How to Configure Audit & Reporting with IPFIX

https://campus.barracuda.com/doc/73719598/

On the Barracuda CloudGen Firewall, you can stream audit and reporting information based on the IPFIX protocol to multiple external collectors. Enable IPFIX, add collectors and optionally enable IPFIX streaming for your HTTP proxy access log.

Step 1. Enable and Configure IPFIX

Before you can stream your audit log or HTTP proxy access log, you must enable and configure IPFIX.

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > General Firewall Configuration**.
2. In the left menu, select **Audit and Reporting**.
3. In the left menu, expand **Configuration Mode** and click **Switch to Advanced View**.
4. Click **Lock**.
5. In the **Log Policy Section** click **Edit** to set **Audit Log Data**. The **Audit Log Handling** window opens.
6. Set **Audit Delivery** to **Send IPFIX** or **Forward-and-Send-IPFIX**.
7. Click **OK**.
8. In the **IPFIX Streaming** section, set **Enable IPFIX/Netflow** to **yes**.
9. (optional) Set **Enable intermediate report** to **yes**.
10. (optional) Enter the **IPFIX reporting interval** for intermediate reports in minutes.
11. Choose a **IPFIX Template**:
    - **Default** – Includes basic data. This is the default template used in firmware version 5.4.X.
    - **Extended** – Includes all data from the default template plus octetDeltaCount, packetDeltaCount, reverseOctetDeltaCount, reversePacketDeltaCount and firewallEvent.
12. Click **+** next to **Collectors** to add a IPFIX/Netflow collector.
    1. Enter a **Name** for the collector settings and click **OK**. The **Collectors** window opens.
    2. Select the protocol from the **Export Mode** list. Because IPFIX data streams may contain confidential data, it is recommended that you select **TCP/SSL**.
    3. If you are using TCP/SSL, configure the SSL certificate settings.
    4. Enter the **Collector IP**.
    5. Enter the **Collector Port**.
    6. Select the **Byte order for data**. Default: **BigEndian**
13. Enter the **Collector IP** and **Collector Port** of the IPFIX collector.
14. Click **OK**.
15. Click **Send Changes** and **Activate**.

You must also create a **PASS** host firewall rule to allow traffic between the Barracuda CloudGen Firewall and the IPFIX collector.

Step 2. (optional) Enable HTTP Proxy Access Log Streaming via IPFIX

After you configure IPFIX streaming, you can enable the Barracuda CloudGen Firewall to stream HTTP proxy access log data via IPFIX.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > HTTP-Proxy > HTT Proxy Settings**.
2. From the **Configuration Mode** menu, select **Switch to Advanced View**.
3. Click **Lock**.
4. In the **Log Settings** section, set **IPFIX Streaming** to **yes**.
5. Click **Send Changes** and **Activate**.

Log Stream Information/IPFIX Output

Standard Fields

Field ID	Name
1	octetDeltaCount
1	reverseOctetDeltaCount
2	packetDeltaCount
2	reversePacketDeltaCount
4	protocolIdentifier
7	sourceTransportPort
8	sourceIPv4Address
10	ingressInterface
11	destinationTransportPort
12	destinationIPv4Address
14	egressInterface
56	sourceMacAddress
85	octetTotalCount
85	reverseOctetTotalCount
86	packetTotalCount
86	reversePacketTotalCount
161	flowDurationMilliseconds
233	firewallEvent

Custom Fields

Private Enterprise Number Barracuda Networks: 10704				
Field ID	**Length (octets)**	**Type**	**Name**	**Description**
1	4	Int	Timestamp	Seconds since epoch
2	1	Int	LogOp	*see section LogOp*
3	1	Int	TrafficType	*see section TrafficType*
4	variable	String	FW Rule	Name of the firewall rule
5	variable	String	ServiceName	Name of service
6	4	Int	Reason	Reason in datatype Integer
7	variable	String	ReasonText	Reason in datatype String
8	4	Int	BindIPv4Address	
9	2	Int	BindTransportPort	
10	4	Int	ConnIPv4Address	
11	2	Int	ConnTransportPort	
12	4	Int	AuditCounter	Internal data counter

LogOp

ID	Name
0	Unknown
1	Allow
2	LocalAllow
3	Block
4	LocalBlock
5	Remove
6	LocalRemove
7	Drop
8	Terminate
9	LocalTerminate
10	Change
11	Operation
12	Startup
13	Configuration
14	Rule
15	State
16	LocalState

17	Process
18	AdminAction
19	Deny
20	LocalDeny
21	SecurityEvent
22	Sync
23	Fail
24	LocalFail
25	ARP
26	Detect
27	LocalDetect
28	IntermediateReport

Traffic Type

ID	Name
0	Forwarding
1	Local In
2	Local Out
3	Loopback