

## History Page

<https://campus.barracuda.com/doc/96026507/>

The **History** page is the most powerful tool for troubleshooting. To open the page, click the **FIREWALL** tab and select **History**.


DASHBOARD CONFIGURATION CONTROL <b>FIREWALL</b> VPN LOGS STATISTICS EVENTS SSH												
Monitor Live History Threat Scan Shaping Users Dynamic Host Rules Forwarding Rules Sync Filter Entries: 2779 Max Entries: All Refresh (F5) Disconnect												
History Selection		Access, Fail, Rule Block, Packet Drop		Traffic Selection		Forward, Local In, Local Out, IPv4, IPv6						
A...	IP Proto	Port	Source	Interface	User	Destination	Output-IF	Next Hop	Application	Application Context	Count	Last
⊘	UDP	137	10...	eth0		10...					82	19d 17...
⊘	TCP	33172	10...	eth0		10...					18	19d 18...
⊘	UDP	67	0.0...	eth0		255...					18	19d 18...
⊘	UDP	138	10...	eth0		10...					342	19d 18...
⊘	TCP	15070	18...	eth2		1.1...					9	19d 18...
✓	TCP	443	16...	eth4		3.6...	eth2	1.1.1.254			329	19d 18...
✓	TCP	443	16...	eth4		3.6...	eth2	1.1.1.254	Barracuda Networks Onli...		329	19d 18...
✓	TCP	443	16...	eth4		3.1...	eth2	1.1.1.254			67	19d 18...
✓	TCP	443	16...	eth4		3.1...	eth2	1.1.1.254	Barracuda Networks Onli...		67	19d 18...
⊘	UDP	67	0.0...	eth0		255...					16	19d 19...
⊘	UDP	137	10...	eth0		10...					187	19d 19...
⊘	UDP	137	10...	eth0		10...					221	19d 19...
⊘	UDP	67	0.0...	eth0		255...					46	19d 19...
⊘	TCP	11611	10...	eth0		10...					17	19d 19...
✓	TCP	80	1.1...	eth2		205...		1.1.1.254			977	19d 19...
✓	UDP	53	1.1...	eth2		40...		1.1.1.254			235	19d 19...
✓	TCP	443	16...	eth4		3.1...	eth2	1.1.1.254			77	19d 19...
✓	TCP	443	16...	eth4		3.1...	eth2	1.1.1.254	Barracuda Networks Onli...		77	19d 19...
✓	TCP	443	16...	eth4		205...	eth2	1.1.1.254			257	19d 19...
✓	TCP	443	1.1...	eth2		205...		1.1.1.254			808	19d 19...
✓	TCP	443	16...	eth4		205...	eth2	1.1.1.254	Barracuda Networks Onli...		176	19d 19...
⊘	UDP	137	10...	eth0		10...					87084	19d 21...
⊘	TCP	59753	10...	eth0		10...					26	19d 21...
⊘	UDP	137	10...	eth0		10...					8784	19d 21...
✓	UDP	53	16...	eth4		40...	eth4				134	19d 21...
✓	UDP	53	16...	eth4		13...	eth4				122	19d 21...
✓	UDP	53	16...	eth4		13...	eth4				116	19d 21...
✓	UDP	53	16...	eth4		64...	eth4				116	19d 21...
⊘	UDP	67	0.0...	eth0		255...					393	19d 21...
⊘	UDP	67	0.0...	eth0		255...					383	19d 21...


The **History** page displays all sessions when the slot ends. TCP sessions usually end with the FIN-FINACK-ACK sequence. This is displayed as **Normal operation** in the **Info** column. Resets are terminated with Session idle timeout or Last ACK timeout. For the stateless UDP and ICMP protocols, "pseudo" sessions are created that usually end with a timeout.

The following information is provided for each session:

- **AID** – Access ID, including an icon for established connections (green), blocked connections (red), and impaired connections (yellow), and consecutive numbering for all connections.
- **IP Proto** – The protocol used. For example, TCP, UDP, or ICMP.
- **Port** – The destination port (or internal ICMP ID).
- **Source** – The source IP address.
- **User** – The username of the affected user and group.
- **Destination** – The destination IP address.
- **Destination Info** – Destination Info is a compound string of multiple partial names/symbols and relates to the template:
- **Output-IF** – The outgoing interface.
- **Next Hop** – The next hop.
- **Application** – The name of the affected application, e.g., Web browsing, Ubuntu Update.
- **Application Context** – The context of the affected application., e.g., www.barracuda.com
- **Count** – The number of tries. The counter applies when a connection attempt hits a specific rule

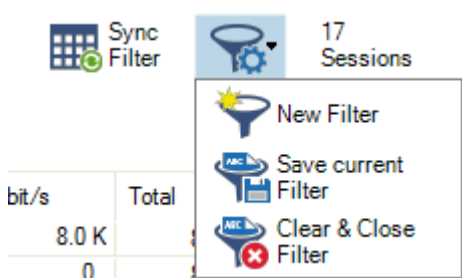
with **Firewall History Entry** enabled in the **Advanced** rule configuration. Removal of old entries is handled according to a fixed buffer size that can be adjusted in the **Infrastructure Services > General Firewall Configuration > History Cache** page.

- **Last** – Time passed since the last try.
- **Rule** – The name of the affected firewall rule.
- **Info** – Additional information.
- **Org** – Origin. The value can be one of the following:
  - **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 the virtual interface.
  - **LRD** – Local Redirect; redirect traffic configured in forwarding ruleset.
- **MAC** – The 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.
- **Src./Dst. Geo** – The geographic source/destination of the active connection.
- **URL Category** – Category of the destination URL.
- **Src. Named Network** – The compound string of a named network used for a source.  
Example: example.com///Location-51/Department-18/Devices-3
- **Dst. Named Network** – The compound string of a named network used for a destination.  
Example: example.com///Location-51/Department-18/Devices-3
- **Src. VR Instance** – The source IP address of a virtual router instance.
- **Dst. VR Instance** – The destination IP address of a virtual router instance.
- **Source Info** – Source Info is a compound string of multiple partial names/symbols and relates to the template:
  - **Source Geo**: An icon that is either
    - a flag symbol that relates to the state at the given geo-location
    - a symbol of a house that stands for a private IP address
  - EITHER:
    - **Source IP**: the source IP address that is associated with the geographical information (Geo-IP).  
Example:  5.5.5.242
  - OR:
    - **Named Network**: If the IP address is defined by a named network, then the name of the **Named Network** is used.
- **Destination Info** – Destination Info is a compound string of multiple partial names/symbols and relates to the template:
  - **Destination Geo**: An icon that is either
    - a flag symbol that relates to the state at the given geo-location

- a symbol of a house that stands for a private IP address
- EITHER:
  - **Destination IP:** the destination IP address that is associated with the geographical information (Geo-IP).  
Example:  5.5.5.242
- OR:
  - **Named Network:** If the IP address is defined by a named network, then the name of the **Named Network** is used.
- **Interface** – The name of the interface is a compound of multiple partial names and relates to the template:
  - **Output interface** (see also **Output-IF** in this list)
  - "@"
  - (Optional): Name of the tunnel
  - Name of the box
  - " "
  - (Optional): Name of the cluster
  - " "
  - (Optional): Name of the range
  - Example: pvpn0@PGRP-MYBOX\_Cluster2\_1

## Filter Options

You can filter the list of sessions by traffic type, status, and properties. Click the **Filter** icon on the top right of the ribbon bar to access the filtering options.



1. Click the **Filter** icon.
2. Select **New Filter**. The **Traffic Selection** section opens on the top left of the list.
3. Expand the **Traffic Selection** drop-down menu and select the required checkboxes:
  - **Forward** – Sessions that are handled by the Forwarding Firewall.
  - **Loopback** – System-internal data exchanged by the loopback interface.
  - **Local In** – Incoming sessions that are handled by the box firewall.
  - **Local Out** – Outgoing sessions that are handled by the box firewall.
  - **IPv4** – IPv4 traffic.
  - **IPv6** – IPv6 traffic.
4. From the **Status Selection** list, you can select the following options to filter for certain traffic

statuses:

- **Closing** – Closing connections.
- **Established** – Established connections.
- **Failing** – Failed connections.
- **Pending** – Connections that are currently being established.

5. You can set additional filters based on the content of the menu list when you click the '+' symbol in the blue ribbon bar. Although these filters are displayed together in a common menu list for selection, they belong to two groups of filters:

1. "Single filter" – A single filter relates directly to a single column name in the table view of the window, e.g., **IP Protocol**, **Port**, **Source**, **Destination**.
2. "Compound filter" – A compound filter relates to two columns of the table, e.g., **Source/Destination**, **Any Interface**, **VR Instance (Src/Dst)**, that have a certain category in common, e.g., an **IP address**, a **Named Network Object**. You can regard such a filter as consisting of two separate filters (e.g., **Source** and **Destination**) that are linked to each other with a logical 'OR' operator and substituted by the filter

**Source/Destination.**

Traffic Selection		Forward, Local In, Local Out, IPv4, IPv6		Status Selection		Closing, Established, Failing, Pending		Source/Destin...			
ID	State	IP Protocol	Port	Source	Interface	User	Destination	Output-IF	Application	Application Context	QoS
.....	↔	TCP	807	10.27.251.2	eth0		10.17.84.65	eth0			Interactive /
.....	↔	TCP	807	10.27.251.2	eth0		10.17.84.65	eth0			Interactive /
I.....	↔	ICMP		10.17.84.65	eth0		10.17.84.1	eth0			Interactive /
II.....	↔	TCP	807	10.27.251.2	eth0		10.17.84.65	eth0			Interactive /
III.....	↔	TCP	807	10.27.251.2	eth0		10.17.84.65	eth0			Interactive /
.....	↔	TCP	807	10.27.251.2	eth0		10.17.84.65	eth0			Interactive /

These additional filters can be used both on visible and blanked-out columns. As an example, you can activate a certain filter, e.g., **Source/Destination**, and the table view will display all matching records even if the column **Destination** is not visible.

Traffic Selection		Forward, Local In, Local Out, IPv4, IPv6		Status Selection		Closing, Established, Failing, Pending		Source/Destin...			
ID	State	IP Protocol	Port	Source	Interface	User	Output-IF	Application	Application Context	QoS	Rule
.....	↔	TCP	807	10.27.251.2	eth0		eth0			Interactive /	MGMT-ACCESS
.....	↔	TCP	807	10.27.251.2	eth0		eth0			Interactive /	MGMT-ACCESS
I.....	↔	ICMP		10.17.84.65	eth0		eth0			Interactive /	BOX-GW-TEST
II.....	↔	TCP	807	10.27.251.2	eth0		eth0			Interactive /	MGMT-ACCESS
III.....	↔	TCP	807	10.27.251.2	eth0		eth0			Interactive /	MGMT-ACCESS
.....	↔	TCP	807	10.27.251.2	eth0		eth0			Interactive /	MGMT-ACCESS

Currently, there are the following compound filters you can select: **Source/Destination**, **Any Interface**, **VR Instance (Src/Dst)**.

When you click the '+' icon in the blue ribbon bar, the menu list is created at runtime. The menu list first displays the filters that relate to the visible columns in the table view, followed by all remaining filters whose related columns are not visible. The following menu list is an example of the contained filters:

IP Protocol
Port
Source
Source/Destination
Interface
User
Destination
Output_IF
Application
App Context
Rule
Src. Named Networks
Any Interface
Dst. Named Networks
Src. VR Instance
Dst. VR Instance
VR Instance (Src/Dst)
Protocol
Content
URL Category
Source Geo
Destination Geo
Idle Time [s]

6. Select the requested filter category from the list.
7. Enter the exact value into the edit field of the filter criterion you want the data to match against, e.g., filter Source, filter value 10.17.84.65:





Traffic Selection		Forward, Local In, Local Out, IPv4, IPv6		Status Selection		Established, Failing, Pending		Source					
ID	State	IP Protocol	Port	Source	Interface	User	Destination	Output-IF	Application	Application Context	QoS	Rule	bit/s
1...	↔	ICMP		10.17.84.65	eth0		10.17.84.1	eth0			Interactive /	BOX-GW-TEST	0

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". Clicking the **Sync Filter** icon on the top right of the ribbon bar above the filters allows you to switch to the **Live** view but with the same filters applied.

## Managing Sessions

You can view additional information for a specific session by double-clicking an entry.

## Session Details

ID:	..... 138
State:	
IP Protocol:	TCP
Port:	807
Source:	10.0.10.11
Interface:	eth0
User:	
Destination:	10.0.10.33
Output-IF:	eth0
Application:	
Application Context:	
QoS:	
Rule:	 MGMT-ACCESS
bit/s:	0
Total:	46.0 K
Idle:	25s
TI ID:	-
Type:	LIN
Src.Port:	58671
In:	25.8 K
Out:	20.1 K
Start:	1h 49m 33s
SNAT:	
DNAT:	
Status:	LOC-EST
Policy:	NOSYNC
FWD Shape:	- / Out: -
REV Shape:	- / Out: -
Protocol:	NGF-MGMT
File Content:	
Src. Geo:	 Non-routable or Private IP Addresses
Dst. Geo:	 Non-routable or Private IP Addresses
URL Category:	
User Agent:	
Src. Prefix:	
Dst. Prefix:	

Right-click into the listing to make 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.
- **Clear History** – 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 are only resolved to hostnames if enabled in **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > General Firewall Configuration > Firewall History**.
- **Apply Rule Tester** – Offers the option for firewall rule testing.
- **Find** – Opens a search window at the top of the list.

For more settings, see: [Barracuda Firewall Admin](#).

---

The size of the caches is configured in the General Firewall settings and requires a firmware restart. For more information, see [General Firewall Configuration](#).

## Video

---

For a hands-on demo, please see the following training video: [Firewall Policies](#)

## Figures

1. firewall\_history.png
2. example\_source\_info\_field.png
3. example\_source\_info\_field.png
4. filter\_options.png
5. firewall\_live\_filter\_compound\_filter\_active.png
6. firewall\_live\_compound\_filter\_active\_with\_only\_source\_column.png
7. firewall\_live\_filter\_list\_menu.png
8. firewall\_live\_filter\_individual\_filter\_configured.png
9. sessions.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.