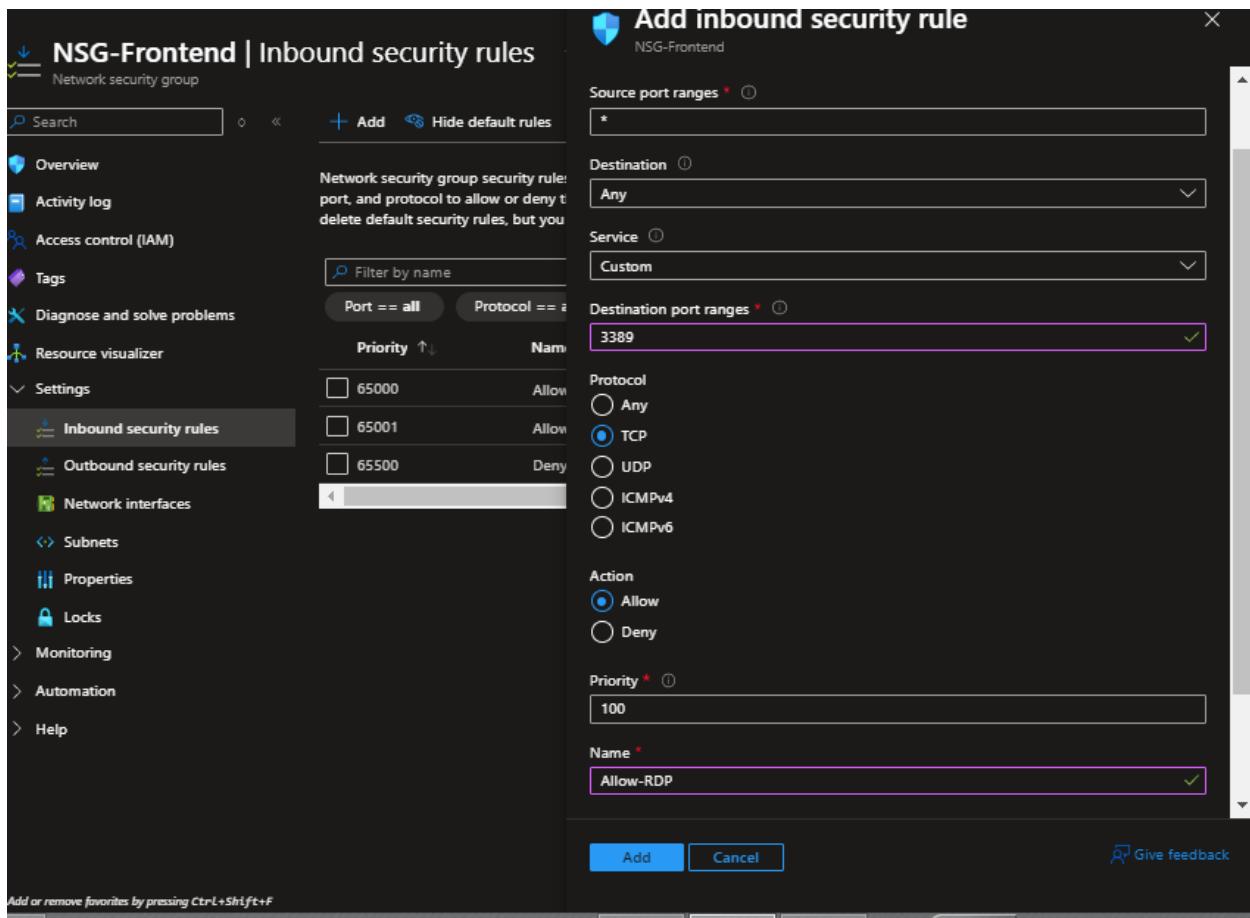
Tags

None

Create < Previous Next > Download a template for automation

Step 4: Configure NSG Rules

Inbound rule: Allow RDP (port 3389) to the Frontend subnet for administrative access
Outbound rule: Restrict the Backend subnet to only receive traffic from the Frontend subnet



The screenshot shows the Azure portal interface for managing Network Security Groups (NSGs). On the left, the navigation menu is open, showing options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Settings, Inbound security rules (which is selected), Outbound security rules, Network interfaces, Subnets, Properties, Locks, Monitoring, Automation, and Help. The main area displays the 'Inbound security rules' for the 'NSG-Frontend' group. A modal window titled 'Add inbound security rule' is open, allowing the creation of a new rule. The configuration includes:

- Source port ranges:** * (Any)
- Destination:** Any
- Service:** Custom
- Destination port ranges:** 3389
- Protocol:** TCP
- Action:** Allow
- Priority:** 100
- Name:** Allow-RDP

At the bottom of the modal, there are 'Add' and 'Cancel' buttons, and a 'Give feedback' link.

Step 5: Associate NSGs with subnets

Associate each NSG with its corresponding subnet to apply network rules.
This ensures traffic policies are applied automatically to all resources deployed within those subnets

NSG-Frontend | Subnets

Network security group

Search Associate

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Resource visualizer
- Subnets
- Properties
- Locks

Monitoring

Automation

Help

Add or remove favorites by pressing *Ctrl+Shift+F*

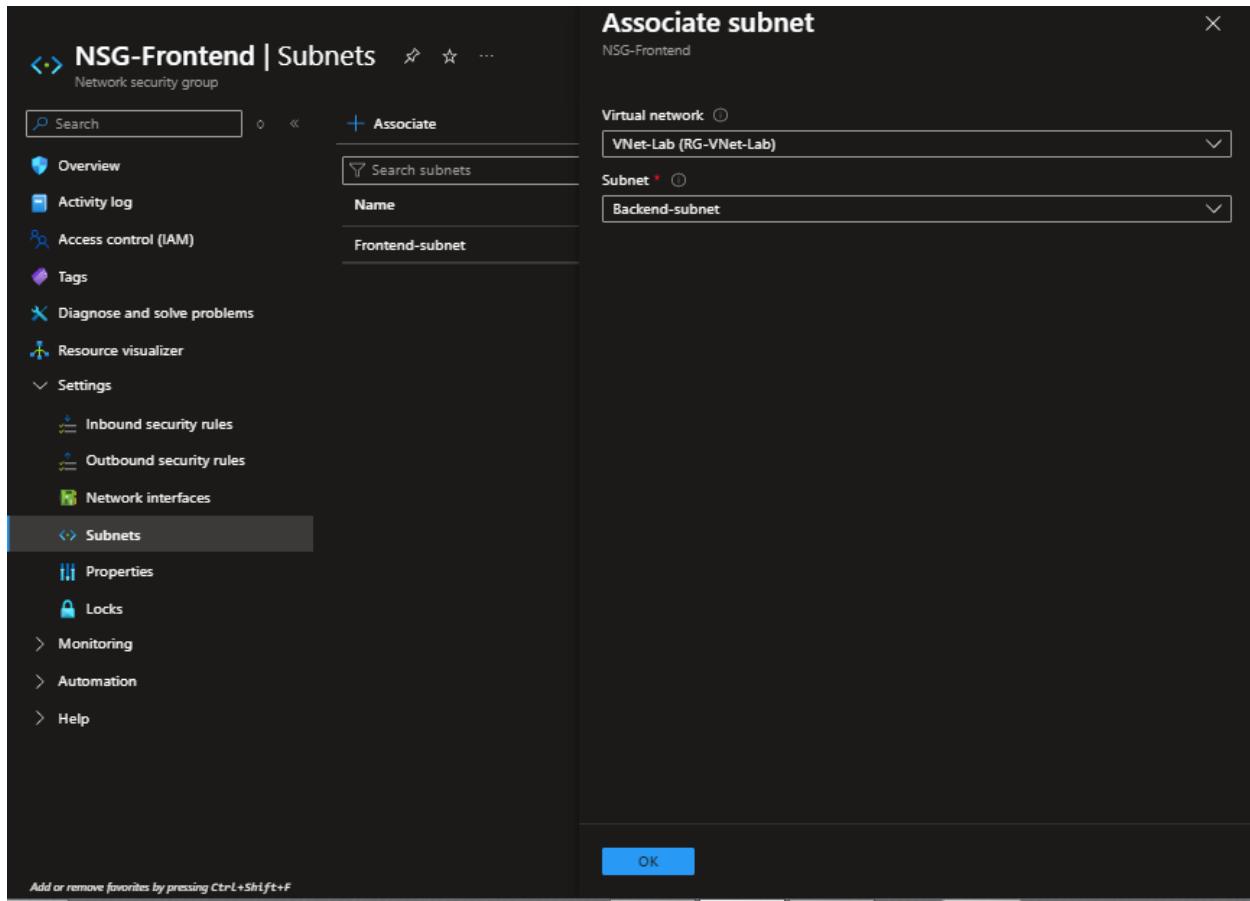
Associate subnet

NSG-Frontend

Virtual network VNet-Lab (RG-VNet-Lab)

Subnet * Frontend-subnet

OK



Step 6: Create two Virtual Machines

Home > Compute infrastructure | Virtual machines >

Create a virtual machine

Help me create a VM optimized for high availability Help me choose the right VM size for my workload Help me create a low cost VM

Validation passed

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my workload

Basics

Subscription	Azure subscription 1
Resource group	RG-VNet-Lab
Virtual machine name	VM-Frontend
Region	South Africa North
Availability options	No infrastructure redundancy required
Zone options	Self-selected zone
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable vTPM	Yes
Integrity monitoring	No
Image	Windows Server 2025 Datacenter - Gen2
VM architecture	x64
Size	Standard B1s (1 vcpu, 1 GiB memory)
Enable Hibernation	No
Username	zembe1722
Already have a Windows license?	No
Azure Spot	No

Disks

< Previous Next > Create

Networking

Virtual network	VNet-Lab
Subnet	Frontend-subnet
Public IP	(new) VM-Frontend-ip
NIC network security group	None
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No
Delete public IP and NIC when VM is deleted	Disabled

FRONTEND VM

Home > Compute infrastructure | Virtual machines >

Create a virtual machine

Validation passed

Help me choose the right VM size for my workload | Help me create a VM optimized for high availability | Help me create a low cost VM

Help me create a low cost VM | Help me create a VM optimized for high availability | Help me choose the right VM size for my workload

Basics

Subscription	Azure subscription 1
Resource group	RG-VNet-Lab
Virtual machine name	VM-Backend
Region	South Africa North
Availability options	No infrastructure redundancy required
Zone options	Self-selected zone
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable vTPM	Yes
Integrity monitoring	No
Image	Windows Server 2025 Datacenter - Gen2
VM architecture	x64
Size	Standard B1s (1 vcpu, 1 GiB memory)
Enable Hibernation	No
Username	zembe1722
Already have a Windows license?	No
Azure Spot	No

Disk

OS disk size: Image default

< Previous | Next > | Create

Networking

Virtual network	VNet-Lab
Subnet	Backend-subnet
Public IP	(new) VM-Backend-ip
NIC network security group	None
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No
Delete public IP and NIC when VM is deleted	Disabled

.BACKEND VM

Step 7: Test Connectivity Between VMs

**Use RDP to connect to the Frontend VM.
Open the command Prompt and run.**

ping <Backend-VM private IP>

The screenshot shows the 'VM-Frontend | Connect' blade in the Azure portal. The left sidebar has a 'Connect' section with 'Connect' selected. The main area displays connection details for a 'Native RDP' session:

- Source machine**: Windows, Local IP | 10.219.245.1, Connecting using RDP
- Destination VM**: Public IP | 4.221.167.68, Port 3389
- Connection prerequisites**: Check inbound RDP rules
- VM access**: Check access (button)
- Connect using RDP file**: Download RDP file
- Username**: zombie1722 (Forgot password? Reset password)
- Edit settings**

Below the main area, there's a link to 'More ways to connect (4)'.

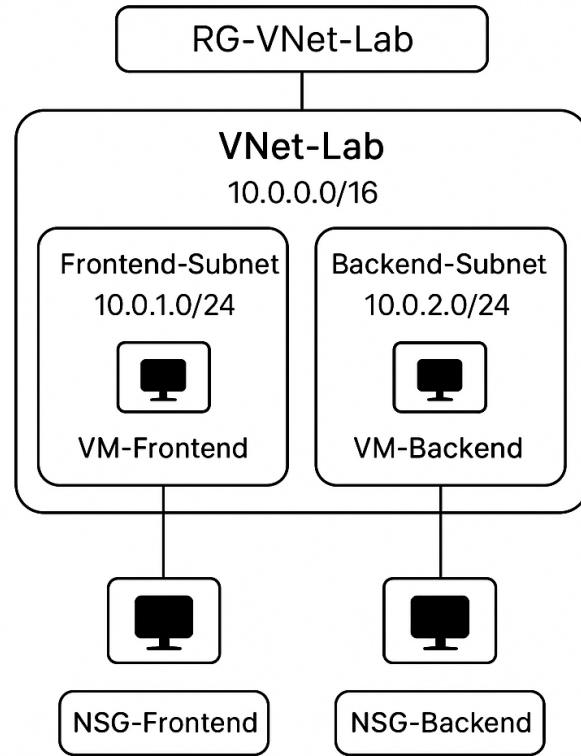
Step 8: Verifying All Resource

The screenshot shows the 'Resource Manager | Resource groups' blade in the Azure portal. The left sidebar has a 'Resource groups' section with 'RG-VNet-Lab' selected. The main area displays the 'RG-VNet-Lab' resource group details:

- Overview**: You are viewing a new version of Browse experience. Click here to access the old experience.
- Essentials**: Resources (11), Recommendations (0)
- Resources** table (JSON View):

Name	Type	Location
NSG-Backend	Network security group	South Africa North
NSG-Frontend	Network security group	South Africa North
VM-Backend	Virtual machine	South Africa North
VM-Backend-ip	Public IP address	South Africa North
vm-backend564	Network Interface	South Africa North
VM-Backend_OsDisk_1_5c1aeff2de73d4b82b606e6	Disk	South Africa North
VM-Frontend	Virtual machine	South Africa North
VM-Frontend-ip	Network Interface	South Africa North
vm-frontendl769	Network Interface	South Africa North
VM-Frontend_OsDisk_1_8a8da09671ed4286acbee	Disk	South Africa North
VNet-Lab	Virtual network	South Africa North

DIAGRAM



LEARNING OUTCOME

- .Configure and managed Azure Virtual Networks (Vnet and Subnets)***
- .Applied Network Security Groups to control traffic***
- .Deployed and connected multiple VMs securely***