How to Enable the Firewall Audit Log Service

https://campus.barracuda.com/doc/73719608/

The Barracuda CloudGen Firewall generates Audit Log entries for both local and/or forwarding traffic. The Firewall Audit Info viewer is accessible by selecting the **Firewall** tab and clicking the **Audit Log** icon in the ribbon bar. The local Audit Info viewer is available on every Barracuda CloudGen Firewall generating a Firewall Audit logfile.

Enable Audit Logs

Activate the generation of Firewall Audit data:

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. In the **Log Policy** section enable **Generate Audit Log**.
6. Click **Set** next to **Audit Log Data**.
7. From the **Audit Delivery** list select how audit log data is stored or processed
   - **Local-DB** – Store audit data within a local sqlite3 DB.
   - **Forward-Only** – Forward natively to an audit collector service.
   - **Local-DB-And-Forward** – The combination of both.
   - **Send-IPFIX** – Hand off data to separate IPFIX exporter.
   - **Forward-and-Send-IPFIX** – Combination of forwarding and send data to an IPFIX exporter.
   - **Regular Log File** – Plain ASCII based log file.
   - **Syslog-Proxy** – Generate syslog messages.
   - **Executable** – Feed into custom executable on stdin.
   - **Send-UDP-Packet** – Send via plain UDP stream.
8. Select **Regular Logfile** from the **Audit Delivery** drop-down.
9. Click **OK**.
10. Click **Send Changes** and **Activate**.

Firewall Audit data is stored locally by default, but may be forwarded to the Barracuda Firewall Control Center or to a dedicated Barracuda CloudGen Firewall running the Firewall Audit Log service for central audit log file collection. For more information, see FW Audit.

© 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.