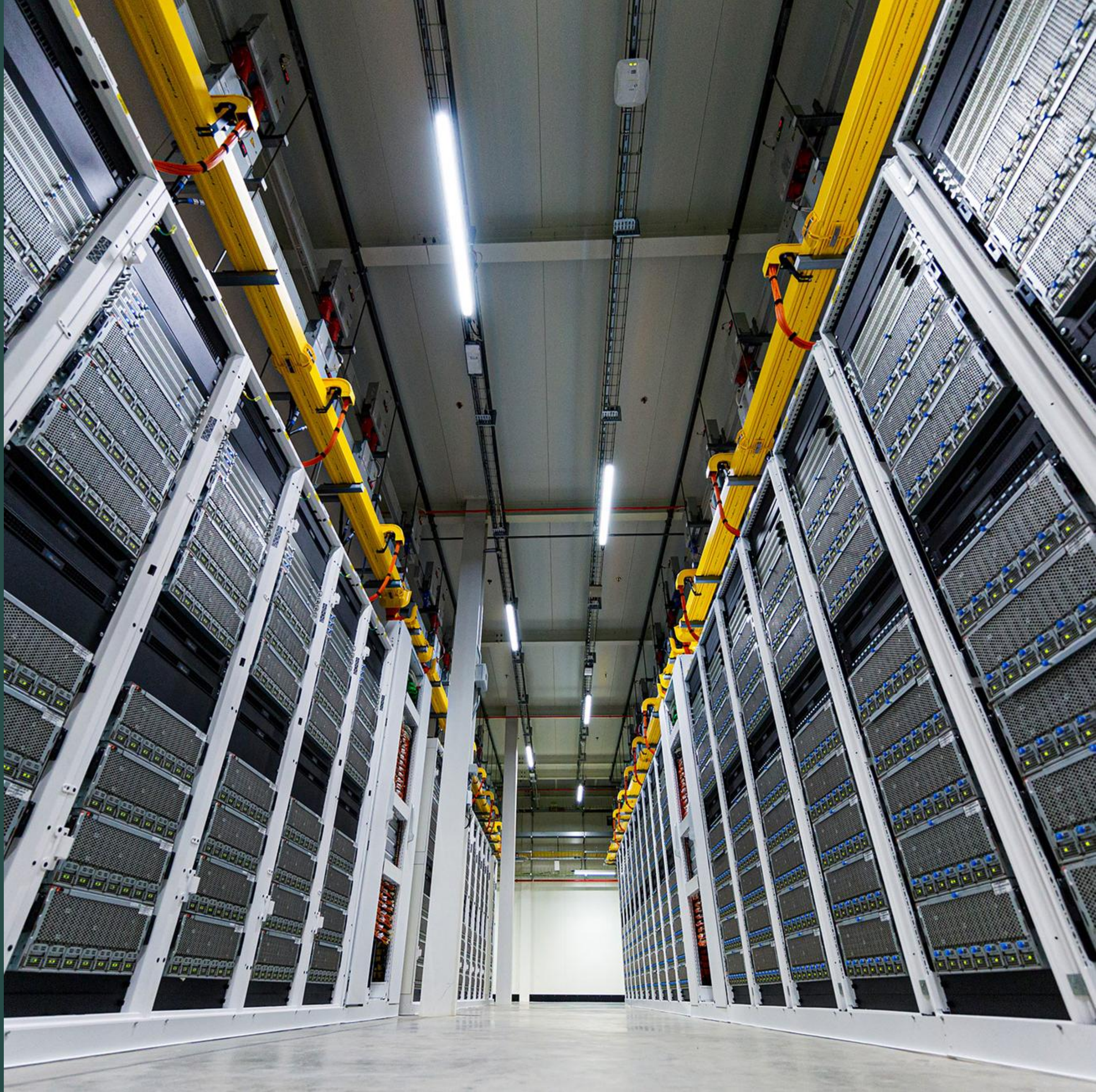
Microsoft

Azure Application Gateway

Taoufik AIT ALLA
Cloud Solution Architect



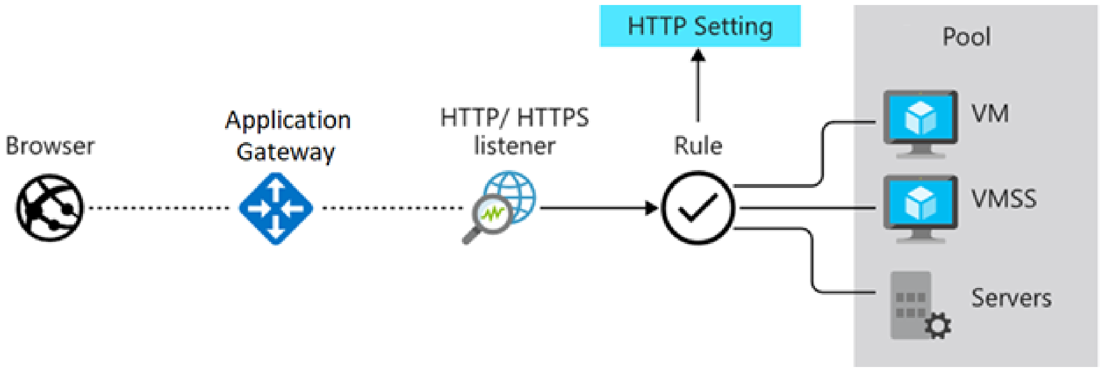
Agenda

- Azure Application Gateway
- Azure Web Application Firewall
- Monitoring and Alerting

What is Application Gateway

What is Application Gateway

- Key Components



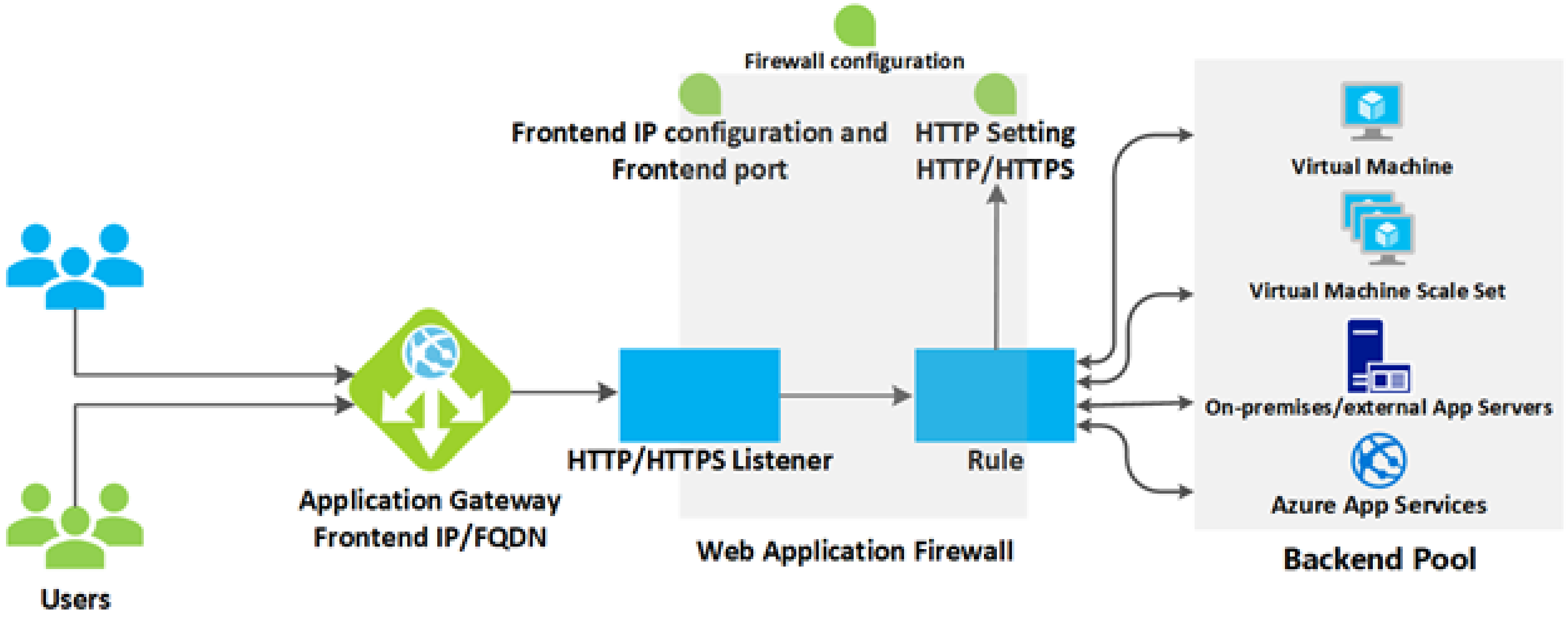
- **Core Features**

- **Traffic Management**
  - HTTP load balancing
  - Round-robin distribution
  - Session stickiness
  - E-commerce optimization
- **Security**
  - Web Application Firewall (WAF)
  - TLS/SSL encryption
  - End-to-end request encryption
- **Protocol Support**
  - HTTP, HTTPS
  - HTTP/2
  - WebSocket
- **Advanced Capabilities**
  - Autoscaling
  - Connection draining
  - Planned maintenance support

How Azure Application Gateway works ?

Key Components

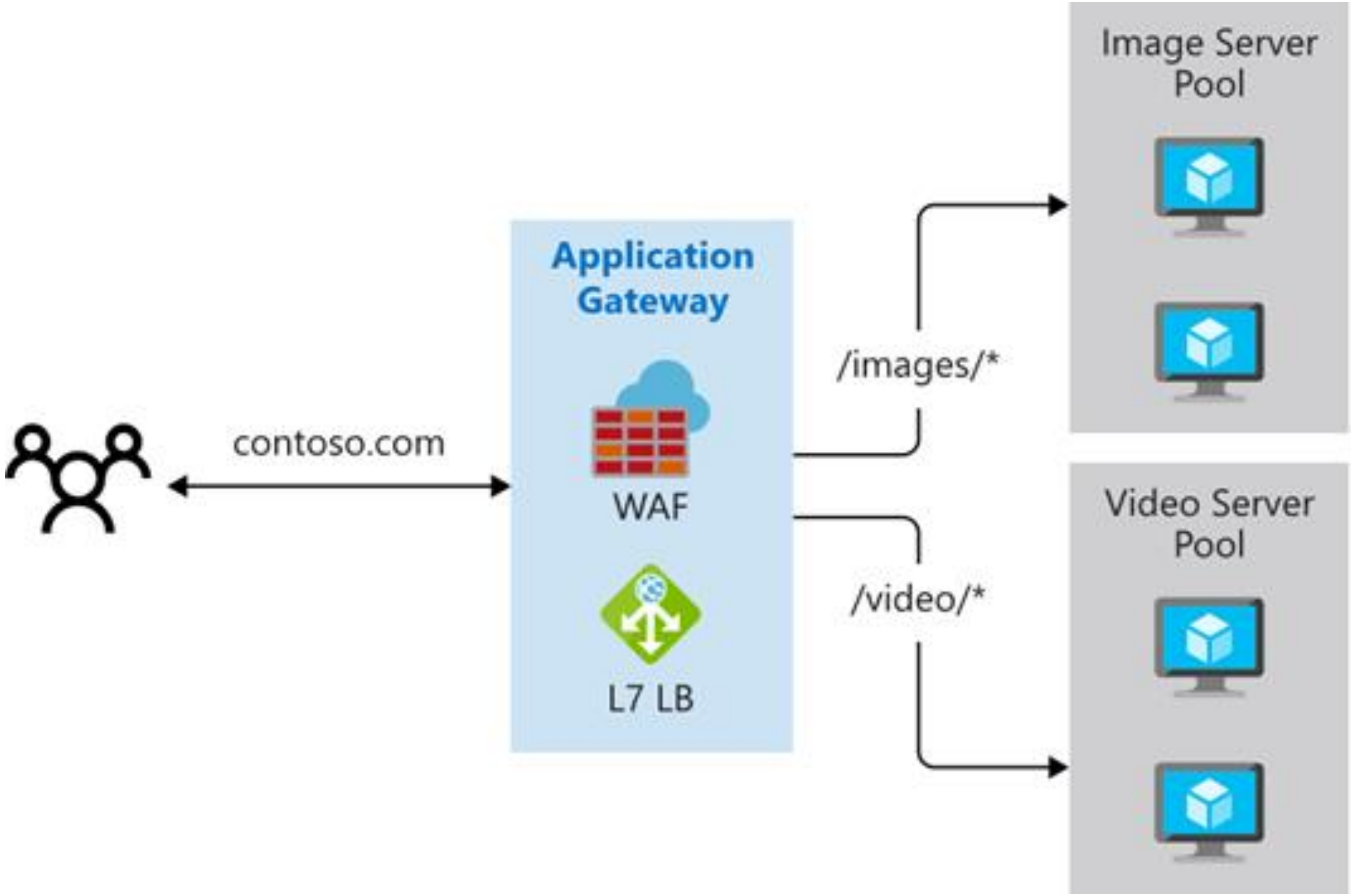
- Frontend Configuration
- Listeners
- Routing Rules
- Backend Pool
- Web Application Firewall



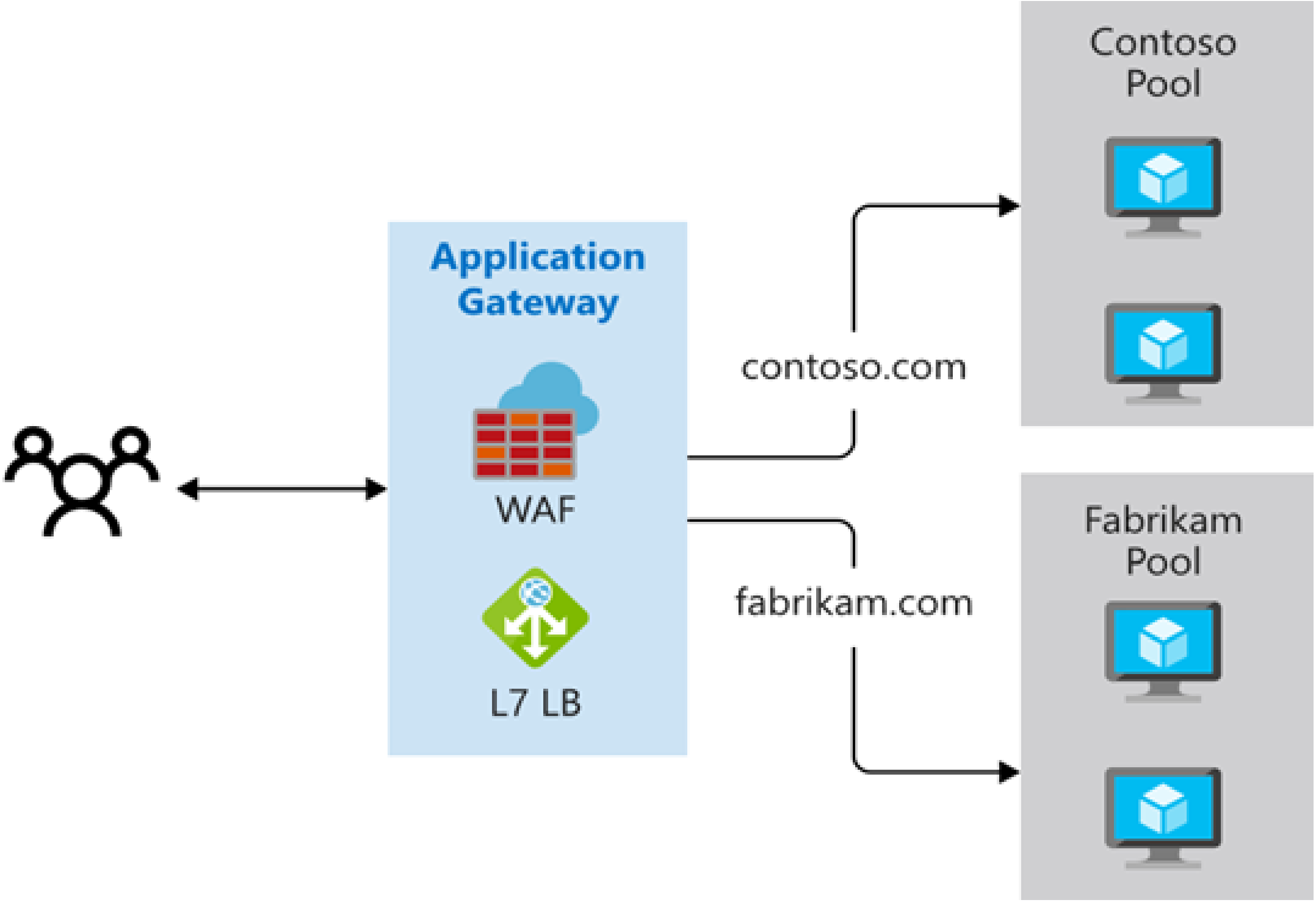
Setup Requirements

- To be able to create an azure application, the requirements are:
- A virtual network and subnet in which the Application Gateway will be deployed
- Public IP Address (if applicable)
- Certificates for SSL/TLS
- Public domain name (if applicable)
- CNAME DNS entry (if applicable)
- WAF Policy (if applicable)

Application Gateway routing – Path Based Routing



Application Gateway routing – Multiple-site routing



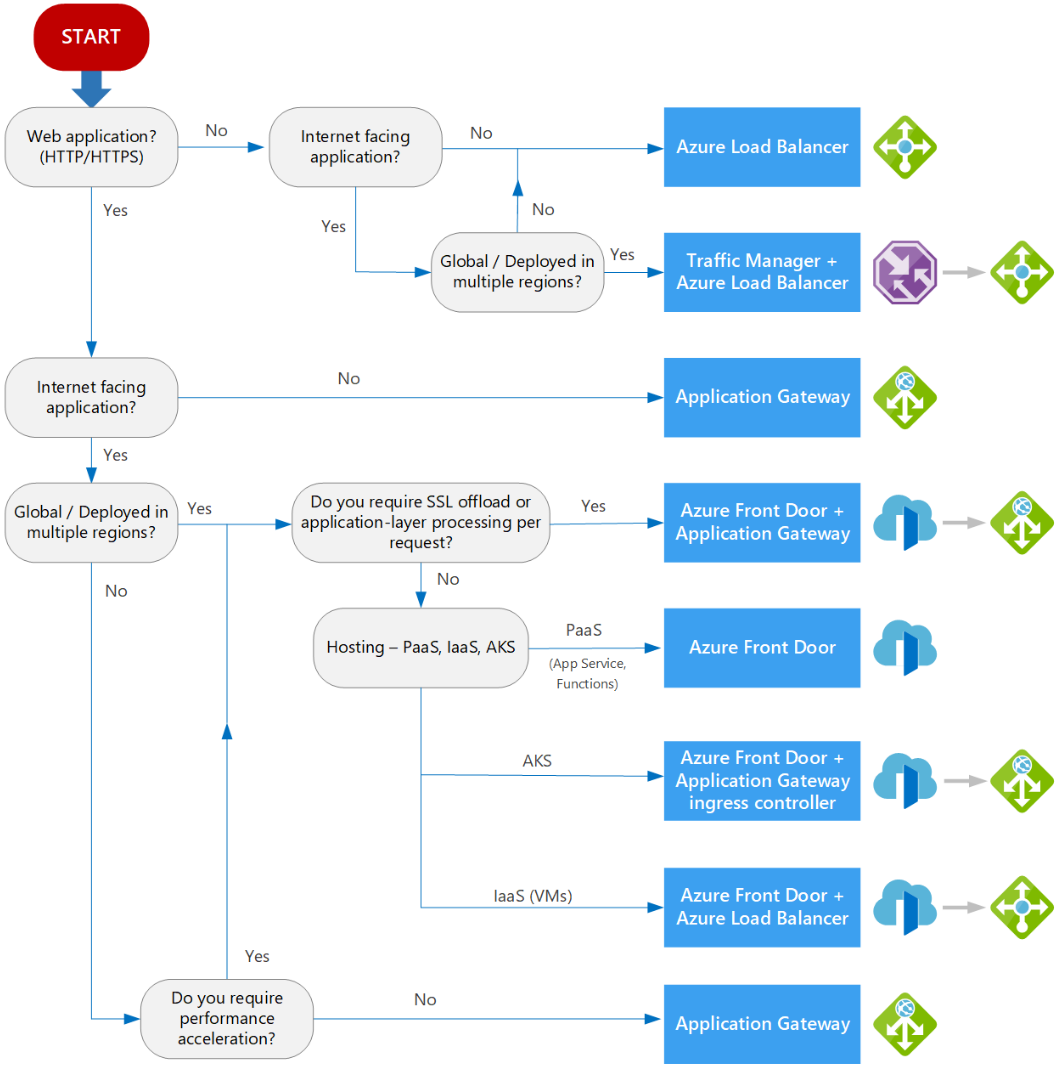
When to Use Azure Application Gateway

Criteria	Use Application Gateway	Don't Use Application Gateway	Alternative Solution
Traffic Volume	• High traffic web applications • Multiple backend servers • Complex routing needs	• Low traffic applications • Single backend server • Simple infrastructure	Basic web hosting
Load Balancing Needs	• Layer 7 (HTTP/HTTPS) routing required • Health probe monitoring needed • Session affinity required	• Basic load balancing only • No routing complexity • No session management	Azure Load Balancer
Security Requirements	• WAF protection needed • SSL/TLS termination required • Protection against XSS and SQL injection	• Basic security sufficient • No specific web threats • No SSL offloading needed	Network Security Groups
Geographic Distribution	• Regional distribution • Hybrid deployments (Azure + On-premises)	• Global distribution needed • Multi-region deployment • DNS-based routing	Azure Front Door Traffic Manager
Performance Optimization	• CPU offloading needed • SSL termination required • Backend server optimization	• No performance issues • Simple architecture • Low resource usage	Standard hosting

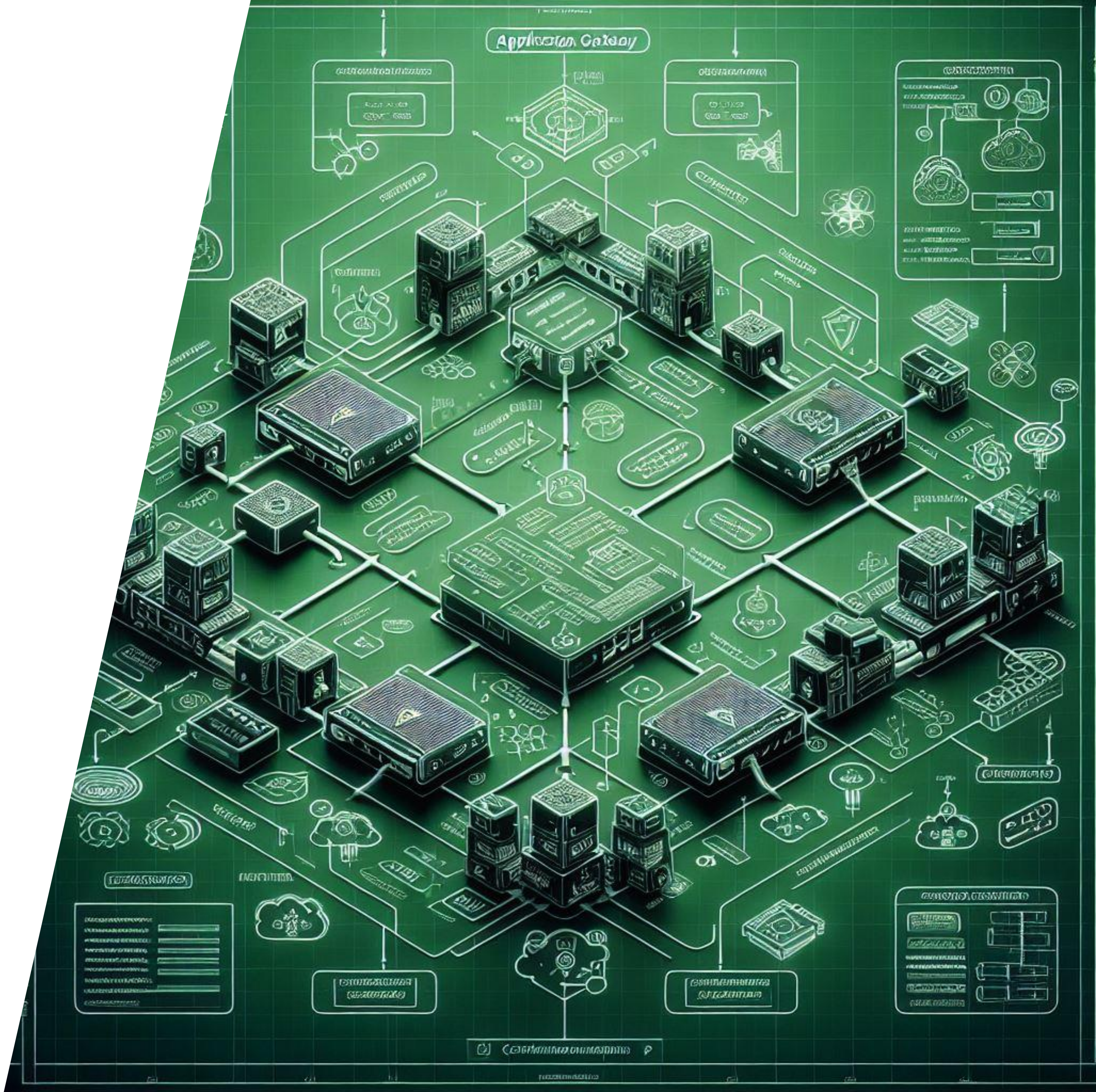
Alternatives Solutions

Service	Best For	Key Features
Front Door	Global applications	• Global load balancing • Site acceleration • Multi-region deployments
Traffic Manager	DNS-based routing	• DNS load balancing • Global availability • Slower failover
Load Balancer	Network load balancing	• Layer 4 balancing • Ultra-low latency • TCP/UDP protocols

Front Door vs App Gateway


START
Web application? (HTTP/HTTPS)
No
Internet facing application?
No
Azure Load Balancer
Yes
No
Global / Deployed in multiple regions?
Yes
Traffic Manager + Azure Load Balancer
Yes
Internet facing application?
No
Application Gateway
Yes
Global / Deployed in multiple regions?
Yes
Do you require SSL offload or application-layer processing per request?
Yes
Azure Front Door + Application Gateway
No
Hosting – PaaS, IaaS, AKS
PaaS
(App Service, Functions)
Azure Front Door
AKS
Azure Front Door + Application Gateway ingress controller
IaaS (VMs)
Azure Front Door + Azure Load Balancer
No
Yes
Do you require performance acceleration?
No
Application Gateway

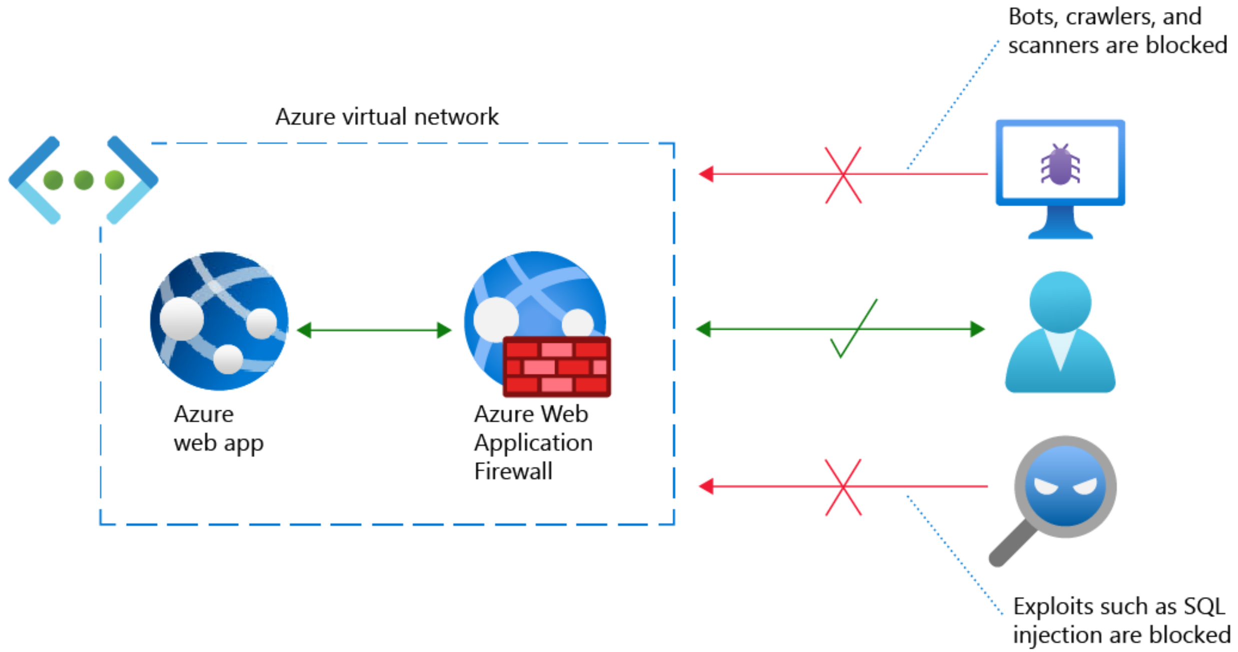
Demo



Azure Web Application Firewall

What is Azure Web Application Firewall

Key Components


Bots, crawlers, and scanners are blocked
Azure virtual network
Azure web app
Azure Web Application Firewall
Exploits such as SQL injection are blocked

Core Features

Instant Protection

- Deployment in minutes
- No security code required
- Centralized protection for Azure-hosted apps

Threat Prevention

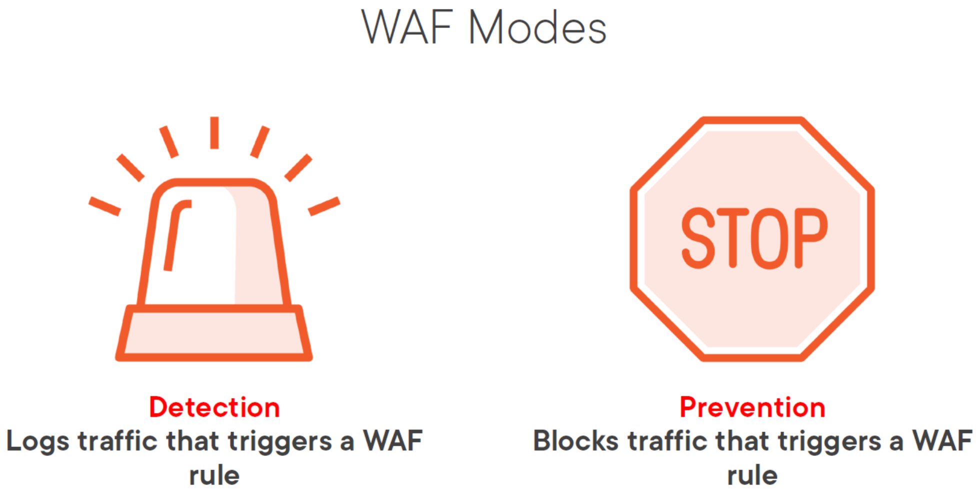
- Common Attack Protection:
  - SQL Injection
  - Cross-site Scripting (XSS)
  - Local/Remote File Inclusion
  - HTTP/HTTPS Floods
- Bot Management:
  - Blocks malicious bots
  - Filters automated scanners
  - Prevents crawlers
  - Real-time threat monitoring

Key features of Azure Web Application Firewall

- **Managed rules**, to protect against common vulnerabilities and exploits
- **Custom rules**, to control access to your web applications based on your compliance and security standard
  - **Exclusion lists**
  - **Geo-filtering**
  - **Bot Protection**
  - **IP restriction**
  - **Monitor and logging**
- **WAF mode**, can be configured to run in 2 modes:
  - **Detection mode:** Monitors and logs all threat alerts
  - **Prevention mode:** Blocks intrusions and attacks that the rules detect

How Azure Web Application Firewall works?

1. **Enable Managed rules** to protect against common vulnerabilities and exploits
2. **Add Custom rules**, to be aligned with your security standard
3. **Tuning,** enable or disable specific managed rules
4. **WAF mode**
   1. **Activate Detection mode on stagging environment for a short period to** monitor and logs all threat alerts
   2. **Switch to Prevention mode** to blocks intrusions and attacks that the rules detect



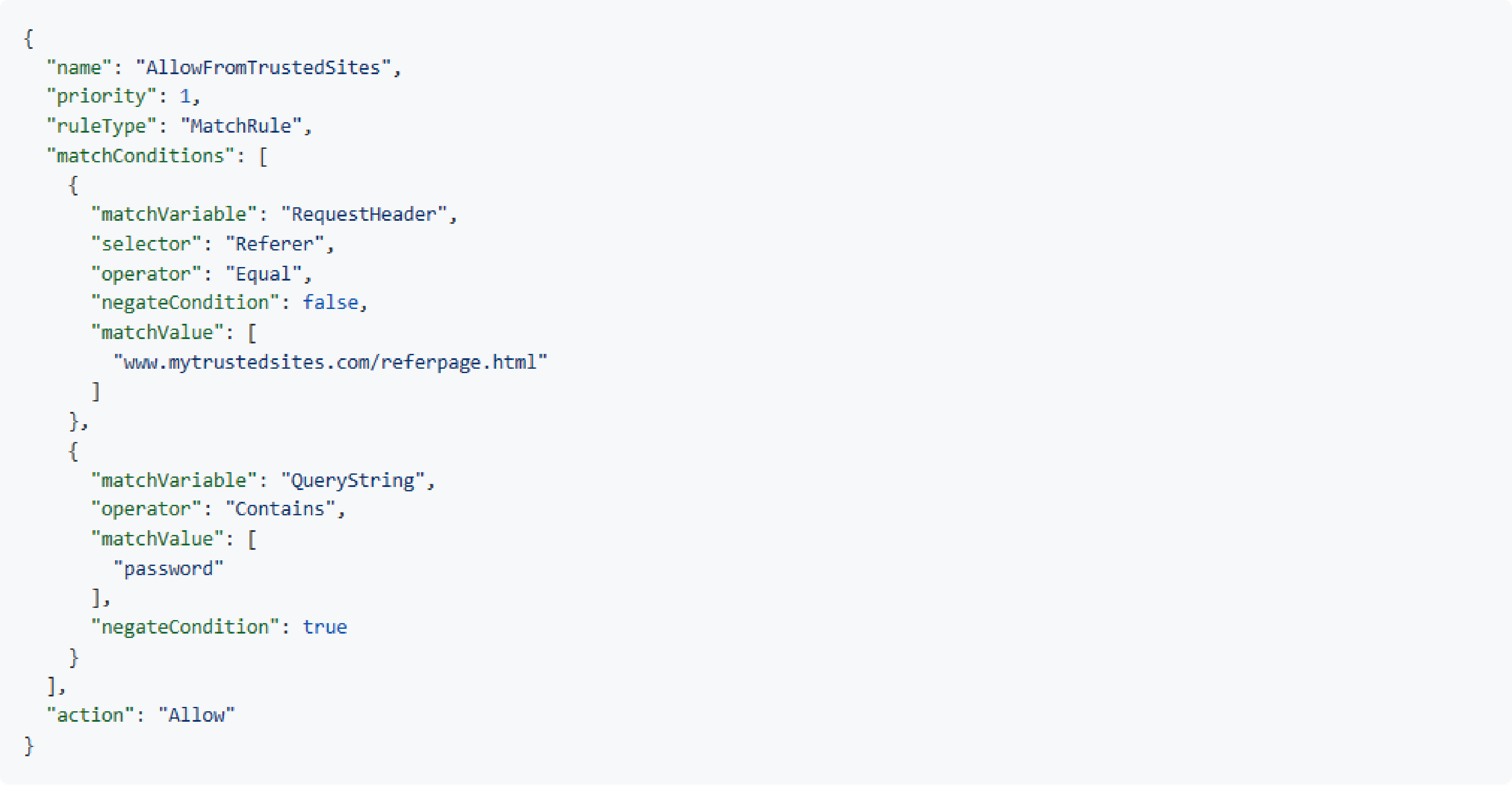
WAF Modes

Detection
Logs traffic that triggers a WAF rule

Prevention
Blocks traffic that triggers a WAF rule

WAF configuration and Best practices

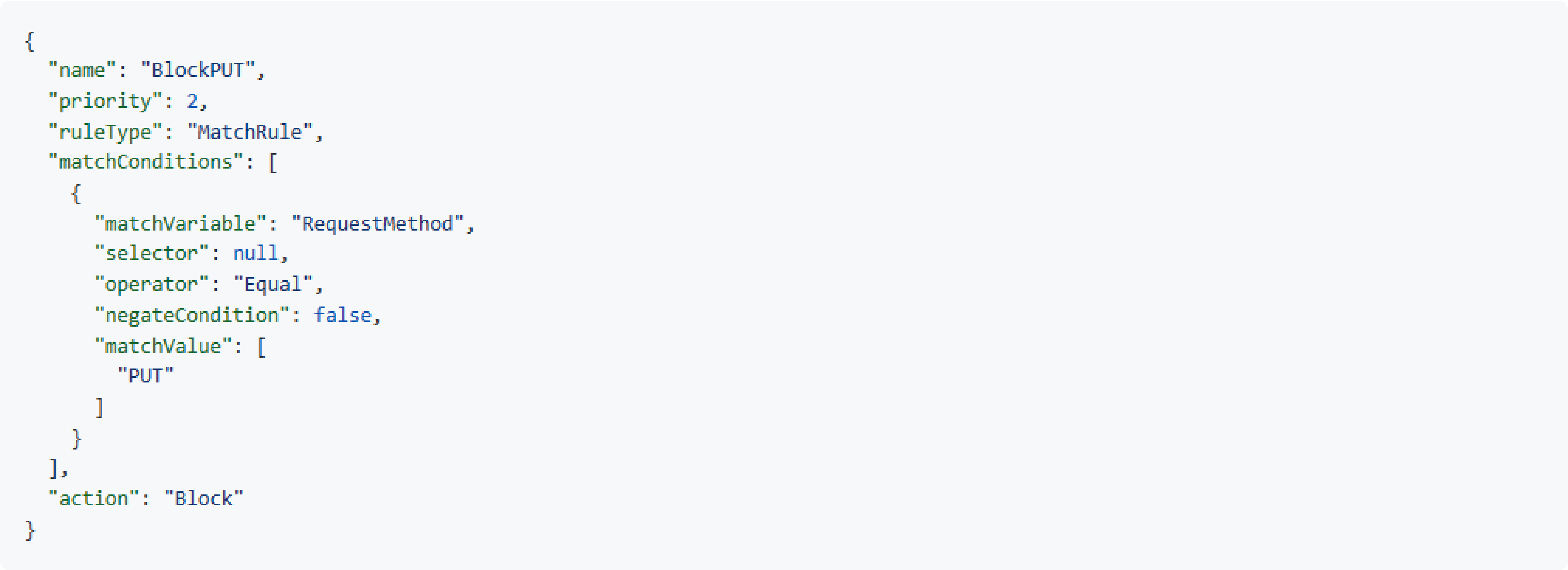
Match based on HTTP request parameters



```json
{
  "name": "AllowFromTrustedSites",
  "priority": 1,
  "ruleType": "MatchRule",
  "matchConditions": [
    {
      "matchVariable": "RequestHeader",
      "selector": "Referer",
      "operator": "Equal",
      "negateCondition": false,
      "matchValue": [
        "www.mytrustedsites.com/referpage.html"
      ]
    },
    {
      "matchVariable": "QueryString",
      "operator": "Contains",
      "matchValue": [
        "password"
      ],
      "negateCondition": true
    }
  ],
  "action": "Allow"
}
```

WAF configuration and Best practices

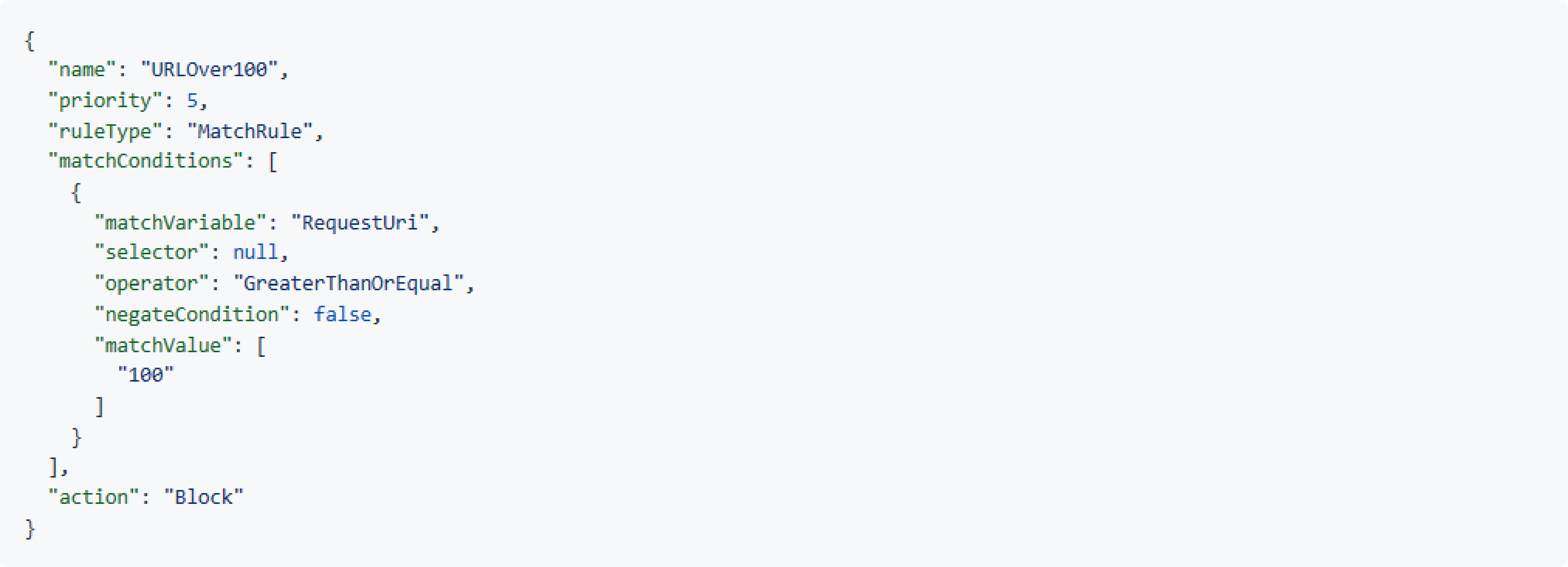
Block HTTP PUT requests



```json
{
  "name": "BlockPUT",
  "priority": 2,
  "ruleType": "MatchRule",
  "matchConditions": [
    {
      "matchVariable": "RequestMethod",
      "selector": null,
      "operator": "Equal",
      "negateCondition": false,
      "matchValue": [
        "PUT"
      ]
    }
  ],
  "action": "Block"
}
```

WAF configuration and Best practices

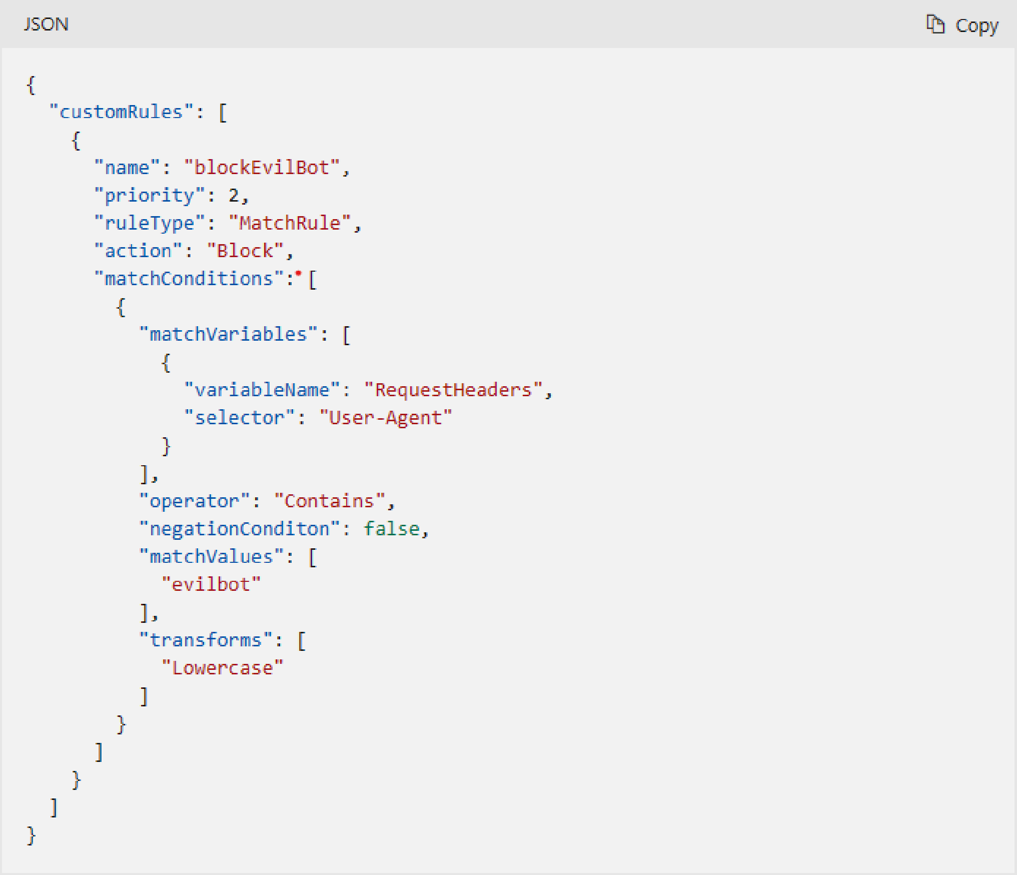
Size constraint



```
{
  "name": "URLOver100",
  "priority": 5,
  "ruleType": "MatchRule",
  "matchConditions": [
    {
      "matchVariable": "RequestUri",
      "selector": null,
      "operator": "GreaterThanOrEqual",
      "negateCondition": false,
      "matchValue": [
        "100"
      ]
    }
  ],
  "action": "Block"
}
```

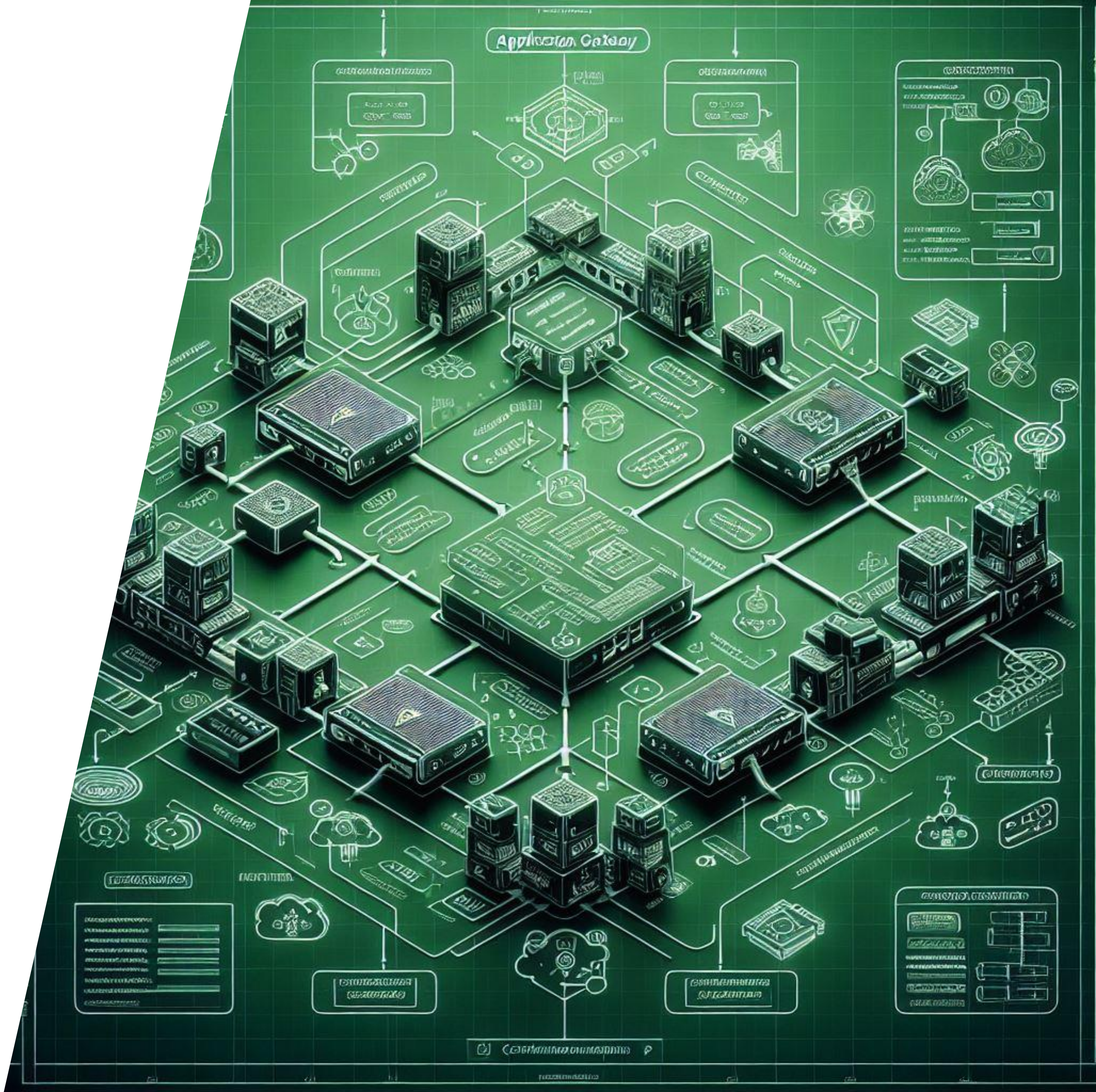
WAF configuration and Best practices

Block **bot named *evilbot***



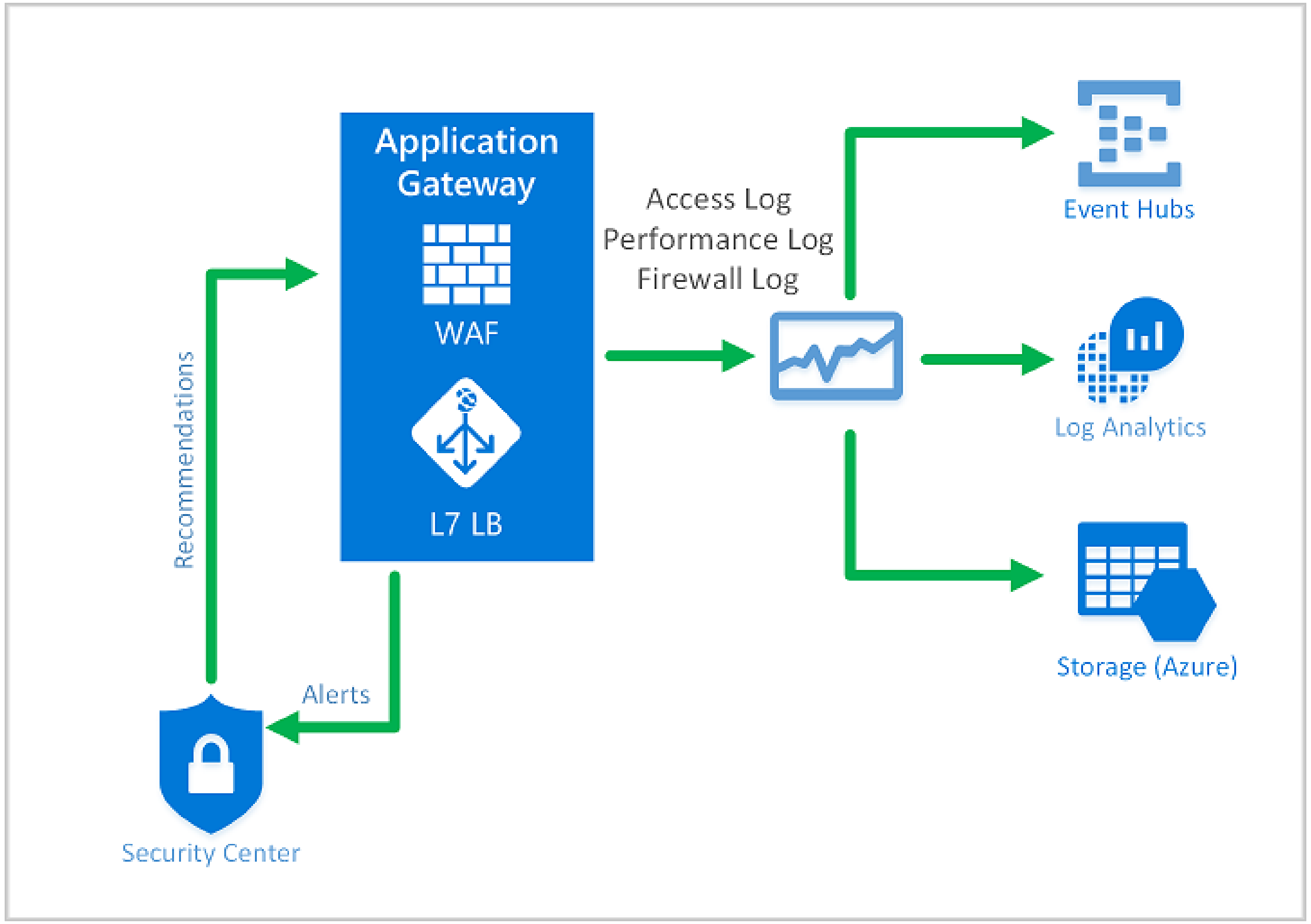
```json
{
  "customRules": [
    {
      "name": "blockEvilBot",
      "priority": 2,
      "ruleType": "MatchRule",
      "action": "Block",
      "matchConditions": [
        {
          "matchVariables": [
            {
              "variableName": "RequestHeaders",
              "selector": "User-Agent"
            }
          ],
          "operator": "Contains",
          "negationConditon": false,
          "matchValues": [
            "evilbot"
          ],
          "transforms": [
            "Lowercase"
          ]
        }
      ]
    }
  ]
}
```

Demo



Monitoring and Alerting

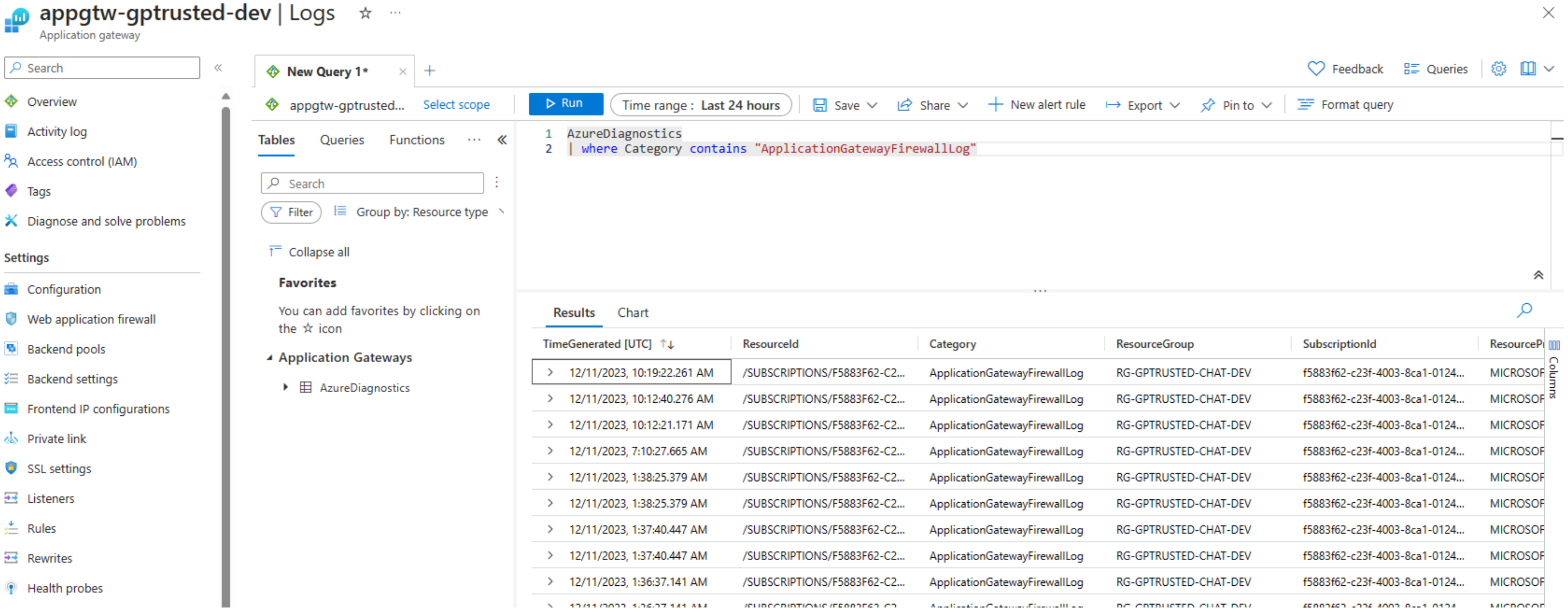
Monitoring and logging



Best practices: enable Diagnostic settings to send logs and metrics to Log analytics workspace

WAF monitoring

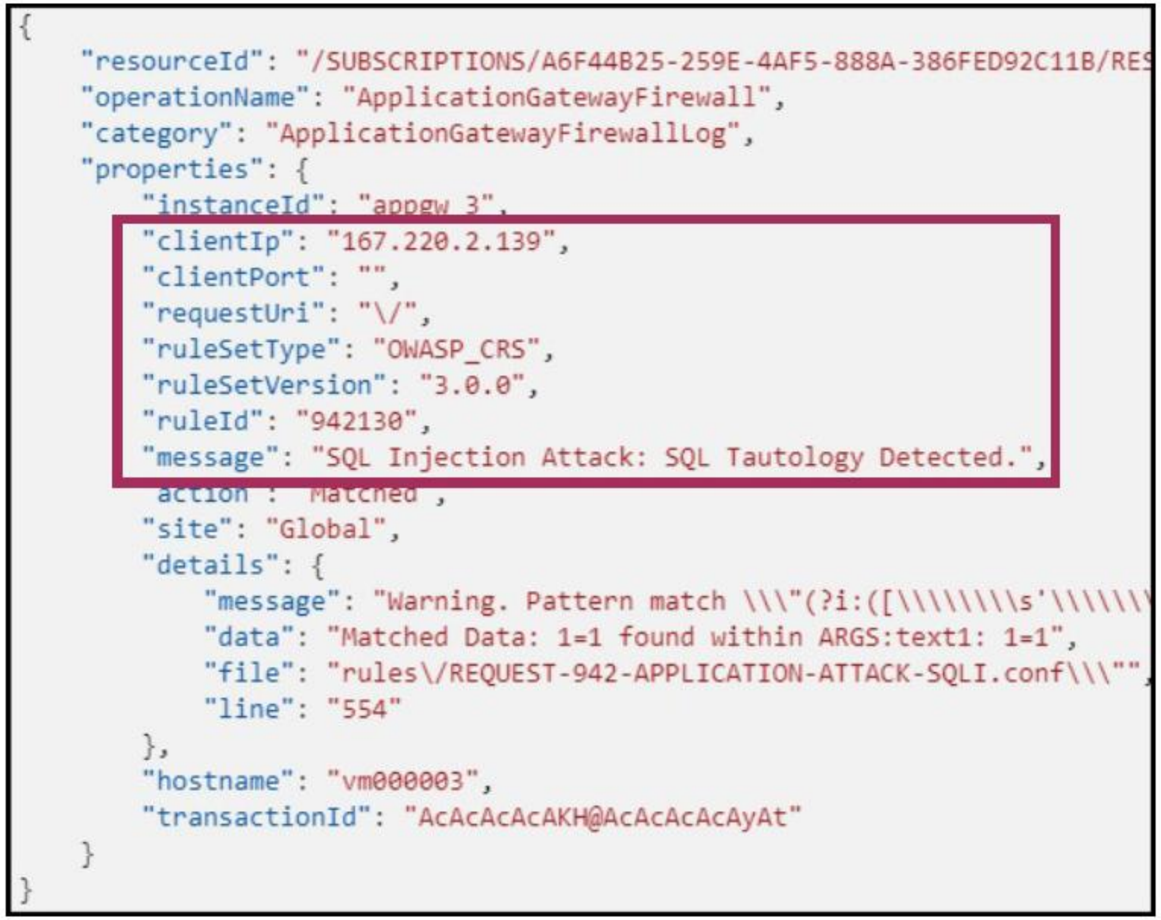
- The WAF logs are available under the AzureDiagnostics categories
  - “ApplicationGatewayAccessLog”
  - “ApplicationGatewayFirewallLog”



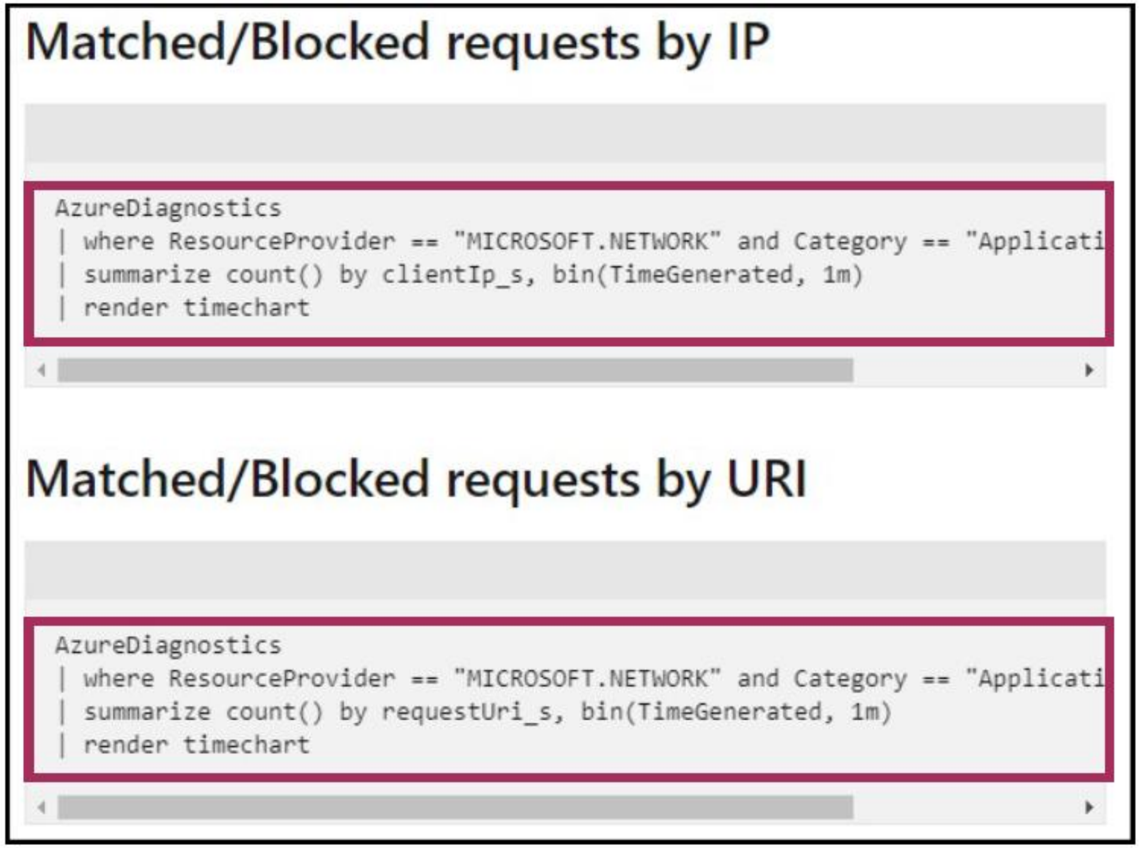
```
AzureDiagnostics
| where Category contains "ApplicationGatewayFirewallLog"
```

TimeGenerated [UTC]	ResourceId	Category	ResourceGroup	SubscriptionId	ResourceP
12/11/2023, 10:19:22.261 AM	/SUBSCRIPTIONS/F5883F62-C2...	ApplicationGatewayFirewallLog	RG-GPTRUSTED-CHAT-DEV	f5883f62-c23f-4003-8ca1-0124...	MICROSOF
12/11/2023, 10:12:40.276 AM	/SUBSCRIPTIONS/F5883F62-C2...	ApplicationGatewayFirewallLog	RG-GPTRUSTED-CHAT-DEV	f5883f62-c23f-4003-8ca1-0124...	MICROSOF
12/11/2023, 10:12:21.171 AM	/SUBSCRIPTIONS/F5883F62-C2...	ApplicationGatewayFirewallLog	RG-GPTRUSTED-CHAT-DEV	f5883f62-c23f-4003-8ca1-0124...	MICROSOF
12/11/2023, 7:10:27.665 AM	/SUBSCRIPTIONS/F5883F62-C2...	ApplicationGatewayFirewallLog	RG-GPTRUSTED-CHAT-DEV	f5883f62-c23f-4003-8ca1-0124...	MICROSOF
12/11/2023, 1:38:25.379 AM	/SUBSCRIPTIONS/F5883F62-C2...	ApplicationGatewayFirewallLog	RG-GPTRUSTED-CHAT-DEV	f5883f62-c23f-4003-8ca1-0124...	MICROSOF
12/11/2023, 1:38:25.379 AM	/SUBSCRIPTIONS/F5883F62-C2...	ApplicationGatewayFirewallLog	RG-GPTRUSTED-CHAT-DEV	f5883f62-c23f-4003-8ca1-0124...	MICROSOF
12/11/2023, 1:37:40.447 AM	/SUBSCRIPTIONS/F5883F62-C2...	ApplicationGatewayFirewallLog	RG-GPTRUSTED-CHAT-DEV	f5883f62-c23f-4003-8ca1-0124...	MICROSOF
12/11/2023, 1:37:40.447 AM	/SUBSCRIPTIONS/F5883F62-C2...	ApplicationGatewayFirewallLog	RG-GPTRUSTED-CHAT-DEV	f5883f62-c23f-4003-8ca1-0124...	MICROSOF
12/11/2023, 1:36:37.141 AM	/SUBSCRIPTIONS/F5883F62-C2...	ApplicationGatewayFirewallLog	RG-GPTRUSTED-CHAT-DEV	f5883f62-c23f-4003-8ca1-0124...	MICROSOF
12/11/2023, 1:36:37.141 AM	/SUBSCRIPTIONS/F5883F62-C2...	ApplicationGatewayFirewallLog	RG-GPTRUSTED-CHAT-DEV	f5883f62-c23f-4003-8ca1-0124...	MICROSOF

WAF logs



```
{
    "resourceId": "/SUBSCRIPTIONS/A6F44B25-259E-4AF5-888A-386FED92C11B/RES
    "operationName": "ApplicationGatewayFirewall",
    "category": "ApplicationGatewayFirewallLog",
    "properties": {
        "instanceId": "appgw_3",
        "clientIp": "167.220.2.139",
        "clientPort": "",
        "requestUri": "\/",
        "ruleSetType": "OWASP_CRS",
        "ruleSetVersion": "3.0.0",
        "ruleId": "942130",
        "message": "SQL Injection Attack: SQL Tautology Detected.",
        "action": "Matched",
        "site": "Global",
        "details": {
            "message": "Warning. Pattern match \\\"(?i:([\\\\\\\\\s'\\\\\\
            "data": "Matched Data: 1=1 found within ARGS:text1: 1=1",
            "file": "rules\/REQUEST-942-APPLICATION-ATTACK-SQLI.conf\\\"",
            "line": "554"
        },
        "hostname": "vm000003",
        "transactionId": "AcAcAcAcAKH@AcAcAcAcAyAt"
    }
}
```



Matched/Blocked requests by IP

```
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.NETWORK" and Category == "Applicati
| summarize count() by clientIp_s, bin(TimeGenerated, 1m)
| render timechart
```

Matched/Blocked requests by URI

```
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.NETWORK" and Category == "Applicati
| summarize count() by requestUri_s, bin(TimeGenerated, 1m)
| render timechart
```

Alerts

- Enable Diagnostic settings on the resource to be monitored
- Create a Kusto query and verify the result
- Create a new rule base on the previous Kusto query
- Configure the alert to be trigged based on specific condition
- Configure action groups to notify appropriate people when alert is fired

Demo