

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

 Give feedback

Step 3: Create Virtual Machine without Public IP

Home > CreateVm-MicrosoftWindowsServer.WindowsServer-202-20251111193208 | Overview >

app-vm Virtual machine

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

Your VM has a default outbound IP, which is insecure and will no longer be assigned by default for new subnets after March 2026. To secure your VM and subnets and ensure future compatibility, follow guidance to add an explicit method of outbound and set your subnets to private. →

Help me copy this VM in any region

Connect Start Restart Stop Hibernate Capture Delete Refresh Open in mobile Feedback CLI / PS

Properties Monitoring Capabilities (8) Recommendations Tutorials

Virtual machine

| | |
|----------------------------|-----------|
| Computer name | app-vm |
| Operating system | Windows |
| VM generation | V2 |
| VM architecture | x64 |
| Agent status | Not Ready |
| Agent version | Unknown |
| Hibernation | Disabled |
| Host group | - |
| Host | - |
| Proximity placement group | - |
| Colocation status | N/A |
| Capacity reservation group | - |
| Disk controller type | SCSI |

Networking

| | |
|---------------------------|-----------------------|
| Public IP address | - |
| Public IP address (IPv6) | - |
| Private IP address | 10.0.1.4 |
| Private IP address (IPv6) | - |
| Virtual network/subnet | SecureVnet/app-subnet |
| DNS name | - |

Size

| | |
|-------|--------------|
| Size | Standard B1s |
| vCPUs | 1 |
| RAM | 1 GiB |

Source image details

| | |
|------------------------|------------------------|
| Source image publisher | MicrosoftWindowsServer |
|------------------------|------------------------|

Step 4: Enable Azure Defender For Cloud

It provides security recommendations and threat detection

Home > Microsoft Defender for Cloud | Environment settings >

Settings | Defender plans

Search Save Settings & monitoring

Settings

Defender plans

Security policies

Email notifications

Workflow automation

Continuous export

| Resource type | Plan | Instances | Status | Settings |
|------------------|---|--|-----------------|-------------------------------|
| Servers | Plan 2 (\$15/Server/Month) Change plan > | 1 servers | Full | Settings > |
| App Service | \$15/Instance/Month Details > | 0 instances | Full | Settings > |
| Databases | Selected: 4/4 Select types > | 0 instances | Full | Settings > |
| Storage | \$10/Storage account/month \$0.15/GB scanned for On-Upload Malware Scanr Details > | 0 storage accounts | Full | Settings > |
| Containers | \$6.8693/VM core/Month Details > | 0 container registries; 0 kubernetes coi | Full | Settings > |
| AI Services | \$0.0008/1K tokens/month Details > | 0 AI resources | Partial | Settings > |
| Key Vault | \$0.25/Vault/Month Details > | 0 key vaults | Full | Settings > |
| Resource Manager | \$5/Subscription/Month Details > | | Full | Settings > |
| APIs | Plan 1 (\$200/month - 1 million API calls) Change plan > | 0 Azure API Management services | Action required | Settings > |

* The price displayed represents the list price prior to any discounts or special offers being applied.
When you select Save, Microsoft Defender for Cloud's enhanced security features will be enabled on all the resource types you've selected. The first 30 days are free.

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

Home > Key vaults >

Create a key vault ...

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

Home > SecureKV1 | Secrets >

Create a secret ...

| | |
|-------------------------|---|
| Upload options | Manual |
| Name * | vmAdminPassword |
| Secret value * | ***** |
| Content type (optional) | |
| Set activation date | <input type="checkbox"/> |
| Set expiration date | <input type="checkbox"/> |
| Enabled | <input checked="" type="radio"/> Yes <input type="radio"/> 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

