**APPLICATION GATEWAY**

**INDEX**

1. **The new v2 SKU enhancements**
2. **FEATURE COMPARISON BETWEEN V1 SKU AND V2 SKU**
3. **limitations** **in v2 SKU from v1 SKU**
4. **WAF Available**
5. **Rule Groups**
6. **Custom WAF in v2 SKU**
7. **Pricing**
8. **How to use Azure Front Door with Azure Application Gateway**
9. **The new v2 SKU includes the following enhancements:**

* **Autoscaling:** allowing elasticity for their applications by scaling the application gateway as needed based on the application’s traffic pattern.
* **Zone redundancy**: enabling their application gateway to survive zonal failures and offering better resilience.
* **Static VIP**: This feature ensuring that their endpoint addresses will not change over its lifecycle Header Rewrite - allowing them to add, remove or update HTTP request and response headers on their application gateway.
* **Header Rewrite**: Application Gateway allows you to add, remove, or update HTTP request and response headers with v2 SKU.
* **Key Vault Integration**: Application Gateway v2 supports integration with Key Vault for server certificates that are attached to HTTPS enabled listeners.
* **Azure Kubernetes Service Ingress Controller**: The Application Gateway v2 Ingress Controller allows the Azure Application Gateway to be used as the ingress for an Azure Kubernetes Service.
* **Performance enhancements**: The v2 SKU offers up to 5X better TLS offload performance as compared to the Standard/WAF SKU.
* **Faster deployment and update time:** The v2 SKU provides faster deployment and update time as compared to Standard/WAF SKU(Including WAF configuration changes).

1. **FEATURE COMPARISON BETWEEN V1 SKU AND V2 SKU**

|  |  |  |
| --- | --- | --- |
| **Feature** | **v1 SKU** | **v2 SKU** |
| Autoscaling |  | ✓ |
| Zone redundancy |  | ✓ |
| Static VIP |  | ✓ |
| Azure Kubernetes Service (AKS) Ingress controller |  | ✓ |
| Azure Key Vault integration |  | ✓ |
| Rewrite HTTP(S) headers |  | ✓ |
| URL-based routing | ✓ | ✓ |
| Multiple-site hosting | ✓ | ✓ |
| Traffic redirection | ✓ | ✓ |
| Web Application Firewall (WAF) | ✓ | ✓ |
| WAF custom rules |  | ✓ |
| Transport Layer Security (TLS)/Secure Sockets Layer (SSL) termination | ✓ | ✓ |
| End-to-end TLS encryption | ✓ | ✓ |
| Session affinity | ✓ | ✓ |
| Custom error pages | ✓ | ✓ |
| WebSocket support | ✓ | ✓ |
| HTTP/2 support | ✓ | ✓ |
| Connection draining | ✓ | ✓ |

1. **Differences from v1 SKU**

This section describes features and limitations of the **v2 SKU** that differ from the **v1 SKU.**

|  |  |
| --- | --- |
| **Difference** | **Details** |
| Authentication certificate | Not supported. |
| Mixing Standard\_v2 and Standard Application Gateway on the same subnet | Not supported |
| User-Defined Route (UDR) on Application Gateway subnet | Supported (specific scenarios). In preview. |
| NSG for Inbound port range | - 65200 to 65535 for Standard\_v2 SKU  - 65503 to 65534 for Standard SKU |
| Performance logs in Azure diagnostics | Not supported. Azure metrics should be used. |
| Billing | Billing started on July 1, 2019. |
| FIPS mode | These are currently not supported. |
| ILB only mode | This is currently not supported. Public and ILB mode together is supported. |
| Net watcher integration | Not supported. |
| Azure Security Center integration | Not yet available. |

1. **WAF Available**

**The WAF protects against the following web vulnerabilities:**

* SQL-injection attacks
* Cross-site scripting attacks
* Other common attacks, such as command injection, HTTP request smuggling, HTTP response splitting, and remote file inclusion
* HTTP protocol violations
* HTTP protocol anomalies, such as missing host user-agent and accept headers
* Bots, crawlers, and scanners
* Common application misconfigurations (for example, Apache and IIS)
  1. **OWASP CRS 3.1**

CRS 3.1 includes 13 rule groups, as shown in the following table. Each group contains multiple rules, which can be disabled.

|  |  |
| --- | --- |
| **Rule group** | **Description** |
| General | General group |
| REQUEST-911-METHOD-ENFORCEMENT | Lock-down methods (PUT, PATCH) |
| REQUEST-913-SCANNER-DETECTION | Protect against port and environment scanners |
| REQUEST-920-PROTOCOL-ENFORCEMENT | Protect against protocol and encoding issues |
| REQUEST-921-PROTOCOL-ATTACK | Protect against header injection, request smuggling, and response splitting |
| REQUEST-930-APPLICATION-ATTACK-LFI | Protect against file and path attacks |
| REQUEST-931-APPLICATION-ATTACK-RFI | Protect against remote file inclusion (RFI) attacks |
| REQUEST-932-APPLICATION-ATTACK-RCE | Protect again remote code execution attacks |
| REQUEST-933-APPLICATION-ATTACK-PHP | Protect against PHP-injection attacks |
| REQUEST-941-APPLICATION-ATTACK-XSS | Protect against cross-site scripting attacks |
| REQUEST-942-APPLICATION-ATTACK-SQLI | Protect against SQL-injection attacks |
| REQUEST-943-APPLICATION-ATTACK-SESSION-FIXATION | Protect against session-fixation attacks |
| REQUEST-944-APPLICATION-ATTACK-SESSION-JAVA | Protect against JAVA attacks |

* 1. **OWASP CRS 3.0**

CRS 3.0 includes 12 rule groups, as shown in the following table. Each group contains multiple rules, which can be disabled.

|  |  |
| --- | --- |
| **Rule group** | **Description** |
| General | General group |
| REQUEST-911-METHOD-ENFORCEMENT | Lock-down methods (PUT, PATCH) |
| REQUEST-913-SCANNER-DETECTION | Protect against port and environment scanners |
| REQUEST-920-PROTOCOL-ENFORCEMENT | Protect against protocol and encoding issues |
| REQUEST-921-PROTOCOL-ATTACK | Protect against header injection, request smuggling, and response splitting |
| REQUEST-930-APPLICATION-ATTACK-LFI | Protect against file and path attacks |
| REQUEST-931-APPLICATION-ATTACK-RFI | Protect against remote file inclusion (RFI) attacks |
| REQUEST-932-APPLICATION-ATTACK-RCE | Protect again remote code execution attacks |
| REQUEST-933-APPLICATION-ATTACK-PHP | Protect against PHP-injection attacks |
| REQUEST-941-APPLICATION-ATTACK-XSS | Protect against cross-site scripting attacks |
| REQUEST-942-APPLICATION-ATTACK-SQLI | Protect against SQL-injection attacks |
| REQUEST-943-APPLICATION-ATTACK-SESSION-FIXATION | Protect against session-fixation attacks |

* 1. **OWASP CRS 2.2.9**

CRS 2.2.9 includes 10 rule groups, as shown in the following table. Each group contains multiple rules, which can be disabled.

|  |  |
| --- | --- |
| **Rule group** | **Description** |
| crs\_20\_protocol\_violations | Protect against protocol violations (such as invalid characters or a GET with a request body) |
| crs\_21\_protocol\_anomalies | Protect against arguments or files that exceed limitations |
| crs\_23\_request\_limits | Protect against arguments or files that exceed limitations |
| crs\_30\_http\_policy | Protect against restricted methods, headers, and file types |
| crs\_35\_bad\_robots | Protect against web crawlers and scanners |
| crs\_40\_generic\_attacks | Protect against generic attacks (such as session fixation, remote file inclusion, and PHP injection) |
| crs\_41\_sql\_injection\_attacks | Protect against SQL-injection attacks |
| crs\_41\_xss\_attacks | Protect against cross-site scripting attacks |
| crs\_42\_tight\_security | Protect against path-traversal attacks |
| crs\_45\_trojans | Protect against backdoor trojans |

1. **Rule Groups**

**The following rule groups and rules are available when using Web Application Firewall on Application Gateway.**

* 1. **OSWAP 3.1**

**Rule sets**

**GENERAL**

**RuleId Description**

200004 Possible Multipart Unmatched Boundary**.**

**REQUEST-911-METHOD-ENFORCEMENT**

**RuleId Description**

911100 Method is not allowed by policy

**REQUEST-913-SCANNER-DETECTION**

**RuleId Description**

913100 Found User-Agent associated with security scanner

913101 Found User-Agent associated with scripting/generic HTTP client

913102 Found User-Agent associated with web crawler/bot

913110 Found request header associated with security scanner

913120 Found request filename/argument associated with security scanner

**REQUEST-920-PROTOCOL-ENFORCEMENT**

**RuleId Description**

920100 Invalid HTTP Request Line

920120 Attempted multipart/form-data bypass

920121 Attempted multipart/form-data bypass

920130 Failed to parse request body.

920140 Multipart request body failed strict validation

920160 Content-Length HTTP header is not numeric.

920170 GET or HEAD Request with Body Content.

920171 GET or HEAD Request with Transfer-Encoding.

920180 POST request missing Content-Length Header.

920190 Range = Invalid Last Byte Value.

920200 Range = Too many fields (6 or more)

920201 Range = Too many fields for pdf request (35 or more)

920202 Range = Too many fields for pdf request (6 or more)

920210 Multiple/Conflicting Connection Header Data Found.

920220 URL Encoding Abuse Attack Attempt

920230 Multiple URL Encoding Detected

920240 URL Encoding Abuse Attack Attempt

920250 UTF8 Encoding Abuse Attack Attempt

920260 Unicode Full/Half Width Abuse Attack Attempt

920270 Invalid character in request (null character)

920271 Invalid character in request (non printable characters)

920272 Invalid character in request (outside of printable chars below ascii 127)

920273 Invalid character in request (outside of very strict set)

920274 Invalid character in request headers (outside of very strict set)

920280 Request Missing a Host Header

920290 Empty Host Header

920300 Request Missing an Accept Header

920310 Request Has an Empty Accept Header

920311 Request Has an Empty Accept Header

920320 Missing User Agent Header

920330 Empty User Agent Header

920340 Request Containing Content but Missing Content-Type header

920341 Request containing content requires Content-Type header

920350 Host header is a numeric IP address

920360 Argument name too long

920370 Argument value too long

920380 Too many arguments in request

920390 Total arguments size exceeded

920400 Uploaded file size too large

920410 Total uploaded files size too large

920420 Request content type is not allowed by policy

920430 HTTP protocol version is not allowed by policy

920440 URL file extension is restricted by policy

920450 HTTP header is restricted by policy (%@{MATCHED\_VAR})

920460 Abnormal Escape Characters

920470 Illegal Content-Type header

920480 Restrict charset parameter within the content-type header

**REQUEST-921-PROTOCOL-ATTACK**

**RuleId Description**

921110 HTTP Request Smuggling Attack

921120 HTTP Response Splitting Attack

921130 HTTP Response Splitting Attack

921140 HTTP Header Injection Attack via headers

921150 HTTP Header Injection Attack via payload (CR/LF detected)

921151 HTTP Header Injection Attack via payload (CR/LF detected)

921160 HTTP Header Injection Attack via payload (CR/LF and header-name detected)

921170 HTTP Parameter Pollution

921180 HTTP Parameter Pollution (%{TX.1})

**REQUEST-930-APPLICATION-ATTACK-LFI**

**RuleId Description**

930100 Path Traversal Attack (/../)

930110 Path Traversal Attack (/../)

930120 OS File Access Attempt

930130 Restricted File Access Attempt

**REQUEST-931-APPLICATION-ATTACK-RFI**

**RuleId Description**

931100 Possible Remote File Inclusion (RFI) Attack = URL Parameter using IP Address

931110 Possible Remote File Inclusion (RFI) Attack = Common RFI Vulnerable Parameter Name used w/URL Payload

931120 Possible Remote File Inclusion (RFI) Attack = URL Payload Used w/Trailing Question Mark Character (?)

931130 Possible Remote File Inclusion (RFI) Attack = Off-Domain Reference/Link

**REQUEST-932-APPLICATION-ATTACK-RCE**

**RuleId Description**

932100 Remote Command Execution: Unix Command Injection

932105 Remote Command Execution: Unix Command Injection

932106 Remote Command Execution: Unix Command Injection

932110 Remote Command Execution: Windows Command Injection

932115 Remote Command Execution: Windows Command Injection

932120 Remote Command Execution = Windows PowerShell Command Found

932130 Remote Command Execution = Unix Shell Expression Found

932140 Remote Command Execution = Windows FOR/IF Command Found

932150 Remote Command Execution: Direct Unix Command Execution

932160 Remote Command Execution = Unix Shell Code Found

932170 Remote Command Execution = Shellshock (CVE-2014-6271)

932171 Remote Command Execution = Shellshock (CVE-2014-6271)

932180 Restricted File Upload Attempt

932190 Remote Command Execution: Wildcard bypass technique attempt

**REQUEST-933-APPLICATION-ATTACK-PHP**

**RuleId Description**

933100 PHP Injection Attack = Opening/Closing Tag Found

933110 PHP Injection Attack = PHP Script File Upload Found

933111 PHP Injection Attack: PHP Script File Upload Found

933120 PHP Injection Attack = Configuration Directive Found

933130 PHP Injection Attack = Variables Found

933131 PHP Injection Attack: Variables Found

933140 PHP Injection Attack: I/O Stream Found

933150 PHP Injection Attack = High-Risk PHP Function Name Found

933151 PHP Injection Attack: Medium-Risk PHP Function Name Found

933160 PHP Injection Attack = High-Risk PHP Function Call Found

933161 PHP Injection Attack: Low-Value PHP Function Call Found

933170 PHP Injection Attack: Serialized Object Injection

933180 PHP Injection Attack = Variable Function Call Found

933190 PHP Injection Attack: PHP Closing Tag Found

**REQUEST-941-APPLICATION-ATTACK-XSS**

**RuleId Description**

941100 XSS Attack Detected via libinjection

941101 XSS Attack Detected via libinjection

941110 XSS Filter - Category 1 = Script Tag Vector

941130 XSS Filter - Category 3 = Attribute Vector

941140 XSS Filter - Category 4 = Javascript URI Vector

941150 XSS Filter - Category 5 = Disallowed HTML Attributes

941160 NoScript XSS InjectionChecker: HTML Injection

941170 NoScript XSS InjectionChecker: Attribute Injection

941180 Node-Validator Blocklist Keywords

941190 XSS using style sheets

941200 XSS using VML frames

941210 XSS using obfuscated Javascript

941220 XSS using obfuscated VB Script

941230 XSS using 'embed' tag

941240 XSS using 'import' or 'implementation' attribute

941250 IE XSS Filters - Attack Detected

941260 XSS using 'meta' tag

941270 XSS using 'link' href

941280 XSS using 'base' tag

941290 XSS using 'applet' tag

941300 XSS using 'object' tag

941310 US-ASCII Malformed Encoding XSS Filter - Attack Detected.

941320 Possible XSS Attack Detected - HTML Tag Handler

941330 IE XSS Filters - Attack Detected.

941340 IE XSS Filters - Attack Detected.

941350 UTF-7 Encoding IE XSS - Attack Detected.

**REQUEST-942-APPLICATION-ATTACK-SQLI**

**RuleId Description**

942100 SQL Injection Attack Detected via libinjection

942110 SQL Injection Attack: Common Injection Testing Detected

942120 SQL Injection Attack: SQL Operator Detected

942130 SQL Injection Attack: SQL Tautology Detected.

942140 SQL Injection Attack = Common DB Names Detected

942150 SQL Injection Attack

942160 Detects blind sqli tests using sleep() or benchmark().

942170 Detects SQL benchmark and sleep injection attempts including conditional queries

942180 Detects basic SQL authentication bypass attempts 1/3

942190 Detects MSSQL code execution and information gathering attempts

942200 Detects MySQL comment-/space-obfuscated injections and backtick termination

942210 Detects chained SQL injection attempts 1/2

942220 Looking for integer overflow attacks, these are taken from skipfish, except 3.0.00738585072

942230 Detects conditional SQL injection attempts

942240 Detects MySQL charset switch and MSSQL DoS attempts

942250 Detects MATCH AGAINST, MERGE and EXECUTE IMMEDIATE injections

942251 Detects HAVING injections

942260 Detects basic SQL authentication bypass attempts 2/3

942270 Looking for basic sql injection. Common attack string for mysql oracle and others

942280 Detects Postgres pg\_sleep injection, waitfor delay attacks and database shutdown attempts

942290 Finds basic MongoDB SQL injection attempts

942300 Detects MySQL comments, conditions and ch(a)r injections

942310 Detects chained SQL injection attempts 2/2

942320 Detects MySQL and PostgreSQL stored procedure/function injections

942330 Detects classic SQL injection probings 1/2

942340 Detects basic SQL authentication bypass attempts 3/3

942350 Detects MySQL UDF injection and other data/structure manipulation attempts

942360 Detects concatenated basic SQL injection and SQLLFI attempts

942361 Detects basic SQL injection based on keyword alter or union

942370 Detects classic SQL injection probings 2/2

942380 SQL Injection Attack

942390 SQL Injection Attack

942400 SQL Injection Attack

942410 SQL Injection Attack

942420 Restricted SQL Character Anomaly Detection (cookies): # of special characters exceeded (8)

942421 Restricted SQL Character Anomaly Detection (cookies): # of special characters exceeded (3)

942430 Restricted SQL Character Anomaly Detection (args): # of special characters exceeded (12)

942431 Restricted SQL Character Anomaly Detection (args): # of special characters exceeded (6)

942432 Restricted SQL Character Anomaly Detection (args): # of special characters exceeded (2)

942440 SQL Comment Sequence Detected.

942450 SQL Hex Encoding Identified

942460 Meta-Character Anomaly Detection Alert - Repetitive Non-Word Characters

942470 SQL Injection Attack

942480 SQL Injection Attack

942490 Detects classic SQL injection probings 3/3

**REQUEST-943-APPLICATION-ATTACK-SESSION-FIXATION**

**RuleId Description**

943100 Possible Session Fixation Attack = Setting Cookie Values in HTML

943110 Possible Session Fixation Attack = SessionID Parameter Name with Off-Domain Referrer

943120 Possible Session Fixation Attack = SessionID Parameter Name with No Referrer

**REQUEST-944-APPLICATION-ATTACK-SESSION-JAVA**

**RuleId Description**

944120 Possible payload execution and remote command execution

944130 Suspicious Java classes

944200 Exploitation of Java deserialization Apache Commons

* 1. **OWASP3.0**

**Rule sets**

**GENERAL**

**RuleId Description**

200004 Possible Multipart Unmatched Boundary.

**REQUEST-911-METHOD-ENFORCEMENT**

**RuleId Description**

911100 Method is not allowed by policy

**REQUEST-913-SCANNER-DETECTION**

**RuleId Description**

913100 Found User-Agent associated with security scanner

913110 Found request header associated with security scanner

913120 Found request filename/argument associated with security scanner

913101 Found User-Agent associated with scripting/generic HTTP client

913102 Found User-Agent associated with web crawler/bot

**REQUEST-920-PROTOCOL-ENFORCEMENT**

**RuleId Description**

920100 Invalid HTTP Request Line

920130 Failed to parse request body.

920140 Multipart request body failed strict validation

920160 Content-Length HTTP header is not numeric.

920170 GET or HEAD Request with Body Content.

920180 POST request missing Content-Length Header.

920190 Range = Invalid Last Byte Value.

920210 Multiple/Conflicting Connection Header Data Found.

920220 URL Encoding Abuse Attack Attempt

920240 URL Encoding Abuse Attack Attempt

920250 UTF8 Encoding Abuse Attack Attempt

920260 Unicode Full/Half Width Abuse Attack Attempt

920270 Invalid character in request (null character)

920280 Request Missing a Host Header

920290 Empty Host Header

920310 Request Has an Empty Accept Header

920311 Request Has an Empty Accept Header

920330 Empty User Agent Header

920340 Request Containing Content but Missing Content-Type header

920350 Host header is a numeric IP address

920380 Too many arguments in request

920360 Argument name too long

920370 Argument value too long

920390 Total arguments size exceeded

920400 Uploaded file size too large

920410 Total uploaded files size too large

920420 Request content type is not allowed by policy

920430 HTTP protocol version is not allowed by policy

920440 URL file extension is restricted by policy

920450 HTTP header is restricted by policy (%@{MATCHED\_VAR})

920200 Range = Too many fields (6 or more)

920201 Range = Too many fields for pdf request (35 or more)

920230 Multiple URL Encoding Detected

920300 Request Missing an Accept Header

920271 Invalid character in request (non printable characters)

920320 Missing User Agent Header

920272 Invalid character in request (outside of printable chars below ascii 127)

920202 Range = Too many fields for pdf request (6 or more)

920273 Invalid character in request (outside of very strict set)

920274 Invalid character in request headers (outside of very strict set)

920460 Abnormal escape characters

**REQUEST-921-PROTOCOL-ATTACK**

**RuleId Description**

921100 HTTP Request Smuggling Attack.

921110 HTTP Request Smuggling Attack

921120 HTTP Response Splitting Attack

921130 HTTP Response Splitting Attack

921140 HTTP Header Injection Attack via headers

921150 HTTP Header Injection Attack via payload (CR/LF detected)

921160 HTTP Header Injection Attack via payload (CR/LF and header-name detected)

921151 HTTP Header Injection Attack via payload (CR/LF detected)

921170 HTTP Parameter Pollution

921180 HTTP Parameter Pollution (%@{TX.1})

**REQUEST-930-APPLICATION-ATTACK-LFI**

**RuleId Description**

930100 Path Traversal Attack (/../)

930110 Path Traversal Attack (/../)

930120 OS File Access Attempt

930130 Restricted File Access Attempt

**REQUEST-931-APPLICATION-ATTACK-RFI**

**RuleId Description**

931100 Possible Remote File Inclusion (RFI) Attack = URL Parameter using IP Address

931110 Possible Remote File Inclusion (RFI) Attack = Common RFI Vulnerable Parameter Name used w/URL Payload

931120 Possible Remote File Inclusion (RFI) Attack = URL Payload Used w/Trailing Question Mark Character (?)

931130 Possible Remote File Inclusion (RFI) Attack = Off-Domain Reference/Link

**REQUEST-932-APPLICATION-ATTACK-RCE**

**RuleId Description**

932120 Remote Command Execution = Windows PowerShell Command Found

932130 Remote Command Execution = Unix Shell Expression Found

932140 Remote Command Execution = Windows FOR/IF Command Found

932160 Remote Command Execution = Unix Shell Code Found

932170 Remote Command Execution = Shellshock (CVE-2014-6271)

932171 Remote Command Execution = Shellshock (CVE-2014-6271)

**REQUEST-933-APPLICATION-ATTACK-PHP**

**RuleId Description**

933100 PHP Injection Attack = Opening/Closing Tag Found

933110 PHP Injection Attack = PHP Script File Upload Found

933120 PHP Injection Attack = Configuration Directive Found

933130 PHP Injection Attack = Variables Found

933150 PHP Injection Attack = High-Risk PHP Function Name Found

933160 PHP Injection Attack = High-Risk PHP Function Call Found

933180 PHP Injection Attack = Variable Function Call Found

933151 PHP Injection Attack = Medium-Risk PHP Function Name Found

933131 PHP Injection Attack = Variables Found

933161 PHP Injection Attack = Low-Value PHP Function Call Found

933111 PHP Injection Attack = PHP Script File Upload Found

**REQUEST-941-APPLICATION-ATTACK-XSS**

**RuleId Description**

941100 XSS Attack Detected via libinjection

941110 XSS Filter - Category 1 = Script Tag Vector

941130 XSS Filter - Category 3 = Attribute Vector

941140 XSS Filter - Category 4 = Javascript URI Vector

941150 XSS Filter - Category 5 = Disallowed HTML Attributes

941180 Node-Validator Blocklist Keywords

941190 XSS using style sheets

941200 XSS using VML frames

941210 XSS using obfuscated Javascript

941220 XSS using obfuscated VB Script

941230 XSS using 'embed' tag

941240 XSS using 'import' or 'implementation' attribute

941260 XSS using 'meta' tag

941270 XSS using 'link' href

941280 XSS using 'base' tag

941290 XSS using 'applet' tag

941300 XSS using 'object' tag

941310 US-ASCII Malformed Encoding XSS Filter - Attack Detected.

941330 IE XSS Filters - Attack Detected.

941340 IE XSS Filters - Attack Detected.

941350 UTF-7 Encoding IE XSS - Attack Detected.

941320 Possible XSS Attack Detected - HTML Tag Handler

**REQUEST-942-APPLICATION-ATTACK-SQLI**

**RuleId Description**

942100 SQL Injection Attack Detected via libinjection

942110 SQL Injection Attack: Common Injection Testing Detected

942130 SQL Injection Attack: SQL Tautology Detected.

942140 SQL Injection Attack = Common DB Names Detected

942160 Detects blind sqli tests using sleep() or benchmark().

942170 Detects SQL benchmark and sleep injection attempts including conditional queries

942190 Detects MSSQL code execution and information gathering attempts

942200 Detects MySQL comment-/space-obfuscated injections and backtick termination

942230 Detects conditional SQL injection attempts

942260 Detects basic SQL authentication bypass attempts 2/3

942270 Looking for basic sql injection. Common attack string for mysql oracle and others.

942290 Finds basic MongoDB SQL injection attempts

942300 Detects MySQL comments, conditions and ch(a)r injections

942310 Detects chained SQL injection attempts 2/2

942320 Detects MySQL and PostgreSQL stored procedure/function injections

942330 Detects classic SQL injection probings 1/2

942340 Detects basic SQL authentication bypass attempts 3/3

942350 Detects MySQL UDF injection and other data/structure manipulation attempts

942360 Detects concatenated basic SQL injection and SQLLFI attempts

942370 Detects classic SQL injection probings 2/2

942150 SQL Injection Attack

942410 SQL Injection Attack

942430 Restricted SQL Character Anomaly Detection (args): # of special characters exceeded (12)

942440 SQL Comment Sequence Detected.

942450 SQL Hex Encoding Identified

942251 Detects HAVING injections

942460 Meta-Character Anomaly Detection Alert - Repetitive Non-Word Characters

**REQUEST-943-APPLICATION-ATTACK-SESSION-FIXATION**

**RuleId Description**

943100 Possible Session Fixation Attack = Setting Cookie Values in HTML

943110 Possible Session Fixation Attack = SessionID Parameter Name with Off-Domain Referrer

943120 Possible Session Fixation Attack = SessionID Parameter Name with No Referrer

* 1. **OWASP 2.2.9**

**Rule sets**

**crs\_20\_protocol\_violations**

**RuleId Description**

960911 Invalid HTTP Request Line

981227 Apache Error = Invalid URI in Request.

960912 Failed to parse request body.

960914 Multipart request body failed strict validation

960915 Multipart parser detected a possible unmatched boundary.

960016 Content-Length HTTP header is not numeric.

960011 GET or HEAD Request with Body Content.

960012 POST request missing Content-Length Header.

960902 Invalid Use of Identity Encoding.

960022 Expect Header Not Allowed for HTTP 1.0.

960020 Pragma Header requires Cache-Control Header for HTTP/1.1 requests.

958291 Range = field exists and begins with 0.

958230 Range = Invalid Last Byte Value.

958295 Multiple/Conflicting Connection Header Data Found.

950107 URL Encoding Abuse Attack Attempt

950109 Multiple URL Encoding Detected

950108 URL Encoding Abuse Attack Attempt

950801 UTF8 Encoding Abuse Attack Attempt

950116 Unicode Full/Half Width Abuse Attack Attempt

960901 Invalid character in request

960018 Invalid character in request

**crs\_21\_protocol\_anomalies**

**RuleId Description**

960008 Request Missing a Host Header

960007 Empty Host Header

960015 Request Missing an Accept Header

960021 Request Has an Empty Accept Header

960009 Request Missing a User Agent Header

960006 Empty User Agent Header

960904 Request Containing Content but Missing Content-Type header

960017 Host header is a numeric IP address

**crs\_23\_request\_limits**

**RuleId Description**

960209 Argument name too long

960208 Argument value too long

960335 Too many arguments in request

960341 Total arguments size exceeded

960342 Uploaded file size too large

960343 Total uploaded files size too large

**crs\_30\_http\_policy**

**RuleId Description**

960032 Method is not allowed by policy

960010 Request content type is not allowed by policy

960034 HTTP protocol version is not allowed by policy

960035 URL file extension is restricted by policy

960038 HTTP header is restricted by policy

**crs\_35\_bad\_robots**

**RuleId Description**

990002 Request Indicates a Security Scanner Scanned the Site

990901 Request Indicates a Security Scanner Scanned the Site

990902 Request Indicates a Security Scanner Scanned the Site

990012 Rogue web site crawler

**crs\_40\_generic\_attacks**

**RuleId Description**

960024 Meta-Character Anomaly Detection Alert - Repetitive Non-Word Characters

950008 Injection of Undocumented ColdFusion Tags

950010 LDAP Injection Attack

950011 SSI injection Attack

950018 Universal PDF XSS URL Detected.

950019 Email Injection Attack

950012 HTTP Request Smuggling Attack.

950910 HTTP Response Splitting Attack

950911 HTTP Response Splitting Attack

950117 Remote File Inclusion Attack

950118 Remote File Inclusion Attack

950119 Remote File Inclusion Attack

950120 Possible Remote File Inclusion (RFI) Attack = Off-Domain Reference/Link

981133 Rule 981133

981134 Rule 981134

950009 Session Fixation Attack

950003 Session Fixation

950000 Session Fixation

950005 Remote File Access Attempt

950002 System Command Access

950006 System Command Injection

959151 PHP Injection Attack

958976 PHP Injection Attack

958977 PHP Injection Attack

**crs\_41\_sql\_injection\_attacks**

**RuleId Description**

981231 SQL Comment Sequence Detected.

981260 SQL Hex Encoding Identified

981320 SQL Injection Attack = Common DB Names Detected

981300 Rule 981300

981301 Rule 981301

981302 Rule 981302

981303 Rule 981303

981304 Rule 981304

981305 Rule 981305

981306 Rule 981306

981307 Rule 981307

981308 Rule 981308

981309 Rule 981309

981310 Rule 981310

981311 Rule 981311

981312 Rule 981312

981313 Rule 981313

981314 Rule 981314

981315 Rule 981315

981316 Rule 981316

981317 SQL SELECT Statement Anomaly Detection Alert

950007 Blind SQL Injection Attack

950001 SQL Injection Attack

950908 SQL Injection Attack.

959073 SQL Injection Attack

981272 Detects blind sqli tests using sleep() or benchmark().

981250 Detects SQL benchmark and sleep injection attempts including conditional queries

981241 Detects conditional SQL injection attempts

981276 Looking for basic sql injection. Common attack string for mysql oracle and others.

981270 Finds basic MongoDB SQL injection attempts

981253 Detects MySQL and PostgreSQL stored procedure/function injections

981251 Detects MySQL UDF injection and other data/structure manipulation attempts

**crs\_41\_xss\_attacks**

**RuleId Description**

973336 XSS Filter - Category 1 = Script Tag Vector

973338 XSS Filter - Category 3 = Javascript URI Vector

981136 Rule 981136

981018 Rule 981018

958016 Cross-site Scripting (XSS) Attack

958414 Cross-site Scripting (XSS) Attack

958032 Cross-site Scripting (XSS) Attack

958026 Cross-site Scripting (XSS) Attack

958027 Cross-site Scripting (XSS) Attack

958054 Cross-site Scripting (XSS) Attack

958418 Cross-site Scripting (XSS) Attack

958034 Cross-site Scripting (XSS) Attack

958019 Cross-site Scripting (XSS) Attack

958013 Cross-site Scripting (XSS) Attack

958408 Cross-site Scripting (XSS) Attack

958012 Cross-site Scripting (XSS) Attack

958423 Cross-site Scripting (XSS) Attack

958002 Cross-site Scripting (XSS) Attack

958017 Cross-site Scripting (XSS) Attack

958007 Cross-site Scripting (XSS) Attack

958047 Cross-site Scripting (XSS) Attack

958410 Cross-site Scripting (XSS) Attack

958415 Cross-site Scripting (XSS) Attack

958022 Cross-site Scripting (XSS) Attack

958405 Cross-site Scripting (XSS) Attack

958419 Cross-site Scripting (XSS) Attack

958028 Cross-site Scripting (XSS) Attack

958057 Cross-site Scripting (XSS) Attack

958031 Cross-site Scripting (XSS) Attack

958006 Cross-site Scripting (XSS) Attack

958033 Cross-site Scripting (XSS) Attack

958038 Cross-site Scripting (XSS) Attack

958409 Cross-site Scripting (XSS) Attack

958001 Cross-site Scripting (XSS) Attack

958005 Cross-site Scripting (XSS) Attack

958404 Cross-site Scripting (XSS) Attack

958023 Cross-site Scripting (XSS) Attack

958010 Cross-site Scripting (XSS) Attack

958411 Cross-site Scripting (XSS) Attack

958422 Cross-site Scripting (XSS) Attack

958036 Cross-site Scripting (XSS) Attack

958000 Cross-site Scripting (XSS) Attack

958018 Cross-site Scripting (XSS) Attack

958406 Cross-site Scripting (XSS) Attack

958040 Cross-site Scripting (XSS) Attack

958052 Cross-site Scripting (XSS) Attack

958037 Cross-site Scripting (XSS) Attack

958049 Cross-site Scripting (XSS) Attack

958030 Cross-site Scripting (XSS) Attack

958041 Cross-site Scripting (XSS) Attack

958416 Cross-site Scripting (XSS) Attack

958024 Cross-site Scripting (XSS) Attack

958059 Cross-site Scripting (XSS) Attack

958417 Cross-site Scripting (XSS) Attack

958020 Cross-site Scripting (XSS) Attack

958045 Cross-site Scripting (XSS) Attack

958004 Cross-site Scripting (XSS) Attack

958421 Cross-site Scripting (XSS) Attack

958009 Cross-site Scripting (XSS) Attack

958025 Cross-site Scripting (XSS) Attack

958413 Cross-site Scripting (XSS) Attack

958051 Cross-site Scripting (XSS) Attack

958420 Cross-site Scripting (XSS) Attack

958407 Cross-site Scripting (XSS) Attack

958056 Cross-site Scripting (XSS) Attack

958011 Cross-site Scripting (XSS) Attack

958412 Cross-site Scripting (XSS) Attack

958008 Cross-site Scripting (XSS) Attack

958046 Cross-site Scripting (XSS) Attack

958039 Cross-site Scripting (XSS) Attack

958003 Cross-site Scripting (XSS) Attack

973300 Possible XSS Attack Detected - HTML Tag Handler

973301 XSS Attack Detected

973302 XSS Attack Detected

973303 XSS Attack Detected

973304 XSS Attack Detected

973305 XSS Attack Detected

973306 XSS Attack Detected

973307 XSS Attack Detected

973308 XSS Attack Detected

973309 XSS Attack Detected

973311 XSS Attack Detected

973313 XSS Attack Detected

973314 XSS Attack Detected

973331 IE XSS Filters - Attack Detected.

973315 IE XSS Filters - Attack Detected.

973330 IE XSS Filters - Attack Detected.

973327 IE XSS Filters - Attack Detected.

973326 IE XSS Filters - Attack Detected.

973346 IE XSS Filters - Attack Detected.

973345 IE XSS Filters - Attack Detected.

973324 IE XSS Filters - Attack Detected.

973323 IE XSS Filters - Attack Detected.

973348 IE XSS Filters - Attack Detected.

973321 IE XSS Filters - Attack Detected.

973320 IE XSS Filters - Attack Detected.

973318 IE XSS Filters - Attack Detected.

973317 IE XSS Filters - Attack Detected.

973329 IE XSS Filters - Attack Detected.

973328 IE XSS Filters - Attack Detected.

**crs\_42\_tight\_security**

**RuleId Description**

950103 Path Traversal Attack

**crs\_45\_trojans**

**RuleId Description**

950110 Backdoor access

950921 Backdoor access

950922 Backdoor access

1. **Custom WAF in v2 SKU**

The Azure Application Gateway Web Application Firewall v2 comes with a pre-configured, platform-managed ruleset that offers protection from many different types of attacks(including cross site scripting, SQL injection, and others).

Custom rules allow you to create your own rules that are evaluated for each request that passes through the WAF. These rules hold a higher priority than the rest of the rules in the managed rule sets. The custom rules contain a rule name, rule priority, and an array of matching conditions. If these conditions are met, an action is taken (to allow or block).

**Sample script to block:**

"customRules": [

{

"name": "blockEvilBot",

"priority": 2,

"ruleType": "MatchRule",

"action": "Block",

"matchConditions": [

{

"matchVariables": [

{

"variableName": "RequestHeaders",

"selector": "User-Agent"

}

],

"operator": "Contains",

"negationCondition": false,

"matchValues": [

"evilbot"

],

"transforms": [

"Lowercase"

]

}

]

}

],

1. **Pricing**
   1. **Application Gateways**

It’s charged based on the amount of time that the gateway is provisioned and available, as well as the amount of data processed by the application gateways.

|  |  |  |
| --- | --- | --- |
| **Application Gateway Type** | **Basic Application Gateway** | **Web Application Firewall Application Gateway** |
| Small | $0.025 per gateway-hour (~$18.25/month) | Not available |
| Medium | $0.07 per gateway-hour (~$51.10/month) | $0.126 per gateway-hour (~$91.98/month) |
| Large | $0.32 per gateway-hour (~$233.60/month) | $0.448 per gateway-hour (~$327.04/month) |

* 1. **Data processing**

Data processing charge is based on the amount of data processed by the application gateways.

|  |  |  |  |
| --- | --- | --- | --- |
| **Data Processing** | **Small** | **Medium** | **Large** |
| First 10 TB/month | $0.008 per GB | $0 per GB | $0 per GB |
| Next 30 TB (10–40 TB)/month | $0.008 per GB | $0.007 per GB | $0 per GB |
| Over 40 TB/month | $0.008 per GB | $0.007 per GB | $0.0035 per GB |

* 1. **Data transfers**

Inbound-free

Outbound- Charged at data transfer rates

* 1. **Application Gateway Standard\_v2 and WAF\_v2 SKU**

|  |  |  |
| --- | --- | --- |
|  | **Application Gateway** | **Web Application Firewall Application Gateway** |
| Fixed | $0.20 per gateway-hour | $0.36 per gateway-hour |
| Capacity Unit1 | $0.008 per capacity unit-hour | $0.0144 per capacity unit-hour |

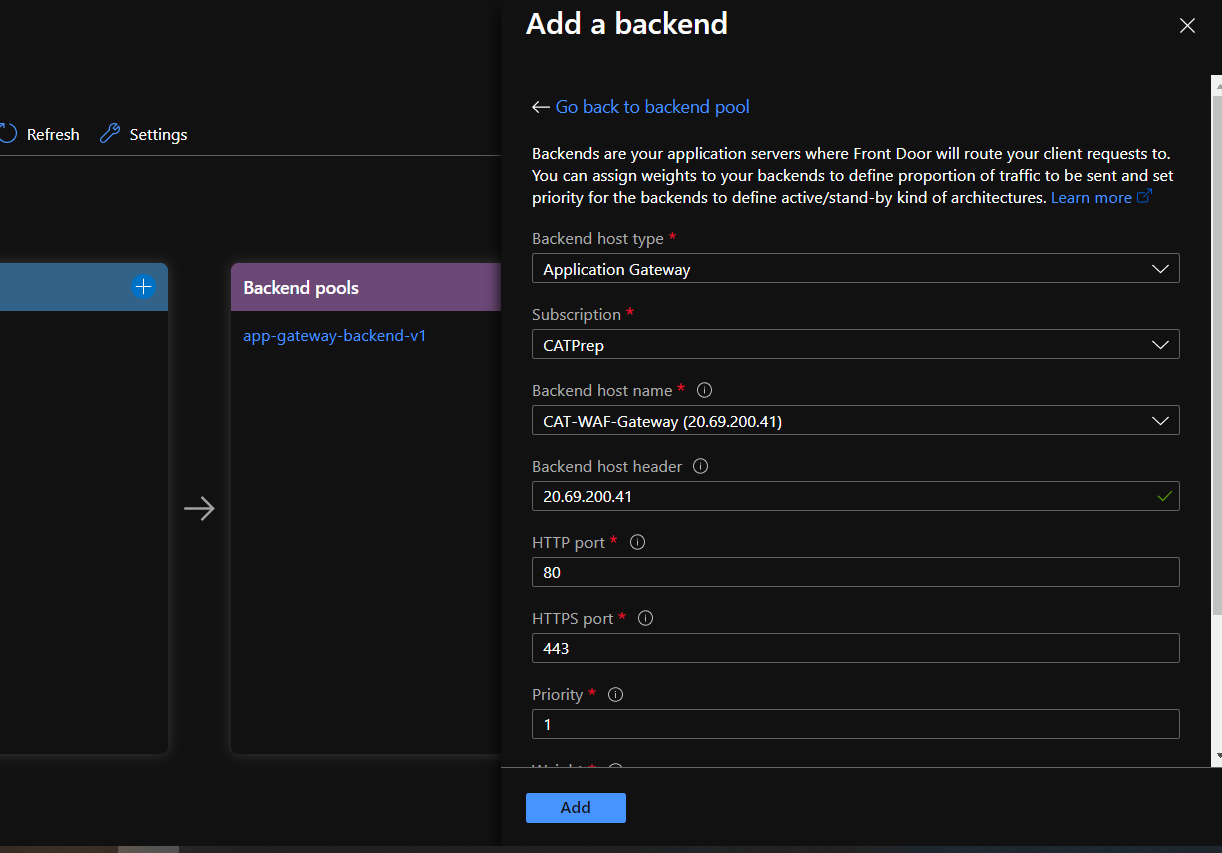
1. **How to use Azure Front Door with Azure Application Gateway**

To use Azure Front Door with Azure Application Gateway we have to add Application Gateway as a Backend Pool in Azure Front Door.

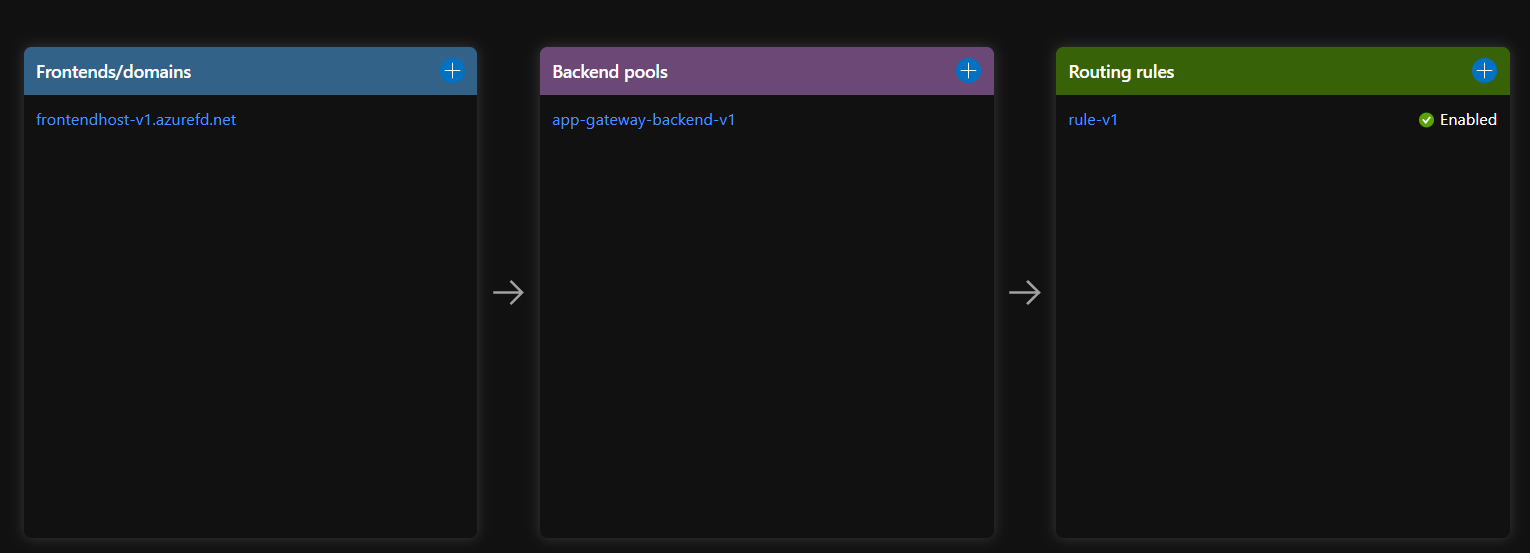
Steps:

* Create an Incoming i.e. Azure Web Service.
* Create an Azure Application Gateway connected with desired Azure Web Service.
* Create an Azure Front Door and connect it with Desired Azure Application Gateway as a Backend Pool.
* Configure Frontend, Backend pools and Routing Rules.
* Get Api Response.

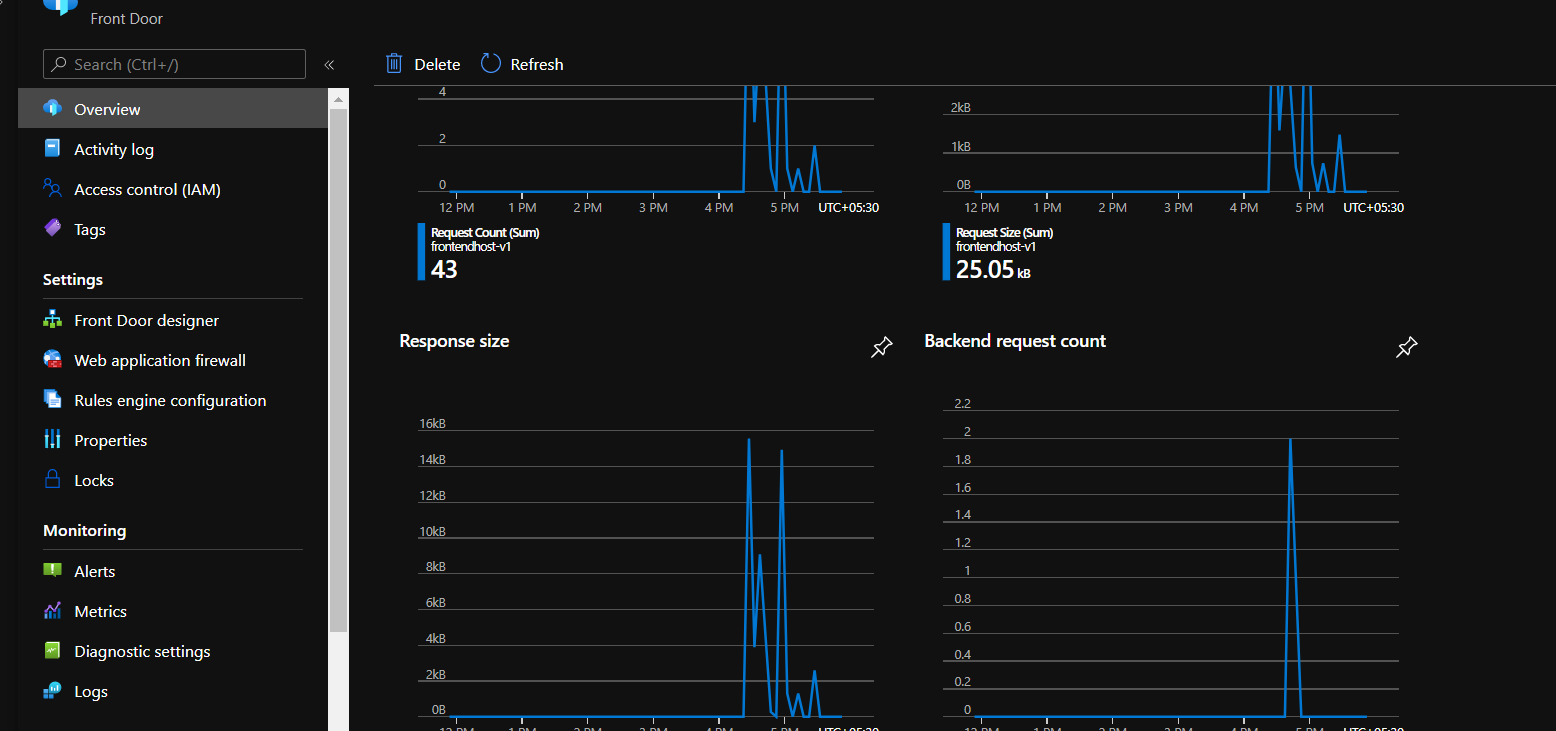
(Note: In pics v1 represents version and not v1 SKU)

Pic 1)To add Application Gateway as a Backend Pool.

Pic 2) Configure Frontend, Backend pools and Routing Rules.



Pic3) Requests Received.



Pic 4) Api Response.

