



Barracuda Syslog

Barracuda Web Application Firewall

Overview

There are four types of logs generated by the Barracuda Web Application Firewall which can be configured to be sent over the syslog mechanism to remote servers specified by the Barracuda Web Application Firewall administrator. These logs are also resident on the Barracuda Web Application Firewall in a log database and are visible on the GUI under various tabs and can be exported in CSV format to external files. This document describes each element of such syslog messages to help the administrator analyze the events and understand the activity performed by the Barracuda Web Application Firewall for each traffic request. The document also helps in understanding the formats so that the information can be utilized in a better way through external parsers or other agents which can be run on the syslog messages sent from the Barracuda Web Application Firewall starting with version 7.0.x of the firmware.

The following four types of logs are explained briefly below. These logs can be logged at LOCAL 0 to LOCAL 7 facility to help manage them well on the external syslog servers that they get transferred to.

System Events: These are the events generated by the system and show the general activity of the system.

Web Firewall Logs: These are the events which indicate the web firewall activity in terms of allowing, blocking or modifying the incoming requests and responses as defined in the Barracuda Web Application Firewall rules and policies.

Access Logs: These events pertain to the traffic activity and log various elements of the incoming HTTP request and the responses from the backend servers.

Audit Logs: These events pertain to the auditing events generated by the system which log the configuration and UI activity by users like admin.

If you have any questions after reading this document, please call us at 408-342-5400 or email us at support@barracuda.com.

Enabling Syslog

To enable exporting of logs to remote syslog servers, navigate to the **ADVANCED > Export Logs** page. Remote syslog servers for system events is specified under **Syslog** in the web GUI. Enter the name and IP addresses of up to 3 syslog servers to which you wish to direct the System Events, Web Firewall logs, Access logs, and Audit logs. 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 have to install a separate program to utilize the syslog since the Windows OS does not include the syslog capability. Kiwi Syslog is a popular solution, but there are many others to choose from, both free and commercial.

The syslog messages are sent over UDP to the standard syslog port of 514. If there are any firewalls between the Barracuda Web Application Firewall and the servers receiving the syslog messages, then be sure that port 514 is open on the firewalls.



Barracuda Syslog

Barracuda Web Application Firewall

Syslog Facility

As the syslogd receives different types of log messages from various hosts, it is important to differentiate and store them in unique log files according to their log type. Classification of these log messages is based on the logging priority and the logging facility found in each log messages. A log message contains a logging facility and a priority, in addition to the actual messages and the IP address. The **facility** denotes the device that sent the particular type of message, individualizing it from other hosts using the same syslog server.

You mark all the log messages with one of the following facilities:

local0
local1
local2
local3
local4
local5
local6
local7

Setting a different facility (default = local0) for each log type allows the syslog server to segregate the logs into different files. The Barracuda Web Application Firewall has the configuration options to group the log messages. This configuration involves assigning a syslog facility to different types of log messages.

To configure facilities for different log types

1. Navigate to the **ADVANCED > Export Logs** page.
2. In the **Syslog** section, click **Syslog Settings**. The Syslog Settings dialog box appears.
3. Select the appropriate facility (Local0 to Local7) from the drop-down list for each log type and click **Save Changes**.

Note: You can also set the same facility for all the log types. For example, you can set Local0 for System Logs, Web Firewall Logs, Access Logs, and Audit Logs.

To configure log levels for different modules

1. Navigate to the **ADVANCED > Export Logs** page.
2. In the **Module Log Levels** section, specify values for the following fields:
 - a) **Name** - Enter a name for the new setting.
 - b) **Module** - Select a module name from the drop-down list.
 - c) **Log Level** - Select a log level from the drop-down list.
 - d) **Comment** - Enter comment about the new setting.
3. Select the appropriate option from the drop-down list for each log type and click **Save Changes**.



Barracuda Syslog

Barracuda Web Application Firewall

Custom Log Formats

The format of the Web Firewall Logs, Access Logs, and Audit Logs to be sent to the syslog sever can be customized. You can choose between the Common Log Format, NCSA Extended Format, W3C Extended Format, Default or the Custom Format. The Common Log Format, NCSA Extended Format, W3C Extended Format, and the Default formats are already defined and cannot be edited. Given below are the steps to specify the Custom Format.

To customize the log format for any Log Type (except System Logs)

1. Navigate to **ADVANCED > Export Logs** page.
2. On the **Logs Format** section, select **Custom Format** for any of the log types. The Custom Format can be defined in two ways:

Specify "%" followed by the alphabet. The alphabets and its meaning are given in the [Table of Log Formats](#) for different log types. For example, if you configure "%h %u %t %r %ua %ci" as the custom format, the output will be "Jan 13 16:19:22 wsf 192.168.132.211 /cgi-bin/process.cgi 2010-01-13 05:49:22.350 -0500 "-" "Wget/1.10.2 (Red Hat modified)" 192.168.128.7".

OR

Specify "name=value" format. For example, if you configure "host=%h url=%u time=%t ref=%r uagent=%ua src=%ci" as the custom format, the output will be "Jan 13 16:19:22 wsf host=192.168.132.211 url=/cgi-bin/process.cgi time=2010-01-13 05:49:22.350 -0500 ref="-" uagent="Wget/1.10.2 (Red Hat modified)" src=192.168.128.7". This format is used by some SEIM vendors such as ArchSight.

3. Click **Save Changes** to save the settings.

For information on how to manage these logs please see the documentation available for your syslog server.

The following sections describe the formats of the logs and elements sent over in each type of the event generated by the Barracuda Web Application Firewall. Please be aware that the various syslog implementations may not display the messages in this exact format. However, the sections should still be present in the syslog lines.

System Events

The default log format for the events generated by the Barracuda Web Application Firewall system is as follows:

```
%t %md %ll %ei %ms
```

Note:

- You cannot customize the format of System Logs.
- Refer [Table of Log Formats](#) for the meanings of the alphabets.



Barracuda Syslog Barracuda Web Application Firewall

Example:

Feb 3 15:09:02 wsf STM: LB 5 00141 LookupServerCtx = 0xab0bb600

Detailed Description

The following table describes each element of a system log with respect to the above example:

Field Name	Example	Description
Time Stamp	Feb 3 15:09:02 wsf STM:	The date and time at which the event occurred.
Module Name	LB	Denotes the name of the module that generated the logs. For example: STM, SAPD, LB, etc.
Log Level	5	The log level number. Values: 0-Emergency – System is unusable (highest priority). 1-Alert – Response must be taken immediately. 2-Critical – Critical conditions. 3-Error – Error conditions. 4-Warning – Warning conditions. 5-Notice – Normal but significant condition. 6-Information – Informational message (on ACL configuration changes). 7-Debug – Debug-level message (lowest priority).
Event ID	000141	The event ID of the module.
Message	LookupServerCtx = 0xab0bb600	Denotes the log message for the event that occurred.

Web Firewall Logs

All the actions/events on the web firewall are logged under **Web Firewall Logs**. These logs help the administrator to analyze the traffic for suspicious activity and also fine tune the web firewall policies.

Navigate to the **BASIC > Web Firewall Logs** page to view the generated log messages. This log data is obtained from the log database on the Barracuda Web Application Firewall itself. As noted above, the external syslog server IP for these logs is specified under **ADVANCED > Export Logs > Syslog**. Over syslog, every log in the Barracuda Web Application Firewall has a level associated with



Barracuda Syslog Barracuda Web Application Firewall

it, which indicates the severity of the logs. An administrator can configure what level of logs should be recorded for each service by editing the service under the **BASIC > Services** page.

The default log format for Web Firewall Logs is as follows:

```
%t %un %lt %sl %ad %ci %cp %ai %ap %ri %rt %at %fa %adl %m %u %p %sid %ua %px
%pp %au %r %aid %ag
```

Note:

1. Refer [Table of Log Formats](#) for the meanings of the alphabets.
2. Unit Name, Log Type, and Log ID are not displayed on the **BASIC > Web Firewall Logs** page.

Example:

```
2010-02-03 01:49:09.077 -0800 wafbox1 WF ALER
SQL_INJECTION_IN_PARAM 192.168.128.7 39661 192.168.132.21180 webapp1:deny_ban_dir
GLOBAL LOG NONE "[type=""sql-injection-medium"" pattern=""sql-quote"" token="" or ""
Parameter=""address"" value=""hi' or 1=1--""]" POST
192.168.132.211/cgi-bin/process.cgi HTTP REQ-0+RES-0 "Mozilla/5.0 (X11; U; Linux i686
(x86_64); en-US; rv:1.8.1.20) Gecko/20081217 Firefox/2.0.0.20" 192.168.128.7
39661 Kevin http://192.168.132.211/cgi-bin/1.pl 11956 ATTACK_CATEGORY_INJECTION
```

Detailed Description

The following table describes each element of a web firewall log with respect to the above example:

Field Name	Example	Description
Time Stamp	2010-02-03 01:49:09.077 -0800	The time recorded in the following format: yyyy-mm-dd hh:mm:ss.s (one or more digits representing a decimal fraction of a second)TZD(time zone designator which is either Z or +hh:mm or -hh:mm)
Unit Name	wafbox1	Specifies the name of the unit which is same as the Default Hostname on the BASIC > IP Configuration page.
Log Type	WF	Specifies whether it is of type Web Firewall Log, Access Log, or Audit Log. Values: TR, WF, AUDIT



Barracuda Syslog Barracuda Web Application Firewall

Field Name	Example	Description
Severity Level	ALER	<p>Defines the seriousness of the attack.</p> <p>Values:</p> <p>Emergency - System is unusable (highest priority). Alert - Response must be taken immediately. Critical - Critical conditions. Error - Error conditions. Warning - Warning conditions Notice - Normal but significant condition. Information - Informational message (on ACL configuration changes). Debug – Debug-level message (lowest priority).</p>
Attack Description	SQL_INJECTION_IN_PARAM	The name of the attack triggered by the request.
Client IP	192.168.128.7	<p>The IP address of the client sending the request.</p> <p>Note that an intermediate proxy or gateway may have overwritten the actual source IP of the client with its own. To retrieve the actual client IP for logging you should configure the Header Name For Actual Client IP under the Edit actions for a service on the BASIC > Services page.</p> <p>If the above is configured, the actual client IP is extracted from the header, e.g. X-Forwarded-For and used to populate this field and used in security policy checks involving the client IP as well. See related Proxy IP field below as well.</p>
Client Port	39661	The port relevant to the client IP address.
Application IP	192.168.132.211	The IP address of the application that receives the traffic.
Application Port	80	The port relevant to the IP address of the application.
Rule ID	webapp1:deny_ban_dir	The path of the URL ACL that matched with the request. Here "webapp1" is the web application and "deny_ban_dir" is the name of the URL ACL created on the WEBSITES > Allow/Deny page.



Barracuda Syslog

Barracuda Web Application Firewall

Field Name	Example	Description
Rule Type	GLOBAL	<p>This indicates the type of rule that was hit by the request that caused the attack. The following is the list of expected values for Rule Type:</p> <p>Global - indicates that the request matched one of the global rules configured under Security Policies.</p> <p>Global URL ACL - indicates that the request matched one of the global URL ACL rules configured under Security Policies.</p> <p>URL ACL - indicates that the request matched one of the Allow/Deny rules configured specifically for the given Web site.</p> <p>URL Policy - indicates that the request matched one of the Advanced Security rules configured specifically for the given Web site.</p> <p>URL Profile - indicates that the request matched one of the rules configured on the URL Profile.</p> <p>Parameter Profile - indicates that the request matched one of the rules configured on the Parameter Profile.</p> <p>Header Profile - indicates that the request matched one of the rules configured on the Header Profile.</p>
Action Taken	LOG	<p>The appropriate action applied on the traffic.</p> <p>DENY denotes that the traffic is denied.</p> <p>LOG denotes monitoring of the traffic with the assigned rule.</p> <p>WARNING warns about the traffic.</p>
Follow-up Action	NONE	<p>The follow-up action as specified by the action policy. It could be either None or Locked in case the lockout is chosen.</p>
Attack Details	[type=""sql-injection-medium"" pattern=""sql-quote"" token="" or "" Parameter=""address"" value=""hi' or 1=1--""]	<p>The details of the attack triggered by the request.</p>



Barracuda Syslog

Barracuda Web Application Firewall

Field Name	Example	Description
Method	POST	The HTTP method used by the request. Values: GET, POST, HEAD, etc.
URL	192.168.132.211/cgi-bin/process.cgi	The URL specified in the request.
Protocol	HTTP	The protocol used for the request.
Session ID	REQ-0+RES-0	The value of the session tokens found in the request if session tracking is enabled. Session Tracking is configured on the WEBSITES > Advanced Security page.
User Agent	Mozilla/5.0 (X11; U; Linux i686 (x86_64); en-US; rv:1.8.1.20) Gecko/20081217 Firefox/2.0.0.20	The value contained in the User-Agent request header. Normally, this information is submitted by the clients which details the browser, operating system, software vendor or software revision, in an identification string.
Proxy IP	192.168.128.7	<p>If the client requests are coming through a proxy or gateway, then this field provides the IP address of the proxy.</p> <p>A client side proxy or gateway changes the source IP of the request to its own and embeds the actual client's IP in an HTTP header such as X-Forwarded-For or X-Client-IP.</p> <p>The Barracuda Web Application Firewall, if configured, will ignore the proxy IP and extract the actual client IP from the appropriate header to apply security policies as well as for logging the Client IP field above.</p> <p>This field preserves the proxy IP address for cases where it is required, e.g. forensics and analytics</p> <p>Note: The actual client IP header configuration is done using the Header Name For Actual Client IP under the Edit actions for a service on the BASIC > Services page.</p>
Proxy Port	39661	The port of the proxy server whose IP address has been logged in the Proxy IP field above.



Barracuda Syslog Barracuda Web Application Firewall

Field Name	Example	Description
Authenticated User	Kevin	The username of the currently authenticated client requesting the web page. This is available only when the request is for a service that is using the AAA (User Access Control) module.
Referrer	http://192.168.132.211/cgi-bin/1.pl	The value contained in the Referrer HTTP request header. It identifies the Web resource from which the client was "referred" to the requested URL.
Attack ID	11956	Denotes an internally stored attack identification number.
Attack Group	ATTACK_CATEGORY_INJECTION	The attack group under which some of the attacks are defined.

Attack Names

The following is the list of Attack Names arranged as per Attack Groups:

Event ID	Attack Name	Description	Severity	Attack Type
Advanced Policy Violations				
29012	INVALID_URL_CHARSET	The request contained the character that is not valid in the character set. To determine the character set of the request, the Barracuda Web Application Firewall relies on several configuration elements like Default Character Set, Detect Response Charset and Response Charset.	Warning	Attack obfuscation
29145	BRUTE_FORCE_FORCE_IP	The number of accesses to the resource by the client IP exceeded the number defined in the bruteforce prevention policy for this application.	Alert	DOS attack
29146	BRUTE_FORCE_FORCE_ALL_SOURCES	The cumulative number of accesses to the resource by all the sources exceeded the number defined in the bruteforce prevention policy for this application.	Alert	DOS attack



Barracuda Syslog Barracuda Web Application Firewall

Event ID	Attack Name	Description	Severity	Attack Type
Application Profile Violations				
29130	NO_DOMAIN_MATCH_IN_PROFILE	The request sent by the browser corresponds to a domain which is not found in the application profile.	Alert	Forceful browsing
29131	NO_URL_PROFILE_MATCH	The request sent by the browser contained an URL for which, a matching URL Profile is not found in the application profile.	Alert	Forceful browsing
Header Violations				
29007	HEADER_META_VIOLATION	The header contained a metacharacter which is part of the Denied Metacharacters configured in the Header ACL for this application.	Alert	Command injection
29035	CUSTOM_ATTACK_PATTERN_IN_HEADER	The header contained an attack pattern that matched an attack pattern configured as a part of Custom Blocked Attack Types for this header in the Header ACL.	Alert	Command injection
29036	SQL_INJECTION_IN_HEADERSQL	The header contained SQL injection attack which matched an attack pattern configured as a Blocked Attack Types for this header in the Header ACL.	Alert	SQL injection
29037	CROSS_SITE_SCRIPTING_IN_HEADER	The header contained cross-site scripting attack which matched an attack pattern configured as a Blocked Attack Types for this header in the Header ACL.	Alert	Cross-site scripting
29038	OS_CMD_INJECTION_IN_PARAM	The header contained OS command injection attack which matched an attack pattern configured as a Blocked Attack Types for this header in the Header ACL.	Alert	Command injection
29039	DIRECTORY_TRAVERSAL_IN_HEADER	The header contained directory traversal attack which matched an attack pattern configured as a Blocked Attack Types for this header in the Header ACL.	Alert	Directory traversal



Barracuda Syslog Barracuda Web Application Firewall

Event ID	Attack Name	Description	Severity	Attack Type
Param Profile Violations				
29134	READ_ONLY_PARAM_TAMPERED	The read-only parameter had a value, which was different from what was learned by Barracuda Web Application Firewall based on the form that was sent to the browser.	Alert	Form tampering
29135	SESSION_INVARIANT_PARAM_TAMPERED	The session-invariant parameter had a value, which was different from what was learned by Barracuda Web Application Firewall based on the form that was sent to the browser for this session.	Alert	Form tampering
29136	SESSION_CHOICE_PARAM_TAMPERED	The session choice parameter had a value, which was different from what was learned by Barracuda Web Application Firewall based on the form that was sent to the browser for this session.	Alert	Form tampering
29137	TOO_MANY_PARAM_INSTANCES	The URL sent by the browser contained more instances of the parameter than what is learned to be allowed in the Parameter Profile.	Alert	Form tampering
29138	MISSING_MANDATORY_PARAM	The URL sent by the browser contained no instances of the parameter, which is learned to be mandatory in the Parameter Profile.	Alert	Form tampering
29139	PARAM_VAL_NOT_ALLOWED	The Global Choice parameter had a value, which is different from the values configured for this parameter in the Parameter Profile.	Alert	Form tampering
29150	FILE_EXTENSION_NOT_ALLOWED	The extension of the filename of a file-upload parameter does not match any one of the configured File Upload Extensions for the parameter profile.	Alert	Form tampering
29151	FILE_UPLOAD_SIZE_EXCEEDED	The size of the file-upload parameter is greater than the maximum configured value in the Default Parameter Protection.	Alert	Form tampering
29152	METACHARACTER_IN_PARAMETER	The parameter contained a metacharacter, which matched an attack pattern configured as a Parameter Class in the parameter profile.	Alert	Command injection



Barracuda Syslog Barracuda Web Application Firewall

Event ID	Attack Name	Description	Severity	Attack Type
29154	PARAM_NAME_LENGTH_EXCEEDED	The length of the parameter exceeded the Max Length configured in the parameter profile.	Alert	Buffer overflow
29155	CUSTOM_ATTACK_PATTERN_IN_PARAMETER	The parameter contained custom attack pattern, which matched an attack pattern configured as a Parameter Class in the parameter profile.	Alert	Command injection
29156	PARAM_INPUT_VALIDATION_FAILED	The parameter does not match the input type validation configured in the Parameter Profile.	Alert	Form tampering
29157	SQL_INJECTION_IN_PARAMETER	The parameter contained SQL injection pattern, which matched an attack pattern configured as a Parameter Class in the parameter profile.	Alert	SQL injection
29158	CROSS_SITE_SCRIPTING_IN_PARAMETER	The parameter contained cross-site scripting pattern, which matched an attack pattern configured as a Parameter Class in the parameter profile.	Alert	Cross-site scripting
29159	OS_CMD_INJECTION_IN_HEADER	The parameter contained OS command injection pattern, which matched an attack pattern configured as a Parameter Class in the parameter profile.	Alert	Command injection
29160	DIRECTORY_TRAVERSAL_IN_PARAMETER	The parameter contained directory traversal pattern which matched an attack pattern configured as a Parameter Class in the parameter profile.	Alert	Directory traversal
29162	SESSION_CONTEXT_NOT_FOUND	The session parameter (parameter type=read-only, session-choice or session-invariant) value does not match with the learned value in the parameter profile. This is a possible tampering of the session parameter value.	Alert	Form tampering
29164	REMOTE_FILE_INCLUSION_IN_URL	The parameter contained remote file inclusion pattern which matched an attack pattern configured as a Parameter Class in the parameter profile.	Alert	Malicious-File-Execution



Barracuda Syslog Barracuda Web Application Firewall

Event ID	Attack Name	Description	Severity	Attack Type
29165	CROSS_SITE_REQUEST_FORGERY	The Barracuda Web Application Firewall inserted state parameter 'ncforminfo', is either not found or found tampered in the form that matched the URL profile.	Alert	Forceful browsing
Protocol Violations				
29016	DIRECTORY_TRAVERSAL_BEYOND_ROOT	The request attempted to traverse the directory using multiple ../ or ..\ elements, resulting in a directory beyond the document root, and this is disallowed by the Barracuda Web Application Firewall.	Alert	Directory traversal
29025	POST_WITHOUT_CONTENT_LENGTH	The POST request does not have a 'Content-Length' header. The Content-Length header must be present for the POST to be processed correctly.	Alert	Protocol exploit
29060	PRE_1_0_REQUEST	The request sent by the browser did not contain the HTTP Version string.	Alert	Protocol exploit
29077	INVALID_OR_MALFORMED_REQUEST	The request sent by the browser is either not conforming to the HTTP RFC or is malformed or disallowed by Barracuda Web Application Firewall for violating basic HTTP conformance checks.	Alert	Protocol exploit
29118	METHOD_NOT_ALLOWED	The request sent by the browser contained a method which is not conforming to the HTTP RFC.	Alert	Protocol exploit
29119	MALFORMED_VERSION	The request sent by the browser contained a HTTP version which is not conforming to the HTTP RFC.	Alert	Protocol exploit
29120	MALFORMED_REQUEST_LINE	The request sent by the browser contained a request line with no CRLF termination.	Alert	Protocol exploit
29121	MALFORMED_HEADER_LINE	The request sent by the browser contained a header field which is not conforming to the HTTP RFC.	Alert	Protocol exploit
29122	INVALID_HEADER	The request sent by the browser contained a header field with no CRLF termination.	Alert	Protocol exploit



Barracuda Syslog Barracuda Web Application Firewall

Event ID	Attack Name	Description	Severity	Attack Type
29123	MALFORMED_CONTENT_LEN	The request sent by the browser contained a content length header with a non numeric value.	Alert	Protocol exploit
29124	MALFORMED_COOKIE	The request sent by the browser contained a cookie whose name value attributes were not conforming to HTTP RFC.	Alert	Protocol exploit
29125	GET_REQUEST_WITH_CONTENT_LENGTH	The request sent by the browser was a GET method but had a content length header which may indicate a HTTP request smuggling attack attempt.	Alert	Protocol exploit
29126	MISSING_HOST_HEADER	The request sent by the browser was a HTTP/1.1 request but there was no host header which is necessary for HTTP/1.1 requests.	Alert	Protocol exploit
29127	MULTIPLE_CONTENT_LENGTH	The request sent by the browser contained multiple content length headers which may indicate a HTTP request smuggling attempt.	Alert	Protocol exploit
29128	MALFORMED_PARAMETER	The syntax of the request parameters does not comply with the content type for them or the normalization of the parameters failed.	Alert	Protocol exploit
29129	PARAM_TOO_LARGE	The value of the parameter is larger than the internal maximum limit of 1 MB.	Alert	Protocol exploit
Request Policy Violations				
29000	REQUEST_LINE_LENGTH_EXCEEDED	The HTTP request length exceeded the Max Request Length configured in the Web Firewall Policy.	Alert	Buffer overflow
29006	HEADER_VALUE_LENGTH_EXCEEDED	The length of the header-value of header exceeded the "Max Header Length" configured.	Alert	Buffer overflow
29011	INVALID_URL_ENCODING	The request contained the string, which is an invalid URL encoded sequence. A valid URL encoded sequence is a % followed by two hexadecimal digits, that is, 0-9, a-f, A-F.	Alert	Attack obfuscation



Barracuda Syslog Barracuda Web Application Firewall

Event ID	Attack Name	Description	Severity	Attack Type
29014	SLASH_DOT_IN_URL	The request URL contains a forward-slash (/) or a backward-slash (\) followed by a dot (.) and is disallowed by the Barracuda Web Application Firewall. A URL with a \. OR /. may be an attempt to view hidden files.	Alert	Directory Traversal
29015	TILDE_IN_URL	The URL in the request contained a tilde (~) character, and is disallowed by the Barracuda Web Application Firewall. The tilde usually depicts user's home directories, and allowing tilde can give access even to files owned by root.	Alert	Directory Traversal
29030	UNRECOGNIZED_COOKIE	The cookie present in the request could not be decrypted by the Barracuda Web Application Firewall.	Warning	Cookie poisoning
29031	COOKIE_TAMPERED	The verification of the signature of the cookie in the request has failed.	Warning	Cookie poisoning
29032	COOKIE_EXPIRED	The browser returned a stale cookie.	Warning	Cookie poisoning
29041	COOKIE_LENGTH_EXCEEDED	The length of the cookie exceeded the Max Cookie Length configured in the Web Firewall Policy.	Alert	Buffer overflow
29042	URL_LENGTH_EXCEEDED	The URL length exceeded the Max URL Length configured in the Web Firewall Policy.	Alert	Buffer overflow
29043	QUERY_LENGTH_EXCEEDED URL	The length of query string exceeded the Max Query Length configured in the Web Firewall Policy.	Alert	Buffer overflow
29044	HEADER_COUNT_EXCEEDED	The number of headers received exceeded the "Max Number of Headers" configured in Request Limits. The number of headers includes any Cookie headers.	Alert	Buffer overflow
29116	COOKIE_REPLAY_MISMATCHED_HEADER		Warning	Cookie poisoning



Barracuda Syslog Barracuda Web Application Firewall

Event ID	Attack Name	Description	Severity	Attack Type
29117	COOKIE_REPLAY_MISMATCHED_IP		Warning	Cookie poisoning
29140	REQUEST_LENGTH_EXCEEDED	The length of request line, including Method, URI and Protocol exceeds the maximum configured limit in the Web Firewall Policy.	Alert	Buffer overflow
29141	COOKIE_COUNT_EXCEEDED	The number of cookies exceeded the "Max Number of Cookies" configured in the Web Firewall Policy.	Alert	Buffer overflow
29142	COOKIE_NAME_LENGTH_EXCEEDED	The length of the cookie name exceeded the Max Cookie Name Length configured in the Web Firewall Policy.	Alert	Buffer overflow
29143	HEADER_NAME_LENGTH_EXCEEDED	The length of the header-name of header exceeded the "Max Header Name Length" configured.	Alert	Buffer overflow
29144	TOO_MANY_SESSIONS_FOR_IP	The number of new sessions being given out to the Client IP in an interval exceeds the number defined for this Web application.	Alert	DOS attack
Response Violations				
29017	ERROR_RESPONSE_SUPPRESSED	The response page contains the HTTP error status code, which is suppressed by the configuration in Web site Cloaking. The request is not denied.	Notice	Error message interception
29061	RESPONSE_HEADER_SUPPRESSED	The response page contained the header, which is configured to be suppressed in Web site Cloaking. The Server header exposes the OS and/or server version, and known vulnerabilities can be exploited by an attacker based on this knowledge. The request is not denied, so it is safe to suppress any header. Note: It is recommended not to create an exception, if the header is "Server". Create the exception only if the browser or other User Agents require this header to be present for normal behavior.	Information	Error message interception



Barracuda Syslog Barracuda Web Application Firewall

Event ID	Attack Name	Description	Severity	Attack Type
29063	IDENTITY_THEFT_PATTERN_MATCHED	The response contained identity theft pattern, which matched an attack pattern configured as a "Data Theft Element" and the "Data Theft Protection" status in the URL Policy is "On".	Error	Authentication Hijacking
URL Profile Violations				
29005	INVALID_METHOD	The request sent by the browser contained a method which is not allowed by the Barracuda Web Application Firewall.	Alert	Application platform exploit
29026	UNKNOWN_CONTENT_TYPE	The Content-Type of the POST request was not recognized by the Barracuda Web Application Firewall.	Alert	Attack obfuscation
29040	CONTENT_LENGTH_EXCEEDED	The length of the content (typically the body of POST or PUT methods), exceeded the "Max Content Length" configured.	Alert	Buffer overflow
29132	QUERY_STRING_NOT_ALLOWED	The request sent by the browser contained a query string, even though query strings have been disallowed by the URL Profile.	Alert	Forceful browsing
29147	PARAM_LENGTH_EXCEEDED	The name of the parameter is longer than the max name length allowed.	Alert	Form tampering
29148	TOO_MANY_UPLOAD_FILES	The number of parameters of type "file-upload" sent by the browser exceeds the maximum configured limit for the parameter profile.	Alert	Form tampering
29149	TOO_MANY_PARAMETERS	The number of parameters in the request exceeds the limit of parameters allowed by the default URL protection.	Alert	Form tampering
29161	SESSION_COOKIE_NOT_FOUND	Either the Barracuda Web Application Firewall inserted session cookie is not in the request header or the Barracuda Web Application Firewall inserted hidden parameter is missing.	Alert	Forceful browsing
29163	NO_PARAMETER_PROFILE_MATCH	The request sent by the browser contained a parameter, which is not found in the application profile.	Alert	Forceful browsing



Barracuda Syslog

Barracuda Web Application Firewall

Event ID	Attack Name	Description	Severity	Attack Type
XML Violations				
29082	SOAP_REQUEST_VALIDATION_FAILED	The client sent a SOAP request which was invalid. The request was validated against the WSDL applicable to the logged URL.	Alert	Application platform exploit
29083	SOAP_RESPONSE_VALIDATION_FAILED	The back-end server sent a SOAP response which was invalid. The request was validated against the WSDL applicable to the logged URL.	Error	Application platform exploit
Access Violations				
29078	ACCESS_CONTROL_COOKIE_EXPIRED	The cookie identifying the user has expired due to idle time. The default idle time is 15 minutes, after which, a user login is invalidated. The user must login again to continue accessing the Web site.	Warning	Forceful browsing
29079	ACCESS_CONTROL_COOKIE_INVALID	The authentication cookie submitted by the user agent is invalid.	Warning	Forceful browsing
29080	ACCESS_CONTROL_ACCESS_DENIED	The requested URL is protected by Access Control, and the logged in user is not part of the Allowed Groups or Allowed Users who are authorized to access this URL.	Warning	Forceful browsing
29081	ACCESS_CONTROL_NO_COOKIE	The requested URL is protected by Access Control, and there is no cookie identifying the user. The cookie is generated only on a login, and the user has not logged in.	Warning	Forceful browsing
ACL Violations				
29001	DENY_ACL_MATCHED	The value of "Action" is configured to "Deny" for the URL in the ADR.	Alert	Forceful browsing
29056	REDIRECT_ACL_MATCHED	The request is redirected because it matched the ADR with a "Redirect" in the "Action" parameter.	Information	Information



Barracuda Syslog Barracuda Web Application Firewall

Access Logs

All Web traffic activities are logged under the Access Logs. These logs help the administrator to obtain information about the Web site traffic and performance.

The **BASIC > Access Logs** page allows you to view the generated log messages stored on the Barracuda Web Application Firewall in a log database.

The default log format for Access Logs is as follows:

```
%t %un %lt %ai %ap %ci %cp %id %cu %m %p %h %v %s %bs %br %ch %tt %si %sp %st
%sid %rtf %pmf %pf %wmf %u %q %r %c %ua %px %pp %au %cs1 %cs2 %cs3
```

Note:

- Refer [Table of Log Formats](#) for the meanings of the alphabets.
- Unit Name, Log Type, and Log ID are not displayed on the **BASIC > Access Logs** page.

Example:

```
2010-02-02 21:16:59.914 -0800 wafbox1 TR 192.168.132.211 80 192.168.128.7 37754 "-" "-" POST
HTTP 192.168.132.211 HTTP/1.1 200812 6401 0 230 192.168.128.7 80 0 SERVER DEFAULT
PASSIVE VALID /cgi-bin/process.cgi "-" http://192.168.132.211/cgi-bin/1.pl ys-grid_firewall_log-
grid=o%3Acolumns%3Da%253Ao%25253Aid%25253Ds%2525253Aiso_timestamp%25255Ewidth%
25253Dn%2525253A38%255Eo%252 "Mozilla/5.0 (X11; U; Linux i686 (x86_64);en-US; rv:1.8.1.20)
Gecko/20081217 Firefox/2.0.0.20" 192.168.128.7 37754 John en-us,or;q=0.5 gzip,deflate ISO-8859-
15,utf-8;q=0.7,*;q=0.7
```

Detailed Description

The following table describes each element of an access log with respect to the above example:

Field Name	Example	Description
Time Stamp	2010-02-02 21:16:59.914 -0800	The time recorded in the following format: yyyy-mm-dd hh:mm:ss.s (one or more digits representing a decimal fraction of a second)TZD(time zone designator which is either Z or +hh:mm or -hh:mm)
Unit Name	wafbox1	Specifies the name of the unit which is same as the Default Hostname on the BASIC > IP Configuration page.
Log Type	TR	Specifies whether it is of type Web Firewall Log, Access Log, or Audit Log. Values: TR, WF, AUDIT



Barracuda Syslog Barracuda Web Application Firewall

Field Name	Example	Description
Application IP	192.168.132.211	The IP address of the application that receives the traffic.
Application Port	80	The port relevant to the IP address of the application.
Client IP	192.168.128.7	<p>The IP address of the client sending the request.</p> <p>Note that an intermediate proxy or gateway may have overwritten the actual source IP of the client with it's own. To retrieve the actual client IP for logging you should configure the Header Name For Actual Client IP under the Edit actions for a service on the BASIC > Services page.</p> <p>If the above is configured, the actual client IP is extracted from the header, e.g. X-Forwarded-For and used to populate this field and used in security policy checks involving the client IP as well. See related Proxy IP field below as well.</p>
Client Port	37754	The port relevant to the client IP address.
Login ID	-	The login ID used by the client for the request. This is available only when authentication is set to 'ON' for the Service whose URL was requested.
Certificate User	-	The username as found in the SSL certificate when Client Authentication is enforced by the Barracuda Web Application Firewall.
Method	POST	The request method of the traffic.
Protocol (HTTP or HTTPS)	HTTP	The protocol used for communication with the web server, either HTTP or HTTPS.
Host	192.168.132.211	The IP address of the host or website accessed by the user.
Version	HTTP/1.1	The HTTP version used by the request.
HTTP status	200	The standard response code which helps identify the cause of the problem when a web page or other resource does not load properly.



Barracuda Syslog Barracuda Web Application Firewall

Field Name	Example	Description
Bytes Sent	812	The bytes sent as response by the Barracuda Web Application Firewall to the client.
Bytes Received	6401	The bytes received from the client as a part of the request.
Cache Hit	0	Specifies whether the response is served out of Barracuda Web Application Firewall cache or from the backend. Possible values are: 0 – if the request is fetched from the back-end and given to the user. 1 – if the request is fetched from the cache and given to the user.
Time Taken (sec)	230	The total time taken to serve the request from the time the request landed on the Barracuda Web Application Firewall till the last byte given out to the client.
Server IP	192.168.128.7	The IP address of the back-end Web server.
Server Port	80	The port relevant to the back-end Web server.
Server Time (ms)	0	The total time taken by the backend server to serve the request forwarded to it by the Barracuda Web Application Firewall.
Session ID	-	The value of the session tokens found in the request if session tracking is enabled. Session Tracking is configured on the WEBSITES > Advanced Security page.
Response Type Field	SERVER	Specifies whether the response came from the backend or from the Barracuda Web Application Firewall. Possible values are: INTERNAL, SERVER.
Profile Matched Field	DEFAULT	Specifies whether the request matched a defined URL or Parameter Profile. Possible values are: DEFAULT, PROFILED.



Barracuda Syslog

Barracuda Web Application Firewall

Field Name	Example	Description
Protected Field	PASSIVE	Specifies whether the request went through the Barracuda Web Application Firewall rules and policy checks. Possible values are: PASSIVE, PROTECTED, UNPROTECTED.
WF Matched Field	VALID	Specifies whether the request is valid or not. Possible values are: INVALID, VALID.
URL	/cgi-bin/process.cgi	The URL of the request without the query part.
Query	-	The query part of the request.
Referrer	http://192.168.132.211/cgi-bin/1.pl	The value contained in the Referrer HTTP request header. It identifies the Web resource from which the client was "referred" to the requested URL.
Cookie	ys-grid_firewall_log-grid=o%3Acolumns%3Da%253Ao%25253Aid%25253Ds%2525253Aiso_timestamp%25255Ewidth%25253Dn%2525253A38%255Eo%252	The cookie as found in the HTTP request headers.
User Agent	Mozilla/5.0 (X11; U; Linux i686 (x86_64);en-US; rv:1.8.1.20) Gecko/20081217 Firefox/2.0.0.20	The value contained in the User-Agent request header. Normally, this information is submitted by the clients which details the browser, operating system, software vendor or software revision, in an identification string.



Barracuda Syslog Barracuda Web Application Firewall

Field Name	Example	Description
Proxy IP	192.168.128.7	<p>If the client requests are coming through a proxy or gateway, then this field provides the IP address of the proxy.</p> <p>A client side proxy or gateway changes the source IP of the request to its own and embeds the actual client's IP in an HTTP header such as X-Forwarded-For or X-Client-IP.</p> <p>The Barracuda Web Application Firewall, if configured, will ignore the proxy IP and extract the actual client IP from the appropriate header to apply security policies as well as for logging the Client IP field above.</p> <p>This field preserves the proxy IP address for cases where it is required, e.g. forensics and analytics.</p> <p>Note: The actual client IP header configuration is done using the Header Name For Actual Client IP under the Edit actions for a service on the BASIC > Services page.</p>
Proxy Port	37754	The port of the proxy server whose IP address has been logged in the Proxy IP field above.
Authenticated User	John	The username of the currently authenticated client requesting the web page. This is available only when the request is for a service that is using the AAA (User Access Control) module.
Custom Header 1	en-us,or;q=0.5	The header name for which you want to see the value in the Access Logs.
Custom Header 2	gzip,deflate	The header name for which you want to see the value in the Access Logs.
Custom Header 3	ISO-8859-15,utf-8;q=0.7,*;q=0.7	The header name for which you want to see the value in the Access Logs.



Barracuda Syslog

Barracuda Web Application Firewall

Audit Logs

The audit logs record the activity of the users logged in to the GUI of the Barracuda Web Application Firewall for the purpose of administration. These logs are visible on the **BASIC > Audit Logs** page and are also stored on the Barracuda Web Application Firewall in its native database. Additionally, when the administrator chooses an external remote syslog server through the configuration available at **ADVANCED > Export Logs**, these logs are streamed to the remote syslog servers with the priority as INFO.

The default log format for Audit Logs is as follows:

```
%t %un %lt %an %ct %li %lp %trt %tri %cn %cht %ot %on %var %ov %nv %add
```

Note:

- Refer [Table of Log Formats](#) for the meanings of the alphabets.
- Unit Name, Log Type, and Log ID are not displayed on the **BASIC > Audit Logs** page.

Example:

```
2010-02-02 21:08:53.861 -0800 wafbox1 AUDIT Adam GUI 192.168.128.7 0 CONFIG 17 - SET
web_firewall_policy default url_protection_max_upload_files "5" "6" "[]"
```

Detailed Description

The following table describes each element of an audit log with respect to the above example:

Field Name	Example	Description
Time Stamp	2010-02-02 21:08:53.861 -0800	The time recorded in the following format: yyyy-mm-dd hh:mm:ss.s (one or more digits representing a decimal fraction of a second)TZD(time zone designator which is either Z or +hh:mm or -hh:mm)
Unit Name	wafbox1	Specifies the name of the unit which is same as the Default Hostname on the BASIC > IP Configuration page.
Log Type	AUDIT	Specifies whether it is of type Web Firewall Log, Access Log, or Audit Log. Values: TR, WF, AUDIT
Admin Name	Adam	The name of the logged in user.
Client Type	GUI	This indicates that GUI is used as client to access the Barracuda Web Application Firewall.



Barracuda Syslog Barracuda Web Application Firewall

Field Name	Example	Description
Login IP	192.168.128.7	The IP address from which the activity happened.
Login Port	0	The port from which the activity happened.
Transaction Type	CONFIG	Denotes the type of transaction done by the system administrator. Possible values are: LOGIN, LOGOUT, CONFIG, COMMAND, ROLLBACK, RESTORE, REBOOT, SHUTDOWN, FIRMWARE UPDATE, ENERGIZE UPDATE, SUPPORT TUNNEL OPEN, SUPPORT TUNNEL CLOSED, FIRMWARE APPLY, FIRMWARE REVERT, TRANSPARENT MODE, UNSUCCESSFUL LOGIN, ADMIN ACCESS VIOLATION.
Transaction ID	17	Specifies the transaction ID for the transaction that makes the persistent change. Note: Events that do not change anything do not have a transaction ID. This is indicated by transaction ID of -1.
Command Name	-	The name of the command that was executed on the Barracuda Web Application Firewall.
Change Type	SET	Denotes the type of change made to the configuration. Possible values are: NONE, ADD, DELETE, SET.
Object Type	web_firewall_policy	The type of the object which is being modified.
Object Name	Default	The name of the object type that is being modified.
Variable	url_protection_max_upload_files	The internal name of the parameter which is under modification.
Old Value	5	The value before modification.
New Value	6	The value to which the parameter is modified.
Additional Data	[]	Provides more information on the parameter changed.



Barracuda Syslog Barracuda Web Application Firewall

Table of Log Formats

System Logs	Web Firewall Logs	Access Logs	Audit Logs
%t - Time Stamp	%t - Time Stamp	%t - Time Stamp	%t - Time Stamp
%md - Module Name	%un - Unit Name	%un - Unit Name	%un - Unit Name
%ll - Log Level	%lt - Log Type	%lt - Log Type	%lt - Log Type
%ei - Event ID	%sl - Severity Level	%ai - Application IP	%an - Admin Name
%ms - Message	%ad - Attack Description	%ap - Application Port	%ct - Client Type
	%ci - Client IP	%ci - Client IP	%li - Login IP
	%cp - Client Port	%cp - Client Port	%lp - Login Port
	%ai - Application IP	%id - Login ID	%trt - Transaction Type
	%ap - Application Port	%cu - Certificate User	%tri - Transaction ID
	%ri - Rule ID	%m - Method	%cn - Command Name
	%rt - Rule Type	%p - Protocol	%cht - Change Type
	%at - Action Taken	%h - Host	%ot - Object Type
	%fa - Follow-up Action	%v - Version	%on - Object Name
	%adl - Attack Details	%s - HTTP Status	%var - Variable
	%m - Method	%bs - Bytes Sent	%ov - Old Value
	%u - URL	%br - Bytes Received	%nv - New Value
	%p - Protocol	%ch - Cache Hit	%add - Additional Data
	%sid - Session ID	%tt - Time Taken	
	%ua - User Agent	%si - Server IP	
	%px - Proxy IP	%sp - Server Port	
	%pp - Proxy Port	%st - Server Time	
	%au - Authenticated User	%sid - Session ID	
	%r - Referrer	%rtf - Response Type Field	
	%aid - Attack ID	%pmf - Profile Matched Field	
	%ag - Attack Group	%pf - Protected Field	
		%wmf - WF Matched Field	



Barracuda Syslog Barracuda Web Application Firewall

System Logs	Web Firewall Logs	Access Logs	Audit Logs
		%u - URL	
		%q - Query	
		%r - Referrer	
		%c - Cookie	
		%ua - User Agent	
		%px - Proxy IP	
		%pp - Proxy Port	
		%au - Authenticated User	
		%cs1 - Custom Header 1	
		%cs2 - Custom Header 2	
		%cs3 - Custom Header 3	