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

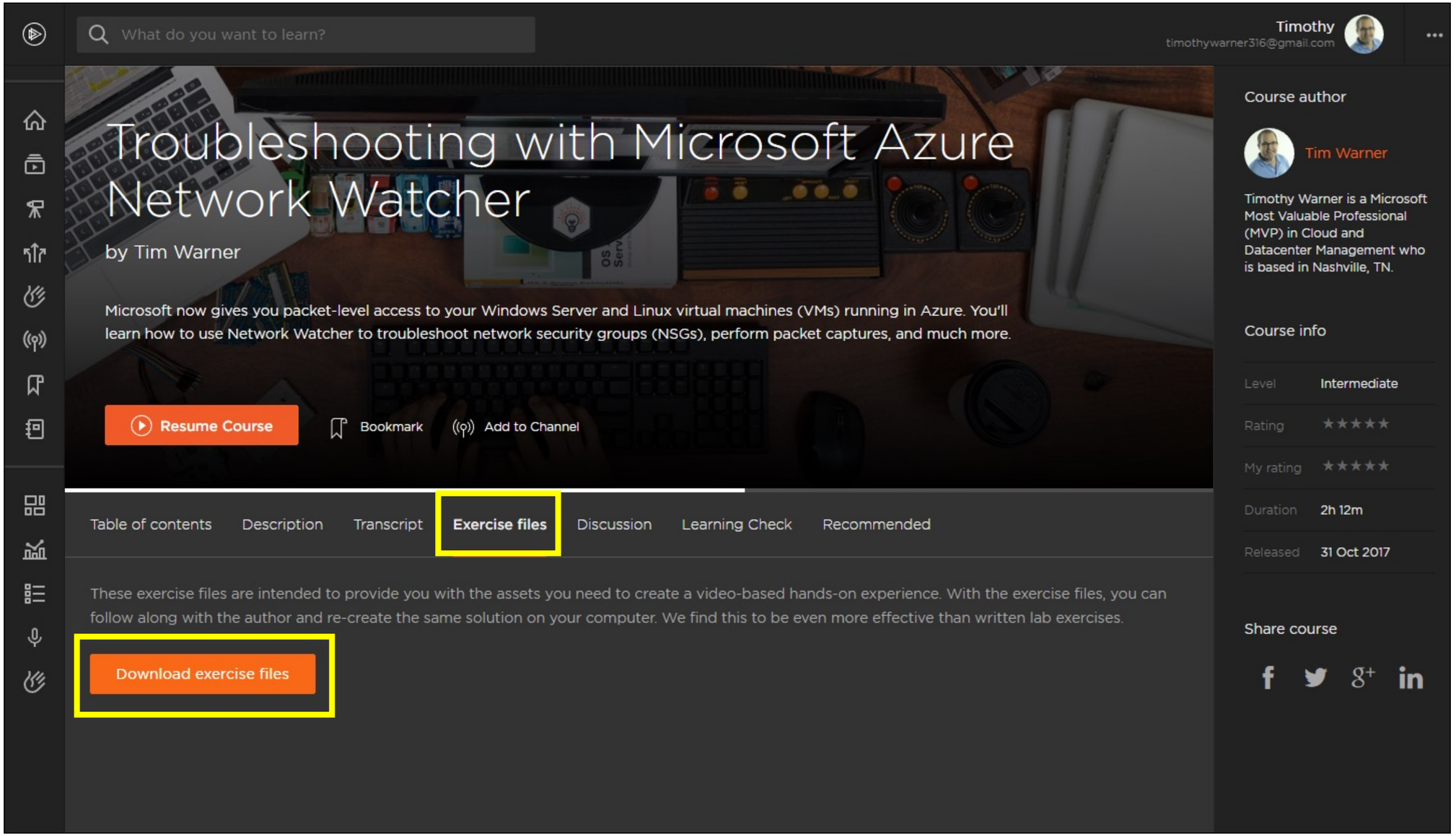
Overview

Design and implement an Azure Firewall deployment

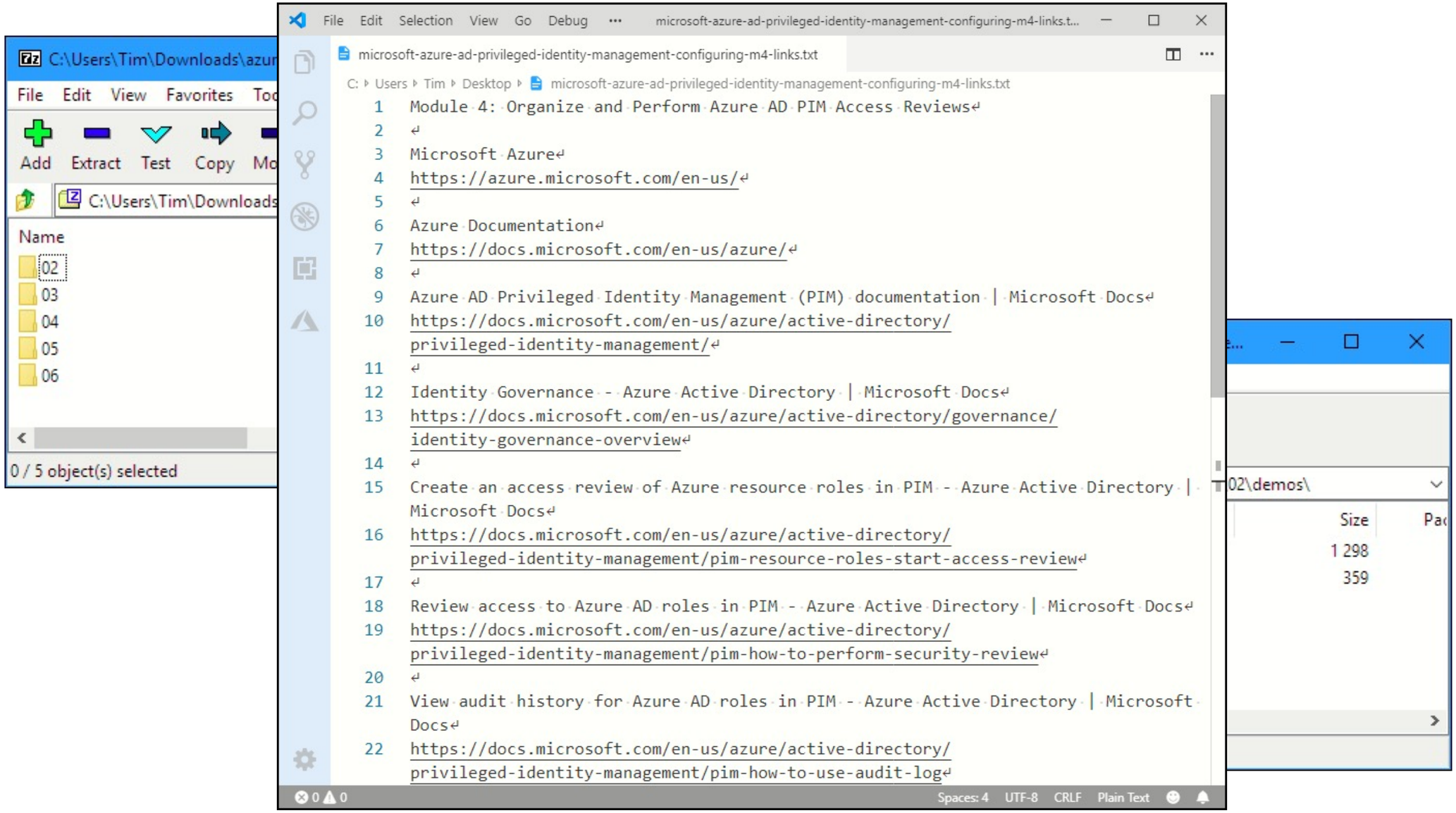
Create and implement Azure Firewall Manager policies and rules

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

Exercise Files



Exercise Files



Exam AZ-700

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

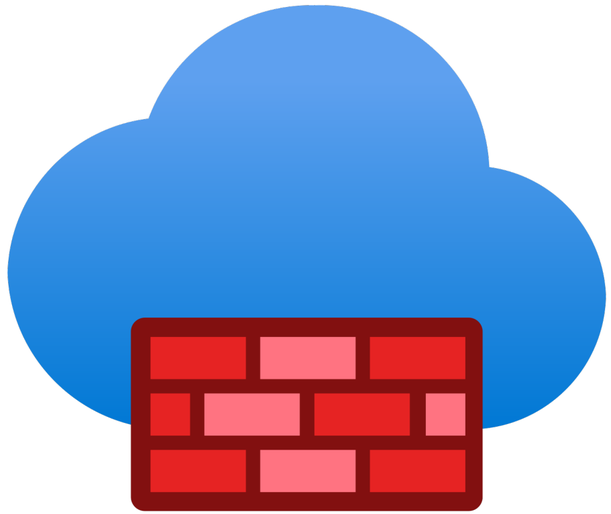
Secure and Monitor Networks (15–20%)

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

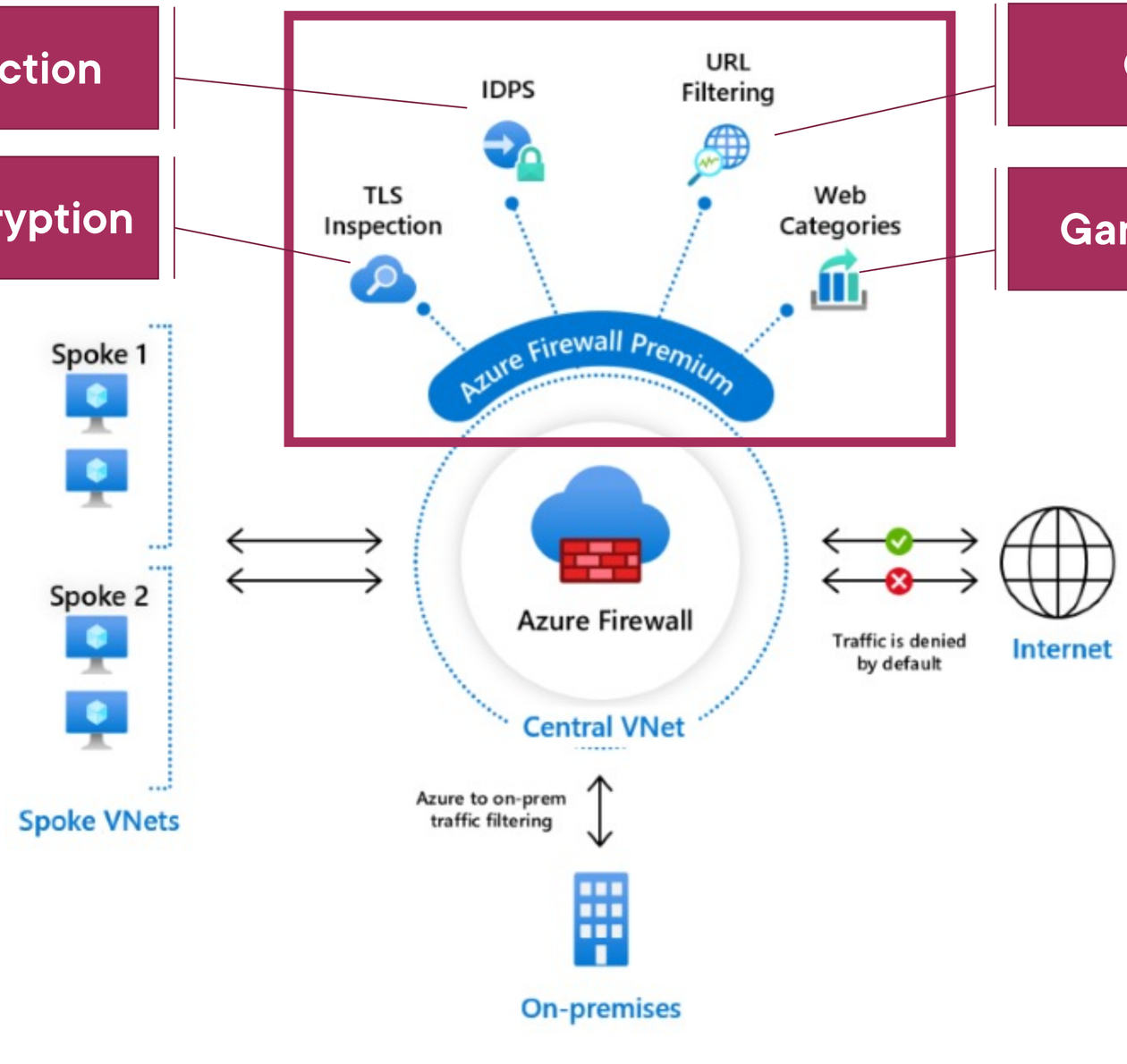


- Managed stateful firewall that works from OSI Layer 3 to Layer 7
- Integration with Microsoft Threat Intelligence
- Centralized policy management
- Availability zone awareness
- SNAT and DNAT support
- Azure Monitor integration

Azure Firewall Premium

Signature-based detection

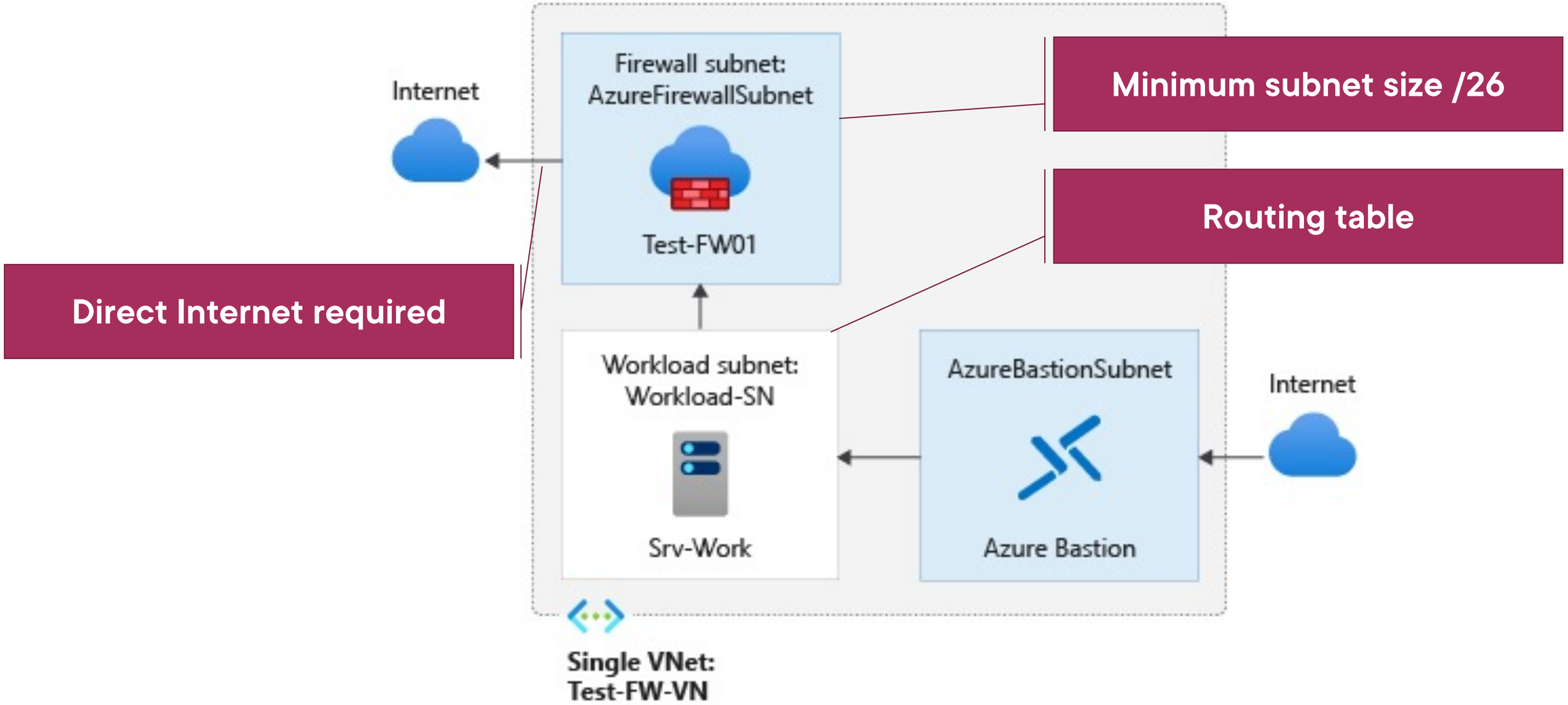
TLS decryption/re-encryption



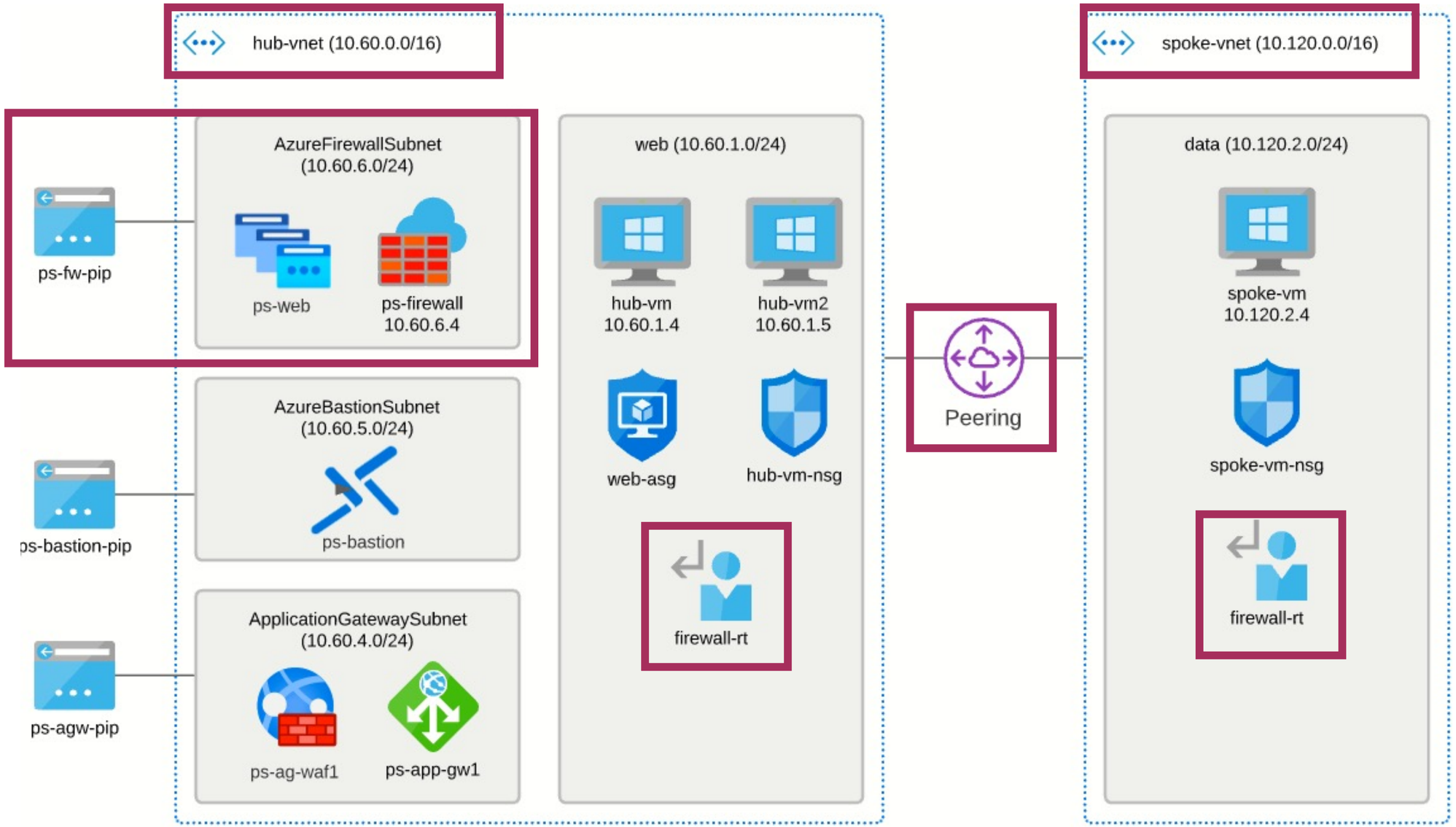
Considers entire URL

Gambling, social media, etc

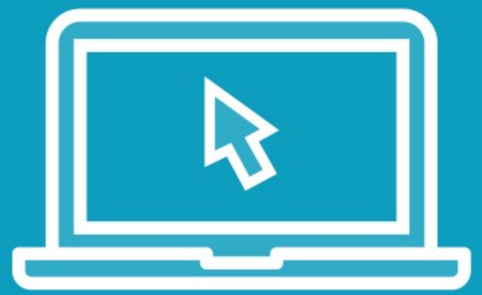
Azure Firewall Deployment Notes



Our Lab Topology



Demo



1

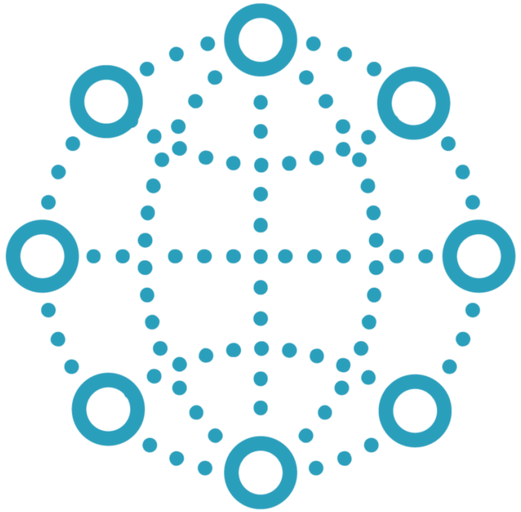
Set up hub-spoke Vnets

Deploy Azure Firewall

Configure routing tables

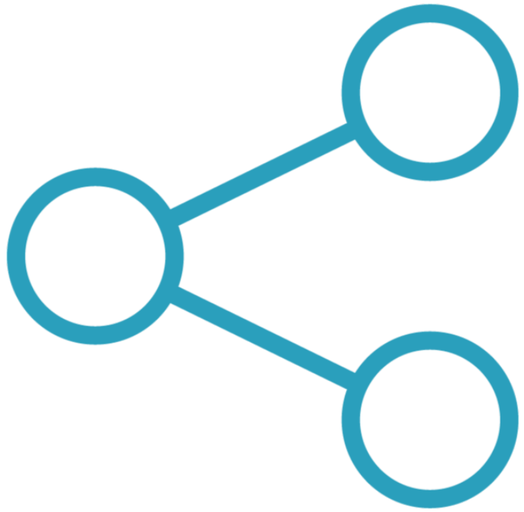
Define Azure Firewall Policies and Rules

Azure Firewall Rule Types



Network
OSI Layer 4
5-tuple match

Application
OSI Layer 7
FQDN match

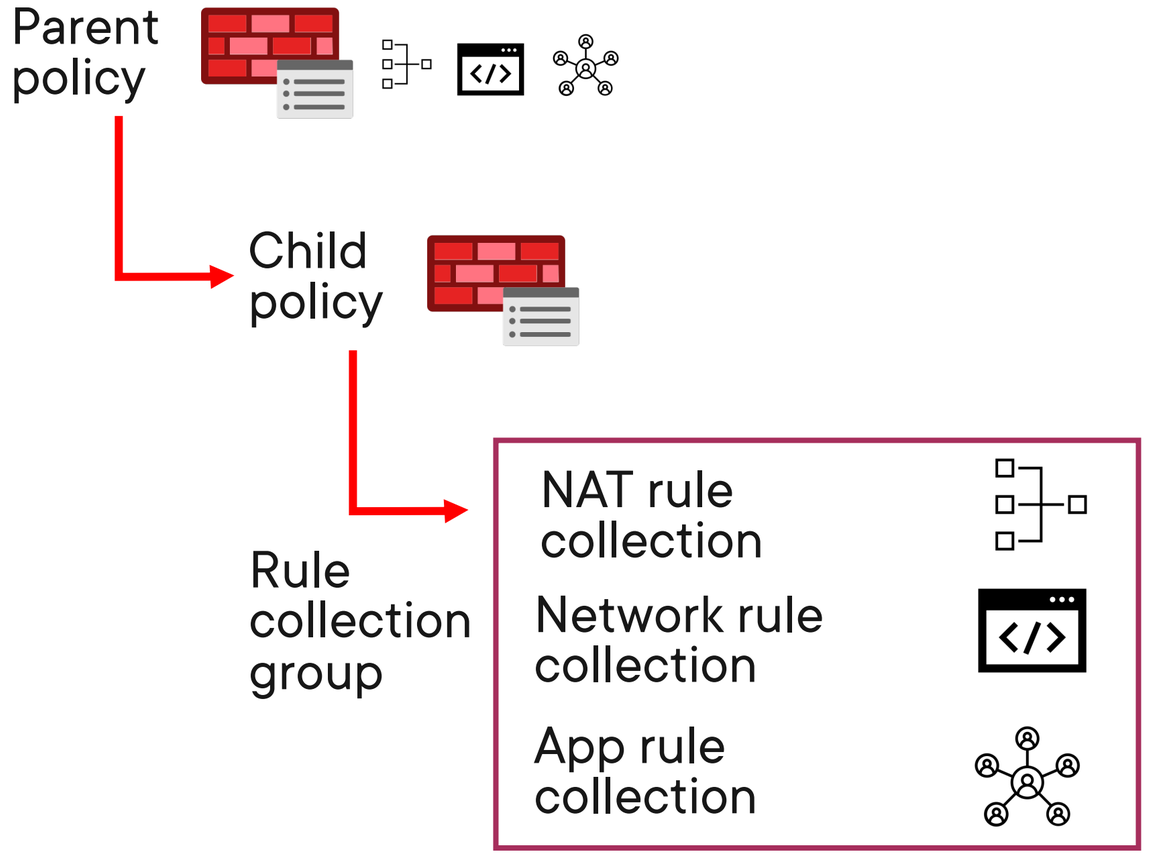


DNAT
OSI Layer 4
Inbound connections

Azure Firewall Policy-Based Rule Processing

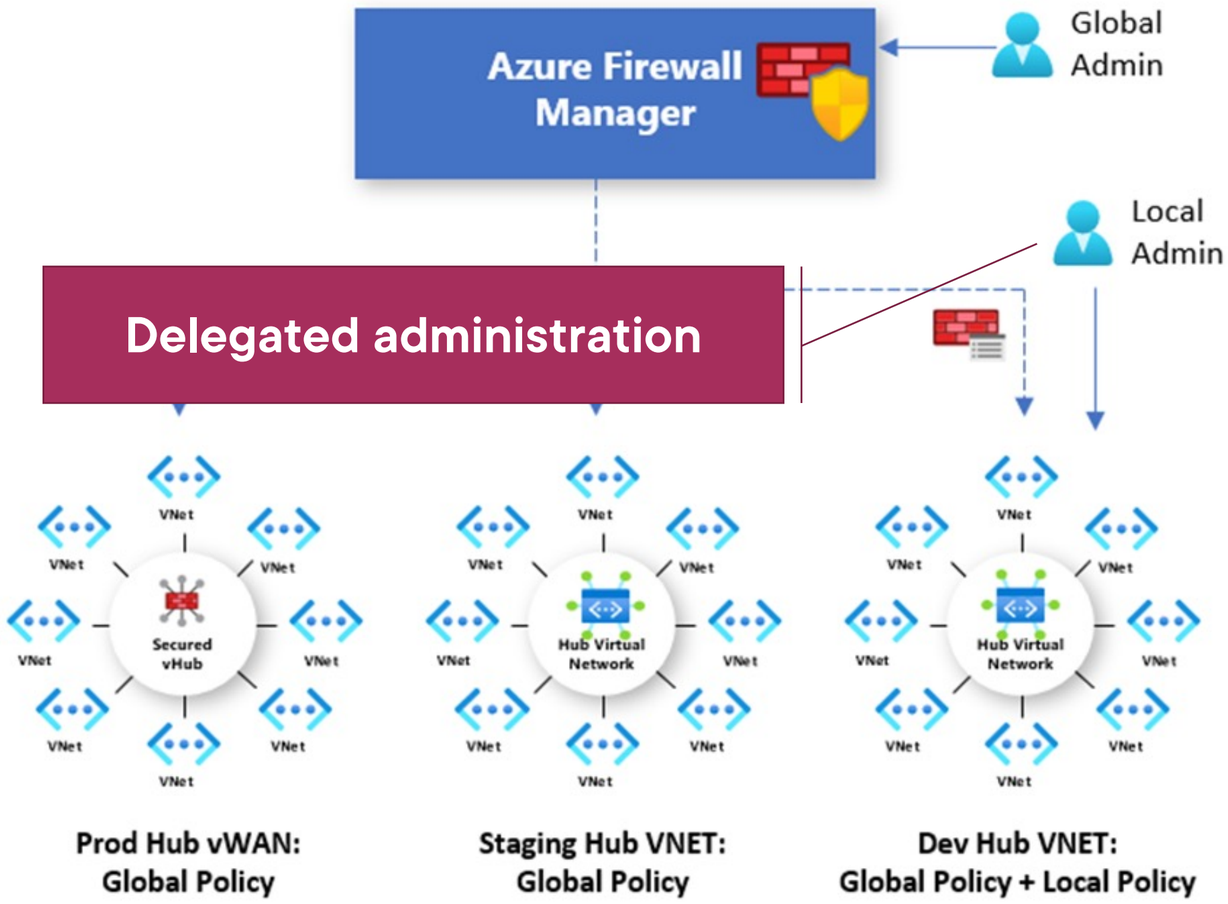
Priority values: 100-65000

Lower numbers are higher priority



Azure Firewall Policy-Based Rule Processing

- **Global resource**
- **Manage multiple firewalls**
- **Centralize rule collections**
- **Deploy threat Intelligence**



Demo

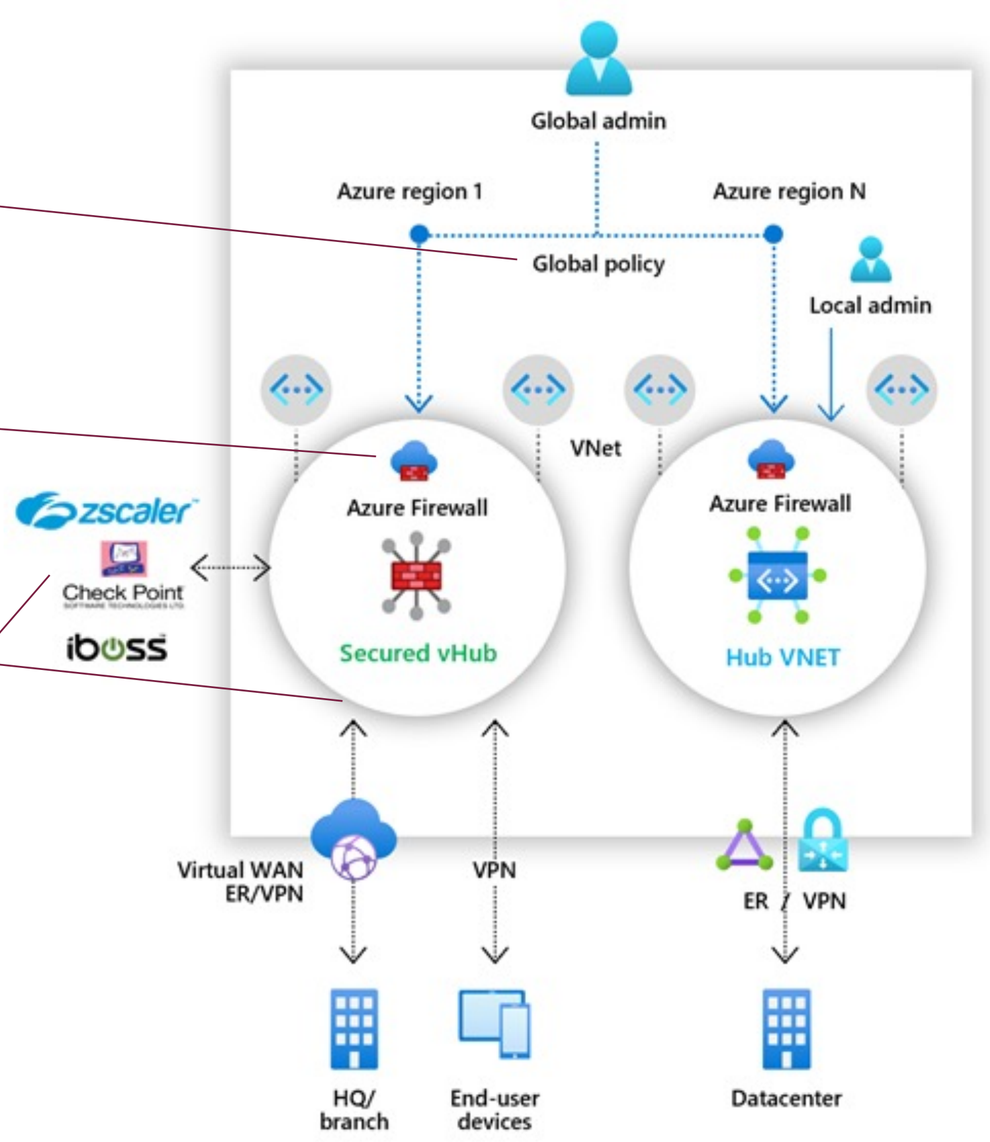
Create rulesets

Test precedence/inheritence

Integrate Azure Firewall with Virtual WAN

Secured Virtual Hubs

- Azure Firewall Manager
- Firewall / policies
- BGP-powered routing
- Third-party integrations



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