Syslog and the Barracuda Web Security Gateway

https://campus.barracuda.com/doc/6160435/

The Barracuda Web Security Gateway generates syslog messages as a means of logging both changes to the web interface configuration and what happens to each traffic request performed by your users. The syslog messages are stored in text file format on the Barracuda Web Security Gateway and can be sent to a remote server configurable by the administrator. There are two syslog outputs you can monitor: the *Web Interface* syslog and the *Web Traffic* syslog.

This article describes each element of a syslog message so you can better analyze why your Barracuda Web Security Gateway performs a particular action for each traffic request. If you are using wireless AP devices in your network, see also Accepted Syslog Formats From Wireless APs.

How to Enable Syslog

To enable syslog reporting on your Barracuda Web Security Gateway:

1. Log into the web interface as *admin* and navigate to the **Advanced > Syslog** page.
2. For both the Web Traffic Syslog and Web Interface Syslog, enter the IP address of the syslog server to which you want to direct messages.
3. 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 must 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.

How Syslog Messages are Delivered

Syslog messages are, by default, sent to the standard syslog UDP port 514. If there are any firewalls between the Barracuda Web Security Gateway 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 Security Gateway 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.

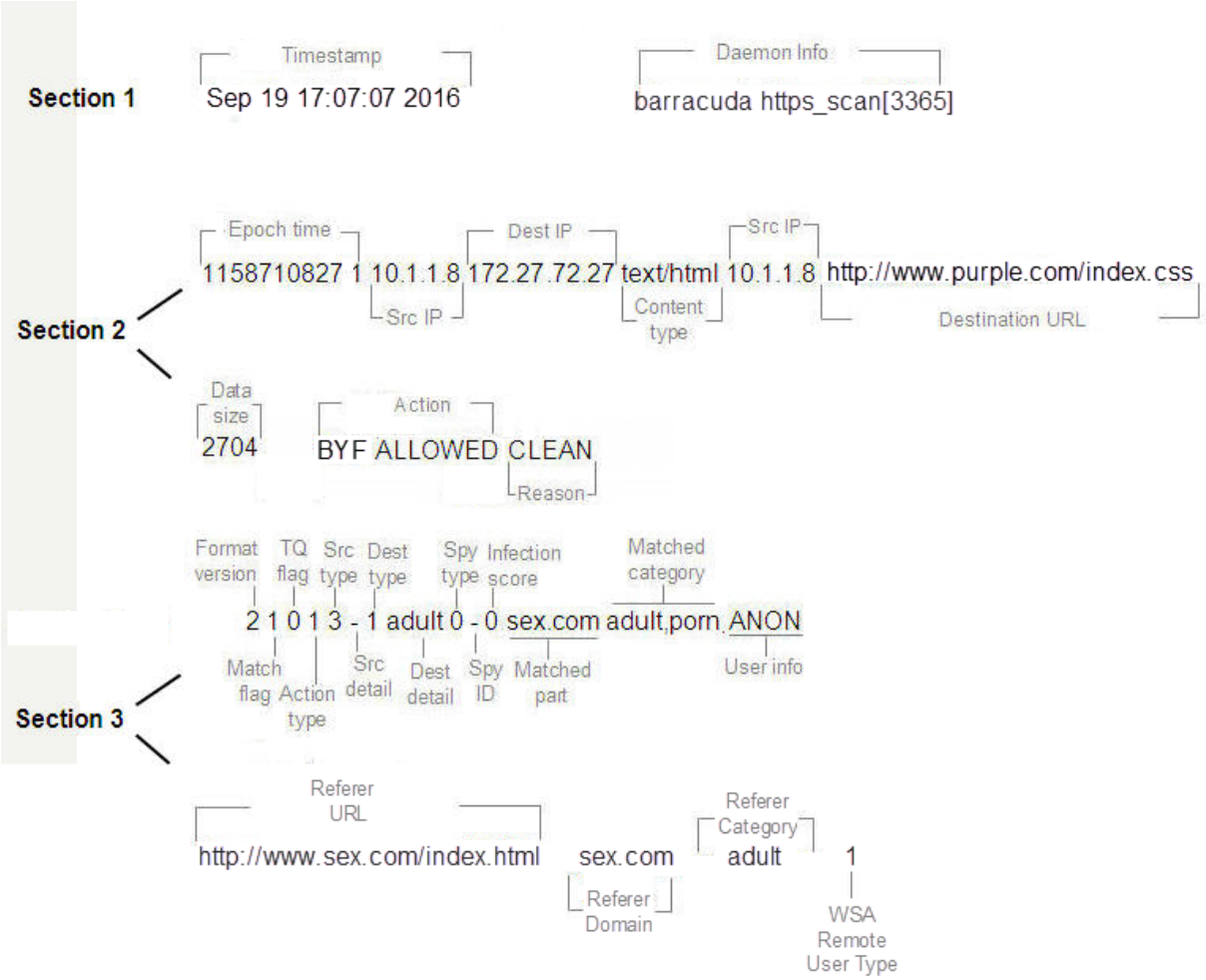
Barracuda Syslog Format

Each syslog message contains three types of information:

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

The graphic below identifies each element of the syslog based on the following example:

Sep 19 17:07:07 2016 barracuda https_can[3365]: 1158710827 1 10.1.1.8 172.27.72.27 text/html 10.1.1.8 http://www.purple.com/index.css 2704 BYF ALLOWED CLEAN 2 1 0 1 3 (-) 1 adult 0 - 0 sex.com adult,porn ANON http:.//www.sex.com/index.html sex.com adult 1



How to Parse the Syslog

The following table describes each element of a syslog message, as illustrated above.

Field Name	Example	Description
Epoch Time	1158710827	Seconds since 1970, UNIX timestamp.
Src IP	10.1.1.8	IP address of the client (source).
Dest IP	172.27.72.27(72.32.54.242)	IP address for the page (destination) that was blocked by the Barracuda Web Security Gateway.
Content Type	text/html	HTTP header designated content type.
Src IP	10.1.1.8	IP address of the (source).
Destination URL	http://www.sex.com	The URL the client tried to visit.
Data Size	2704	The size of the content.
Action	BYF ALLOWED	Action performed by the transparent proxy. "BYF" is a static string. The type of actions include: • 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: • CLEAN: Traffic does not contain any virus or spyware. • VIRUS: Traffic was blocked because it contains a virus. • SPYWARE: Traffic was blocked because it contains spyware.
Details (only for blocked traffic)	Stream=>Eicar-Test-Signature FOUND	If traffic was blocked, this field is populated with the name of the virus or spyware that was detected, and appended to the **Reason** field. If no virus or spyware was found, this field is not displayed.
Format Version	2	The version of the policy engine output.
Match flag	1	Indicates whether an existing policy matched the traffic. 1: Yes 0: No

TQ flag	0	Indicates whether the rule is time-qualified. For example, during work hours 9am - 5pm. 1: Yes 0: No
Action Type	1	The action performed by the policy engine on this request: 0 : allowed 1 : denied 2 : redirected 3 : rewritten by add/set a new parameter in query 4 : rewritten by deleting 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: • ANON: Anonymous, unauthenticated users • ldap: Username: LDAP user info • username: Non-LDAP user info (users created in the admin interface).
Referer URL	http://www.purple.com/purple.html	If enabled, displays URL of referer. If disabled, displays a dash '–' .
Referer Domain	purple.com http://www.cnn.com/ www.cnn.com	If enabled, displays domain of referer. If disabled, displays a dash '–' .
Referer Category	news, adult, hosted-personal-pages	If enabled, displays the category to which the referer domain belongs. If disabled, displays a dash '–'.
WSA Remote User Type	1	Indicates whether traffic comes from a Barracuda WSA client (Windows or Macintosh) or is local traffic. 0: local (inline) traffic 1: remote traffic from the Barracuda WSA

Syslog Examples

Example 1. Clean, policy-allowed traffic

The following example shows a syslog message for clean traffic from a Barracuda WSA client going to an allowed website (cnn.com). The term “clean” represents traffic that does not contain viruses or spyware.

Sep 19 17:06:59 2015 barracuda http_scan[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 BYF ALLOWED CLEAN 2 0 0 0 0 - 0 - 0 - 0 cnn.net news ANON http://www.cnn.com www.cnn.com news 1

Example 2: Virus-infected traffic blocked by the Barracuda Web Security Gateway

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

Sep 19 17:08:00 2016 barracuda http_scan[3365]: 1158710880 1 10.1.1.8 127.0.0.1 - 10.1.1.8 http://www.eicar.org/download/eicar.com.txt 0 BYF BLOCKED VIRUS stream=>Eicar-Test-Signature FOUND 2 0 0 0 0 - 0 - 0 - 0 eicar.org computing-technology ANON http://www.somedomain.com/index.html somedomain.com news 0

Example 3: Inline traffic showing simple content

Nov 28 20:13:35 2016 barracuda http_scan[30041]: 1480360415 1 10.1.2.200 52.37.201.150 - 10.1.2.200 https://self-repair.mozilla.org/ 7652 BYF ALLOWED CLEAN 2 0 0 0 0 (-) 0 - 0 - 0 self-repair.mozilla.org computing-technology,CUSTOM-142556317732606,CUSTOM-1425889735316,CUSTOM-1425890081323,CUSTOM-1425890385330,CUSTOM-1425890704337,CUSTOM-1425890996342 [hspecter@pearson-spectar.com] https://self-repair.mozilla.org - - 0

Sending System Logs to an External Syslog Server in W3C Format

If you are running the Barracuda Web Security Gateway version 11.0 or higher, you can send system logs to your external syslog server in W3C extended log file format. Configure on the **ADVANCED > Syslog** page.

Figures