

Microsoft Azure Administrator: Secure Access to Virtual Networks

PROTECTING AZURE VIRTUAL NETWORK TRAFFIC WITH
NSGS



Tim Warner

AUTHOR EVANGELIST, PLURALSIGHT

@TechTrainerTim TechTrainerTim.com





The picture can't be displayed.

Overview

Describe this course

Create NSGs and security rules

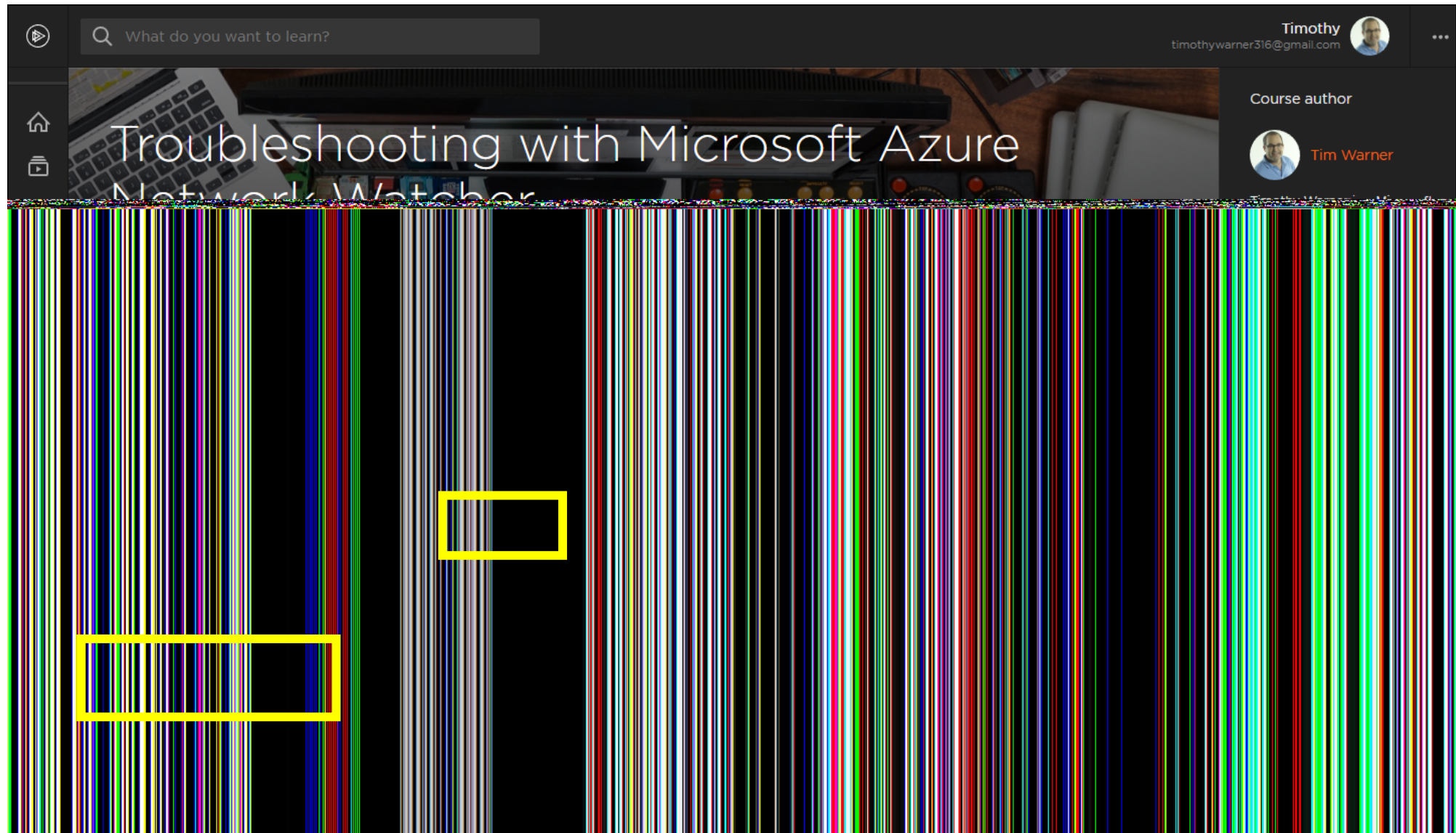
Associate an NSG to a subnet or network interface

Evaluate effective security rules



T
h
e
p

Exercise Files



Exercise Files

The screenshot displays a Windows desktop environment with three overlapping windows:

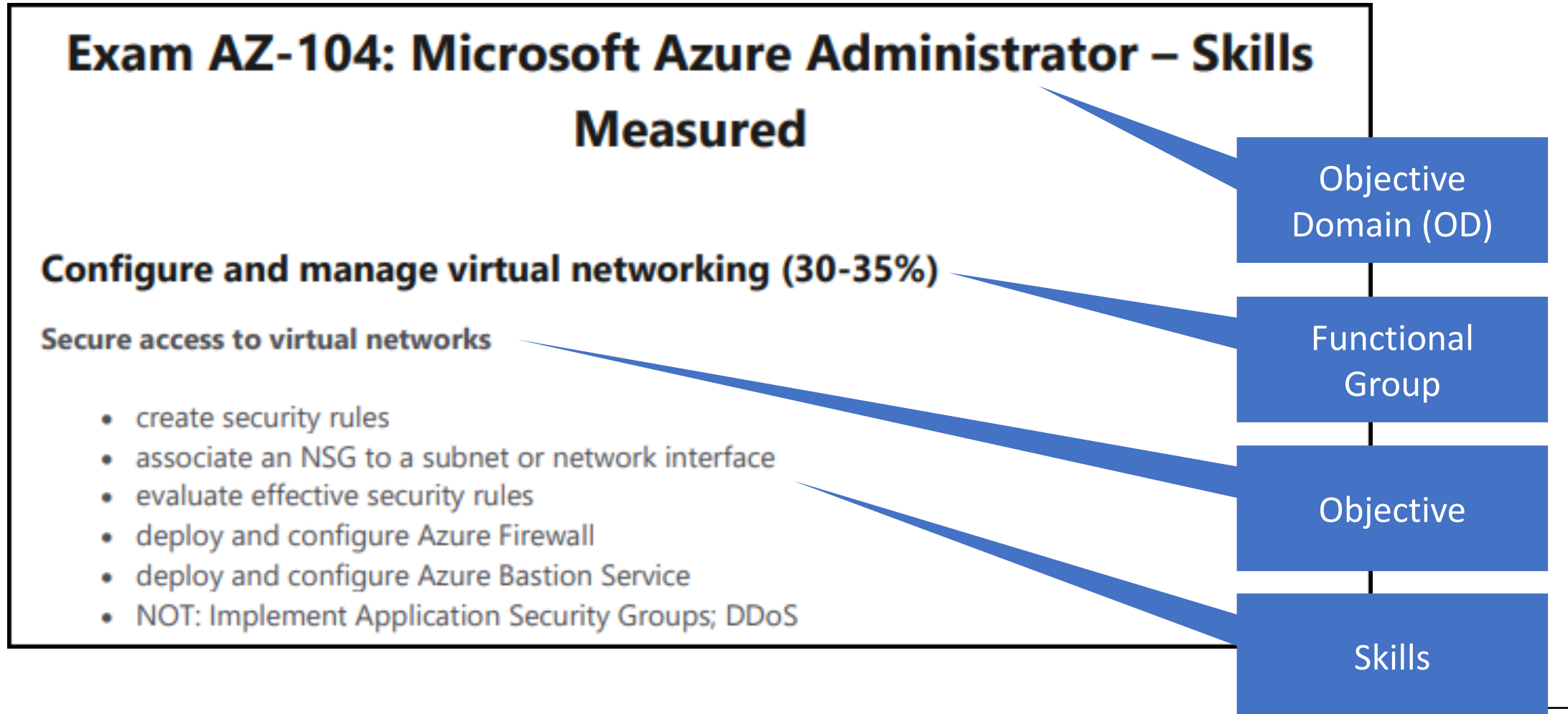
- File Explorer (Left):** Shows the 'Downloads' folder for user 'Tim'. It contains a list of folders named 02, 03, 04, 05, and 06. The status bar indicates '0 / 5 object(s) selected'.
- Text Editor (Center):** A Notepad window titled 'microsoft-azure-ad-privileged-identity-management-configuring-m4-links.txt'. It contains a list of 22 numbered items, each consisting of a title and a URL. The status bar shows 'Spaces: 4 UTF-8 CRLF Plain Text'.
- File Download Window (Right):** A small window showing a file named '02\demos\' with a size of 1,298 bytes and a package size of 359 bytes.

The text editor content is as follows:

```
1 Module 4: Organize and Perform Azure AD PIM Access Reviews
2
3 Microsoft Azure
4 https://azure.microsoft.com/en-us/
5
6 Azure Documentation
7 https://docs.microsoft.com/en-us/azure/
8
9 Azure AD Privileged Identity Management (PIM) documentation | Microsoft Docs
10 https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/
11
12 Identity Governance - Azure Active Directory | Microsoft Docs
13 https://docs.microsoft.com/en-us/azure/active-directory/governance/identity-governance-overview
14
15 Create an access review of Azure resource roles in PIM - Azure Active Directory | Microsoft Docs
16 https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-start-access-review
17
18 Review access to Azure AD roles in PIM - Azure Active Directory | Microsoft Docs
19 https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-perform-security-review
20
21 View audit history for Azure AD roles in PIM - Azure Active Directory | Microsoft Docs
22 https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-use-audit-log
```

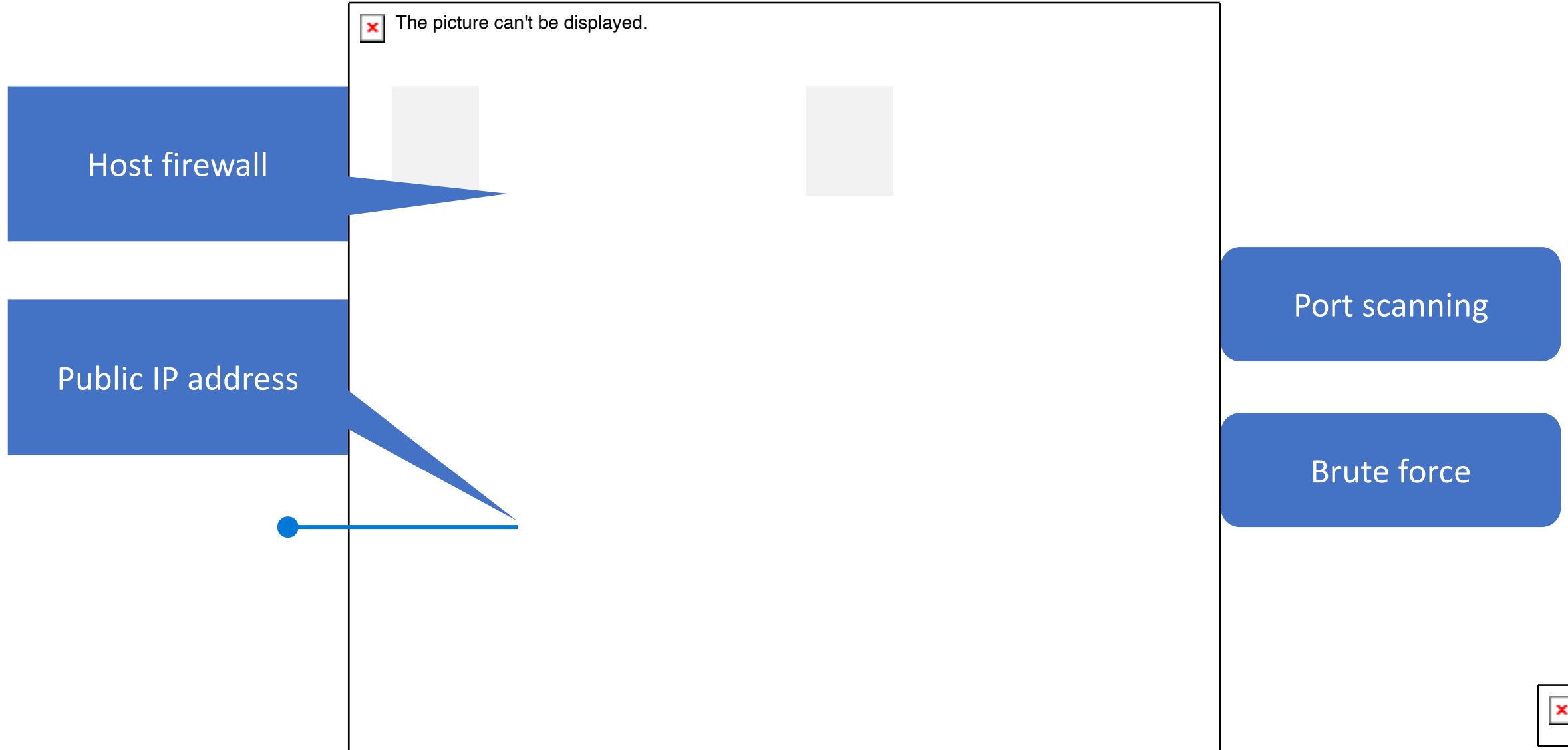
Understand this Course

Azure Administrator Certification (AZ-104)



Create NSGs and Security Rules

The Use Case



Network Security Groups (NSGs)



Stateful network traffic filter

- Inbound and outbound traffic

OSI Layer 4

- Source & destination IP address
- Source & destination port
- Protocol

Security rules evaluated in priority order

Service Tags

Microsoft-defined set
of IP address prefixes

Aligned to Azure
services and regions

Helpful for firewall rule
management

Microsoft publishes
their IP ranges monthly

You can retrieve these
prefixes with an API

Some are usable in
Azure Firewall



Default Rules

Inbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✔ Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✔ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✘ Deny

Outbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✔ Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	✔ Allow
65500	DenyAllOutBound	Any	Any	Any	Any	✘ Deny

Augmented Security Rules

 **Add inbound security rule** ×

ps-nsg

 Basic

Source * ⓘ

IP Addresses ✓

Source IP addresses/CIDR ranges * ⓘ

192.168.1.2, 172.16.0.0/16, 10.1.10.1 ✓

Source port ranges * ⓘ

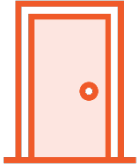
80, 443, 8080-8088 ✓



Just-in-Time (JIT) VM Access



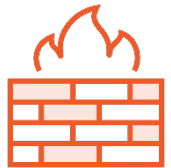
Part of Azure Security Center Standard



Uses NSGs to keep VM management ports closed



Time-windowed port access only from selected IP addresses



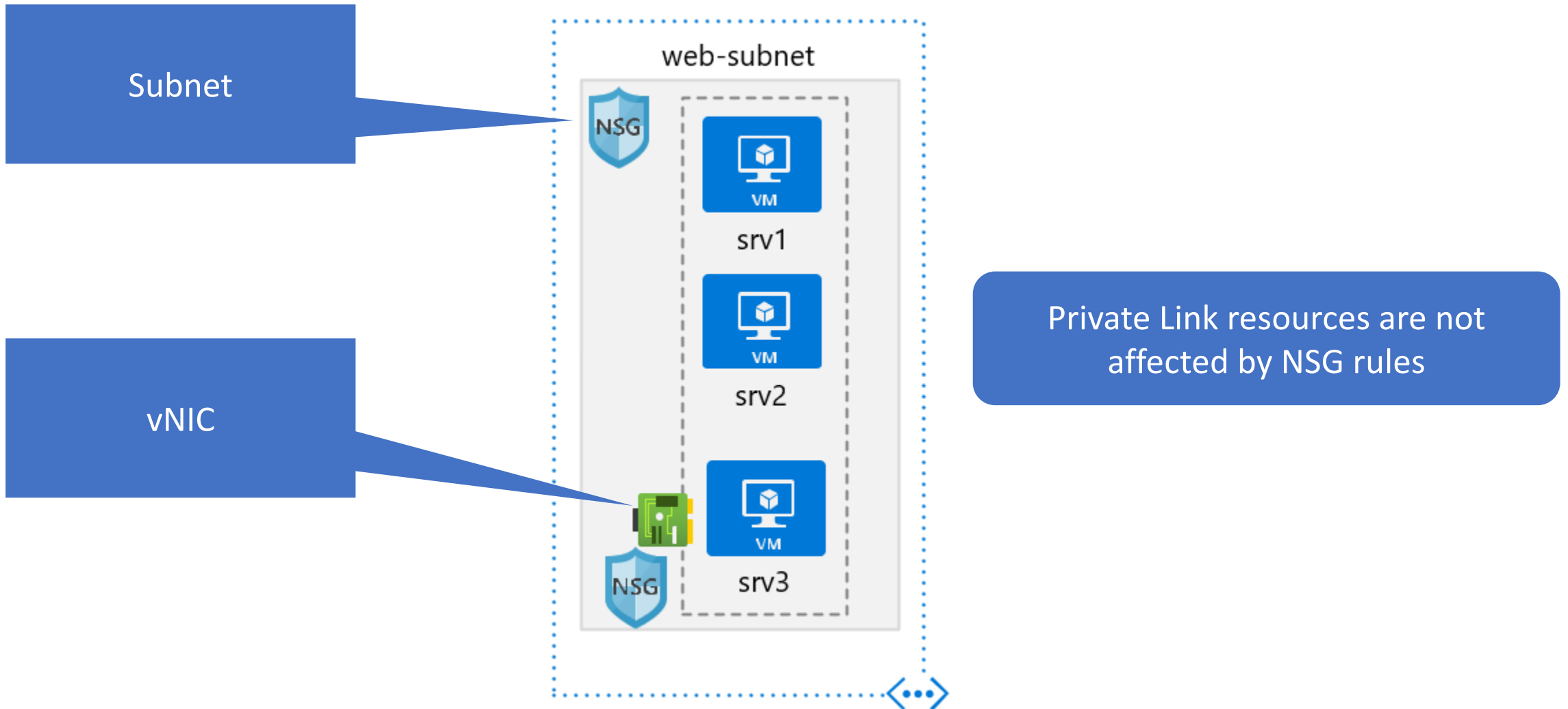
Works with Azure Firewall as well



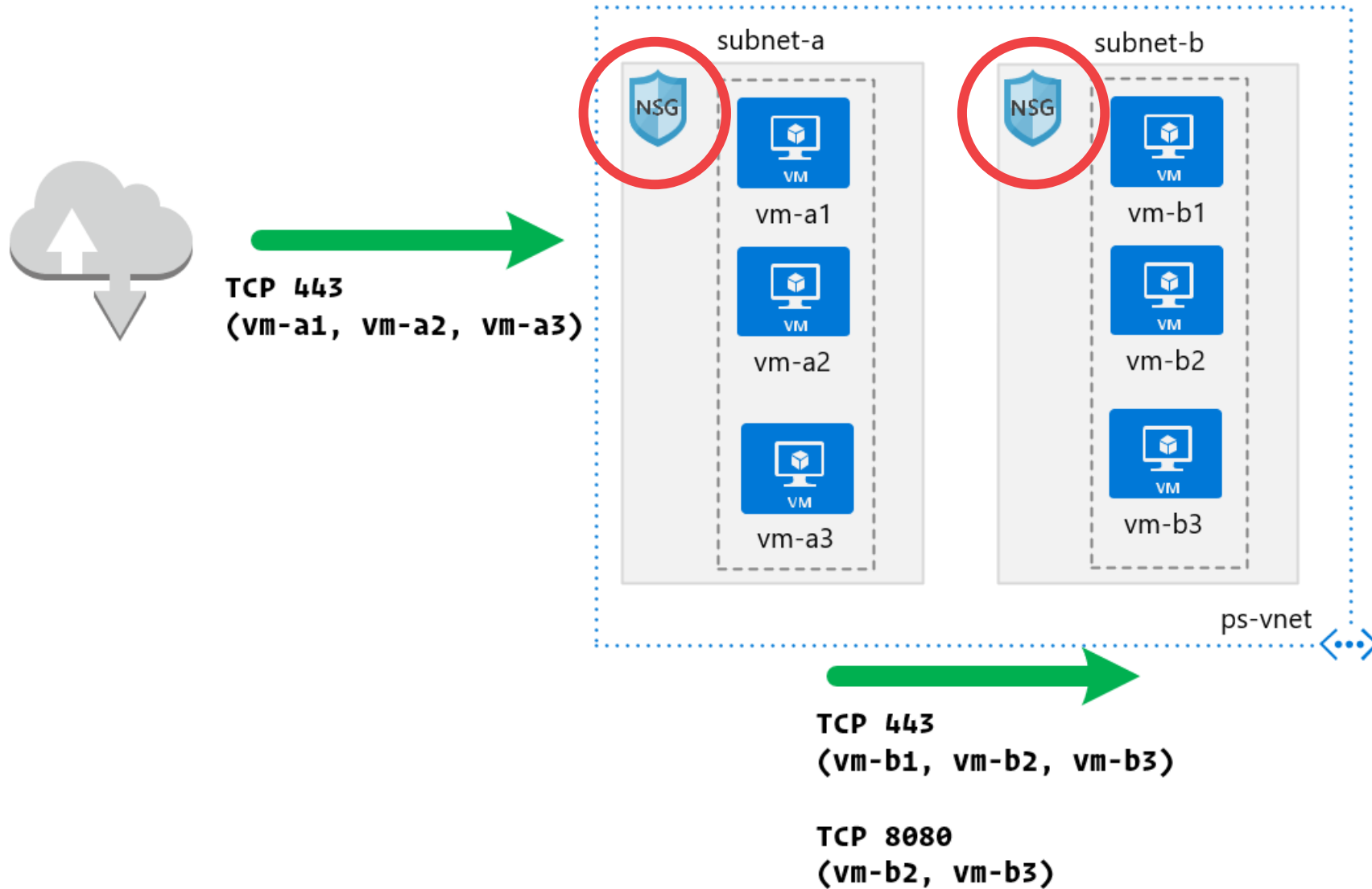
Associate NSGs with Azure Resources



NSG Associations



Lab Topology





The picture can't be displayed.

Demo

1

Explain lab topology

Create NSG

Associate it

Verify at VM level

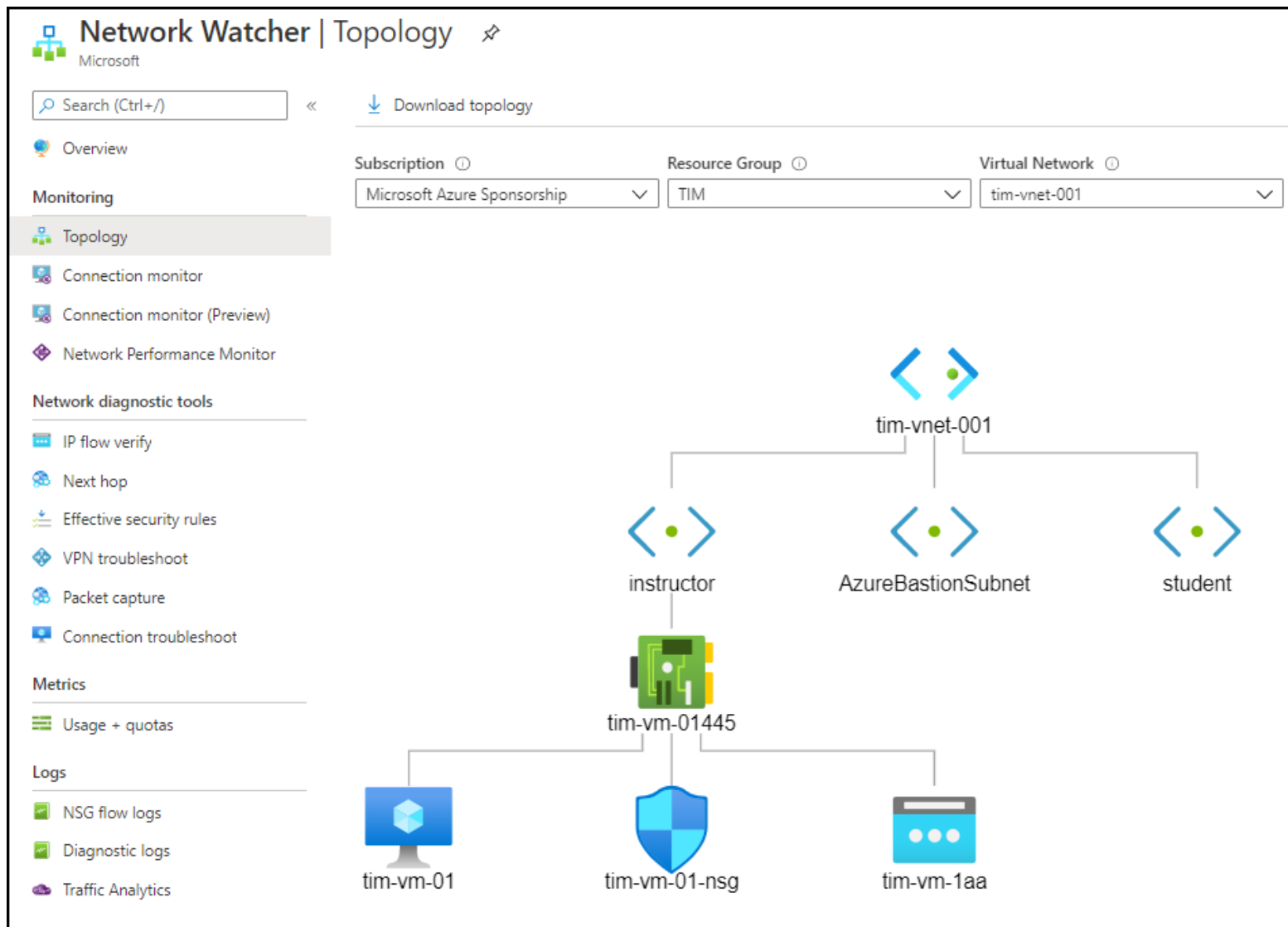


The
p

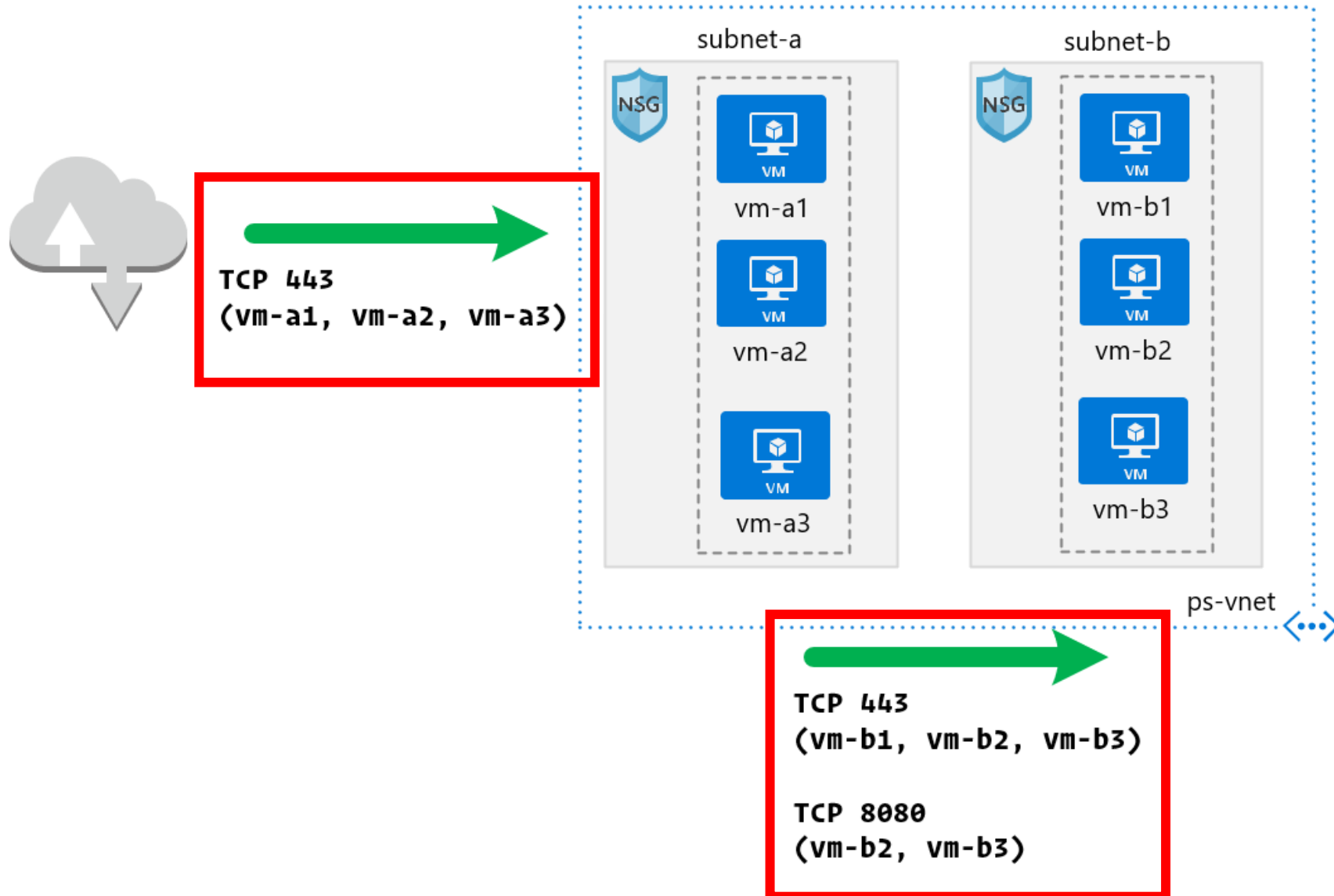
Evaluate Effective Security Rules



Network Watcher



Lab Topology





The picture can't be displayed.

Demo

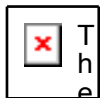
2

Enable Network Watcher

IP flow verify

Next hop

Effective rules



The

picture



The picture can't be displayed.

Summary

Don't forget about your host firewalls

You can use a NVA as an adjunct to NSGs

Next module: Implementing Azure Bastion and
Azure Firewall



T
h
e
p