How to Configure Exception Profiling

https://campus.barracuda.com/doc/4259904/

Exception Profiling

Exception Profiling fine-tunes security policies associated with a service to reduce incorrectly blocked requests. Typically, when a service is created, it is associated with the default security policy. All URLs and parameters are compared to the default security policy settings, which may block some genuine requests. Blocked genuine requests are called false positives. Exception Profiling uses a heuristics-based strategy to refine web application security settings in response to logged traffic in the Web Firewall logs, viewable on **BASIC > Web Firewall Logs**. It reduces the false positives either by creating URL and parameter profiles that relax the default security policy settings or by modifying existing URL profile or parameter profile settings, thereby fine-tuning them to the service. If a profile does not exist, Exception Profiling can create a new profile. If a profile does already exists, it is fine-tuned to reflect the exception.

You can enable Exception Profiling for a service by clicking **Edit** next to the service on the **WEBSITES > Exception Profiling** page and setting the Exception Profiling level to one of three levels for untrusted traffic. Each level has corresponding settings for exception handling. The levels are:

- Low
- Medium
- High

Trusted traffic is always handled according to separately configured Trusted settings.

Exception Profiling Levels

A **Low** profiling level indicates a low tolerance to violations, so logged traffic violations are reviewed frequently to properly adjust security settings. On the other hand, a **High** profiling level indicates a greater tolerance of violations and a higher confidence in the security settings, so review or adjustment of the profile only happens if a violation is seen more frequently. Exception Profiling treats traffic violations differently for trusted hosts. Trusted hosts heuristics have a trigger count permanently set to one (1) for all violations. Any request from a trusted host is assumed to be a genuine request, so an exception from any trusted host automatically refines security, creating or modifying profiles for the service as required.

Because only three levels of Exception Profiling heuristics for untrusted traffic apply to all services, a change in the settings of any level applies to any service using that level (Low, Medium, or High). Exception Profiling provides default settings for each violation type. The settings indicate how

exceptions update profiles (Automatically, Manually, or not at all), how the new setting in the profile is generated (increasing the current value, or accepting the observed value, for example), and how many times the logged error needs to be seen before generating an exception (trigger count). These default settings for an Exception Profiling level can be edited and saved. For information on how to edit request violation settings, see Configuring Exception Heuristics.

Selecting an Exception Profiling level of **Low** will increase the number of exceptions or recommendations for profile adjustment, causing a more rapid adjustment of the profile to reflect observed traffic. On the other hand, an Exception Profiling level of **High** results in fewer exceptions and pending recommendations, indicating increased confidence in the profile, and higher tolerance for traffic violations. The **Trusted** profiling level is recommended for trusted hosts.

Configuring Exception Profiling

You can configure Exception Profiling for a service by setting the Exception Profiling level, thereby applying the corresponding Exception Heuristics settings to that service. Perform the following steps to configure exception profiling:

1. From the **WEBSITES > Exception Profiling** page, identify the service for which you want exception profiling enabled.
2. Click **Edit** next to that service. The **Edit Exception Profiling** window appears.
3. To learn from a trusted hosts group, select the trusted host group from the **Trusted Hosts Group** drop-down list and set **Learn From Trusted Host Group** to *Yes*. For information on trusted hosts, see Configuring Trusted Hosts .
4. To learn from untrusted traffic, select the level of tolerance to violations (Low, Medium, or High) from the **Exception Profiling Level** drop-down list. For information on exception profiling levels, see Exception Profiling Levels .
5. Click **Save**.

Configuring Exception Heuristics

The **WEBSITES > Exception Heuristics** page allows you to view the definitions for any exception profiling level and adjust settings for various violation types if required.

Exception Profiling Level Settings

The Exception Profiling level determines the exception creation heuristics for the service to which it is bound. Four policies, or levels, are provided: Low, Medium, High (for untrusted traffic), and Trusted.

To view the settings for a profiling level:

1. Go to the **WEBSITES > Exception Heuristics** page.
2. Select the desired level to view the heuristics settings in the **Exception Profiling Level** module, and click **Show Definition**.

The **Request Violation Handling** module gets populated with the settings for that level and can be modified. The levels are shareable across multiple services. Any change made to an exception heuristics level setting applies to any service bound to this level. Services may have an untrusted traffic exception profiling level (Low, Medium, or High) as well as designated trusted hosts using the Trusted Hosts exception profiling settings.

The exception heuristics for various violation types are classified into the following:

- Length Violations
- Input Violations
- Header Violations
- Cookie Violations
- Forceful Browsing

For each violation type, set the following parameters:

- **Setting** – How exceptions are created: Automatically, Manually through approval of pending recommendations, or no exceptions should be created.
- **New Value** – How to modify the parameter after learning. New Value can be a function of the old value (increase 100%, for example). Or the new value can be based on the default option provided. New Value is selected from provided options.
- **Trigger Count** – This threshold sets the number of times a violation must be received from unique sources before triggering exception learning either automatically or manually. Only unique requests from a client are counted. Multiple violations from the same client generate a single violation in the trigger count. This neutralizes a hacker conducting repeated attacks on the service. An exception profiling agent processes the web firewall logs that generated the violations defined on the Exception Heuristics page. It maintains a cache of the trigger counts and compares the running count with the configured trigger count. When the trigger count is met, it invokes the exception profiling process.

Learned false positives are either applied automatically or displayed on the **WEBSITES > Exception Profiling > Pending Recommendations** section every 600 seconds (10 mins) depending on **Setting** (Auto or Manual).

When set to *Auto*, the profiles are automatically updated every 600 seconds. If set to *Manual*, the recommendations are generated after 600 seconds and displayed on the **WEBSITES > Exception Profiling > Pending Recommendations** section.