How to Configure Audit and Reporting

https://campus.barracuda.com/doc/41115974/

The firewall audit service allows propagating firewall events to the Barracuda NG Control Center for collection and analysis.

Configure Audit and Reporting

1. Go to **CONFIGURATION > Full Configuration > Box > Infrastructure Services > General Firewall Configuration**.
2. In the left menu, select **Audit and Reporting**.
3. Expand the **Configuration Mode** menu and select **Switch to Advanced View**.
4. Click **Lock**.
5. To enable the firewall dashboard, set **Generate Dashboard Information** to **yes**.
6. Configure the following settings:
   - **Statistics for Host Firewall** – Enable if you want to create statistics for the host firewall.
   - **Generate Protocol Statistics** – Enable to create protocol and P2P specific statistics. These statistic can be seen using the event viewer under `.../server/BOX/proto_stat/.`
   - **Generate Events** – Enable eventing settings configuration.
   - **Event Data** – Click **Edit** to enable or disable specific events.
   - **Forward Log Policy** – This parameter defines whether server specific FFW logs should be written to both box and server log (**Box-And-Server File**; default), only to the server logs (**Server-File-Only**) or only to the box logs (**Box-File-Only**).
   - **Log Level –** Cumulative logging allows some reduction of log file lengths and tries to avoid indirect denial of service (DoS) attacks.
   - **Cumulative Interval [s] –** Interval (in sec) for which cumulative logging is activated for either matching or similar log entries. To enter cumulative logging the entries need to be identical in all of the identifiers of a log entry except of the source port (min: 1; max: 60; default: 1).
   - **Cumulative Maximum** – Maximum number of log entries within the same rule and resulting in the same reason which triggers cumulative logging (default: *10*).
   - **Generate Audit Log** – Enables Firewall Audit.
   - **Audit Log Data**:
     - Click **Edit** to configure **Firewall Audit** settings.
   - **Enable IPFIX/Netflow** – Internet Protocol Flow Information Export (IPFIX, RFC 3917) is based on NetFlow version 9. You can use this to stream the Firewall Audit logs via IPFIX:
     - Click **Edit** to configure the **IPFIX/Netflow** settings.
     - Click **Edit** to configure the **Connection Tracing** settings.
7. Click **Send Changes** and **Activate**.

Activation

To activate changes made to the audit and reporting configuration, you must perform a firmware restart. To do so, go to the **Box** page (**CONTROL > Box**), expand the **Operating System** section and click **Firmware Restart**.

All active connections will be terminated when performing a firmware restart.

Audit Events

An audit event entry consists of a CR terminated line of ASCII characters. Each line holds 23 pipe ("|") separated values.

Example: *1129102500|Block:|FWD|eth0|ICMP|BLOCKALL|10.0.3.80|0|10.0.3.73|0||4002|Block by Rule|0.0.0.0|0|0.0.0.0|0||00:07:e9:09:04:30|0|0|0|0|0|4552264444*

Column	Value	Type
1	Time	Unix seconds
2	Log Operation	Log Operations (Unknown, Allow, LocalAllow, Block, LocalBlock, Remove, LocalRemove, Drop, Terminate, LocalTerminate, Change, Operation, Startup, Configuration, Rule, State, LocalState, Process, AdminAction, Deny, LocalDeny, SecurityEvent, Sync, Fail, or LocalFail)
3	Session Type	Session Type (Forwarding, Local In, Local Out, or Loopback)
4	Input Network Device	String
5	IP Protocol	String
6	Firewall Rule	String
7	Source IP Address	IP Address
8	Source Port Number	0–65535
9	Destination IP Address	IP Address
10	Destination Port Number	0-65535
11	Service Name	String
12	Reason Code	Number
13	Reason	String

14	Bind IP Address	IP Address
15	Bind Port Number	0-65535
16	Connection IP Address	IP Address
17	Connection Port Number	0–65535
18	Output Network Device	String
19	MAC Address	6 colon separated hex bytes
20	# of Input Packets	Number
21	# of Output Packets	Number
22	# of Input Bytes	Number
23	# of Output Bytes	Number
24	Duration	in seconds
25	ID	audit entry number