

LAB BT THATO KGOLE

DATE : 17 - 18 NOVEMBER 2025

CLOUD PLATFORM : MICROSOFT AZURE

Secure Virtual Machine Access Using JIT-Style Authentication Without Bastion

OVERVIEW

This project demonstrates how to secure an Azure Virtual Machine (Windows Server) without exposing RDP to the internet, using a JIT-style (just in time) access workflow built entirely with free tier services

Instead of Azure Bastion or Defender for Cloud JIT (both paid), the project implements:

- . A locked-down Network Security Group
- . Time-bound access controlled manually
- . NSG change detection
- . Real-time email alerts using Azure Monitor

PROBLEM STATEMENT

Virtual Machines exposed to the internet through RDP (port 3389) are vulnerable to:

- . Brute-force attacks
- . Port scanning
- . Credential stuffing
- . Persistent attack probing

Organizations often use Bastion or paid JIT features - but these require higher subscription tiers.

GOAL

Secure a VM without Bastion, Defender for Cloud, or any paid features while maintaining operational access.

IMPLEMENTATION STEPS

Step 1: Create Resource Group

Logical container for all resources

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

Create a resource group ...

[Basics](#) [Tags](#) [Review + create](#)

[Automation Link](#)

Basics

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

Tags

None

[Previous](#)

[Next](#)

[Create](#)

**Step 2: Create Virtual Network + Subnet
Private network environment for the VM.**

Create virtual network

Validation passed

Basics Security IP addresses Tags **Review + create**

Subscription	ZEMBE
Resource Group	JIT-RG
Name	Jit-Vnet
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	management-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: Deploy Windows VM (No Public Access)

A VM that cannot be accessed by default.

Setting	Value
Subscription	ZEMBE
Resource group	JIT-RG
Virtual machine name	jit-vm
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 2019 Datacenter - Gen2
VM architecture	x64
Size	Standard B1s (1 vcpu, 1 GiB memory)
Enable Hibernation	No
Username	zembe
Already have a Windows license?	No
Azure Spot	No

Disks

OS disk size	Image default
OS disk type	Standard SSD LRS
Use managed disks	Yes
Delete OS disk with VM	Enabled
Ephemeral OS disk	No

Networking

Virtual network	Jit-Vnet
Subnet	app-subnet
Public IP	None
NIC network security group	None
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No
Delete NIC when VM is deleted	Enabled

< Previous

Next >

Create

Step 4: Lock Down the Network Security Group

[Home](#) > [Network foundation | Network security groups](#) >

[Create network security group](#) ...

Validation passed

Basics Tags Review + create

Basics

Subscription	ZEMBE
Resource group	JIT-RG
Region	South Africa North
name	jit-nsg

Tags

None

Create

< Previous

Next >

[Download a template for automation](#)

Home > jit-nsg

jit-nsg | Inbound security rules

Network security group

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

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](#)

Priority ↑	Name ↑	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
<input type="checkbox"/> 65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
<input type="checkbox"/> 65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
<input type="checkbox"/> 65500	DenyAllInBound	Any	Any	Any	Any	Deny

<https://portal.azure.com/#@zembecloudcomputing@gmail.onmicrosoft.com/resource/subscriptions/4cd54f7c-69e8-48d9-bed1-3bd001fa344d/resourceGroups/JIT-RG/providers/Microsoft.Network/networkSecurityGroups/jit-nsg/inboundSecurityRules>

Home > jit-nsg

↑ jit-nsg | Outbound security rules

Network security group

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

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](#)

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
<input type="checkbox"/> 65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
<input type="checkbox"/> 65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
<input type="checkbox"/> 65500	DenyAllOutBound	Any	Any	Any	Any	Deny

<https://portal.azure.com/#@zembecloudcomputing@gmail.onmicrosoft.com/resource/subscriptions/4cd54f7c-69e8-48d9-bed1-3bd001fa344d/resourceGroups/JIT-RG/providers/Microsoft.Network/networkSecurityGroups/jit-nsg/outboundSecurityRules>

Add inbound security rule

Source: IP Addresses
Source IP addresses/CIDR ranges: 102.219.24.52

Source port ranges: *

Destination: Any

Service: RDP

Destination port ranges: 3389

Protocol: TCP

Priority	Name	Port	Protocol
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBalancerInBound	Any	Any
65500	DenyAllInBound	Any	Any

Step 5: Configure Azure Monitor Alert

To detect any time someone opens port 3389 - even for a moment

Home > Network foundation | Network security groups > jit-nsg | Activity log >

Create an alert rule ...

Review + create

Scope

Scope level: Subscription
Resource: ZEMBE > JIT-RG > jit-nsg/jit-temp-access

Condition

Condition preview: Whenever the Activity Log has an event with Category='Administrative', Signal name='Create or Update Network Security Group (Network Security Group)'

Actions

Action group name: NSG-Alert-Group
Contain actions: 1 Email

Details

Project details: Subsciption: ZEMBE

Create **Previous**

Home > Network foundation | Network security groups > jit-nsg | Activity log >

Create an alert rule

Condition

Condition preview Whenever the Activity Log has an event with Category='Administrative', Signal name='Create or Update Network Security Group (Network Security Group)'

Actions

Action group name Contain actions

NSG-Alert-Group 1 Email ⓘ

Details

Project details

Subscription ZEMBE

Resource group JIT-RG

Region global

Alert rule details

Alert rule name NSG RDP Access Change Alert

Alert rule description Triggers when any Network Security Group rule is created or updated, including opening RDP (3389). Helps detect unauthorized access.

Enable upon creation

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

The screenshot shows the Azure portal interface. On the left, the 'Network foundation | Network security groups' blade is open, displaying a list of network security groups including 'jit-nsg'. A message box indicates a new version of the browser experience is available. On the right, the 'jit-nsg | Activity log' blade is open, showing a table of activity logs with columns for Operation name, Status, Time, Time stamp, Subscription, and Event initiator. The logs show two successful operations: 'Create or Upd' succeeded at 9 minutes ago and 44 minutes ago, both by the user 'ZEMBE' from 'zembedcloudi'.

Operation name	Status	Time	Time stamp	Subscription	Event initiator
> Create or Upd	Succeeded	9 minutes ago	Sun Nov 16...	ZEMBE	zembedcloudi
> Create or Upd	Succeeded	44 minutes ago	Sun Nov 16...	ZEMBE	zembedcloudi

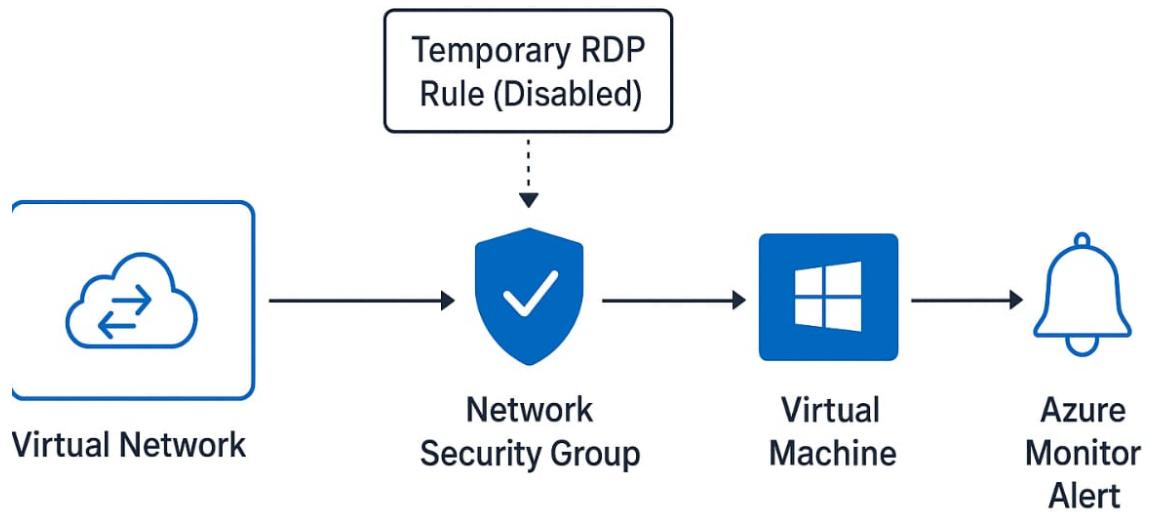
Step 6: Test Scenario (Documented)

- > **Modify the RDP rule to allow your public IP**
- > **Save the rule**
- > **Azure Monitor detects the change**
- > **Action Group sends an email alert**

Learning Outcome

- . NSG firewall design
- . Zero-Trust network access
- . How to manually implement a free JIT-style model
- . Monitoring NSG changes
- . Creating alert rules & action groups
- . Least privilege security governance
- . Real - world security operations workflow

Diagram



Secure VM with JIT-Style Access (No Bastion)