How to Configure Adaptive Profiling

https://campus.barracuda.com/doc/4259863/

Overview

Adaptive Profiling and Exception Profiling are the two significant modules incorporated to fine-tune the security settings of a service. Exception Profiling works with generated log files to refine security settings, customizing them to the web application. For more information on Exception Profiling, see How to Configure Exception Profiling. Adaptive Profiling analyzes the request and response traffic to generate customized security profiles for the web application.

Adaptive Profiling learns the intricate structure of an application and enforces conformance to that structure. Detailed security profiles are created by learning from requests and responses served by a particular web application. Learning creates a positive security model by generating valid URL and parameter profiles.

The learned structure of the application is called a profile of the website. A website profile consists of individual URL and parameter profiles. These profiles are initially generated using the settings in the default security policy, but over time the profiler refines them to accurately reflect the safe incoming traffic for the web application.

How Adaptive Profiling Differs from Exception Profiling

In Exception Profiling, URL and parameter profiles are created for a service in Active mode on the **WEBSITES > Website Profiles** page. This means any created profiles are immediately in Active mode. So in this case, profiles are created/updated periodically, every 600 seconds (10 minutes), and then only when violations from unique sources are encountered the number of times indicated in **Trigger Count** on the **WEBSITES > Exception Heuristics** page. To learn more about how profiles are created in Exception Profiling, see Configuring Exception Profiling. In Adaptive Profiling, the entire service is in Learning mode, so any URL and parameter profiles created for the service are in Learning mode. In Learning mode, violations are logged on the **BASIC > Web Firewall Logs** page. Any changes in the request or response are learned and respective URL and/or parameter profiles are created/updated instantly.

Enabling Adaptive Profiling for a Service

By default, adaptive profiling is disabled.

Steps to Enable Adaptive Profiling for a Service

1. Go to the **WEBSITES > Website Profiles** page.
2. Select the service you want to "learn" from the **Website** drop-down list.
3. Click **Start Learning**.
4. Navigate to the **WEBSITES > Adaptive Profiling** page and verify the **Status** is set to *On* for the relevant service.

Editing Adaptive Profiling Settings

By default, each service is configured for adaptive profiling with predefined settings. The predefined settings include **Request Learning** and **Response Learning** set to *Successful* and learning **Status** set to *Off*. To modify the predefined settings for adaptive profiling, do the following:

1. From the **WEBSITES > Adaptive Profiling** page, identify the service to requiring modification of adaptive profiling settings.
2. Click **Edit** next to that service. The **Edit Service Adaptive Profiling** window appears.
3. Specify values for the required fields and modify the learning settings if required:
   - **Status** – By default, this is set to *Off*. To enable adaptive profiling for the service, see Enabling Adaptive Profiling for a Service.
   - **Request Learning** – Specify when to learn the requests:
     - *Successful* – Learn from requests that result in a successful response (Usually 200 OK).
     - *Trusted* – Learn only if the requests are from trusted client IP address(es).
     - *None* – No requests are learned.
   - **Response Learning**– Specify when to learn the responses:
     - *Successful* – Learn elements only from successful responses (Usually 200 OK).
     - *Trusted* – Learn the responses only if the request sent was from trusted client IP address(es).
     - *None* – No elements in the response are learned.
   - **Navigation Parameters** – Enter the constant query parameters that are shared among multiple URLs. For example, consider the Barracuda Web Application Firewall user interface URL: **http://waf.barracuda.com/cgi-bin/index.cgi?primary_tab=basic&secondary_tab=status** . Here, the values of primary tab and secondary tab together determine which page displays. Different value combinations of parameters display completely different pages. For more information on navigation parameters, see Working with Navigation Parameters .
   - **Ignore Parameters** – Enter the list of parameters that should be ignored while learning the corresponding URL profile. A "*" is allowed as a prefix or suffix. For example, an Ignore Parameter "ctl*" would result in ctl1, ctl2, ctl3, etc. being ignored during learning, so no parameter profiles for parameters ctl1, ctl2 and ctl3 would be created/updated.
   - **Trusted Hosts Group** – Select the trusted hosts group to which **Request Learning** and/or **Response Learning** are restricted. To learn more about trusted hosts, see

Configuring Trusted Hosts.
- **Content Types** – Enter the type of content to be learned from the responses.

4. Click **Save** to save your adaptive profiling settings.

Adding an Adaptive Profiling Rule

The **WEBSITES > Adaptive Profiling** page enables you to add Adaptive Profiling rules for a URL space that needs to be learned. One or more rules can be created for a URL space and host match.

To Add an Adaptive Profiling Rule

1. From the **WEBSITES > Adaptive Profiling** page, identify the service to which you want to add a rule.
2. Click **Add** next to that service. The **Add Adaptive Profiling Rule** window appears. Specify values for the following fields:
   - **Learn Rule Name** – Enter a name to identify the adaptive profiling rule.
   - **Status** – Set to *On* to enable learning for this rule.
   - **URL Match** – Enter a URL to be matched against the URL in the request. The URL should start with a "/" and can have at most one " * " anywhere in the URL. Examples: **/Bank/Forms/***, **/images/***.
   - **Host Match** – Enter the host to be matched against the host in the request. The host match can either be a domain name or IP address. A value of '*' means it matches any domain. Examples: **www.mysite.com**, **192.168.128.2**
   - **Learn From Request** – Set to *Yes* to learn the client requests and create/update URL and parameter profiles if the URL and/or domain space defined above matches. The URL and parameter profiles are created/updated for the corresponding service on the **WEBSITES > Website Profiles** page. Learning from requests includes:
     - URL profile for the requested URL.
     - Parameter profiles for the query parameters (if any).
     - Parameter profile for the FORM parameters (if any).
   - **Learn From Response** – Set to *Yes* to learn the server responses and create/update URL and parameter profiles if the URL and/or domain space defined above matches. The URL and parameter profiles are created/updated for the corresponding service on the **WEBSITES > Website Profiles** page. Learning from responses includes:
     - URL profiles for the links embedded in the response and corresponding query parameter profiles (if any), provided they match the URL and host matching expressions for any one of the Adaptive Profiling rules.
     - URL profile for the URL that is found as an action URL or a URL with a query string in the response.
     - Parameter profiles for the FORM parameters of those forms whose action URL matches the above expressions body.
3. Click **Add** to add the rule you just configured.

How Adaptive Profiling Rules Are Matched

A service can be configured with one or more rules with different URL spaces. When learning is enabled, the Barracuda Web Application Firewall uses a best-match algorithm to match the most specific request URL rule. If no rules are configured for a service, learning is enforced on all URLs based on the default Adaptive Profiling settings of that service. To see the default adaptive profiling settings, click **Edit** next to the service. See Editing Adaptive Profiling Settings.

> Rules must be created before enabling Learning for a service.

For example, consider the following two rules configured for a service (Service_1):

Learn Rule Name – Rule 1

- Status – On
- URL Match – **/Bank/Forms/***
- Host Match – **www.a_bank.com**
- Learn From Request – No
- Learn From Response – Yes

Learn Rule Name – Rule 2

- Status – On
- URL Match – **/***
- Host Match – **www.a_bank.com**
- Learn From Request – Yes
- Learn From Response – Yes

For a request for **www.a_bank.com /Bank/Forms/loan.html**, Rule 1 is considered as the best match.

Working with Navigation Parameters

To distinguish between two requests with the same URL but different query parameters, specify those parameters as Navigation Parameters. By doing so, a page is uniquely defined using the combination of the request URL and the navigation parameter settings. To define navigation parameters for a Service, edit the Adaptive Profiling settings. SeeEditing Adaptive Profiling Settings.

For example, consider the following Barracuda web user interface URL:

http://waf.barracuda.com/cgi-bin/index.cgi?primary_tab=basic&secondary_tab=status

Here, the values of query parameters primary_tab and secondary_tab together determine which page displays. Different value combinations of navigation parameters display completely different pages, containing different FORM elements and content.

To protect this application, primary_tab and secondary_tab would be defined as Navigation Parameters forcing the profiler to generate separate profiles for each possibility. For example, the above case would produce the following profiles:

/cgi-bin/index.cgi?primary_tab=basic&secondary_tab=ip_config

/cgi-bin/index.cgi?primary_tab=basic&secondary_tab=services

/cgi-bin/index.cgi?primary_tab=advanced&secondary_tab=troubleshooting

By default, parameters are considered non-navigation parameters.