

## Access, Firewall, and Event Logs

<https://campus.barracuda.com/doc/76284371/>

Barracuda WAF-as-a-Service includes Firewall Logs, Access, and Event Logs.

- **Firewall Logs** are generated whenever suspicious HTTP requests are detected and denied, based on access control lists.
- **Access Logs** are generated for all user requests, providing information about website traffic and performance.
- **Event Logs** are generated for specific network activity, including events related to Certificate, DDoS, or DNS.

For information on Audit Logs, refer to [Audit Logs](#).

For information on Event Log Messages, refer to [Event Log Messages](#).

To view logs for an application:

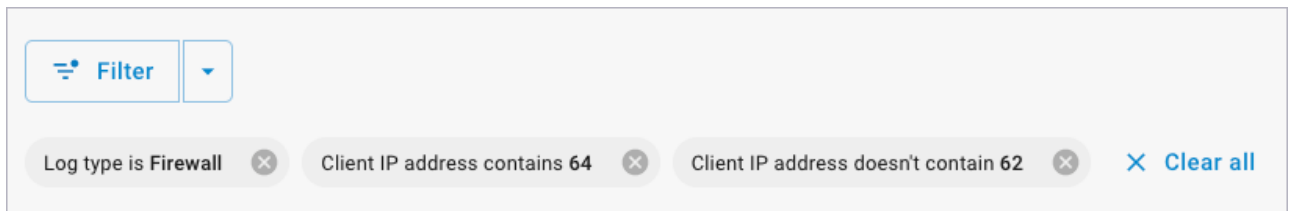
1. Under **Applications**, click an application.
2. In the left navigation bar, click **Logs**. On the **Logs** page, select **All Logs**, **Firewall Logs**, **Access Logs**, or **Event Logs**.
3. For details on a specific log entry, click the plus icon for the record. The record expands to reveal details about the event.


## Focusing Log Results

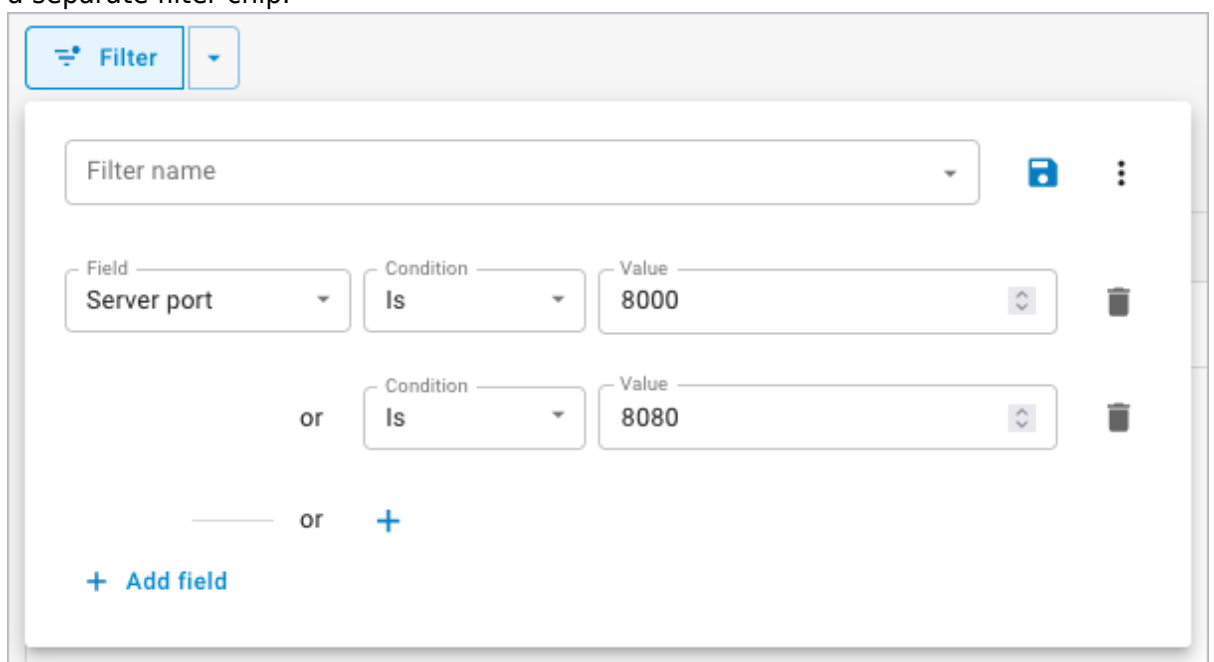
You can build filters to focus on specific log data, including Query Strings, URLs, and Methods.


### Steps to create a filter

1. Click the **Filter** button to bring up the filter builder model.
2. You can ignore the **Filter name** field unless you plan on saving the filter you create.
3. Use the **Field**, **Condition**, and **Value** fields to create a filtering expression. The **Field** and **Condition** fields are dropdown lists you can select from. The **Value** field can either be a dropdown list or fill in depending on your other selections. As you complete each expression, the logs will automatically update to reflect the search criteria you entered. Also, the expression and any others you create will appear as filter chips above the logs.



- Expressions can be removed by clicking the garbage can icon  or clicking the **X** on the filter chip.
- Some expressions come with the option to add an "Or" scenario. Example: if you select **Server port** in the **Field** dropdown list, the word "**Or**" and a plus sign **+** appear. Click the plus sign to extend the expression. Each portion of the expression will appear as a separate filter chip.



- Click **Add field** to add additional filter criteria.
- When viewing the details of a log item, many of the fields can be added to the existing filter by clicking the  icon. This additional filtering will occur immediately and a filter chip will be added above the logs.

### Specifying a Date Range


To filter by specific dates, click the date/time filter. There, you can:

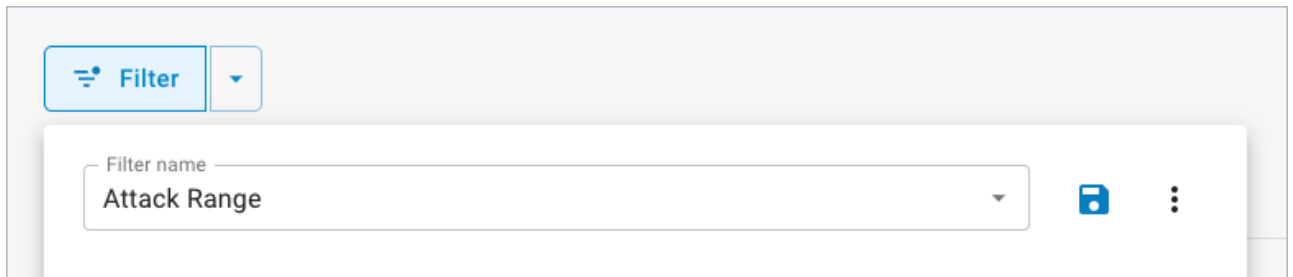
- Choose a pre-defined Quick Range value, like the last 7 or 30 days.
- Define a custom date and time range.

### Saved Filters

#### Save a filter


- Click the **Filter** button.
- Enter a **Filter name**.

3. Configure as many filter expressions as you like.
4. Click the Save icon  to the right of the **Filter name** field.



#### Using a saved filter




You can find the saved filters by clicking the down arrow  next to the **Filter** button, or by clicking the **Filter** button and selecting from the **Filter name** dropdown list. The filter expressions will display for any saved filter you select.

#### Edit a saved filter

1. Click the down arrow next to the **Filter** button and select the saved filter you want to edit.
2. Click the **Filter** button to see the parameters configured for this filter.
3. Add, delete or change any desired parameters.
4. Click the Save icon to the right of the **Filter name** field.

#### Delete a saved filter

1. Click the down arrow next to the **Filter** button and select the saved filter you want to edit.
2. Click the **Filter** button to see the parameters configured for this filter.
3. Click the three dots  to the right of the **Filter name** field.
4. Select **Delete**.
5. Confirm that you would like to delete the filter.

#### Resetting Filters

There are three ways to reset or reduce the amount of filtering.

- Click the **X** on one or more of the filter chips. The page will automatically update and show results that include only the remaining filter parameters.
- Click the **Clear all** link to the right of the filter chips. All filtering will be removed and the results will automatically update.
- Click the **Filter** button and add or remove parameters from currently displayed results. The results automatically update.

---

## Downloading Log Data

---

When you have focused your log results, click **Download**. A CSV file of your results downloads automatically.

Note that there is a limit to the number of rows you can download. Only the first 10,000 rows of data can be exported to a CSV file. If your table displays more than 10,000 rows, a warning displays, instructing you to use more restrictive filters to view a smaller set of data, so you can download all of the log rows.

### Converting Timestamps to a Readable Time and Date Format

The exported CSV file will have the **Date** column in a timestamp format, meaning each date will show up as the number of milliseconds since January 1, 1970 (epoch timestamp x 1000). Most spreadsheet applications will have a way to convert to something more easily readable. The following steps apply to most Microsoft Excel versions:

1. Open the downloaded CSV file in Excel.
2. Right click at the top of the column to the right of the **Date** column. Example: For the Access Logs, column **B** contains the time and date, so you would right click at the top of column **C**.
3. Select **Insert** in the menu that opens. This creates a new, empty **C** column.
4. In the second field of column **C** (row 2), enter this formula:  $= ( (B2/1000) / 86400 ) + 25569$  and copy down by clicking and dragging from the bottom-right corner of this field.
  - For an understanding of this formula, see <https://www.epochconverter.com>. Note that we divide by 1000 because our timestamps are in milliseconds.
5. Right click at the top of column **C** and select **Format cells**.
6. Choose your desired format. Example: 3/14/22 1:30 PM. All data in this column will then match this format.

## Marking as False Positive

---

When you review Firewall Logs, you might encounter a log entry that is a false positive: that is, where Barracuda WAF-as-a-Service detected a request as an attack, but the request was legitimate. Most often, this happens because a default limit on Barracuda WAF-as-a-Service is too restrictive.

To allow the legitimate request through, you must loosen security rules. It is advisable to loosen only the rules required, only for that particular page and/or parameter, and only by the minimum amount necessary to allow the legitimate request through. In many instances, Barracuda WAF-as-a-Service can do this automatically for you.

To loosen a restriction:

1. In the Firewall Log, locate the entry that is a false positive.

LOG TYPE	DATE (GMT-0800)	ID	CLIENT IP	METHOD	STATUS	DESCRIPTION	URL
Firewall	2023-01-31 10:34:06	186091b8e11-3de09130	162.142.125.210	PRI	Logged	Error Response Suppressed	/*
<div> <div> <b>Event details</b> <p>Log type: Firewall</p> <p>Date: 2023-01-31 10:34:06</p> <p>ID: 186091b8e11-3de09130</p> <p>Severity: Notification</p> <p>Processor ID: 9911184</p> </div> <div> <b>Client details</b> <p>Client IP: 162.142.125.210:52332</p> <p>Country: United States</p> <p>Host: 10.244.0.123</p> <p>User Agent: Unknown</p> <p>Session ID: </p> <p>Authenticated user: </p> <p>Referer: </p> <p>Processor ID: 9911184</p> </div> <div> <b>Attack details</b> <p>Attack category: Outbound Attacks</p> <p>Attack: Error Response Suppressed</p> <p>Detail: code="400"</p> </div> <div> <b>Prevention details</b> <p>Action: LOG</p> <p>Follow Up Action: NONE</p> </div> </div> <div> <b>Request details</b> <p>Endpoint: app987293.azurelab.cudawaas.com</p> <p>URL: /*</p> <p>Method: PRI</p> <p>Query string: *</p> </div> <div> <b>Bot protection</b> <p>Client risk score: 0</p> <p>Request risk score: 420</p> <p>Client fingerprint: g_c5a999a0b18228f0b4f6f602bf8bba9b</p> </div>							
							<a href="#">Mark as False Positive</a>

2. Click **Mark as False Positive**, in the lower right corner of the screen.  
 Barracuda WAF-as-a-Service will suggest one or more configuration changes that will allow this request through. If more than one option is shown, you will typically choose the one that Barracuda WAF-as-a-Service displays as **Recommended**; however, review all the options and choose the one that is most appropriate for your application.

### Mark as False Positive

Error responses from your application server can often contain sensitive information and even snippets of your source code. To prevent this, WAF-as-a-Service cloaks error responses by default.

Your application configuration will be changed so that this kind of request will not be blocked in the future. Please choose from the suggested configuration changes below:

#### Stop cloaking status codes

☒ This will stop cloaking all error responses from your application server. Ensure no sensitive data is passed in error responses from your application server.

**RECOMMENDED**

COMPONENT	ATTRIBUTE	CURRENT	NEW
Response Cloaking	cloak_status_code	true	false

#### Pass through HTTP code 400

☐ This will allow all responses from your application server with this code to be passed through as-is. Ensure no sensitive data is passed in this error.

COMPONENT	ATTRIBUTE	CURRENT	NEW
Response Cloaking	status_codes_to_pass_thro...	404	404,400

[Cancel](#)
[Apply change](#)

3. Click **Apply Change**.

## Figures

1. search-chips.png
2. garbage-can-icon.png
3. plus-icon.png
4. server-ports.png
5. add-field-to-filter.png
6. save-button.png
7. filter-name-field-and-buttons.png
8. down-arrow.png
9. three-dots.png
10. log-detail.png
11. mark-as-false-positive.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.