

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

Create a resource group ...

- Basics
- Tags
- Review + create

 Automation Link

Basics

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

Tags

None

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](#)

Home > Jit-Vnet

Jit-Vnet | Subnets ☆ ...

Virtual network

Search

+ Subnet

Refresh

Manage users

Delete

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

Showing 2 subnets

<input type="checkbox"/>	Name ↑	IPv4
<input type="checkbox"/>	app-subnet	10.0.1.0/24
<input checked="" type="checkbox"/>	management-subnet	10.0.0.0/24

Edit subnet

Include an IPv6 address space

☐ This virtual network has no IPv6 address ranges.

Private subnet

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. [Learn more](#)

Enable private subnet (no default outbound access)

☐

After March 31, 2026, private subnet will be the default selection for new virtual networks. [Learn more](#)

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

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

Network security group

jlt-nsg

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](#)

Save

Cancel

Give feedback

Step 3: Deploy Windows VM (No Public Access)

A VM that cannot be accessed by default.

Home > Compute infrastructure | Virtual machines >

Create a virtual machine ...

Help me create a low cost VM

Help me create a VM optimized for high availability

Help me choose the right VM size for my workload

Validation passed

Help me create a low cost VM

Help me create a VM optimized for high availability

Help me choose the right VM size for my workload

Subscription	ZEMBE
Resource group	JIT-RG
Virtual machine name	jlt-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

< Previous

Next >

Create

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](#)

Filter by name		Port == all	Protocol == all	Source == all	Destination == all	Action == all
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/#@zembeccloudcomputingmail.onmicrosoft.com/resource/subscriptions/4cd547c-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](#)

Filter by name

Port == all

Protocol == all

Source == all

Destination == all

Action == all

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/#@zembeccloudcomputingmail.onmicrosoft.com/resource/subscriptions/4cd547c-69e8-48d9-bed1-3bd001fa344d/resourceGroups/JIT-RG/providers/Microsoft.Network/networkSecurityGroups/jit-nsg/outboundSecurityRules

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

Filter by name

Port == all Protocol == all Source == all

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

Add inbound security rule

jit-nsg

Source

IP Addresses

Source IP addresses/CIDR ranges

102.219.24.52

Source port ranges

*

Destination

Any

Service

RDP

Destination port ranges

3389

Protocol

Any

TCP

UDP

ICMPv4

ICMPv6

Add Cancel

Give feedback

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

Scope Condition Actions Details Tags Review + create

Scope

Scope levelSubscription

ResourceZEMBE > JIT-RG > jit-nsg/jit-temp-acces

Condition

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

Actions

Action group nameContain actions

NSG-Alert-Group1 Email

Details

Project details

SubscriptionZEMBE

CreatePrevious

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

Network foundation | Network security groups

Preview

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

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

Name ↑

jit-nsg

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

jit-nsg | Activity log

Network security group

Search

Activity

Edit columns

Refresh

Export Activity Logs

Download as CSV

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

Looking for Log Analytics? In Log Analytics you can search for performance, diagnostics, health logs, and more. Visit Log Analytics

Search

Quick Insights

Management Group : None

Subscription : ZEMBE

Event severity : All

Timespan : Last 6 hours

Resource group : JIT-RG

Resource : jit-nsg

Event category : Administrative

Add Filter

2 items.

Operation name	Status	Time	Time stamp	Subscription	Event initiat
> Create or Upd	Succeeded	9 minutes a...	Sun Nov 16 ...	ZEMBE	zembecloudi
> Create or Upd	Succeeded	44 minutes ...	Sun Nov 16 ...	ZEMBE	zembecloudi

Add or remove favorites by pressing Ctrl+L+Shift+F

Add or remove favorites by pressing Ctrl+L+Shift+F

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

Create an alert rule

Scope Condition Actions Details Tags Review + create

Configure when the alert rule should trigger by selecting a signal and defining its logic.

Signal name * Create or Update Security Rule (networkSecurityGroups/secu... [See all signals](#)

Chart period
Over the last 6 hours

1
0.8
0.6
0.4
0.2
0

6:30 PM 7 PM 7:30 PM 8 PM 8:30 PM 9 PM 9:30 PM

actualFullAndHistoricalSeries

[Review + create](#) [Previous](#) [Next: Actions >](#)

Select a signal

[Signal type : All](#) [Signal source : All](#)

Signal name	Signal source
Activity log	
All Administrative operations	Administrative
Create or Update Network Security Group (Network Security Group)	Administrative
Delete Network Security Group (Network Security Group)	Administrative
Join Network Security Group. (Network Security Group)	Administrative

[Apply](#) [Cancel](#)

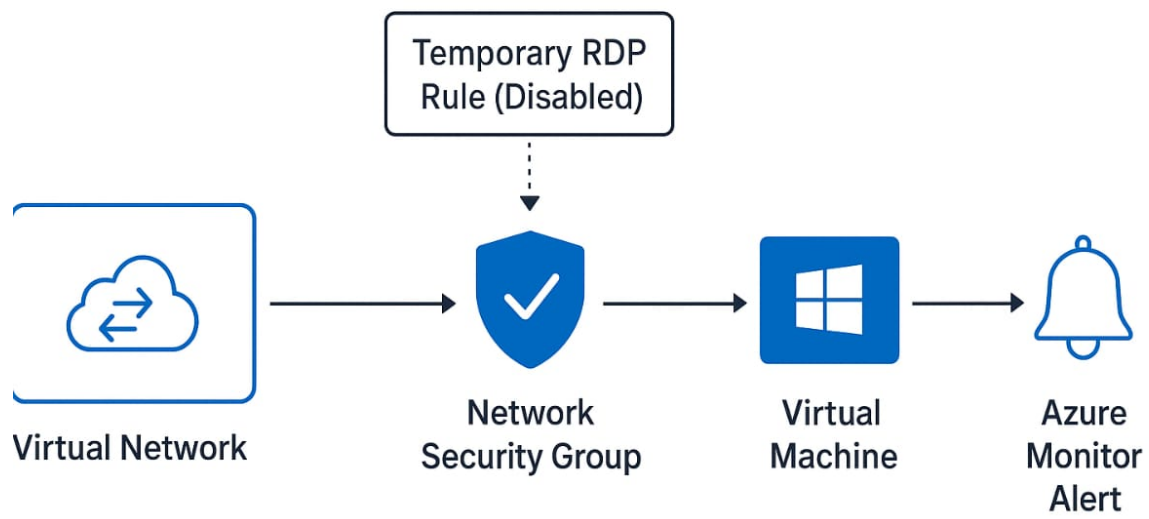
Step 6: Test Scenario (Documented)

- > 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)