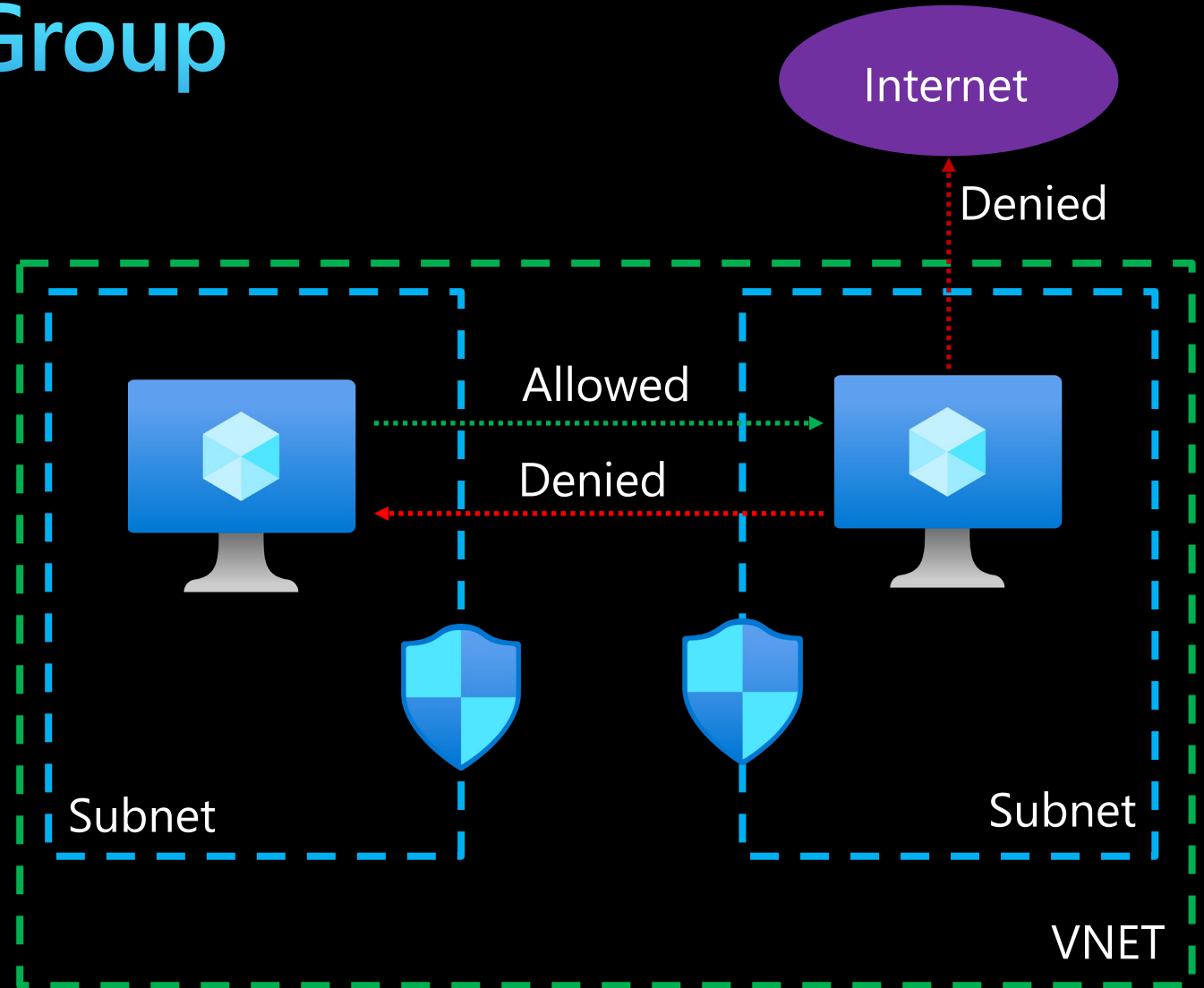


Network Security Group

NSG



What is the problem ?

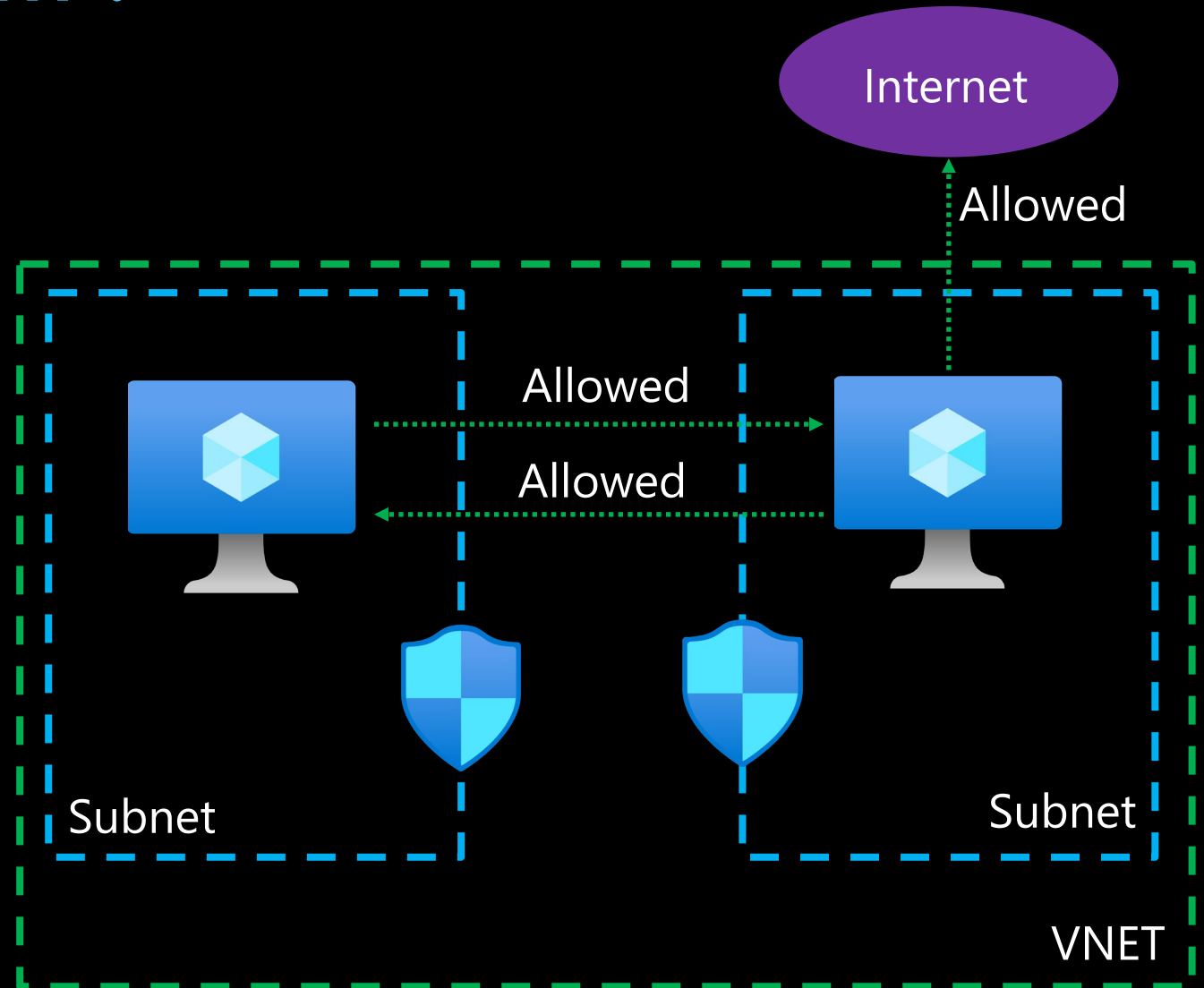
By default, **network traffic is allowed** inside a virtual network (VNET) and to and from the internet.

All services can communicate with each other within a VNET.

This is **not secure!**
Potential data exfiltration.

You should apply **Zero Trust Network**.

You should **limit as much as possible the unnecessary traffic**.



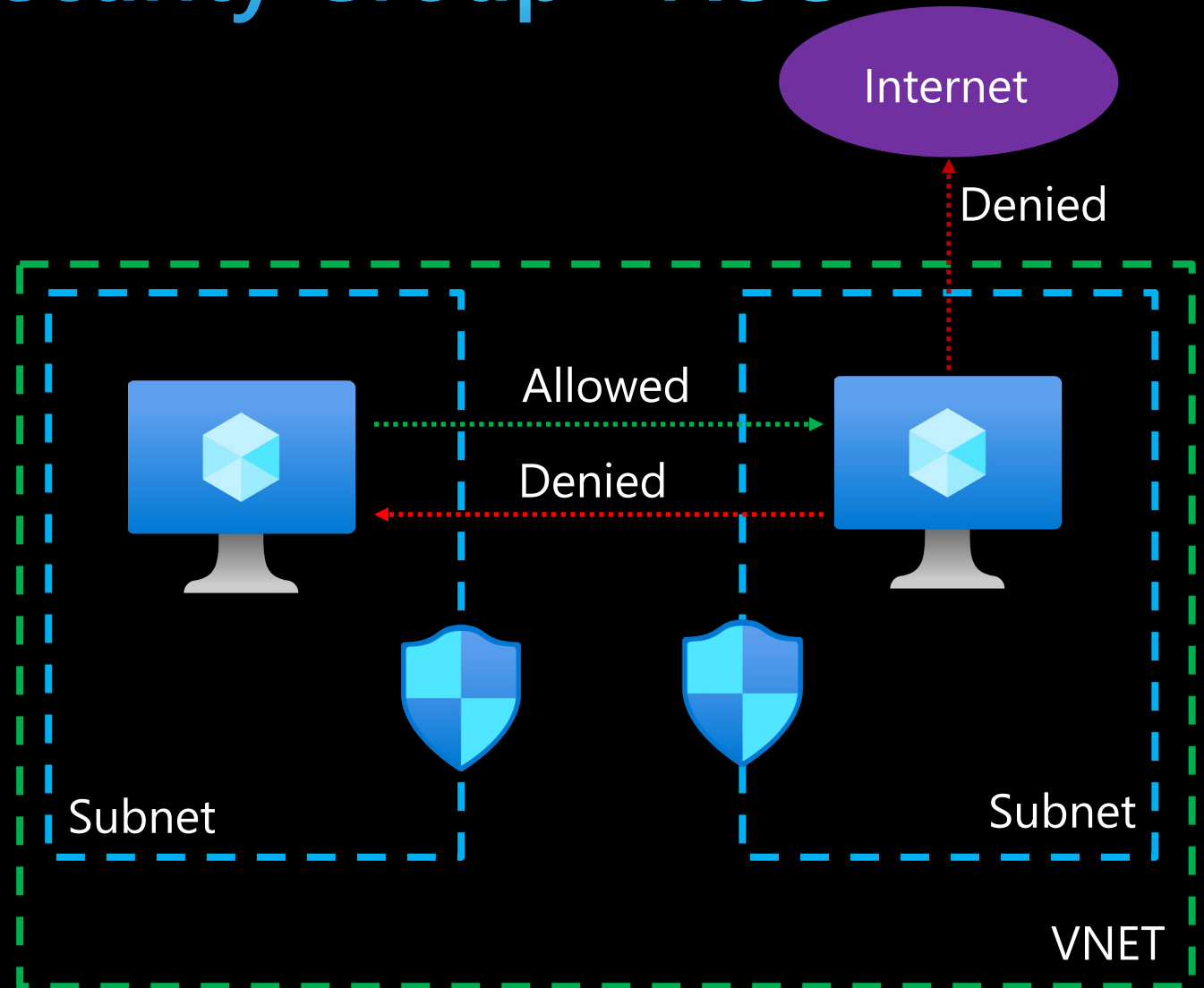
What is Network Security Group - NSG

You should limit as much as possible the unnecessary traffic.

NSG filters network traffic between Azure resources in an Azure VNET.

NSG uses security rules to allow or deny the inbound or outbound traffic for Azure resources.

For each rule it specifies the source and destination IP address(es), port number and protocol.



Creating Network Security Group

Create network security group

...



Basics

Tags

Review + create

Project details

Subscription *

Microsoft-Azure-T



Resource group *

rg-spoke



[Create new](#)

Instance details

Name *

nsg-spoke



Region *

West Europe



Review + create

< Previous


Next : Tags >




Download a


[template for automation](#)


Default rules in Network Security Group


You can't remove the default rules, but you can override them by creating rules with higher priorities.


 **nsg-spoke**
Network security group


  

 Overview


 Activity log


 Access control (IAM)


 Tags


 Diagnose and solve problems


Settings


 Inbound security rules



 Outbound security rules


 Network interfaces


 Subnets


 Properties


 Locks

 Move 

 Delete

 Refresh

 Give feedback

 Essentials






















Port == all

Protocol == all

Source == all

Destination == all

Action == all

Priority 	Name 	Port 	Protocol 	Source 	Destination 	Action 
<div> Inbound Security Rules</div>						
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	 Allow 
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	 Allow 
65500	DenyAllInBound	Any	Any	Any	Any	 Deny 
<div> Outbound Security Rules</div>						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	 Allow 
65001	AllowInternetOutBound	Any	Any	Any	Internet	 Allow 
65500	DenyAllOutBound	Any	Any	Any	Any	 Deny 

[View Cost](#)

[JSON View](#)

Creating Security rule

Each rule have a **priority** between **100 and 4096**.

The lower the priority number, the higher the priority of the rule

Home > Microsoft.NetworkSecurityGroup-20231101110916 | Overview >

↑

msg-spoke | Outbound security rules

☆

Network security group

Search

<<

+ Add

Hide default rules

Add

Network security group security rule port, and protocol to allow or deny delete default security rules, but you

Filter by name

Port == all Protocol ==

Priority ↑↓ Name ↑↓

☐ 65000 AllowVnetOutB

☐ 65001 AllowInternetO

☐ 65500 DenyAllOutBo

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Alerts

D diagnostic settings

Logs

NSG flow logs

Automation

CLI / PS

Tasks (preview)

Export template

Help

Add outbound security rule

✕

nsg-spoke

Source ⓘ

Any

Source port ranges * ⓘ

*

Destination ⓘ

Any

Service ⓘ

HTTP

Destination port ranges ⓘ

80

Protocol

☐ Any

☒ TCP

☐ UDP

☐ ICMP

Action

☒ Allow

☐ Deny

Priority * ⓘ

100

Name *

AllowAnyHTTPOutbound

Description

Add

Cancel

Give feedback

Attach NSG to Subnet or Network Interface (NIC)

NSG could be attached to multiple Subnets. Subnet could use one or multiple NSGs.

The screenshot displays the Azure portal interface for associating a subnet with a Network Security Group (NSG). The left sidebar shows the navigation menu with 'Subnets' selected under the 'nsg-spoke' network security group. The main content area is titled 'Associate subnet' and includes the following elements:

- Virtual network ***: A dropdown menu showing 'vnet-spoke (rg-spoke)'.
- Subnet ***: A dropdown menu showing 'subnet-frontend-servers'.
- OK**: A button at the bottom right to confirm the association.

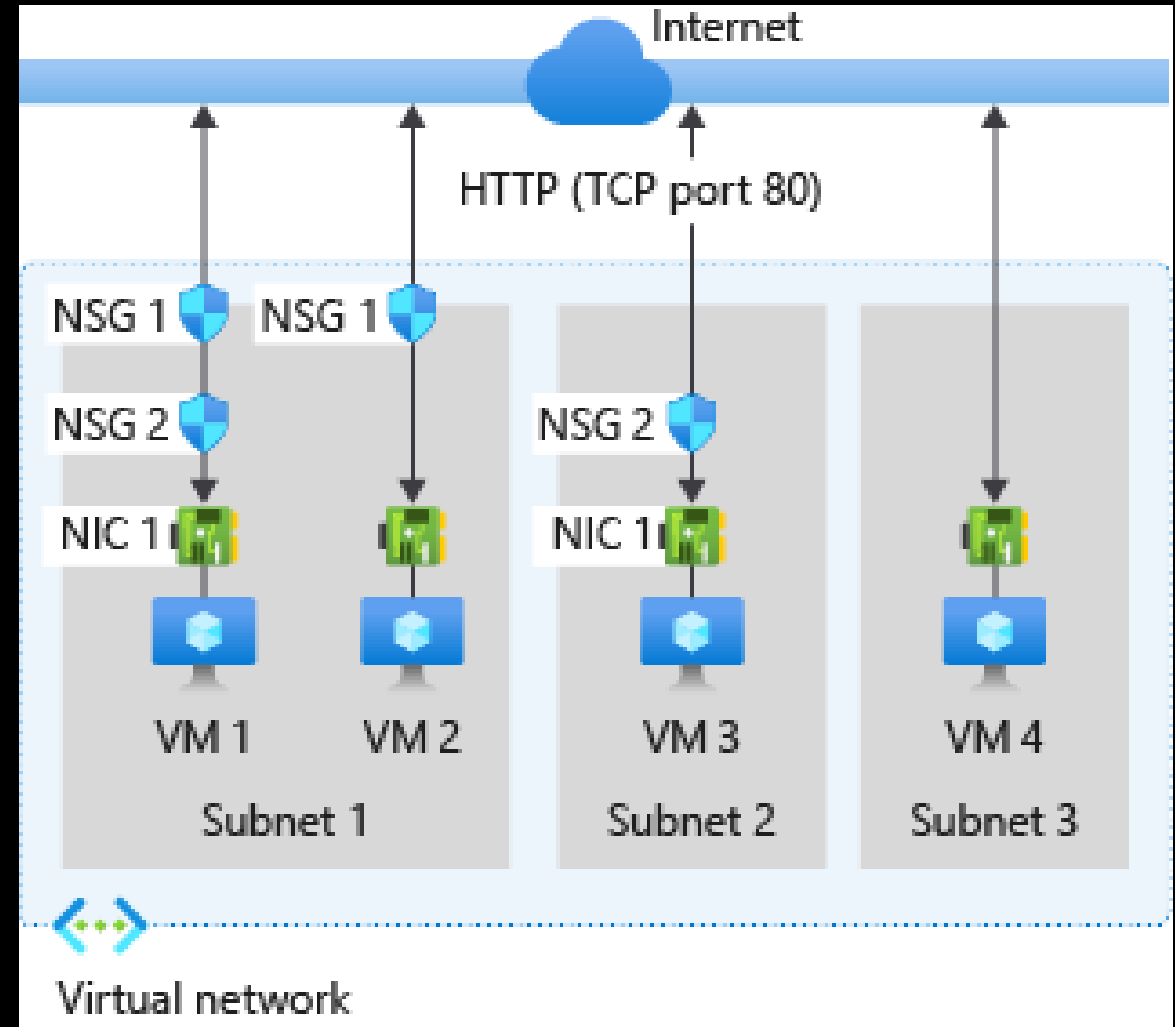
The background shows the 'Subnets' view for the 'nsg-spoke' NSG, with a search bar and a list of subnets. The 'subnet-frontend-servers' subnet is visible in the list.

Network Security Groups in order

For **inbound** traffic, rules in **Subnet NSG** are **processed before NIC's NSG**.

For **outbound** traffic, rules in **Subnet NSG** are **processed before NIC's NSG**.

NSG rules can affect connectivity between resources (like VMs) within a Subnet.



NSG operates at Layer 3 & 4

NSG operates at **Layers 3** (IP addresses and protocols) and **Layer 4** (ports) of the OSI model.

NSG cannot filter traffic at Layer 7.
It cannot use FQDNs.

Layer 7 traffic could be filtered by a Network Virtual Appliance (NVA) like **Azure Firewall**.

