

# **LAB BY THATO KGOLE**

## **DATE : 24 NOVEMBER 2025**

## **DURATION : 1 HOUR**

## **CLOUD PLATFORM : MICROSOFT AZURE**

### **SECURE MULTI-TIER APPLICATION DEPLOYMENT USING NSGs & ASG ON AZURE**

#### **PROBLEM STATEMENT**

In modern cloud environments, organizations need to segregate networks and control access to resources to prevent unauthorized access and potential breaches.

Many cloud setups leave Web, App, and Database servers exposed, allowing unrestricted traffic, which can compromise sensitive data.

#### **PROJECT GOALS**

- . Deploy a multi-tier network (Web, App, DB) in Azure.
- . Use Network Security Groups to simplify traffic rules between VM groups.
- . Implement least privilege access from the internet and internal network.
- . Test and validate connectivity to ensure security policies work as intended.

#### **AZURE SERVICES USED**

- . Resource Group  
Organize and manage project resources.
- . Virtual Network (Vnet)  
Network backbone for Web, App, and DB subnets
- . Subnets  
Segregate Web, App, and DB servers
- . Network Security Groups  
Control traffic to/from subnets or VMs
- . Application Security Group  
Group VMs logically to simplify NSG rules
- . Virtual Machines  
Deploy Web, App, DB, and Management servers

#### **BUILD STEPS**

Step 1: Create Resource Group

Contains all projects resources in one organized structure

[Home](#) > [Resource groups](#) >

## Create a resource group ...

Basics   Tags   Review + create

[Automation Link](#)

### Basics

Subscription	ZEMBE
Resource group name	RG-SecureWebApp
Region	South Africa North

### Tags

None

[Previous](#)

[Next](#)

[Create](#)

## Step 2: Create Virtual Network

[Home](#) > [Network foundation](#) | [Virtual networks](#) >

## Create virtual network ...

✓ Validation passed

Basics   Security   IP addresses   Tags   Review + create

### Basics

Subscription	ZEMBE
Resource Group	RG-SecureWebApp
Name	Vnet-SecureApp
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	Subnet-Web (10.0.0.0/24) (256 addresses)
Subnet	Subnet-App (10.0.1.0/24) (256 addresses)
Subnet	Subnet-DB (10.0.2.0/24) (256 addresses)

### Tags

[Previous](#)

[Next](#)

[Create](#)

[Download a template for automation](#)

## Step 3: Create Application Security Groups

Home > Network foundation

## Network foundation | Application security groups

Preview

Sort Application Security Groups by creation date.

Identify non-compliant Application Security Groups in my environment. +1

Search

+ Create

Manage view

Refresh

Export to CSV

Open query

Assign tags

Add to service group

Group by none

Overview

Virtual network

Virtual Network overview

Virtual networks

NAT gateways

Public IP addresses

Network interfaces

Network security groups

Application security groups

Bastions

Route tables

Route servers

Private Link

DNS

Monitoring and management

Filter for any field...

Subscription equals all

Resource Group equals all

Location equals all

+ Add filter

<input type="checkbox"/>	Name		Network interfaces co...	Virtual network	Type	Resource Group	Location	Subscription
<input type="checkbox"/>	ASG-AppServer	***	0	-	Application security gr...	RG-SecureWebApp	South Africa North	ZEMBE
<input type="checkbox"/>	ASG-DBServer	***	0	-	Application security gr...	RG-SecureWebApp	South Africa North	ZEMBE
<input type="checkbox"/>	ASG-Management	***	0	-	Application security gr...	RG-SecureWebApp	South Africa North	ZEMBE
<input type="checkbox"/>	ASG-WebServer	***	0	-	Application security gr...	RG-SecureWebApp	South Africa North	ZEMBE

Showing 1 - 4 of 4. Display count: 30

Give feedback

Add or remove favorites by pressing Ctrl+Shift+F

## Step 4: Create Network Security Groups

Home > Network foundation | Network security groups

### Create network security group

Validation passed

Basics Tags Review + create

Basics

Subscription

ZEMBE

Resource group

RG-SecureWebApp

Region

South Africa North

Name

NSG-Web

Tags

None

Create

< Previous

Next >

Download a template for automation

### 4.1 NSG-Web (Attach to subnet-web)

Home > Network foundation | Virtual networks > Vnet-SecureApp

Network foundation | Virtual networks

Overview

Virtual network

Virtual Network overview

Virtual networks

NAT gateways

Public IP addresses

Network interfaces

Network security groups

Application security groups

Bastions

Route tables

Route servers

Private Link

DNS

Monitoring and management

Create

Manage view

...

You are viewing a new version of Browse experience. Click here to access the old experience.

Name ?

Vnet-SecureApp

Showing 1 - 1 of 1. Display count: au...

Add or remove favorites by pressing Ctrl+Shift+F

Vnet-SecureApp | Subnets

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

Address space

Connected devices

Subnets

Bastion

DDoS protection

Firewall

Microsoft Defender for Cloud

Network manager

DNS

Peering

Service endpoints

Private endpoints

Edit subnet

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

A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway. [Learn more](#)

Network security group

Route table

Service Endpoints

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

Services

Remove service endpoint

Subnet Delegation

Delegate subnet to a service

Network Policy for Private Endpoints

The network policy affects the types of network policies that control traffic going to the private endpoints in this subnet. [Learn more](#)

Private endpoint network policy

Save Cancel

Give feedback

## (NSG-WEB INBOUND RULES)

Home > Network foundation | Network security groups > NSG-Web

Network foundation | Network security groups

Overview

Virtual network

Virtual Network overview

Virtual networks

NAT gateways

Public IP addresses

Network interfaces

Network security groups

Application security groups

Bastions

Route tables

Route servers

Private Link

DNS

Monitoring and management

Create

Manage view

...

You are viewing a new version of Browse experience. Click here to access the old experience.

Name ?

NSG-App

NSG-DB

NSG-Management

NSG-Web

Showing 1 - 4 of 4. Display count: au...

Add or remove favorites by pressing Ctrl+Shift+F

NSG-Web | Inbound security rules

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Automation

Help

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

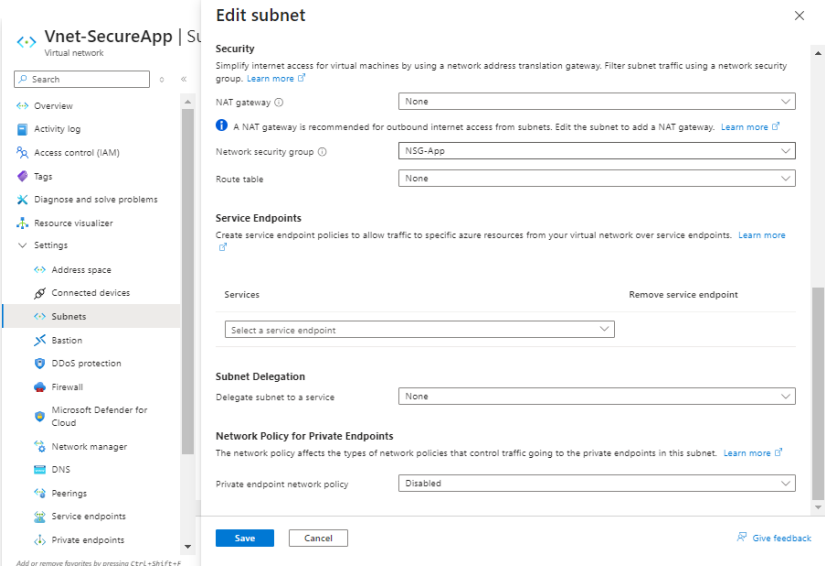
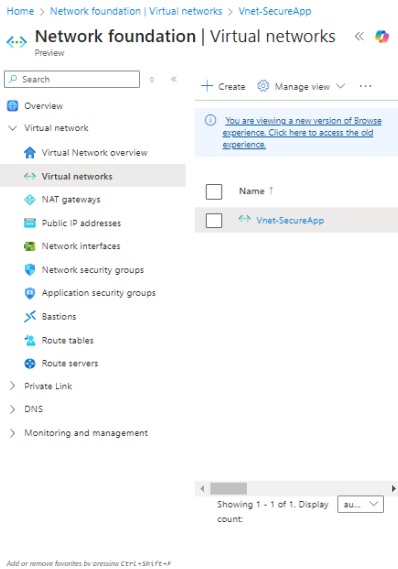
Filter by name

Port == all Protocol == all Source == all Destination == all Action == all

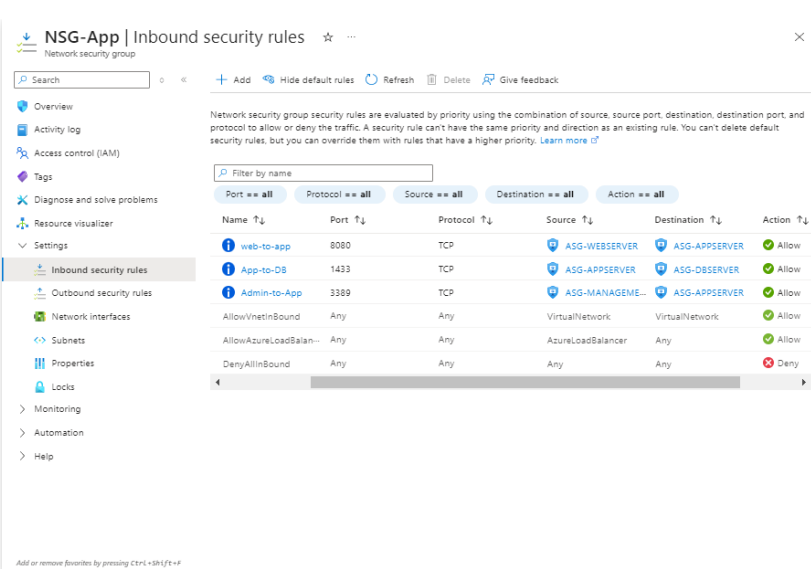
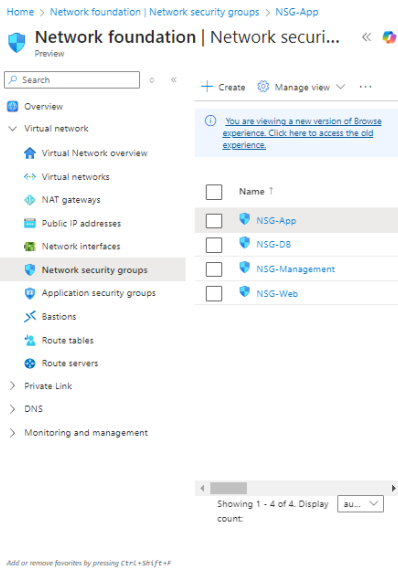
Name	Port	Protocol	Source	Destination	Action
Allow-HTTP	80	TCP	Any	ASG-WEBSEVER	Allow
Allow-HTTPS	443	TCP	Any	ASG-WEBSEVER	Allow
web-app	8080	TCP	ASG-WEBSEVER	ASG-APPSERVER	Allow
AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer	Any	Allow
DenyAllInBound	Any	Any	Any	Any	Deny

Add or remove favorites by pressing Ctrl+Shift+F

## 4.1 NSG-App (Attach to subnet-app)



## (NSG-APP INBOUND RULES)



## 4.3 NSG-DB (Attach to subnet-DB)

Home > Network foundation | Virtual networks > Vnet-SecureApp

Network foundation | Virtual networks

Search

+ Create ...

Overview

Virtual network

Virtual Network overview

Virtual networks

NAT gateways

Public IP addresses

Network interfaces

Network security groups

Application security groups

Bastions

Route tables

Route servers

Private Link

DNS

Monitoring and management

Showing 1 - 1 of 1. Display count.

au...

Vnet-SecureApp | Subnets

Search

+ Create ...

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

Address space

Connected devices

Subnets

Bastion

DDoS protection

Firewall

Microsoft Defender for Cloud

Network manager

DNS

Peerings

Service endpoints

Private endpoints

Edit subnet

Security

NAT gateway

None

Network security group

NSG-DB

Route table

None

Service Endpoints

Services

Remove service endpoint

Subnet Delegation

Delegate subnet to a service

None

Network Policy for Private Endpoints

Private endpoint network policy

Disabled

Save

Cancel

Give feedback

## (NSG-MGMT INBOUND RULES)

Home > Network foundation | Network security groups > NSG-Management

Network foundation | Network security groups

Search

+ Create Manage view ...

Overview

Virtual network

Virtual Network overview

Virtual networks

NAT gateways

Public IP addresses

Network interfaces

Network security groups

Application security groups

Bastions

Route tables

Route servers

Private Link

DNS

Monitoring and management

Showing 1 - 4 of 4. Display count.

au...

NSG-Management | Inbound security rules

Search

+ Add Hide default rules Refresh Delete Give feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Automation

Help

Filter by name

Port == all Protocol == all Source == all Destination == all Action == all

Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action
Allow-RDP-From----	3389	TCP	102.219.27.52	ASG-MANAGEMENT--	Allow
Allow-to-AppDB	3389	TCP	ASG-MANAGEMENT--	(multiple)	Allow
AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	Allow
DenyAllInBound	Any	Any	Any	Any	Deny

## 4.4 NSG-Management (Attached to VM NIC)

### Step 5: Create VM

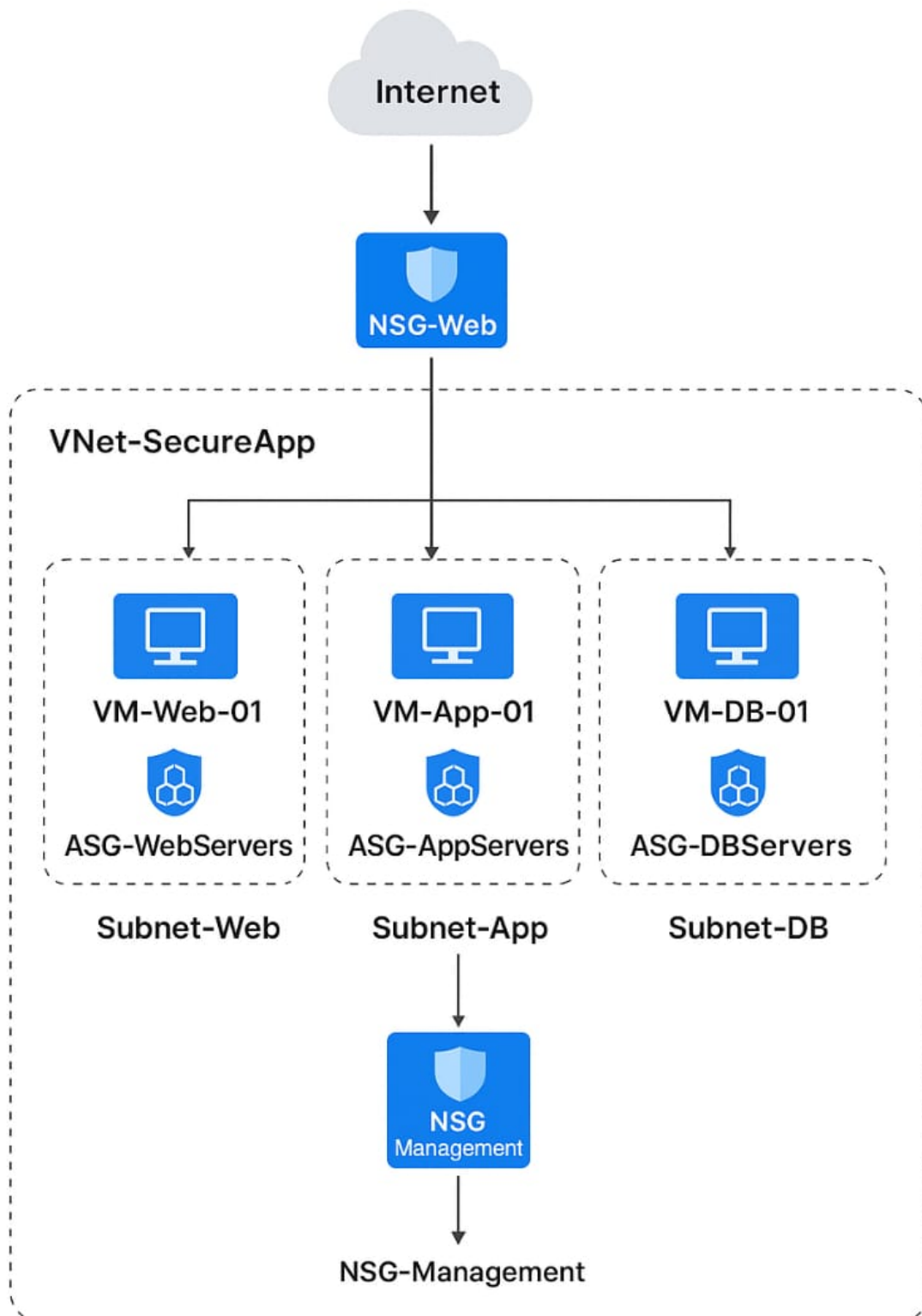
### 5.1 VM-Web







# Secure Multi-Tier Web Application Architecture Using NSGs and ASGs" Azure



## Conclusion

- . This project demonstrates a fully functional, multi-tier, secure Azure network:
- . Multi-tier architecture with Web, App, DB segregation
- . NSGs and ASGs implemented for least privilege access
- . Traffic control and segmentation validated via connectivity testing

## Key Learnings

- . Proper subnet segmentation improves security
- . ASGs simplify NSG rule management for multiple VMs
- . NSGs provide granular control over inbound and outbound traffic
- . Real-world enterprise security best practices