

Secure Azure Virtual Network using Network security Groups

Portfolio Lab By THATO KGOLE

Date: November 2025

Cloud Platform: Microsoft Azure

Overview

This project demonstrates how to secure an Azure Virtual Machine using Network Security Groups.

We'll create and configure an NSG to control inbound and outbound network traffic-applying Zero Trust principles at the network layer.

Problem Statement

Organizations deploy VMs and applications in Azure, but without network segmentation and access controls, these resources are vulnerable to external attacks.

The challenge is to secure cloud-based servers from unwanted traffic while allowing authorized access for applications and administrators.

Step 1: Create a Resource Group

To group all related content for easy management.

All services > Resource Manager | Resource groups >

Create a resource group ...

Basics Tags Review + create

[Automation Link](#)

Basics

Subscription	ZEMBE
Resource group name	SecureInfraRG
Region	South Africa North

Tags

None

[Previous](#)

[Next](#)

[Create](#)

Step 2: Create a Virtual Network

It provides an isolated private network environment for your resources

Add 2 subnets one for public and one for private

All services > Network foundation | Virtual networks >

Create virtual network ...

Validation passed

Basics Security IP addresses Tags Review + create

Subscription	ZEMBE
Resource Group	SecureInfraRG
Name	SecureVnet
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	web-subnet (10.0.0.0/24) (256 addresses)
Subnet	app-subnet (10.0.1.0/24) (256 addresses)

[Previous](#)

[Next](#)

[Create](#)

[Download a template for automation](#)

Step 3: Create Network Security Group

To control traffic

All services > Network foundation | Network security groups >

Create network security group ...

 Validation passed

Basics Tags Review + create

Basics

Subscription	ZEMBE
Resource group	SecureInfraRG
Region	South Africa North
name	app-nsg

Tags

None

[Create](#)

[< Previous](#)

[Next >](#)

[Download a template for automation](#)

 Add inbound security rule

app-nsg

Source ⓘ
Any

Source port ranges * ⓘ
*

Destination ⓘ
Any

Service ⓘ
Custom

Destination port ranges * ⓘ
3389

Protocol
 Any
 TCP
 UDP
 ICMPv4
 ICMPv6

Action
 Allow
 Deny

Add Cancel 

Step 3: Create Virtual Machine without Public IP

Step 4: Enable Azure Defender For Cloud

It provides security recommendations and threat detection

Step 5: Configure Just-In-Time

To reduce the time ports are open

>Defender for cloud – VM (app-vm) –Enable

>Configure allowed ports (RDP)

Step 6: Create Azure Key Vault

To store VM admin secret

Review + Create

Basics

Subscription	ZEMBE
Resource group	SecureInfraRG
Key vault name	SecureKV1
Region	South Africa North
Pricing tier	Standard
Soft-delete	Enabled
Purge protection during retention period	Disabled
Days to retain deleted vaults	90 days

Access configuration

Azure Virtual Machines for deployment	Disabled
Azure Resource Manager for template deployment	Disabled
Azure Disk Encryption for volume encryption	Disabled
Permission model	Azure role-based access control

Networking

Connectivity method	Public endpoint (all networks)
---------------------	--------------------------------

[Previous](#) [Next](#) [Create](#)

Step 7: Enable Disk Encryption

Ensures VM disks are encrypted at rest.

>>Encrypted by default

 Create a secret ...

Upload options	<input type="button" value="Manual"/>
Name *	<input type="text" value="vmAdminPassword"/> ✓
Secret value *	<input type="password" value="*****"/> ✓
Content type (optional)	<input type="text"/>
Set activation date	<input type="checkbox"/>
Set expiration date	<input type="checkbox"/>
Enabled	<input type="radio" value="Yes"/> Yes <input type="radio" value="No"/> No
Tags	0 tags

[Create](#)

[Cancel](#)

Step 8: Attach Key Vault To VM

To avoid storing credentials on the VM, let access Key Vault securely

>VM – Identity – System assigned – On – Save

>Key Vault – Access policies – Add Access Policy – VM's system identity – Add – Save

Step 9: Verify logging & monitoring

Ensures you can see security events–

Home > Log Analytics workspaces >

Create Log Analytics workspace ...

Validation passed

 Log Analytics workspace
by Microsoft

Basics

Subscription	ZEMBE
Resource group	SecureInfraRG
Name	SecWorkspace
Region	South Africa North

Pricing

Pricing tier	Pay-as-you-go (Per GB 2018)
--------------	-----------------------------

The cost of your workspace depends on the volume of data ingested and how long it is retained. Regional pricing details are available on the [Azure Monitor pricing page](#). You can change to a different pricing tier after the workspace is created. [Learn more](#) about Log Analytics pricing models.

Tags

None

[Create](#) [« Previous](#) [Download a template for automation](#)

Follow to complete

- >**Defender for cloud – setting – connect the subscription / resource to this workspace**
- >**VM – Monitoring – Diagnostic settings – Send quest-level logs/events to Log Analytics (selectWorkspace)**

DIAGRAM

