

How to Configure Web Log Streaming

<https://campus.barracuda.com/doc/48202783/>

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 Interception. 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
alpha	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








Step 1. Configure Web Log streaming on the Barracuda NextGen Firewall F-Series

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

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

5. 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.
6. 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 F-Series.
 - **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.
7. Enter the **Destination IP Address**.
8. Enter the **Destination Port**. E.g., 514 for the Barracuda Web Security Gateway

Operational Setup

Enable Web Log Streaming	yes	
Streaming Template	[[: %timestamp% 1 %srcip% %dstip% %content-type% %srcip% %uri% %con	
Streaming Protocol	UDP	
Destination IP Address	172.16.0.111	 
Destination Port	514	
Syslog Server SSL Certificate	<input type="button" value="Show..."/> <input type="button" value="Ex/Import"/> No certificate present	

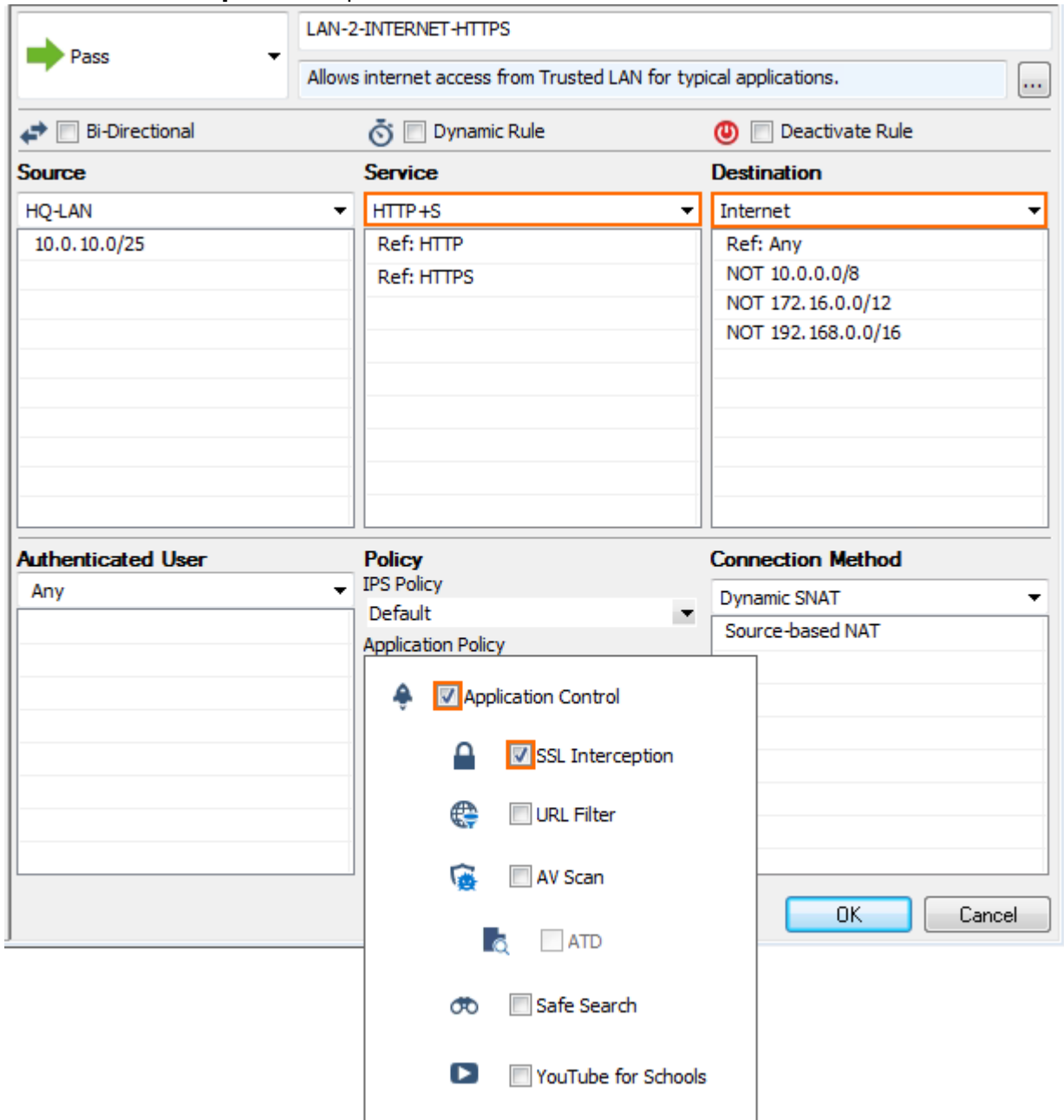
9. (TCP/TLS only) Click **Ex/Import** to import the **Syslog Server SSL Certificate**. The SSL certificate must be in PEM or PKCS12 format.
10. (optional) For advanced configuration options:
 1. In the left menu, expand **Configuration Mode** and click **Switch to Advanced Mode**.
 2. Select the **Syslog 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.
11. Click **Send Changes** and **Activate**.

Step 2. (HTTPS only) Create 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 Interception.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > 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 Interception** - required.



LAN-2-INTERNET-HTTPS

Allows internet access from Trusted LAN for typical applications.

Bi-Directional
 Dynamic Rule
 Deactivate Rule

Source	Service	Destination
HQ-LAN 10.0.10.0/25	HTTP+S Ref: HTTP Ref: HTTPS	Internet Ref: Any NOT 10.0.0.0/8 NOT 172.16.0.0/12 NOT 192.168.0.0/16

Authenticated User	Policy	Connection Method
Any	IPS Policy Default Application Policy	Dynamic SNAT Source-based NAT

Application Control
 SSL Interception
 URL Filter
 AV Scan
 ATD
 Safe Search
 YouTube for Schools

OK Cancel

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

Step 3. 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. web_log_01.png
2. web_log_streaming_access_rule.png

© Barracuda Networks Inc., 2019 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.