Custom Reports - Field Descriptions

https://campus.barracuda.com/doc/96025094/

Firewall Activity Log

Field	Description	Value	Comment
Application	Detected application	string	Application detection must be active.
Application Protocols	Detected application protocol (e.g.: ["HTTPS direct", "HTTPS", “DNS”]	string	
Application Rule	Application rule name (e.g.: "<App>:ALL-APPS")	string	
Contents	Detected content types. (e.g.: ["HTML", "Web Files"]	string	
Destination Interface	Destination interface name (e.g.: ‘’ eth1 ‘’)	string	
Destination IP	Destination IP address	string	
Destination GeoIP	Destination country (e.g.: “US”)	string	
Destination GeoLatitude	Destination coordinates latitude (e.g.: «-98.4935»)	numeric	
Destination GeoLongitude	Destination coordinates longitude (e.g.: «52.152.11»)	numeric	
Destination NAT IP	Destination NAT	string	
Destination MAC	Mac address of destination	string	
Destination Port	Destination port	numeric	
Duration	Duration in milliseconds	numeric	See more details on browse time.
Forwarded Bytes	Number of bytes sent in the session's forward direction	numeric	In bytes
Forwarded Packets	Number of packets sent in the session's forward direction	numeric	
Firewall Info	Detailed information about the action performed by the firewall ACPF ID.	string	See details on Filebeat description.
Firewall Rule	Matching firewall rule name	string	
Serial/Device	Firewall name (e.g.: “1-HQ-HQ-CGF1”)	string	
Source Interface	Source interface name (e.g.: ‘’ eth1‘’)	string	

Source IP	Source IP address	string	
Source GeoIP	Source country (e.g.: “US”)	string	
Source GeoLatitude	Source coordinates latitude (e.g.: «-98.4935»)	numeric	
Source GeoLongitude	Source coordinates longitude (e.g.: «52.152.11»)	numeric	
Source MAC	MAC address of the source	string	
Source Port	Source port	numeric	
Source NAT IP	Source NAT IP	string	
Received Bytes	Number of bytes received in the session's forward direction	numeric	
Received Packets	Number of packets received in the session's forward direction	numeric	
Timestamp / Date	Date (e.g.: “2021-12-27 14:16:48+00:00”)	numeric	
User	Username if available	string	

Web Messages

(type = ngfw-wf)

Field	Description	Value	Comment
Action	Action performed on the firewall “Allow” or “Block”	numeric	Allow = 0, Block =1
Application Rule	Application rule name (e.g.: "<App>:ALL-APPS")	string	
Category	Web category (e.g.: “Computing & Technology”)	string	
Content Type	The content-type response header field	string	
Destination GeoIP	Destination country (e.g.: “US”)	string	
Destination GeoLatitude	Destination coordinates latitude (e.g.: «-98.4935»)	numeric	
Destination GeoLongitude	Destination coordinates longitude (e.g.: «52.152.11»)	numeric	
Destination Port	Destination port	numeric	

Domain	The "Referer" request header field or the host part of the request URI	string	Can be compared to URL to verify if the site was requested directly or through a link from other website site.
Firewall Rule	Matching firewall rule name	string	
Method	The method of the request (e.g.: "GET", "POST", "PUT", "CONNECT")	string	
Size	The content-length response header field	numeric	
Serial/Device	Firewall name (e.g.: “1-HQ-HQ-CGF1”)	string	
Source IP	Source IP address	string	
Source GeoIP	Source country (e.g.: “US”)	string	
Source GeoLatitude	Source coordinates latitude (e.g.: «-98.4935»)	numeric	
Source GeoLongitude	Source coordinates longitude (e.g.: «52.152.11»)	numeric	
Source Port	Source port	numeric	
Status Code	The HTTP status code of the response	numeric	
Super Category	Web general category (e.g.: “Technology”)	string	
Timestamp / Date	Date (e.g.: “2021-12-27 14:16:48+00:00”)	numeric	
Traffic Type	N/A always 0	numeric	
URI (Name)	Name (full URI request)	string	
URL	Reserved for future use	string	
User	The username of the user performing the request or source IP address of the request	string	
User Agent	User agent	string	
User Type	1 if "user" is a username 0 if "user" is an IP address	numeric	

Threat Log

Field	Description	Value	Comment
Application Target	Detected application	string	Application detection must be active.

Component	Reserved for future use (“firewall”)	string	
Description	Description of the threat (e.g.: “ ID: 1059898 EXPLOIT Generic HTML Threat -21 ")	string	
Destination IP	Destination IP address	string	
Destination GeoIP	Destination country (e.g.: “US”)	string	
Destination GeoLatitude	Destination coordinates latitude (e.g.: «-98.4935»)	numeric	
Destination GeoLongitude	Destination coordinates longitude (e.g.: «52.152.11»)	numeric	
IPS Category	The category of an IPS hit (e.g.: “Web Attack”)	string	**Only present for IPS hits.**
Operation	The operation that has been performed by the firewall (e.g.: “Allow”, “Block”)	string	
Port	Destination port	numeric	
Severity	Duration in milliseconds	string	
Serial/Device	Firewall name (e.g.: “1-HQ-HQ-CGF1”)	string	
Source IP	Source IP address	string	
Source GeoIP	Source country (e.g.: “US”)	string	
Source GeoLatitude	Source coordinates latitude (e.g.: «-98.4935»)	numeric	
Source GeoLongitude	Source coordinates longitude (e.g.: «52.152.11»)	numeric	
Threat Severity	A number representing the severity of the threat .	numeric	“0”= Info “1”=Low “2”=Medium “3”= High
Time Zone	Time zone (e.g.: +02:00)	string	
Transport Protocol	Transport protocol of the session that caused the threat hit (e.g.: “TCP”, “UDP”)	string	
Timestamp / Date	Date (e.g.: “2021-12-27 14:16:48+00:00”)	numeric	
Type	Type of threat (e.g.: “Virus”, “ATD”, “IPS”, “Reputation”, ….)	string	
User	Username if available	string	

SD WAN Tunnels

Field	Description	Value	Comment
Geo Latitude	Coordinates latitude (e.g.: «-98.4935»)	numeric	
Geo Longitude	Coordinates longitude (e.g.: «52.152.11»)	numeric	
Serial/Device	Firewall name (e.g.: “1-HQ-HQ-CGF1”)	string	
Timestamp / Date	Date (e.g.: “2021-12-27 14:16:48+00:00”)	numeric	
Tunnelname	Tunnel name including TI ID (e.g.: “FW2FW-1-HQ-BO:9”)	string	
Tunnelstate	Tunnel state (e.g.: “OK”, “ERROR”)	string	
Effective Bandwidth Upstream min.	Effective bandwidth upstream minimum (bit/s)	numeric	
Effective Bandwidth Upstream avg.	Effective bandwidth upstream average (bit/s)	numeric	
Effective Bandwidth Upstream max.	Effective bandwidth upstream maximum (bit/s)	numeric	
Effective Bandwidth Downstream min.	Effective bandwidth downstream minimum (bit/s)	numeric	
Effective Bandwidth Downstream avg.	Effective bandwidth downstream average (bit/s)	numeric	
Effective Bandwidth Downstream max.	Effective bandwidth downstream maximum (bit/s)	numeric	
Latency min.	Latency minimum (ms)	numeric	
Latency avg.	Latency average (ms)	numeric	
Latency max.	Latency maximum (ms)	numeric	
Usage Standard Upstream min.	Usage standard upstream minimum (bytes)	numeric	
Usage Standard Upstream avg.	Usage standard upstream average (bytes)	numeric	
Usage Standard Upstream max.	Usage standard upstream minimum (bytes)	numeric	
Usage Standard Downstream min.	Usage standard downstream minimum (bytes)	numeric	
Usage Standard Downstream avg.	Usage standard downstream average (bytes)	numeric	
Usage Standard Downstream max.	Usage standard downstream maximum (bytes)	numeric	
Usage NoDelay Upstream min.	Usage NoDelay upstream minimum (bytes)	numeric	
Usage NoDelay Upstream min.	Usage NoDelay upstream average (bytes)	numeric	
Usage NoDelay Upstream min.	Usage NoDelay upstream maximum (bytes)	numeric	
Usage NoDelay Downstream min.	Usage NoDelay downstream minimum (bytes)	numeric	
Usage NoDelay Downstream avg.	Usage NoDelay downstream average (bytes)	numeric	
Usage NoDelay Downstream max.	Usage NoDelay downstream maximum (bytes)	numeric	

SD WAN Tunnels Applications and Protocols

Field	Description	Value	Comment
Application	Detected application	string	Application detection must be active.
Protocols	Detected application protocol (e.g.: ["HTTPS direct", "HTTPS", “DNS”]	string	
Inbound Bytes	Inbound traffic in bytes	numeric	
Outbound Bytes	Outbound traffic in bytes	numeric	
Serial/Device	Firewall name (e.g.: “1-HQ-HQ-CGF1”)	string	
Timestamp / Date	Date (e.g.: “2021-12-27 14:16:48+00:00”)	numeric	
Tunnelname	Tunnel name including TI ID (e.g.: “FW2FW-BO1-CGF1-HQ-CGF1:9”)	string	