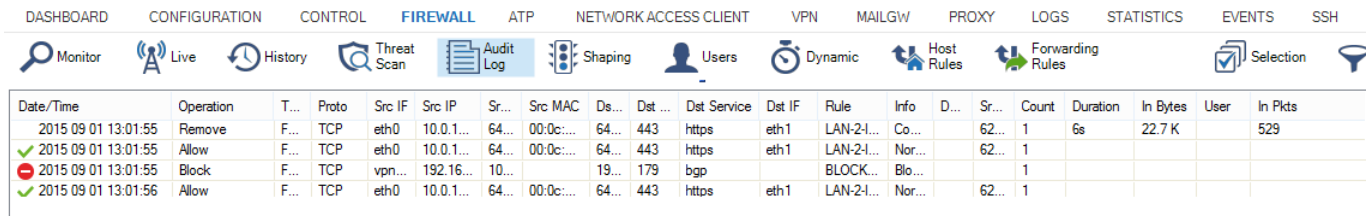
Audit Log Page

Firewall Audit data is stored locally by default, but can also be forwarded to the Control Center. To use the Audit Log feature, you must enable the firewall audit log. For more information, see FW Audit. The collected information is visible on the **Audit Log** page. To access the **Audit Log** page, click the **FIREWALL** tab and select the **Audit Log** icon.



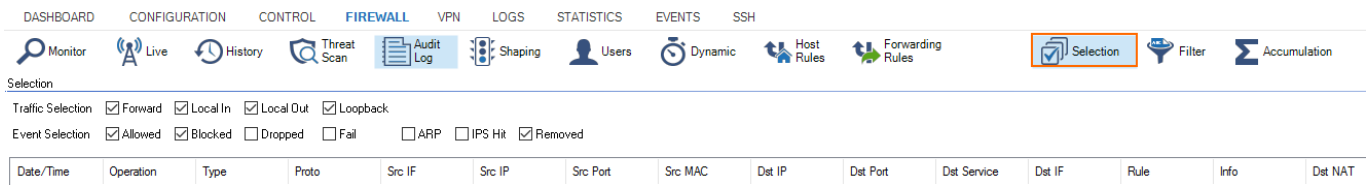
The columns on the **Audit Log** page display the following information:

- **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 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

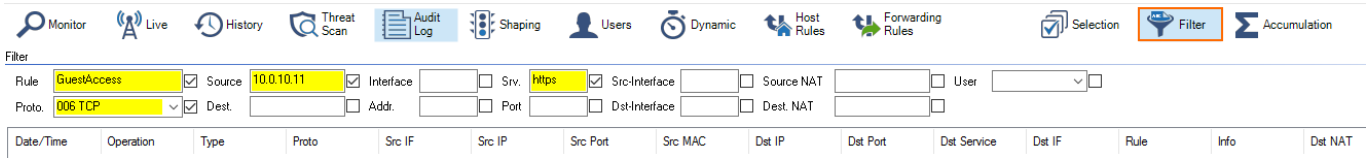
The **Audit Log** page provides several filtering options.

Click the **Selection** icon to open 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.

Click the **Filter** icon in the ribbon bar to open the **Filter** menu, which provides the following options:



- **Rule** – Allows a filter to be set for a specific rule.
- **Proto** – Allows a filter to be set for a specific protocol.
- **Source/Dest.** – Allows a filter to be set for a specific IP address/range that matches either source or destination.
- **Interface** – Allows a filter to be set for a specific interface (for example, eth0).
- **Addr.** – Allows a filter to be set for a specific destination IP address/range.
- **Srv.** – Allows a filter to be set for a specific service.
- **Port** – Allows a filter to be set for a specific port.
- **Src Interface** – Allows a filter to be set for the source interface.
- **Dst Interface** – Allows a filter to be set for the destination interface.
- **Source NAT** – Allows a filter to be set for the source NAT address.
- **Dest. NAT** – Allows a filter to be set for the destination NAT address.
- **User** – Allows a filter to be set for the user affected by the operation.

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".

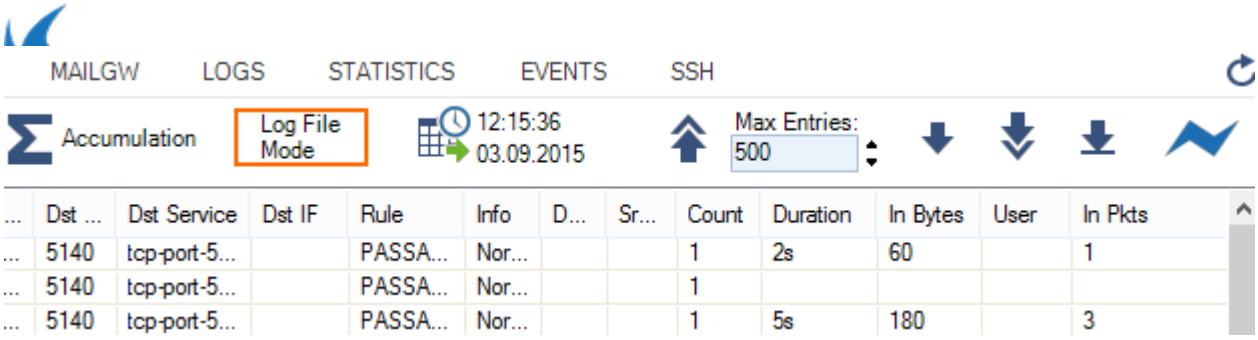
Log File Display Modes

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

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

Log File Mode

By 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.

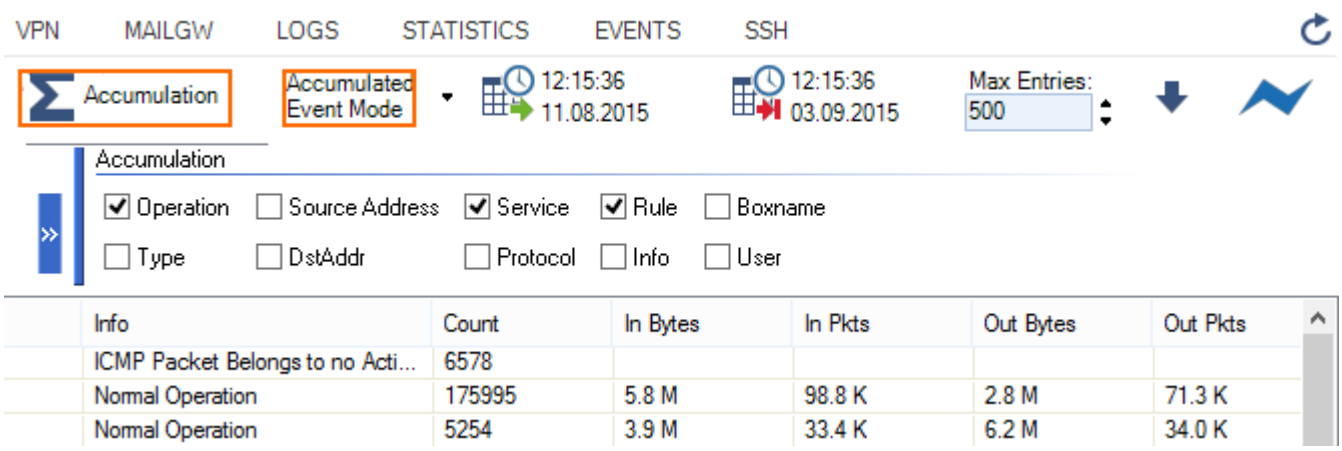
– Display log files / filtering results for selected criteria, such as the specified time and date.

– Browse forward from the current entry.

– Browse to the end of the log.

Accumulated Event Mode

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



Click the icon next to the filter (**Accumulation**) to open the **Accumulation** filter, which provides 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.

Next to the **Log File Mode** icon, you can specify a time and date to view logs that were created within a set time interval.

Figures