Module 6: Design and implement network security

# Chapter 2: Get network security recommendations with Microsoft Defender for Cloud

## Network Security Principles

* Covers controls to secure/protect Azure networks:
  + Securing VNETs, establishing private connections, preventing external attacks, and securing DNS.

### NS-1: Establish network segmentation boundaries

* **Principle**: Insure VNET deployment aligns w/ enterprise segmentation strategy
  + Workload(s) that could incur higher risk should be in isolated VNETs.
    - **Examples**:
      * App storing highly sensitive data.
      * External-facing app accessible by public.
* **Azure Rec**:
  + Segmentation approach w/ VNETs/Subnets, so resources such as VMs are deployed into VNET within a network boundary.
    - Use NSGs to restrict/monitor traffic based on port, protocol, source IP, destination IP
    - Use ASGs to restrict/monitor traffic based on app’s structure (**ex**. Groups of VMs)

### NS-2: Secure cloud services with network controls

* **Principle**: establishing a private access point for the resources.
* **Azure Rec**:
  + Private Endpoints & VNET integration

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

* **Principle**: Deploy firewall to perform advanced filtering on network traffic to/from external networks. Also use Custom Routes to override default ones.
* **Azure Rec**:
  + Use Azure Firewall to provide traffic restriction (such as URL filtering) and/or central management over enterprise segments/spokes (**hub/spoke** topology).
  + Use User Def Routes (UDRs) to ensure traffic goes to desired route

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

* **Principle**: Use IDS/IPS to *inspect* network/payload traffic to/from your workload.
* **Azure Rec**: Azure Firewall’s IDPS capability on VNET control traffic to/from known malicious IPs.

### NS-5: Deploy DDOS protection

* **Azure Rec**: Enable DDoS standard protection plan on VNET

### NS-6: Deploy web application firewall

* **Azure Rec**: Azure WAF in Azure AG, Azure FD, and Azure CDN to protect apps, services and APIs

### NS-7: Simplify network security configuration

* **Azure Rec**: Simply/Manage NSG and Azure Firewall rules w/:
  + MS Defender for Cloud Adaptive Network Hardening
    - It recommends NSG hardening rules
  + Azure Firewall Manager centralizes firewall policy/route management of VNET.

### NS-8: Detect and disable insecure services and protocols

* **Azure Rec**: Azure Sentinel’s built-in Insecure Protocol Workbook to discover the use of insecure services and protocols

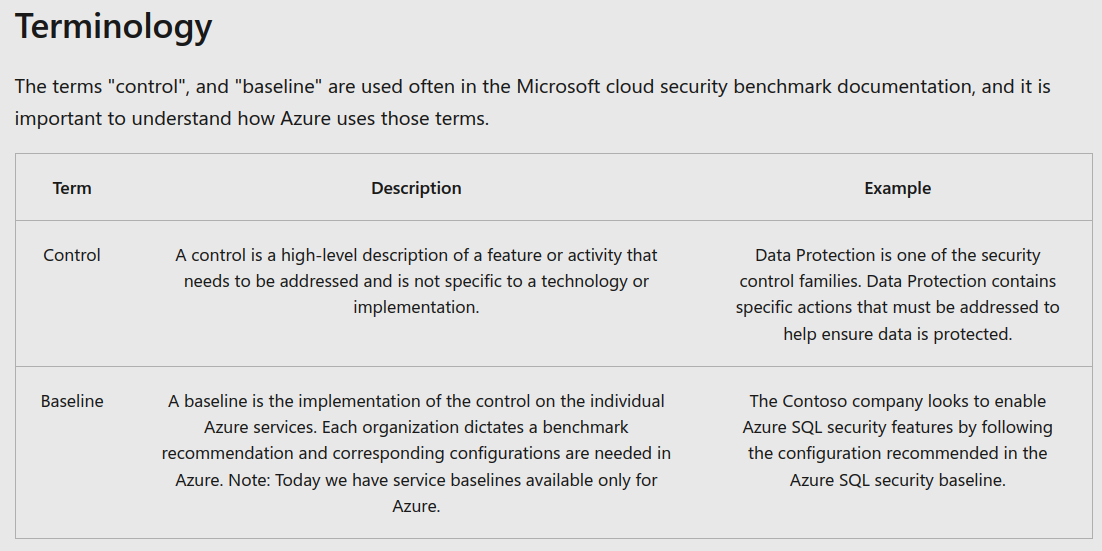
### NS-9: Connect on-premises or cloud network privately

* **Azure Rec**: Use private connections
  + Lightweight connectivity between S2S/P2S:
    - Azure VPN
  + Enterprise-level connection:
    - Azure ExpressRoute (or VWAN)
  + Connect 2+ Azure VNET:
    - Use VNET peering

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

* **Azure Rec**:
  + Azure recursive DNS/trusted external DNS server in workload’s DNS setup (**ex**. VM's OS or app)
  + Azure Private DNS for private DNS zone setup where DNS resolution is Internal to VNET
  + Azure Defender for DNS for advanced protection against:
    - Data exfiltration (DNS tunnelling)
    - Malware communicating w/ server
    - Phishing/crypto mining
    - DNS attacks

## Microsoft cloud security benchmark (MCSB)

* MCSB recommendations – two key types:
  + **Security controls**:
    - Each recommendation identifies stakeholders involved in planning, approval, or implementation of the benchmark.
  + **Service baselines**:
    - These apply the controls to *individual cloud services* to provide recommendations for that specific service’s security configuration.
  + 
* Refer to this for details on MS Defender Security Dashboard:
  + https://learn.microsoft.com/en-us/training/modules/design-implement-network-security-monitoring/2-secure-your-virtual-networks-azure-portal

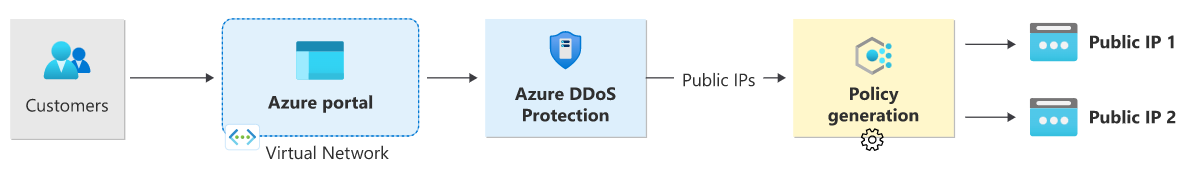
# Chapter 3: Deploy Azure DDoS Protection by using the Azure portal

* 2 Service Tiers for Azure DDoS:
  + **Basic**:
    - Automatically enabled on Azure platform w/ always-on traffic monitoring and real-time mitigation of common network-level attacks
  + **Standard**:
    - Protects resources in VNET including public IP addresses associated with VMs, LBs, and AGs.
    - DDoS Protection Standard is a paid service, design for services that are deployed in VNETs.
* Types of DDoS attacks
  + *Volumetric attacks –* flood network w/ high amounts of legitimate traffic (**ex**. UDP floods, amplification floods, spoofed-packet).
    - DDoS Protection Standard absorbs/scrubs the traffic w/ Azure's global network automatically.
  + *Protocol attacks –* render target inaccessible by exploiting layer 3 and layer 4 protocol stack (**ex**. SYN flood attacks, reflection attacks, etc).
    - Azure mitigates this by differentiating between malicious and legitimate traffic
  + *Resource (application) layer attacks –* target web app packets to disrupt the transmission of data (**ex**. HTTP protocol violations, SQL injection, cross-site scripting, etc.)
    - Azure Web Application Firewall + DDoS Protection Standard protects against this

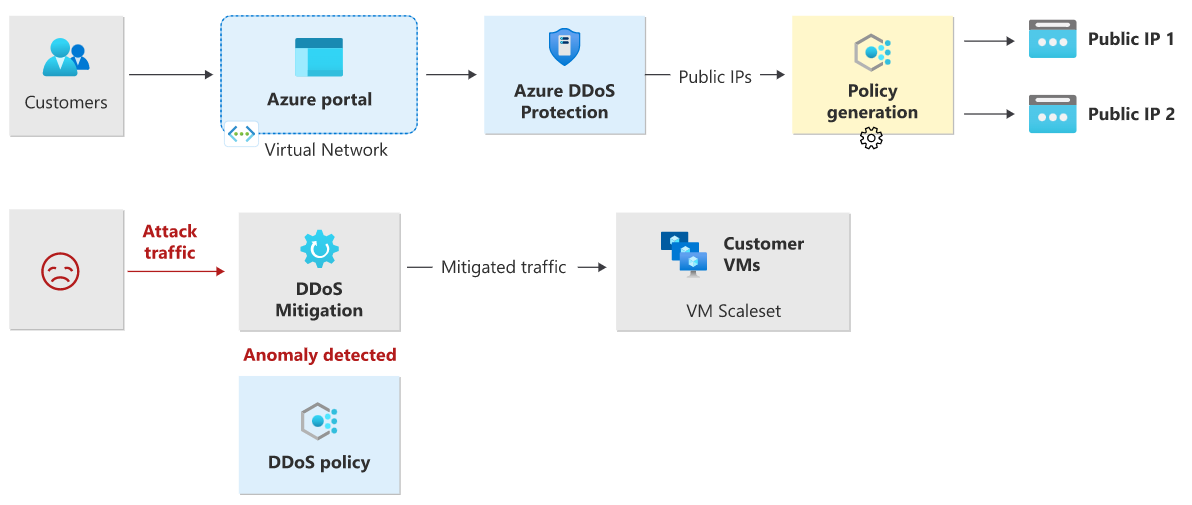
## Azure DDoS protection features

* **Natively integrated into Azure**
* **Turnkey protection**
* **Always-on traffic monitoring**
* **Adaptive tuning to traffic**
* **Attack analytics and detailed reports**
* **Attack metrics and alerts**
* **Multi-layered protection -** protects at network layer (Layer 3 and 4) w/ Azure WAF (Layer 7)

### Always-on traffic monitoring

* 
* When traffic threshold is exceeded, **DDoS mitigation auto-initiates** and checks:
  + Ensure packets aren't malformed.
  + Interact with client to stop potentially spoofed packets
  + Rate-limit packets if no other enforcement method can be performed.
* It then drops attack traffic while forwarding remaining traffic to intended destination

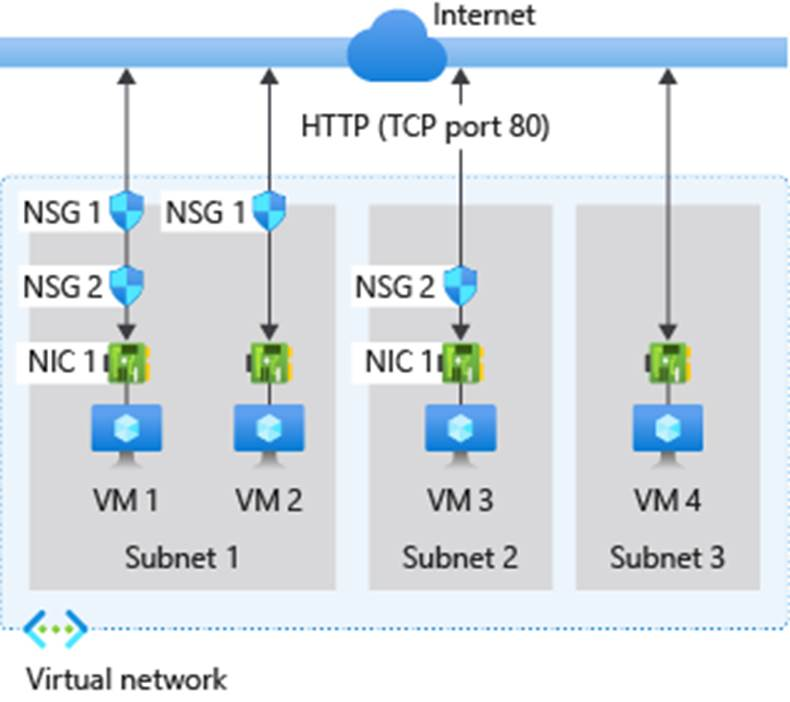
### Adaptive real-time tuning

* 
* Uses these two insights to adapt to attack traffic:
  + Auto-learning of per-customer traffic patterns for Layer 3 and 4.
  + Minimizing false positives, tho scale of Azure allows absorption of significant amount of traffic.

### Multi-layered protection

* Configure Azure WAF to secure web apps in conjunction with Azure DDoS Protection.

# Chapter 5: Deploy Network Security Groups by using the Azure portal

* **NSG**:
  + Link: https://learn.microsoft.com/en-us/training/modules/design-implement-network-security-monitoring/5-deploy-network-security-groups-by-using-the-azure-portal
  + 

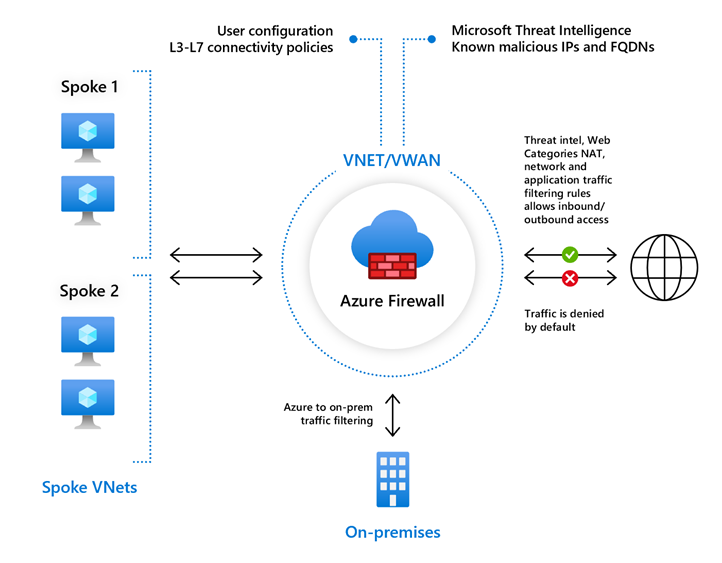
## Application Security Groups (ASG)

* ASG enables configuration of NSGs as a natural extension of an app’s structure, allowing you to group VMs and define NSG policies based on those groups.

## Filter network traffic with an NSG using the Azure portal

* Key stages to filter network traffic w/ an NSG are:
  + Create RGP
  + Create VNET
  + Create ASG (**ex**. MyAsgWebServers and MyAsgMgmtServers)
  + Create NSG
  + Associate NSG w/ a subnet
  + Create/Add security in/outbound rules to NSG
  + Create VMs
  + Associate NICs to an ASG
  + Test traffic filters by:
    - Attempt to connect to the management server VM using an RDP connection to verify connection to port 3389 (allowed inbound from the Internet to VM’s ASG)

# Chapter 6: Design and implement Azure Firewall

* Firewall protects Azure VNET resources:
  + 

## Azure Firewall features

* Built-in high availability (no LBs needed) & Unrestricted cloud scalability
* Application FQDN filtering rules
* Network traffic filtering rules
  + Centrally create allow/deny network filtering rules by source/destination IP address, port, and protocol.
* FQDN tags – **Allows well-known** Azure service network traffic through your firewall (ex. Windows Update tag)
* Service tags – **reps group of IP address** prefixes but you cannot create your own service tag (MS managed)
* Threat intelligence
* Outbound SNAT / Inbound DNAT support – All in/outbound VNET traffic IP addresses are translated to the Azure Firewall public IP (Source Network Address Translation (SNAT) or Destination Network Address Translation)
* Multiple public IP addresses
* Azure Monitor logging
* Forced tunnelling – route all Internet-bound traffic to a designated next hop (ex. Route to Virtual Appliance instead of Internet)
* Web categories (preview) – allow/deny user access to web site categories such as gambling websites, social media websites, etc.
* Certifications - Azure Firewall is Payment Card Industry (PCI), Service Organization Controls (SOC), International Organization for Standardization (ISO), and ICSA Labs compliant.

## Rule processing in Azure Firewall

### Method 1: Rule processing with classic rules

* Rule collections (RC) processed according to rule type in priority order, lower numbers to higher numbers from 100 to 65,000

### Method 2: Rule processing with Firewall Policy

* Rules are organized into RCs inside in RC Groups:
  + 3 Types of RCs (ordered by this priority):
    - DNAT (Destination Network Address Translation)
    - Network
    - Application
  + \*\*\*parent rules are processed first!

#### Outbound connectivity using net rules and app rules

* NET rules are applied in priority order before APP rules (all rules are terminating – if match is found no other rules are processed).

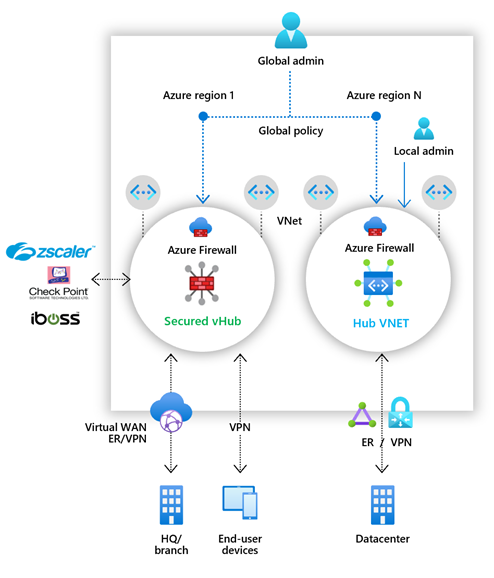
#### Inbound connectivity using DNAT rules and NET rules

* DNAT rules applied in priority before NET rules.
  + If match is found, an **implicit corresponding NET rule** to allow the translated traffic is added
* APP rules **aren't applied for inbound** connections (use WAF)

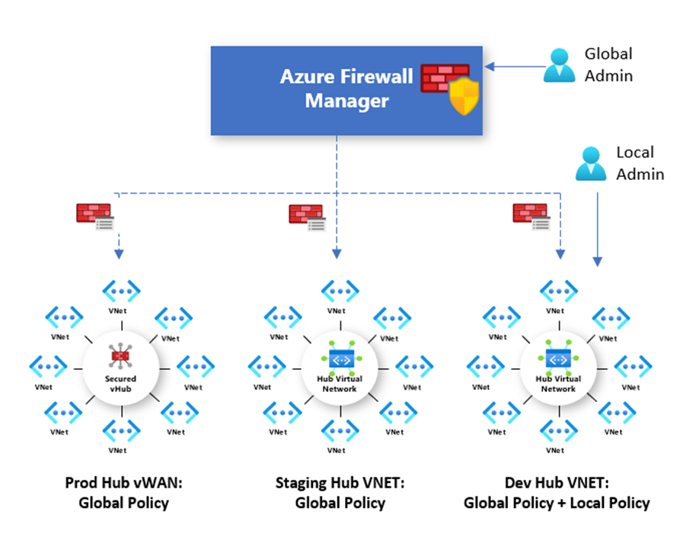
## Deploying and configuring Azure Firewall (AF)

* Steps to config Az Firewall:
  + Create RGP
  + Create VNET/subnets
    - Create VM in a subnet
  + Deploy the AF and policy to VNET
  + Create a default outbound route
    - Configure an APP rule
    - Configure a NET rule
    - Configure a Destination NAT (DNAT) rule

# Chapter 8: **Secure your networks with Azure Firewall Manager (FM)**

* Azure FM – security management service that provides central security policy and route management for cloud-based security perimeters.
  + 
* FM provides security management for 2 network arch types:
  + **Secured Virtual Hub –** any Azure vWAN Hub w/ security/routing policies associated with it.
  + **Hub Virtual Network –** any standard Azure VNET w/ security policies associated with it.

## Azure Firewall Manager features

* *Central Azure Firewall deployment* (centrally deploy/config multiple AF instances across diff regions and subs).
* *Hierarchical policies* (global and local)
  + Centrally manage AF policies across multiple secured VHUBs.
* *Integrate w/ third-party security-as-a-service providers for advanced security*
* *Centralized route management –* route traffic to secured hub to filter/log w/o using UDRs on spoke VNETs
* *Region availability across regions*
* 

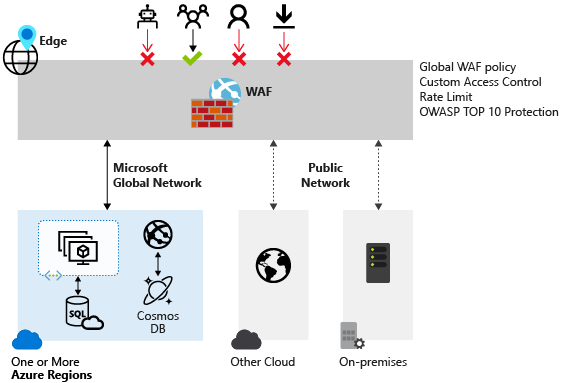
## Deploying Azure FM for Hub Virtual Networks

* Steps to deploy FM to Hub Virtual Networks:
  + **Create a firewall policy**
  + **Create hub and spoke architecture**
  + **Select security providers and associate firewall policy**.
  + **Configure User Defined Routes** to route traffic to your Hub VNET firewall.

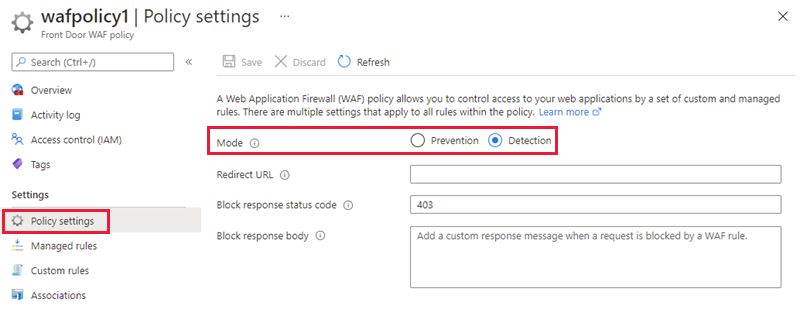
## Deploying Azure FM for Secured Virtual Hubs

* Steps to deploy FM to Secured VHUBs:
  + **Create your hub and spoke architecture**
  + **Select security providers**
  + **Create a firewall policy and associate it with your hub**
  + **Configure route settings to route traffic** to your Secured VHUB

# Chapter 10: Implement a Web Application Firewall (WAF) on Azure Front Door (FD)

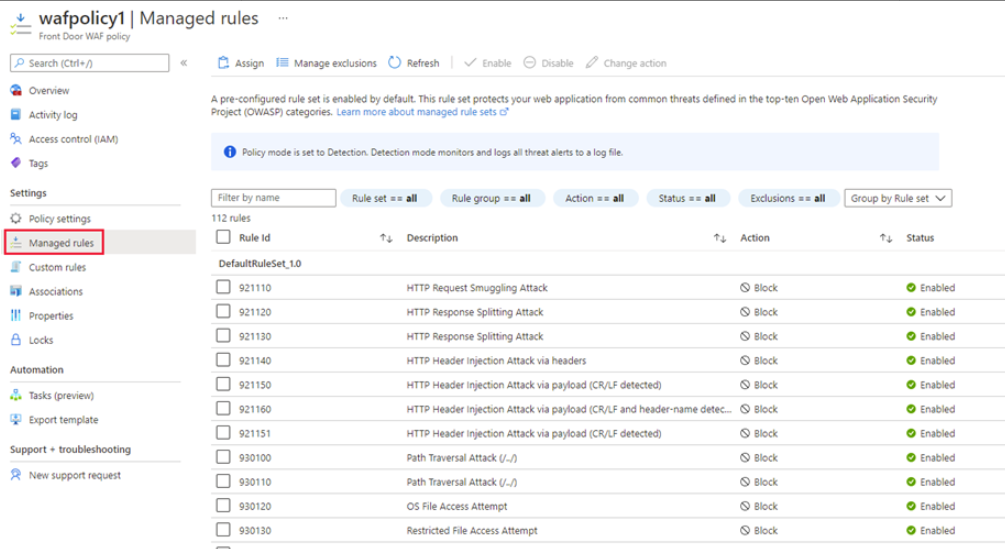
* WAF provides centralized protection of web apps:
  + 

## Web Application Firewall policy modes

* 
* **Detection** only logs requests that match WAF rules; **Prevention** blocks & logs requests from Default Rule Set (DRS)

## WAF Default Rule Set rule groups and rules

### Azure-managed rule

* These rules provide easy way to deploy protection against a common set of security 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
* 

### Custom rules

* Custom WAF rule consists of a priority number, rule type, match conditions, and an action
  + 2 Types:
    - Match rule controls access based on a set of matching conditions
    - 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

* Steps to create WAF policy on Azure FD:
  + Create a WAF policy
  + Associate the WAF policy with a FD profile
  + Configure WAF policy settings and rules (optional)
    - Configure policy settings such as the Mode (*Prevention or Detection*) and configure **managed rules and custom** rules.