Web Application Firewall

Protect your website and keep it online and accessible with Yottaa Web Application Firewall (WAF) integration. Allow, Block, throttle, or redirect threat traffic. Implement predefined rules, or quickly implement custom rules to handle new threats. Review logs and analytics to understand traffic threats and take appropriate action.

WAF rule creation allows selection of different conditions in each rule definition, including:

- Client IP
- Client user agent
- State/Region
- HTTP Request Header
- Country
- Request URL
- Cookies
- Request Payload

Website Protection

Multiple different layers of protection can be used to prevent threats and maintain website's online presence. Working together, security threats can be prevented from impacting legitimate visitors' online experience.

- **Origin Shield** - Provides an additional layer of defense for your website by preventing attackers from directly targeting your origin servers. It forces traffic to go through the Yottaa intelligent security solution, where attacks can be detected and mitigated. Only two ports are open (80, 443) to reduce vulnerabilities.
- **DDoS Protection** – Operates alongside WAF and provides protection at the OSI later 3 and 4 levels. DDoS protection can also protect at layer 7, comes with a default setting of 300 requests per second per IP, and will generate notifications if there is an attack. Throttling and rate limiting rules can be configured.
- **Throttling Rules (Rate Limiting)** – Ensure the site is protected from excessive requests and ensures other site visitors are not impacted. There is no limit to the number of IP addresses, but overall increased traffic may be caught by the Rate Limiting capability.
- **Threat Signature** – Yottaa's advanced web application firewall maintains a core rule set to block against known threat signatures, enabling protection against security issues such as SQL Injection, XSS and protocol violations. A Learn mode can be selected to apply the signature but take no action. An initial set of over 600 OWASP rules are available that can be customized for each site.
- **Bot Mitigation** – Increased traffic and threats from bots is a growing concern. Yottaa can provide protection from bots. More details are covered in the bot mitigation datasheet.

Web Application Firewall Rules

Firewall rules allow you to secure access to and ensure consistent performance of your site. There are four rule types: Whitelist, Block, Throttle, Redirect. There are no limits to the number of rules that can be created and applied. Firewall rules are applied in the order listed below with earlier rules superseding later rules.

- **Whitelist -** Allow certain types of traffic, such as users with certain cookies or IP addresses, as exceptions to a blocking rule. Allow specific visitors to access your site by specifying individual IP addresses or CIDR blocks to whitelist (allow to access your site).
- **Block Rules** - Requests sent to your site that matched a blocking rule and received a 403 (Forbidden) error. Control visitor access to your site by specifying individual IP addresses or CIDR blocks to block (blacklist). Stops certain types of traffic from accessing your site. By default, Yottaa WAF returns HTTP 403 errors, but WAF allows a custom web page to be created so that messaging can be served to customers based on block rules. You can enter your own HTML, and specify a HTTP status code, to respond to blocked requests. These requests do not reach your origin server.
- **Throttle Rules (Rate Limiting)** – Protects your site from excessive site requests and avoids service interruptions or errors for other site visitors. You set limits for the number of requests over a certain time period based on conditions such as the URL, user agent, or client IP. When the site reaches a throttle limit, it returns HTTP 429 errors (Too Many Requests).
  - Each throttle rule can be defined for any of the conditions listed below and by setting the limit of number of requests per 'x' second(s), minute(s), hour(s), day(s), or week(s).
  - You can enter your own HTML, and status code, to respond to throttled requests with.
- **Redirect Rules** – Control where your site visitors are redirected by defining specific URL redirect rules. Requests sent to your site that received a 3xx response redirect to another URL, or can just be redirected to another page rather than the page they requested.

Support Services

Yottaa has support experts that can monitor and identify new threats and quickly create custom rules to mitigate them. These are created and managed by the Yottaa Customer Success team. The Premium Support offering provides a named Technical Account Manager who can regularly review and discuss security concerns and recommend new rules. This is supplemented with a weekly security email highlighting the top active rules and volume of blocked requests.

YOTTAA

Conditions can be set when defining WAF rules, and are available for all rules as listed below:

- **HTTP Request Header** – Applies the firewall rule to certain traffic based on request headers e.g. a rule can be applied based on cookies or header values.
- **Request URL** – Applies the firewall rule to specific pages on your site.
- **Client user agent** – Applies rule based on how the user accessed your site, whether from a browser, an app, a command line prompt, or any other user agent.
- **Client IP** – A list of IPs or CIDRs can be either included or excluded by setting the option to 'In', so that the rule is applied to all IPs in the list, or 'Not in' which applies the rule to all IPs not in the list.
- **Country** – Applies the firewall rule to traffic from specific countries using the options 'In' to apply to all countries in the list, or 'Not in' to apply the rule to all countries that are not in the list.
- **Request Payload** – Rules will check against HTTP body data, protocol conformities, and HTTP method conformities to detect and prevent protocol violations and malicious requests for data. Examples include blocking a POST request with no content-length header, or a GET request with request body data, or HTTP smuggling attacks.

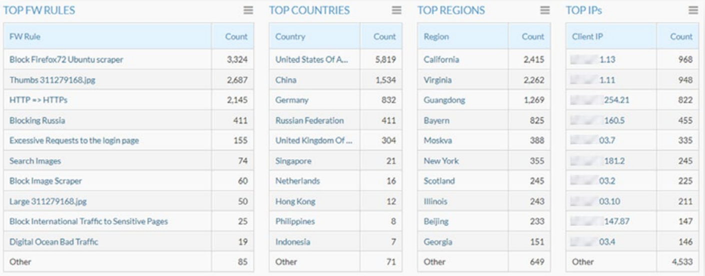
Learn mode and Mirroring allow WAF rules to be fine tuned before setting them active and enables new WAF configurations to be tested while still providing protection. An existing configuration can continue to monitor for threats while mirroring allows new WAF configurations (with updated CRS and/or custom rules, etc) to be tested. This helps reduce False Positives and increases WAF effectiveness as A/B testing can be done while having the site WAF-protected.

Visibility and Analytics

Multiple tables are viewable in the dashboard which not only show the top firewall rules that are executing, but also break down the traffic into several categories. Each rule listed can be expanded to show the defined conditions that will trigger the rule. The top traffic volume for each category can be clearly seen and provides a detailed understanding of what threats are present and where those threats are coming from, down to the IP.

While multiple rules can be created the dashboards will show the rules that are taking effect such as what is blocked and what is throttled.

Each table can be exported to a .csv file for greater analysis and contains the full list of all entries in that category. Any individual item in a table can be selected and the follow-on tables will adjust its listing to be relevant for that initial selection (e.g. If Germany is selected in the top countries list then the top regions will change to show the traffic for the top German regions and the top IPs will change to show the IP addresses within Germany.)



TOP FW RULES

FW Rule	Count
Block Firefox72 Ubuntu scraper	3,324
Thumbs 311279168.jpg	2,687
HTTP => HTTPs	2,145
Blocking Russia	411
Excessive Requests to the login page	155
Search Images	74
Block Image Scraper	60
Large 311279168.jpg	50
Block International Traffic to Sensitive Pages	25
Digital Ocean Bad Traffic	19
Other	85

TOP COUNTRIES

Country	Count
United States Of A...	5,819
China	1,534
Germany	832
Russian Federation	411
United Kingdom Of ...	304
Singapore	21
Netherlands	16
Hong Kong	12
Philippines	8
Indonesia	7
Other	71

TOP REGIONS

Region	Count
California	2,415
Virginia	2,262
Guangdong	1,269
Bayern	825
Moskva	388
New York	355
Scotland	245
Illinois	243
Beijing	233
Georgia	151
Other	649

TOP IPs

Client IP	Count
[redacted] 1.13	968
[redacted] 1.11	948
[redacted] 254.21	822
[redacted] 160.5	455
[redacted] 03.7	335
[redacted] 181.2	245
[redacted] 03.2	225
[redacted] 03.10	211
[redacted] 147.87	147
[redacted] 03.4	146
Other	4,533

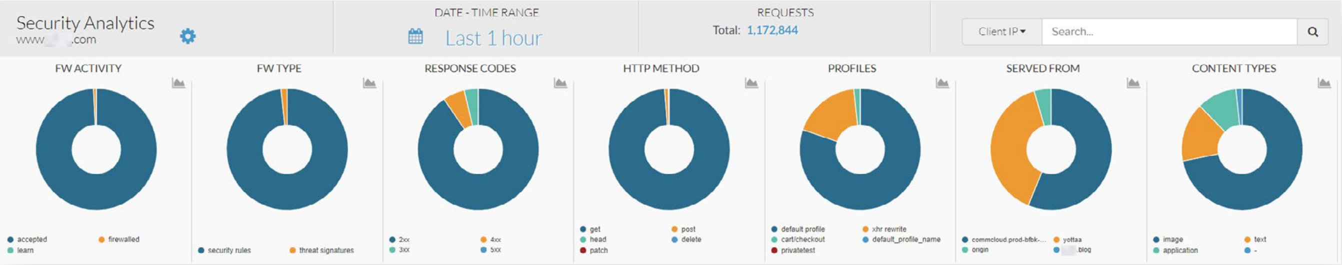
Top level view of the analytics information.

WAF anomalies are tracked and flagged. These occur when there is a spike or drop in activity that is blocked by your web application firewall. A spike in WAF metrics could potentially be due to an attack by malicious bots. Although the site is safe from any attack blocked by WAF protocols, this information can be used to monitor and prepare for potential subsequent attacks that might be more sophisticated. Triggering Requests information can be used to see if a high number of WAF anomalies are coming from a specific country or region. WAF errors can also be further broken down into the WAF security and WAF threat categories.

Alerts can be setup to check on response codes or rate limiting thresholds.

Logs are gathered from all rule activity and made available to customers for analysis and leverage.

Being able to see the active rules and the traffic sources provides an understanding of the level of threat traffic and the effect the rules are having on it.



Security Analytics
www.[redacted].com

DATE - TIME RANGE
Last 1 hour

REQUESTS
Total: 1,172,844

Client IP ▾ Search...

Web Application Firewall protection is a key part of any website security approach. Testing and fine tuning allows for increased protection which can be monitored and alerted on with detailed analytics and metrics. The flexible rules and conditions of Yottaa WAF, along with the additional security features available ensures clear threat visibility and quick action to maintain website protection without impacting visitor experience.

The Next Step

Don't just assume that your eCommerce site is performing as fast as it needs to – be sure with a free, no obligation YOTTAA trial. Start the process today with a FREE Performance Snapshot. **Click HERE for more information. You can't afford not to.**