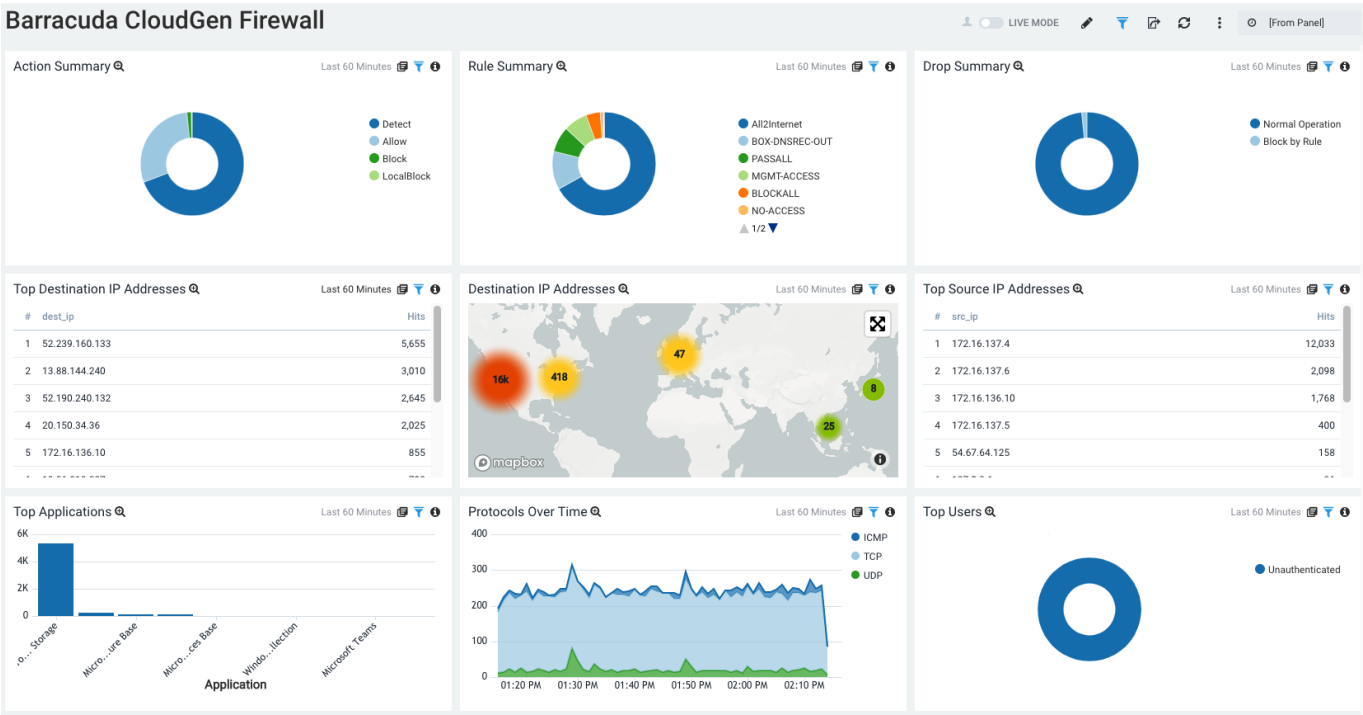
Sumo Logic Integration

https://campus.barracuda.com/doc/91132156/

Sumo is a third-party log management and analytics service, transforming your data into sources of operations, security, and compliance intelligence. The Barracuda CloudGen Firewall app provides a dashboard to monitor actions, IP addresses, and rule and application usage. Data is imported into Sumo via syslog streaming of the Firewall logs.



Before You Begin

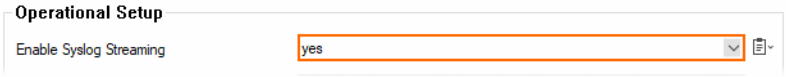
- Configure a cloud syslog source in your Sumo account. For the **Source Category**, it is recommended to use a self-explanatory name like **'CGFW'**.
  For information and help, see also https://help.sumologic.com/03Send-Data/Sources/02Sources-for-Hosted-Collectors/Cloud-Syslog-Source.
- Run and configure syslog-ng on a host within your network.
  For information and help, see also https://help.sumologic.com/03Send-Data/Sources/02Sources-for-Hosted-Collectors/Cloud-Syslog-Source#Send_data_to_cloud_syslog_source_with_syslog-ng.

Configure Syslog Streaming on a Barracuda CloudGen Firewall

Configure and enable syslog streaming for every Barracuda CloudGen Firewall you want to include in the Sumo app.

Step 1.1. Enable Syslog Streaming

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Syslog Streaming**.
2. Click **Lock**.
3. Set **Enable the Syslog service** to **yes**.

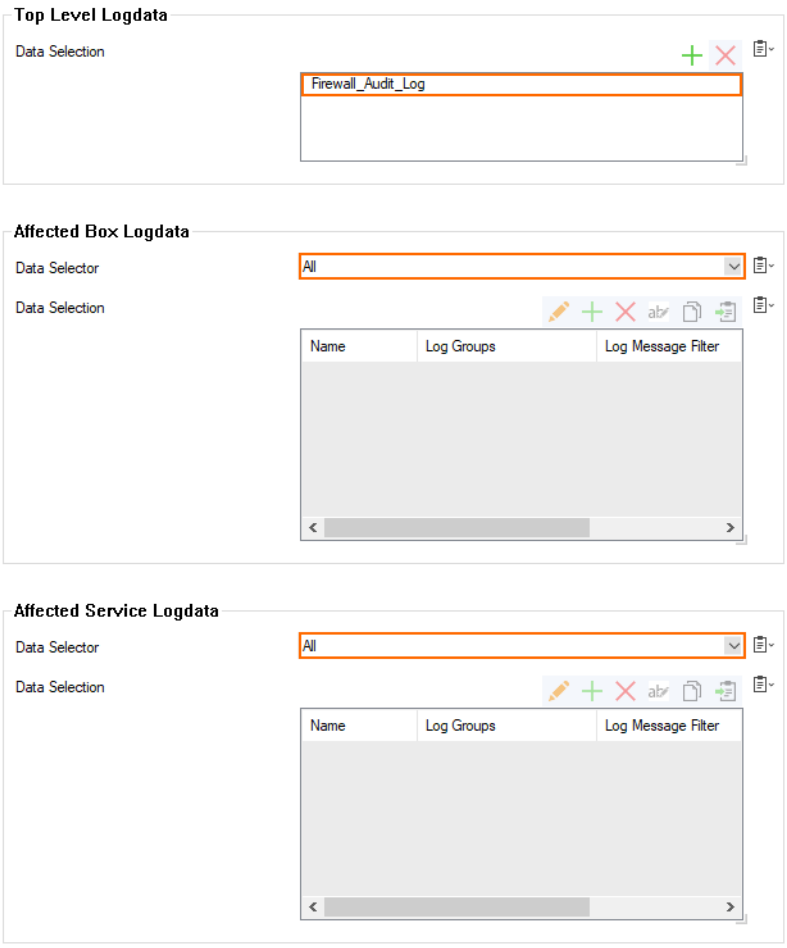


4. Click **Send Changes** and **Activate**.

Step 1.2. Configure Logdata Filters

Define profiles specifying the log file types to be transferred / streamed.

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Syslog Streaming**.
2. In the left menu, select **Logdata Filters**.
3. Click **Lock**.
4. Click **+** to add a new filter.
5. Enter an expressive **Name** that refers to Sumo, e.g., *SumoFilter*.
6. Click **OK**.
7. The **Filters** window opens.
8. Click **+** in the **Data Selection** table and select **Firewall_Audit_Log**.
   Fatal_log and **Panic_log** data can also be streamed to the Sumo server but are currently not processed by the Barracuda CloudGen Firewall Sumo app.
9. In the **Affected Box Logdata** section, select **All** from the **Data Selector** drop-down menu.
10. In the **Affected Service Logdata** section, select **All** from the **Data Selector** list.
11. Click **OK**.
12. Click **Send Changes** and **Activate**.



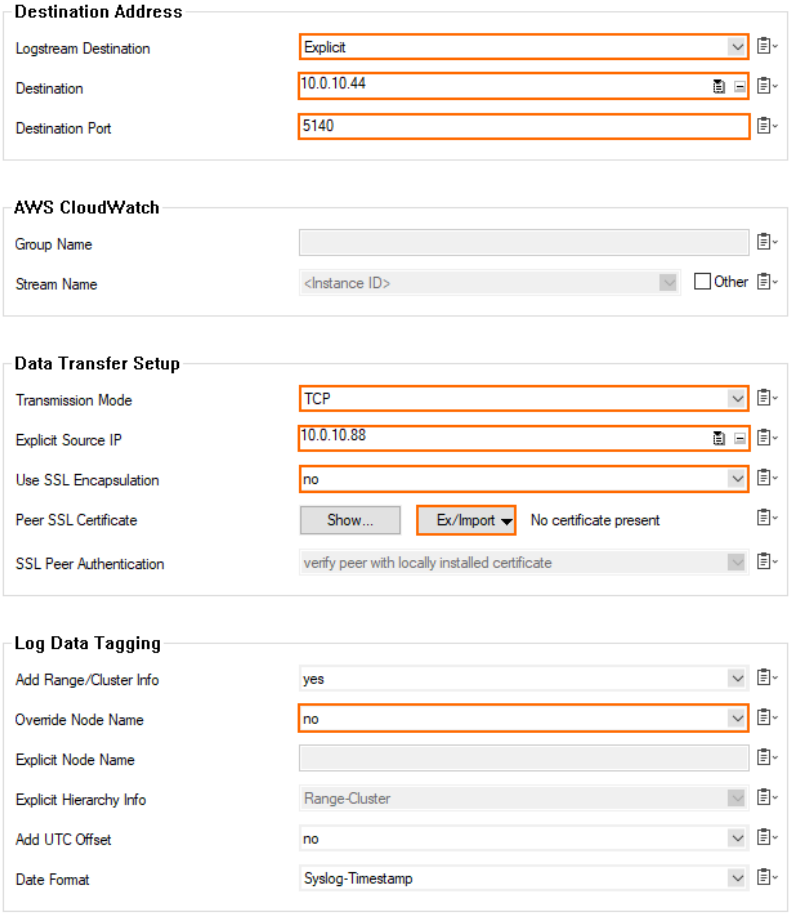
Step 1.3. Configure the Logstream Destinations

Configure the data transfer settings for the Sumo server. You can optionally choose to send all syslog data via an SSL-encrypted connection.

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Syslog Streaming**.
2. In the left menu, select **Logstream Destinations**.
3. Click **Lock**.
4. Click **+** in the **Destinations** table.
5. The **Destinations** window opens.
6. For **Name**, enter an expressive name that refers to Sumo, e.g., *Sumo*.
7. Click **OK**.
8. The window for configuring the specific destination to Sumo is displayed.
9. Configure the syslog-ng server logstream destination:
    1. **Logstream Destination** – Select **explicit-IP**.
    2. **Destination** – Enter the IP address of the syslog-ng server that will be forwarding logs to Sumo.
    3. **Destination Port** – Enter **5140** for plaintext of **5141** for SSL-encrypted connections.
    4. **Transmission Mode** – Select **TCP** or **UDP** (only for unencrypted connections).

5. **(optional) Explicit Source IP** – Enter the management IP address of the Barracuda CloudGen Firewall, or leave blank for the CloudGen Firewall to do a routing lookup to determine the sender IP address.
6. **(optional) Use SSL Encapsulation** – Select **yes** to send the syslog stream over an SSL-encrypted connection.
7. **(optional) Peer SSL Certificate** – Import the SSL certificate configured on the syslog-ng server for this stream.
8. **Override Node Name** – Select **no**.

10. Click **OK**.



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

Step 1.4. Configure Logdata Streams

Create a logdata stream configuration combining the previously configured **Log Destinations** and **Log Filters**.

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Syslog Streaming**.
2. In the left menu, select **Logdata Streams**.
3. Click **Lock**.
4. Click **+** in the **Streams** table.
5. Enter a **Name** and click **OK**.

6. The **Streams** window opens.
7. In the **Log Destinations** table, click **+** and select the **Log Destination** created in Step 1.3, e.g., *Sumo*.
8. In the **Log Filters** table, click **+** and select the **Log Filter** created in Step 1.2, e.g., *SumoFilter*.

9. Click **OK**.
10. Click **Send Changes** and **Activate**.

Step 1.5 Configure WebLog Streaming (optional)

As a first step, you must activate web log streaming:

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Syslog Streaming**.
2. In the left menu, select **Logdata Streams**.
3. Click **Lock**.
4. **Enable Web Log Streaming** – Select **yes**.

As the second step, you must configure the web log syslog streaming:

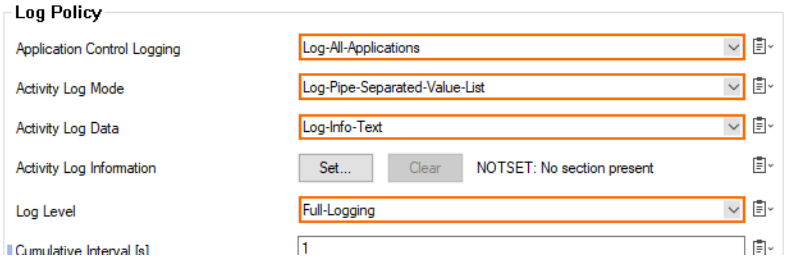
1. **Streaming Protocol** – Select **TCP** or **UDP** (only for unencrypted connections).
2. **Destination IP Address** – Enter the IP address of the syslog-ng server that will be forwarding logs to Sumo.
3. **Destination Port** – Enter **5140** for plaintext or **5141** for SSL-encrypted connections.
4. **SSL ...** (optional) – Configure the key and certificates to send logs to this server.

Step 1.6 Configure Audit and Reporting

Configure the settings for log policies.

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 section **Statistics Policy**, set **Generate Dashboard Information** to **yes**.
6. In the section **Statistics Policy**, set **Generate Monitor Information** to **yes**.

7. In the **Log Policy** section, set **Application Control Logging** to **Log-All-Applications**.
8. In the **Log Policy** section, set **Activity Log Mode** to **Log-Pipe-Separated-Value-List**.
9. In the **Log Policy** section, set **Activity Log Data** to **Log-Info-Text**.
10. In the **Log Policy** section, set **Log Level** to **Full-Logging**.

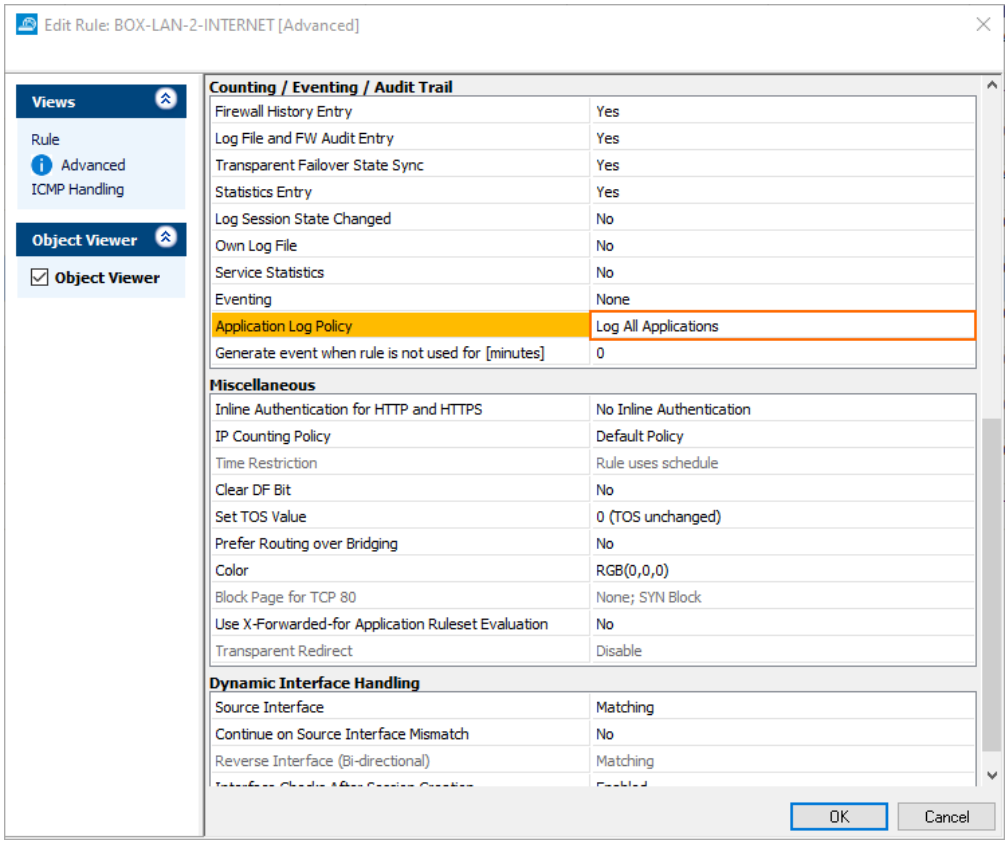


All firewall log data is now being streamed to Sumo via the syslog-ng server.

Enable Application Logging in the Firewall

Application data is collected on a per-access-rule basis. Set the **Application Log Policy** to **Log All Applications** in the **Advanced Firewall Rule Settings** for each access rule that matches traffic you want to include in the data collected on the Sumo server.

For more information, see Advanced Access Rule Settings.



The Barracuda CloudGen Firewall Sumo App

In the Sumo Logic App Catalog, search for **Barracuda CloudGen Firewall**.

Click **Add to Library** to install this app.

(optional) Configure Sumo Logic Field Extraction Rules

In Sumo Logic, click **Manage Data > Settings > Field Extraction Rules**.

Add the following 4 rules as needed.

CGFW Activity Log

```
parse regex " (?<action>[\S]*):
type=(?<type>[^|]*)\|proto=(?<proto>[^|]*)\|srcIF=(?<srcif>[^|]*)\|srcIP=(?<s
rc_ip>[^|]*)\|srcPort=(?<src_port>[^|]*)\|srcMAC=(?<srcmac>[^|]*)\|dstIP=(?<d
```

```
est_ip>[^|]*)\|dstPort=(?<dest_port>[^|]*)\|dstService=(?<dstservice>[^|]*)\|
dstIF=(?<dstif>[^|]*)\|rule=(?<rule>[^|]*)\|info=(?<info>[^|]*)\|srcNAT=(?<sr
cnat>[^|]*)\|dstNAT=(?<dstnat>[^|]*)\|duration=(?<duration>[^|]*)\|count=(?<c
ount>[^|]*)\|receivedBytes=(?<receivedbytes>[^|]*)\|sentBytes=(?<sentbytes>[^
|]*)\|receivedPackets=(?<receivedpackets>[^|]*)\|sentPackets=(?<sentpackets>[
^|]*)\|user=(?<user>[^|]*)\|protocol=(?<protocol>[^|]*)\|application=(?<appli
cation>[^|]*)\|target=(?<target>[^|]*)\|content=(?<content>[^|]*)\|urlcat=(?<
urlcat>[^|]*)"
```

CGFW Web Log

```
parse " - * 1 * * * * * * BYF * * * * * * * (*) * * * * * * * [*] * - - 0" as
timestamp, src_ip, dest_ip, content_type, srcip, uri, content_length, action,
reason, version, match, tq, action_type, src_type, src_detail, dst_type,
dst_detail, spy_type, spy_id, inf_score, host, urlcat, user, host2
```

ATP Event Log

```
parse regex
"\(\S\|\d\|\S+\|\d\|\S+\|\d+\|(?<atp_action>[^|]*)\|(?<hostname>[^|]*)\|(?<at
p_timestamp>\d+)\|(?<atp_message>.*)\)"|parse regex field=atp_message
"(?<src_ip>\d+.\d+.\d+.\d+):(?<src_port>\d+) ->
(?<dest_ip>\d+.\d+.\d+.\d+):(?<dest_port>\d+)"
```

ATP Scan

```
parse " - * 1 * * * * * * BYF * * * * * * * (*) * * * * * * * [*] * - - 0" as
timestamp, src_ip, dest_ip, content_type, srcip, uri, content_length, action,
reason, version, match, tq, action_type, src_type, src_detail, dst_type,
dst_detail, spy_type, spy_id, inf_score, host, urlcat, user, host2
```

Figures

1. 1App_Dashboard.png
2. sumo_logic_enable_syslog_streaming.png
3. sumo_logic_logdata_filters.png
4. sumo_logic_logstream_destinations.png
5. sumo_logic_stream_configuration.png
6. sumo_logic_configure_statistics_policy.png
7. sumo_logic_configure_log_policy.png
8. sumo_logic_configure_access_rule_advanced_app_log_policy.png