Step 3: Configuring Basic Service Settings

https://campus.barracuda.com/doc/4259891/

After a service is created, a basic set of web firewall features are activated automatically using the Barracuda default security policy. The service defaults to a *pa ssive* mode of enforcement using the default security policy.

Configuring Service Settings

The default configuration options provide a sufficient amount of attack protection from the majority of web attacks. Refinements to the default security policy can be required for different web applications. You can edit basic service settings to tailor attack prevention for a service. To edit service settings, go to the **BASIC > Services** page, identify the service you want to edit in the **Services** list, and click **Edit** next to it. The service window displays the following sections:

- Service
- Basic Security
- SSL
- Load Balancing

Service

Verify the settings displayed are correct. Modify the settings if necessary.

Basic Security

You can modify the basic set of web firewall options in the **Basic Security** section. Specify values for the following fields:

    - **Web Firewall Policy** – By default, all services are associated with the default security policy. To enforce a new security policy, click the drop-down list and select the desired security policy. The list includes security policies provided by the Barracuda Web Application Firewall (default, SharePoint, SharePoint2013, OWA, OWA2010, OWA2013, and Oracle) and any previously saved customized policies. To create a new policy or to edit an existing policy, see Security Policies. If you wish to fine-tune the Security Policies, see Tuning Security Rules Using Web Firewall Logs .
    - **Web Firewall Log Level** – Threshold for logging the error messages for the service. This

log level determines whether only the most urgent attack information or less serious attack information, including warnings or debug information, is written to the logs. For example, if the log level is set to *3-Error*, logs with 0-3 log levels are logged in the **BASIC > Web Firewall Logs** page. The 0-3 log levels include 0-Emergency, 1-Alert, 2-Critical and 3-Error logs.

  - **Mode** – The mode determines how the service responds to offending traffic. It can either be Active Mode or Passive Mode.
    - *Passive* mode logs violating events but allows the request to pass through. This is the **default** mode.
    - *Active* mode performs the action configured in association with the perceived threat.
      Note: *Passive* mode is recommended in the initial stages of deployment so that traffic to the service is not broken due to false positives. All traffic translation rules continue to work in both Active and Passive modes. Refer to the Modes (Active / Passive) : Additional notes section below for more details.
  - **Trusted Hosts Action** – You can override default settings and configure a specific response to violations for a set of trusted hosts accessing the service. If set to *Allow* or *Passive*, all requests from trusted hosts, including those that are possible attacks, are ignored and passed through. *Allow* mode does not log events, whereas in *Passive* mode, events are logged. Set to *Default* if trusted hosts requests do not need special handling.
  - **Trusted Hosts Group** – Select the trusted hosts group to which you want to apply the configured trusted hosts action. **Trusted Hosts** and **Trusted Hosts Groups** are configured in the **WEBSITES > Trusted Hosts** page.
  - **Ignore Case** – This determines how the service URLs are matched to rules like URL, ACL, and URL profiles. When set to *Yes*, text in upper or lower case can match the specified URL for any Barracuda Web Application Firewall rule. **Note**: This is applicable only to URLs and not parameter names.
  - **Header Name For Actual Client IP** – Header name for the client IP address that the server stores for identification.

    > Enabling the Client IP header name will automatically allow all IP-related features to check the header value.
  - **Rate Control Status** – Set to *On* to bind a rate control pool to limit the rate of requests for the service.
  - **Rate Control Pool** – If the rate control pool is configured with a set of preferred clients, then the rate control policy is applied only to the requests from the preferred clients. Otherwise, the rate control policy is applied to all requests forwarded to the service.

Modes (Active / Passive) : Additional notes

The Barracuda Web Application Firewall executes the following operations in both active and passive modes if they are configured by the administrator.

- All SSL configurations for the front-end and back-end connections.
- Insertion of JavaScript code for client tracking.
- Submission of traffic data to the cloud layer for analysis if an Advanced Bot Protection license has been purchased and if data submission has not been explicitly turned off.

- Client-side checks for web scraping such as run-time modification of robots.txt, insertion of cooking, and JS file checks.
- Enforcement of CAPTCHA / reCAPTCHA for suspicious clients in App DDoS rules.
- All network-level rules and Network Firewall rules.
- Enforcement of Access Control rules
- Website Translation rules that rewrite content, URLs, and domains in HTTP requests and responses.
- Malformed HTTP requests are not processed and will be denied in the Passive mode.

In addition to the mode being configured at the service, rule group, or specific rule level, the mode is also configured for individual smart signatures. This can be validated in the **ADVANCED > View Internal Patterns** page.

SSL

See: Configuring SSL for SSL Enabled Services.

Load Balancing

See Configuring Load Balancing for a Service.

You can configure additional security for a service by using URL policies. URL policies allow Anti-Virus protection, Data Theft protection, and Brute Force protection to be enabled or disabled for specific URL spaces.