# Implementing Azure Bastion and Azure Firewall


**Tim Warner**

AUTHOR EVANGELIST, PLURALSIGHT

@TechTrainerTim TechTrainerTim.com



# Overview

Describe network virtual appliances

Plan, deploy, and configure Azure Bastion Service

Plan, deploy, and configure Azure Firewall

# Describe Network Virtual Appliances

# Network Virtual Appliances (NVAs)

**Preconfigured virtual machines (VMs)**

- Web application firewalls
- Application delivery controllers
- Load balancers
- WAN optimizers

**Thin Linux layer plus enterprise software**

# Network Virtual Appliances (NVAs)

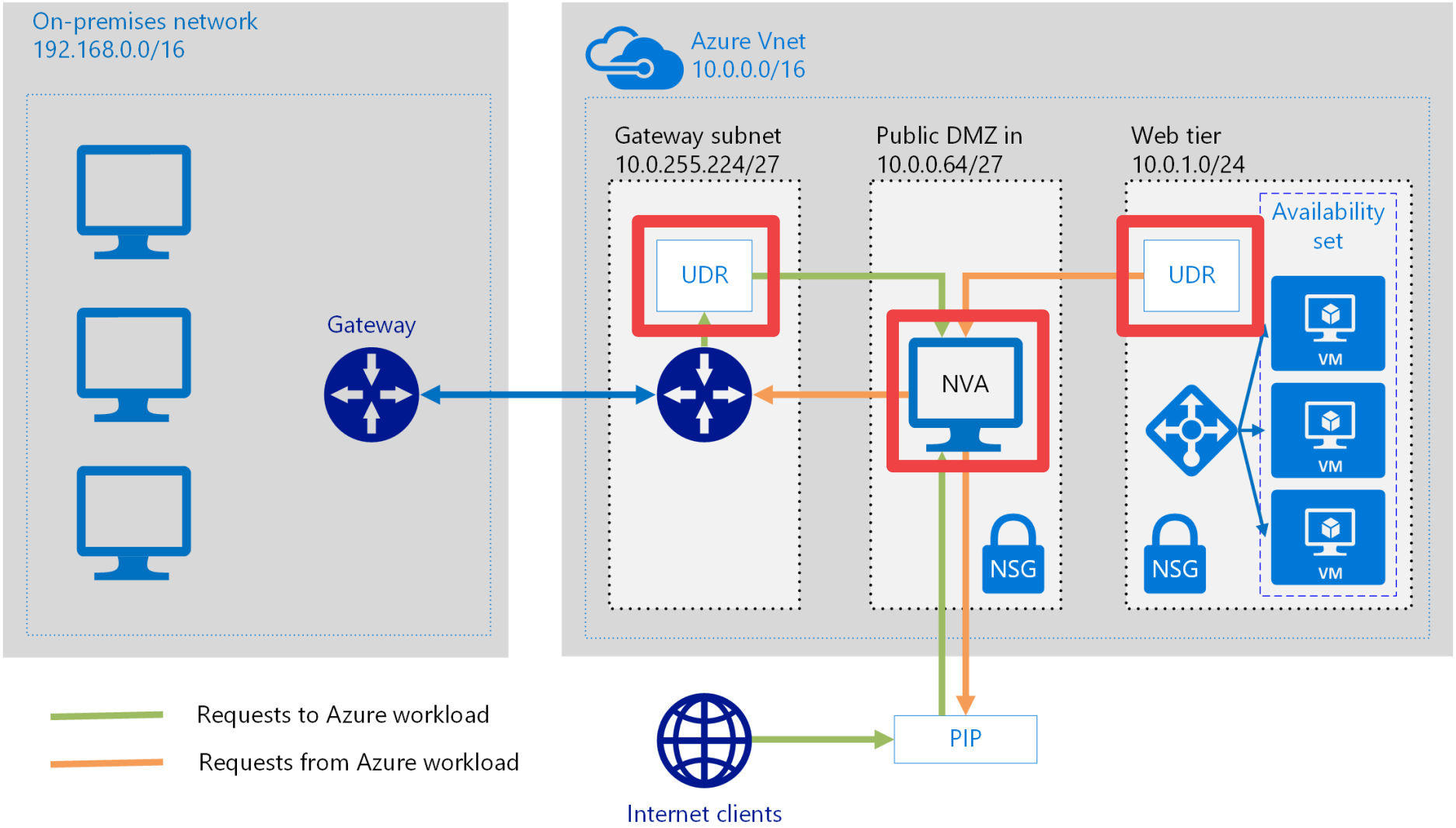
**Popular vendors**

- Cisco
- F5 Networks
- NetApp

**Flexible licensing**

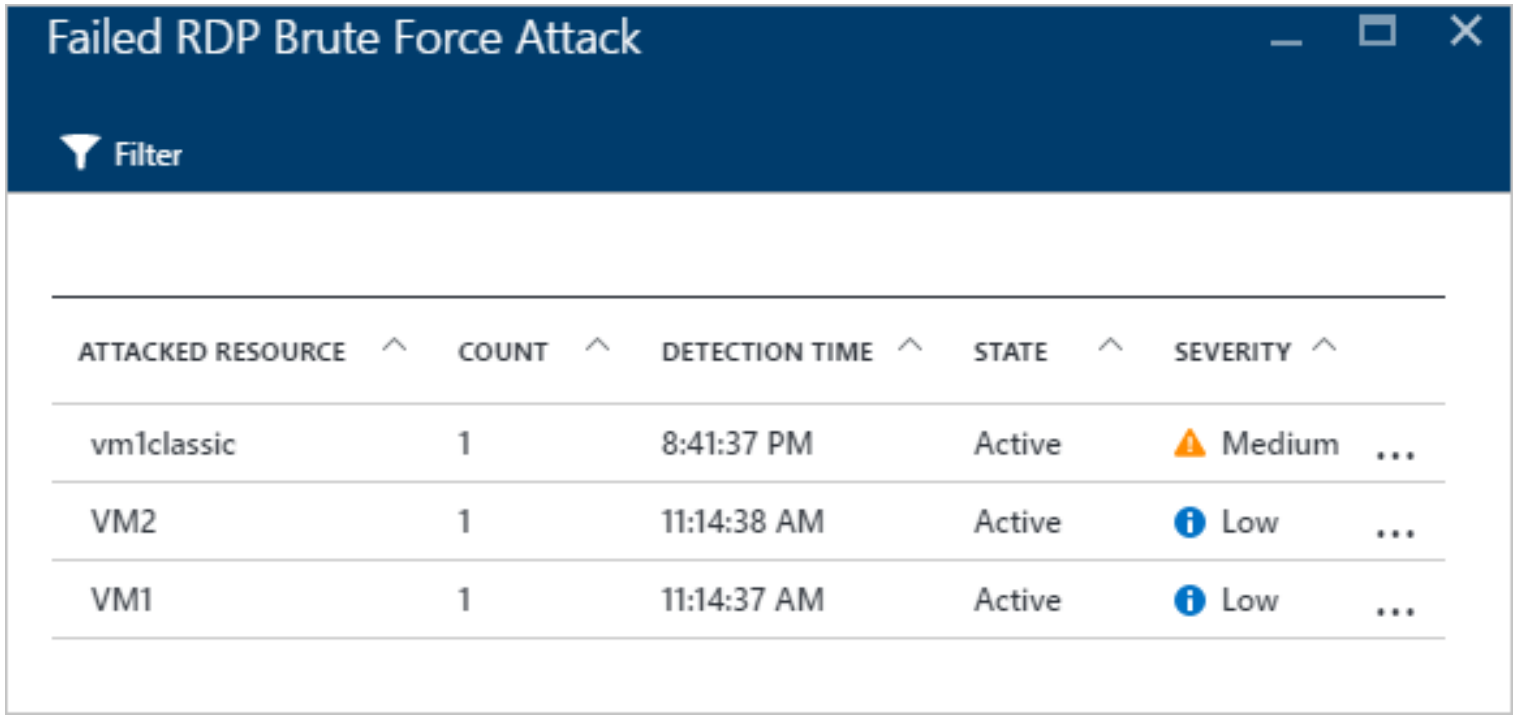
**Requires an understanding of user-defined routing (UDR) in Azure**

# Sample NVA Topology



# Azure Bastion

# The Use Case



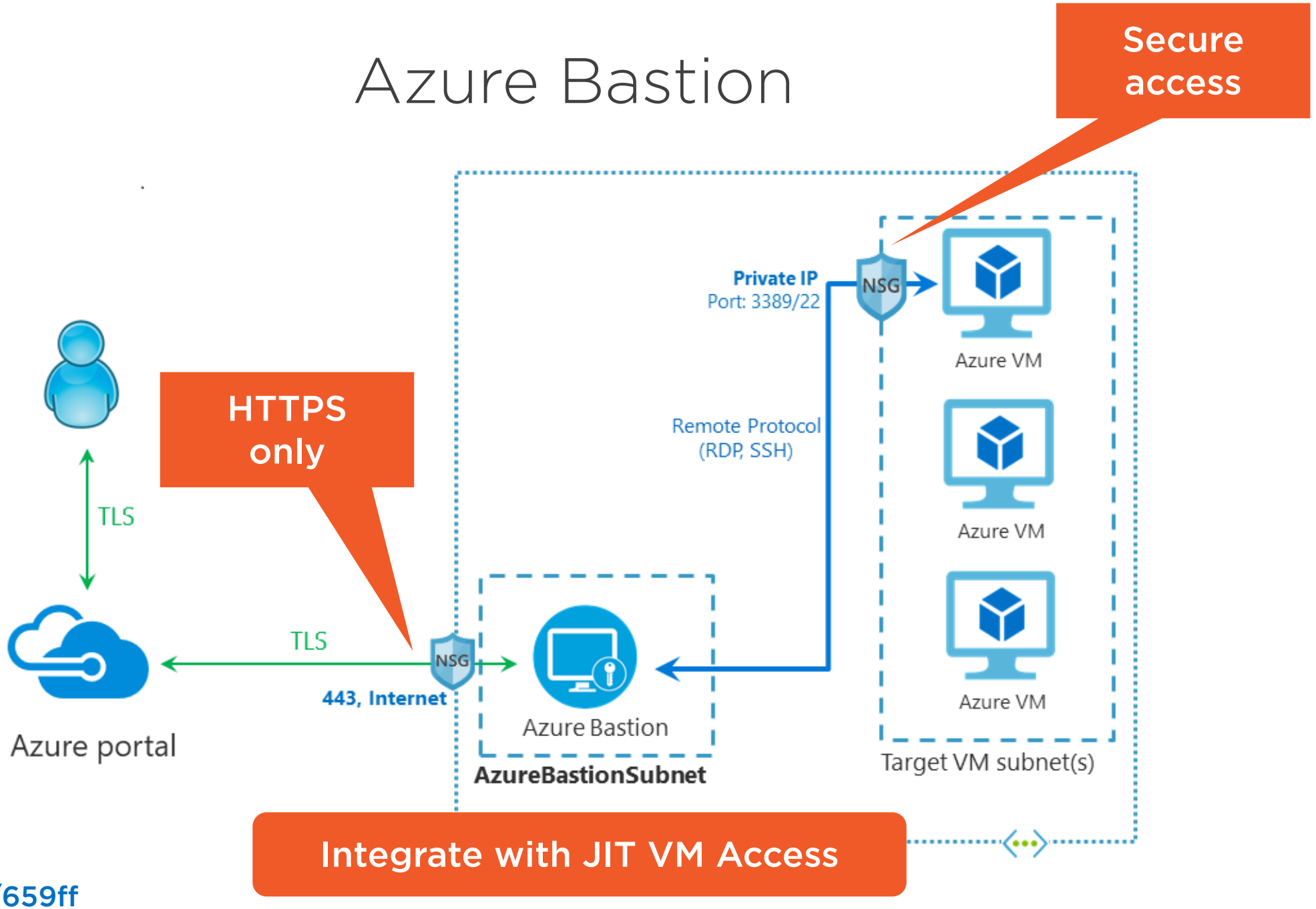

Microsoft publishes their service tags every month

You may have VMs with public IP addresses

Bad actors perform port scanning for RDP (3389) and SSH (22)

https://timw.info/b7dc7

# Azure Bastion




https://timw.info/659ff

# Azure Bastion Points to Ponder

**No service chaining**

One Bastion per virtual network

**Fully managed**

No stop; no RDP policy

**Browser experience**

Client tools are on the roadmap

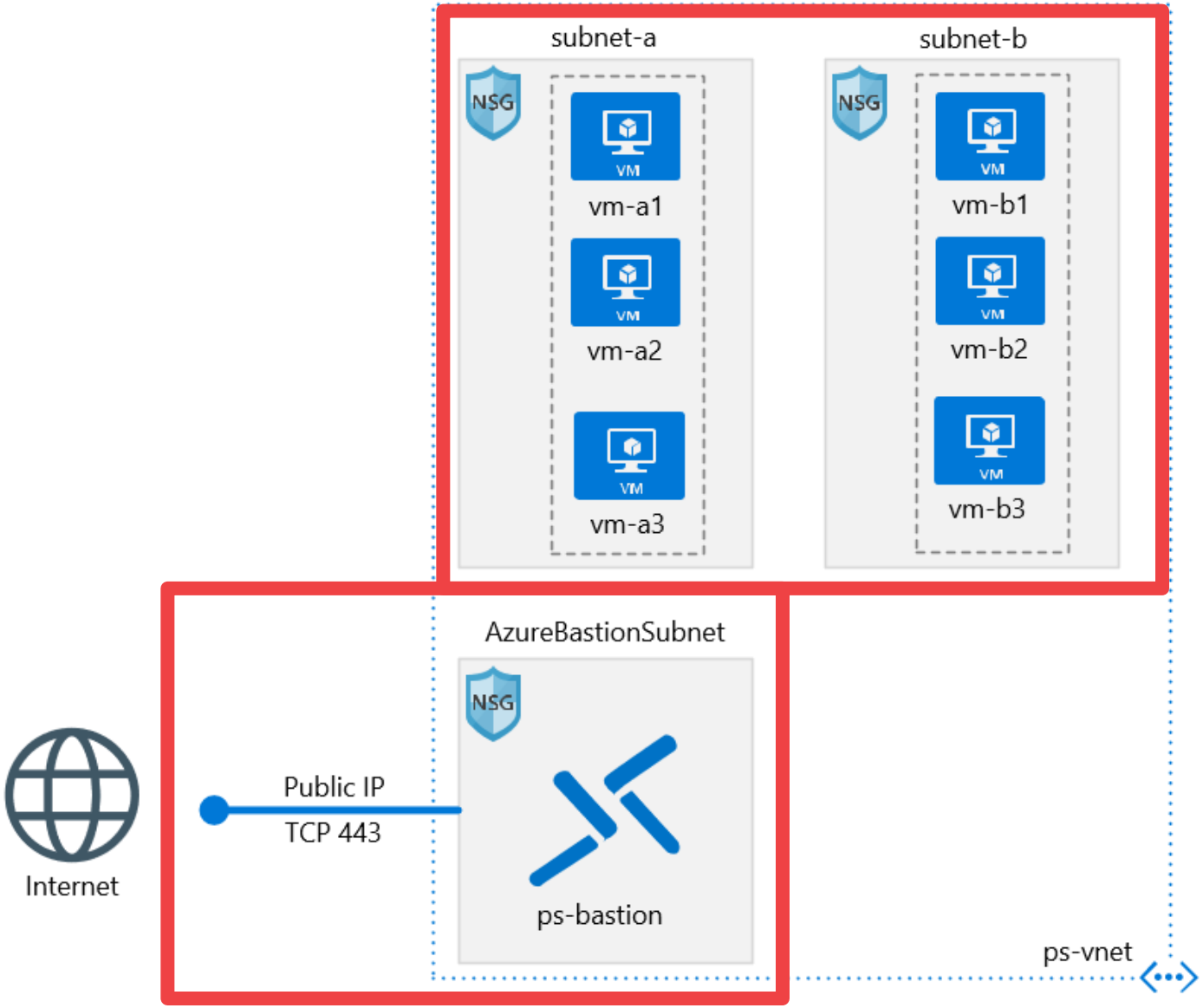
**NSGs**

Ingress from Internet and AB control plane

**NSGs**

Egress to VMs and AzureCloud tag

# Lab Topology



# Demo

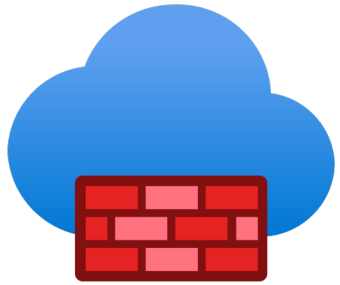

Add a Bastion

Connect

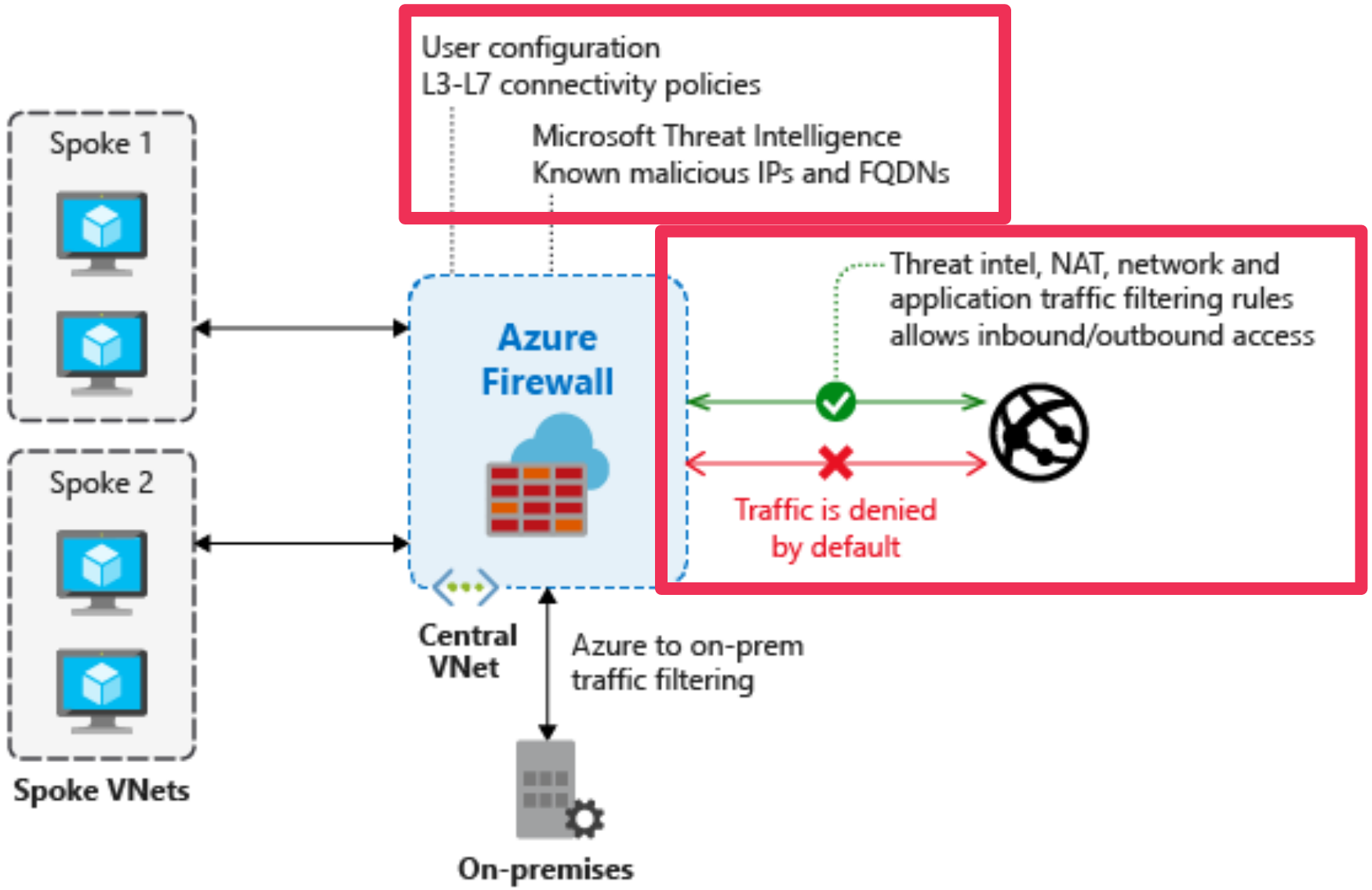
Layer in JIT VM Access

Connect

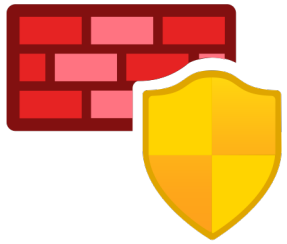
# Azure Firewall



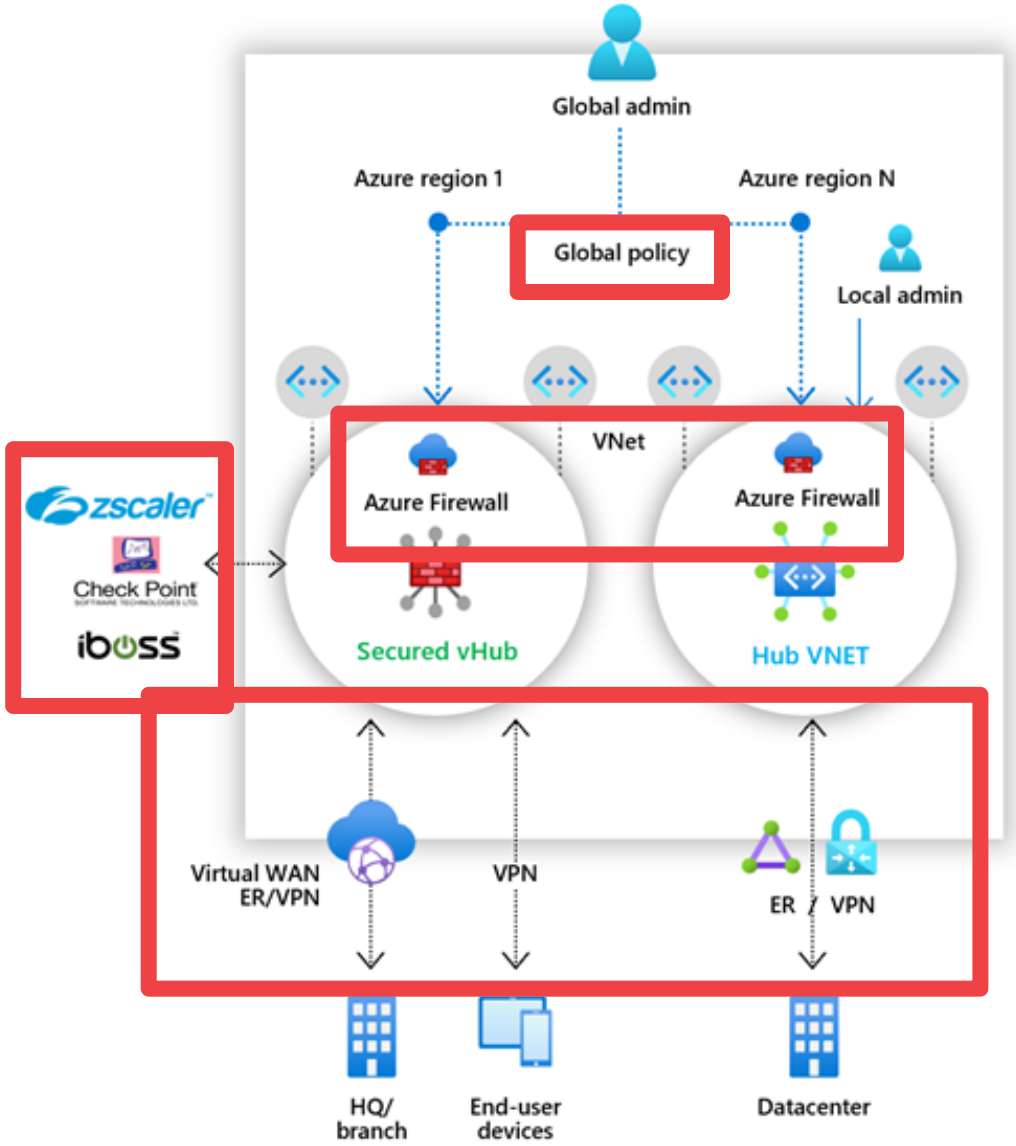
# Azure Firewall



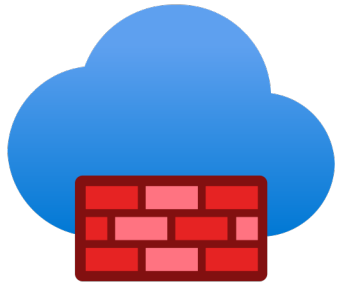

https://timw.info/51b82



# Azure Firewall Manager




https://timw.info/d0517



# Azure Firewall Points to Ponder

**No NSGs**

Firewall disables NSGs on its subnet

**Cost savings**

Deallocate and allocate

**Service chaining**

Firewall can centrally route and filter

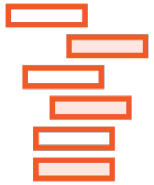
**Forced Tunneling**

Useful in a hybrid cloud environment

**Scale-out**

You need a /26 firewall subnet

# Azure Firewall, Bastion, and JIT VM Access

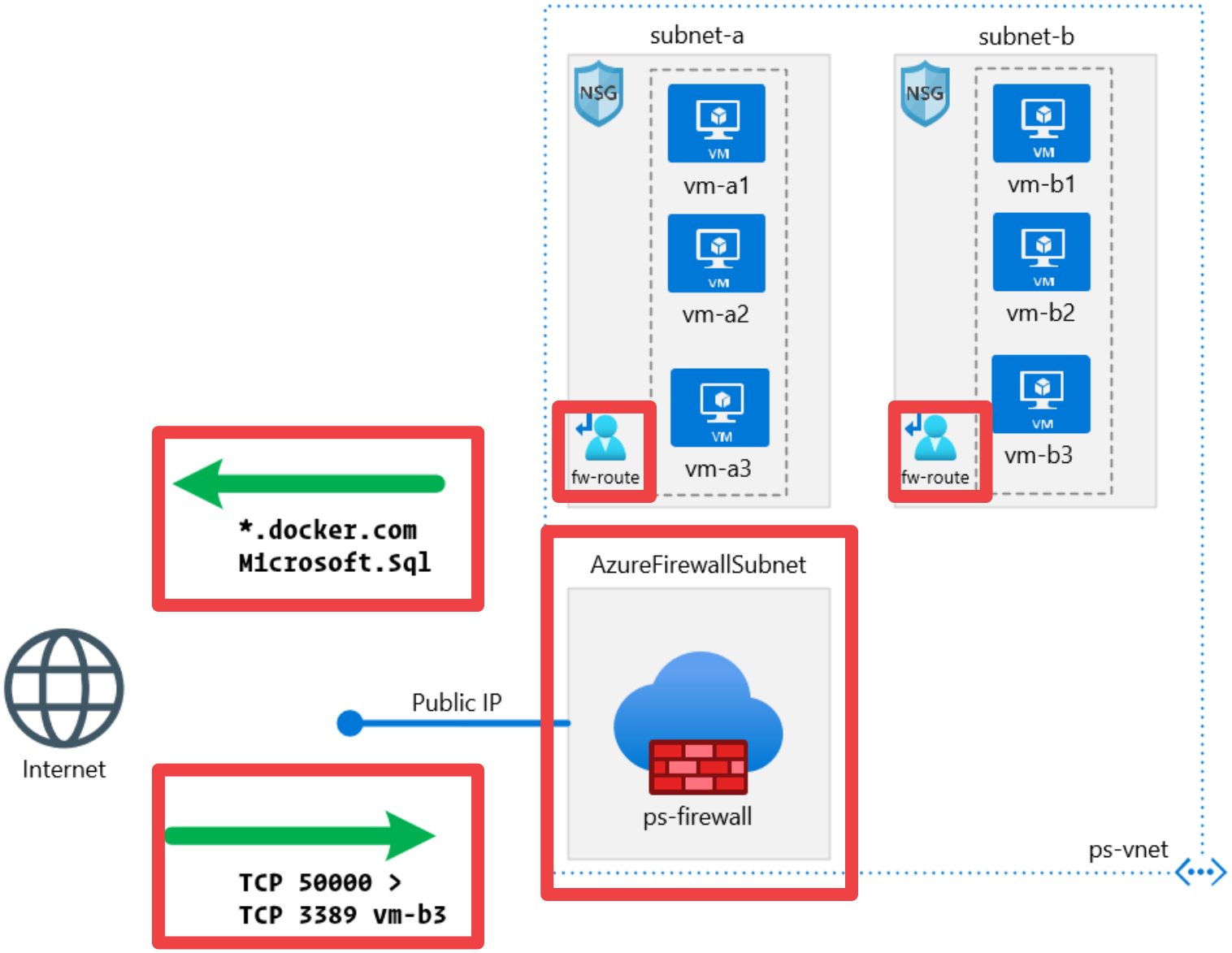


Either an NSG or Azure Firewall can be used with JIT VM Access

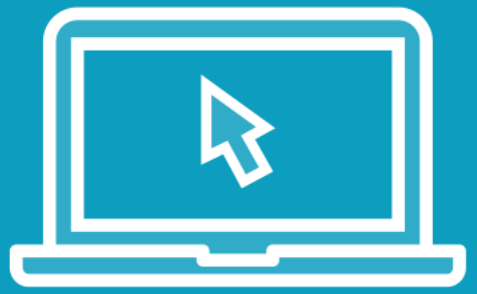

Connect through the Firewall's public IP (DNAT)

Bastion and JIT VM Access are incompatible (according to Microsoft)

# Lab Topology



# Demo



2

**Add Azure Firewall**

- Route tables

**Make DNS rule**

**Make a DNAT rule**

# Summary

At this point, there is no good reason to have your Azure VM management ports open

Consider Azure Firewall Manager policy for centralized administration

Don't forget about third-party NVAs

Thanks!

Courses: timw.info/ps

Twitter: @TechTrainerTim

Website: TechTrainerTim.com