

History Page

<https://campus.barracuda.com/doc/79463237/>

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

DASHBOARD CONFIGURATION CONTROL FIREWALL 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	Rule
⚠	UDP	137	10...	eth0		10...					82	19d 17...	BLOCKALL
⚠	TCP	33172	10...	eth0		10...					18	19d 18...	drop
⚠	UDP	67	0.0...	eth0		255...					18	19d 18...	BLOCKALL
⚠	UDP	138	10...	eth0		10...					342	19d 18...	BLOCKALL
⚠	TCP	15070	18...	eth2		1.1...					9	19d 18...	drop
✓	TCP	443	165...	eth4		3.6...	eth2	1.1.1.254			329	19d 18...	BOX-LAN-2-INTERNET
✓	TCP	443	165...	eth4		3.6...	eth2		Barracuda Networks Onli...		329	19d 18...	APPOL-AppDefault
✓	TCP	443	165...	eth4		3.1...	eth2	1.1.1.254			67	19d 18...	BOX-LAN-2-INTERNET
✓	TCP	443	165...	eth4		3.1...	eth2		Barracuda Networks Onli...		67	19d 18...	APPOL-AppDefault
⚠	UDP	67	0.0...	eth0		255...					16	19d 19...	BLOCKALL
⚠	UDP	137	10...	eth0		10...					187	19d 19...	BLOCKALL
⚠	UDP	137	10...	eth0		10...					221	19d 19...	BLOCKALL
⚠	UDP	67	0.0...	eth0		255...					46	19d 19...	BLOCKALL
⚠	TCP	11611	10...	eth0		10...					17	19d 19...	drop
⚠	TCP	80	1.1...	eth2		205...		1.1.1.254			977	19d 19...	OP-SRV-PX
✓	UDP	53	1.1...	eth2		40...		1.1.1.254			235	19d 19...	BOX-DNSREC-OUT
✓	TCP	443	165...	eth4		3.1...	eth2	1.1.1.254			77	19d 19...	BOX-LAN-2-INTERNET
✓	TCP	443	165...	eth4		3.1...	eth2		Barracuda Networks Onli...		77	19d 19...	APPOL-AppDefault
✓	TCP	443	165...	eth4		205...	eth2	1.1.1.254			257	19d 19...	BOX-LAN-2-INTERNET
✓	TCP	443	1.1...	eth2		205...		1.1.1.254			808	19d 19...	OP-SRV-VPN
✓	TCP	443	165...	eth4		205...	eth2		Barracuda Networks Onli...		176	19d 19...	APPOL-AppDefault
⚠	UDP	137	10...	eth0		10...					87084	19d 21...	BLOCKALL
⚠	TCP	59753	10...	eth0		10...					26	19d 21...	drop
⚠	UDP	137	10...	eth0		10...					8784	19d 21...	BLOCKALL
✓	UDP	53	165...	eth4		40...	eth4				134	19d 21...	BOX-LOCALDNSCACHE
✓	UDP	53	165...	eth4		13...	eth4				122	19d 21...	BOX-LOCALDNSCACHE
✓	UDP	53	165...	eth4		13...	eth4				116	19d 21...	BOX-LOCALDNSCACHE
✓	UDP	53	165...	eth4		64...	eth4				116	19d 21...	BOX-LOCALDNSCACHE
⚠	UDP	67	0.0...	eth0		255...					393	19d 21...	BLOCKALL
⚠	UDP	67	0.0...	eth0		255...					383	19d 21...	BLOCKALL

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.

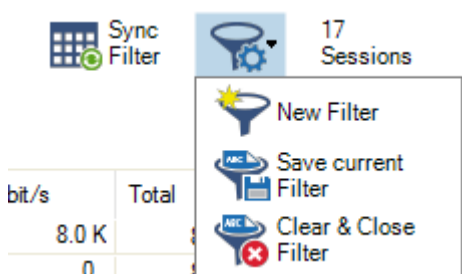
The following information is provided for each session:

- **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.
- **Src. Prefix** – The source prefix.
- **Dst. Prefix** – The destination prefix.
- **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** – The next hop.
- **Application** – The name of the affected application.

- **Application Context** – The context of the affected application.
- **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 last try.
- **Rule** – The name of the affected firewall rule.
- **Info** – Additional information.
- **Org** – Origin:
 - **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** – 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.

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 check boxes:
 - **Forward** – Sessions handled by the Forwarding Firewall.

- **Loopback** – System-internal data exchanged by the loopback interface.
 - **Local In** – Incoming sessions handled by the box firewall.
 - **Local Out** – Outgoing sessions 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 currently being established.
5. To define more filters for specific properties:
1. Click the **+** icon.
 2. Select the required criteria.
 3. Select or enter the value in the blank field.





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](#) 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. filter_options.png
3. 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.