
History Page

<https://campus.barracuda.com/doc/41116101/>

The firewall history is the most powerful tool for troubleshooting. The following article lists the functionalities of the **History** page and explains how to configure the cache settings. To open the history view, click the **History** icon, located in the ribbon bar under the **FIREWALL** tab.

In this article:

Video

To get a feel for how to use the **FIREWALL > History** page in NG Admin, watch the following video:



Information Display

The **History** page displays all connections that were established on the Barracuda NG Firewall and provides several filtering options. You can view additional details for a specific session by double-clicking an entry.

The following information is provided for each session:

Info	Description
AID	Access ID, including an icon for blocked connections (red), an icon for established connections (green), and consecutive numbering for both blocked and established connections.
IP Proto	The protocol that is used. For example, TCP, UDP, or ICMP.
Port	The destination port (or internal ICMP ID).
Source	The source IP address.
Interface	The affected interface.
User	The username of the affected user and group.
Destination	The destination IP address.
Output-IF	The outgoing interface.
Next Hop	Next Hop
Application	The name of the affected application.
Application Context	The context of the affected application.
Count	Number of tries. The counter applies when a connection attempt hits a specific rule with Firewall History Entry enabled in the Advanced rule configuration. Removal of old entries is handled according to a fixed buffer size that can be adjusted in Infrastructure Services > General Firewall Configuration > History Cache .
Last	Time passed since last try.
Rule	The name of the affected firewall rule.
Info	Reason why things happen.
Org	Origin: <ul style="list-style-type: none"> • LIN: Local In; incoming traffic on the box firewall. • LOUT: Local Out; outgoing traffic from the box firewall. • LB: Loopback; traffic via the loopback interface. • FWD: Forwarding; outbound traffic via the forwarding firewall. • IFWD: Inbound Forwarding; inbound traffic to the firewall. • PXY: Proxy; outbound traffic via the proxy. • IPXY: Inbound Proxy; inbound traffic via the proxy. • TAP: Transparent Application Proxying; traffic via virtual interface. • LRD: Local Redirect; redirect traffic configured in forwarding ruleset.

MAC	MAC address of the interface.
Src NAT	The source NAT address.
Dst NAT	The destination NAT address.
Out Route	Unicast or local.
Protocol	The affected protocol.
Status	The status of the connection.
Src. Geo	The geographic source of the active connection.
Dst. Geo	The geographic destination of the active connection.
URL Category	Category of the destination URL.

Filter Options

To create a filter, click the arrow icon next to the respective filter in the filter section to expand the dropdown lists and select the required checkboxes.

- **Cache Selection** – From the **Cache Selection** list, you can select the following options to filter for certain traffic types:
 - **Access** – Displays all allowed and successfully established connections.
 - **ARP** – Displays all ARP requests.
 - **Fail** – Displays all connections matching the fail reasons.
 - **Rule Block** – Displays all connections matching deny reasons.
 - **Scan** – Displays all SCAN tasks.
 - **Packet Drop** – Displays all connections matching the drop reasons.
 - **Term** – Displays all terminated sessions.
- **Traffic Selection** – From the **Traffic Selection** list, you can select the following options to filter for certain traffic types:
 - **Forward** – Displays the traffic on the Forwarding Firewall.
 - **Loopback** – Traffic over the loopback interface.
 - **Local In** – Displays the incoming traffic on the box firewall.
 - **Local Out** – Displays the outgoing traffic from the box firewall.
 - **IPv4** – Show IPv4 sessions.
 - **IPv6** – Show IPv6 sessions.

The filter section also allows you to add filters for very specific properties by clicking the + icon.

Note that some fields allow the use of wildcards (*?; !*?). Example: !Amazon* excludes all entries starting with Amazon; Y*|A* includes all entries starting with "Y" or "A".

- **IP Protocol** – Allows setting a filter for a specific IP protocol.

- **Port** – Allows setting a filter for a specific port.
- **Source** – Allows setting a filter for a specific source IP address/range.
- **Source/Destination** – Allows setting a filter for a specific IP address/range that matches either source or destination.
- **Interface** – Allows setting a filter for a specific interface (for example eth0).
- **User** – Allows setting a filter for a user.
- **Destination** – Allows setting a filter for a specific destination IP address/range.
- **Output-IF** – Allows setting a filter for a specific output interface.
- **Application** – Name of the affected application.
- **App Context** – Context of the affected application.
- **Rule** – Allows setting a filter for a specific rule.
- **Any Interface** – Allows setting a filter for a specific forward or reverse interface.
- **Protocol** – Allows setting a filter for a specific protocol.
- **URL Category** – Filters for URL categories.
- **Source Geo** – Filters for the source host's geographic location.
- **Destination Geo** – Filters for the destination host's geographic location.

The size of the caches is configured in the **Firewall Settings** and requires a service restart.

Filter Icons

Clicking the first filter icon (**Open Live with same filter**) in the ribbon bar above the filters lets you switch to the [Live Page](#) with the same filters applied. Clicking the second filter icon (**Save and Restore Filter and Column Settings**) opens a dropdown menu that enables you to save, restore, or delete filter and column view settings.

Context Menus

Right-clicking into the listing makes the following context menus available:

- **Remove Selected** – Removes selected entries from the list. To select one or more entries, select an entry and use the shift and CTRL keys.
- **Flush Cache** – Removes all entries from the access cache, depending on the criteria selected selected in the sub-menu.
- **Show Hostnames** – Translates source and destination IPs to hostnames and vice versa. IP addresses will only be resolved to hostnames, if enabled in the firewall DNS settings.
- **Apply Rule Tester** – Offers the option for firewall rule testing.
- **Find** – Opens a search window at the top of the list.
- **Select All / Deselect All** – Selects / deselects all entries displayed on the list.
- **Copy <...> to Clipboard** – Copies a selected entry to the clipboard.

- **Copy List to Clipboard** – Copies the list to the clipboard.
- **Copy selected to Clipboard** – Copies a selected row to the clipboard.
- **Export to File** – Exports a selected entry to a (*.txt) file.
- **Print List** – Prints the Firewall History list.
- **Group by User** – For better lucidity, access cache entries can be grouped by users. Grouped entries are arranged in pop-up menus topped by a labelled title bar.
- **Columns** – This option allows you to display all entries by selected columns. To add or remove a column, check or uncheck it in the sub-menu.
 - **Default Columns** – Offers the standard view.
 - **Optimize All Columns** – Adjusts the column size for best display.
 - **Adjust All Columns** – Displays all columns that are selected.

Configure Cache Settings

To specify the cache settings for the Barracuda NG Firewall, complete the following steps:

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > General Firewall Configuration**.
2. In the left menu, select **History Cache**.
3. Expand the **Configuration Mode** menu and select **Switch to Advanced View**.
4. Click **Lock**.
5. In the left navigation, select **History Cache**.
6. Configure the cache settings according to your requirements.
7. Click **Send Changes** and **Activate**.

To activate changes made in this part of the configuration, you must perform a firmware restart.

Figures

1. history.png

© Barracuda Networks Inc., 2019 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.