Microsoft

AZ-700

Module 06

Design and Implement Network Security

AZ-700 Agenda

Module 01: Introduction to Azure Virtual Networks

Module 02: Designing and Implementing Hybrid Networking

Module 03: Designing and Implementing Azure ExpressRoute

Module 04: Load balance non-HTTP(S) traffic in Azure

Module 05: Load balance HTTP(S) traffic in Azure

Module 06: Design and Implement Network Security

Module 07: Design and Implement private access to Azure Services

Module 08: Design and Implement Network Monitoring

Module Overview

- Get network security recommendations with Microsoft Defender for Cloud

- Deploy Azure DDoS Protection by using the Azure portal

- Deploy and configure Network Security Groups

- Design and implement Azure Bastion

- Design and implement Azure Firewall

- Working with Azure Firewall Manager

- Implement a Web Application Firewall

- Exercise – Configure DDoS Protection on a virtual network

- Exercise – Deploy and configure Azure Firewall using the Azure portal

- Exercise – Secure your virtual hub using Azure Firewall Manager

Get network security recommendations with Microsoft Defender for Cloud

Network Security Controls

NS-1: Establish network segmentation boundaries

NS-2: Secure cloud services with network controls

NS-3: Deploy firewall at the edge of enterprise network

NS-4: Deploy intrusion detection/intrusion prevention systems (IDS/IPS)

NS-5: Deploy DDOS protection

NS-6: Deploy web application firewall

NS-7: Simplify network security configuration

NS-8: Detect and disable insecure services and protocols

NS-9: Connect on-premises or cloud network privately

NS-10: Ensure Domain Name System (DNS) security

Microsoft cloud security benchmark

The Microsoft cloud security benchmark (MCSB) includes a collection of high-impact security recommendations you can use to help secure your cloud services in a single or multi-cloud environment

Security controls: These recommendations are generally applicable across your cloud workloads. Each recommendation identifies a list of stakeholders that are typically involved in planning, approval, or implementation of the benchmark.

Service baselines: These apply the controls to individual cloud services to provide recommendations on that service's security configuration.

Term	Description	Example
Control	A control is a high-level description of a feature or activity that needs to be addressed and is not specific to a technology or implementation.	Data Protection is one of the security controls. This control contains specific actions that must be addressed to help ensure data is protected.
Baseline	A baseline is the implementation of the control on the individual Azure services. Each organization dictates a benchmark recommendation and corresponding configurations are needed in Azure. Note: Today we have service baselines available only for Azure.	The Contoso company looks to enable Azure SQL security features by following the configuration recommended in the Azure SQL security baseline.

Using Microsoft Defender for Cloud for regulatory compliance

Microsoft Defender for Cloud helps streamline the process for meeting regulatory compliance requirements, using the regulatory compliance dashboard.
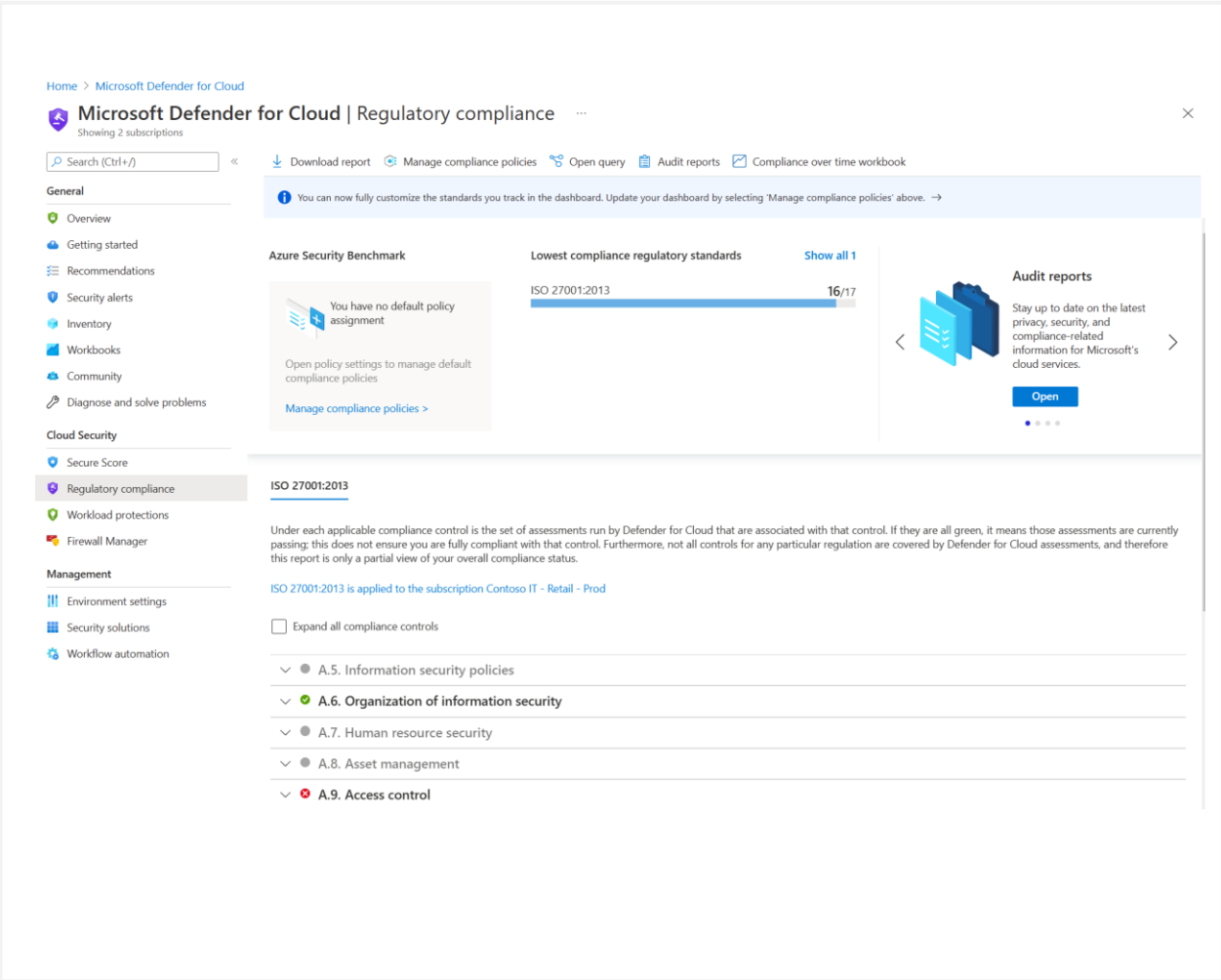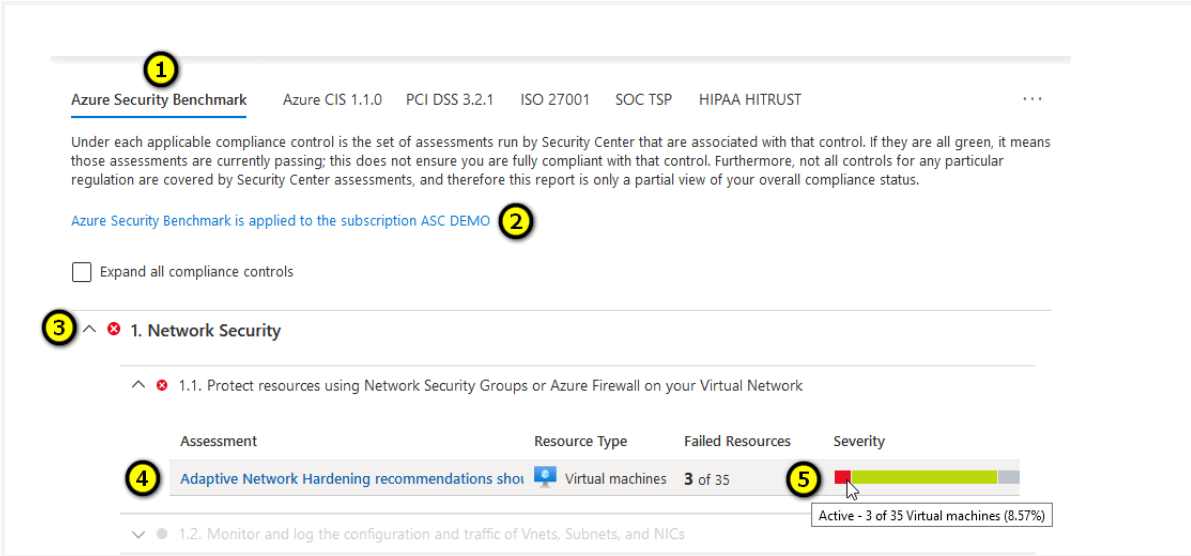
Alerts in Microsoft Defender for Cloud
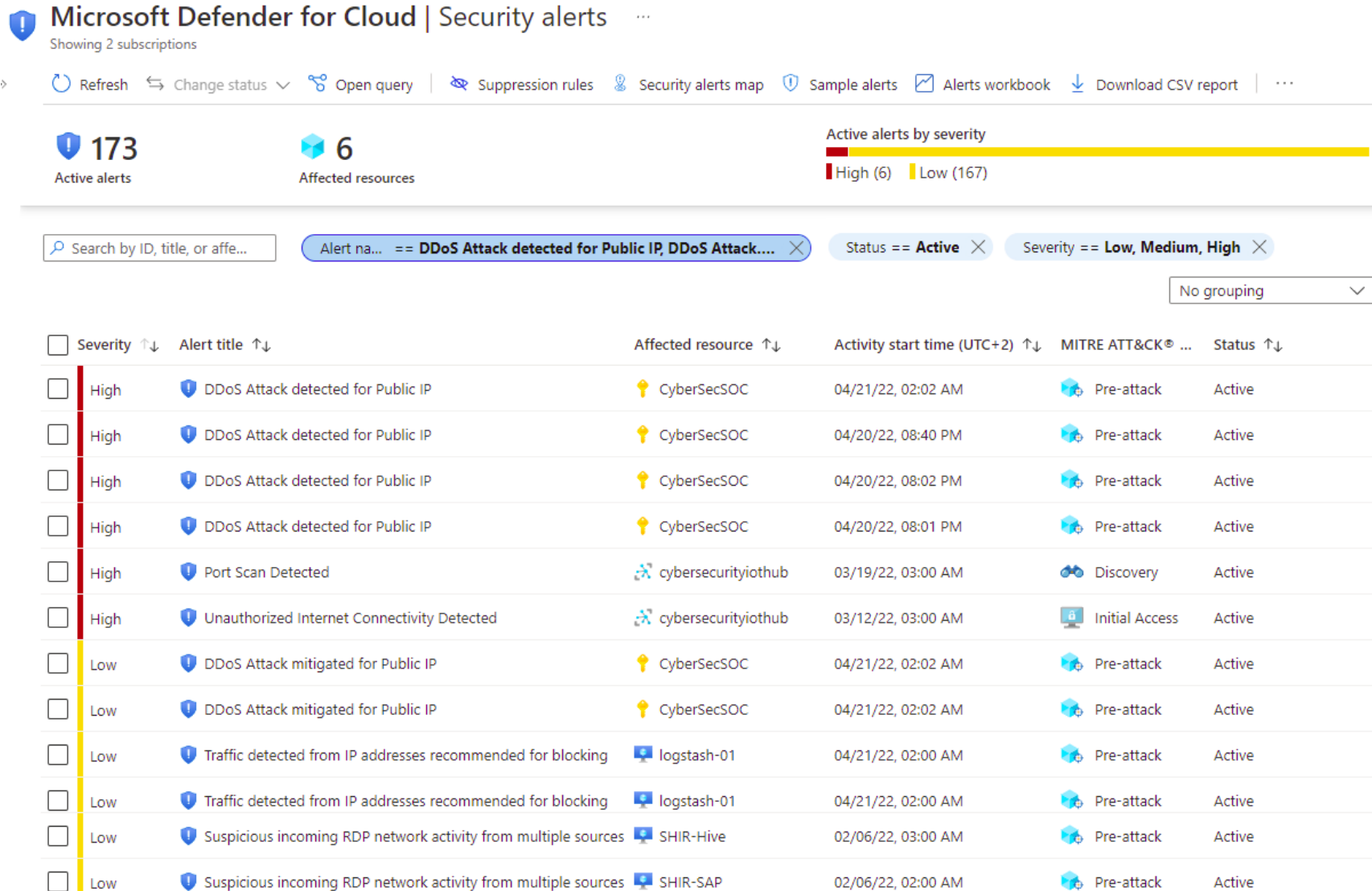
# Deploy Azure DDoS Protection by using the Azure portal

Distributed Denial of Service (DDoS)

The goal of a DoS (Denial of Service) attack is to prevent access to services or systems.

Botnets are collections of internet-connected systems that an individual controls and uses without their owners' knowledge

DDoS is a collection of attack types aimed at disrupting the availability of a target

DDoS involves many systems sending traffic to targets as part of a botnet

Bot

Bot

Target

Bot

Bot

Bot
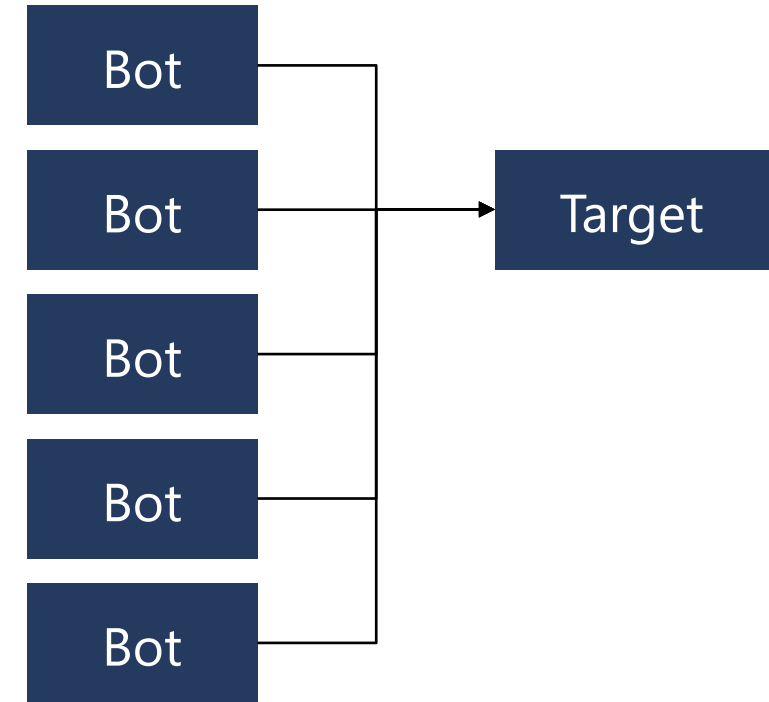
Types of DDoS attacks

Volumetric attacks
These attacks flood the network layer with a substantial amount of seemingly legitimate traffic. They include UDP floods, amplification floods, and other spoofed-packet floods. DDoS Protection Standard mitigates these potential multi-gigabyte attacks by absorbing and scrubbing them, with Azure's global network scale, automatically.

Protocol attacks
These attacks render a target inaccessible, by exploiting a weakness in the layer 3 and layer 4 protocol stack. They include SYN flood attacks, reflection attacks, and other protocol attacks. DDoS Protection Standard mitigates these attacks, differentiating between malicious and legitimate traffic, by interacting with the client, and blocking malicious traffic.

Resource (application) layer attacks
These attacks target web application packets, to disrupt the transmission of data between hosts. They include HTTP protocol violations, SQL injection, cross-site scripting, and other layer 7 attacks. Use a Web Application Firewall, such as the Azure Application Gateway web application firewall, as well as DDoS Protection Standard to provide defense against these attacks. There are also third-party web application firewall offerings available in the Azure Marketplace.

Azure DDoS protection tiers

DDoS Network Protection
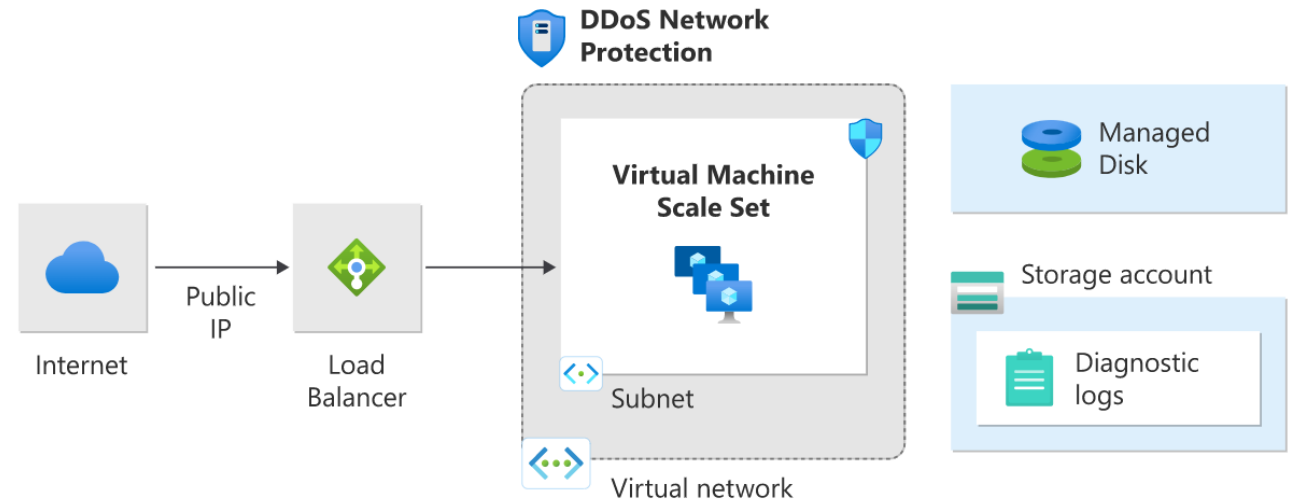
DDoS IP Protection
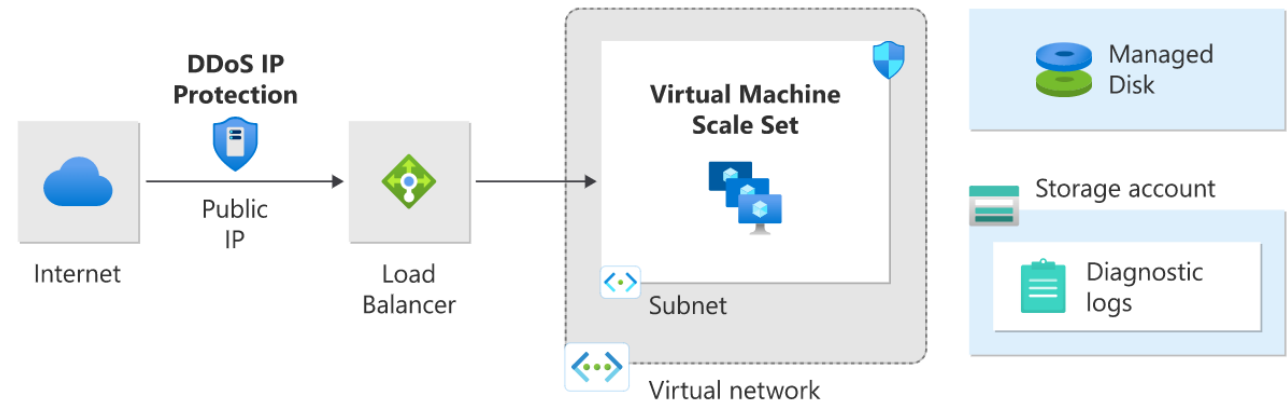
Azure DDoS protection features

- Always-on traffic monitoring

- Adaptive real time tuning

- DDoS Protection analytics, metrics, and alerting

- Azure DDoS Rapid Response

- Turnkey protection

- Multi-Layered protection

- Extensive mitigation scale

Deploying a DDoS protection plan

Create a DDoS protection plan

Enable DDoS protection on a new or existing VNet

Configure DDoS telemetry

Configure DDoS diagnostic logs and alerts

Run a test DDoS attack and monitor the results

Deploy and configure Network Security Groups

Network Security Groups

nsg0
Network security group | ℹ️ Directory: Microsoft

🔍 Search (Ctrl+/) «

→ Move   🗑️ Delete   ↻ Refresh

🛡️ Overview

📘 Activity log

👥 Access control (IAM)

🟣 Tags

🔧 Diagnose and solve problems

Resource group (change) : rg01

Location : East US

Subscription (change) :

Subscription ID :

Tags (change) : Click here to add tags

Custom security rules : 1 inbound, 0 outbound

Associated with : 1 subnets, 0 network interfaces

| Limits network traffic to resources in a virtual network | Lists the security rules that allow or deny inbound or outbound network traffic | Associated to a subnet or a network interface | Can be associated multiple times |

NSG Rules

Inbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
100	⚠ RDP_Inbound	3389	Any	Any	Any	✅ Allow
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

Security rules in NSGs enable you to filter network traffic that can flow in and out of virtual network subnets and network interfaces

There are default security rules. You cannot delete the default rules, but you can add other rules with a higher priority
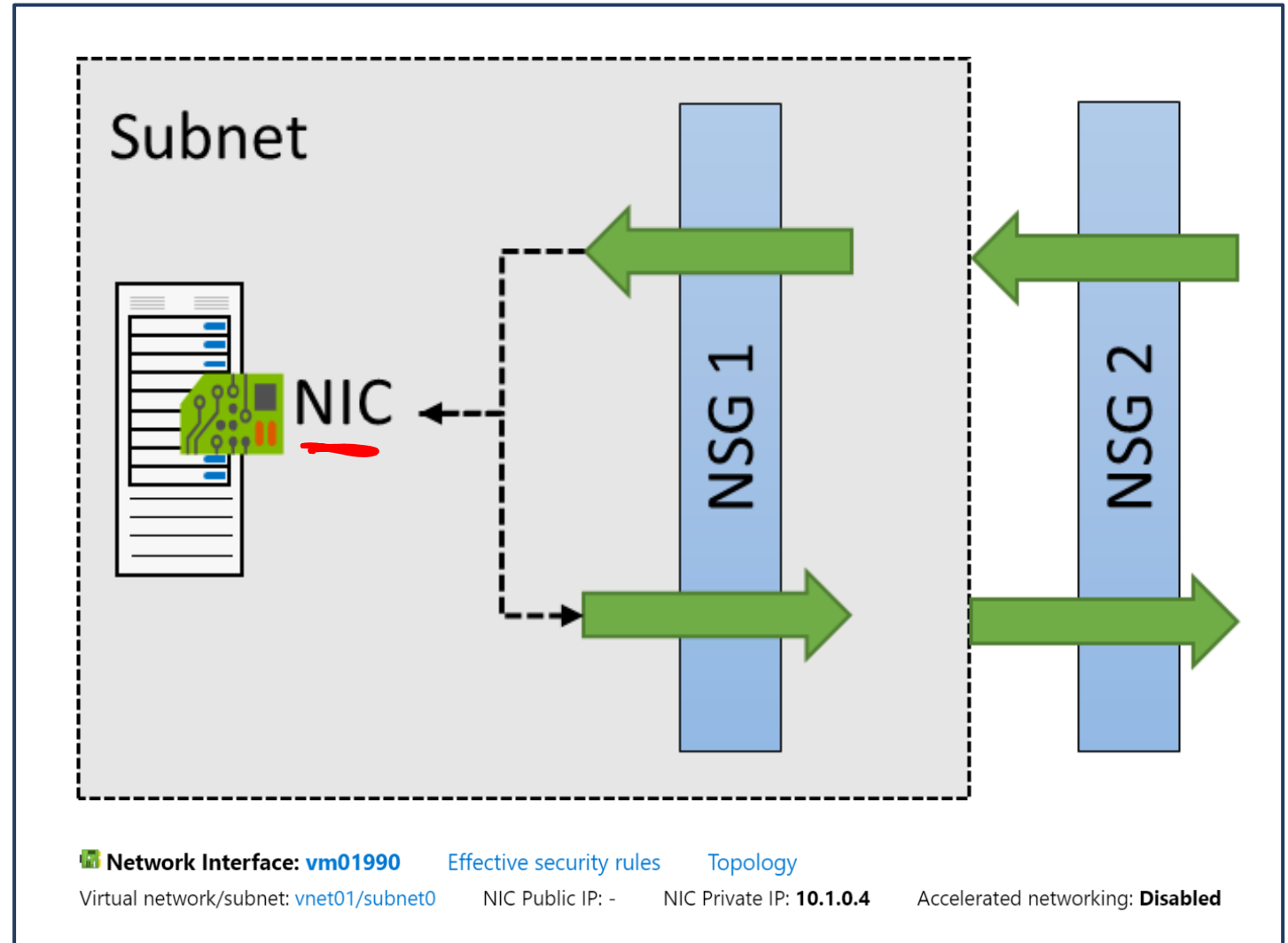
NSG Effective Rules

NSGs are evaluated independently for the subnet and NIC

An "allow" rule must exist at both levels for traffic to be admitted

Use the Effective Rules link if you are not sure which security rules are being applied
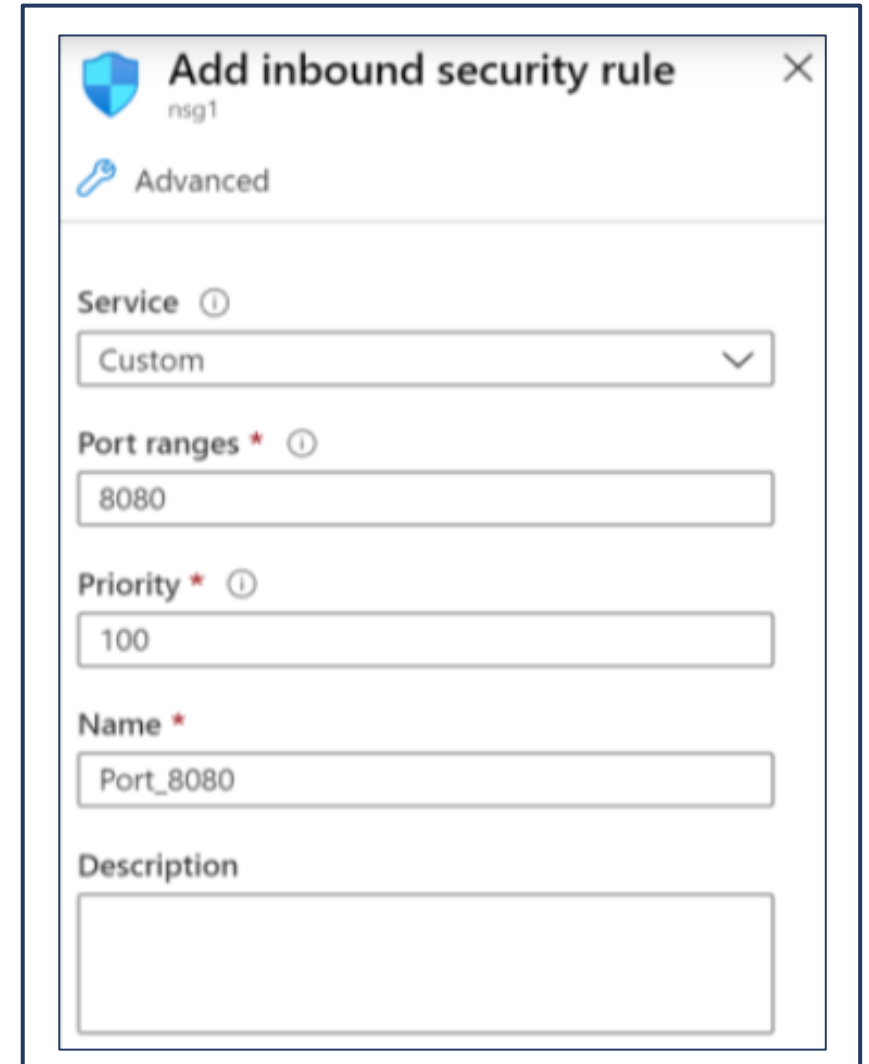

Subnet

Subnet

NIC

NSG 1

NSG 2

Network Interface: vm01990   Effective security rules   Topology
Virtual network/subnet: vnet01/subnet0   NIC Public IP: -   NIC Private IP: **10.1.0.4**   Accelerated networking: **Disabled**

Creating NSG rules

Select from a large variety of services

Service – The destination protocol and port range for this rule

Port ranges – Single port or multiple ports

Priority – The lower the number, the higher the priority

Add inbound security rule
nsg1

Advanced

Service ⓘ

Custom

Port ranges * ⓘ

8080

Priority * ⓘ

100

Name *

Port_8080

Description

Use Service Tags to define network access controls

© Copyright Microsoft Corporation. All rights reserved.
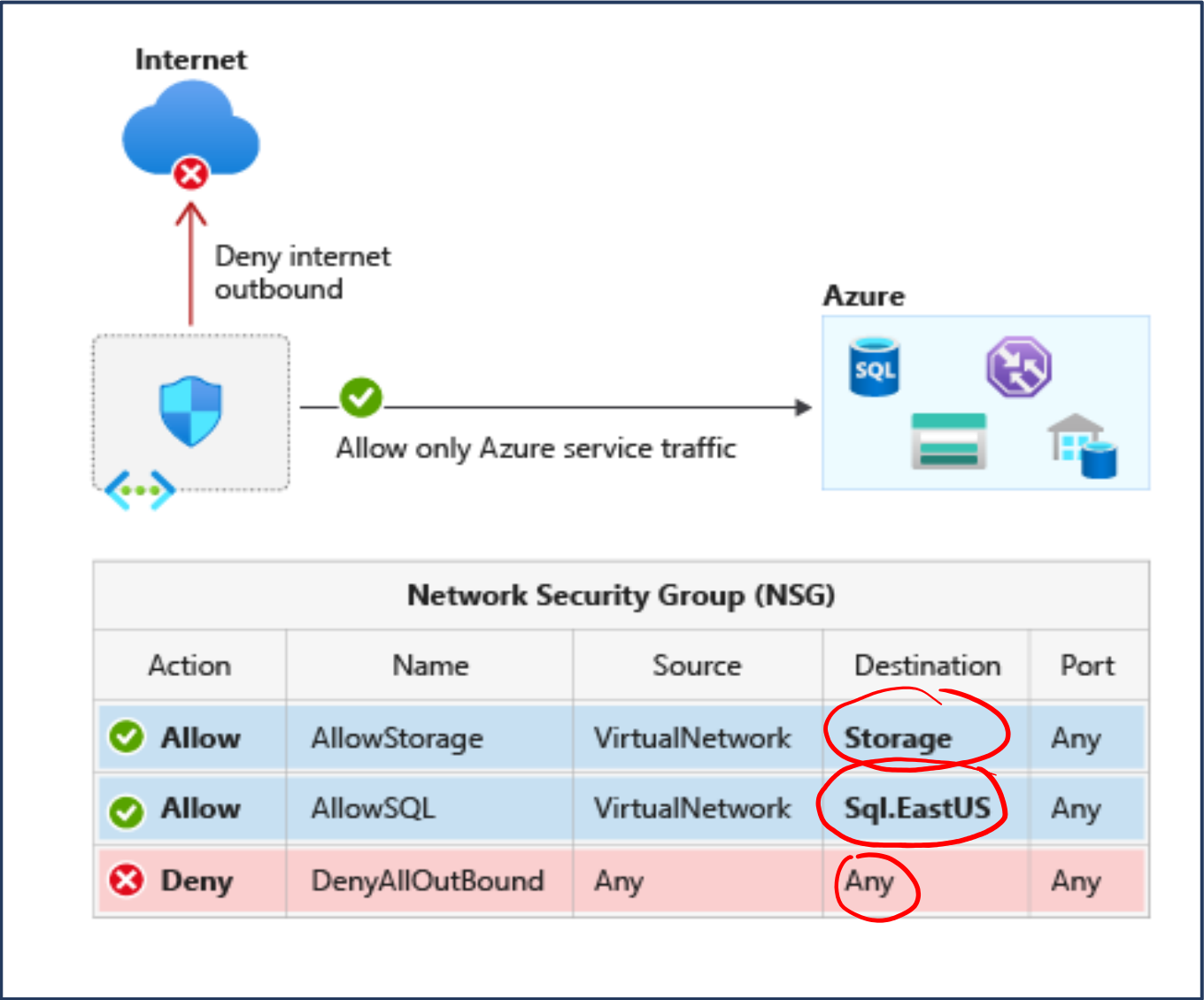
Application Security Groups (ASG)

Configure ASG as a natural extension of an application's structure

ASG can be the source and destination in a security rule

All NIC assigned to an ASG must exist in the same virtual network that the first NIC assigned to the ASG is in
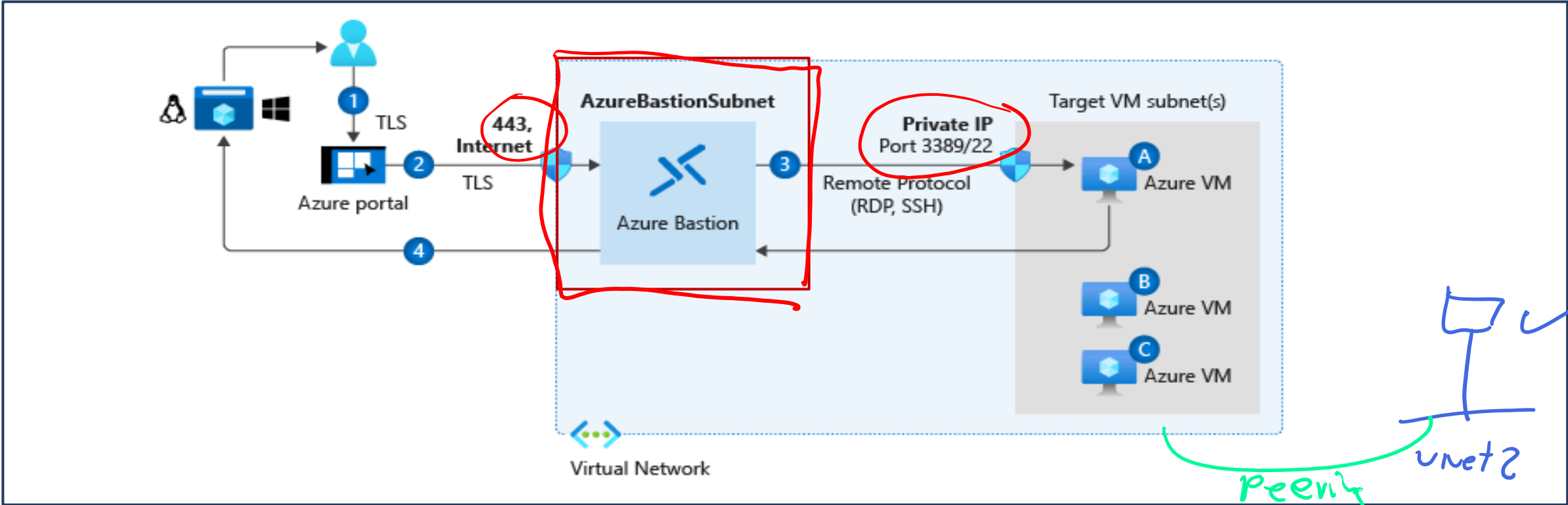
If you specify an ASG as the source and destination in a security rule, the NIC in both ASG must exist in the same virtual network
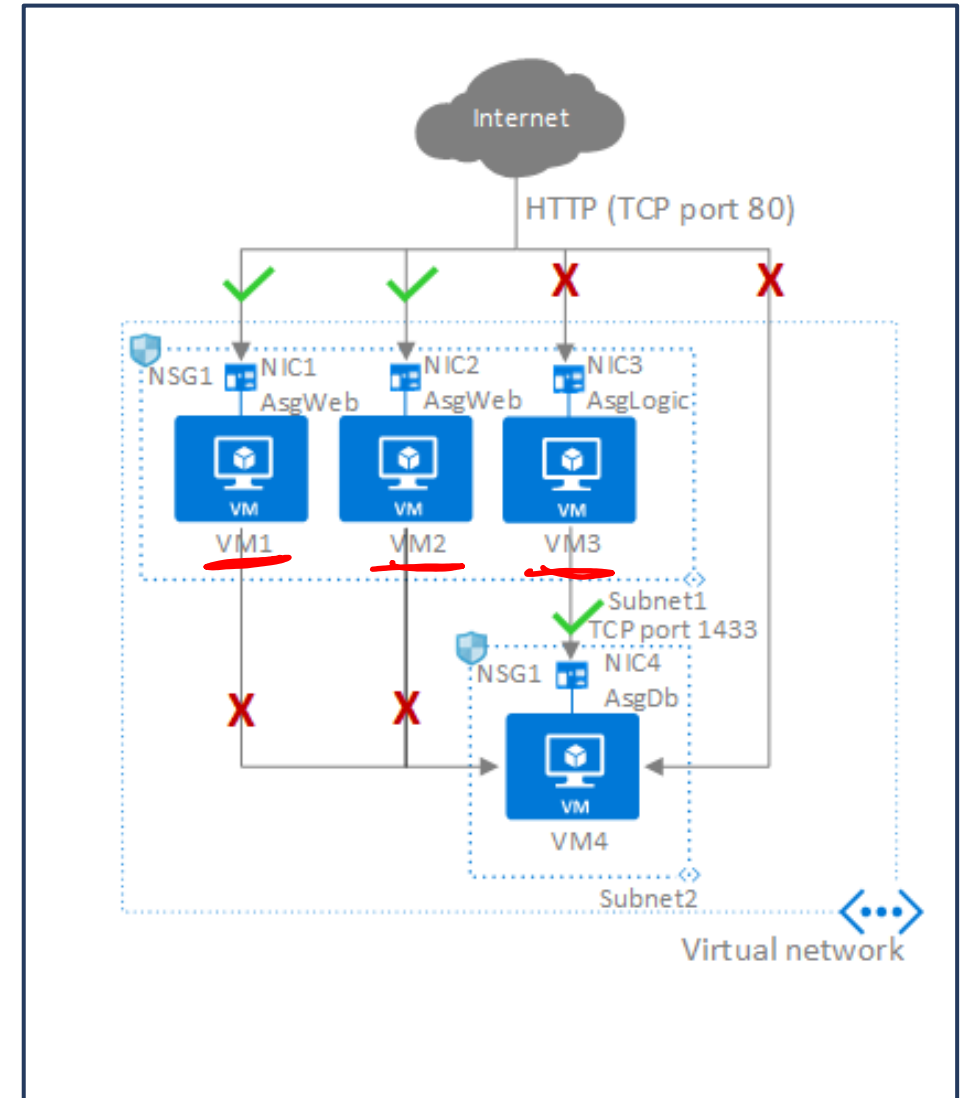
Design and implement Azure Bastion

Connect to Virtual Machines

Bastion Subnet for RDP/SSH through the Portal over SSL	Remote Desktop Protocol for Windows-based Virtual Machines	Secure Shell Protocol for Linux based Virtual Machines

Design and implement Azure Firewall

Azure Firewall features
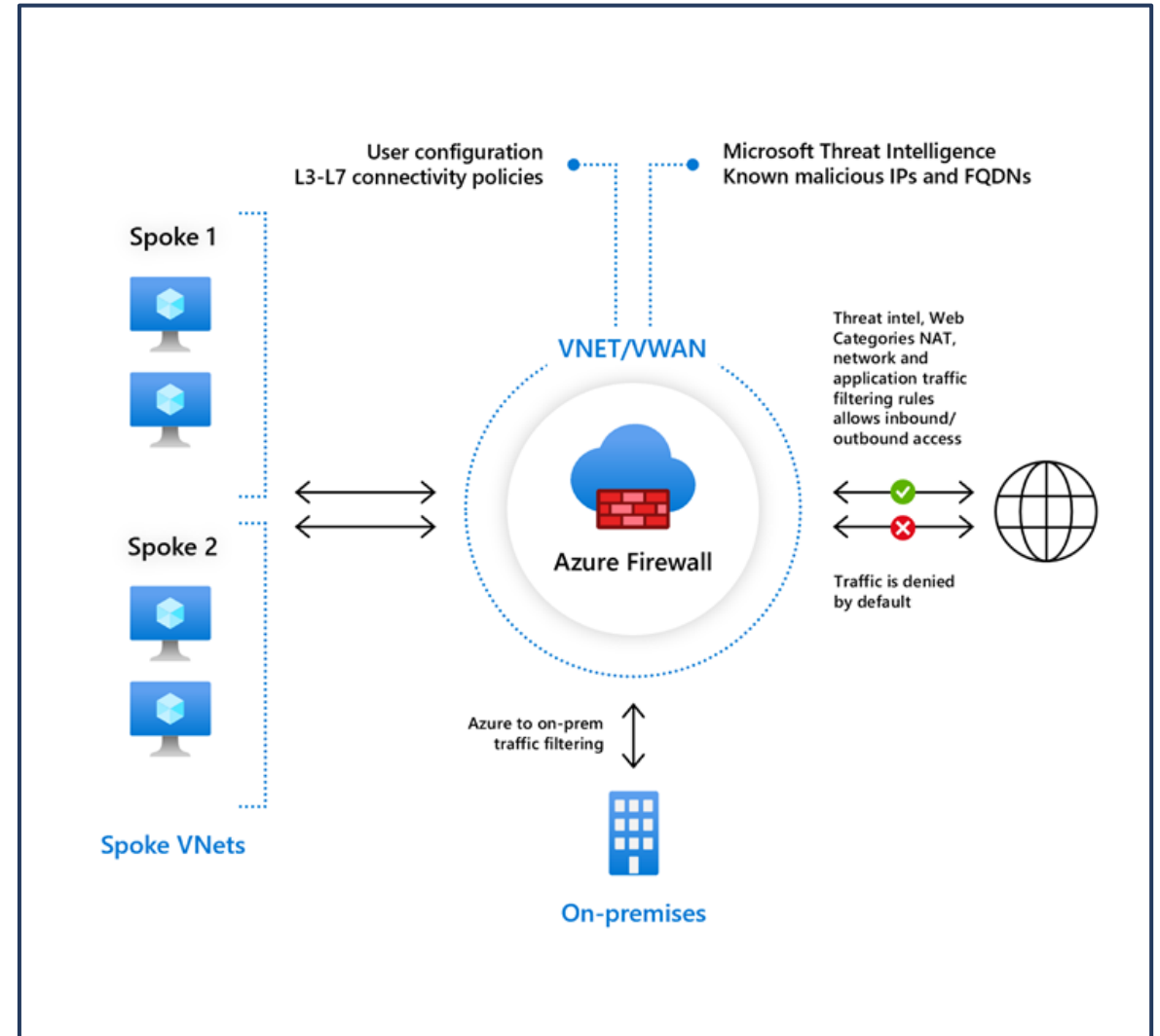
Stateful firewall as a service

Built-in high availability with unrestricted cloud scalability

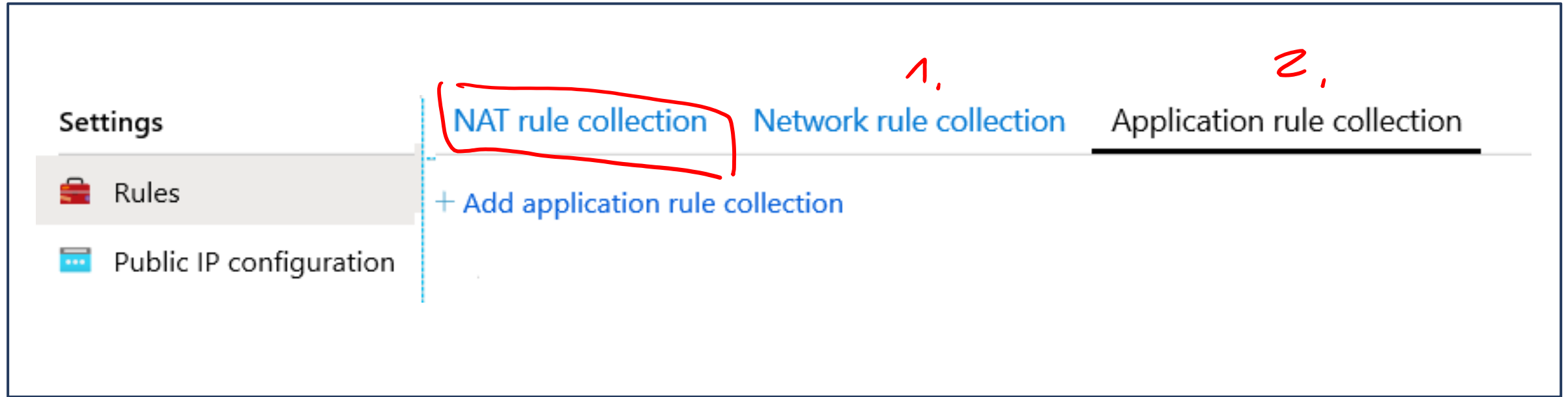Create, enforce, and log application and network connectivity policies

Threat intelligence-based filtering for L3-L7

Fully integrated with Azure Monitor for logging and analytics

Support for hybrid connectivity through deployment behind VPN and ExpressRoute Gateways

Rule processing in Azure Firewall

Settings	NAT rule collection	Network rule collection	Application rule collection
📦 Rules	+ Add application rule collection		
🖥️ Public IP configuration			

NAT rules. Configure DNAT rules to allow incoming connections

Network rules. Configure rules that contain source addresses, protocols, destination ports, and destination addresses

Application rules. Configure fully qualified domain names (FQDNs) that can be accessed from a subnet

Deploying Azure Firewall in the Azure portal

On the Create a Firewall page enter the following:

Subscription

Resource Group

Instance Name, region and Availability Zone if any

Firewall tier

Firewall management

Firewall Policy

Choose a virtual network

Forced tunneling

Basics   Tags   Review + create

Azure Firewall is a managed cloud-based network security service that protects your Azure Virtual Network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network. The service is fully integrated with Azure Monitor for logging and analytics. Learn more.

Project details

Subscription * | Contoso IT - Retail - Prod ▾ |

    Resource group * | ▾ |
                        Create new

Instance details

Name * | |

Region * | West US 2   ▾ |

Availability zone ⓘ | None   ▾ |

ℹ Premium firewalls support additional capabilities, such as SSL termination and IDPS. Additional costs may apply. Migrating a Standard firewall to Premium will require some down-time. Learn more

Firewall tier   ◉ Standard
                        ○ Premium (preview)

Firewall management   ◉ Use a Firewall Policy to manage this firewall
                        ○ Use Firewall rules (classic) to manage this firewall

Firewall policy * | Select   ▾ |
                        Add new

Choose a virtual network ◉ Create new
                        ○ Use existing

Virtual network name * | |

Address space * | 10.0.0.0/16 |
                                              (0 addresses)

Subnet   AzureFirewallSubnet

Subnet address space * | 10.0.0.0/24 |
                                              (0 addresses)

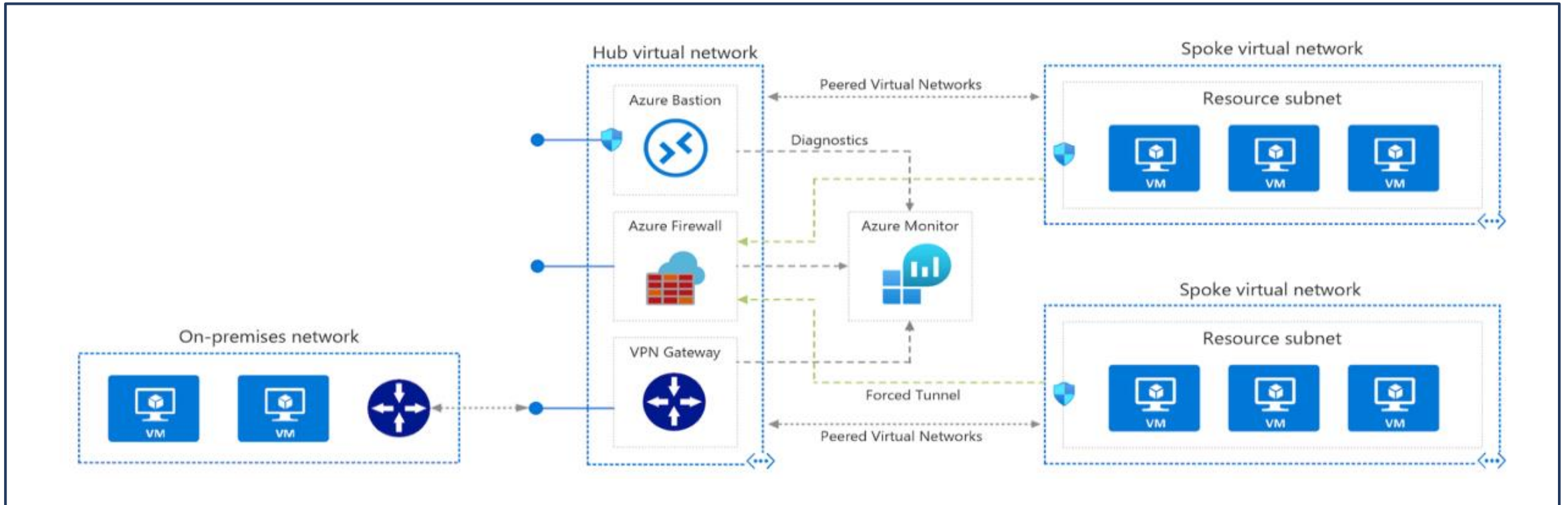Public IP address * | Choose public IP address   ▾ |
                        Add new
                        ⊗ The value must not be empty.

Forced tunneling ⓘ   ◯━ Disabled

Deploying Azure Firewall in a Hub-Spoke network topology

A Hub-Spoke network topology is recommended

Shared services are placed in the hub virtual network

Each environment is deployed to a spoke to maintain isolation

Compare Azure Firewall to NSGs

	NSG	Azure Firewall
Protocol based traffic filtering	Yes	Yes
Support Service Tags	Yes	Yes
Support Application FQDN Tags	No	Yes
Integrated with Azure Monitor for diagnostic logging	Yes	Yes
SNAT and DNAT support	No	Yes

Inspection

Working with Azure Firewall Manager

Azure Firewall Manager features

Central Azure Firewall deployment and configuration

Hierarchical policies (global and local)

Integrated with third-party security-as-a-service for advanced security

Centralized route management

Region availability
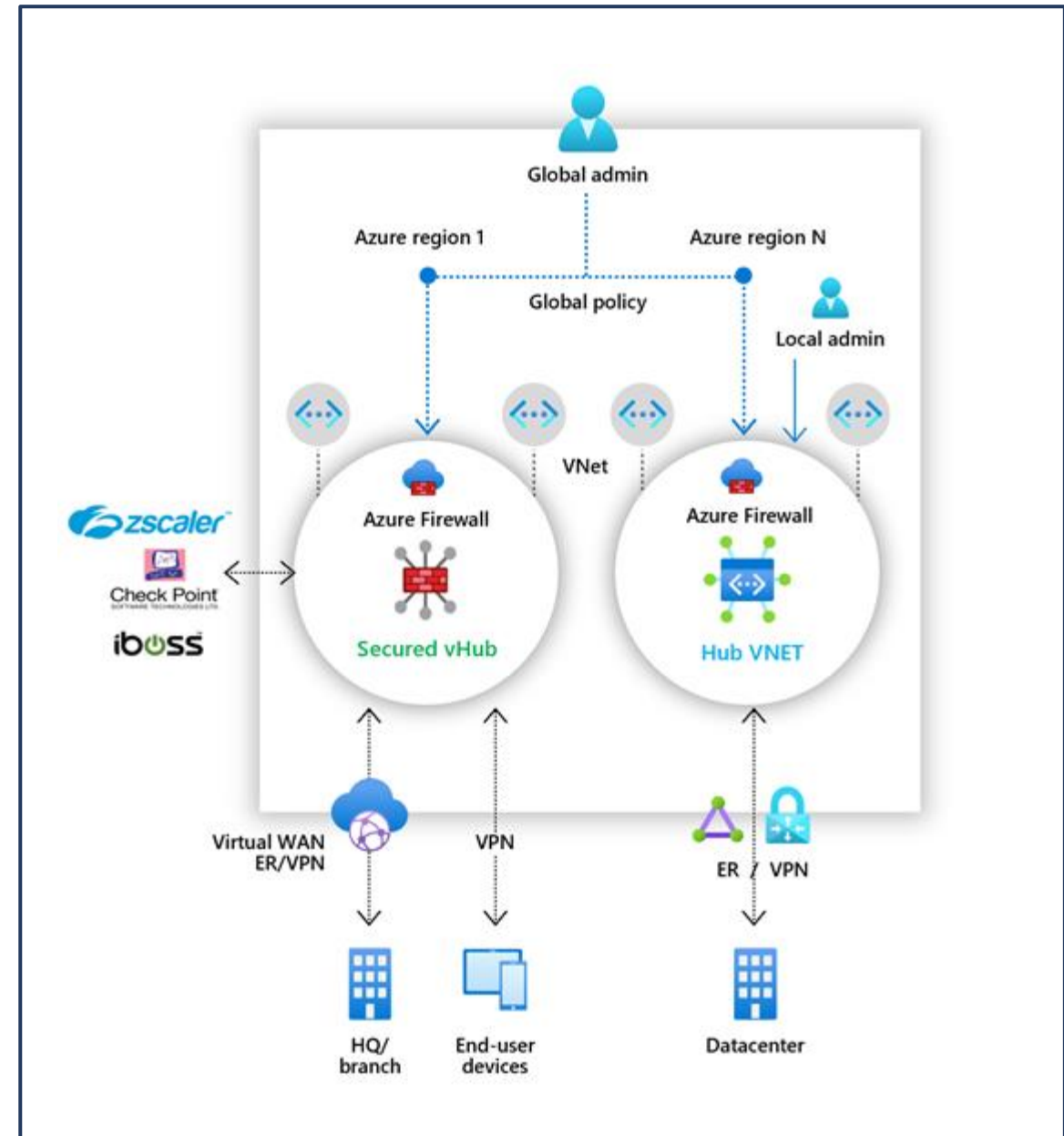
Azure Firewall Manager policies

A policy can be created and managed in multiple ways, including the Azure portal, REST API, templates, Azure PowerShell, and CLI.

Policies can be associated with one or more virtual hubs or VNets. The firewall can be in any subscription associated with your account and in any region.
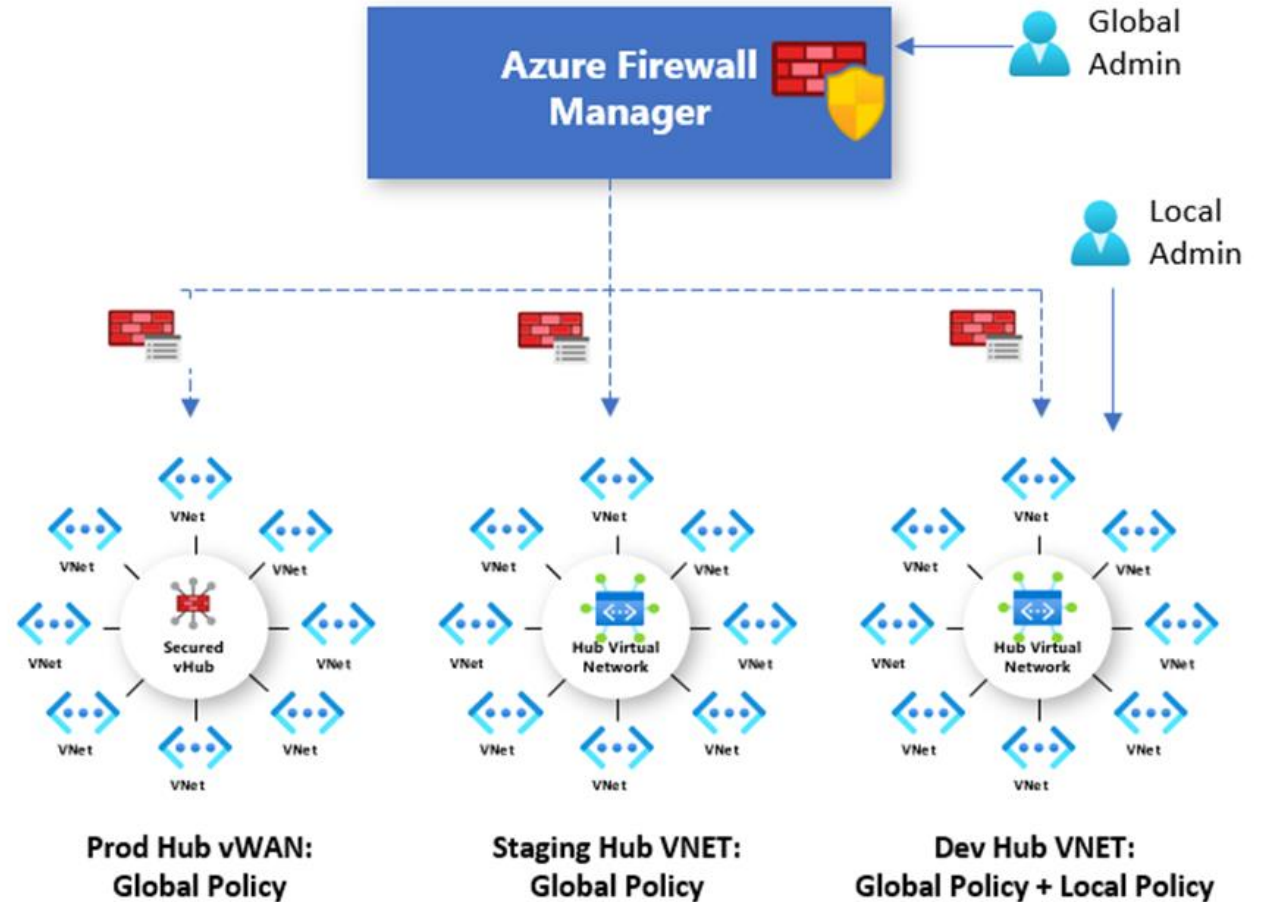
Prod Hub vWAN:
Global Policy

Staging Hub VNET:
Global Policy

Dev Hub VNET:
Global Policy + Local Policy

Azure Firewall Manager for Hub Virtual Networks vs Secured Virtual

	Hub virtual network	Secured virtual hub
Underlying resource	Virtual network	Virtual WAN Hub
Hub & Spoke	Uses Virtual network peering	Automated using hub virtual network connection
On-prem connectivity	VPN Gateway up to 10 Gbps and 30 S2S connections; ExpressRoute	More scalable VPN Gateway up 20 Gbps and 1000 S2S connections; Express Route
Automated branch connectivity using SDWAN	Not supported	Supported
Hubs per region	Multiple Virtual Networks per region	Single Virtual Hub per region. Multiple hubs possible with multiple Virtual WANs
Azure Firewall – multiple public IP addresses	Customer provided	Auto generated

Azure Firewall Manager for Hub Virtual Networks vs Secured Virtual

	Hub virtual network	Secured virtual hub
Azure Firewall Availability Zones	Supported	Not yet available
Advanced Internet security with third-party Security as a Service partners	Customer established and managed VPN connectivity to partner service of choice	Automated via security partner provider flow and partner management experience
Centralized route management to route traffic to the hub	Customer-managed User Defined Route	Supported using BGP
Multiple security provider support	Supported with manually configured forced tunneling to third-party firewalls	Automated support for two security providers: Azure Firewall for private traffic filtering and third party for Internet filtering
Web Application Firewall on Application Gateway	Supported in Virtual Network	Currently supported in spoke network
Network Virtual Appliance	Supported in Virtual Network	Currently supported in spoke network
Azure DDoS Protection Standard support	Yes	No

Deploying Azure Firewall Manager

Hub virtual networks

1. Create a firewall policy
2. Create your hub and spoke architecture
3. Select security providers and associate firewall policy. Currently, only Azure Firewall is a supported provider.
4. Configure User Define Routes to route traffic to your Hub Virtual Network firewall.

Secured virtual WAN hubs

1. Create your hub and spoke architecture
2. Select security providers
3. Create a firewall policy and associate it with your hub
4. Configure route settings to route traffic to your secured hub

Implement a Web Application Firewall

Web Application Firewall overview

Provides centralized protection of your web applications from common exploits and vulnerabilities

A centralized web application firewall helps make security management much simpler

A WAF also gives application administrators better assurance of protection against threats and intrusions

A WAF solution can react to a security threat faster by centrally patching a known vulnerability, instead of securing each individual web application

Based on OWASP TOP 10 protection

Edge

WAF

Global WAF policy
Custom Access Control
Rate Limit
OWASP TOP 10 Protection

Microsoft Global Network

Public Network

SQL

Cosmos DB

One or More Azure Regions

Other Cloud

On-premises
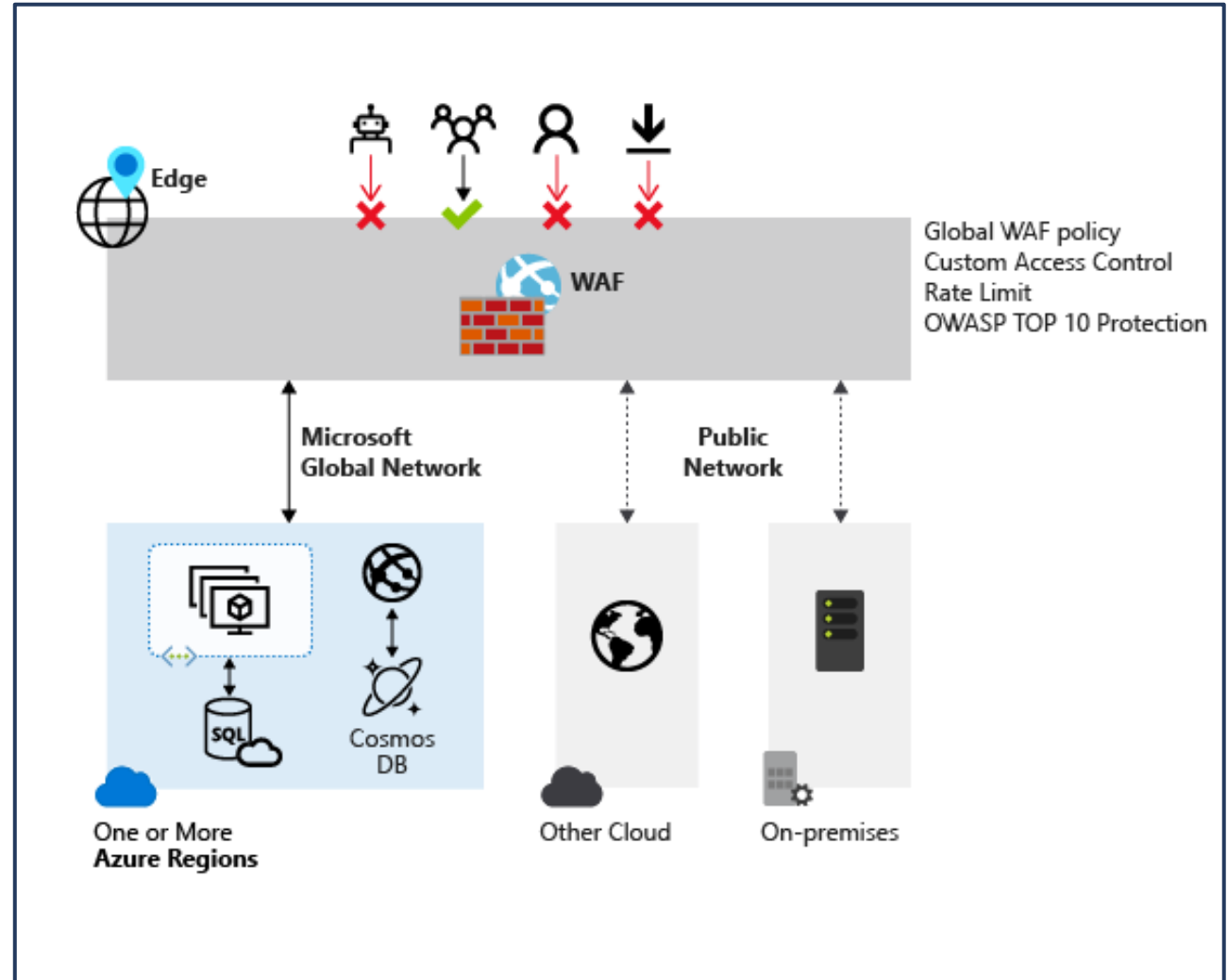
Web Application Firewall with Azure services
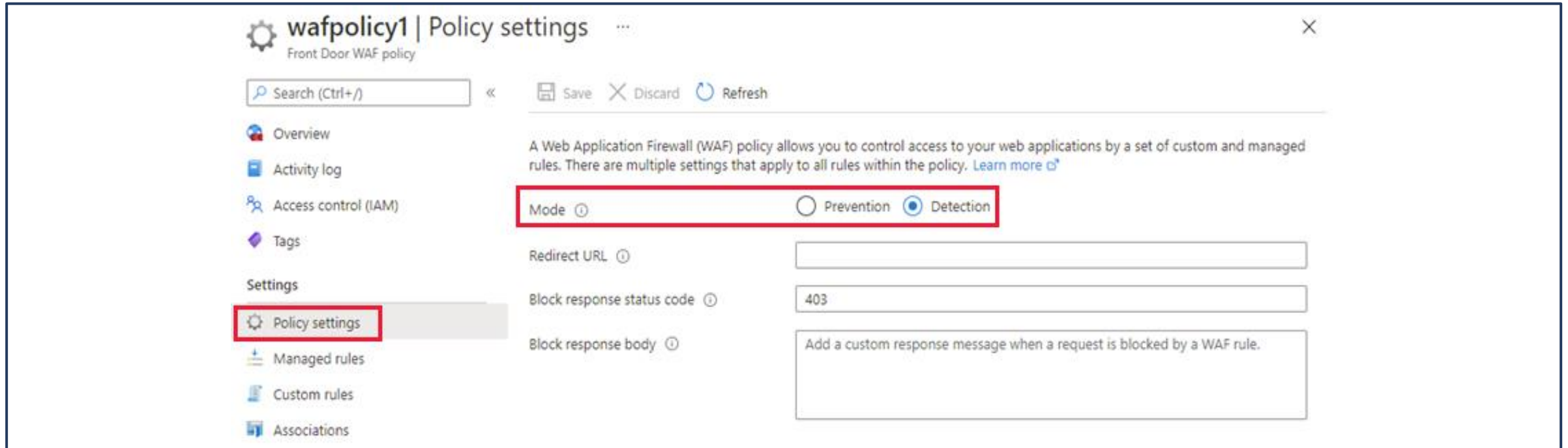
WAF on Azure Application Gateway

- You can create multiple policies, and they can be associated with an Application Gateway, to individual listeners, or to path-based routing rules on an Application Gateway
- Customizable and separate policies for each site behind your Application Gateway if needed
- Monitor attacks

WAF on Azure Front Door

- Global and centralized solution
- WAF enabled web applications inspect every incoming request delivered by Front Door at the network edge
- WAF policy can be associated to one or more Front Door front-ends for protection

Web Application Firewall policy modes

by default, the WAF policy is in Detection mode

In Detection mode, WAF does not block any requests; instead, requests matching the WAF rules are logged at WAF logs
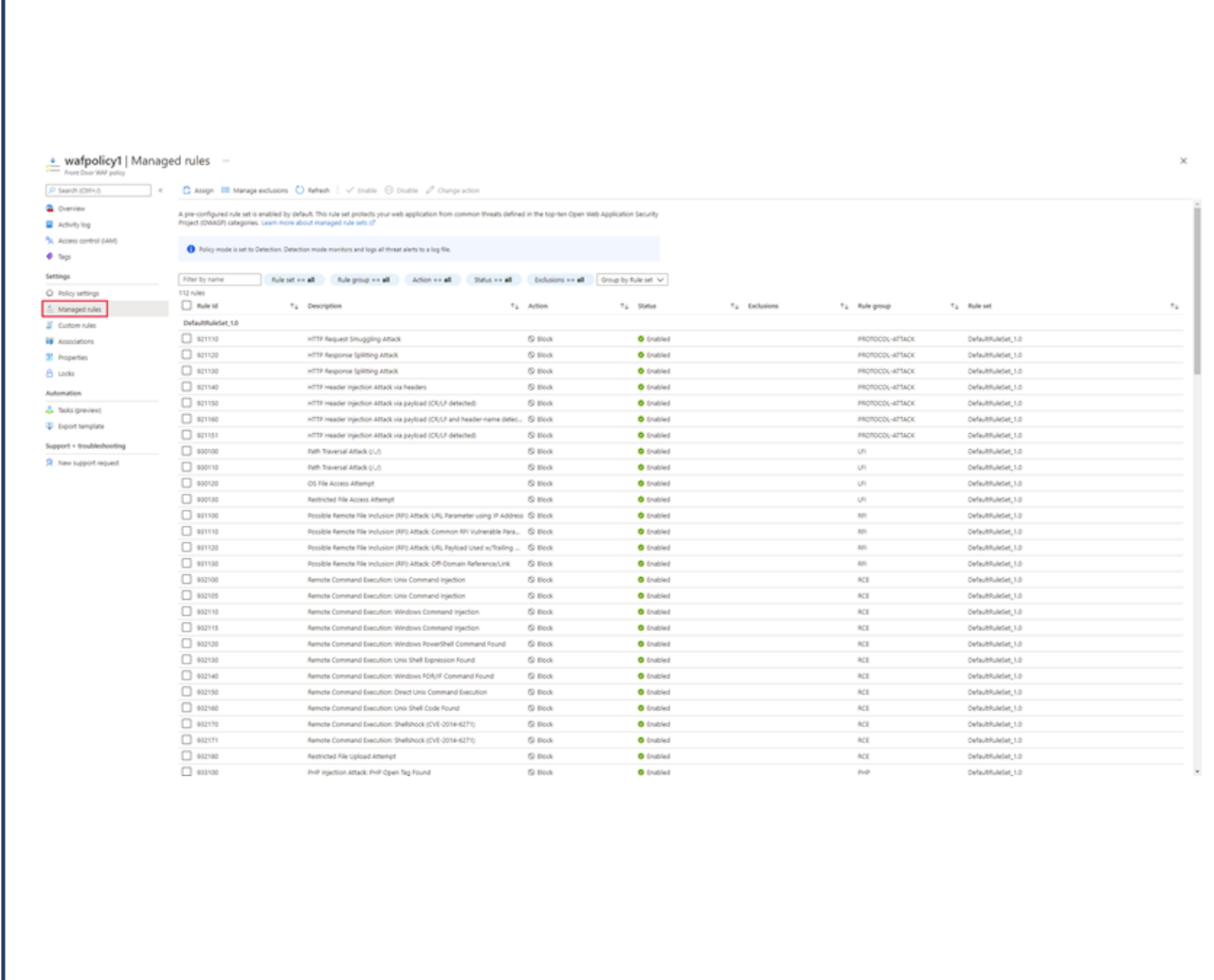
you can change the mode settings from Detection to Prevention

In Prevention mode, requests that match rules that are defined in Default Rule Set (DRS) are blocked and logged at WAF logs

Web Application Firewall Default Rule Set rule groups and rules

Azure-managed Default Rule Set includes rules against the following threat categories:

- Cross-site scripting
- Java attacks
- Local file inclusion
- PHP injection attacks
- Remote command execution
- Remote file inclusion
- Session fixation
- SQL injection protection
- Protocol attackers

Web Application Firewall Custom Rules

wafpolicy1 | Custom rules
Front Door WAF policy

Search (Ctrl+/) «

- Overview
- Activity log
- Access control (IAM)
- Tags

Settings
- Policy settings
- Managed rules
- Custom rules
- Associations

💾 Save ✕ Discard 🔄 Refresh

Configure a policy with custom-authored rules. Once a rule is matched, the corresponding action defined in the rule is applied to the request. Once such a match is processed, rules with lower priorities are not processed further. A smaller integer value for a rule denotes a higher priority. Learn more ↗

➕ Add custom rule

Priority	Name	Rule type	Action	Status

No custom rules to display.

Add custom rule ✕

A custom rule is made up of one or more conditions followed by an action. All custom rules for a WAF policy are match rules. Learn more about custom rules ↗

Custom rule name *   blockQSexample ✓

Status ⓘ   [Enabled] Disabled

Rule type ⓘ   [Match] Rate limit

Priority * ⓘ   4 ✓

Conditions

If 🗑

Match type ⓘ
String ⌄

Match variable *
QueryString ⌄

Operation
◉ is ○ is not

Operator *
Contains ⌄

Transformation ⓘ
Select a transformation ⌄

Match values
blockme ✓ 🗑
Enter a match value

➕ Add new condition

Then   Deny traffic ⌄

[Add] [Cancel]

A custom WAF rule consists of a priority number, rule type, match conditions, and an action

There are two types of custom rules: a match rule controls access based on a set of matching conditions

a rate limit rule controls access based on matching conditions and the rates of incoming requests

Create a Web Application Firewall policy on Azure Front Door

Create a Web Application Firewall policy - this is where you create a basic WAF policy with managed Default Rule Set (DRS).

Associate the WAF policy with a Front Door profile - this is where you associate the WAF policy created in stage 1 with a Front Door profile. This association can be done during the creation of the WAF policy, or it can be done on a previously created WAF policy. During the association you specify the Front Door profile and the domain/s within the Front Door profile you want the WAF policy to be applied to.

Configure WAF policy settings and rules - this is an optional stage, where you can configure policy settings such as the Mode (Prevention or Detection) and configure managed rules and custom rules.

Associate a Front door profile ✕

Front door profiles can be added and removed after a WAF policy is created.

Front door profile * ⓘ

| contosoafd | ⌄ |

Domain

Multiple domains can be associated with a front door profile. Select those you want your WAF policy to apply to.

Domain *

| contosoafd1 | ⌄ |

Add   **Cancel**

Exercise: Configure DDoS Protection on a virtual network using the Azure portal

Configure DDoS Protection on a virtual network using the Azure portal

Task 1: Create a resource group
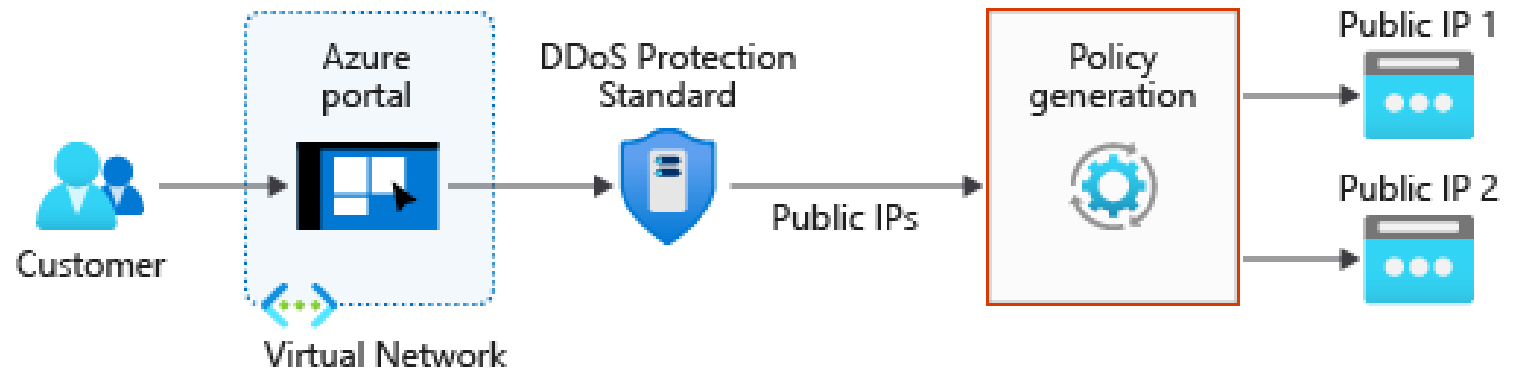Task 2: Create a DDoS Protection plan
Task 3: Enable DDoS Protection on a new virtual network
Task 4: Configure DDoS telemetry
Task 5: Configure DDoS diagnostic logs
Task 6: Configure DDoS alerts
Task 7: Submit a DDoS service request to run a DDoS attack

Customer → Azure portal / Virtual Network → DDoS Protection Standard → Public IPs → Policy generation → Public IP 1, Public IP 2

Exercise – Deploy and configure Azure Firewall using the Azure portal

Deploy and configure Azure Firewall using the Azure portal

Create a resource group, virtual network and subnets

Create a virtual machine

Deploy the firewall and firewall policy

Create a default route

Configure an application rule

Configure a network rule

Configure a Destination NAT (DNAT) rule

Change the primary and secondary DNS address for the server's network interface

Test the firewall

Exercise- Secure your virtual hub using Azure Firewall Manager

Secure your virtual hub using Azure Firewall Manager

Create two spoke virtual networks

and subnets

Create the secured virtual hub

Connect the hub and spoke virtual networks

Deploy the servers

Create a firewall policy and secure your hub

Associate the firewall policy

Route traffic to your hub

Test the application rule

Test the network rule

End of presentation