

---

## History Page

<https://campus.barracuda.com/doc/46209334/>

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 NextGen Admin, watch the following video:



Connection Blocked  
Troubleshooting  
Barracuda *NG Firewall*

### Information Display

---

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

DASHBOARD										CONFIGURATION		CONTROL		FIREWALL		NAC		VPN		MAILGW		LOGS		STATISTICS		EVENTS		SSH											
Monitor		Live		History		Threat Scan		ATD		Audit Log		Trace		Shaping		Entries: 3886		Max Entries: All																					
Cache Selection										Access, Fail, Rule Block, Packet Drop										Traffic Selection										Forward, Local In, Local Out, IPv4, IPv6									
A.	IP Proto	Port	Source	Interface	User	Destinat...	Out...	Ne...	Application	Ap...	Count	Last	Rule	Info																									
⊖	UDP	67	0.0.0.0	eth0		255.255...					13522	0s	BLOCKALL	Block by Rule																									
⊖	UDP	67	0.0.0.0	eth0		255.255...					13521	1s	BLOCKALL	Block by Rule																									
⊖	UDP	801	10.0.1...	eth0	administrator	192.168...					43631	1s	BLOCKALL	Block by Rule																									
✓	TCP	5049	10.0.1...	eth0		10.0.10.1...					175003	4s	BOX-AUTH-MSAD-SYNC	Normal Operation																									
⊖	UDP	68	10.0.1...	eth0	administrator	255.255...					16223	5s	LAN-2-INTERNET	Block Broadcast																									
⊖	UDP	123	10.0.1...	eth0		10.0.10.1...					13420	11s	BO-2-HQ-ALL	Block Broadcast																									
⊖	UDP	801	10.0.1...	eth0		10.0.13.1...					26537	11s	drop	Source is Local Address																									

The following information is provided for each session:

Info	Description
<b>AID</b>	Access ID, including an icon for blocked connections (red), an icon for established connections (green), and consecutive numbering for both blocked and established connections.
<b>IP Proto</b>	The protocol that is used. For example, TCP, UDP, or ICMP.
<b>Port</b>	The destination port (or internal ICMP ID).
<b>Source</b>	The source IP address.
<b>Interface</b>	The affected interface.
<b>User</b>	The username of the affected user and group.
<b>Destination</b>	The destination IP address.
<b>Output-IF</b>	The outgoing interface.
<b>Next Hop</b>	Next Hop
<b>Application</b>	The name of the affected application.
<b>Application Context</b>	The context of the affected application.
<b>Count</b>	Number of tries. The counter applies when a connection attempt hits a specific rule with <b>Firewall History Entry</b> enabled in the <b>Advanced</b> rule configuration. Removal of old entries is handled according to a fixed buffer size that can be adjusted in <b>Infrastructure Services &gt; General Firewall Configuration &gt; History Cache</b> .
<b>Last</b>	Time passed since last try.
<b>Rule</b>	The name of the affected firewall rule.
<b>Info</b>	Reason why things happen.

<b>Org</b>	Origin: <ul style="list-style-type: none"> <li>• <b>LIN</b>: Local In; incoming traffic on the box firewall.</li> <li>• <b>LOUT</b>: Local Out; outgoing traffic from the box firewall.</li> <li>• <b>LB</b>: Loopback; traffic via the loopback interface.</li> <li>• <b>FWD</b>: Forwarding; outbound traffic via the forwarding firewall.</li> <li>• <b>IFWD</b>: Inbound Forwarding; inbound traffic to the firewall.</li> <li>• <b>PXY</b>: Proxy; outbound traffic via the proxy.</li> <li>• <b>IPXY</b>: Inbound Proxy; inbound traffic via the proxy.</li> <li>• <b>TAP</b>: Transparent Application Proxying; traffic via virtual interface.</li> <li>• <b>LRD</b>: Local Redirect; redirect traffic configured in forwarding ruleset.</li> </ul>
<b>MAC</b>	MAC address of the interface.
<b>Src NAT</b>	The source NAT address.
<b>Dst NAT</b>	The destination NAT address.
<b>Out Route</b>	Unicast or local.
<b>Protocol</b>	The affected protocol.
<b>Src. Geo</b>	The geographic source of the active connection.
<b>Dst. Geo</b>	The geographic destination of the active connection.
<b>URL Category</b>	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.
- **Source** – When checked, this field allows filtering for the traffic source IP address.

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

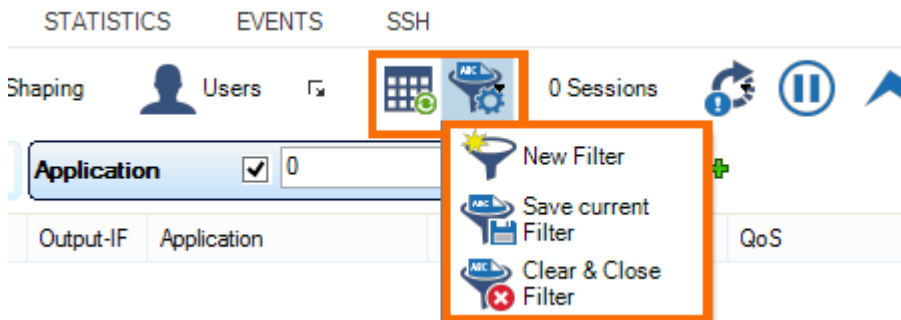
Note that some fields allow the use of wildcards (\*?; !\*?). Example: !Amazon\* excludes all entries starting with Amazon; Y\*|A\* includes all entries starting with "Y" or "A".

- **IP Protocol** - Displays the IP protocol.
- **Port** - Displays the port.
- **Source** - The source IP address/range.
- **Source/Destination** - IP address/range that matches either source or destination.
- **Interface** - Displays the interface (for example eth0).
- **User** - Displays the user.
- **Destination** - The destination IP address/range.
- **Output-IF** - The output interface.
- **Application** - Name of the affected application.
- **App Context** - Context of the affected application.
- **Rule** - Displays the rule that affects the traffic.
- **Any Interface** - Shows the forward or reverse interface.
- **Idle Time [s]** - The time sessions are in idle state. If specified, the idle time and less (<) in seconds is implied. Entering < and > is possible.
- **Protocol** - Shows the protocol.
- **File Content** - Shows the file type.
- **User Agent** - User agent for HTTP and HTTPS connections.
- **URL Category** - Shows the URL category.
- **Source Geo** - The source host's geographic location.
- **Destination Geo** - 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 drop-down 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 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

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 menu, 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. fw\_hist\_01.png
2. fw\_tab\_filter.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.