Phase 3 – Network Security Group (NSG) Design & Hardening

Intro (What & Why)

In this phase, we **intentionally design network security** for the VM.

Although an NSG was auto created during VM deployment, that NSG was:

- Generic
- Auto-generated
- Not designed with security intent

*Here, we **create a new NSG from scratch** to:*

- Demonstrate conscious security decisions
- Control inbound and outbound traffic explicitly
- Prepare the VM for realistic SOC scenarios

This phase focuses only on **traffic control**, not logging or Sentinel.

Steps

1. Create a New NSG

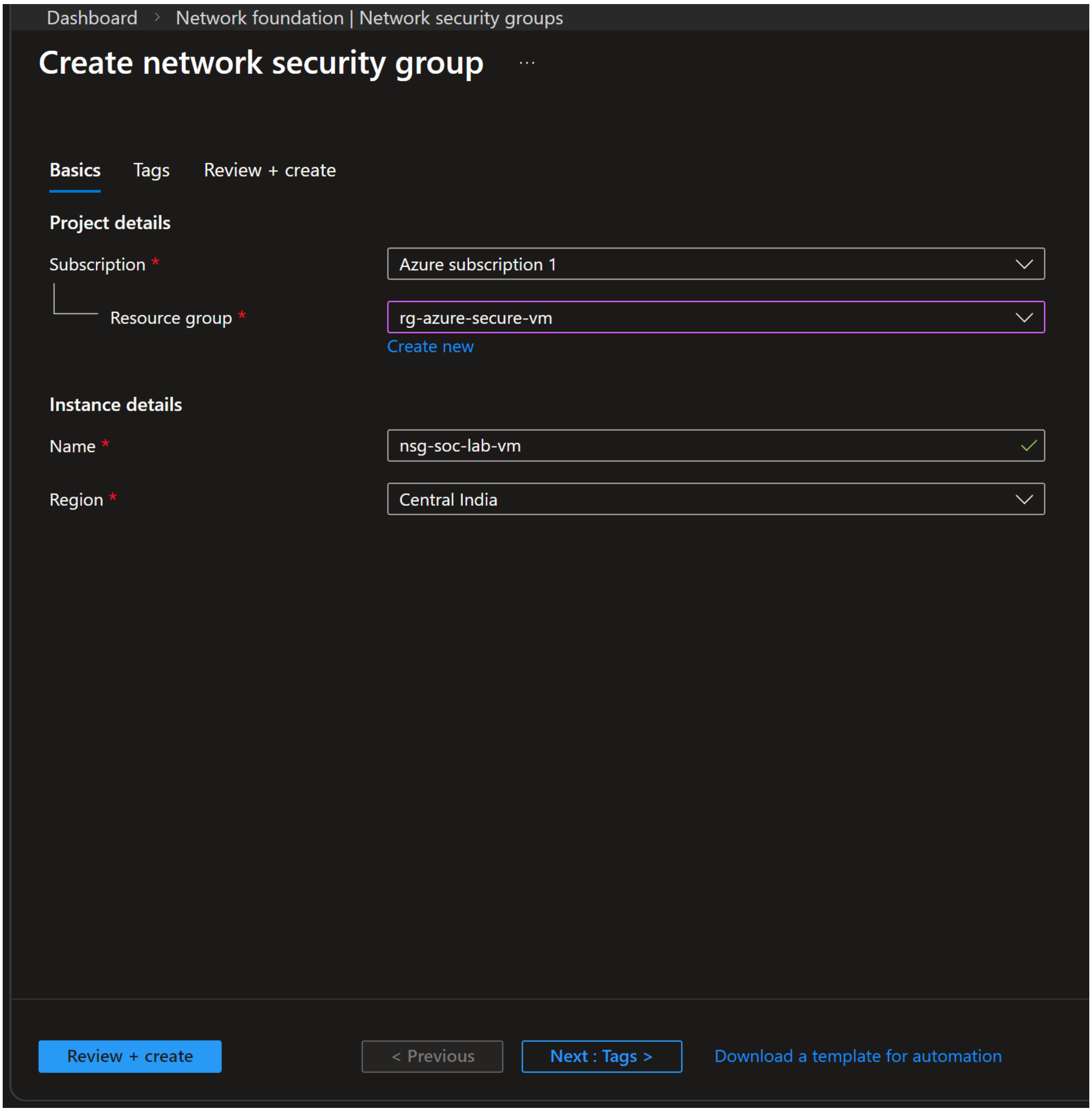
We need to **create a new Network Security Group explicitly**.

We should:

- Give it a meaningful name (example: azure-secure-web-vm-nsg)
- Place it in the same resource group as the VM
- Use the same region to avoid cross-region issues

GUI Flow

Azure Portal → Global search bar → Type Network security group → Network security groups → Create → Select subscription → Resource group → Enter NSG name → Select region → Review + Create → Create



Dashboard > Network foundation | Network security groups

Create network security group ...

Basics
Tags
Review + create

Project details

Subscription * Azure subscription 1

Resource group * rg-azure-secure-vm

Instance details

Name * nsg-soc-lab-vm ✓

Region * Central India

Review + create
< Previous
Next : Tags >
Download a template for automation

2. Review Default NSG Rules

After creation, we should **review the default rules**.

We need to:

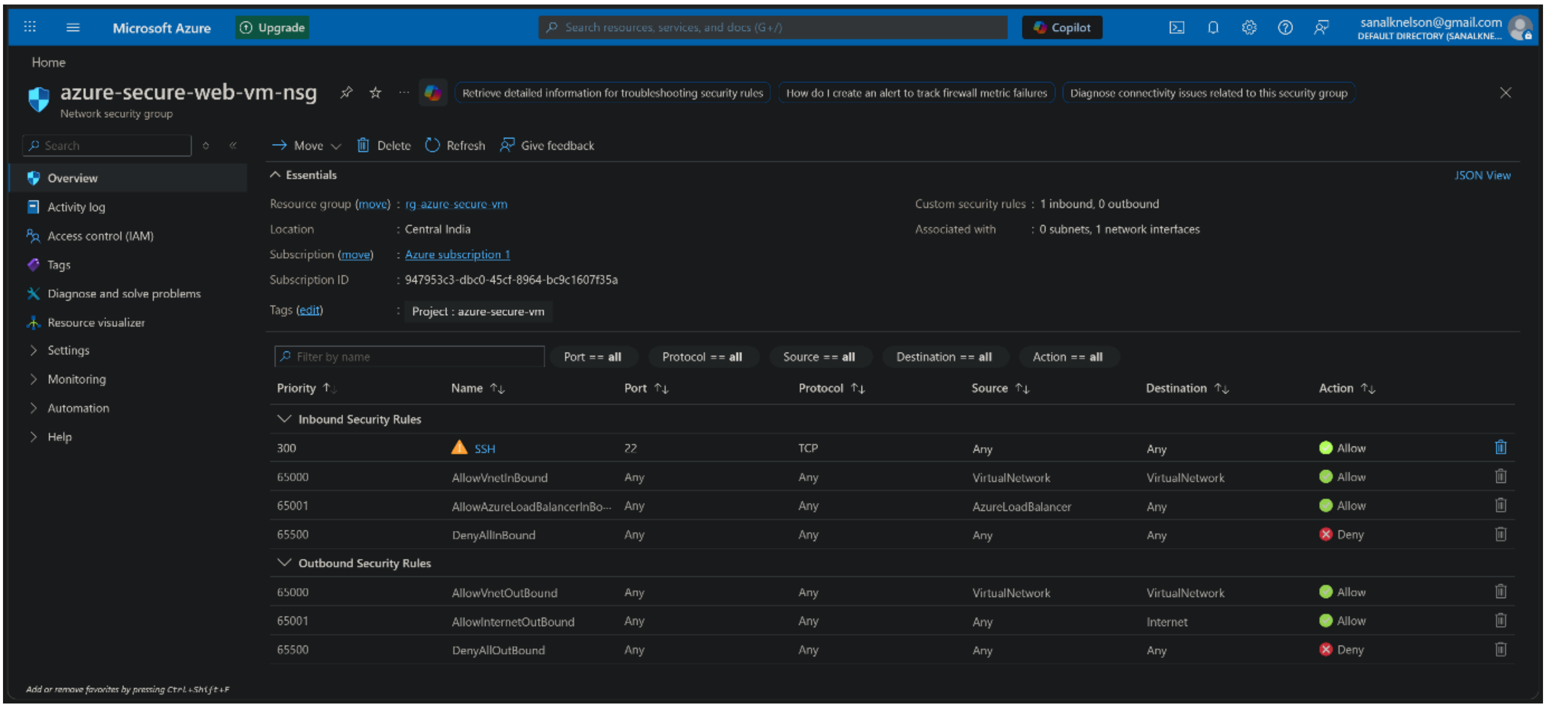
- Observe default inbound deny rules

- Observe default outbound allow rules
- Understand priority numbering

Default rules are important because many security issues come from misunderstanding rule precedence.

GUI Flow

Azure Portal → Network security groups → Select new NSG → Settings → Inbound security rules / Outbound security rules


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
sanalknelson@gmail.com
DEFAULT DIRECTORY (SANALKNE...
Home
Network security group
Retrieve detailed information for troubleshooting security rules
How do I create an alert to track firewall metric failures
Diagnose connectivity issues related to this security group
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Monitoring
Automation
Help
Move
Delete
Refresh
Give feedback
Essentials
JSON View
Filter by name
Port == all
Protocol == all
Source == all
Destination == all
Action == all
Add or remove favorites by pressing Ctrl+Shift+F

azure-secure-web-vm-nsg

Resource group (move) : rg-azure-secure-vm
Location : Central India
Subscription (move) : Azure subscription 1
Subscription ID : 947953c3-dbc0-45cf-8964-bc9c1607f35a
Tags (edit) : Project : azure-secure-vm
Custom security rules : 1 inbound, 0 outbound
Associated with : 0 subnets, 1 network interfaces

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
300	⚠ SSH	22	TCP	Any	Any	● Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	● Allow
65001	AllowAzureLoadBalancerInBo...	Any	Any	AzureLoadBalancer	Any	● Allow
65500	DenyAllInBound	Any	Any	Any	Any	☒ Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	● Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	● Allow
65500	DenyAllOutBound	Any	Any	Any	Any	☒ Deny

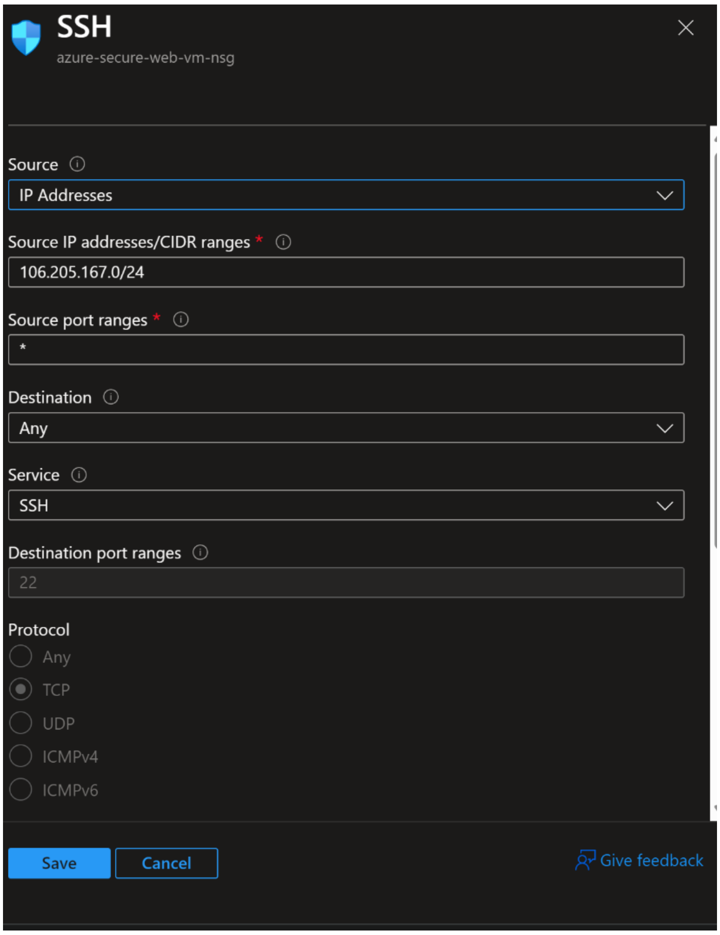
3. Define Inbound Rules Intentionally

We now add only the access we actually need.

For this lab:

- Allow SSH (22) for administrative access
- Keep the rule scope broad for learning purposes
- Maintain lowest required priority

This is intentionally permissive for a lab.
In real environments, SSH should be restricted to trusted IP ranges.



SSH

azure-secure-web-vm-nsg

Source: IP Addresses

Source IP addresses/CIDR ranges *: 106.205.167.0/24

Source port ranges *: *

Destination: Any

Service: SSH

Destination port ranges: 22

Protocol

○ Any
● TCP
○ UDP
○ ICMPv4
○ ICMPv6

4. Keep Outbound Rules Default (For Now)

At this stage, we **do not modify outbound rules**.

Reason:

- Outbound traffic is required for:
  - Updates
  - Agent communication
  - Future log ingestion

Outbound hardening will be discussed only after log flow is fully understood.

5. Associate the New NSG with the VM

We now **attach the new NSG** to the VM.

We need to:

- Associate the NSG at the **NIC level**

- Ensure the VM is governed by the new rules
- Confirm the old auto-created NSG is no longer effective

Attaching at NIC level provides tighter control and clearer scope for this lab. You will see the VM attached NIC as a resource after this.

GUI Flow

Azure Portal → Virtual machines → Select VM → Networking → Network interface → Network security group → Select existing NSG → Save

Outcome

By the end of this phase:

- A **custom, intentionally designed NSG** is in place
- Traffic control is explicit and understandable
- SSH access is preserved for lab work
- The VM is now **security-controlled**, not just reachable
- The environment is ready for **log pipeline setup** in the next phase