

Microsoft Azure Network Engineer: Secure and Monitor Networks

Design, Implement, and Manage an Azure Firewall Deployment



Tim Warner

Principal Author Evangelist, Pluralsight

@TechTrainerTim TechTrainerTim.com



Overview



Design and implement an Azure Firewall deployment

Create and implement Azure Firewall Manager policies and rules

Integrate Azure Firewall and third-party NVAs with an Azure Virtual WAN hub



Exercise Files

What do you want to learn?

Timothy
timothywarner316@gmail.com

Troubleshooting with Microsoft Azure Network Watcher

by Tim Warner

Microsoft now gives you packet-level access to your Windows Server and Linux virtual machines (VMs) running in Azure. You'll learn how to use Network Watcher to troubleshoot network security groups (NSGs), perform packet captures, and much more.

Resume Course

Bookmark

Add to Channel

Table of contents

Description

Transcript

Exercise files

Discussion

Learning Check

Recommended

These exercise files are intended to provide you with the assets you need to create a video-based hands-on experience. With the exercise files, you can follow along with the author and re-create the same solution on your computer. We find this to be even more effective than written lab exercises.

Download exercise files

Course author

Tim Warner

Timothy Warner is a Microsoft Most Valuable Professional (MVP) in Cloud and Datacenter Management who is based in Nashville, TN.

Course info

Level	Intermediate
Rating	★★★★★
My rating	★★★★★
Duration	2h 12m
Released	31 Oct 2017

Share course

Exercise Files

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

- File Explorer:** Located on the left, it shows the path `C:\Users\Tim\Downloads\azure`. The file list contains folders named 02, 03, 04, 05, and 06. The status bar at the bottom indicates "0 / 5 object(s) selected".
- Code Editor:** The central window is titled `microsoft-azure-ad-privileged-identity-management-configuring-m4-links.txt`. It displays a list of 22 lines of text, which are links to various Microsoft documentation pages. The text 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↵
```
- File Details Window:** A small window on the right shows details for a file in the `02\demos\` folder. It includes a table with the following data:

Size	Pa
1 298	
359	

The code editor's status bar at the bottom shows "Spaces: 4", "UTF-8", "CRLF", and "Plain Text".



Exam AZ-700

Exam AZ-700: Designing and Implementing Microsoft Azure Networking Solutions – Skills Measured

Secure and Monitor Networks (15–20%)

Design, implement, and manage an Azure Firewall deployment

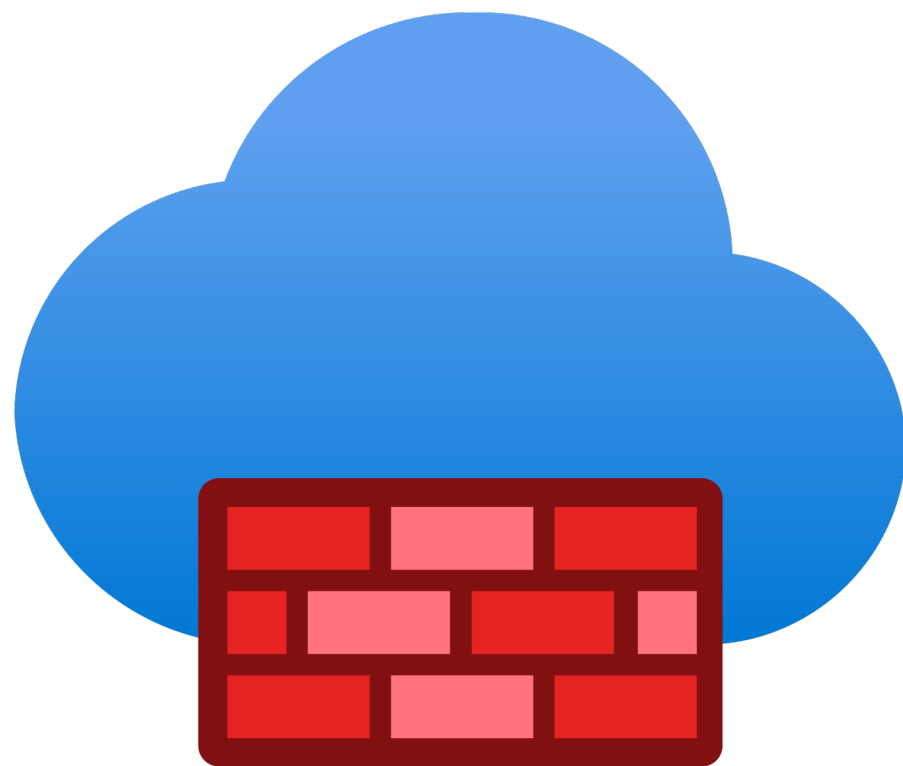
- design an Azure Firewall deployment
- create and implement an Azure Firewall deployment
- configure Azure Firewall rules
- create and implement Azure Firewall Manager policies
- create a secure hub by deploying Azure Firewall inside an Azure Virtual WAN hub
- integrate an Azure Virtual WAN hub with a third-party NVA



Design and Implement an Azure Firewall Deployment



Azure Firewall



Managed stateful firewall that works from OSI Layer 3 to Layer 7

Integration with Microsoft Threat Intelligence

Centralized policy management

Availability zone awareness

SNAT and DNAT support

Azure Monitor integration



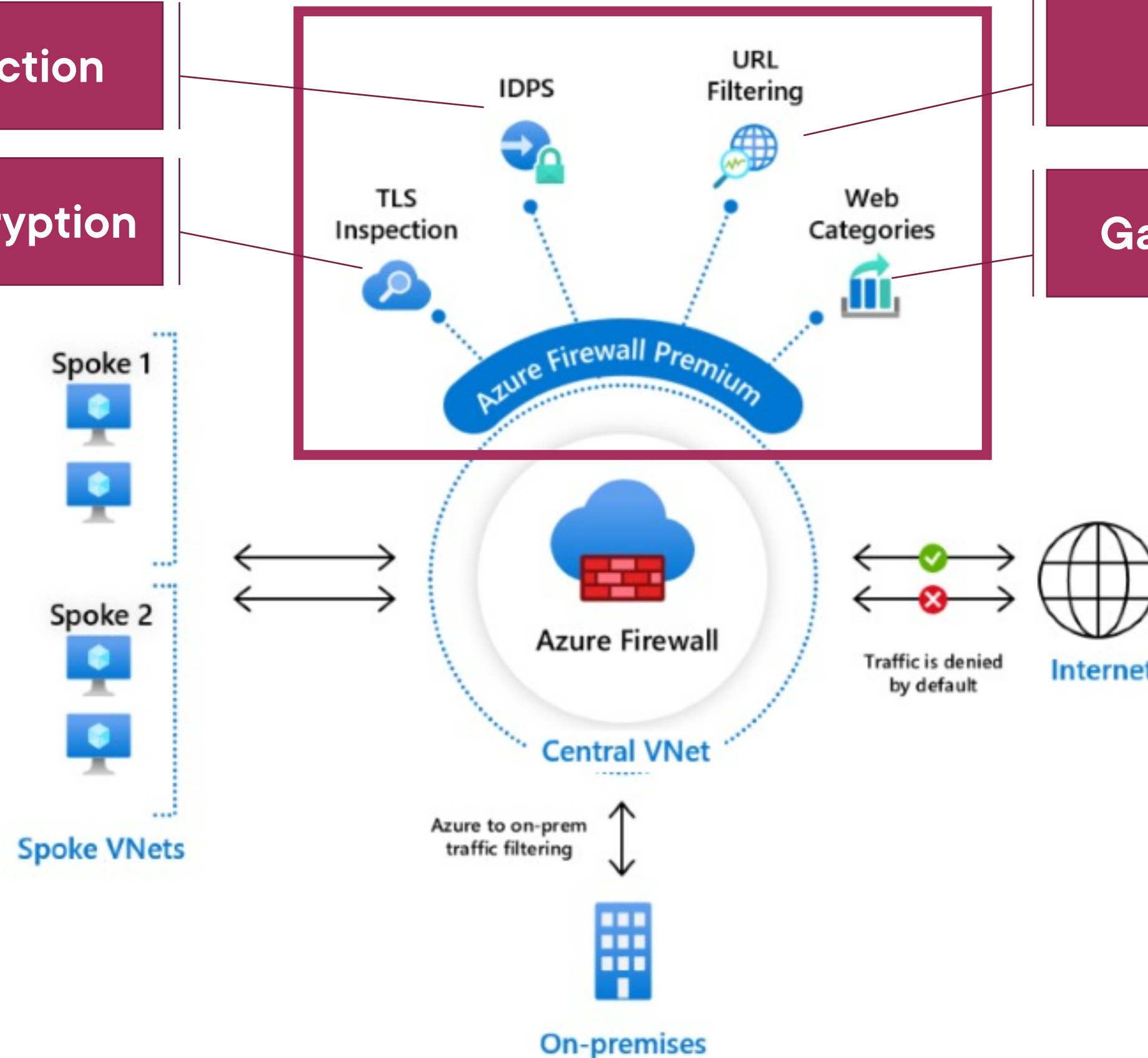
Azure Firewall Premium

Signature-based detection

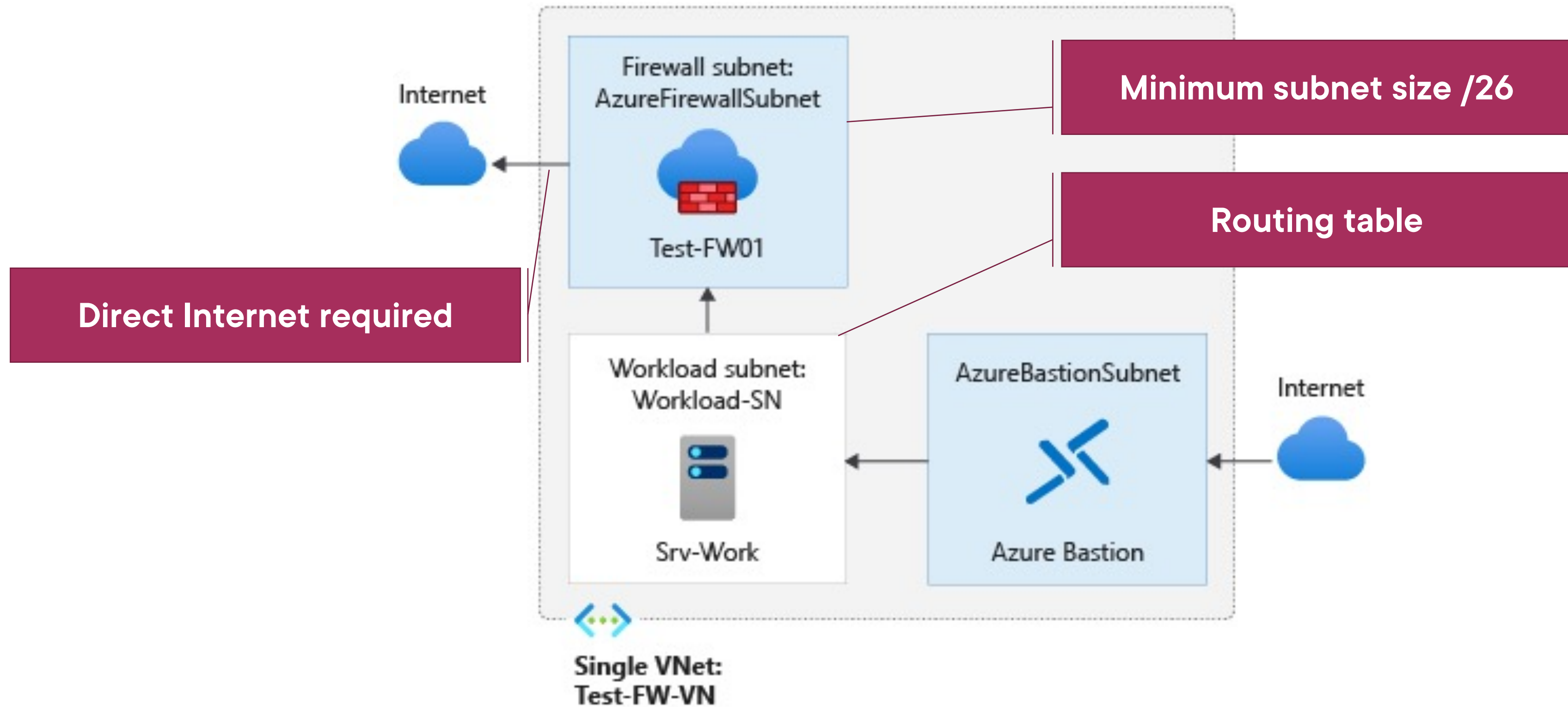
TLS decryption/re-encryption

Considers entire URL

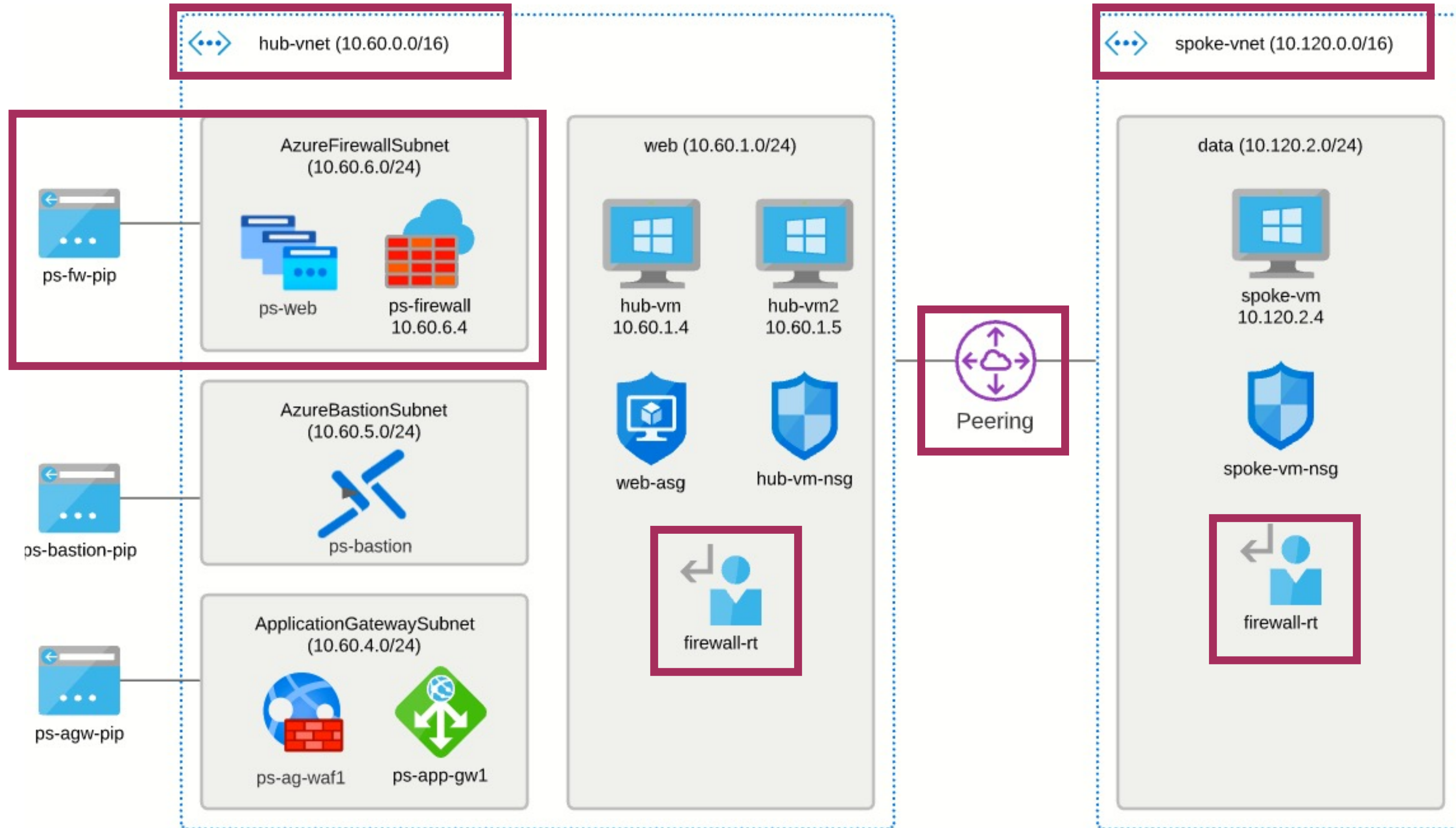
Gambling, social media, etc



Azure Firewall Deployment Notes



Our Lab Topology



Demo



1

Set up hub-spoke Vnets

Deploy Azure Firewall

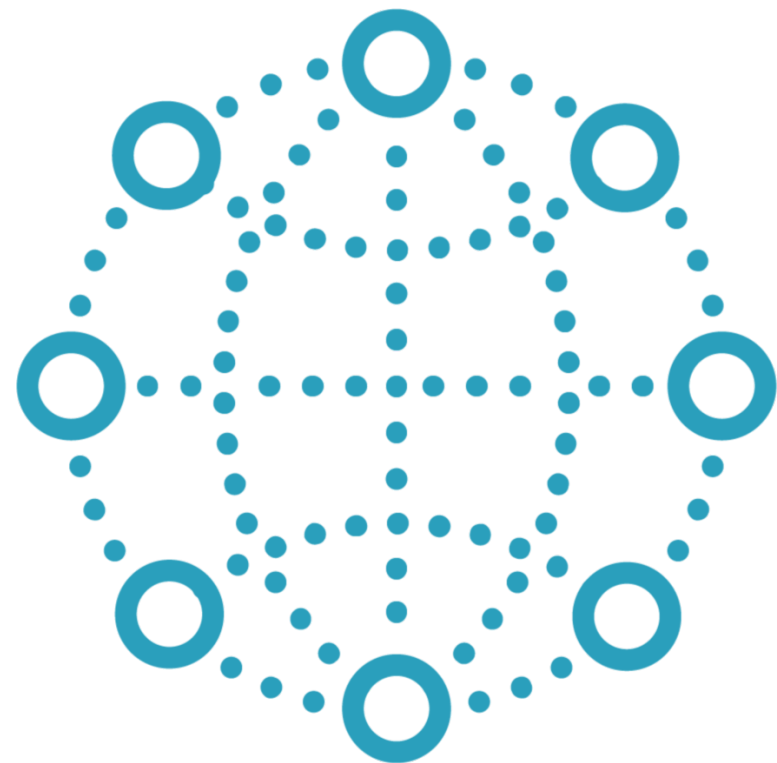
Configure routing tables



Define Azure Firewall Policies and Rules



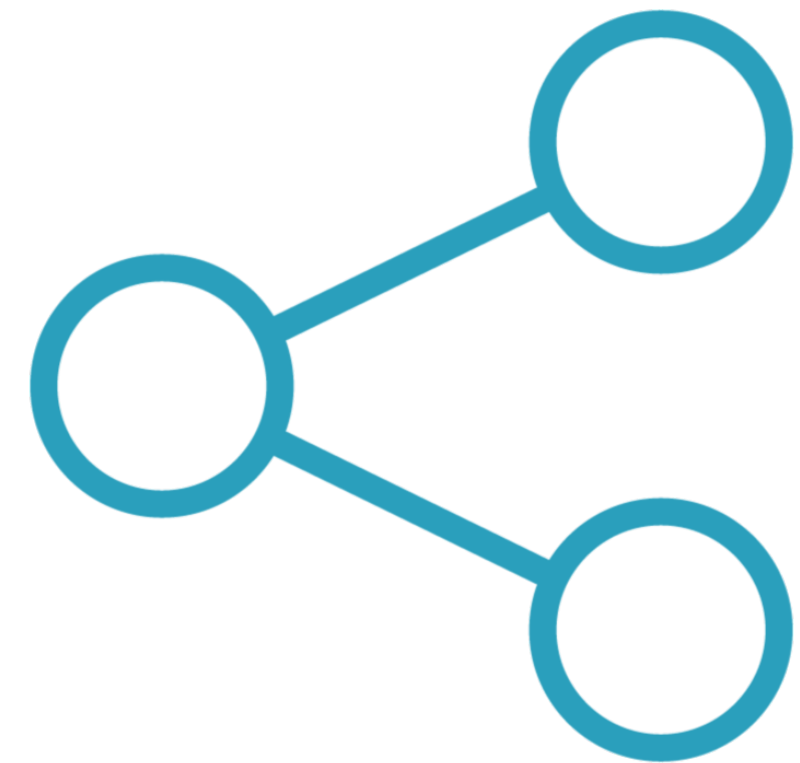
Azure Firewall Rule Types



Network
OSI Layer 4
5-tuple match

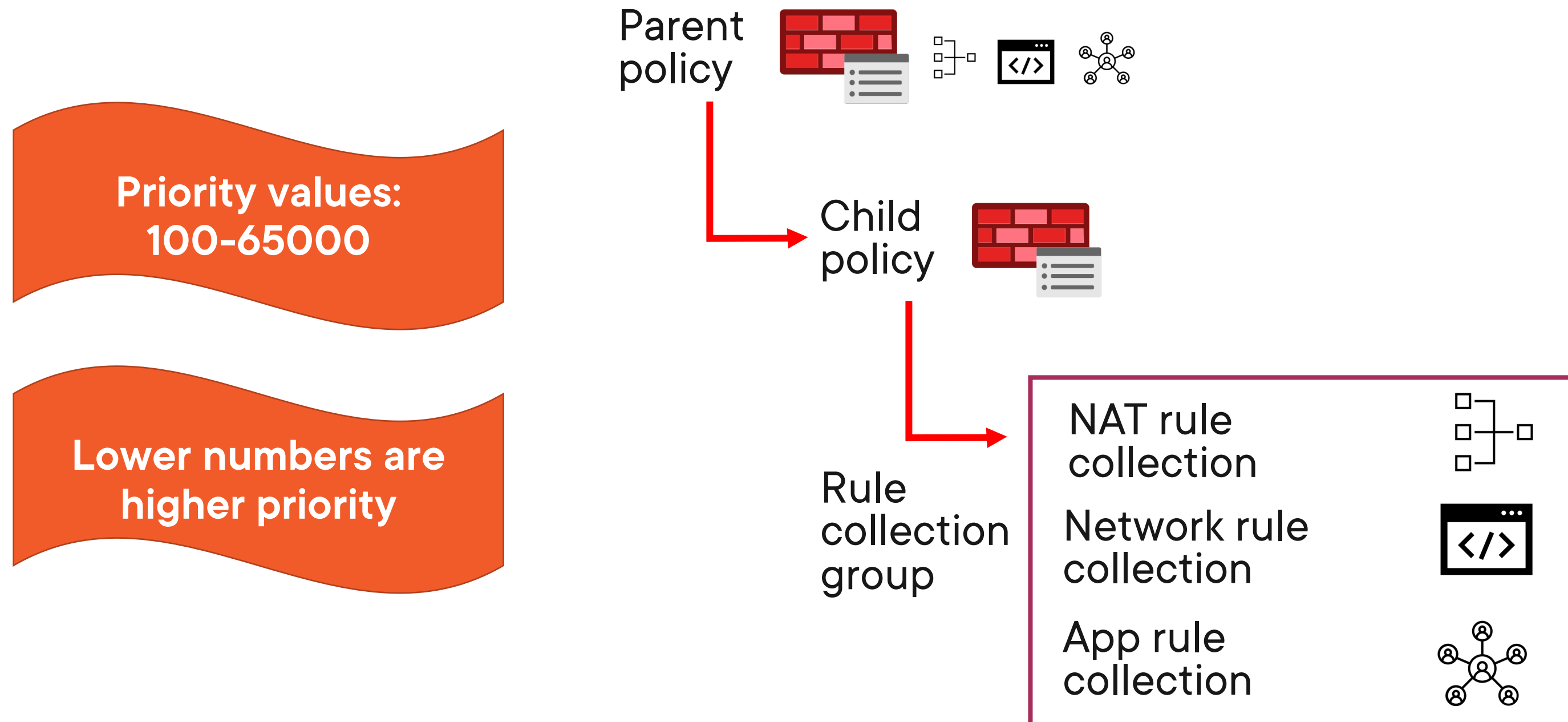


Application
OSI Layer 7
FQDN match



DNAT
OSI Layer 4
Inbound connections

Azure Firewall Policy-Based Rule Processing



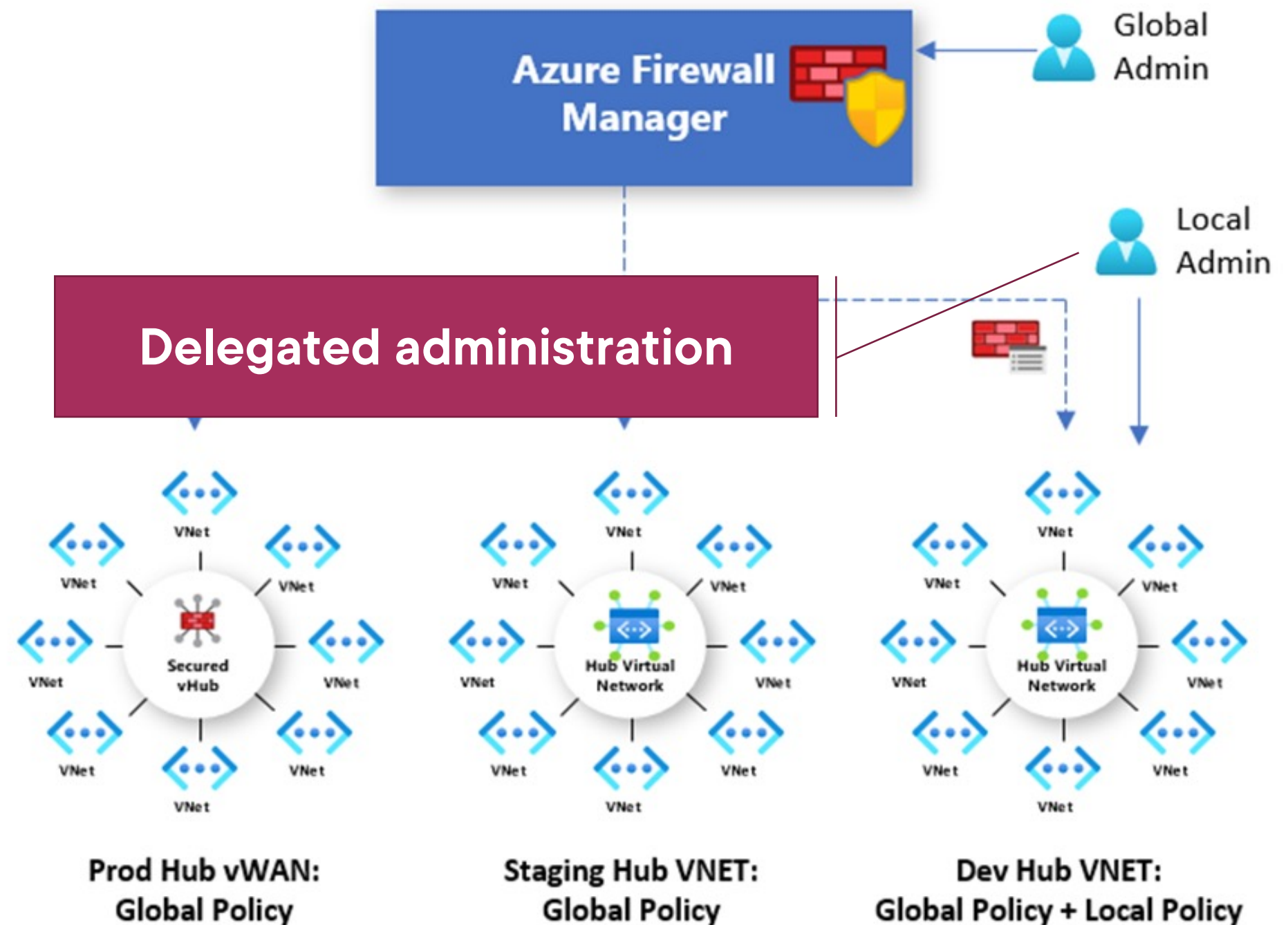
Azure Firewall Policy-Based Rule Processing

Global resource

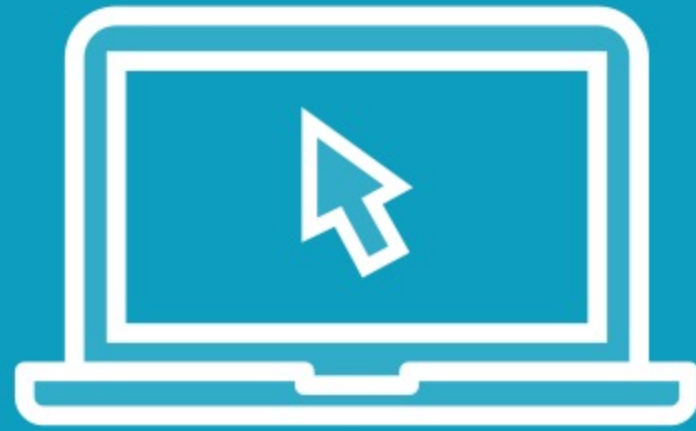
Manage multiple
firewalls

Centralize rule
collections

Deploy threat
Intelligence



Demo



2

Create rulesets

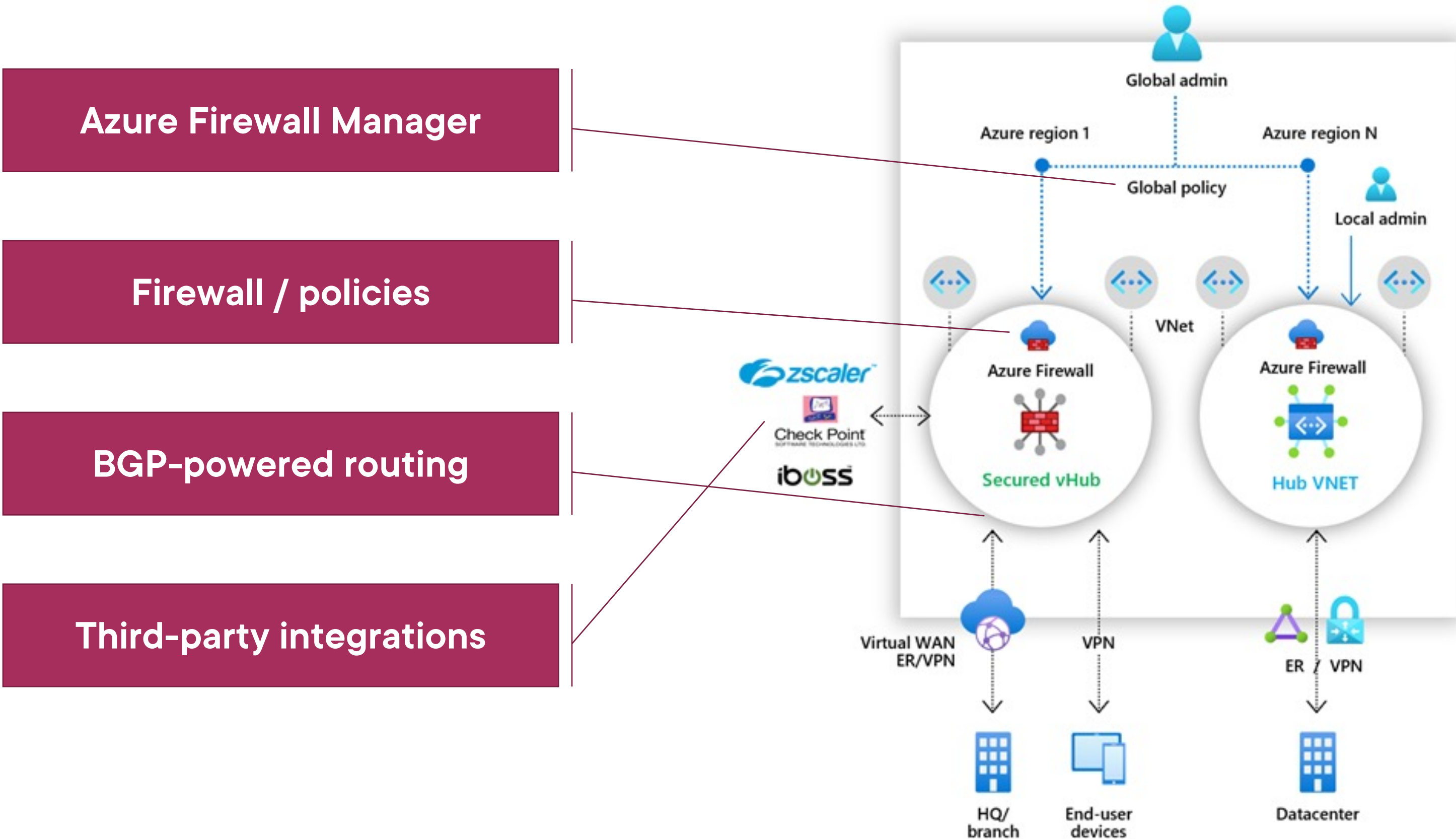
Test precedence/inheritance



Integrate Azure Firewall with Virtual WAN



Secured Virtual Hubs



Secured Virtual Hub Appliance Options

Partners

- Requires S2S VPN tunnels
- AAD service principals and APIs
 - Zscaler
 - iboss Cloud
 - Check Point CloudGuard Connect

Integrated NVA partners

- Managed Application offers in the Azure Marketplace
- Virtual machines or physical servers
 - Barracuda CloudGen WAN
 - Cisco Cloud Service Router VWAN
 - VMware SD-WAN



Summary



Microsoft continues to add functionality to Azure Firewall over the past year or so

- ICSA Labs Certified Corporate Firewall

You can always opt to use a third-party NVA

- The exam is “All Microsoft, all the time”



Up Next:

Implement and Manage Network Security Groups

