Microsoft Azure Administrator: Secure Access to Virtual Networks

PROTECTING AZURE VIRTUAL NETWORK TRAFFIC WITH NSGS

Tim Warner
AUTHOR EVANGELIST, PLURALSIGHT

@TechTrainerTim TechTrainerTim.com

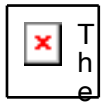
Overview

Describe this course

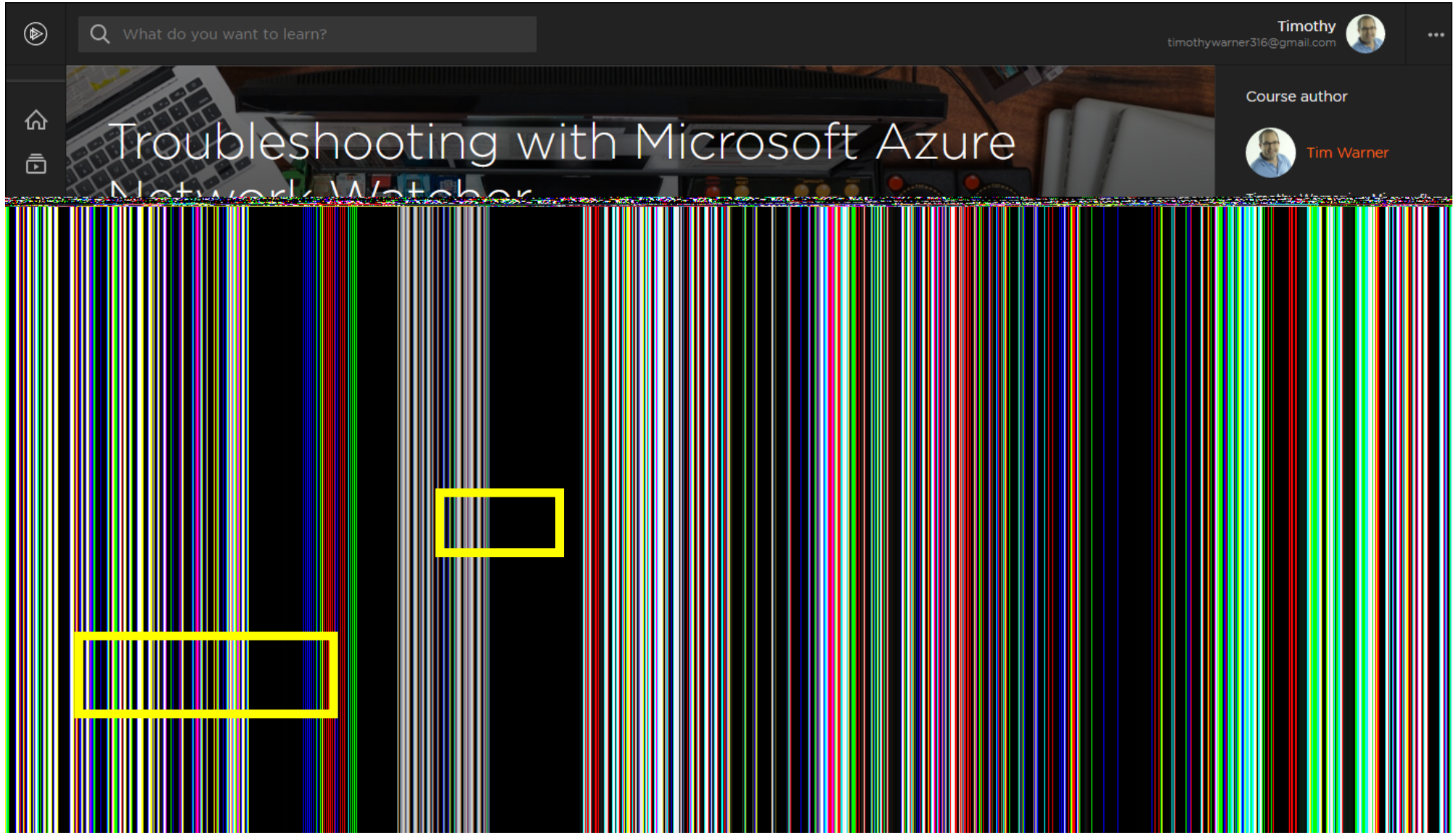
Create NSGs and security rules

Associate an NSG to a subnet or network interface

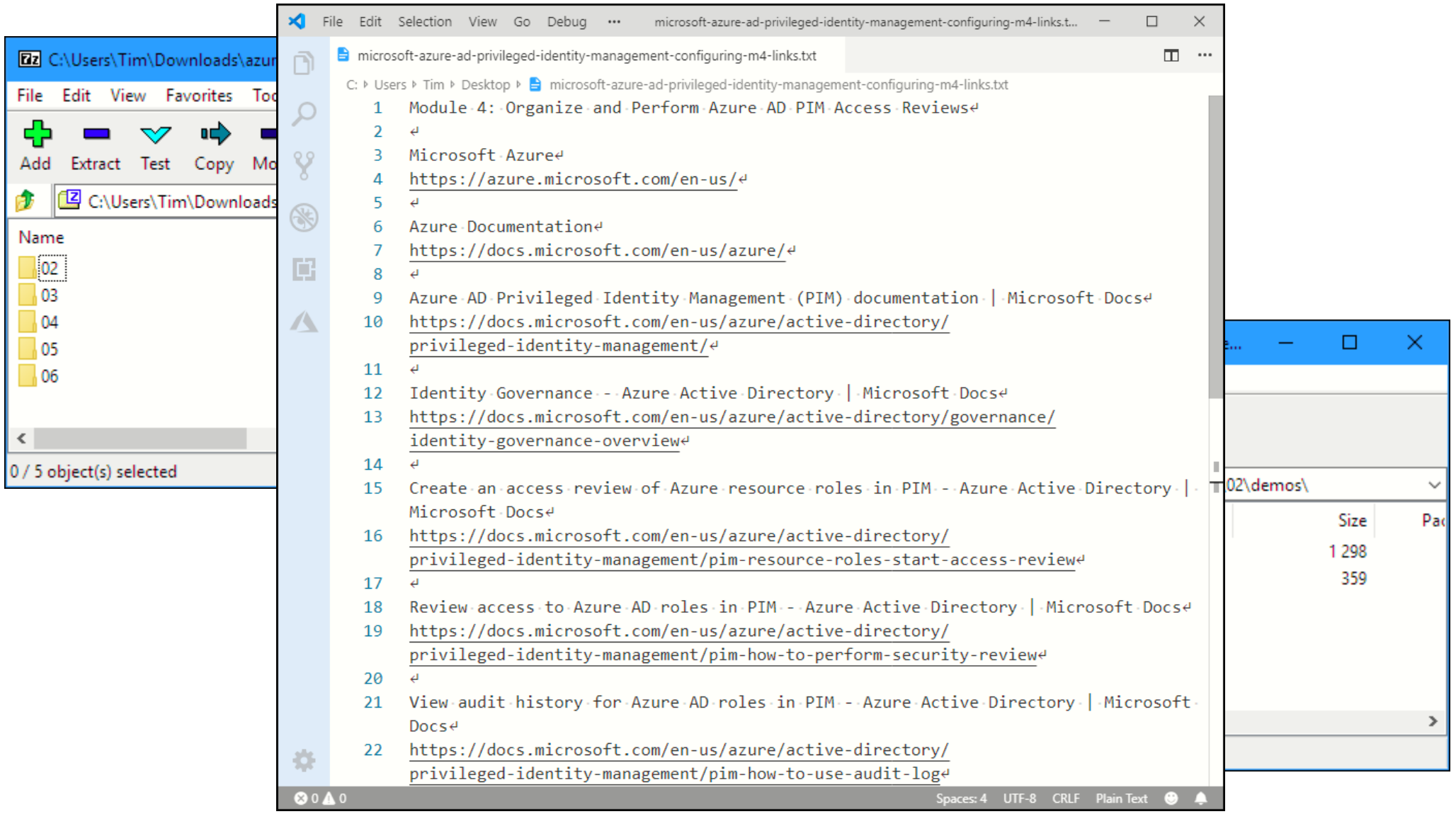
Evaluate effective security rules



Exercise Files

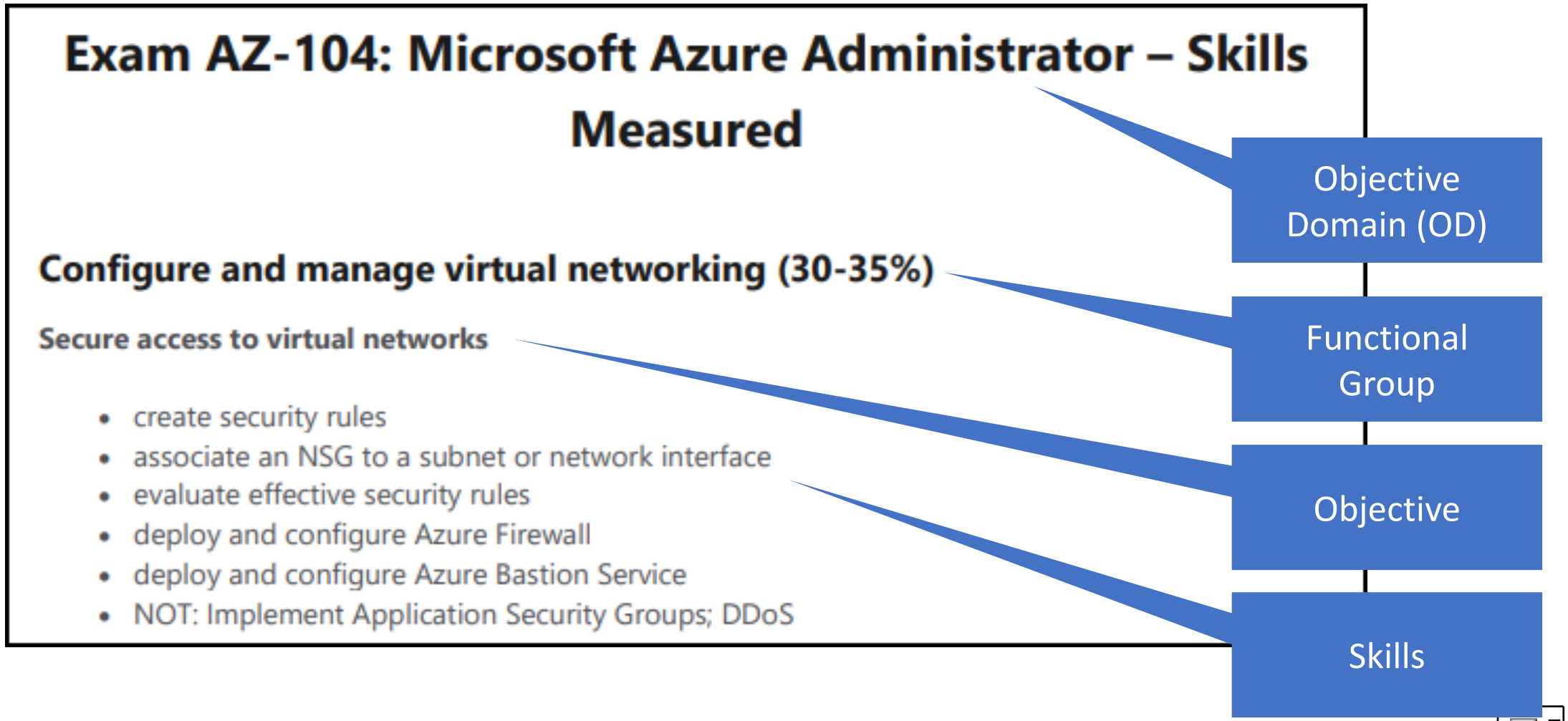


Exercise Files



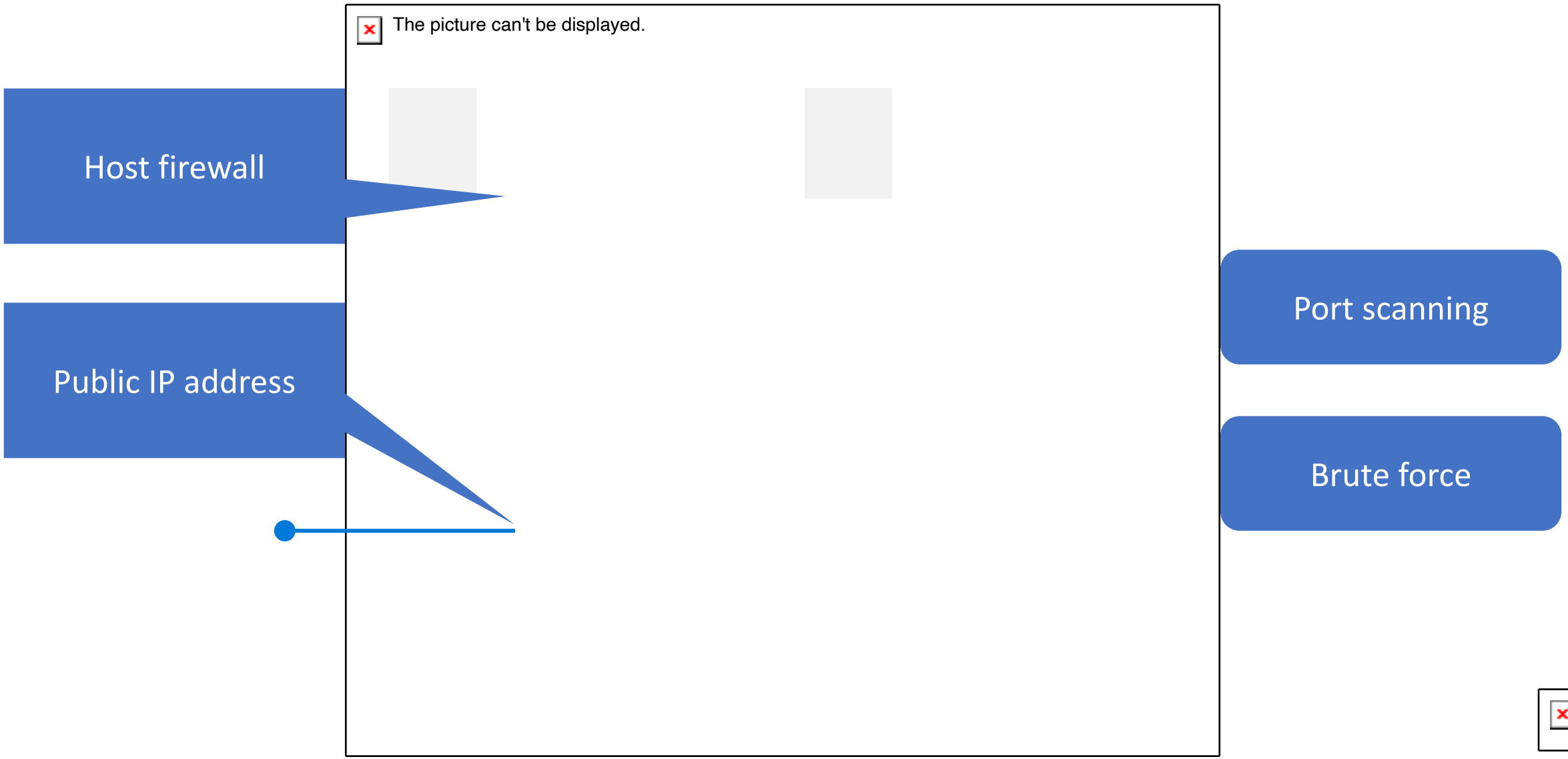
Understand this Course

Azure Administrator Certification (AZ-104)



Create NSGs and Security Rules

The Use Case


The picture can't be displayed.
Host firewall
Public IP address
Port scanning
Brute force

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

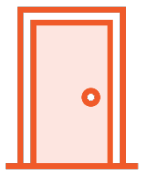
Outbound security rules

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

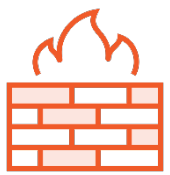
Just-in-Time (JIT) VM Access

Part of Azure Security Center Standard

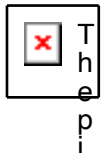


Uses NSGs to keep VM management ports closed

Time-windowed port access only from selected IP addresses



Works with Azure Firewall as well

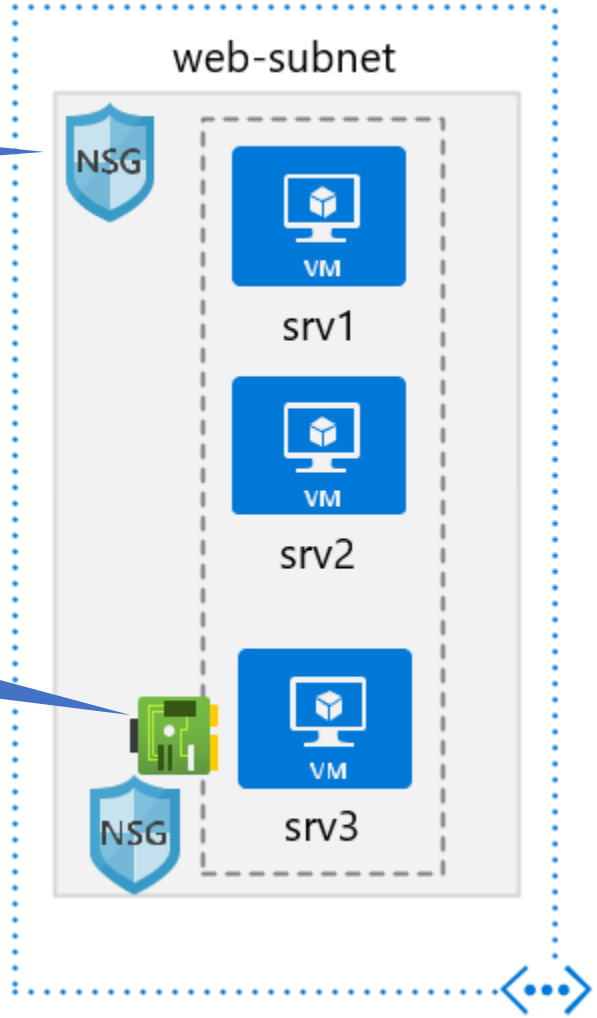


Associate NSGs with Azure Resources

NSG Associations

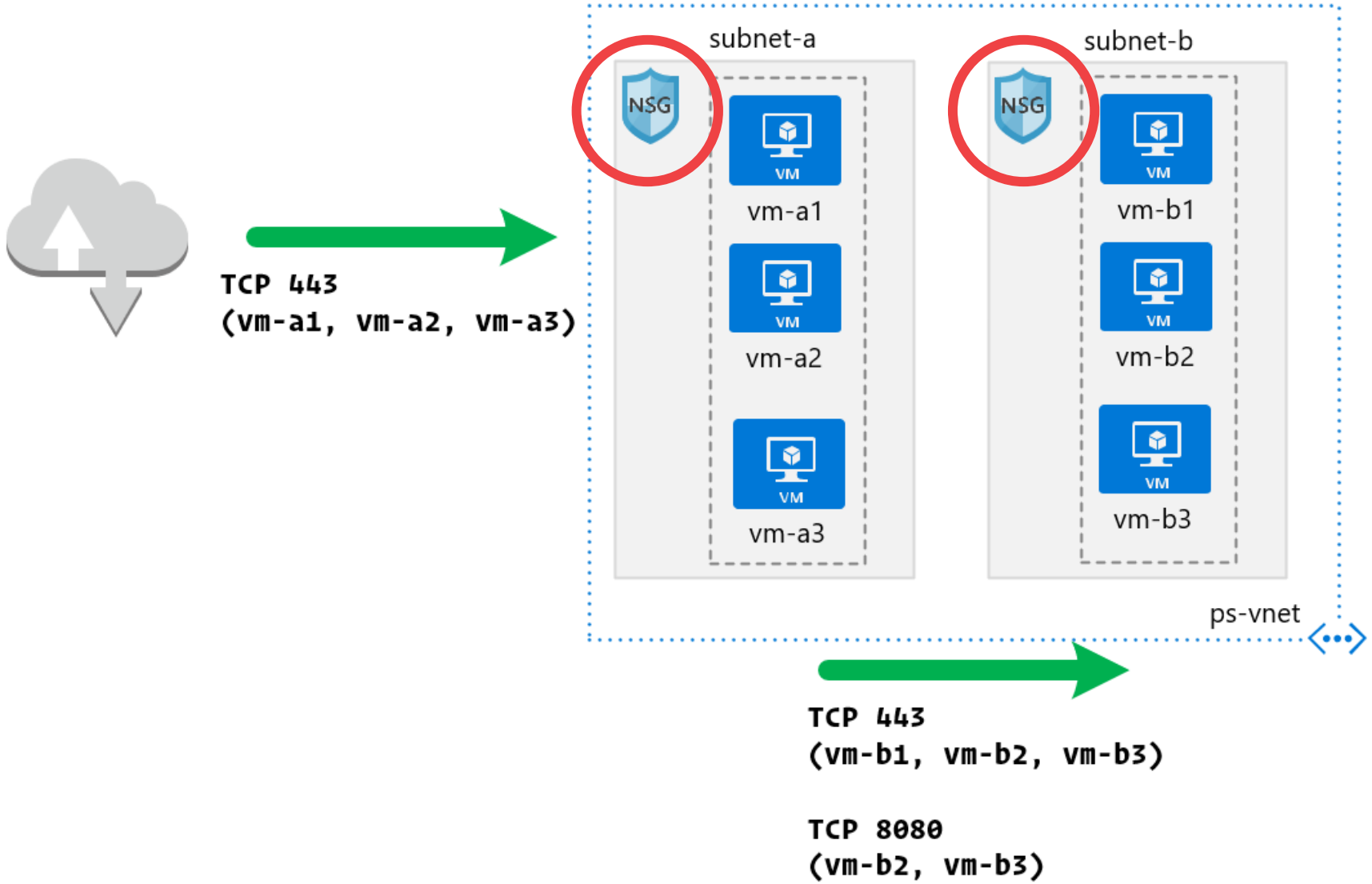
Subnet

vNIC



Private Link resources are not affected by NSG rules

Lab Topology



The picture can't be displayed.

Demo

1

Explain lab topology

Create NSG

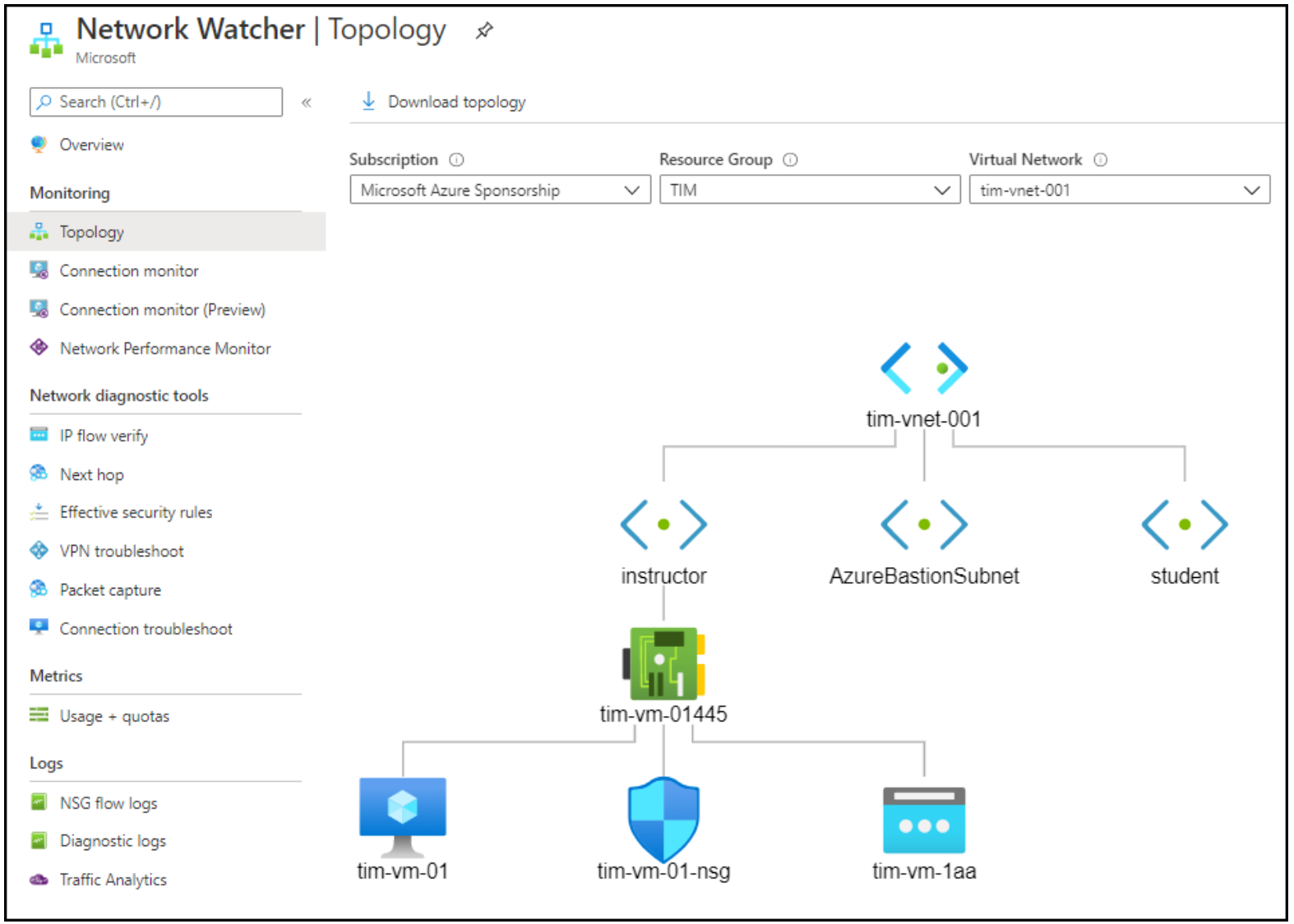
Associate it

Verify at VM level

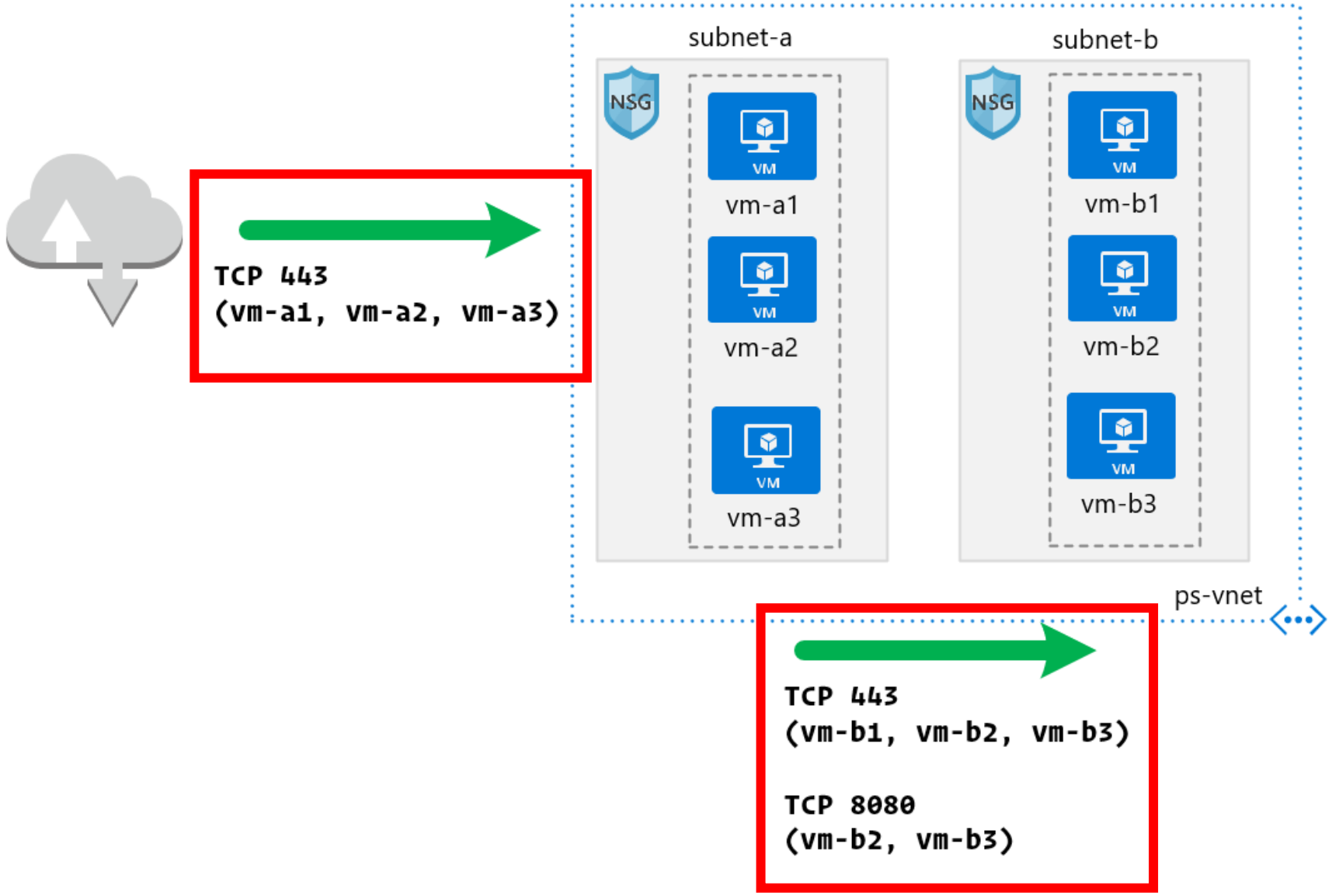
The pi

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 pi

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