

FW Audit

<https://campus.barracuda.com/doc/96026398/>

FW audit is a strictly chronological log of all sessions and events on your Barracuda CloudGen Firewall. Information written to this log may contain the following:

- **Traffic** – Forward, Local In, Local Out, and Loopback traffic
- **Events** – Allowed, Blocked, Dropped, Failed, and Removed events
- **ARP**
- **IPS Hits**

This data can be stored and viewed locally and/or centrally on the Barracuda Firewall Control Center depending on the audit delivery method configured on your firewall:

- **Local-DB** – Store audit log data locally in a database.
- **Forward-Only** – Forward audit logs to an Audit Collector service on the Control Center.
- **Local-DB-And-Forward** (default) – Store data in a local database and simultaneously send it to the Control Center.
- **Send-IPFIX** – Send audit logs via IPFIX exporter.
- **Forward-and-Send-IPFIX** – Forward audit logs to the Control Center and simultaneously send them via IPFIX exporter.
- **Regular-Log-File** – Write audit log to an ASCII log file.
- **Syslog-Proxy** – Generate syslog messages.
- **Executable** – Feed into a custom executable via STDIN.
- **Send-UDP-Packet** – Send a plain UDP stream.

Audit log viewers on both the firewall and Control Center allow you to view the collected data either as plain log files in Log File mode, or similar to the Firewall Live view in Accumulated Event view.

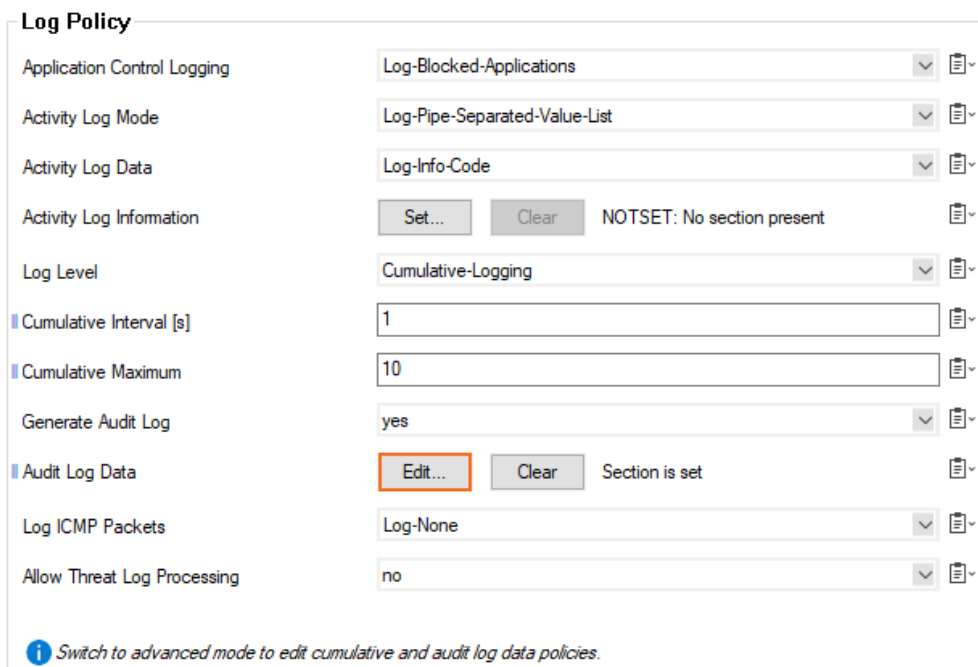
Limitations

- IPS Port scan information displayed on the **Firewall > Threat Scan** page are not included in the Audit logs.
- Keep in mind that the Control Center must receive and write data from a large number of firewalls, each of which may be capable of handling thousands of sessions. Accessing or writing FW Audit large data sets in the relational database is very CPU- and IO-intensive. Make use of the granular configuration options to limit the amount of data included in the audit log.
- The FW Audit Log Service does not synchronize Audit data within an HA cluster. For the CC Audit Info viewer and for the FW Audit Info collector, the service may run on the backup box to collect new data. In case of a failover to the backup box, new Audit data is stored on the backup box, and querying of this data needs to be performed on the backup box.

Step 1. Enable FW Audit on CloudGen Firewall

You must enable the audit log and choose where it is sent and/or stored. Repeat these steps for every firewall that should send audit logs to the Control Center.

1. Go to **YOUR CloudGen Firewall > Infrastructure Services > General Firewall Configuration**.
2. In the **Configuration Mode** section of the left menu, click **Switch to Advanced View**.
3. In the left menu, click **Audit and Reporting**.
4. Click **Lock**.
5. In the **Log Policy** section, click **Edit** next to **Audit Log Data**. The **Audit Log Data** window opens.



Log Policy	
Application Control Logging	Log-Blocked-Applications
Activity Log Mode	Log-Pipe-Separated-Value-List
Activity Log Data	Log-Info-Code
Activity Log Information	Set... Clear NOTSET: No section present
Log Level	Cumulative-Logging
Cumulative Interval [s]	1
Cumulative Maximum	10
Generate Audit Log	yes
Audit Log Data	Edit... Clear Section is set
Log ICMP Packets	Log-None
Allow Threat Log Processing	no

Switch to advanced mode to edit cumulative and audit log data policies.

6. Select the **Audit Delivery** method. E.g., **Local-DB-And-Forward** to send audit log to an Control Center while also storing them locally.
7. Depending on the delivery method, you may have to configure additional settings.
For the default **Local-DB-And-Forward** and **Forward-Only** delivery methods, configure the following:
 - **Send to IP Address** – Enter the IP address of the Control Center.
 - **Send to Port** – Enter 680. This is the listening port of the CC Audit Service on the Control Center.

Audit Log Handling

Audit Delivery	Local-DB-And-Forward	
Executable		
Send to IP Address	10.0.91.70	
Send to Port	680	
Use Source IP Address [Optional]		
Transport Mode	Encrypted-Transport	
Report User Name	Yes	

8. In the **Recorded Conditions** section, select the type of data is included in the audit log.

Recorded Conditions

Allowed Sessions (Fwd)	yes	
Allowed Sessions (Local)	yes	
Protocol Detection (Fwd)	yes	
Protocol Detection (Local)	yes	
Failed Sessions (Fwd)	no	
Failed Sessions (Local)	no	
Session Termination (Fwd)	yes	
Session Termination (Local)	yes	
Blocked Sessions (Fwd)	no	
Blocked Sessions (Local)	no	
Dropped Packets	no	
Invalid ARPs	no	

9. In the **Log File Rotation and Removal** section, configure the retention period of the audit logs (default: 3 days).

10. Click **OK**.

11. Click **Send Changes** and **Activate**.

Step 2. Create CC Audit Service on the Control Center

1. Log into the box level of your Control Center.
2. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services**.
3. Right-click on **Assigned Services** and click **Create Service**. The **Wizard** window opens.
4. Enter the **Service Name**.
5. Select **CC FW Audit Log Service** from the **Software Module** list.
6. Click **Finish**.
7. Click **Activate**.

8. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > CC-Audit-Service > Central Firewall Audit**.
9. Click **Lock**.
10. (optional) To receive audit logs from unmanaged firewalls, add the public keys of the box certificate to the **Explicit Box Keys** list.
11. (optional) For large deployments, select **Multiple Box Handler** from the **Box Handler Method** drop-down list.
12. Click **Send Changes** and **Activate**.

The Control Center will now receive and store all audit log data sent by firewalls using the **Forward-Only** and **Local-DB-And-Forward** delivery methods.

Local FW Audit Viewer on the CloudGen Firewall

To view the audit log directly on the firewall, you must use the Local-DB delivery method. Go to **FIREWALL > Audit Log** to view the audit log. For more information, see [Audit Log Page](#).

DASHBOARD CONFIGURATION CONTROL FIREWALL VPN LOGS STATISTICS EVENTS SSH															
Monitor	Live	History	Threat Scan	Audit Log	Shaping	Users	Dynamic	Host Rules	Forwarding Rules	Log File Mode	09:17:42 22.12.2020	Max Entries: 500			
Date/Time	Operation	Type	Proto	Src IF	Src IP	Src Port	Src MAC	Dst IP	Dst Port	Dst Service	Dst IF	Rule	Info	Dst NAT	Src NAT
2015 08 2...	Local/Allow	LOUT	TCP	eth0	10.0.10.88	21835		10.0.10.44	5140	tcp-port-5140	eth0	PASSALL	Normal Operat...		
2015 08 2...	Local/Remove	LOUT	TCP	eth0	10.0.10.88	47892		10.0.10.44	5140	tcp-port-5140	eth0	PASSALL	Normal Operat...		
2015 08 2...	Block	FWD	UDP	eth0		68	00:0c:29:3b:f6...	255.255.255.2...	67	bootps		BLOCKALL	Block by Rule		
2015 08 2...	Local/Allow	LOUT	TCP	eth0	10.0.10.88	22033		10.0.10.44	5140	tcp-port-5140	eth0	PASSALL	Normal Operat...		
2015 08 2...	Local/Remove	LOUT	TCP	eth0	10.0.10.88	21835		10.0.10.44	5140	tcp-port-5140	eth0	PASSALL	Normal Operat...		
2015 08 2...	Block	FWD	UDP	eth0		68	00:0c:29:3b:f6...	255.255.255.2...	67	bootps		BLOCKALL	Block by Rule		
2015 08 2...	Allow	FWD	UDP	eth0	10.0.10.100	62717	00:0c:29:b3:2...	8.8.8.8	53	domain	eth1	LAN-2-INTER...	Normal Operat...	62.99.0.40.64...	
2015 08 2...	Local/Remove	LOUT	UDP	eth0	10.0.10.88	123		10.0.10.44	123	ntp	eth0	BOX-NTP-OUT	Balanced Ses...		
2015 08 2...	Remove	FWD	TCP	eth0	10.0.10.100	59889	00:0c:29:b3:2...	68.232.34.200	443	https	eth1	LAN-2-INTER...	Normal Operat...	62.99.0.40.32...	
2015 08 2...	Local/Allow	LOUT	TCP	eth0	10.0.10.88	59540		10.0.10.44	5140	tcp-port-5140	eth0	PASSALL	Normal Operat...		
2015 08 2...	Allow	FWD	UDP	eth0	10.0.10.100	63797	00:0c:29:b3:2...	8.8.4.4	53	domain	eth1	LAN-2-INTER...	Normal Operat...	62.99.0.40.55...	

FW Audit Info Viewer on the Control Center

To view audit log data on the Control Center, you must use the **Forward-Only** or **Local-DB-And-Forward** delivery methods. Only selected firewalls (green check mark) are included in the FW Audit log viewer. In the left menu, double-click on the CloudGen Firewall to add the units audit log to the viewer. For more information, see [CC FWAUDIT Tab](#).

CONTROL CONFIGURATION DATABASE ADMINS STATISTICS EVENTS NETWORK ACCESS CLIENT FW AUDIT															
Selection		Filter		Accumulation		Log File Mode		09:46:15 22.12.2020		Max Entries: 500		Refresh (F5)			
Box	Date/Time	Box	Operation	Type	Proto	Src IF	Src IP	Src Port	Src M...	Dst IP	Dst Port	Dst Service	D...	Rule	Info
✓ HQ-NG1	2015 09 0...	HQ-NG...	Local/Allow	LOUT	TCP	eth0	10.0.10.88	45724		10.0.10.44	5140	tcp-port-5140		PASSALL	Normal Operation
✓ BO2-NG1	2015 09 0...	HQ-NG...	Local/Remove	LOUT	TCP	eth0	10.0.10.88	52584		10.0.10.44	5140	tcp-port-5140	eth0	PASSALL	Normal Operation
✓ HQ-NG2	2015 09 0...	HQ-NG...	Local/Allow	LOUT	TCP	eth0	10.0.10.88	52584		10.0.10.44	5140	tcp-port-5140		PASSALL	Normal Operation
	2015 09 0...	HQ-NG...	Local/Remove	LOUT	TCP	eth0	10.0.10.88	42347		10.0.10.44	5140	tcp-port-5140	eth0	PASSALL	Normal Operation
	2015 09 0...	HQ-NG...	Drop	FWD	TCP	eth1	64.235.151.8	443	00:0c...	62.99.0.40	8365	tcp-port-8365			TCP Packet Belor
	2015 09 0...	HQ-NG...	Local/Remove	LOUT	TCP	eth0	10.0.10.88	61911		10.0.10.33	801	device	eth0	HA-SYNC	Normal Operation
	2015 09 0...	HQ-NG...	Local/Allow	LIN	UDP	eth0	10.0.10.63	123	00:50...	10.0.10.88	123	ntp	eth0	OP-SRV-NTP	Normal Operation
	2015 09 0...	HQ-NG...	Local/Allow	LOUT	TCP	eth0	10.0.10.88	42347		10.0.10.44	5140	tcp-port-5140		PASSALL	Normal Operation
	2015 09 0...	HQ-NG...	Block	FWD	TCP	vpn...	192.168.20.3	21500		192.168.20.1	179	bgp		BLOCKALL	Block by Rule

Figures

1. log_policy01.png
2. log_policy02.png
3. log_policy03.png
4. fw_audit_viewer_standalone.png
5. fw_audit_viewer_cc.png

© 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.