

# 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

LB  
App GW

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 **ASC**
- Deploy Azure DDoS Protection by using the Azure portal **Basic ✓ Standard**
- Deploy and configure Network Security Groups **NSG** **ASG (Label)**
- Design and implement Azure Bastion
- Design and implement Azure Firewall



- Working with Azure Firewall Manager
- Implement a Web Application Firewall **WAF** **App GW Front Door**
- 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

pro Subscription Free n. Security Score 42%  
2. Recommendation- 10%

Server  
DB  
K8S

VM  
Size  
SKU  
DS2\_V3 → B1  
Location

# 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.

1

Azure Security Benchmark

Azure CIS 1.1.0

PCI DSS 3.2.1

ISO 27001

SOC TSP

HIPAA HITRUST

...

Under each applicable compliance control is the set of assessments run by Security Center that are associated with that control. If they are all green, it means those assessments are currently passing; this does not ensure you are fully compliant with that control. Furthermore, not all controls for any particular regulation are covered by Security Center assessments, and therefore this report is only a partial view of your overall compliance status.

Azure Security Benchmark is applied to the subscription ASC DEMO 2

☐ Expand all compliance controls

3

1. Network Security

1.1. Protect resources using Network Security Groups or Azure Firewall on your Virtual Network

4

Adaptive Network Hardening recommendations show

Virtual machines

3 of 35

5

Active - 3 of 35 Virtual machines (8.57%)

1.2. Monitor and log the configuration and traffic of Vnets, Subnets, and NICs

Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Regulatory compliance

Showing 2 subscriptions

Search (Ctrl+J)

Download report

Manage compliance policies

Open query

Audit reports

Compliance over time workbook

General

Overview

Getting started

Recommendations

Security alerts

Inventory

Workbooks

Community

Diagnose and solve problems

Cloud Security

Secure Score

Regulatory compliance

Workload protections

Firewall Manager

Management

Environment settings

Security solutions

Workflow automation

You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above. →

Azure Security Benchmark

Lowest compliance regulatory standards

ISO 27001:2013

16/17

You have no default policy assignment

Open policy settings to manage default compliance policies

Manage compliance policies >

Audit reports

Stay up to date on the latest privacy, security, and compliance-related information for Microsoft's cloud services.

Open

ISO 27001:2013

Under each applicable compliance control is the set of assessments run by Defender for Cloud that are associated with that control. If they are all green, it means those assessments are currently passing; this does not ensure you are fully compliant with that control. Furthermore, not all controls for any particular regulation are covered by Defender for Cloud assessments, and therefore this report is only a partial view of your overall compliance status.

ISO 27001:2013 is applied to the subscription Contoso IT - Retail - Prod

☐ Expand all compliance controls

A.5. Information security policies

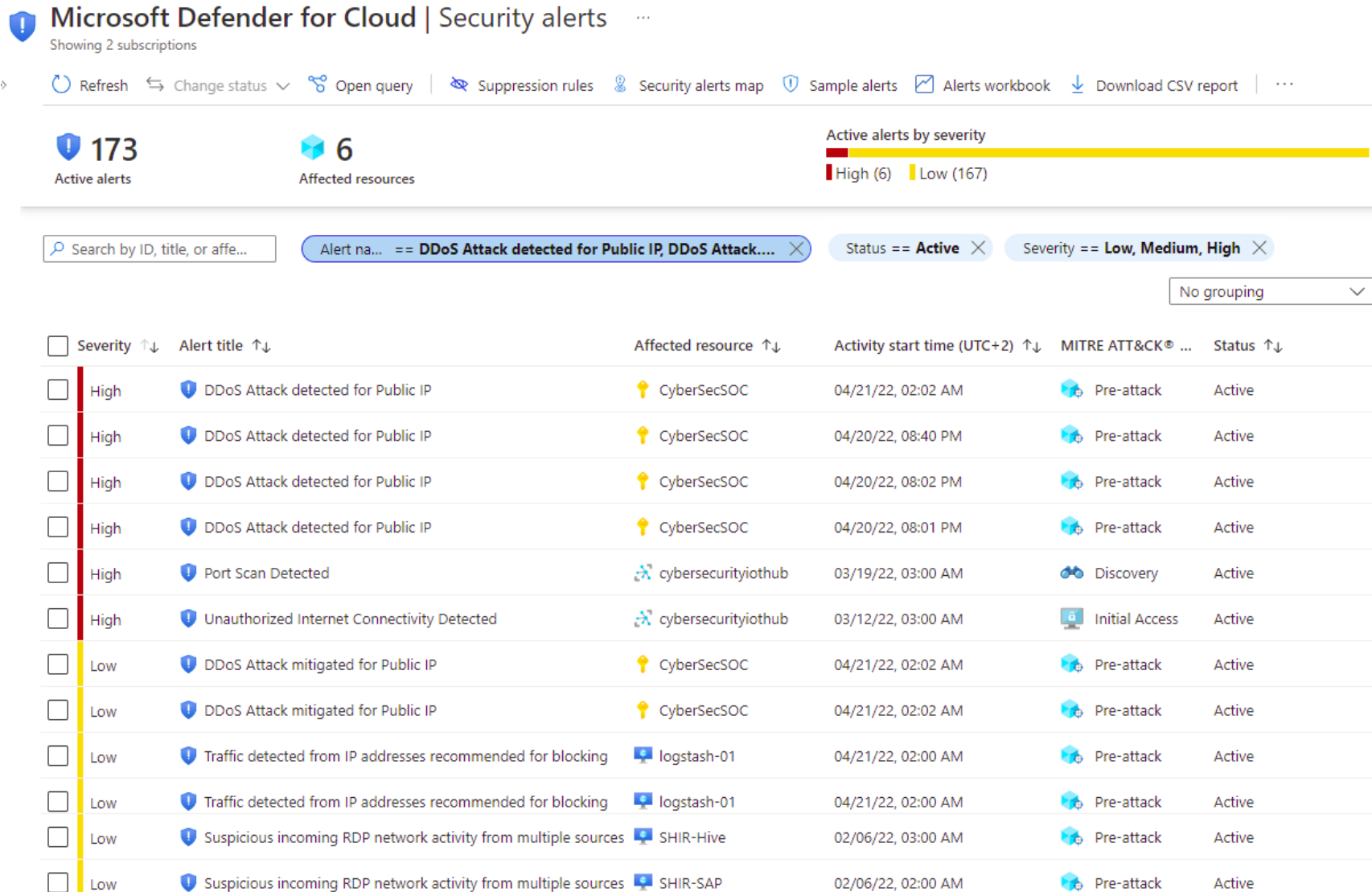
A.6. Organization of information security

A.7. Human resource security

A.8. Asset management

A.9. Access control

# Alerts in Microsoft Defender for Cloud





# Deploy Azure DDoS Protection by using the Azure portal



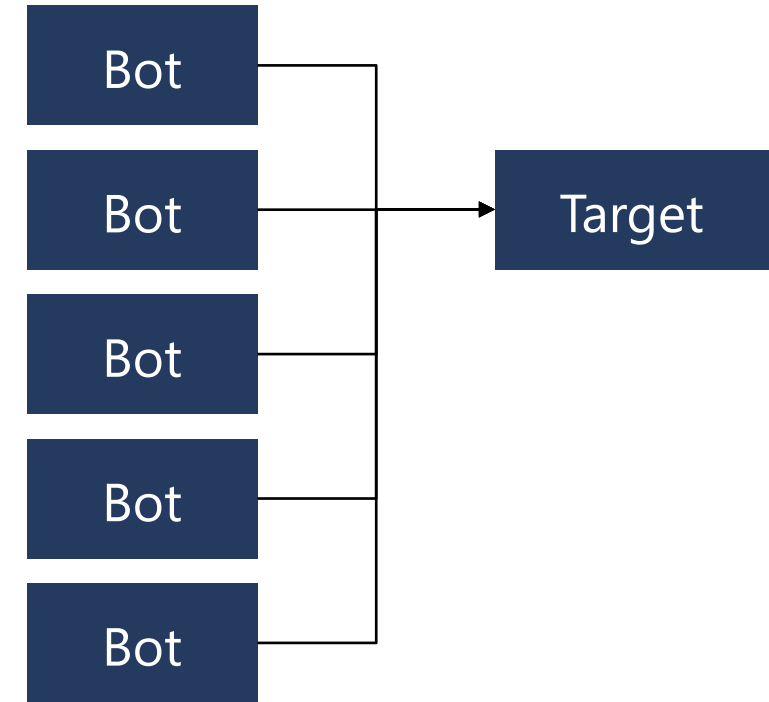
# Distributed Denial of Service (DDoS)

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



# 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**

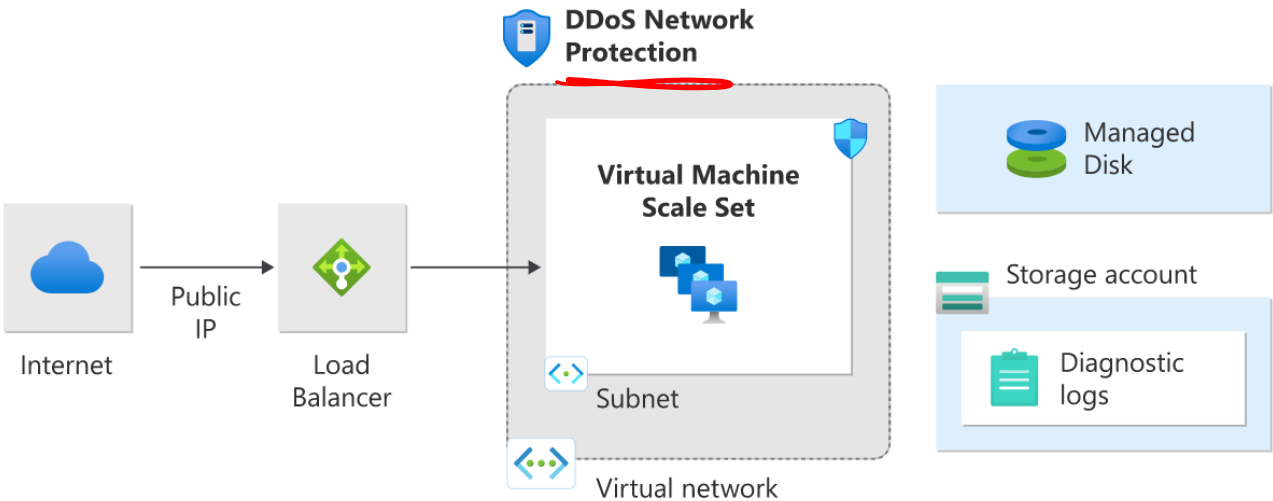
These attacks render a target inaccessible, by exploiting a weakness in the layer 3 and layer 4 protocol stack. They include SYN flood attacks, reflection attacks, and other protocol attacks. DDoS Protection Standard mitigates these attacks, differentiating between malicious and legitimate traffic, by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

## **Resource (application) layer attacks**

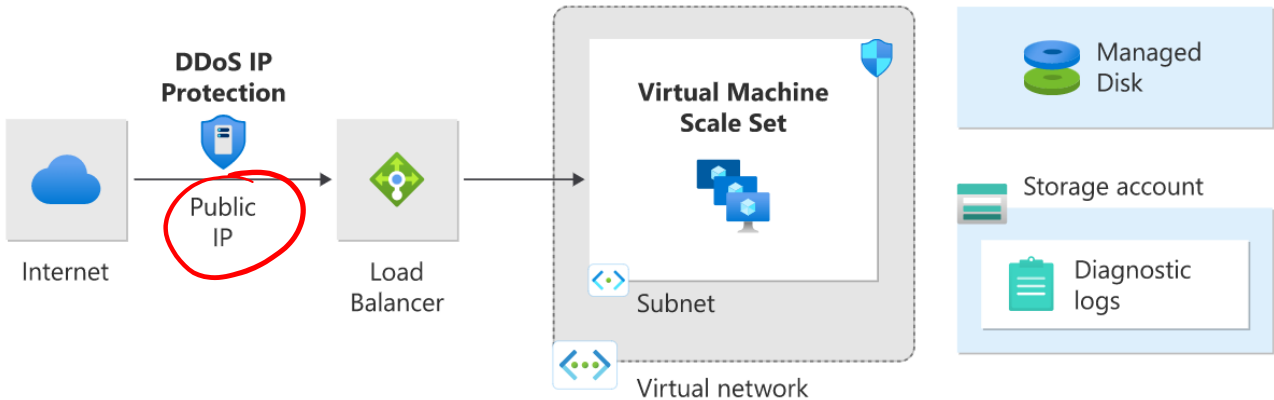
These attacks target web application packets, to disrupt the transmission of data between hosts. They include HTTP protocol violations, SQL injection, cross-site scripting, and other layer 7 attacks. Use a Web Application Firewall, such as the Azure Application Gateway web application firewall, as well 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

**SOCNSDDOSPLAN** | Protected resources ...

DDoS protection plan | Directory: [ ]

Search (Ctrl+ /) << + Add Refresh

Overview  
Activity log  
Access control (IAM)  
Tags  
Diagnose and solve problems

Settings  
Protected resources

VNET Firewall Application Gateway Bastion Host Load Balancer NIC

Filter by name... Subscription == 3 selected Resource Group == all

Showing 1 to 1 of 1 records.

Virtual network ↑↓	Resource group ↑↓
VN-HUB	soc-ns

Previous Page 1 of 1 Next

# Deploy and configure Network Security Groups

Stateful  
no Header

NSG  
in  
out

allow  
deny

# Network Security Groups

**nsg0**  
Network security group | 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

Label  
ASG

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

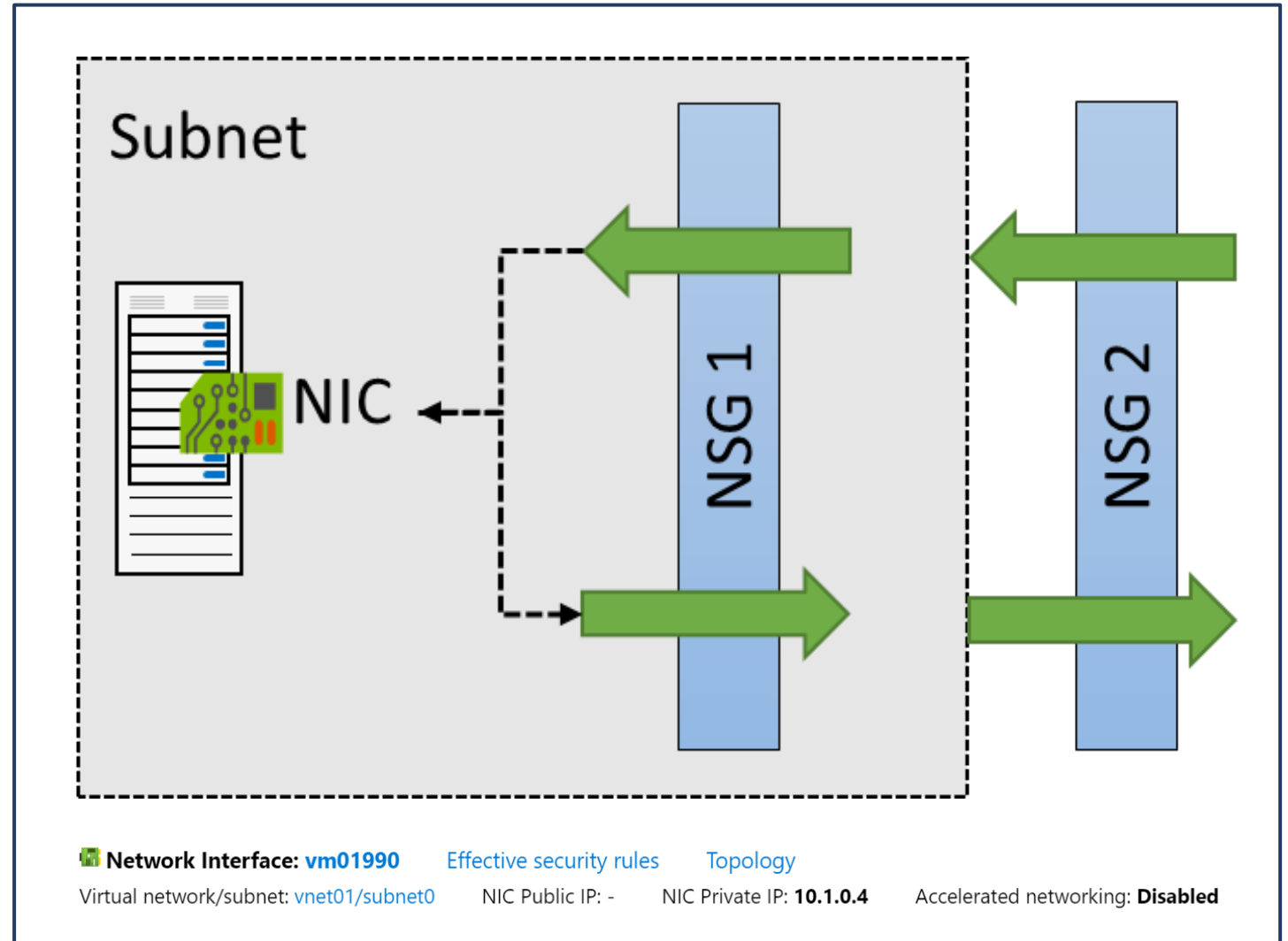
There are default security rules. You cannot delete the default rules, but you can add other rules with a higher priority

# 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



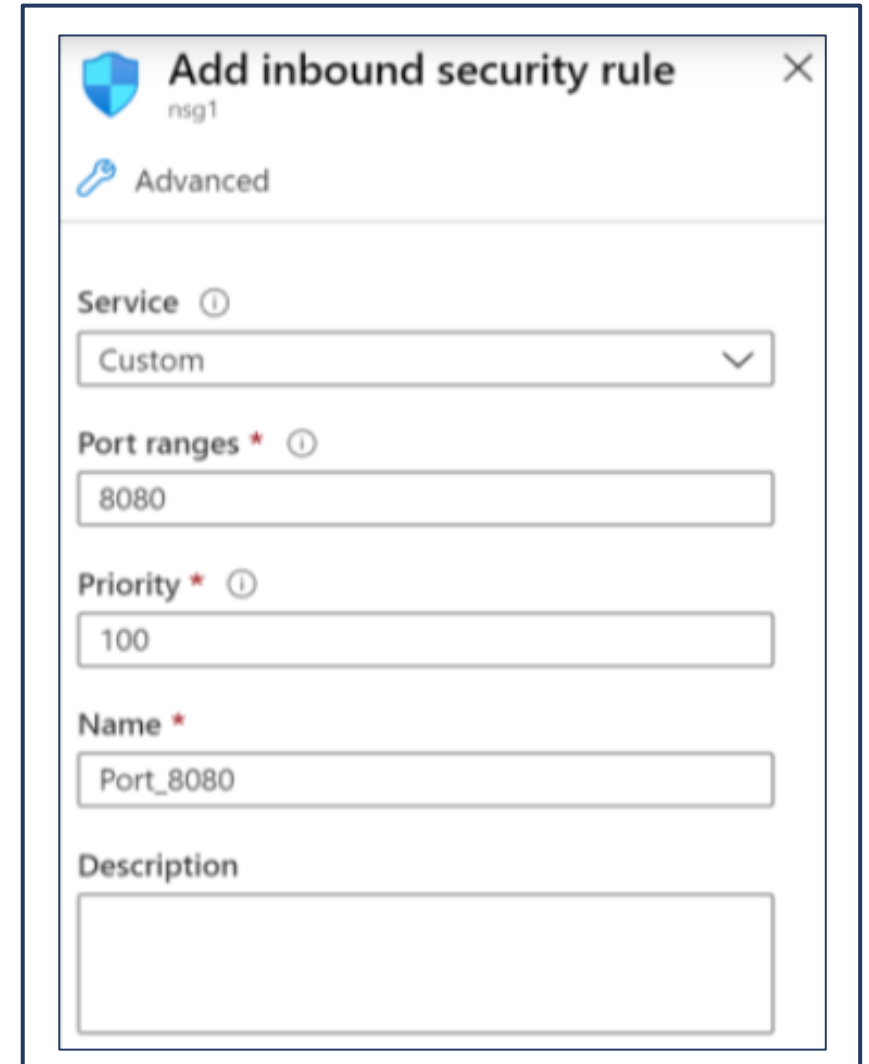
# Creating NSG rules

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



The screenshot shows the 'Add inbound security rule' dialog box for a network security group named 'nsg1'. The 'Advanced' tab is selected. The 'Service' dropdown is set to 'Custom'. The 'Port ranges' field contains '8080'. The 'Priority' field contains '100'. The 'Name' field contains 'Port\_8080'. The 'Description' field is empty.

Field	Value
Service	Custom
Port ranges	8080
Priority	100
Name	Port_8080
Description	

# Use Service Tags to define network access controls

Home > Microsoft.NetworkSecurityGroup-202106241

ContosoPrivateNSG | Outbound security rules

Network security group

Search (Ctrl+/)

+ Add

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Alerts

Diagnostic settings

Logs

NSG flow logs

Automation

Tasks (preview)

Export template

Support + troubleshooting

Effective security rules

New support request

Add outbound security rule

ContosoPrivateNSG

Source port ranges \*

\*

Destination

Service Tag

Destination service tag

Storage

Service

Custom

Destination port ranges \*

\*

Protocol

☒ Any

☐ TCP

☐ UDP

☐ ICMP

Action

☒ Allow

☐ Deny

Priority \*

100

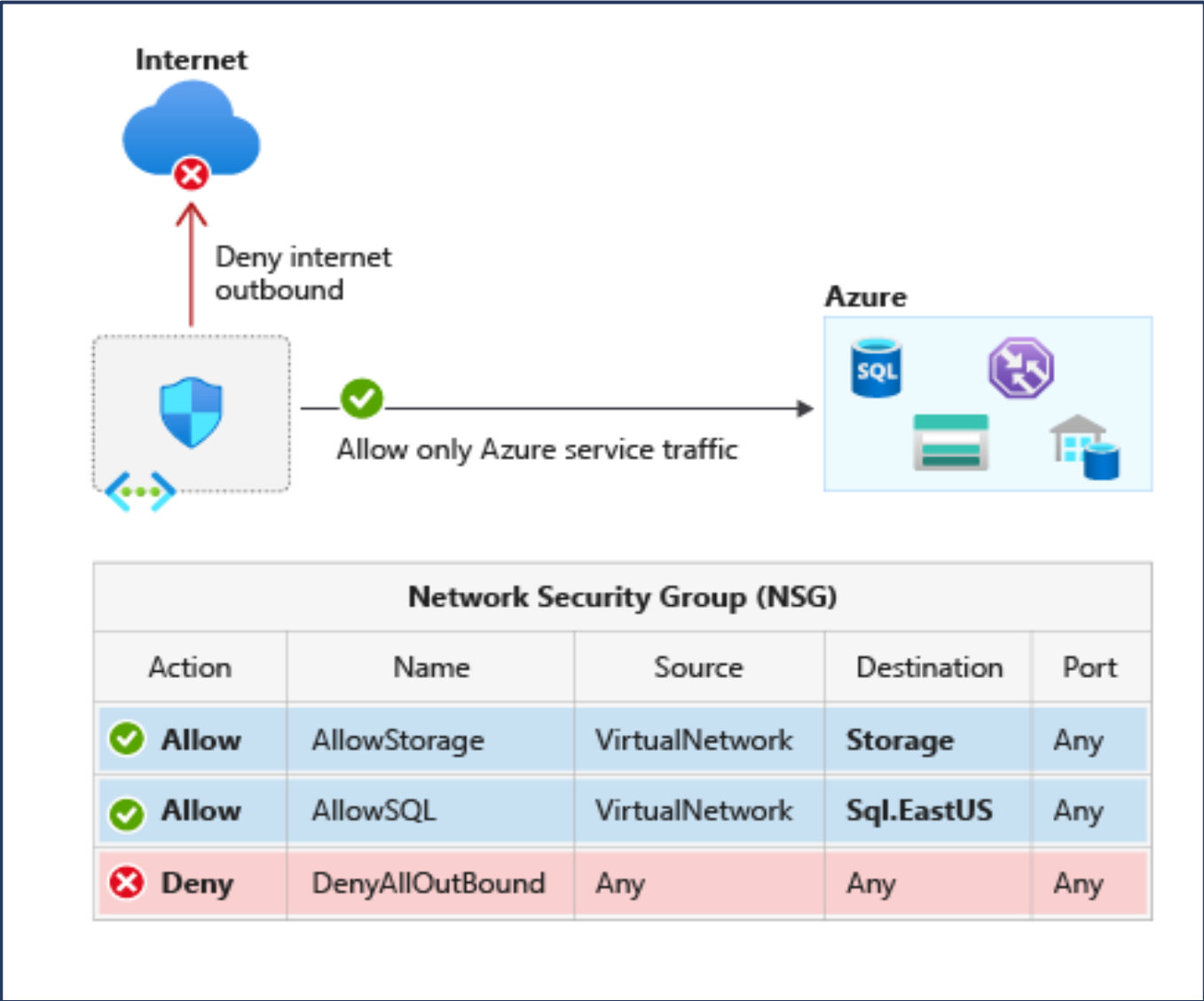
Name \*

Allow-Storage\_All

Description

Add

Cancel



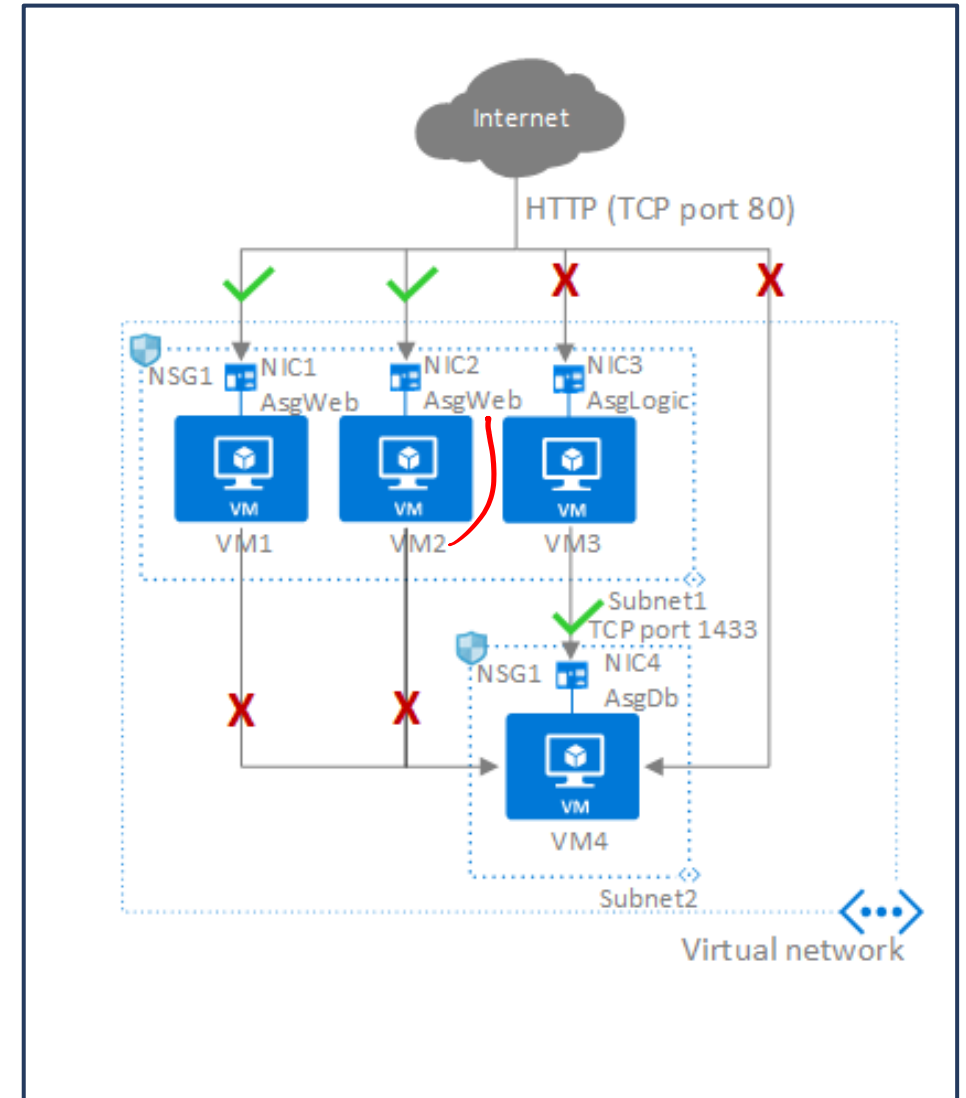
# Application Security Groups (ASG)

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

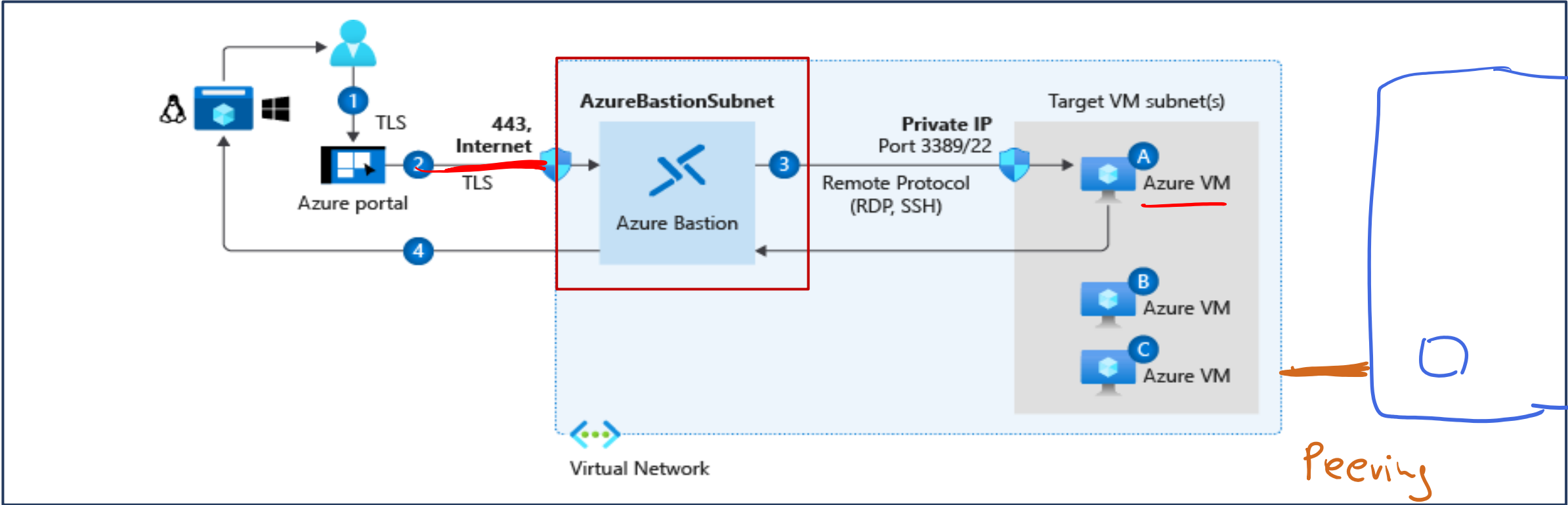
If you specify an ASG as the source and destination in a security rule, the NIC in both ASG must exist in the same virtual network



# 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

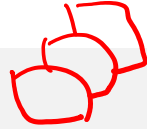
# Design and implement Azure Firewall





# Azure Firewall features

Stateful firewall as a service



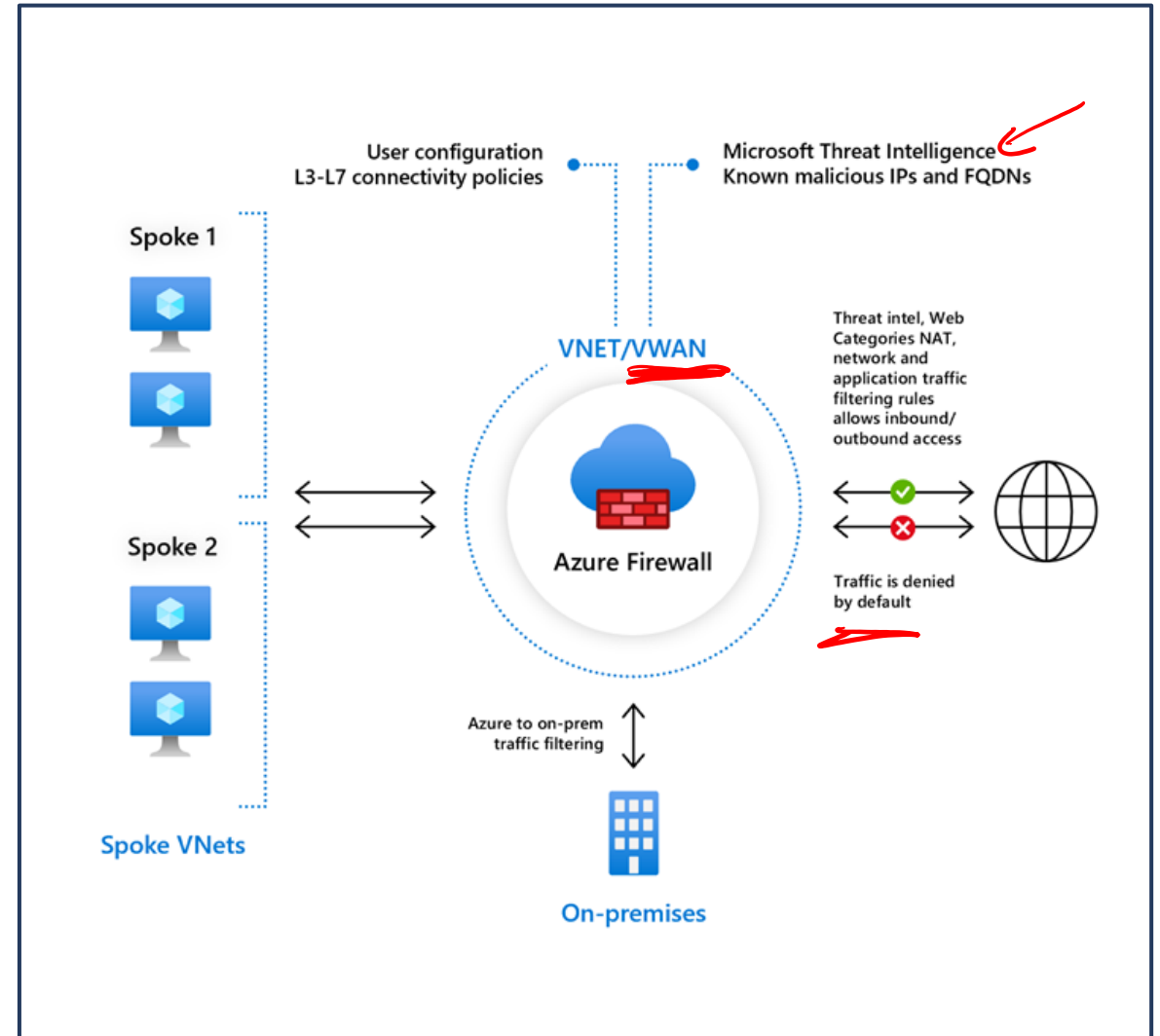
Built-in high availability with unrestricted cloud scalability

Create, enforce, and log application and network connectivity policies

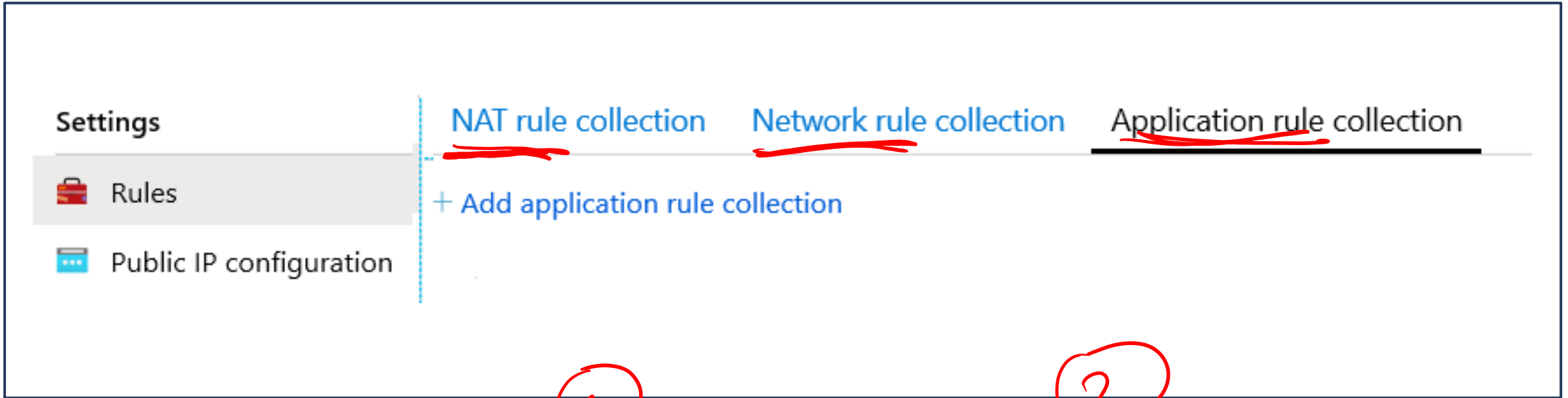
Threat intelligence-based filtering for L3-L7

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



**NAT rules.** Configure DNAT rules to allow incoming connections

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

**2. 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 \*

Resource group \*

[Create new](#)

## Instance details

Name \*

Region \*

Availability zone ⓘ

**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 \*

[Add new](#)

Choose a virtual network ☒ Create new ☐ Use existing

Virtual network name \*

Address space \*

(0 addresses)

Subnet

Subnet address space \*

(0 addresses)

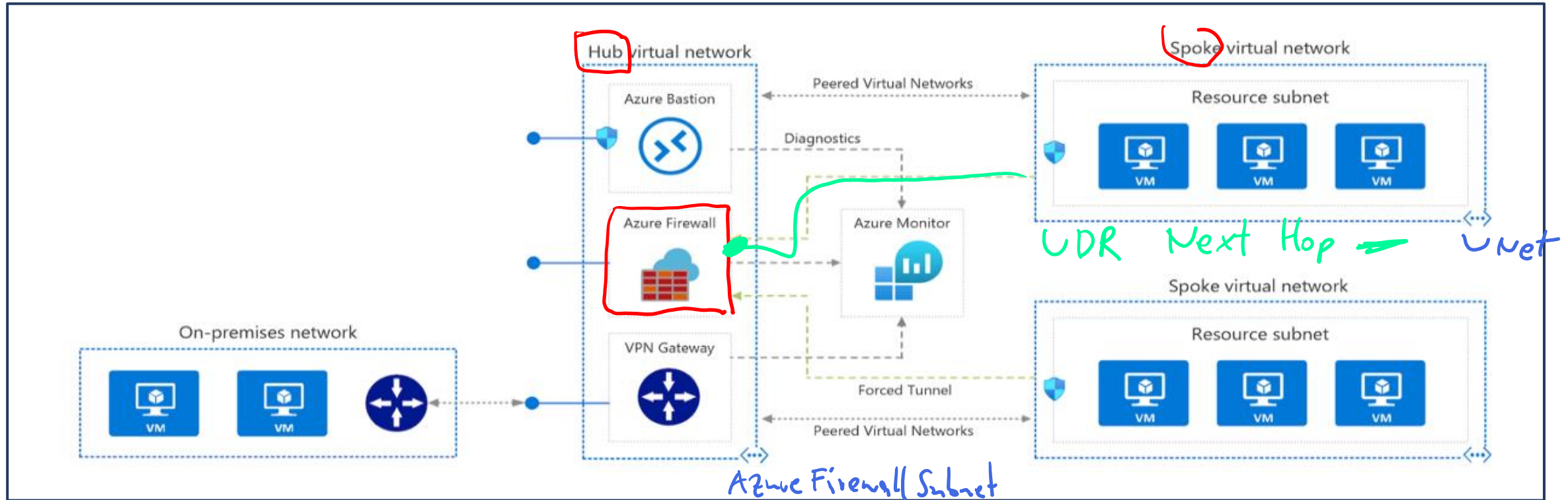
Public IP address \*

[Add new](#)

**x** 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

No

SSL

# Working with Azure Firewall Manager



# Azure Firewall Manager features

Central Azure Firewall deployment and configuration

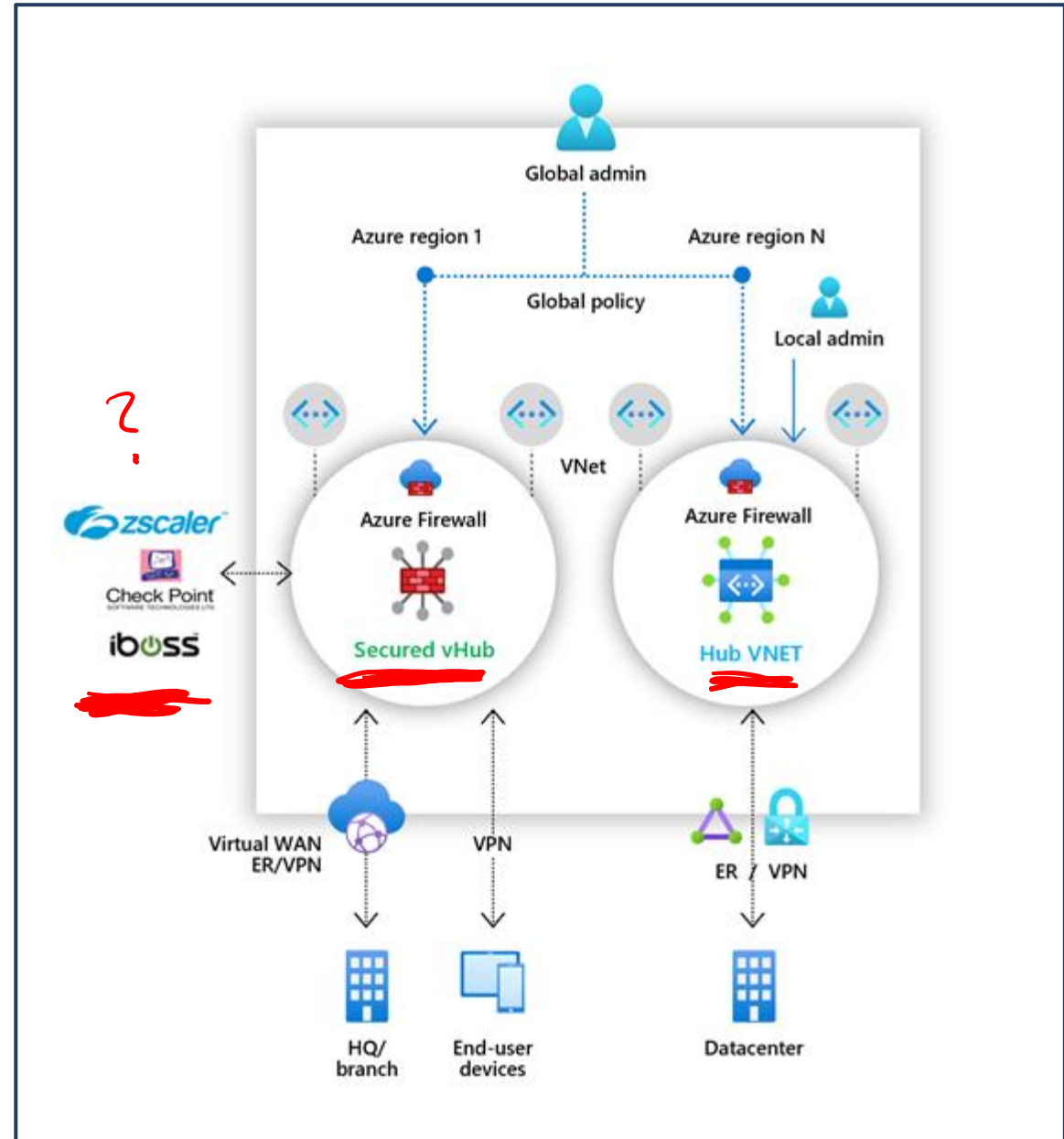
Hierarchical policies (global and local)

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

Centralized route management

Region availability

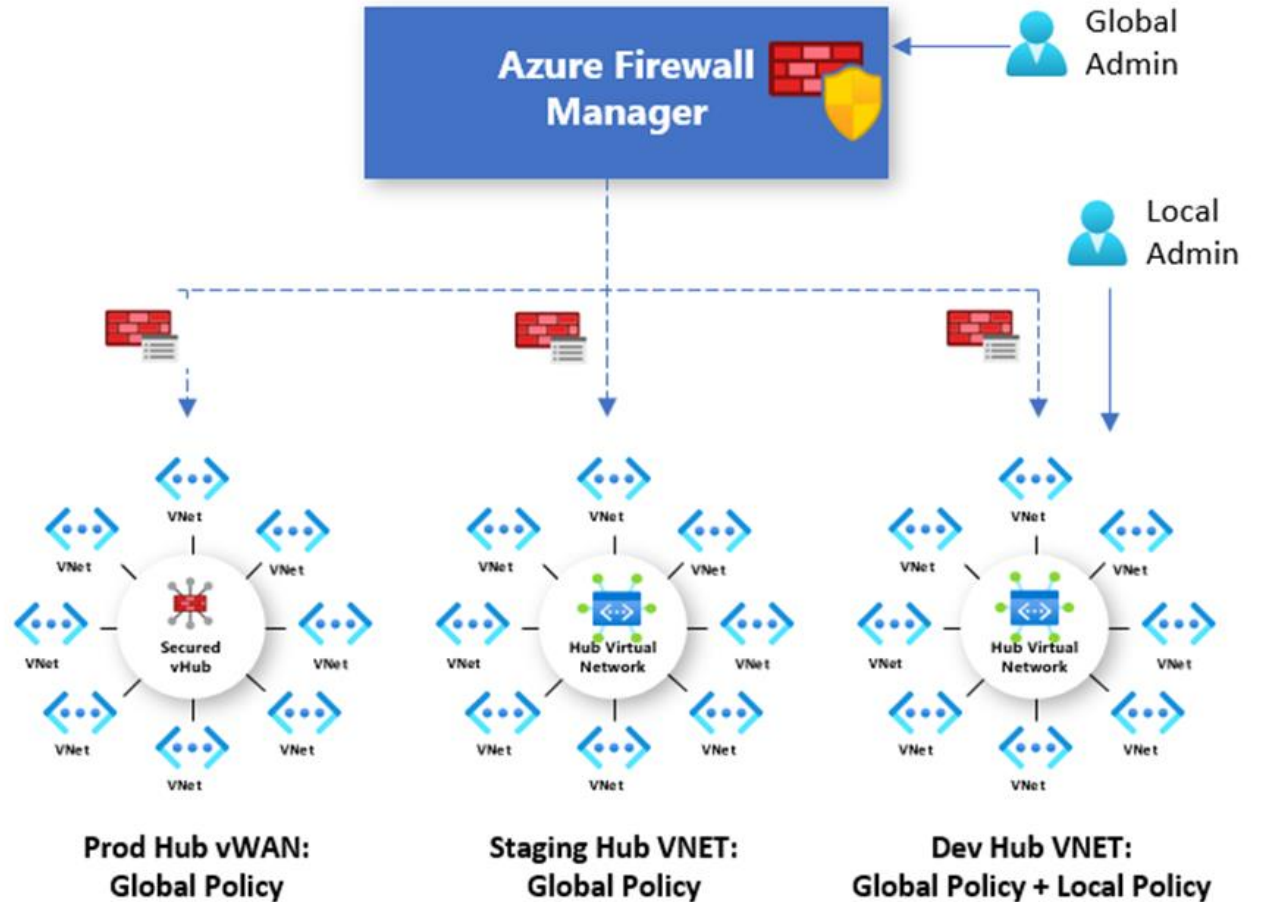
© Copyright Microsoft Corporation. All rights reserved.



# 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.





# Azure Firewall Manager for Hub Virtual Networks vs Secured Virtual

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

# Azure Firewall Manager for Hub Virtual Networks vs Secured Virtual

	Hub virtual network	Secured virtual hub
<b>Azure Firewall Availability Zones</b>	Supported	Not yet available
<b>Advanced Internet security with third-party Security as a Service partners</b>	Customer established and managed VPN connectivity to partner service of choice	Automated via security partner provider flow and partner management experience
<b>Centralized route management to route traffic to the hub</b>	Customer-managed User Defined Route	Supported using BGP
<b>Multiple security provider support</b>	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
<b>Web Application Firewall on Application Gateway</b>	Supported in Virtual Network	Currently supported in spoke network
<b>Network Virtual Appliance</b>	Supported in Virtual Network	Currently supported in spoke network
<b>Azure DDoS Protection Standard support</b>	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.

3rd party FW

## 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

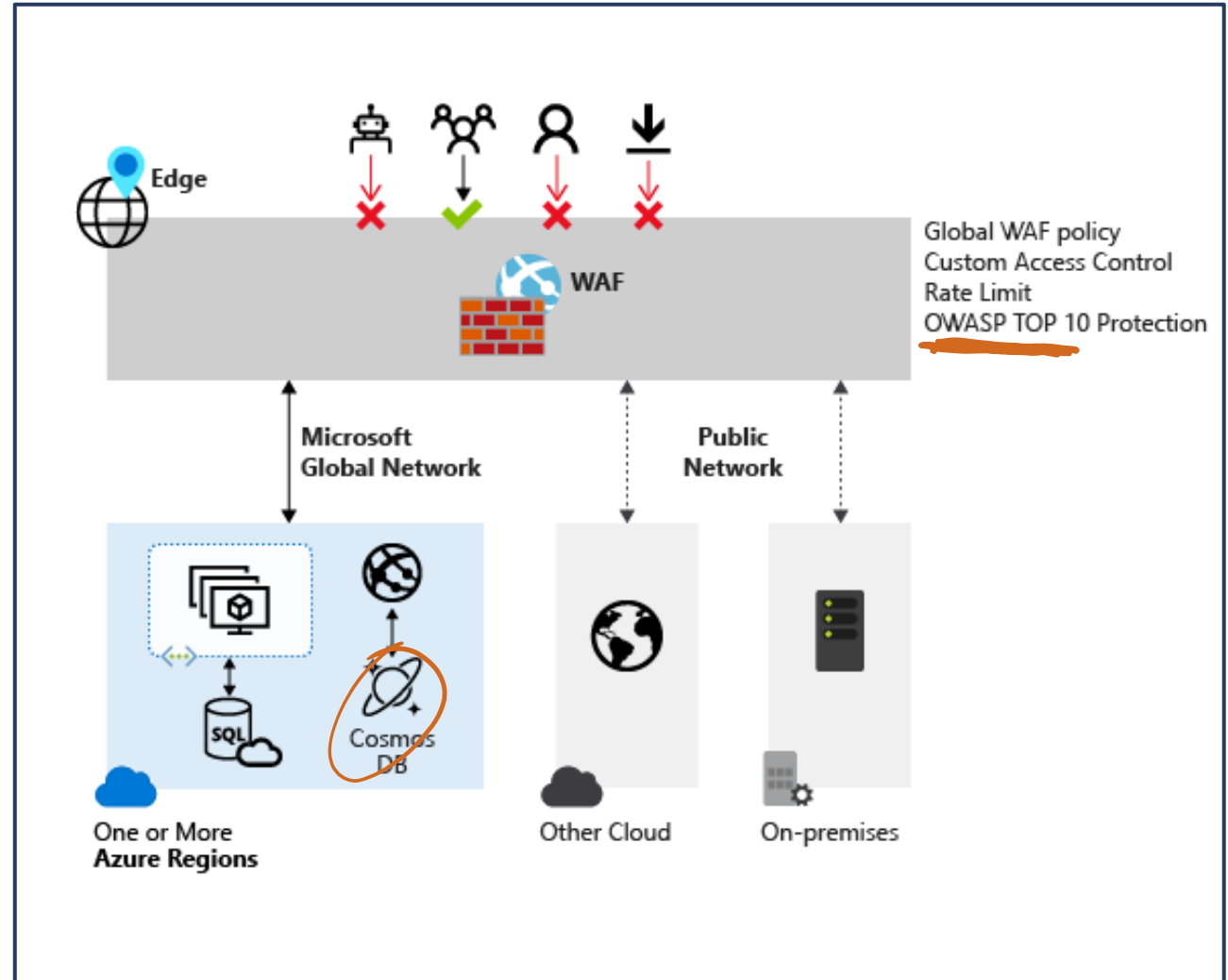
Provides centralized protection of your web applications from common exploits and vulnerabilities

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



# 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

**wafpolicy1 | Policy settings** Front Door WAF policy

Search (Ctrl+ /) Save Discard Refresh

Overview  
Activity log  
Access control (IAM)  
Tags

Settings

- Policy settings**
- Managed rules
- Custom rules
- Associations

A Web Application Firewall (WAF) policy allows you to control access to your web applications by a set of custom and managed rules. There are multiple settings that apply to all rules within the policy. [Learn more](#)

Mode ☐ Prevention ☒ Detection

Redirect URL

Block response status code

Block response body

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

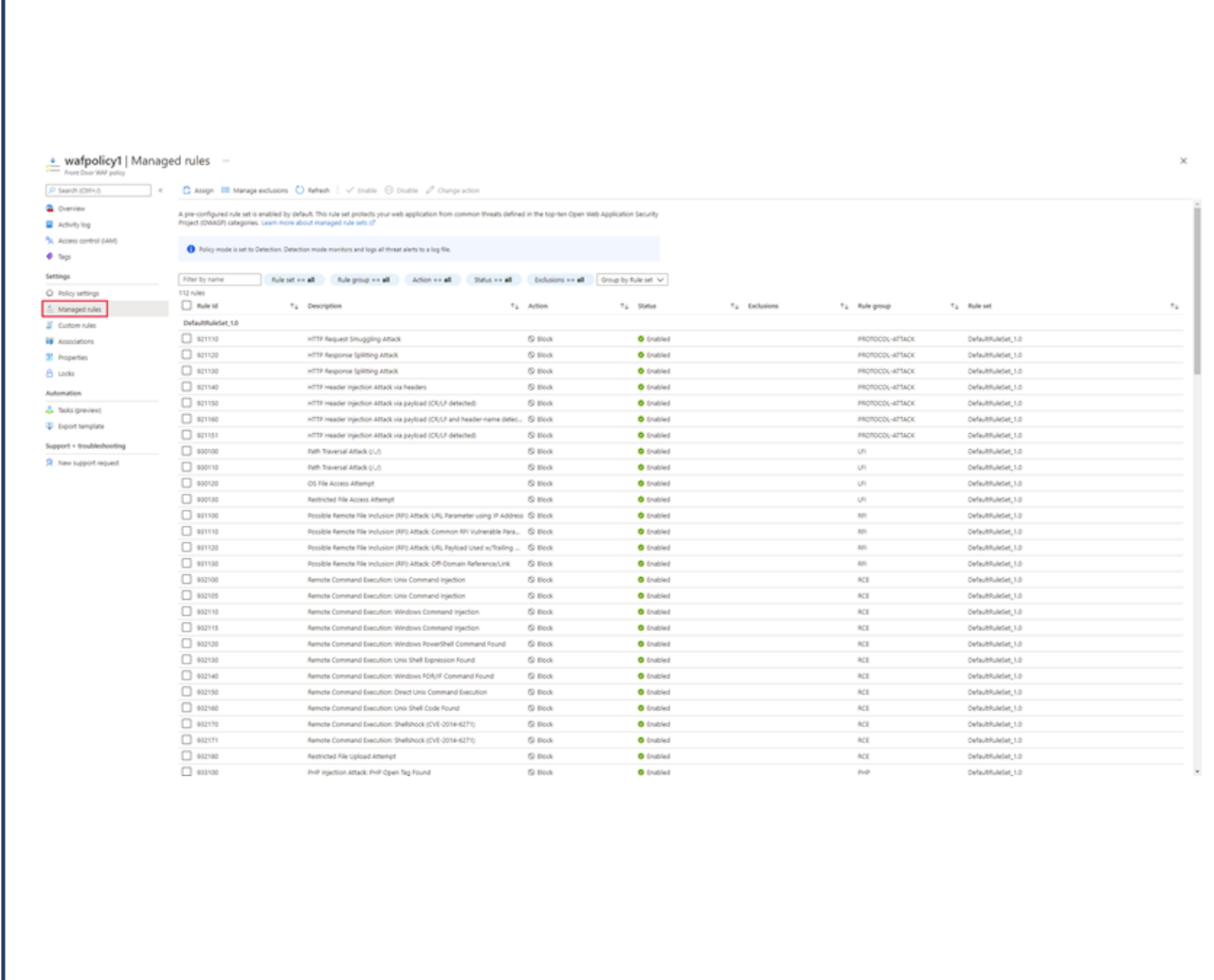
you can change the mode settings from Detection to Prevention

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

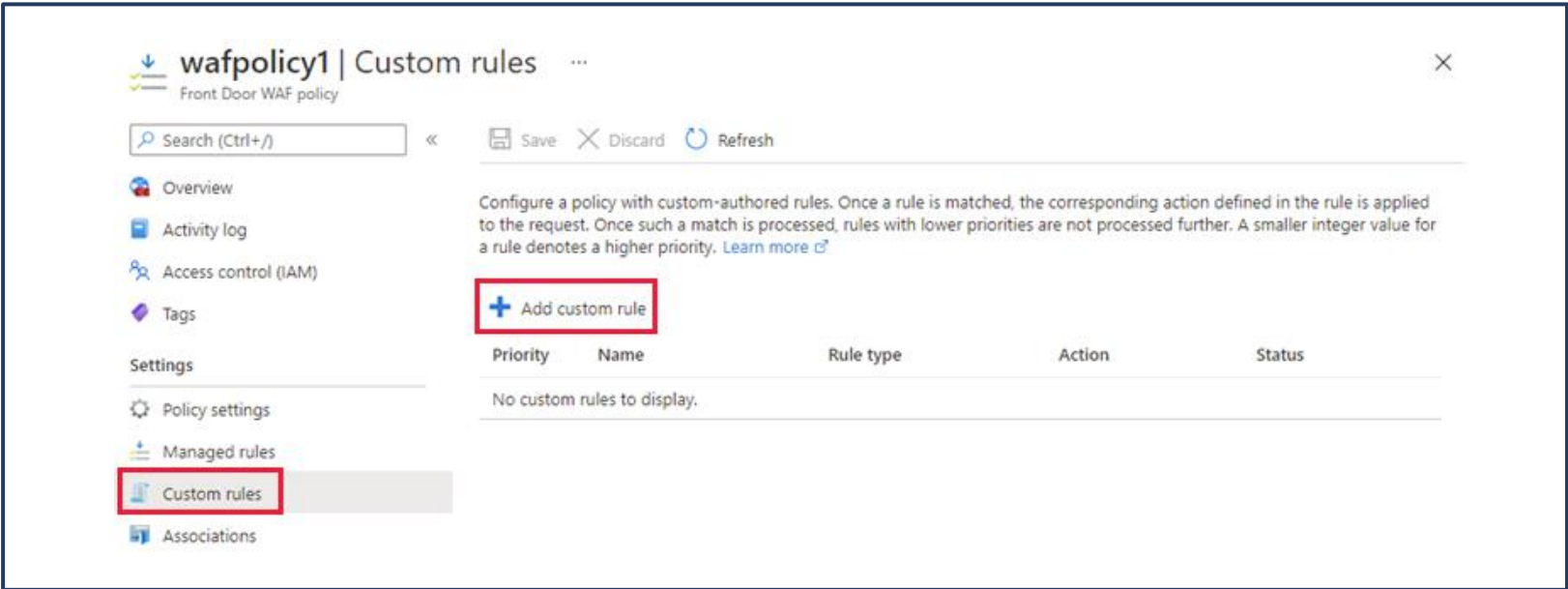


The screenshot displays the 'wafpolicy1 | Managed rules' interface in the Azure portal. The left sidebar shows navigation options: Overview, Activity log, Access control (IAM), Tags, Settings, Policy settings, Managed rules (highlighted), Custom rules, Associations, Properties, Locks, Automation, Tasks (preview), Export template, and Support + troubleshooting. The main area shows a table of 132 rules for the 'DefaultRuleSet\_1.0' rule set. The table columns are: Rule ID, Description, Action, Status, Exclusions, Rule group, and Rule set. The rules are categorized into various threat types such as HTTP Request Smuggling, HTTP Response Splitting, HTTP Header Injection, Path Traversal, OS File Access Attempt, Restricted File Access Attempt, Possible Remote File Inclusion (RFI) Attacks, Remote Command Execution, Remote File Inclusion, Remote Command Execution: Unix Command Injection, Remote Command Execution: Windows Command Injection, Remote Command Execution: Windows PowerShell Command Found, Remote Command Execution: Unix Shell Expression Found, Remote Command Execution: Windows PowerShell Command Found, Remote Command Execution: Direct Unix Command Execution, Remote Command Execution: Unix Shell Code Found, Remote Command Execution: Shellshock (CVE-2014-4271), Remote Command Execution: Shellshock (CVE-2014-4271), Restricted File Upload Attempt, and PHP Injection Attack: PHP Open Tag Found.

Rule ID	Description	Action	Status	Exclusions	Rule group	Rule set
921110	HTTP Request Smuggling attack	Block	Enabled		PROTOCOL_ATTACK	DefaultRuleSet_1.0
921120	HTTP Response Splitting attack	Block	Enabled		PROTOCOL_ATTACK	DefaultRuleSet_1.0
921130	HTTP Response Splitting attack	Block	Enabled		PROTOCOL_ATTACK	DefaultRuleSet_1.0
921140	HTTP header injection Attack via headers	Block	Enabled		PROTOCOL_ATTACK	DefaultRuleSet_1.0
921150	HTTP header injection Attack via payload (CRLF detected)	Block	Enabled		PROTOCOL_ATTACK	DefaultRuleSet_1.0
921160	HTTP header injection Attack via payload (CRLF and header name detected)	Block	Enabled		PROTOCOL_ATTACK	DefaultRuleSet_1.0
921170	HTTP header injection Attack via payload (CRLF detected)	Block	Enabled		PROTOCOL_ATTACK	DefaultRuleSet_1.0
921180	Path Traversal Attack (LFI)	Block	Enabled		LFI	DefaultRuleSet_1.0
921190	Path Traversal Attack (LFI)	Block	Enabled		LFI	DefaultRuleSet_1.0
921200	OS File Access Attempt	Block	Enabled		LFI	DefaultRuleSet_1.0
921210	Restricted File Access Attempt	Block	Enabled		LFI	DefaultRuleSet_1.0
921220	Possible Remote File Inclusion (RFI) Attack: URL Parameter using IP Address	Block	Enabled		RFI	DefaultRuleSet_1.0
921230	Possible Remote File Inclusion (RFI) Attack: Common RFI Vulnerable Parameters	Block	Enabled		RFI	DefaultRuleSet_1.0
921240	Possible Remote File Inclusion (RFI) Attack: URL Payload Used in Trailing	Block	Enabled		RFI	DefaultRuleSet_1.0
921250	Possible Remote File Inclusion (RFI) Attack: Off-Domain Reference Link	Block	Enabled		RFI	DefaultRuleSet_1.0
921260	Remote Command Execution: Unix Command Injection	Block	Enabled		RCE	DefaultRuleSet_1.0
921270	Remote Command Execution: Unix Command Injection	Block	Enabled		RCE	DefaultRuleSet_1.0
921280	Remote Command Execution: Windows Command Injection	Block	Enabled		RCE	DefaultRuleSet_1.0
921290	Remote Command Execution: Windows PowerShell Command Found	Block	Enabled		RCE	DefaultRuleSet_1.0
921300	Remote Command Execution: Unix Shell Expression Found	Block	Enabled		RCE	DefaultRuleSet_1.0
921310	Remote Command Execution: Windows PowerShell Command Found	Block	Enabled		RCE	DefaultRuleSet_1.0
921320	Remote Command Execution: Direct Unix Command Execution	Block	Enabled		RCE	DefaultRuleSet_1.0
921330	Remote Command Execution: Unix Shell Code Found	Block	Enabled		RCE	DefaultRuleSet_1.0
921340	Remote Command Execution: Shellshock (CVE-2014-4271)	Block	Enabled		RCE	DefaultRuleSet_1.0
921350	Remote Command Execution: Shellshock (CVE-2014-4271)	Block	Enabled		RCE	DefaultRuleSet_1.0
921360	Restricted File Upload Attempt	Block	Enabled		RCE	DefaultRuleSet_1.0
921370	PHP Injection Attack: PHP Open Tag Found	Block	Enabled		PHP	DefaultRuleSet_1.0



# Web Application Firewall Custom Rules



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

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

# 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

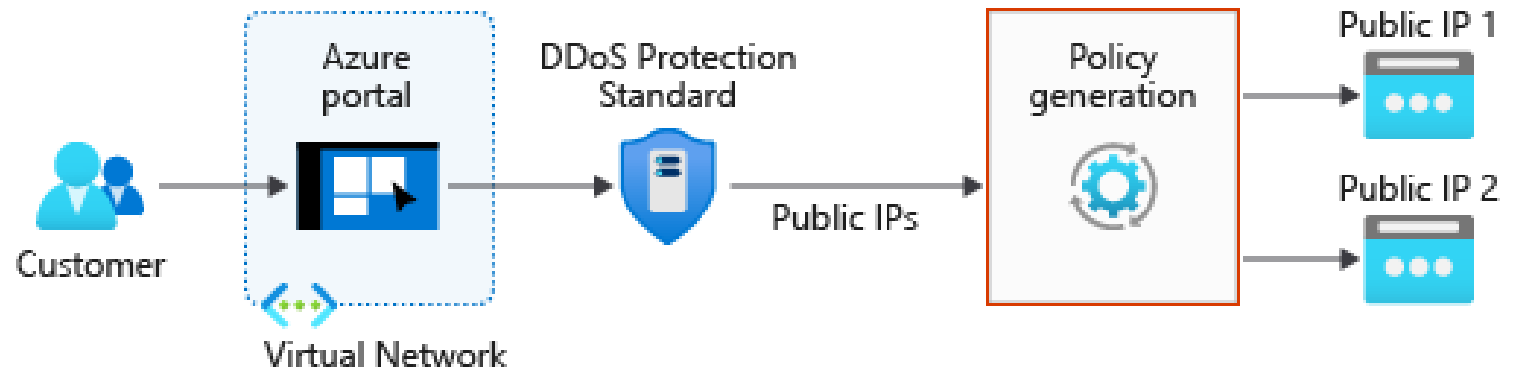
# Exercise: Configure DDoS Protection on a virtual network using the Azure portal



# 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



# 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

