**Existing WAF Gateway V2, no Frontdoor = WAF Gateway V2 hardening, implement new Frontdoor**

**Required Resources:**

* App Gateway.
* If using custom DNS , need key vault secret name.
* Backend Pool.
* Routing rules to harden.
* Custom Rules.
* Frontdoor WAF Policy.

**Requirement for Creation of Frontdoor:**

* Basic Information.
* Add Frontend Host.
* Add backend pools.

-Select backend host type as "App Gateway".

-Desired Http & Https Ports.

-Priority and Weight are 1 and 50 by default, we can change the Priority and Weight of backend as per our requirement.

* Now Add Health Probe.
* Add Load Balancing setting.

-add Sample size & Latency details.

* Create Route Rules.

-On Basic:- Name ,Frontend host, Backend pool, Accepted Protocols,

Advanced: Forwarding Protocol, URL Rewrite, caching.

**After App Gateway is created(for WAF Rules):**

**Step 1:**

* All Services > Web Application Firewall > Create
* Fill Basic details.

**Step 2:**

* Select Policy Settings.
* There are two modes Prevention and Detection.
* Prevention:

This mode of firewall is recommended as it blocks all the malicious requests directly and throws 403-Forbidden error message in response to that request.

* Detection:

This mode does not block any requests but logs all malicious requests to log analytics and can be seen using log search query. This mode can be used while developing to find if a genuine/valid request is getting blocked due to coding (OWASP) incompatibility and later resolve it.

**Step 3:**

* Select Managed Rules
* Select DefaultRuleSet\_1.0 & BotProtection\_preview-0.1 for malicious attacks and bot protection(select more according to need ).

**Step 4:**

* Add Custom Rules accordingly.

**Step 5:**

* Select Association.
* Add frontend host

**Step 6:** Testing the deployment

* Click on hostname.