

Types of Logs

<https://campus.barracuda.com/doc/78810008/>

This section provides a description of each type of log on the Barracuda Web Application Firewall.

Note: The number of logs stored in the system depends on the model of the Barracuda Web Application Firewall. The details are available [here](#).

Web Firewall Logs

Web Firewall logs are generated whenever suspicious activities, as specified in the access control lists, are detected. The log contains entries for every HTTP request that the Barracuda Web Application Firewall has denied. This data allows the administrator to identify the client that made the request, the method used, and the result of the request. Using these logs, you can fine-tune the security settings. For more information, see [Tuning Security Rules Using Web Firewall Logs](#).

When a service is created, the default web firewall policy is associated with the service, and the threshold for logging error messages is initially set to 5-Notice. At that threshold, all violations/error messages (critical attack information to debug information) are logged on the **BASIC > Web Firewall Logs** page. You can change the log level, based on your requirements, by editing service on the **BASIC > Services** page.

Note:

- Whenever a log is generated in **Web Firewall Logs** and **Access Logs**, a unique ID (UID) is associated with the log. You can select the filter option **ID** and enter a unique ID to search for a specific log.
- The unique ID can be embedded in the custom response page. For more information, see [How to Create a Custom Response Page](#).

Access Logs

Access logs are generated for all user request patterns. Access logs allow you to monitor the web traffic that passes through the Barracuda Web Application Firewall for a specific user traffic pattern, or for a group of patterns. These logs provide information about website traffic and performance.

Access logs are enabled by default. To disable Access logs, edit the service on the **BASIC > Services** page and set **Enable Access Logs** to **Off**.

Audit Logs

Audit logs are generated whenever users log in or log out of the web interface of the Barracuda Web Application Firewall, except in a few rare cases:

The **Login** action is not logged when:

- The maintenance command is executed by a user or by the Barracuda Web Application Firewall. A new login session will be created in maintenance mode, but it will not be logged.

The **Logout** action is not logged, when:

- The Barracuda Web Application Firewall is restarted because critical processes have crashed, in which case the current existing sessions will not be logged out.
- The Maintenance command is executed by a user or by the Barracuda Web Application Firewall, in which case the current existing sessions will not be logged out.

System Logs

The System logs provide a centralized collection point for all types of error reports, system alerts, diagnostic messages, and status messages of the Barracuda Web Application Firewall. Both hardware and software components of the Barracuda Web Application Firewall generate System logs providing information about the problems and performance of a module. System logs are required for security and troubleshooting. System logs are enabled by default and are displayed on the **ADVANCED > System Logs** page.

Network Firewall Logs

The Network Firewall logs are generated whenever network traffic passing through the interfaces (WAN, LAN, and MGMT) matches a configured Network ACL rule. Network Firewall log entries provide information about each packet the Barracuda Web Application Firewall allowed or denied based on the **Action** specified in the ACL rule. This data allows the administrator to identify where network traffic originated, was destined for, and the action applied.

Filtering Log Entries

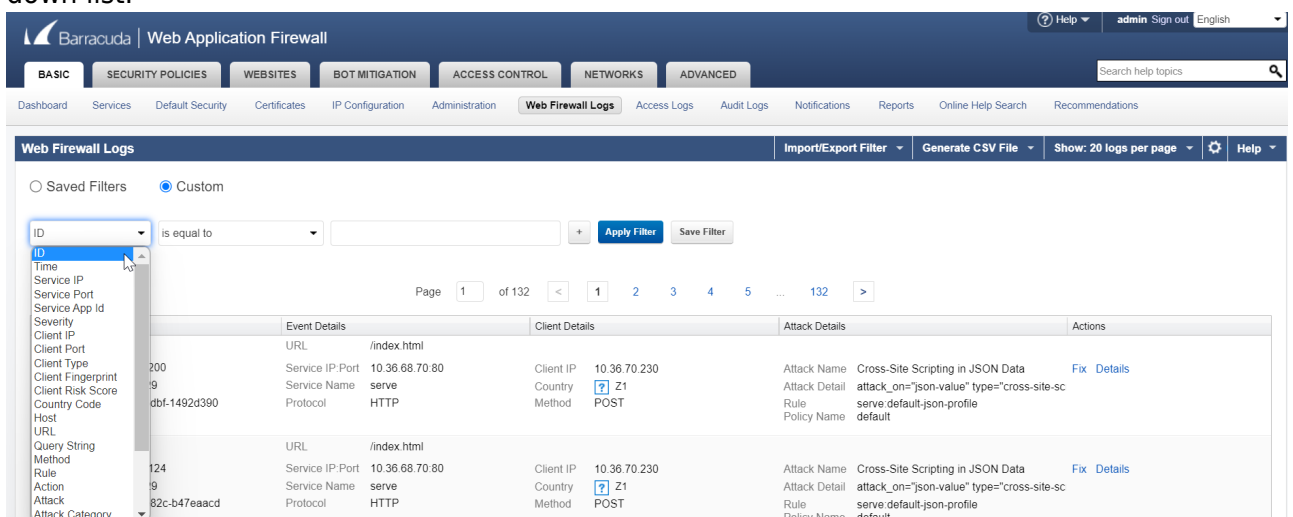
You can use filters to quickly locate specific types of log entries. The applied filter can be saved locally on the Barracuda Web Application Firewall for later use. A filter can be created with specific search criteria or multiple search criteria can be combined together with the help of the AND operator. The saved filters are displayed when **Saved Filter** is selected from the **Select Filter** drop-down list.

Whenever a log is generated in Web Firewall logs and Access logs, a unique ID (UID) is associated with the log. You can select the filter option **ID** and enter a unique ID to search for a specific log.

You can also specify the range for some of the filters, such as "Client Port" in **BASIC > Web Firewall Logs**, "Time Taken (ms)", "Client Port", "Bytes Sent", and "Bytes Received" in **BASIC > Access Logs**, "Source Port" and "Destination Port" in **NETWORKS > Network Firewall Logs**, and "Event ID" in **ADVANCED > System Logs**. The range should be specified with a <start value> and an <end value> separated by a comma (,). For example, the range for the client port can be specified as: 4000,7000.

Save a Filter with Specific Search Criteria

1. Select the **Custom** radio button.
2. Select a filter from the drop-down list. For example, the filter "ID" is selected from the drop-down list.



The screenshot shows the Barracuda Web Application Firewall interface. The top navigation bar includes tabs for BASIC, SECURITY POLICIES, WEBSITES, BOT MITIGATION, ACCESS CONTROL, NETWORKS, and ADVANCED. The 'Web Firewall Logs' tab is active. Below the navigation bar, there are links for Dashboard, Services, Default Security, Certificates, IP Configuration, Administration, Web Firewall Logs, Access Logs, Audit Logs, Notifications, Reports, Online Help Search, and Recommendations. The 'Web Firewall Logs' section has a sub-header with 'Import/Export Filter', 'Generate CSV File', 'Show: 20 logs per page', and a 'Help' link. The 'Custom' filter is selected. A dropdown menu is open, showing various filter options, with 'ID' selected. The main log table displays columns for Event Details, Client Details, and Attack Details. The first row shows an event with ID 200, URL /index.html, Service IP 10.36.68.70:80, Client IP 10.36.70.230, and an attack named 'Cross-Site Scripting in JSON Data'.

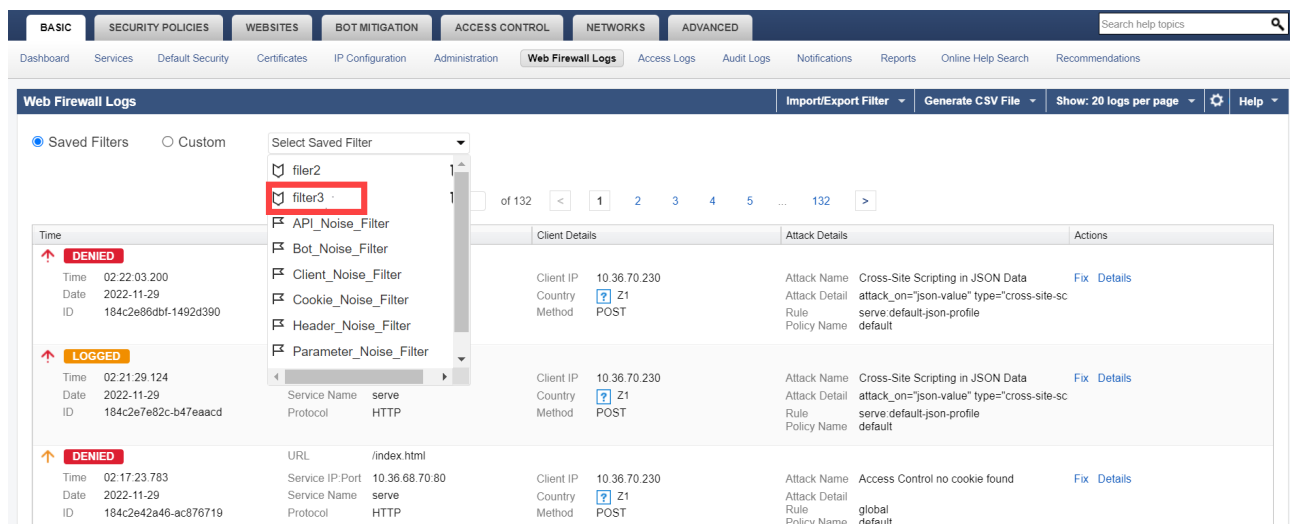
3. Select an operator from the drop-down list, and then specify a value for the selected filter.
4. Click the plus icon to add more search fields and click **Save Filter**. The **Save Filter** window appears.
5. In the **Save Filter** window, enter a name for the filter, add a description, and click **Save**.

Save a Filter with Multiple Search Criteria

1. Select a filter from the drop-down list. Click the plus icon to add more search fields.
2. Select an operator from the drop-down list for all the filters and then specify a value for the filters. You can add multiple search criteria that can be combined together with the help of the AND operator.
3. Click **Save Filter**. The **Save Filter** window appears.
4. In the **Save Filter** window, enter a name for the filter, add a description, and click **Save**.

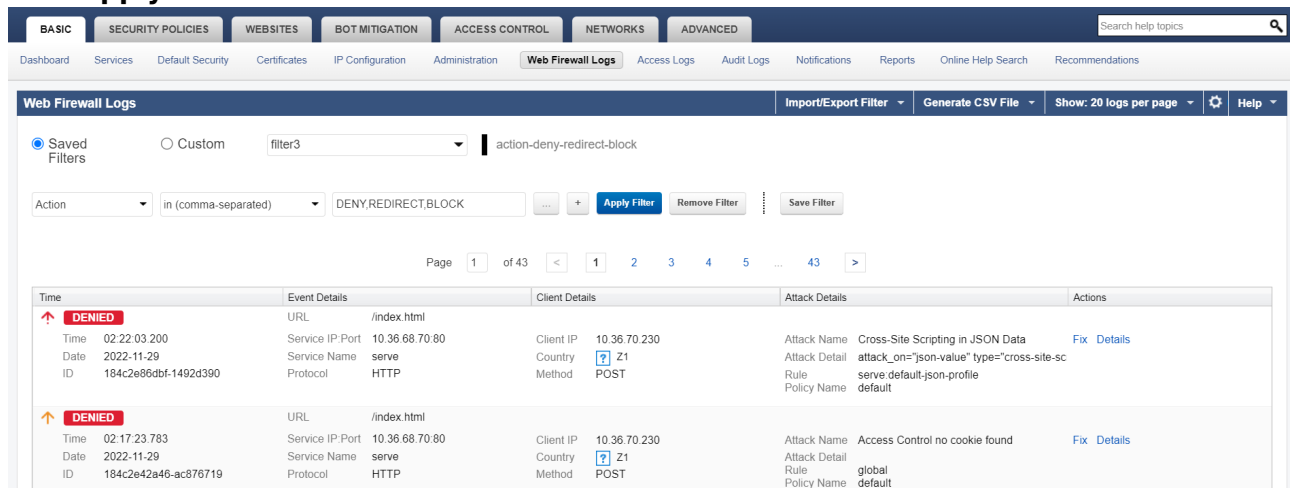
To apply a saved filter:

1. Select **Saved Filters** radio button.
2. Select the filter for which you want to view the logs from the **Select Saved Filters** drop-down list.



The screenshot shows the 'Web Firewall Logs' page. The 'Saved Filters' radio button is selected. A dropdown menu is open, showing a list of saved filters: 'filter2', 'filter3' (highlighted with a red box), 'API_Noise_Filter', 'Bot_Noise_Filter', 'Client_Noise_Filter', 'Cookie_Noise_Filter', 'Header_Noise_Filter', and 'Parameter_Noise_Filter'. The main log table displays three entries: a 'DENIED' entry for a Cross-Site Scripting attack, a 'LOGGED' entry for a successful request, and another 'DENIED' entry for an 'Access Control no cookie found' error.

3. Click **Apply Filter**.



The screenshot shows the 'Web Firewall Logs' page with the 'filter3' filter applied. The 'Saved Filters' radio button is selected, and the 'filter3' dropdown is set. The 'Action' field is set to 'in (comma-separated)' and 'DENY,REDIRECT,BLOCK'. The 'Apply Filter' button is highlighted. The main log table displays two entries: a 'DENIED' entry for a Cross-Site Scripting attack and a 'DENIED' entry for an 'Access Control no cookie found' error.

While using multiple search criteria, the same fields cannot be specified more than once. Specify the complete timestamp while searching for the log messages generated within the specified period. Regular expressions can be entered for these filters: URL and Rule.

Import a Saved Log Filter

1. Click the **Import/Export Filter** drop-down list and select **Import Log Filter**. The **Import Log Filter** window appears.
2. On the **Import Log Filter** window, do the following:
 1. **Filter Name**: Specify a name for the filter.
 2. **Import File**: Click **Choose File** to browse and select the log filter (JSON file) that needs to be imported.
 3. Click **Import File**.
3. After the import is complete, the filter is applied, and the logs are displayed as per the filter.

Export a Saved Log Filter

1. Click the **Import/Export Filter** drop-down list and select **Export Log Filter**. The **Export Log Filter** window appears.
2. On the **Export Log Filter** window, do the following:
 1. **Name**: Click the **Select Saved Filters** drop-down list and select the filter that you want to export.
 2. **Description**: Provide the description for the filter.
 3. **Filter**: Review the filter details.
 4. Click **Export Filter**.
3. After the download is complete, the filter is exported as a JSON file to your local machine.

Figures

1. Select_a_Filter.png
2. Select_Saved_Filter.png
3. Saved_Filter.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.