Exporting Log Formats

https://campus.barracuda.com/doc/92767349/

Custom Log Format

Customize the Log Format for any Log Type (except System Logs)

1. Navigate to the **ADVANCED > Export Logs** page.
2. In the **Logs Format** section, select **Custom Format** for any of the log types. The **Custom Format** can be defined in two ways:
    1. Specify "%" followed by the alphabet. The alphabet 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,
    2. 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** to save the settings.

Log Format Separators

When defining log formats, you can use *space* as a separator between each log format for **Web Firewall Logs Format**, **Access Logs Format,** and **Audit Logs Format**.

For **Access Logs Format**, you can also use pipe (|) or semicolon (;) separators. Log formats can be separated by a single separator or a combination of space, pipe, and semicolon separators.

> Log formats can use only one separator in each place, i.e., space (" "), pipe (|) or semicolon. For example: %h %id|%u;%t %r|%s

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

Configure Logs Format

1. Go to the **ADVANCED > Export Logs** page.
2. In the Logs Format section, specify values for the following fields:
    - **Syslog Header** – Specify a header format, which will be displayed when **%header** is

used in the logs format. For example, consider the header format is "Barracuda", and the defined custom format is "%header %h %u %t %r %ua %ci". The output will be "Barracuda 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". **Values**:

    - **ArcSight Log Header** – Uses this header format in the logs format.
    - **QRadar Log Header** – Uses this header format in the logs format.
    - **Custom Header** – Define a custom header format to be used in the logs format.

- **Web Firewall Logs Format** – Select the format in which the Web firewall logs should be sent to the export log server. **Values**:
    - **Default** – The default Web firewall log format defined by the Barracuda Web Application Firewall
    - **CEF:0 (ArcSight)** – The Common Event Format (CEF) log used by ArcSight.
    - **HPE ArcSight CEF:0** - The Common Event Format (CEF) log used by HP ArcSight. This is the updated version of **CEF:0 (ArcSight)**.
    - **LEEF1.0 (QRadar)** – The Log Event Enhanced Format (LEEF) log used by QRadar.
    - **Symantec SIM** – The default log format used by Symantec SIM.
    - **RSA enVision** – The default log format used by RSA envision.
    - **Microsoft Azure Log Analytics** - The default log format used by Microsoft Azure Log Analytics.
    - **Splunk** – The default log format used by Splunk.
    - **Custom Format**– Define a custom log format using the values displayed under Web Firewall Logs in the Table of Log Formats
- **Access Logs Format** – Select the format in which the access logs should be sent to the export log server. Values:
    - **Default** – The default access log format defined by the Barracuda Web Application Firewall.
    - **Common Log Format** – The default format for logged HTTP information.
    - **NCSA Extended Format** – The Common Log Format appended with referer and agent information.
    - **W3C Extended Format** – The default log format used by Microsoft Internet Information Server (IIS).
    - **CEF:0 (ArcSight)** – The Common Event Format (CEF) log used by ArcSight.
    - **HPE ArcSight CEF:0** - The Common Event Format (CEF) log used by HP ArcSight. This is the updated version of **CEF:0 (ArcSight)**
    - **LEEF1.0 (QRadar)** – The Log Event Enhanced Format (LEEF) log used by QRadar.
    - **Symantec SIM** – The default log format used by Symantec SIM.
    - **RSA enVision** – The default log format used by RSA enVision.
    - **Splunk** – The default log format used by Splunk.
    - **Microsoft Azure Log Analytics** - The default log format used by Microsoft Azure Log Analytics.
    - **Custom Format** – Define a custom log format using the values displayed under Access Logs in Table of Log Formats.
- **Audit Logs Format** – Select the format in which the audit logs should be sent to the export log server. Values:
    - **Default**– The default audit logs format defined by the Barracuda Web Application Firewall.

        - **CEF:0 (ArcSight)** – The Common Event Format (CEF) log used by ArcSight.
        - **HPE ArcSight CEF:0** - The Common Event Format (CEF) log used by HP ArcSight. This is the updated version of **CEF:0 (ArcSight)**
        - **LEEF1.0 (QRadar)** – The Log Event Enhanced Format (LEEF) log used by QRadar.
        - **Symantec SIM** – The default log format used by Symantec SIM.
        - **RSA envision** – The default log format used by RSA envision.
        - **Splunk** – The default log format used by Splunk.
        - **Microsoft Azure Log Analytics** - The default log format used by Microsoft Azure Log Analytics.
        - **Custom Format** – Define a custom log format using the values displayed under Audit Logs in the Table of Log Formats.
    - **Network Firewall Logs Format** - Select the format in which the network firewall logs should be sent to the export log server. Values:
        - **Default** - The default network firewall logs format defined by the Barracuda Web Application Firewall.
        - **HPE ArcSight CEF:0** - The Common Event Format (CEF) log used by HP ArcSight. This is the updated version of **CEF:0 (ArcSight)**
        - **Custom Format** - Define a custom log format using the values displayed under Network Firewall Logs in the Table of Log Formats.
    - **System Logs Format** - Select the format in which the system logs should be sent to the export log server. Values:
        - **Default** - The default system logs format defined by the Barracuda Web Application Firewall.
        - **CEF:0 (ArcSight)** - The Common Event Format (CEF) log used by ArcSight.
        - **HPE ArcSight CEF:0** - The Common Event Format (CEF) log used by HP ArcSight. This is the updated version of **CEF:0 (ArcSight)**
        - **LEEF1.0 (QRadar)** - The Log Event Enhanced Format (LEEF) log used by QRadar.
        - **Symantec SIM** - The default log format used by Symantec SIM.
        - **RSA enVision** - The default log format used by RSA envision.
        - **Splunk** - The default log format used by Splunk.
        - **Microsoft Azure Log Analytics** - The default log format used by Microsoft Azure Log Analytics.
        - **Custom Format** - Define a custom log format using the values displayed under System Logs in the Table of Log Formats.
3. Click **Save**.

The sections below 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 syslog implementations vary, and may not display the messages in this exact format. However, these sections should be present in the syslog lines.

System Logs

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

```
%t %un %lt %md %ll %ei %ms
```

For information on default log formats and their meanings, see the table below.

Example:

```
2014-05-20 00: 54:44.627 -0700  WAF1 SYS ADMIN_M ALER 51001 Account has been
locked for user Kevin because the number of consecutive log-in failures
exceeded the maximum allowed
```

Detailed Description

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

Field Name	Example	Description
Time	2014-05-20 00: 54:44.627 -0700	The date and time at which the event occurred.
Unit Name	WAF1	Specifies the name of the unit, which is same as the **Default Hostname** on the **BASIC > IP Configuration** page.
Log Type	SYS	Specifies the type of log: Web Firewall Log, Access Log, Audit Log, Network Firewall Log or System Log. Values: WF, TR, AUDIT, NF, SYS
Module Name	ADMIN_M	Denotes the name of the module that generated the logs. Example: STM, SAPD, LB, PROCMON, etc.
Log Level	ALER	The level of severity. Values: • **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).
Event ID	51001	The event ID of the module.

Message	Account has been locked for user Kevin because the number of consecutive log-in failures exceeded the maximum allowed.	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 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:

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

Unit Name, Log Type, and Log ID are not displayed on the **BASIC > Web Firewall Logs** page.

IPv4 Example:

```
2014-04-11 10:50:30.411 +0530  wafbox1 WF ALER PRE_1_0_REQUEST 99.99.1.117
34006 99.99.109.2 80 global GLOBAL LOG NONE [POST /index.cgi] POST
99.99.109.2/index.cgi HTTP REQ-0+RES-0 “Mozilla/5.0 (X11; Linux
i686; rv:12.0) Gecko/20100101 Firefox/12.0”  99.99.1.117 34005 Kevin
http://99.99.109.2/index.cgi
```

IPv6 Example:

```
2014-04-11 10:52:01.579 +0530  wafbox1 WF ALER PRE_1_0_REQUEST 2001::117
43655 2001::1:109 80 global GLOBAL LOG NONE [POST /index.cgi] POST
2001::1:109/index.cgi HTTP REQ-0+RES-0  " Mozilla/5.0 (X11; Linux
i686; rv:12.0) Gecko/20100101 Firefox/12.0" 2001::117 43654
Kevin http://2001::109/index.cgi
```

Detailed Description

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

Field Name	Example	Description
Time	2014-04-11 10:50:30.411 +0530	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 the same as the **Default Hostname** on the **BASIC > IP Configuration** page.
Log Type	WF	Specifies the type of log: Web Firewall Log, Access Log, Audit Log, Network Firewall Log, or System Log. Values: WF, TR, AUDIT, NF, SYS
Severity	ALER	Defines the seriousness of the attack. Values: • **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).
Attack Type	PRE_1_0_REQUEST	The name of the attack triggered by the request. For detailed information about attack names and descriptions, see Attacks Description - Action Policy.
Client IP	99.99.1.117 **OR** 2001::117	The IP address of the client sending the request. 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, configure the **Header Name For Actual Client IP** under the Edit actions for a service on the **BASIC > Services** page. Then, the actual client IP can be extracted from the header, (e.g., *X-Forwarded-For*) logged in this field and used in security policy checks involving the client IP. See also the related **Proxy IP** field below.

Client Port	34006 **OR** 43655	The port relevant to the client IP address.
Service IP	99.99.109.2 **OR** 2001::1:109	The IP address of the service that receives the traffic.
Service Port	80	The port relevant to the IP address of the service.
Rule	global	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.
Rule Type	GLOBAL	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: • **Global** – indicates that the request matched one of the global rules configured under Security Policies. • **Global URL ACL** – indicates that the request matched one of the global URL ACL rules configured under Security Policies. • **URL ACL** – indicates that the request matched one of the Allow/Deny rules configured specifically for the given website. • **URL Policy** – indicates that the request matched one of the Advanced Security rules configured specifically for the given website. • **URL Profile** – indicates that the request matched one of the rules configured on the URL Profile. • **Parameter Profile** – indicates that the request matched one of the rules configured on the Parameter Profile. • **Header Profile** – indicates that the request matched one of the rules configured on the Header Profile.
Action	LOG	The appropriate action applied on the traffic. **DENY** – denotes that the traffic is denied. **LOG** – denotes monitoring of the traffic with the assigned rule. **WARNING** – warns about the traffic.
Follow-up Action	NONE	The follow-up action as specified by the action policy. It can be either **None** or **Locked** in case the lockout is chosen.
Attack Details	[POST /index.cgi]	The details of the attack triggered by the request.
Method	POST	The HTTP method used by the request. Values: GET, POST, HEAD, etc.

Host + URL	99.99.109.2/index.cgi **OR** 2001::1:109/index.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; Linux i686; rv:12.0) Gecko/20100101 Firefox/12.0	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	99.99.1.117 **OR** 2001::117	If the client requests are coming through a proxy or gateway, then this field provides the IP address of the proxy. 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. 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. This field preserves the proxy IP address for cases where it is required, e.g., forensics and analytics 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.
Proxy Port	34005 **OR** 43654	The port of the proxy server whose IP address has been logged in the **Proxy IP** field above.
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 (Access Control) module.
Referrer	http://99.99.109.2/index.cgi **OR** http://2001::109/index.cgi	The value contained in the Referrer HTTP request header. It identifies the web resource from which the client was "referred" to the requested URL.

Access Logs

All web traffic activities are logged under the Access Logs. These logs help the administrator to obtain information about the website 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:

%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

Unit Name, Log Type, and Log ID are not displayed on the **BASIC > Access Logs** page.

IPv4 Example:

```
2014-04-11 12:04:04.735 +0530  wafbox1 TR 99.99.109.2 80 99.99.1.117 34065 "-
" "-" GET HTTP 99.99.106.25 HTTP/1.1 200 2829 232 0 1127 10.11.25.117 80 21
REQ-0+RES-0  SERVER DEFAULT PASSIVE VALID /index.html name=srawat
http://99.99.109.2/index.cgi  namdksih=askdj "Mozilla/5.0 (X11; Linux
i686; rv:12.0) Gecko/20100101 Firefox/12.0" 99.99.1.117 34065 John
gzip,deflate 99.99.1.128 keep-alive
```

IPv6 Example:

```
2014-04-11 12:11:24.964 +0530  wafbox1 TR 2001::1:109 80 2001::117 43740 "-"
"-" GET HTTP 2001::1:109 HTTP/1.1 200 2837 232 0 1008 2001::117 80 10
REQ-0+RES-0   SERVER DEFAULT PASSIVE VALID /index.html
name=srawat http://2001::1:109/index.cgi namdksih=askdj "Mozilla/5.0 (X11;
Linux i686; rv:12.0) Gecko/20100101 Firefox/12.0" 2001::117 43740 John
gzip,deflate 2001::128 keep-alive
```

Detailed Description

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

Field Name	Example	Description
Time	2014-04-11 12:04:04.735 +0530	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	The name of the unit specified as **Default Hostname** on the **BASIC > IP Configuration** page.
Log Type	TR	Denotes the type of log: Web Firewall Log, Access Log, Audit Log, Network Firewall Log or System Log. Values: WF, TR, AUDIT, NF, SYS
Service IP	99.99.109.2 **OR** 2001::1:109	The IP address of the service that receives the traffic.
Service Port	80	The port relevant to the IP address of the service.
Client IP	99.99.1.117 **OR** 2001::117	The IP address of the client sending the request. 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, configure the **Header Name For Actual Client IP** under the **Edit** actions for a service on the **BASIC > Services** page**.** 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.
Client Port	59589 **OR** 43646	The port relevant to the client IP address.
Login	-	The login ID used by the client when authentication is set to *On* for the service on the **ACCESS CONTROL > Authentication Policies** page. This is the user authenticated by LDAP, RADIUS, RSA SecurID, SAML IDP, or Kerberos authentication service configured on the Barracuda Web Application Firewall.
Certificate User	-	The username as found in the SSL certificate when **Client Authentication** is enforced by the Barracuda Web Application Firewall.
Method	GET	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	99.99.106.25 **OR** 2001::1:109	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 that helps identify the cause of the problem when a web page or other resource does not load properly.
Bytes Sent	2829	The bytes sent as response by the Barracuda Web Application Firewall to the client.
Bytes Received	232	The bytes received from the client as a part of the request.
Cache Hit	0	Specifies whether the response is served out of the Barracuda Web Application Firewall cache or from the backend server. Values: 0 – if the request is fetched from the server and given to the user. 1 – if the request is fetched from the cache and given to the user.
Time Taken (ms)	1127	The total time taken to serve the request from the time the request landed on the Barracuda Web Application Firewall until the last byte given out to the client.
Server IP	10.11.25.117 **OR** 2001::117	The IP address of the backend web server.
Server Port	80	The port relevant to the backend web server.
Server Time (ms)	21	The total time taken by the backend server to serve the request forwarded to it by the Barracuda Web Application Firewall.
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.
Response Type	SERVER	Specifies whether the response came from the backend sever or from the Barracuda Web Application Firewall. Values: INTERNAL, SERVER.
Profile Matched	DEFAULT	Specifies whether the request matched a defined URL or Parameter Profile. Values: DEFAULT, PROFILED.
Protected	PASSIVE	Specifies whether the request went through the Barracuda Web Application Firewall rules and policy checks. Values: PASSIVE, PROTECTED, UNPROTECTED.
WF Matched	VALID	Specifies whether the request is valid. Values: INVALID, VALID.
URL	/index.html	The URL of the request without the query part.

Query String	name-srawat	The query part of the request.
Referrer	http://99.99.109.2/index.cgi **OR** http://2001::1:109/index.cgi	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	namdksih=askdj	The cookie as found in the HTTP request headers.
User Agent	Mozilla/5.0 (X11; Linux i686; rv:12.0) Gecko/20100101 Firefox/12.0	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	99.99.1.117 **OR** 2001::117	If the client requests are coming through a proxy or gateway, this field provides the IP address of the proxy. 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. 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. This field preserves the proxy IP address for cases where it is required, e.g., forensics and analytics. 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.
Proxy Port	34065	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.
Custom Header 1	gzip,deflate (Custom Header used : Accept-Encoding)	The header name for which you want to see the value in the Access Logs.
Custom Header 2	99.99.1.128 **OR** 2001::128 (Custom Header used : Host)	The header name for which you want to see the value in the Access Logs.
Custom Header 3	keep-alive (Custom Header used : Connection)	The header name for which you want to see the value in the Access Logs.
Custom Header 4	no-cache (Custom Header used : Cache-Control)	The header name for which you want to see the value in the Access Logs.

Custom Header 5	Mozilla/5.0 (X11; Linux i686; rv:12.0) Gecko/20100101 Firefox/12.0 (Custom Header used : User-Agent)	The header name for which you want to see the value in the Access Logs.
Custom Header 6	application/json (Custom Header used : Content-Type)	The header name for which you want to see the value in the Access Logs.

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:

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

Unit Name, Log Type, and Log ID are not displayed on the **BASIC > Audit Logs** page.

IPv4 Example:

```
2014-02-24 09:05:17.764 -0800  wafbox1 AUDIT Adam GUI 10.11.18.121 24784
CONFIG 166 config SET virtual_ip_config_address 99.99.130.45
virtual_ip_config_interface "" "WAN" []
```

IPv6 Example:

```
2014-02-24 10:05:17.764 -0800  wafbox1 AUDIT Adam GUI 2001::117 23390 CONFIG
196 config SET virtual_ip_config_address 2001::2:109
virtual_ip_config_interface "" "WAN" []
```

Detailed Description

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

Field Name	Example	Description

Time	2014-02-24 09:05:17.764 -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	The name of the unit specified in the **Default Hostname** field on the **BASIC > IP Configuration** page.
Log Type	AUDIT	Specifies the type of log: Web Firewall Log, Access Log, Audit Log, Network Firewall Log or System Log. Values: WF, TR, AUDIT, NF, SYS
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.
Login IP	10.11.18.121 **OR** 2001::117	The IP address from which the activity happened.
Login Port	24784	The port from which the activity 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 UPDATE, SUPPORT TUNNEL OPEN, SUPPORT TUNNEL CLOSED, FIRMWARE APPLY, FIRMWARE REVERT, TRANSPARENT MODE, UNSUCCESSFUL LOGIN, ADMIN ACCESS VIOLATION.
Transaction ID	166	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	config	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. Values: NONE, ADD, DELETE, SET.
Object Type	virtual_ip_config_address	The type of the object that is being modified.
Object Name	99.99.130.45 **OR** 2001::2:109	The name of the object type that is being modified.
Variable	virtual_ip_config_interface	The internal name of the parameter that is under modification.
Old Value	-	The value before modification.
New Value	WAN	The value after modification.
Additional Data	[]	Provides more information on the parameter changed.

Network Firewall Logs

The network traffic passing through the interfaces (WAN, LAN, and MGMT) that matches the configured Network ACL rule are logged under Network Firewall Logs. The log entries provide information about every packet that the Barracuda Web Application Firewall has allowed or denied based on the Action specified in the ACL rule. Using this information, you can identify where the network traffic originated and where it was destined for, and the action applied. These log entries can be viewed on the **ADVANCED > Network Firewall Logs** page.

The default log format for Network Firewall Logs:

```
%t %un %lt %sl %p %si %sp %di %dp %act %an %dsc
```

IPv4 Example:

```
2014-05-20 00: 56:42.195 -0700  WAF1 NF INFO TCP 99.99.1.117 52676 99.99.79.2
80 ALLOW testacl MGMT/LAN/WAN interface traffic:allow
```

IPv6 Example:

```
2014-05-20 02: 51:36.455 -0700  WAF1 NF INFO TCP 2001:4528::231 46739
2001:4528:2::79 80 ALLOW testacl MGMT/LAN/WAN interface traffic:allow
```

Detailed Description

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

Field Name	Example	Description
Time	2014-04-10 09:37:58.749 -0700	The date and time at which the event occurred. Date format is Year-Month-Day, and time format is Hours: Minutes:Seconds:Milliseconds.
Unit Name	WAF1	The name of the unit specified in the **Default Hostname** field on the **BASIC > IP Configuration** page.
Log Type	NF	Specifies whether it is of type Web Firewall Log, Access Log, Audit Log, Network Firewall Log, or System Log. Values: WF, TR, AUDIT, NF, SYS

Severity	INFO	Defines the seriousness of the attack. Values: • **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).
Protocol	TCP	The Layer 3 protocol type of the corresponding packet.
Source IP	99.99.1.117 **OR** 2001:4528::231	The IP address of the source that originated the network traffic.
Source Port	52676 **OR** 46739	The port number of source that originated the network traffic.
Destination IP	99.99.79.2 **OR** 2001:4528:2::79	The IP address of the destination network or host.
Destination Port	80	The port number of the network or host to which the packet was destined.
ACL Policy	ALLOW	The ACL policy (Allow or Deny) applied to this ACL rule.
ACL Name	testacl	The name of the corresponding ACL rule.
Details	traffic:allow MGMT/LAN/WAN interface	The incoming network interface traffic passes through.

Table of Log Formats

The following table describes names and values for each log:

System Logs	Web Firewall Logs	Access Logs	Audit Logs	Network Firewall Logs
%ei - Event ID	%ai - Service IP	%ai - Service IP	%add - Additional Data	%acl - ACL ID
%ll - Log Level	%ap - Service Port	%ap - Service Port	%an - Admin Name	%act - Action ID
%lt - Log Type	%at - Action	%au - Authenticated User	%cht - Change Type	%dsc - Details

%un - Unit Name	%ad - Attack Type	%br - Bytes Received	%ct - Client Type	%di - Destination IP
%ms - Message	%adl - Attack Details	%bs - Bytes Sent	%cn - Command Name	%dp - Destination Port
%md - Module Name	%ag - Attack Group	%ch - Cache Hit	%li - Login IP	%lt - Log Type
%t - Time	%aid - Attack ID	%cu - Certificate User	%lp - Login Port	%p - Protocol
%tarc - Epoch/Unix Time Stamp	%au - Authenticated User	%ci - Client IP	%lt - Login Type	%srci - Source IP
%uid - Unique ID	%ci - Client IP	%cp - Client Port	%nv - New Value	%srcp - Source Port
%ta - American Standard Format Timestamp	%cp - Client Port	%c - Cookie	%on - Object Name	%sl - Severity
	%fa - Follow-up Action	%ct - Client Type	%ot - Object Type	%t - Time
	%lt - Log Type	%cs1 - Custom Header 1	%ov - Old Value	%tarc - Epoch/Unix Time Stamp
	%m - Method	%cs2 - Custom Header 2	%t - Time	%un - Unit Name
	%p - Protocol	%cs3 - Custom Header 3	%tri - Transaction ID	%uid - Unique ID
	%px - Proxy IP	%h - Host	%trt - Transaction Type	%ta - American Standard Format Timestamp
	%pp - Proxy Port	%s - HTTP Status	%un - Unit Name	%cc - Country Code
	%r - Referer	%id - Login ID	%var - Variable	
	%ri - Rule ID	%lt - Log Type	%tarc - Epoch/Unix Time Stamp	
	%rt - Rule Type	%m - Method	%uid - Unique ID	
	%sid - Session ID	%p - Protocol	%ar - Admin Role	
	%sl - Severity	%pf - Protected	%ta - American Standard Format Timestamp	
	%t - Time	%px - Proxy IP		
	%u - URL	%pmf - Profile Matched		

	%ua - User Agent	%pp - Proxy Port		
	%un - Unit Name	%q - Query String		
	%tarc - Epoch/Unix Time Stamp	%r - Referer		
	%uid - Unique ID	%rtf - Response Type		
	%ta - American Standard Format Timestamp	%sid - Session ID		
	%cfp - Client Fingerprint	%si - Server IP		
	%rrs - Request Risk Score	%sp - Server Port		
	%crs -Client Risk Score	%st - Server Time		
	%cc - Country Code	%t - Time		
		%tt - Time Taken		
		%u - URL		
		%ua - User Agent		
		%un - Unit Name		
		%uid - Unique ID		
		%v - Version		
		%wmf - WF Matched		
		%tarc - Epoch/Unix Time Stamp		
		%ta - American Standard Format Timestamp		
		%cfp - Client Fingerprint		
		%rrs - Request Risk Score		
		%crs -Client Risk Score		
		%cc - Country Code		