Audit Log Page

https://campus.barracuda.com/doc/41116058/

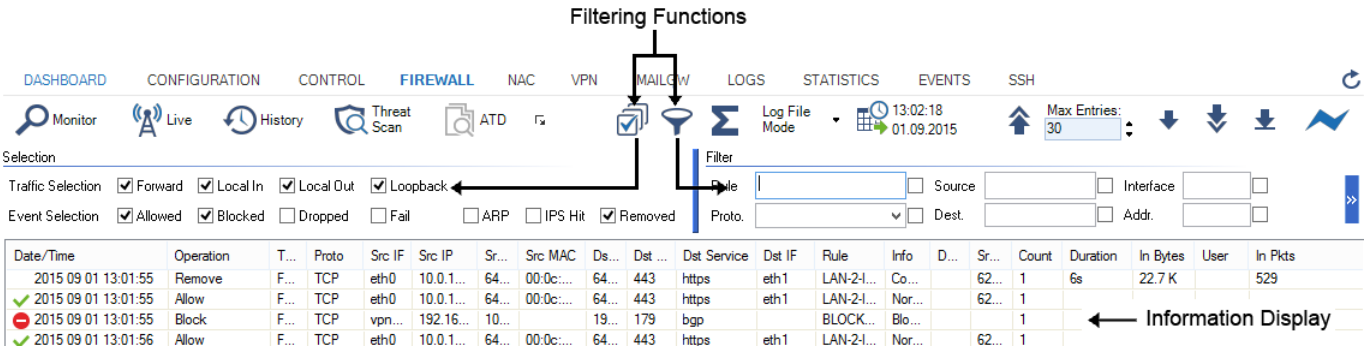
Firewall Audit data is stored locally by default, but can also be forwarded to the Barracuda NG Control Center. The collected information is visible on the **Audit Log** page. To access the **Audit Log** screen, click the **FIREWALL** tab, expand the upper ribbon bar, and click the **Audit Log** icon.

To use the Audit Log feature, enable the firewall audit log. For more information, see FW Audit.

In this article:

Information Display

The **Audit Log** page lists firewall audit data information and provides several filtering options. To display log files and filtering results for selected criteria such as the specified time and date, click the down arrow icon in the upper right of the ribbon bar ( ).



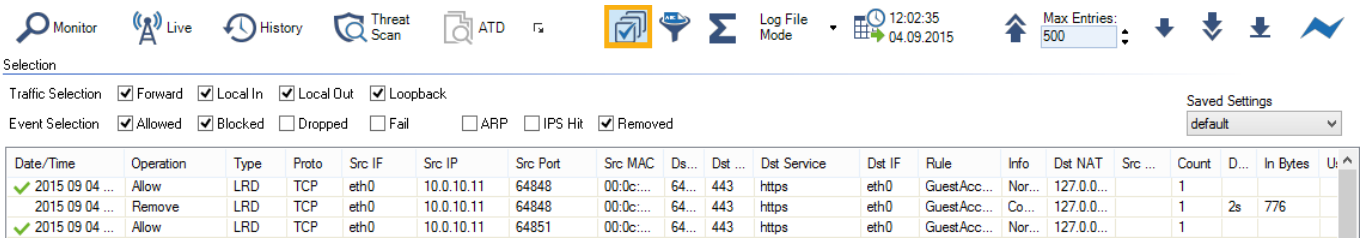
When configured, the columns on the **Audit Log** page display the following information:

- **Date/Time** – Date and time when the operation was performed.
- **Operation** – Displays the operation.
- **Type** – The operation type.
- **Proto** – The protocol used.
- **Src IF** – The source interface.
- **Src IP** – The source IP address.
- **Src Port** – The source port.
- **Src MAC** – The source MAC address if applicable.

- **Dst IP** – The destination IP address.
- **Dst Port** – The destination port.
- **Dst Service** – The destination service.
- **Dst IF** – The destination interface.
- **Rule** – The access or application rule that applies.
- **Info** – Displays additional information, if available.
- **DstNAT** – The Destination NAT address.
- **SrcNAT** – The Source NAT address.
- **Count** – Displays how often the operation was carried out.
- **Duration** – Duration time of the operation.
- **In Bytes** – Amount of incoming traffic in Bytes.
- **In Pkts** – Amount of incoming traffic in Pkts.
- **Out Bytes** – Amount of outgoing traffic in Bytes.
- **Out Pkts** – Amount of outgoing traffic in Pkts.
- **Total Bytes** – Total traffic in Bytes.
- **User** – The user affected by the operation.

Filter Options

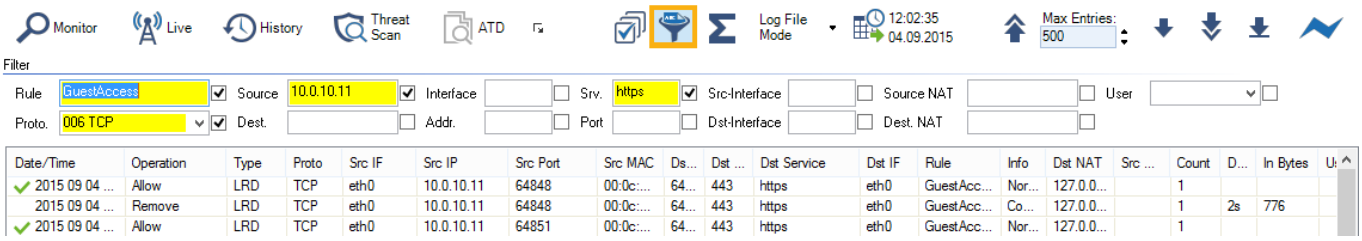
Clicking the first filter icon (**Filter (selection mask)**) in the ribbon bar opens the **Selection** menu, which provides the following options:



- **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.
  - **Local In** – Displays the incoming traffic on the Host Firewall.
  - **Local Out** – Displays the outgoing traffic from the Host Firewall.
  - **Loopback** – Traffic over the loopback interface.
- **Event Selection** – From the **Event Selection** list, you can select the following options to filter for certain traffic types:
  - **Allowed** – Displays all allowed events.
  - **Blocked** – Displays all blocked events.
  - **Dropped** – Displays all dropped events.
  - **Fail** – Displays all failed events.
  - **ARP** – Displays all ARP requests.
  - **IPS Hit** – Displays all events detected by the IPS.

- **Removed** – Displays all removed events.

Clicking the second filter icon (**Filter**) opens the **Filter** menu, which provides the following options:



- **Rule** – Allows setting a filter for a specific rule.
- **Proto** – Allows setting a filter for a specific protocol.
- **Source/Dest.** – 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).
- **Addr.** – Allows setting a filter for a specific destination IP address/range.
- **Srv.** – Allows setting a filter for a specific service.
- **Port** – Allows setting a filter for a specific port.
- **Src Interface** – Allows setting a filter for the source interface.
- **Dst Interface** – Allows setting a filter for the destination interface.
- **Source NAT** – Allows setting a filter for the source NAT address.
- **Dest. NAT** – Allows setting a filter for the destination NAT address.
- **User** – Allows setting a filter for the user affected by the operation.

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".

On the top right of the ribbon bar of the **Audit Log** page, you can specify a time and date to view logs that were created within a set time interval.

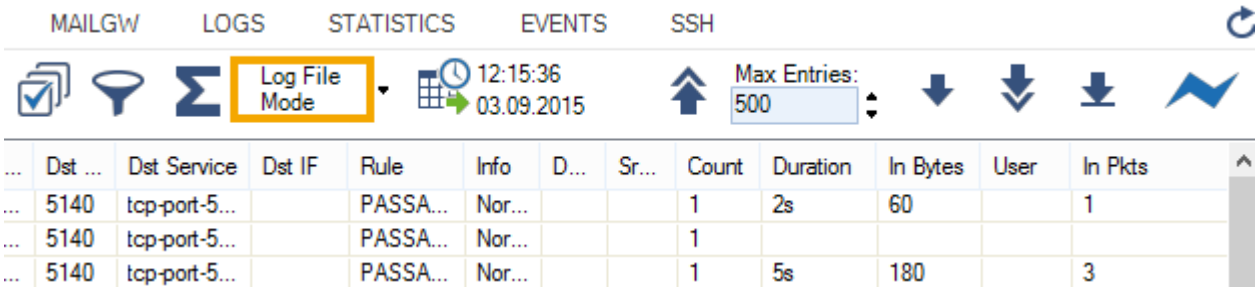
Log File Display Modes

The **Audit Log** page lists firewall audit data information according to the specified filter selection and time interval. Per default, all entries are shown line by line in the list (**Log File Mode**). The **Log File Mode** drop-down provides two display options.

- **Log File Mode** – Log files are shown line by line according to the specified filter selection and time interval.
- **Accumulation Mode** – Log files are shown accumulated by specified merging criteria. This provides a more general overview on similar event categories.

Log File Mode

Per default, all entries are shown line by line in the list (**Log File Mode**). In the navigation bar on the top right of the ribbon bar, you can select how information is displayed in the list. Use the **Max Entries** field to adjust the number of entries displayed in the list. To view a log entry, double click it.



You can navigate through the log entries with the following navigation buttons:

– Browse backward from the current entry.

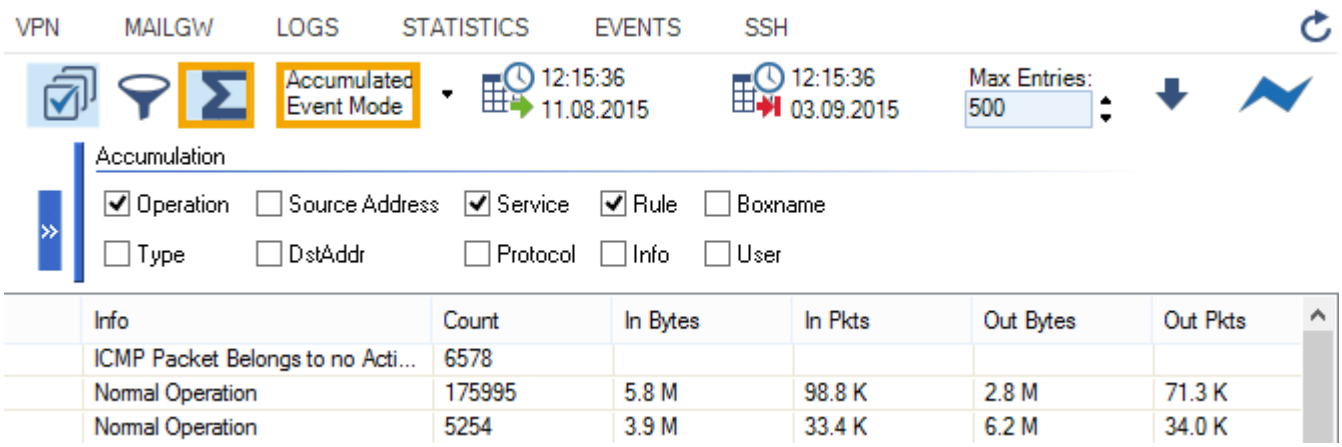
– Display log files / filtering results for selected criteria such as the specified time and date.

– Browse forward from the current entry.

– Browse to the end of the log.

Accumulation Mode

Select **Accumulated Event Mode** from the **Log File Mode** drop-down, to group events by the criteria selected in the **Accumulation** filter.



Clicking the icon next to the filter (**Accumulation**) opens the **Accumulation** filter providing the following options:

- **Operation** – Accumulate entries by operation.
- **Type** – Accumulate entries by operation type.
- **Source Address** – Accumulate entries by source IP address/range.
- **Destination Address** – Accumulate entries by destination IP address.
- **Service** – Accumulate entries by service.
- **Protocol** – Accumulate entries by the protocol used.
- **Rule** – Accumulate entries by access or application rule.
- **Info** – Accumulate entries by additional information.
- **Boxname** – Accumulate entries by box name
- **User** – Accumulate entries by affected user.

To display the log files and filtering results for the selected criteria, click the down arrow icon in the upper right of the ribbon bar ( ). Use the **Max Entries** field to adjust the number of entries displayed in the list.

Figures

1. I2.png
2. audit_01.png
3. selection.png
4. filter.png
5. mode_01.png
6. I1.png
7. I2.png
8. I3.png
9. I4.png
10. mode_02.png
11. I2.png