



# Barracuda Syslog Barracuda Web Site Firewall

---

## Overview

There are four types of logs generated by the Barracuda Web Site Firewall which can be configured to be sent over the syslog mechanism to a remote server specified by the Barracuda Web Site Firewall administrator. These logs are also resident on the Barracuda Web Site 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 Site 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 Site Firewall starting with version 7.0.x of the firmware.

The following four types of events are explained briefly below. These logs are logged at different facilities to help manage them well on the external syslog server that they get transferred to.

**System Events:** These are the events generated by the system and show the general activity of the system. These logs are logged at LOCAL0 facility and at various priority levels depending on the content of the message.

**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 Site Firewall rules and policies. These logs are logged at LOCAL1 facility and at various priorities based on the action taken.

**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. These are logged at LOCAL2 facility at the priority level INFO.

**Audit Logs:** These events pertain to the auditing events generated by the system which log the configuration and UI activity by users like admin. These are logged at LOCAL3 facility and at the priority level INFO.

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

## Enabling Syslog

To enable exporting of logs to a remote syslog server, navigate to the **Advanced > Export Logs** page. Remote syslog server for System Events is specified under **System Logs** in the web GUI. Enter the IP address of the syslog server to which you wish to direct the messages. Remote syslog server for the application logs (i.e. Web Firewall, Access and Audit logs) is specified under Application 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 doesn't include the syslog capability. Kiwi Syslog is a popular solution, but there are many others to choose from, both free and commercial.



## Barracuda Syslog Barracuda Web Site Firewall

The syslog messages are sent over UDP to the standard syslog port of 514. If there are any firewalls between the Barracuda Web Site Firewall and the server receiving the syslog messages, then be sure that port 514 is open on the firewalls. The syslog messages arrive on various facilities depending on the log type and various priority levels based on the severity of the log. These facilities and levels are not configurable and are decided by the Barracuda Web Site Firewall. 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 Site 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

These events get logged at LOCAL0 facility. The log format for the events generated by the Barracuda Web Site Firewall system is as follows:

- Module name
- Message

#### Example:

STM: COOKIE-5 00000 SetSapIpsCookieServicePolicy = 0

### Detailed Description

The following table describes each element of a system log:

Field Name	Example	Description
Module Name	STM	Denotes the name of the module that generated the logs. For example: STM, SAPD, LB, etc.
Message	COOKIE-5 00000 SetSapIpsCookieServicePolicy = 0	Denotes the log message for the event that occurred.

### Web Firewall Logs (Logged at LOCAL1 facility)

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 stored in a database on the Barracuda Web Site Firewall. This log data is obtained from the log database on the Barracuda Web Site Firewall itself. As noted above, the external syslog server IP for these logs is specified under **Advanced > Export Logs > Application Logs**. Over syslog, every log in the Barracuda Web Site Firewall is logged under LOCAL1 facility and has a level associated with it, which



## Barracuda Syslog Barracuda Web Site Firewall

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 log format for Web Firewall Logs is as follows:

- Timestamp
- Severity
- Attack Name
- Client IP
- Client Port
- Application IP
- Application Port
- Rule ID (ACL)
- Rule Name
- Action Taken
- Follow-up Action
- Attack Detail
- Method
- URL

### Example:

```
1225613275.270 ALER SLASH_DOT_IN_URL 192.168.128.11 44273 192.168.132.164 80 default  
GLOBAL LOG NONE "[ ]" GET 192.168.132.164/.init
```

### Detailed Description

The following table describes each element of a web firewall log:

Field Name	Example	Description
Timestamp	1225613275.270	The time recorded in UTC format as number of seconds since 1970.
Severity	ALER	Defines the seriousness of the attack.
Attack Name	SLASH_DOT_IN_URL	The name of the attack triggered by the traffic.
Client IP	192.168.128.11	The IP address of the client sending the request.
Client Port	44273	The port relevant to the client IP address.
Application IP	192.168.132.164	The IP address of the application that receives the traffic.



## Barracuda Syslog Barracuda Web Site Firewall

Field Name	Example	Description
Application Port	80	The port relevant to the application IP address.
Rule ID (ACL)	default	The rule configured for the application in the ACL.
Rule Name	GLOBAL	Specifies if the log is from a GLOBAL policy or a URL ACL or a profile.
Action Taken	LOG	The appropriate action applied on the traffic. <b>Deny</b> denotes that the traffic is denied. <b>LOG</b> denotes monitoring of the traffic with the assigned rule. <b>Warning</b> warns about the traffic.
Follow-up Action	NONE	The follow-up action as specified by the action policy. It could be either "None" or "Locked" in case the lockout is chosen.
Attack Detail	[]	Provides the attack details.
Method	GET	The request method of the traffic.
URL	192.168.132.164/.init	The URL of the request.

### Attack Names

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

Event ID	Attack Name	Description	Severity	Attack Type
<b>Advanced Policy Violations</b>				
29012	INVALID_URL_CHAR SET	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 Controller relies on several configuration elements like Default Character Set, Detect Response Charset, Response Charset.	Warning	Attack obfuscation
29145	BRUTE_FORCE_FRO M_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_FRO M_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 Site Firewall

Event ID	Attack Name	Description	Severity	Attack Type
<b>Application Profile Violations</b>				
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
<b>Header Violations</b>				
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
<b>Param Profile Violations</b>				
29134	READ_ONLY_PARAM_TAMPERED	The read-only parameter had a value, which was different from what was learned by Barracuda Web Application Controller based on the form that was sent to the browser.	Alert	Form tampering



## Barracuda Syslog Barracuda Web Site Firewall

Event ID	Attack Name	Description	Severity	Attack Type
29135	SESSION_INVARIANT_PARAM_TAMPERED	The session-invariant parameter had a value, which was different from what was learned by Barracuda Web Application Controller based on the form that was sent to the browser for this session.	Alert	Form tampering
29136	SESSION_CHOICE_PARAMETER_TAMPERED	The session choice parameter had a value, which was different from what was learned by Barracuda Web Application Controller based on the form that was sent to the browser for this session.	Alert	Form tampering
29137	TOO_MANY_PARAMETER_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_PARAMETER	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
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



## Barracuda Syslog Barracuda Web Site Firewall

Event ID	Attack Name	Description	Severity	Attack Type
29158	CROSS_SITE_SCRIPTING_IN_PARAM	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_PARAM	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_INCLUDE_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
29165	CROSS_SITE_REQUEST_FORGERY	The Barracuda Web Application Controller inserted state parameter '__ncforminfo', is either not found or found tampered in the form that matched the URL profile.	Alert	Forceful browsing
<b>Protocol Violations</b>				
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 Controller.	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 Controller for violating basic HTTP conformance checks.	Alert	Protocol exploit



## Barracuda Syslog Barracuda Web Site Firewall

Event ID	Attack Name	Description	Severity	Attack Type
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
29123	MALFORMED_CONTENT_LENGTH	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
<b>Request Policy Violations</b>				
29000	REQUEST_LINE_LENGTH_EXCEEDED	The HTTP request length exceeded the Max Request Length configured in the Web Firewall Policy.	Alert	Buffer overflow



## Barracuda Syslog Barracuda Web Site Firewall

Event ID	Attack Name	Description	Severity	Attack Type
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
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 Controller. 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 Controller. 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 Controller.	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 Web Firewall or Request Limits. The number of headers includes any Cookie headers.	Alert	Buffer overflow
29116	COOKIE_REPLAY_MISMATCHED_HEADER		Warning	Cookie poisoning
29117	COOKIE_REPLAY_MISMATCHED_IP		Warning	Cookie poisoning



## Barracuda Syslog Barracuda Web Site Firewall

Event ID	Attack Name	Description	Severity	Attack Type
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
<b>Response Violations</b>				
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 Firewall/Website 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.  <b>Note:</b> 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
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
<b>URL Profile Violations</b>				
29005	INVALID_METHOD	The request sent by the browser contained a method which is not allowed by the Barracuda Web Application Controller.	Alert	Application platform exploit



## Barracuda Syslog Barracuda Web Site Firewall

Event ID	Attack Name	Description	Severity	Attack Type
29026	UNKNOWN_CONTENT_TYPE	The Content-Type of the POST request was not recognized by the Barracuda Web Application Controller.	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_STR_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_UPLOADED_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_NOT_FOUND	Either the Barracuda Web Application Controller inserted session cookie is not in the request header or the Barracuda Web Application Controller inserted hidden parameter is missing.	Alert	Forceful browsing
29163	NO_PARAM_PROFILE_MATCH	The request sent by the browser contained a parameter, which is not found in the application profile.	Alert	Forceful browsing
<b>XML Violations</b>				
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.  <b>Note:</b> The following attack groups are not configurable but these type of attacks are detected and logged by the Barracuda Web Application Controller.	Warning	Cookie poisoning



## Barracuda Syslog Barracuda Web Site Firewall

Event ID	Attack Name	Description	Severity	Attack Type
<b>Access Violations</b>				
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 website.	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
<b>ACL Violations</b>				
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

### Access Logs (Logged at LOCAL2 facility)

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 Site Firewall in a log database.

The log format for Access Logs is as follows:

- Timestamp
- Service IP
- Service Port
- Client IP
- Client Port
- Login ID
- Certificate Username



## Barracuda Syslog Barracuda Web Site Firewall

- Method
- Protocol (HTTP or HTTPS)
- Host
- Version
- Status code
- Bytes-Sent
- Cache-Hit
- Bytes-Received
- Total Time Taken
- Backend Server IP
- Backend Server Port
- Time Taken by the Server
- Session ID (if found)
- Response Type Flag
- Profile Matched Flag
- Protected Flag
- Web Firewall Validated Flag
- URI-Stem
- URI-Query
- Referrer
- Cookie

### Example:

```
2008-11-02 01:39:12.744 -0800192.168.132.164 80 192.168.128.11 44346 "adam" "Adam Smith"  
GET HTTP 192.168.132.164 HTTP/1.0 404 420 0 21 205 192.168.128.11 80 18 SERVER DEFAULT  
PASSIVE VALID /.xx "-" "-" "-"
```

### Detailed Description

The following table describes each element of an access log:

Field Name	Example	Description
Timestamp	2008-11-02 01:39:12.744	The date and time in Apache access log time format, at which the event occurred, where, <b>2004-11-02</b> denotes the date in the form of Year-Month-Day <b>01:39:12:744</b> denotes the time in the form of Hours:Minutes:Seconds:Milliseconds [HH:MM:SS:mmm]



## Barracuda Syslog Barracuda Web Site Firewall

Field Name	Example	Description
Service IP	192.168.132.164	The IP address of the service that receives the traffic.
Service Port	80	The port relevant to the service IP address.
Client IP	192.168.128.11	The IP address of the client sending the request.
Client Port	44346	The port relevant to the client IP address.
Login ID	adam	The login ID used by the client when authentication is set to 'ON' on the Web Site Firewall.
Certificate Username	Adam Smith	The username as found in the SSL certificate when Client Authentication is enforced by the Web Site Firewall.
Method	GET	The request method of the traffic.
Protocol	HTTP	The protocol used for communication with the web server, either HTTP or HTTPS.
Host	192.168.132.164	The host used to login.
Version	HTTP/1.0	The HTTP version used by the request.
Status Code	404	The standard response code which helps identify the cause of the problem when a web page or other resource does not load properly.
Bytes Sent	420	The bytes sent as the response by the Web Site Firewall to the client.
Cache Hit	0	Specifies whether the response is served out of Web Site Firewall cache or from the backend.
Bytes Received	21	The bytes received from the client as a part of the request.
Total Time Taken	205	The total time taken to serve the request from the time the request landed on the Web Site Firewall and the last byte is given out to the client.
Backend Server IP	192.168.128.11	The IP address of the backend web server.
Backend Server Port	80	The port relevant to the backend server IP address.
Time Taken by the server	18	The total time taken by the backend server to serve to the request forwarded to it by the Web Site Firewall.
Session ID	-	The value of the session tokens found in the request if session tracking is enabled.



## Barracuda Syslog Barracuda Web Site Firewall

Field Name	Example	Description
Response Type Flag	SERVER	Specifies whether the response came from the backend or from the Web Site Firewall.
Profile Matched Flag	DEFAULT	Specifies whether the request matched a defined URL or Parameter Profile.
Protected Flag	PASSIVE	Specifies whether the request went through the Web Site Firewall rules and policy checks.
Web Firewall Validated Flag	VALID	Specifies whether the request is valid or not.
URI-Stem	/.xx	The URI of the request without the query part.
URI-Query	-	The query part of the request.
Referrer	-	The referrer header found in the incoming request.
Cookie	-	The cookie as found in the HTTP request headers.

### Audit Logs (Logged at LOCAL3 facility)

The audit logs record the activity of the users logged in to the GUI of the box for the purpose of administration. These logs are visible at the **Basic > Audit Logs** page and are also stored on the Barracuda Web Site 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 server at LOCAL3 facility with the priority as INFO.

The log format for Audit Logs is as follows:

- Timestamp
- Administrator name
- Client Type
- IP
- Transaction Type
- Transaction ID
- Command Name
- Change type
- Object Type
- Object Name
- Variable name
- Old value



## Barracuda Syslog Barracuda Web Site Firewall

- New Value
- Additional Data if any

**Example:**

```
1225612215.392 admin GUI 192.168.128.11 0 CONFIG 1321 - SET web_firewall_policy default
aps_cookie_max_age "1441" "1444" "[]"
```

### Detailed Description

The following table describes each element of an audit log:

Field Name	Example	Description
Timestamp	1225612215.392	The time recorded in UTC format as number of seconds since 1970.
Administrator name	admin	Specifies the name of the System Administrator.
Client Type	GUI	Sets the client type, GUI in the case of Barracuda Web Site Firewall 7.1 and 7.1 versions.
IP	192.168.128.11	The IP address from which the administration happened.
Transaction Type	CONFIG	Denotes the type of transaction done by the system administrator.  Values: LOGIN, LOGOUT, CONFIG, COMMAND, ROLLBACK, RESTORE, REBOOT, SHUTDOWN, FIRMWARE UPDATE, ENERGIZE UPDATES, SUPPORT TUNNEL OPEN, SUPPORT TUNNEL CLOSED, FIRMWARE APPLY, FIRMWARE REVERT.
Transaction ID	1321	Specifies the transaction ID for the transaction that makes the persistent change.  <b>Note:</b> Events that do not change anything do not have a transaction ID. This is indicated by transaction ID of -1.
Command Name	-	Specifies the executed command.
Change type	SET	Denotes the type of change made to the configuration.  Values: ADD, CLEAR, DELETE, MODIFY, SET.
Object Type	web_firewall_policy	This refers to the container or the object which is being modified.
Object Name	default	Refers to the name of the instance of the object type that is being modified.



## Barracuda Syslog Barracuda Web Site Firewall

---

Field Name	Example	Description
Variable name	aps_cookie_max_age	Refers to the internal name of the parameter which is under modification.
Old value	"1441"	The value before modification.
New Value	"1444"	The value to which the parameter is modified.
Additional Data if any	[]	Additional information which depends on the transaction type.