

Understanding Syslog Messages for the Barracuda Web Filter

Overview

This document describes each element of a syslog message so you can better analyze why your Barracuda Web Filter performs a particular action for each traffic request.

The Barracuda Web Filter uses syslog messages to log what happens to each traffic request performed by your users. The syslog messages are sent to a text file on the Barracuda Web Filter, as well as to a remote server specified by the Barracuda Web Filter administrator.

Enabling Syslog

To enable syslog reporting on your Barracuda Web Filter, go to the **Advanced > Syslog** page in the admin interface, and enter the IP address of the syslog server that you want to direct messages to. If you are running syslog on a UNIX machine, be sure to start the syslog daemon process with the “-r” option so that it can receive messages from sources other than itself. Windows users will have to install a separate program to use syslog because the Windows OS does not include syslog capabilities. Kiwi Syslog is a popular solution, but many others are available that are both free and commercial.

Syslog messages are sent to the standard syslog UDP port 514. If there are any firewalls between the Barracuda Web Filter and the server receiving the syslog messages, be sure that port 514 is open on the firewalls. The syslog messages arrive on the mail facility at the debug priority level. As the Barracuda Web Filter uses the syslog messages internally for its own message logging, it is not possible to change the facility or the priority level. For more information about where the syslog messages will be placed, refer to the documentation of your syslog server.

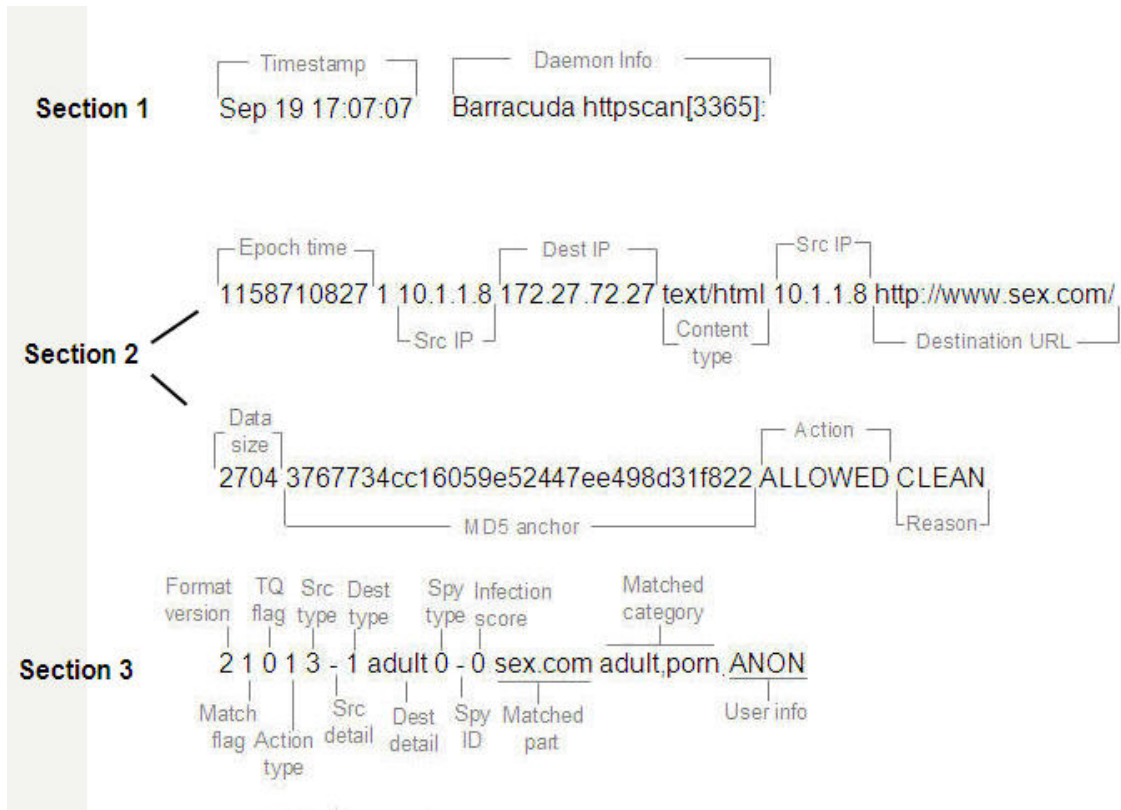
Syslog Format

Each syslog message contains three types of information:

- Section 1: Basic Information
- Section 2: Transparent Proxy Information
- Section 3: Policy Engine Information

This section identifies each element of the syslog using based on the following example:

```
Sep 19 17:07:07 Barracuda httpscan[3365]: 1158710827 1 10.1.1.8 172.27.72.27 text/html 10.1.1.8  
http://www.sex.com/ 2704 3767734cc16059e52447ee498d31f822 ALLOWED CLEAN 2 1 0 1 3 - 1 adult 0 - 0  
sex.com adult.porn ANON
```



Syslog Examples

This section shows three syslog examples.

Example 1. Clean, policy-allowed traffic

The following example shows a syslog message for clean traffic going to an allowed Web site (CNN.com). The term “clean” represents traffic that does not contain viruses or spyware.

```
Sep 19 17:06:59 Barracuda httpscan[3365]: 1158710819 1 10.1.1.8 64.236.16.139 image/gif 10.1.1.8
http://i.cnn.net/cnn/.element/img/1.3/video/tab.middle.on.gif 1744 3767734cc16059e52447ee498d31f822
ALLOWED CLEAN 2 0 0 0 0 - 0 - 0 - 0 cnn.net news ANON
```

Example 2: Clean, policy-denied traffic

The following example shows “clean” traffic going to a Web site that is blocked by one of the Barracuda Web Filter policies. In this example, the web site sex.com is blocked by the...

```
Sep 19 17:07:07 Barracuda httpscan[3365]: 1158710827 1 10.1.1.8 172.27.72.27 text/html 10.1.1.8
http://www.sex.com/ 2704 3767734cc16059e52447ee498d31f822 ALLOWED CLEAN 2 1 0 1 3 - 1 adult 0 - 0
sex.com adult,porn ANON
```

Example 3: Virus-infected traffic blocked by the Barracuda Web Filter

The following example shows traffic that has been blocked by the Barracuda Web Filter because the traffic contains a known virus.

```
Sep 19 17:08:00 Barracuda httpscan[3365]: 1158710880 1 10.1.1.8 127.0.0.1 - 10.1.1.8
http://www.eicar.org/download/eicar.com.txt 0 3767734cc16059e52447ee498d31f822 BLOCKED VIRUS
stream=>Eicar-Test-Signature FOUND 2 0 0 0 0 - 0 - 0 - 0 eicar.org computing-technology ANON
```

Detailed Description

The following table describe each element of a syslog message.

Field Name	Example	Description
Epoch Time	1158710827	Seconds since 1970, unix timestamp.
Src IP	10.1.1.8	IP address of the client.
Dest IP	172.27.72.27(72.32.54.242)	IP address for the page that was blocked by the Barracuda Web Filter.
Content Type	text/html	HTTP header designated content type.
Src IP	10.1.1.8	IP address of the client.
Destination URL	http://www.sex.com	The URL the client tried to visit.
Data Size	2704	The size of the content.
MD5 anchor	37...22	The anchor used for parsing. This information is not usually important.
Action	ALLOWED	Action performed by the transparent proxy. The type of actions include: <ul style="list-style-type: none">• ALLOWED: Traffic was processed by the transparent proxy and no virus or spyware was detected.• BLOCKED: Traffic was blocked by the transparent proxy most likely because the proxy detected virus or spyware.• DETECTED: Another process detected outbound spyware activity.
Reason	CLEAN	Reason for the action: <ul style="list-style-type: none">• CLEAN: Traffic does not contain any virus or spyware.• VIRUS: Traffic was blocked because it contains a virus.• SPYWARE: Traffic was blocked because it contained spyware.
Details (only for blocked traffic)	Stream=>Eicar-Test-Signature FOUND	The name of the virus or spyware that was detected in the blocked traffic.

Field Name	Example	Description
Format Ver	2	The version of the policy engine output. The most current 3.0 firmware uses policy engine version 2.
Match flag	1	Whether an existing policy matched the traffic. 1=Yes and 0=No.
TQ flag	0	Whether the rule is time-qualified. For Example, during work hours 9am - 5pm. 1=Yes and 0=No.
Action Type	1	The action performed by the policy engine on this request: 0 : allowed 1 : denied 2 : redirected 3 : rewrote by add/set a new parameter in query 4 : rewrote by delete an existing parameter in query 5 : matched a rule and allowed but marked as monitored 6 : branched to another rule set.
Src Type	3	If matched by source, what is its type: 0 : always, matches any source 1 : group, matched by group id 2 : ipv4addr, matched by an ipv4 address 3 : login, matched by login 4 : login any, matched any authenticated user 5 : min_score, matched due to minimum infection threshold breached.
Src Detail	-	Any detail related to the matched source.
Dst Type	1	If matched by destination, what is its type? 0 : always, matched any destination 1 : category, matched a particular category 2 : category any, matched any category 3 : domain, matched due to domain or subdomain 4 : mimetype, matched due to mime-type 5 : spyware hit, matched due to spyware hit 6 : uri path regex, matched URI path 7 : uri regex, matched any part of the URI 8 : application, matches an application characteristics
Dst Detail	adult	Detail of the matched destination. In this case it is the first matched category, which is adult.
Spy Type	0	If it is a spyware hit, what is its type: 0: allow 1: block 2: infection
Spy ID	-	The name of the spyware if matched due to spyware hit.
Infection Score	0	Weight of the infection. Currently, mostly 0.
Matched Part	sex.com	The part of the rule that matched.
Matched Category	adult,porn	The policy category that matched the traffic?

User Info	ANON	User information: <ul style="list-style-type: none">• ANON: Anonymous, unauthenticated users• ldap: Username: LDAP user info• username: Non-LDAP user info (users created create in the admin interface).
-----------	------	---