How to Configure Syslog Streaming

https://campus.barracuda.com/doc/73719612/

The syslog streaming configuration defines the handling of log files. Log messages of centrally managed firewalls can be transmitted to the Firewall Control Center Syslog service, but they can just as well be transmitted to any other system designed for log file collection or to another Barracuda CloudGen Firewall.

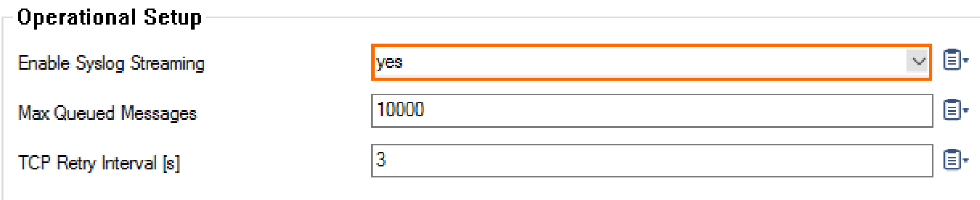
Before You Begin

To send log data from the same source (e.g., VPN) to multiple destinations, there must be only a single entry in the Logdata Filters table that contains the definition of that source. The various Logstream Destinations must be assigned to that single source when configuring logdata streams:

Entry #	Logdata Filters	Logdata Streams	Logstream Destinations
1	FW	--- S1 -->	D1
2	DHCP	--- S2 -->	D2
3	VPN	--- S3 -->	D1, D2

Step 1. Enable the Syslog Service

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



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

Step 2. (optional) Upload External SSL Certificates

If the syslog stream is SSL encrypted, the box certificate and key are used by default. You can upload custom SSL certificates if you want to use them.

1. Go to **CONFIGURATION > Full Configuration > Box > Infrastructure Services > Syslog Streaming**.
2. Click **Lock**.
3. In the left menu, expand the **Configuration Mode** section and click **Switch to Advanced View**.
4. From the **Use Box Certificate/Key** list, select **no**.
5. Import the **SSL Private Key** and **SSL Certificate**
6. Click **Send Changes** and **Activate**.

Step 3. Configure Logdata Filters

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

1. Go to **CONFIGURATION > Full Configuration > Box > Infrastructure Services > Syslog Streaming**.
2. In the left menu, select **Logdata Filters**.
3. Expand the **Configuration Mode** menu and select **Switch to Advanced View**.
4. Click **Lock**.
5. Click the **+** icon to add a new entry.
6. Enter a descriptive name in the **Filters** dialog and click **OK**.
7. In the **Data Selection** table, add the log files to be streamed. You can select:
    - **Fatal_log** – Log contents of the fatal log (log instance name: fatal)
    - **Firewall_Audit_Log** – The log contents of the firewall's machine readable audit data stream. Whether data is streamed into the Firewall_Audit_Log has to be configured in the **General Firewall Configuration** settings on box-level, section **Audit Log Handling** > **Audit-Delivery**: Syslog-Proxy (see: FW Audit). The log instance name corresponding to Syslog-Proxy selected will be trans7.
    - **Panic_log** – log contents of the panic log (log instance name: *panic*)

      When *Log-File* is selected in the firewall's configuration, the data will go into a log file named *Box->Firewall->audit* (which means the instance is named *box_Firewall_audit*) and this filter setting is therefore not applicable. The pertinent one then would be a selection of category *Firewall* within the box selection portion of the filter.
8. In the **Affected Box Logdata** section, define what kind of box logs are to be affected by the syslog daemon from the **Data Selection** list.
9. When choosing **Selection** (default):
    1. Click the **+** icon next to **Data Selection** to add an entry.
    2. Enter a descriptive name for the group and click **OK**. The **Data Selection** window opens.
    3. Add the **Log Groups** for selection or select **Other** and specify an explicit selection. For more information, see User Defined Log Groups.
    4. Set a **Log Message Filter**. When choosing **Selection**,
        - Add the explicit log type to the **Selected Message Types** table.
    5. Click **OK**.

10. In the **Affected Service Logdata** section, define what kind of logs created by services are to be affected by the syslog daemon from the **Data Selection** list.
11. When choosing **Selection** (default),
    1. Click the **+** icon next to **Data Selection** to add an entry.
    2. Enter a descriptive name for the group and click **OK**. The **Data Selection** window opens.
    3. In the **Log Groups** table, add the server and services where log messages are streamed from, or select **Other** and specify a more granulated selection. For more information, see User Defined Log Groups
    4. Set a **Log Message Filter**. When choosing **Selection**,
        - Add the explicit log type to the **Selected Message Types** table.
    5. Click **OK**.
12. Click **Send Changes** and **Activate**.

User Defined Log Groups

For selective syslog streaming, a configured logstream destination is required. This can either be a Barracuda Firewall Control Center or a dedicated third-party syslog server. For granulated selection, configure logdata filters, using the **Data Selection** > **Log Groups** parameter **Other** and enter a string up to sample:

- <modulname>_<logfile>

Example (for Affected Service Logdata):

- virscan_cas
- firewall_auth
- firewall_Rule*

This selection would stream:

- srv_<virscan-servername>_<virscan-servicename>_cas.log
- srv_<firewall-servername>_<firewall-servicename>_auth.log
- srv_<firewall-servername>_<firewall-servicename>_Rule*.log

This selection would not stream:

- srv_<virscan-servername>_<virscan-servicename>.log
- srv_<virscan-servername>_<virscan-servicename>_clamav.log
- srv_<firewall-servername>_<firewall-servicename>.log

List of Available Box Module Names

- Auth: **Auth**

- Config: **Config**
- Control: **Control**
- Event: **Event**
- Firewall: **Firewall**
- Logs: **Logs**
- Network: **Network**
- Release: **Release**
- Settings: **Settings**
- SSH: **SSH**
- Statistics: **Statistics**
- System: **System**
- Watchdog: **Watchdog**

List of Available CC-managed Box Modules

- AV-Scanner: **virscan**
- DHCP-Enterprise-Server: **dhcpe**
- DHCP-Relay: **dhcprelay**
- DNS: **dns**
- Firewall: **firewall**
- FW-Audit-Service: **fwaudit**
- C-Firewall: **cfirewall**
- FTP-Gateway: **ftpgw**
- HTTP-Proxy: **proxy**
- HTTP/HTTPS-Proxy: **sslprx**
- Mail-Gateway: **mailgw**
- OSPFv2-Router: **ospf**
- Policy-Service: **policyserver**
- Secure-Web-Proxy: **sslprx**
- SPAM-Filter: **spamfilter**
- SNMP-Service: **snmp**
- SSH-Proxy: **sshprx**
- ISS-ProventiaWebFilter: **cofs**
- VPN-Server: **vpnserver**

List of Available Single Box Module Names

- AV-Scanner: **virscan**
- DHCP-Enterprise-Server: **dhcpe**
- DHCP-Relay: **dhcprelay**
- DNS: **dns**
- Firewall: **firewall**

- FTP-Gateway: **ftpgw**
- HTTP-Proxy: **proxy**
- HTTP/HTTPS-Proxy: **sslprx**
- ISS-ProventiaWebFilter: **cofs**
- Mail-Gateway: **mailgw**
- OSPFv2-Router: **ospf**
- Policy-Service: **policyserver**
- Secure-Web-Proxy: **sslprx**
- SNMP-Service: **snmp**
- SPAM-Filter: **spamfilter**
- SSH-Proxy: **sshprx**
- VPN-Server: **vpnserver**

List of Available Control Center-Module Names (CC Box)

- DNS: **dns**
- Firewall: **firewall**
- MC-Audit: **fwaudit**
- MC-Conf: **rangeconf**
- MC-Event: **mevent**
- MC-Log: **msyslog**
- MC-PKI: **pki**
- MC-Entegra: **mpolicyserver**
- MC-Reporter: **rsdstats**
- MC-StatView: **qstatm**
- MC-StatCollect: **dstatm**
- MC-VPN: **mastervpn**

List of Available Reporter Module Names (Reporter Box)

- Reporter DB: **reporter**

Configure Logstream Destinations

Define profiles specifying the transfer/streaming destination of log messages. Log lines from remote systems will be added as they are received but also get their creation time in ISODATE format enclosed in parentheses appended at the end, e.g.: (2013-07-01T18:37:17+00:00). Selecting CloudGen Firewall as destination will stream the log data to another unit in exactly the same file structure as on the sender system.

1. Go to **CONFIGURATION > Full Configuration > Box > Infrastructure Services > Syslog Streaming**.
2. In the left menu, select **Logstream Destinations**.
3. Expand the **Configuration Mode** menu and select **Switch to Advanced View**.
4. Click **Lock**.
5. Click the **+** icon to add a new entry.
6. Enter a descriptive name in the upcoming dialog and click **OK**. The **Destinations** window opens.
7. Select the **Logtream Destination**. When an external log host is used:
    1. Select **Explicit IP** (default).
    2. Configure the destination host:
        1. If you have only an IP address – Enter the destination IP address in the **Destination IP Address** field.
        2. If you have configured an IP or hostname network object on Multi-Range, Range, or Cluster level, you can also click the small icon inside of the edit field to specify the logstream destination by selecting a hostname.
        
8. Enter the **Destination Port** for delivering syslog messages. The Barracuda Networks CC syslog service listens on port TCP 5143 for SSL connections and on TCP and UDP port 5144 for unencrypted streaming. The default is to use encryption for delivery; therefore, port 5143 is preconfigured.
    When changing the port, you must also adapt the host firewall rule for syslog traffic to use the new port.
9. Select the **Transmission Mode** (**TCP or UDP** - default; for SSL connections **TCP** is automatically set).
    You may specify a particular **Sender IP** address used for sending the log data. When sending to a Barracuda Firewall Control Center, either the VIP or, in the absence of a management tunnel, the MIP are selected automatically.
10. Click **OK**.
11. Click **Send Changes** and **Activate**.

You may specify a particular address to be used in order to send the log data.

SSL Encapsulation

The option **Use SSL Encapsulation** may be turned off when the log stream is transmitted to the Barracuda Firewall Control Center and the box has a management tunnel to the Control Center. For CC transmission without box tunnel, activating SSL encapsulation is recommended. Note also that transmission to a non-Barracuda CloudGen Firewall system should be SSL encapsulated for reasons of privacy.

SSL Peer Authentication defines the way in which a destination system is authenticated when using SSL-based authentication (authentication of the destination server by the box being a client). The list offers the following choices:

- **verify_peer_with_locally_installed_certificate** – (default) The destination system is verified against a locally stored certificate either in the respective destination section or the Barracuda Firewall Control Center's certificate. This setting is useful when log messages are delivered to a system outside the scope of Barracuda Firewall Control Centers. For centrally administered firewalls, this is the only applicable option.

  If the destination system is not a Barracuda Firewall Control Center, the peer SSL certificate may be required
- **verify_peer_certificate** – The destination system is verified against a locally stored CA certificate.
- **no_peer_verification** – The peer is considered as trusted without verification. For security reasons, this option it is NOT recommended.

Log Data Tagging

The log entities sent to an external log host contain the name and structural information (range/cluster) of the sending box and the name of the log file. With **Override Node Name** enabled, this information can be overridden (default: disabled). If **Override Node Name** is enabled, specifying an explicit node name is possible. This node name is inserted into each log entity sent to the external log host. The setting **Prepend Hierarchy Info** allows fine tuning of the prefix, which is inserted into each log entity sent to the external log host.

Log files generated on a box are stamped with the local box time. The UTC time offset compared to the local time is recorded, though, and can be examined in the TZ column in the Log Viewer. The UTC time offset information is not included by default when log files are streamed to the Barracuda Firewall Control Center. Enabling Add UTC Offset adds the UTC time offset information to streamed log files, so that these files may be analyzed uniformly in case the Barracuda Firewall Control Center collects log files from multiple boxes placed in various time zones.

Configure Logdata Streams

By configuring this section, relations between log patterns and log destinations are established. It is therefore possible to make a combination of each log pattern (a sort of filter) and log destination to allow fine-granulated target selection.

With **Barracuda CC Control** selected as **Remote Loghost**, the streamed log files will be stored under */phion0/mlogs/range/cluster/box* on the Control Center.

1. Go to **CONFIGURATION > Full Configuration > Box > Infrastructure Services > Syslog Streaming**.
2. In the left menu, select **Logdata Streams**.
3. Expand the **Configuration Mode** menu and select **Switch to Advanced View**.
4. Click the **+** icon to add a new entry.

5. Enter a descriptive name in the upcoming dialog and click **OK**.
6. Configure the following settings:
    - **Active Streams –** This parameter allows you to activate/deactivate the selected log stream profile. By default, for example when creating a new profile, this parameter is set to **yes**.
    - **Log Destinations –** Here the available log destinations (defined in the section **Logstream Destinations**) can be selected.
    - **Log Filters –** Here the available log patterns (defined in the section **Logdata Filters**) can be selected.
7. Click **Send Changes** and **Activate**.

Figures

© Barracuda Networks Inc., 2020 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.