Web Protection

Web Application Firewall (WAF)

Web Protection Profiles are a collection of Web Application Firewall (WAF) Rules that can be used to evaluate web-based transactions to ensure the traffic is not malicious.

Upload Custom WAF Rules

Multicloud Defense supports the following WAF Rule Sets:

Table 1: Multicloud Defense supports the following WAF Rule Sets

Rule Sets	Description
Core Rules	TheCore Rules are a standard set of Rules from ModSecurity CRS (Core Rule Set) that provide a base level of protection for any web application.
Trustwave Rules	TheTrustwave Rules are a premium set of Rules from ModSecurity based on intelligence gathered from real-world investigations, penetration tests and research that provide an advanced level of protection for specific web applications and frameworks.
Custom Rules	TheCustom Rules are a particular set of Rules written by customers that provide a specialized level of protection for custom web applications.

A Custom Rules Ruleset containing one or more Rules can be uploaded and used by the Multicloud Defense WAF security engine. The Rules contained within the Ruleset provide specialized web application evaluations required by a customer for their specific web applications and frameworks. The Custom Rules included in the WAF Profile will be evaluated first before evaluating any other Rulesets configured in the WAF Profile.

When uploading a Custom Rules Ruleset, the file should be a Gzip compressed TAR file with extension tar.gz. The compressed TAR file will consist of the following files:

- Readme File - File that gives a description of the Ruleset.
- Changelog File - File that represents the change history.
- Rules Folder - Folder that consists of one or more ModSecurity formatted Rules files. Each file must have an extension .conf. The folder must contain at least one Rule file (cannot be empty). Each file must follow the ModSecurity Rules format guidelines.

Step 1 Navigate to **Manage** > **Threat Research** > **Web Protection**.

Step 2 Click the **Custom** tab.

Step 3 Click the **Import** button and upload the custom Ruleset file.

Create WAF Profile

Step 1 Navigate to **Manage** > **Profiles** > **Web Protection**.

Step 2 Click **Create Protection Profile** > **Application Threat**.

Step 3 Specify the following general settings:

a) Specify a Profile Name and Description

b) Specify the Action:

- **Rule Default** - Allow or Deny the requests based on the action specified in each triggered Rule and log an Event.
- **Allow Log** - Allow the requests and log anEvent.
- **Deny Log** - Deny the requests and log anEvent.

c) Specify whether to generate a Threat HAR file if the WAF Profile detects malicious activity.

d) Specify whether to generate a HTTP Request HAR file if the WAF Profile detects malicious activity.

e) You must specify at least one Ruleset from a Rules library (Core, Trustwave, Custom) in the WAF Profile. Specify the Core Rules:

1. Specify **Manual** or **Automatic**.
   - **Manual**- Specify the Core Rules *Version* to use.
   - **Automatic** - Specify the numbers of days from publish date to delay automatic update to the latest Core Rules version
2. Add specific Core Rules Rulesets to the WAF Profile.

Note If Core Rules Rulesets are specified, the Core Rules cannot be disabled. In order to disable the Core Rules, remove all Core Rules Rulesets from the WAF Profile so they will not be evaluated.

f) Specify the Trustwave Rules:

1. Specify **Disabled**, **Manual** , or **Automatic**.
   - **Disabled** - Specify whether to disable the use of Trustwave Rules (see Tech Notes above).

- **Manual** - Specify the Trustwave Rules *Version* to use.
- **Automatic** - Specify the number of days from publish date to delay automatic update to the latest Trustwave Rules version.

2. Add specific Trustwave Rules Rulesets to the WAF Profile.

Note If Trustwave Rules and Custom Rules Rulesets are used, at least one of the two must be enabled. If the desire is to disable both, remove all Trustwave Rules and Custom Rules Rulesets from the WAF Profile so they will not be evaluated.

g) Specify the Custom Rules:

1. Specify **Disabled**, **Manual** , or **Automatic**.
   - **Disabled** - Specify whether to disable the use of Custom Rules (see Tech Notes above)
   - **Manual** - Specify the Custom Rules *Version* to use
   - **Automatic** - Specify the number of days from publish date to delay automatic update to the latest Custom Rules version
2. Add specific Custom Rules Rulesets to the WAF Profile.

Note If Trustwave Rules and Custom Rules Rulesets are used, at least one of the two must be enabled. If the desire is to disable both, remove all Trustwave Rules and Custom Rules Rulesets from the WAF Profile so they will not be evaluated.

Note If you want to disable the entire WAF Profile, remove the WAF Profile from any Policy Ruleset Rules so the WAF Profile will not be evaluated.

Step 4 Specify the following advanced settings:

a) Specify rules suppression. Rules can be suppressed for a specific IP or a list of CIDRs:

1. Click **Advanced Settings** tab.
2. Under Rule Suppression click **Add**.
3. For **Source IP/CIDR List**, provide a comma-separated list of IPs or CIDRs.
4. For **Rule ID List**, provide a comma-separated list of Rule IDs.

b) Specify whether to generate a Threat HAR file if the WAF Profile detects malicious activity.

c) Specify whether to generate a HTTP Request HAR file if the WAF Profile detects malicious activity.

d) You must specify at least one Ruleset from a Rules library (Core, Trustwave, Custom) in the WAF Profile. Specify the Core Rules:

1. Specify **Manual** or **Automatic**.
   - **Manual**- Specify the Core Rules *Version* to use.
   - **Automatic** - Specify the numbers of days from publish date to delay automatic update to the latest Core Rules version
2. Add specific Core Rules Rulesets to the WAF Profile.

Note If Core Rules Rulesets are specified, the Core Rules cannot be disabled. In order to disable the Core Rules, remove all Core Rules Rulesets from the WAF Profile so they will not be evaluated.

e) Specify the Trustwave Rules:

1. Specify **Disabled**, **Manual** , or **Automatic**.
   - **Disabled** - Specify whether to disable the use of Trustwave Rules (see Tech Notes above).
   - **Manual** - Specify the Trustwave Rules *Version* to use.
   - **Automatic** - Specify the number of days from publish date to delay automatic update to the latest Trustwave Rules version.
2. Add specific Trustwave Rules Rulesets to the WAF Profile.

Note If Trustwave Rules and Custom Rules Rulesets are used, at least one of the two must be enabled. If the desire is to disable both, remove all Trustwave Rules and Custom Rules Rulesets from the WAF Profile so they will not be evaluated.

f) Specify the Custom Rules:

1. Specify **Disabled**, **Manual** , or **Automatic**.
   - **Disabled** - Specify whether to disable the use of Custom Rules (see Tech Notes above)
   - **Manual** - Specify the Custom Rules *Version* to use
   - **Automatic** - Specify the number of days from publish date to delay automatic update to the latest Custom Rules version
2. Add specific Custom Rules Rulesets to the WAF Profile.

Note If Trustwave Rules and Custom Rules Rulesets are used, at least one of the two must be enabled. If the desire is to disable both, remove all Trustwave Rules and Custom Rules Rulesets from the WAF Profile so they will not be evaluated.

Event Filtering

To reduce the number of security Events that are generated when the WAF Profile is triggered, the Event Filtering can be configured to rate limit or sample the Events. The configuration does not alter the detection or protection behavior.

When specifying Type as **Rate**, the generated Events are rate limited based on the specified *Number of Events* triggered over a *Time* evaluation interval (in seconds). For example, if *Number of Events* is specified as 50 and *Time* is specified as 5 seconds, only 10 Events per second will be generated.

When specifying Type as **Sample**, the generated Events are sampled based on the specified *Number of Events*. For example, if *Number of Events* is specified as 10, only 1 Event will be generated for every 10 Events triggered.

Profile Event Filtering

Profile Event Filtering applies to all Rules that are configured in the WAF Profile:

- Specify the Type as **Rate** or **Sample**:
  - **Rate**- Specify the *Number of Events* and the *Time* evaluation interval (in seconds).
  - **Sample**- Specify the *Number of Events*.

Rule Event Filtering

Rule Event Filtering applies to specific Rules that are configured in the IDS/IPS Profile

---

Step 1 Click **Add** under **Rule Event Filtering**.

Step 2 For *Rule ID List*, specify a comma-separated list of *Rule IDs*.

Step 3 Specify Type as *Rate* or *Sample*:

- *Rate* - Specify the *Number of Events* and the *Time* evaluation interval (in seconds)
- *Sample* - Specify the *Number of Events*

What to do next

Associate the Event Filtering Profile

Check this document to create/edit rules

Create L7 DoS Profile

Layer 7 DoS attacks are targeted at depleting web server resources, affecting service availability by sending many HTTP requests. The feature provided by the Multicloud Defense Gateways enables the monitoring, detection and remediation of application layer attacks by continuously monitoring the client requests to a backend web server. This feature is enabled when the Gateways are enabled to proxy inbound connections to a backend web service. Enabling this feature also allows the Gateways to add security depth for cases where a frontend load balancer may not support, or, may not be optimized to detect and remediate against application DoS attacks.

This feature can be applied to backend web services to maintain availability of web based applications and also can be used to provide DoS protection against backend web servers hosting API services.

Step 1 Navigate to **Manage** > **Profiles** > **Web Protection**.

Step 2 Select **Layer 7 DOS**.

Step 3 Provide a name and description.

Step 4 Add **Request Rate Limits**.

Limiting excessive requests to a resource is based on the following parameters. The values for these parameters should be based on measuring and understanding the traffic patterns for your web services to be protected by the Layer 7 DOS option.

Table 2: Parameters

Parameter	Description
URI	A relative URI used to indicate the path to limit requests for a resource. For example, if you intend to monitor and protect your service resource at https://www.example.com/login.html, you would enter /login.html as the URI parameter in the **Request Rate Limits** table.
HTTP Methods	HTTP methods can be specified per-resource URI to control which HTTP methods in the client requests are rate limited and which ones are not. You can select multiple methods from the drop down for each row in the table. An empty HTTP method list means that method is ignored and the rate applies to all calls to the resource. **Note** The rate is applied per-resource; therefore, multiple methods share the rate limit specified in the Request Rate in that row. For example, if the rate is 3 requests per second, and GET, POST and PUT are specified in the HTTP Methods, and 2 GETs and 1 POST happen to that URI from a single client IP in the same second, a PUT will NOT be allowed in that same second.
Request Rate	Thenumber of requests per second. It determines the rate at which a single client can send requests to the URI resource mentioned in the URI part of the rule.
BurstSize	Specifies the maximum number of simultaneous requests that a client can send to the URI resource mentioned in the URI part of the rule. Any requests beyond this threshold, arriving at the proxy at the same time, will not be sent to the backend server.

Step 5 Click **Save** when completed.

Note The order of the rules is important based on the URI as the rules are checked from the top down and applied on first match. If the URI added higher in the list includes a resource path that includes resources in the rules below it, the first rule matched will be applied.

Example

Two (2) web service resources are protected:

1. /login.html is limited to a smaller rate and burst size, and both GET and POST methods share the rate as explained above. All other methods are allowed without any rate limiting applied to them.
2. /index.html is limited to a larger rate and burst size, and only GET calls are rate limited.

What to do next

- **Service Object Association**

  Once the Layer 7 DOS Protection Profile has been created, it needs to be associated with the ReverseProxy Service Object representing the listener and the connection to the backend server address.

- **Associate L7 DoS Profile with a Policy Rule**

  Check this document to create/edit Policy Rules.