Barracuda CloudGen Firewall

History Page

https://campus.barracuda.com/doc/53248395/
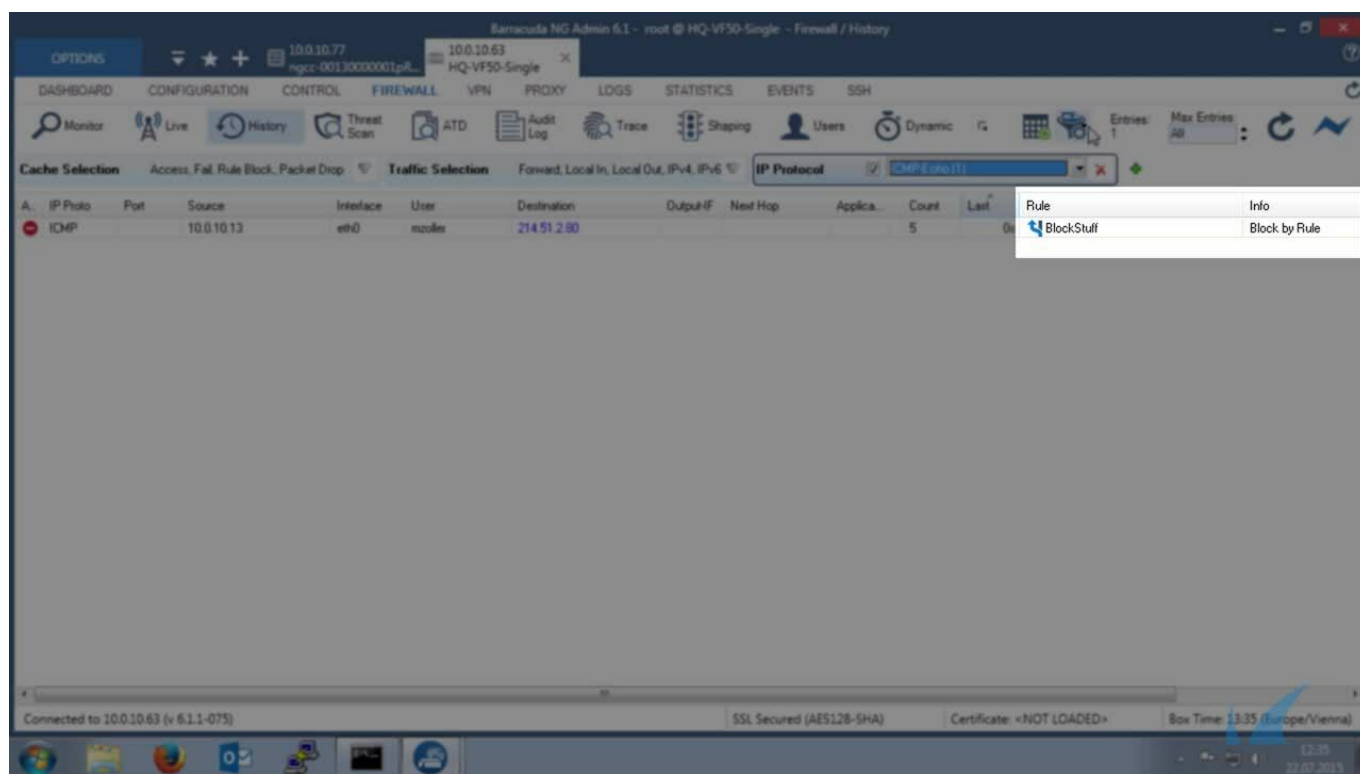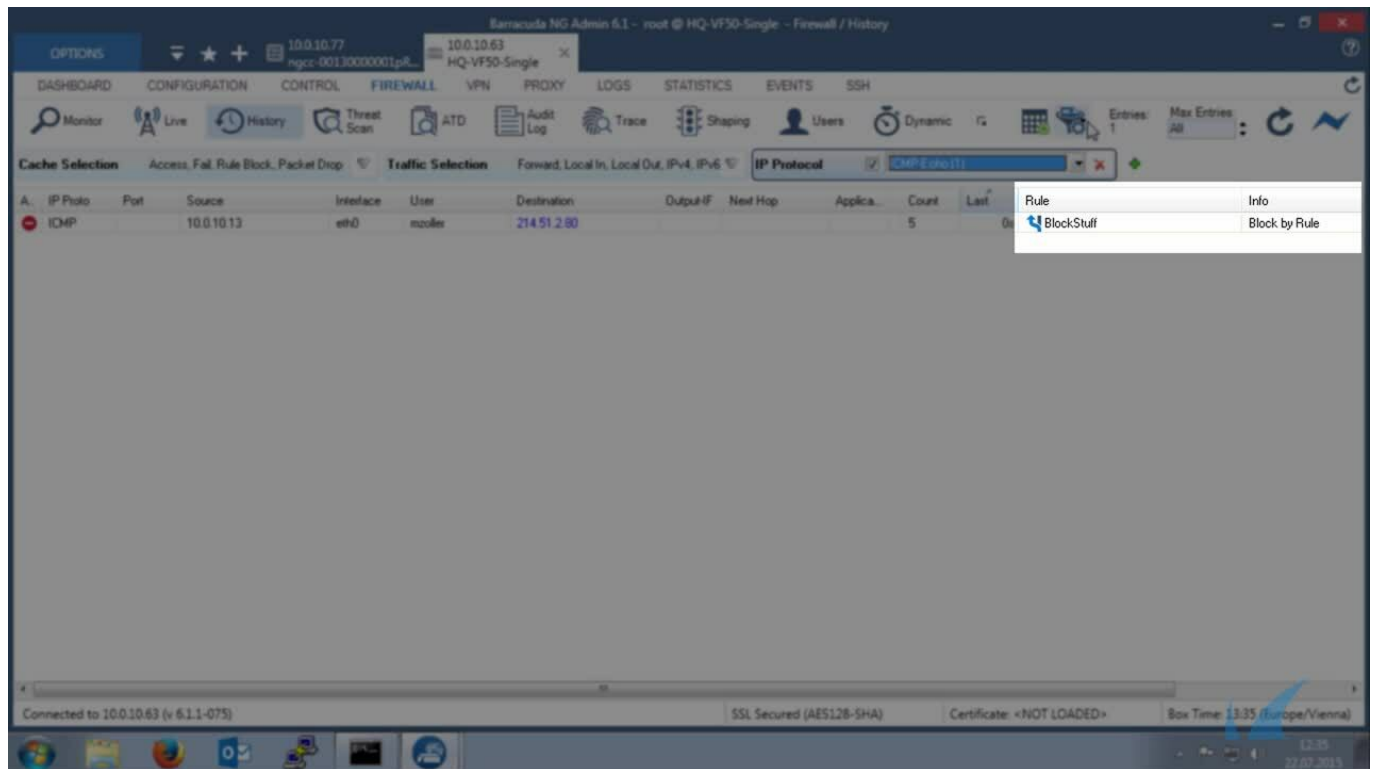
The **History** page is the most powerful tool for troubleshooting. To open the page, click
the **FIREWALL** tab and select **History**.

Video

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

Barracuda CloudGen Firewall

Videolink:

https://campus.barracuda.com/

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** , **Last ACK timeout** . For the stateless UDP and ICMP protocols, "pseudo" sessions are created that usually end with a timeout.
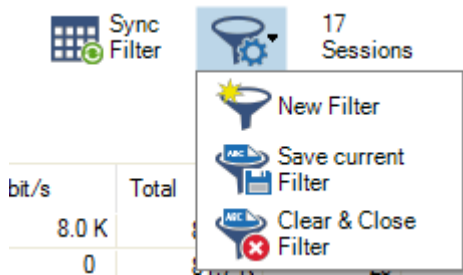

The following information is provided for each session:

- **AID** – Access ID, including an icon for blocked connections (red), an icon for established connections (green), and consecutive numbering for both blocked and established 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.
- **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 are only 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.

For more settings, see: Barracuda NextGen 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.

Figures

3. fw_hist_01.png
4. filter_options.png
5. sessions.png