

**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

Search:  Create Manage view Refresh Export to CSV Open query Assign tags Add to service group Group by none

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

Filter for any field... Subscription equals all Resource Group equals all Location equals all Add filter

Name	Network interfaces co...	Virtual network	Type	Resource Group	Location	Subscription
ASG-AppServer	0	-	Application security gr...	RG-SecureWebApp	South Africa North	ZEMBE
ASG-DBServer	0	-	Application security gr...	RG-SecureWebApp	South Africa North	ZEMBE
ASG-Management	0	-	Application security gr...	RG-SecureWebApp	South Africa North	ZEMBE
ASG-WebServer	0	-	Application security gr...	RG-SecureWebApp	South Africa North	ZEMBE

Bastions Route tables Route servers Private Link DNS Monitoring and management

Showing 1 - 4 of 4. Display count:

Give feedback

## 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)

**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: None

Network security group: NSG-Web

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: Select a service endpoint

**Subnet Delegation**  
Delegate subnet to a service: None

**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: Disabled

**Save** **Cancel** **Give feedback**

## (NSG-WEB INBOUND RULES)

**NSG-Web | Inbound security rules**

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](#)

Name	Port	Protocol	Source	Destination	Action
Allow-HTTP	80	TCP	Any	ASG-WEBSERVER	Allow
Allow-HTTPS	443	TCP	Any	ASG-WEBSERVER	Allow
web-app	8080	TCP	VirtualNetwork	VirtualNetwork	Allow
DenyAllInBound	Any	Any	AzureLoadBalancer	Any	Deny

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

**Network foundation | Virtual networks**

**Edit subnet**

**(NSG-APP INBOUND RULES)**

**NSG-App | Inbound security rules**

The screenshot shows the Azure Network Foundation interface. On the left, the 'Virtual networks' section is selected, showing a list of subnets: 'Vnet-SecureApp' and 'NSG-App'. The 'NSG-App' subnet is currently selected. On the right, the 'Edit subnet' blade is open, showing settings like NAT gateway (None), Network security group (NSG-App), and Route table (None). Below this, the 'Service Endpoints' section is visible. Further down, the 'Subnet Delegation' and 'Network Policy for Private Endpoints' sections are shown. At the bottom, there are 'Save' and 'Cancel' buttons.

**NSG-DB (Attach to subnet-DB)**

## (NSG-MGMT INBOUND RULES)

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

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

### Step 5: Create VM

#### 5.1 VM-Web

Home > VM-Web Virtual machine

Help me copy this VM in any region | Manage this VM with Azure CLI

VM-Web virtual machine agent status is not ready. Troubleshoot the issue →

Help me copy this VM in any region

Connect ▾ Start ▾ Restart ▾ Stop ▾ Hibernate ▾ Capture ▾ Delete ▾ Network ▾ Open in mobile ▾ Feedback ▾ (1/1)

Essentials

Resource group (move) : RG-SecureWebApp

Status : Running

Location : South Africa North

Subscription (move) : ZEMBE

Subscription ID : 4cd54fffc-69e8-48d9-bad1-50d0f77ec0cc

Operating system : Windows

Size : Standard B1s (1 vCore, 1.5 GB memory)

Primary NIC public IP : 42.211.102.22

Virtual network/subnet : rg-sqlserver-subnet-01

VMSS name : rg-sqlserver-vmss-01

Health state : Degraded

Time created : 11/08/2020, 11:00 PM UTC

Properties Monitoring Capabilities Recommendations Tokens

Virtual machine

Computer name : VM-Web

Operating system : Windows

VM generation : V2

VM watermark : 0.00

Agent status : Not Ready

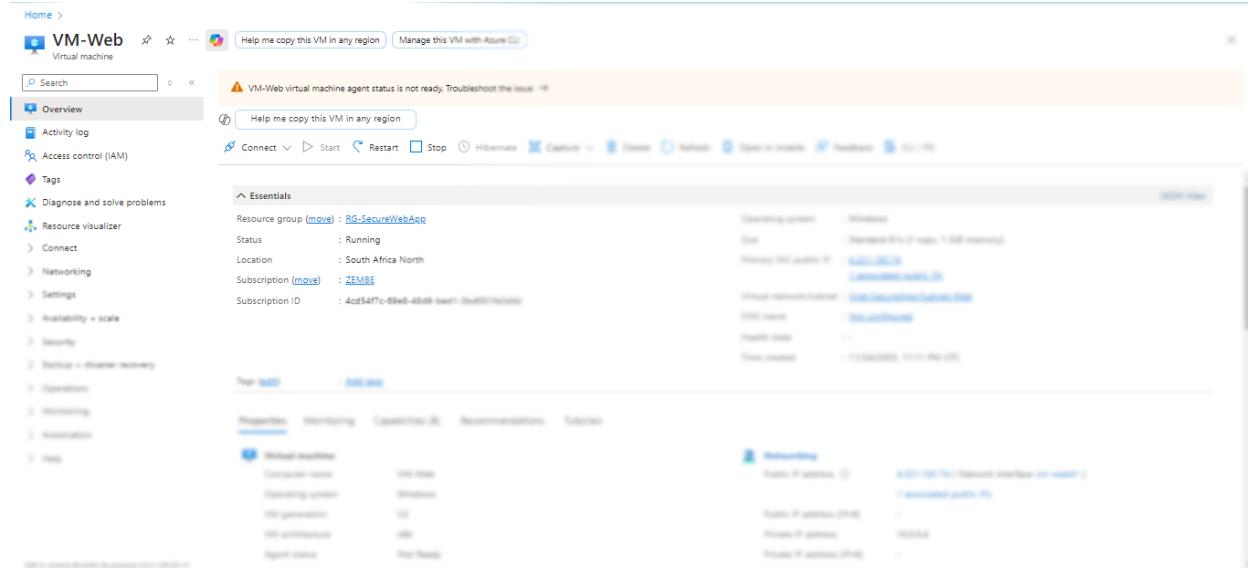
Networking

Public IP address : 42.211.102.22 (Network interface on vmss01)

Associated public IP : -

Private IP address : 10.0.1.4

Private IP address (VNet) : -



## 5.2 VM-App

Home > VM-App Virtual machine

Help me copy this VM in any region | Manage this VM with Azure CLI

VM-App virtual machine agent status is not ready. Troubleshoot the issue →

Help me copy this VM in any region

Connect ▾ Start ▾ Restart ▾ Stop ▾ Hibernate ▾ Capture ▾ Delete ▾ Network ▾ Open in mobile ▾ Feedback ▾ (1/1)

Essentials

Resource group (move) : RG-SecureWebApp

Status : Running

Location : South Africa North

Subscription (move) : ZEMBE

Subscription ID : 4cd54fffc-69e8-48d9-bad1-50d0f77ec0cc

Operating system : Windows

Size : Standard B1s (1 vCore, 1.5 GB memory)

Primary NIC public IP : 42.211.102.22

Virtual network/subnet : rg-sqlserver-subnet-01

VMSS name : rg-sqlserver-vmss-01

Health state : Degraded

Time created : 11/08/2020, 11:00 PM UTC

Properties Monitoring Capabilities Recommendations Tokens

Virtual machine

Computer name : VM-App

Operating system : Windows

VM generation : V2

VM watermark : 0.00

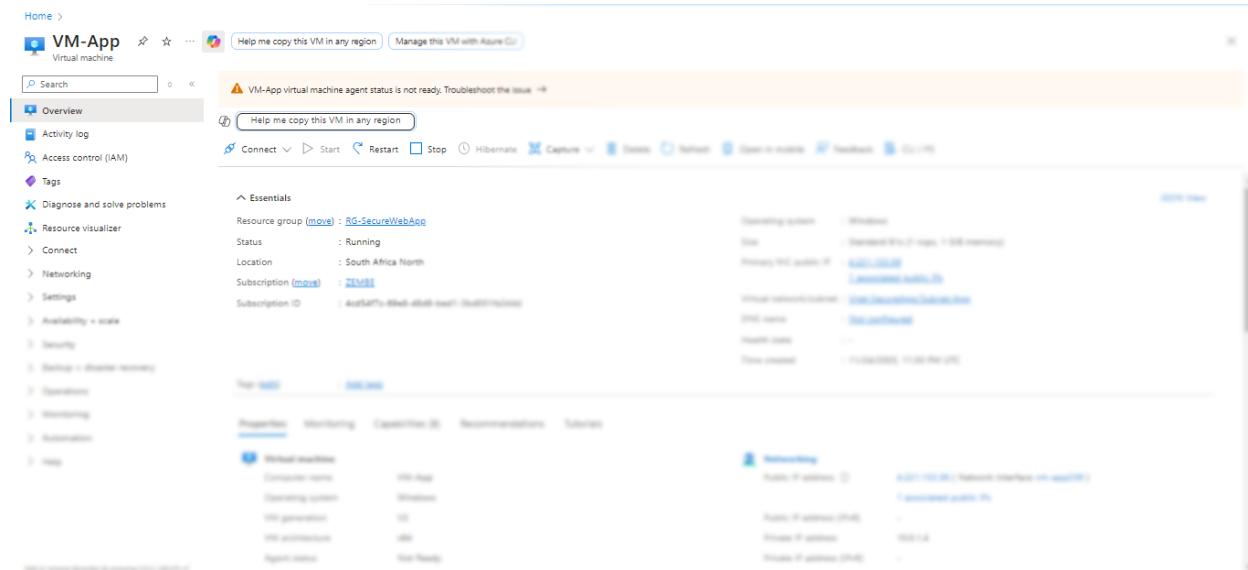
Agent status : Not Ready

Networking

Public IP address (VNet) : -

Private IP address : 10.0.1.4

Private IP address (VNet) : -



## 5.3 VM- DB

**VM-DB** Virtual machine

Help me copy this VM in any region | Manage this VM with Azure CLI

Overview

Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Connect, Networking, Settings, Availability + scale, Security, Backup + disaster recovery, Operations, Monitoring, Automation, Help.

**Essentials**

- Resource group (move) : RG-SecureWebApp
- Status : Running
- Location : South Africa North
- Subscription (move) : ZEMB
- Subscription ID : 4c0f547c-89e8-48d8-be01-0e00017e0000

Operating system : Windows  
Size : Standard Dv2 2 vcores, 1.5GB memory  
Primary NIC public IP : 44.222.192.202 (Last updated: 2023-08-25)  
Virtual network interface : eth0 (Description: Default)  
VM name : VM-DB  
Health state : Not Configured  
Time created : 2023-08-25, 11:08 PM UTC

Properties, Monitoring, Capabilities, Recommendations, Details.

**Networking**

Public IP address	44.222.192.202 (Resource interface on segment 0)
Private IP address (VLAN)	-
Private IP address	10.0.2.4
Private IP address (VLAN)	-

## 5.4 VM-Mgmt

**VM-mgmt** Virtual machine

Help me copy this VM in any region | Manage this VM with Azure CLI

Overview

Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Connect, Networking, Settings, Availability + scale, Security, Backup + disaster recovery, Operations, Monitoring, Automation, Help.

**Essentials**

- Resource group (move) : RG-SecureWebApp
- Status : Running
- Location : South Africa North
- Subscription (move) : ZEMB
- Subscription ID : 4c0f547c-89e8-48d8-be01-0e00017e0000

Operating system : Windows  
Size : Standard Dv2 2 vcores, 1.5GB memory  
Primary NIC public IP : 44.222.192.202 (Last updated: 2023-08-25)  
Virtual network interface : eth0 (Description: Default)  
VM name : VM-mgmt  
Health state : Not Configured  
Time created : 2023-08-25, 11:08 PM UTC

Properties, Monitoring, Capabilities, Recommendations, Details.

**Networking**

Public IP address	44.222.192.202 (Resource interface on segment 0)
Private IP address (VLAN)	-
Private IP address	10.0.2.4
Private IP address (VLAN)	-

## Step 6: Testing Connectivity ( Documented Steps)

**Internet – Web = Allowed**

**Internet – App = Blocked**

**Internet – DB = Blocked**

**Web – App = Allowed**

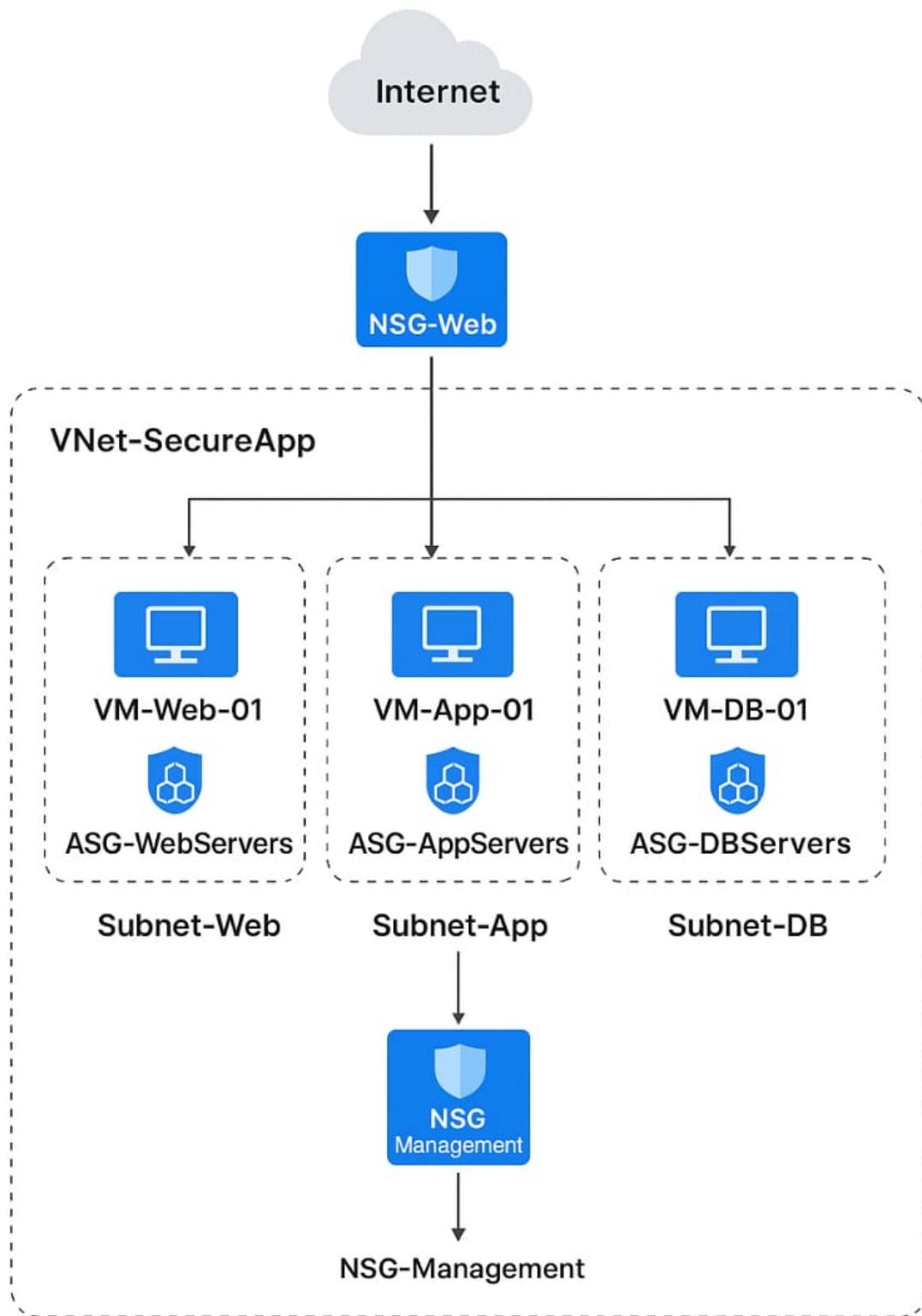
**App – DB = Allowed**

**Management – DB = Allowed**

**Management – Internet = Blocked**

# DIAGRAM

# 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