How to Configure Web Log Streaming

https://campus.barracuda.com/doc/79463289/

Web Log streaming allows you to send a syslog stream to an external device, such as the Barracuda Web Security Gateway, for visualization and reporting purposes. Web Logs can only be streamed, not stored locally, because every HTTP and HTTPS request is logged and may result in a high volume of logs. Although TCP and TCP/TLS are supported as streaming protocols, UDP is recommended for performance reasons. To stream HTTPS session the web traffic must match an access rule using SSL Inspection. For HTTP traffic streaming no additional access rules are required. Depending on the target device, it is possible to customize the log format to match the target device using streaming templates. The default settings for Web Log streaming are configured to work with the Barracuda Web Security Gateway. Streaming web logs over a VPN tunnel using WAN Optimization is not supported.

Template Placeholder Values

Variable	Explanation
%action%	ALLOWED or BLOCKED depending on the matching rule
%srcip%	source IP address
%dstip%	destination IP address
%srcport%	source port
%dstport%	destination port
%proto%	Protocol: HTTP or HTTPS
%host%	hostname E.g., www.barracuda.com
%path%	path of the requested URL E.g., /img/image.png
%uri%	URI E.g., www.barracuda.com/img/image.png
%method%	GET or POST
%agent%	user agent
%content-type%	content type of the HTTP or HTTPS request. E.g., text/html, flash, ...
%content-length%	content length in bytes
%content-encoding%	content-encoding E.g., UTF-8
%user%	detected user name
%rule%	matching access rule name
%apprule%	matching application rule name
%code%	HTTP return code
%timestamp%	UNIX timestamp
%urlcat%	URL Category
%actionnum%	1 or 0 (BLOCKED or ALLOWED)

%%	literal percent sign
!$%&/()=?\}][{*+~-_:.;\<>|^\,'	List of allowed special characters
apha	A-Z and a-z
blank	space
digit	0-9

Example streaming template for the Barracuda Web Security Gateway:

```
NG_Firewall[]: %timestamp% 1 %srcip% %dstip% %content-type% %srcip% %uri% %content-length% BYF ALLOWED CLEAN  2 1 0 %actionnum% 0 (-) %actionnum% %urlcat% 0 - 0 %host% %urlcat% [%user%]   %host% - - 0
```

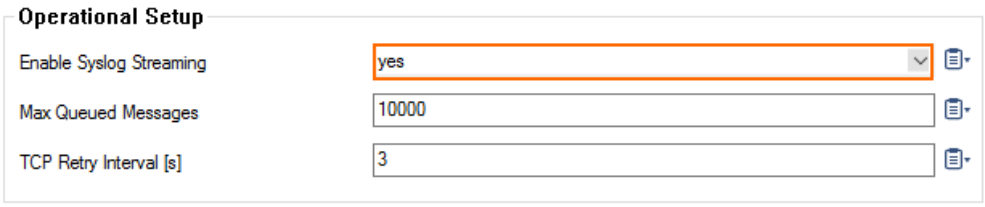
Before You Begin

- When using the Barracuda Web Security Gateway as the destination syslog server, update the Web Security Gateway to the latest available firmware and contact Barracuda Networks Technical Support to set up your Web Security Gateway appliance.
- Collect the following information for your destination device:
  - Destination IP address
  - Destination port
  - Supported streaming protocols
  - Log format
  - Syslog facility
  - Syslog level
- Configure Outbound SSL Inspection. For more information, see How to Configure Outbound SSL Inspection.

Step 1. Activate Syslog Streaming

In order that Web Log Streaming can be (de)activated, Syslog Streaming must be activated prior.

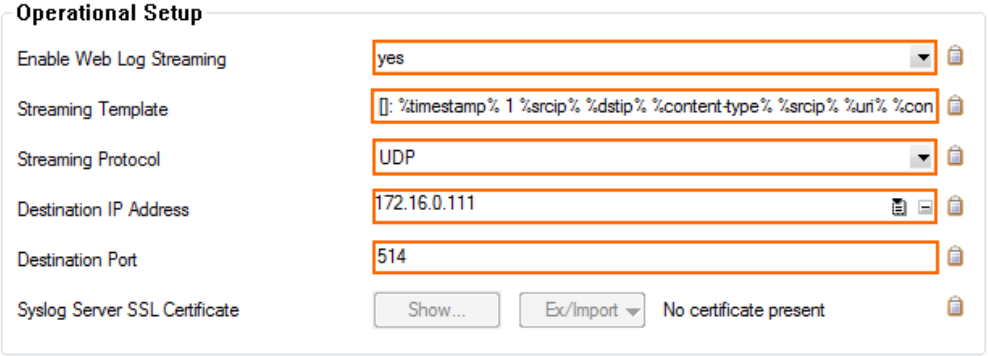
- Go to **CONFIGURATION > Full Configuration > Box > Infrastructure Services > Syslog Streaming**.
- Click **Lock**.
- Set **Enable Syslog Streaming** to **yes**.



Step 2. Configure Web Log Streaming on the Barracuda CloudGen Firewall

Configure the Barracuda CloudGen Firewall to stream every HTTP and HTTPS request to the configured syslog server using the streaming template as the log format.

1. In the left menu, click **Web Log Streaming**.
2. From the **Enable Web Log Streaming** list, select **yes**.
3. Enter the **Streaming Template** as required by the destination device. Use the **template placeholders** and plain text. The default value matches the required log format for the Barracuda Web Security Gateway.
4. Select the **Streaming Protocol**:
   - **UDP** (default) – Unless required by the destination device, use UDP as the streaming protocol because it has the least performance impact on the CloudGen Firewall.
   - **TCP** – Select TCP if required by the destination device. Depending on the streaming volume, using TCP may increase system load.
   - **TCP/TLS** – Select TCP/TLS if required by the destination device. Depending on the streaming volume, using TCP/TLS may significantly increase system load.
5. Enter the **Destination IP Address**.
6. Enter the **Destination Port**. E.g., 514 for the Barracuda Web Security Gateway



7. (TCP/TLS only) Click **Ex/Import** to import the **Syslog Server SSL Certificate**. The SSL certificate must be in PEM or PKCS12 format.
8. (optional) For advanced configuration options:
   1. In the left menu, expand **Configuration Mode** and click **Switch to Advanced Mode**.
   2. Select the **Syslog Facility** as required by the destination device.
   3. Select the **Syslog Level** as required by the destination device.
   4. Enter the **Source IP** used to send the web log stream. Enter `0.0.0.0` for the firewall to use a routing table lookup to select the source IP address.

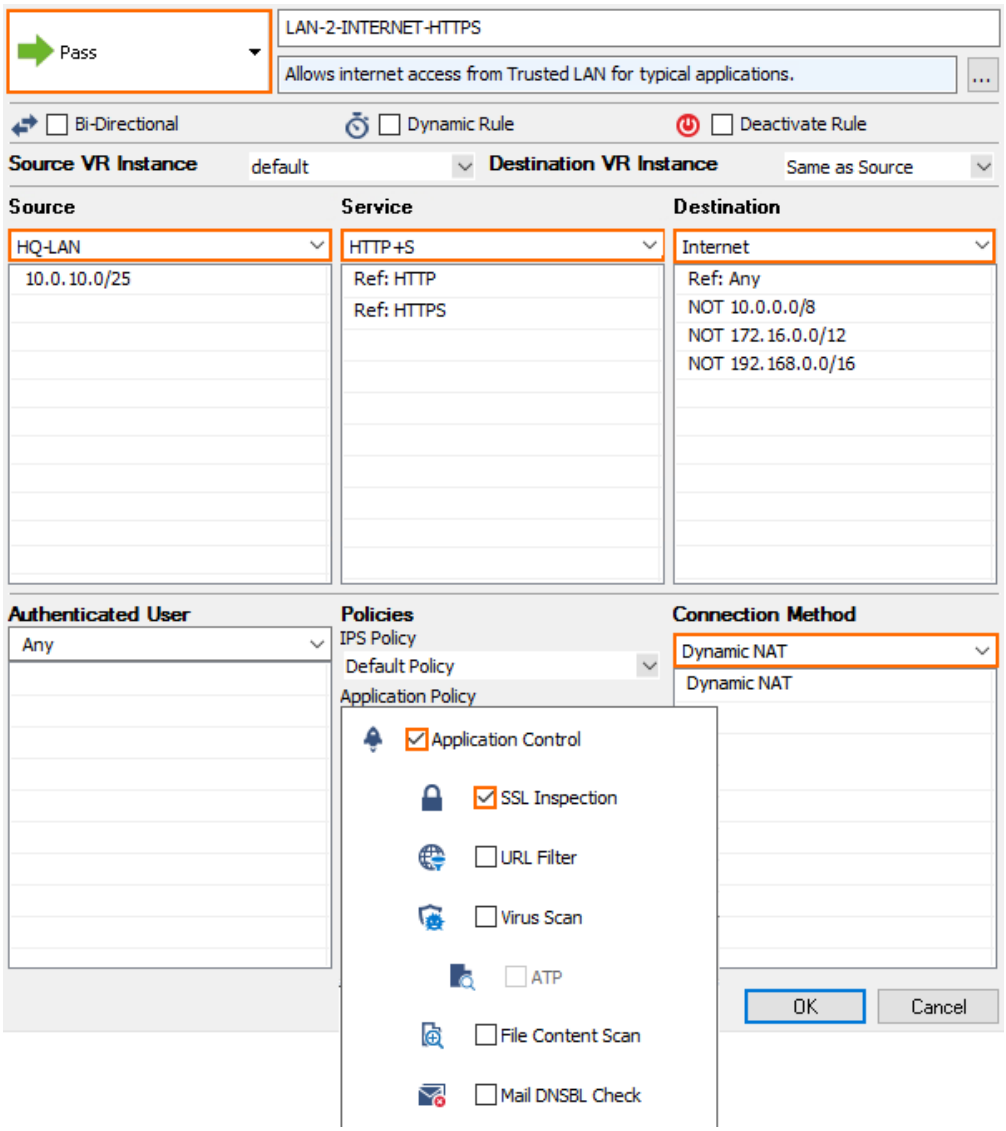
5. Enter the **Source Port** used to send the web log stream. Enter `0` for the firewall to select the source port automatically.

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

Step 3. (HTTPS Only) Create an Access Rule Matching HTTPS Traffic

To be able to stream information about HTTPS connections, ensure that the access rule matching the HTTPS traffic is using SSL Inspection. To use SSL Inspection, the **Feature Level** of the Forwarding Firewall must be set to **7.2** or higher. For more information, see SSL Inspection in the Firewall.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Double-click to edit the access rule matching HTTPS traffic.
3. Click on the **Application Policy** link and select:
   - **Application Control** – required.
   - **SSL Inspection** – required



4. From the **SSL Inspection Policy** drop-down list select a policy for outbound SSL Inspection. For more information, see How to Configure an SSL Inspection Policy for Outbound SSL Inspection.
5. Click **OK**.
6. Click **Send Changes** and **Activate**.

Step 4. Enable Application Control

To enable Application Control, see How to Enable Application Control.

Step 5. Configure the Syslog Service on the Destination Device

Configure the remote device running the syslog service to receive and process the syslog stream from

the firewall.

To use a Barracuda Web Security Gateway as the destination device, contact Barracuda Networks Technical Support to set up your Web Security Gateway appliance.

Figures

1. enable_syslog_streaming.png
2. web_log_01.png
3. web_log_streaming_access_rule.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.