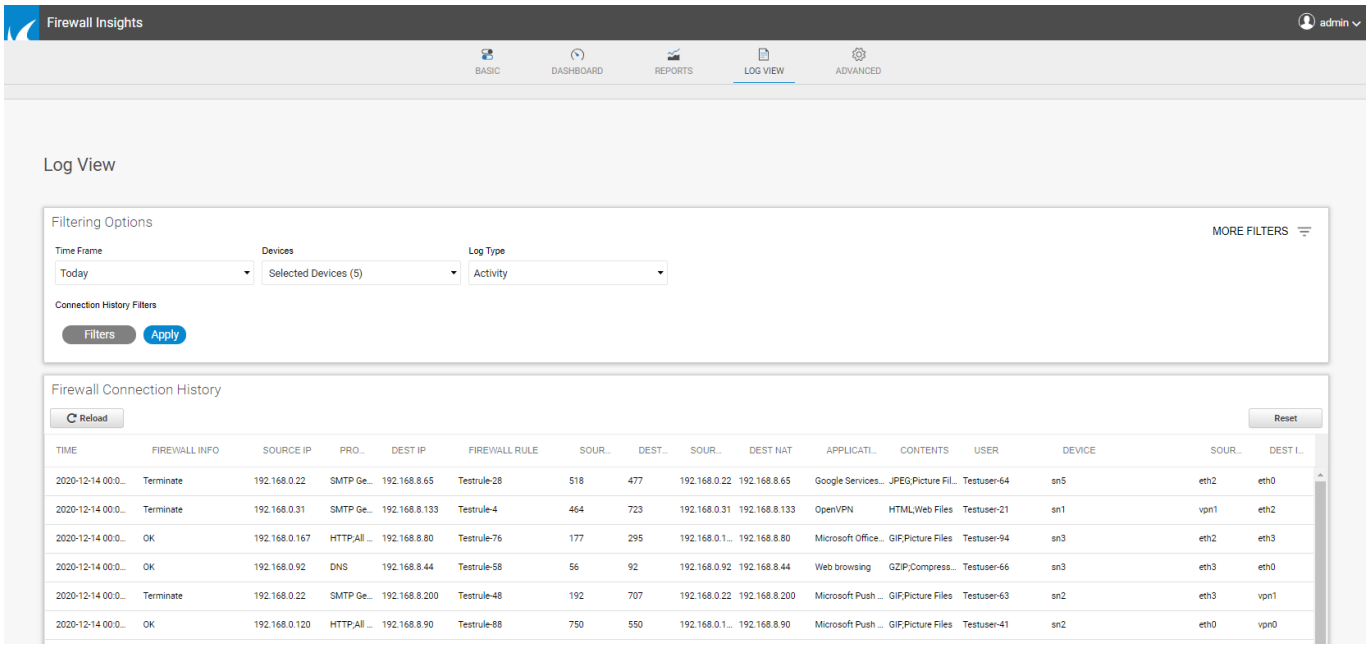
Log View

https://campus.barracuda.com/doc/86544280/

The **Log View** tab allows you to centrally view and filter the events of the activity and threat log of every connected CloudGen Firewall, thereby helping you to keep track of both actions performed by the firewall devices and threats. Use various filters, as described below, to tailor the information to your needs.



The information on the **Log View** page is divided into columns. To expand the view, drag the column header. You can also delete columns by clicking the delete icon (**x**) to the right of the header.

Accessing Firewall Information

The **FIREWALL INFO** column in the log window provides the following details related to access and application rules configured on firewalls:

- **OK** – Normal operation
- **Fail** – Connection failed
- **Terminate** – Connection terminated
- **Drop** – Packet dropped
- **Block** – Connection blocked
- **Deny** – Connection denied
- **Scan** – Scan performed
- **Application Block** – Application blocked

Expand the following section for detailed information:

1. Generic/Normal Operation (0 - 999)

2. ACPF_REASON_NORMAL_OP 0
3. ACPF_REASON_NEW_REQUEST 1
4. ACPF_REASON_MAC_CHANGED 2
5. ACPF_REASON_ARP_DUPLICATE 3
6. ACPF_REASON_SYNC 4
7. ACPF_REASON_REEVALUATE 5
8. ACPF_REASON_APP_ALLOW 6
9. ACPF_REASON_CONTENT_ALLOW 7
10. ACPF_REASON_CONTENT_WARN 8

10. Failed (1000 - 1999)

11. ACPF_REASON_FAIL_ICMP_BASE 1000
12. ACPF_REASON_FAIL_UNREACHABLE_NET 1000
13. ACPF_REASON_FAIL_UNREACHABLE_HOST 1001
14. ACPF_REASON_FAIL_UNREACHABLE_PROTO 1002
15. ACPF_REASON_FAIL_UNREACHABLE_PORT 1003
16. ACPF_REASON_FAIL_UNREACHABLE_FRAG 1004
17. ACPF_REASON_FAIL_UNREACHABLE_SR 1005
18. ACPF_REASON_FAIL_UNREACHABLE_NO_NET 1006
19. ACPF_REASON_FAIL_UNREACHABLE_NO_HOST 1007
20. ACPF_REASON_FAIL_UNREACHABLE_ISOLATED 1008
21. ACPF_REASON_FAIL_UNREACHABLE_NET_DENY 1009
22. ACPF_REASON_FAIL_UNREACHABLE_HOST_DENY 1010
23. ACPF_REASON_FAIL_UNREACHABLE_TOS_NET 1011
24. ACPF_REASON_FAIL_UNREACHABLE_TOS_HOST 1012
25. ACPF_REASON_FAIL_UNREACHABLE_FILTER 1013
26. ACPF_REASON_FAIL_UNREACHABLE_PRECEDENCE1 1014
27. ACPF_REASON_FAIL_UNREACHABLE_PRECEDENCE2 1015
28. ACPF_REASON_FAIL_TIMEOUT_CONNECT 1016
29. ACPF_REASON_FAIL_TIMEOUT_ACCEPT 1017
30. ACPF_REASON_FAIL_NO_ROUTE 1018
31. ACPF_REASON_FAIL_UNKNOWN 1019
32. ACPF_REASON_FAIL_ROUTE_TRIANGLE 1020
33. ACPF_REASON_FAIL_TTL_EXPIRED 1021
34. ACPF_REASON_FAIL_FRAGTIME 1022
35. ACPF6_REASON_FAIL_ICMPV6_BASE 1023
36. ACPF6_REASON_FAIL_NO_ROUTE_TO_DEST 1023
37. ACPF6_REASON_FAIL_COMM_PROHIBITED 1024
38. ACPF6_REASON_FAIL_UNKNOWN_2 1025
39. ACPF6_REASON_FAIL_ADDRESS_UNREACHABLE 1026

40. ACPF6_REASON_FAIL_PORT_UNREACHABLE 1027
41. ACPF_REASON_FAIL_WANOPT_MISMATCH 1028
42. ACPF_REASON_FAIL_WANOPT_OUT_OF_DESC 1029
43. ACPF_REASON_FAIL_WANOPT_PARTNER_WPROTO_MISSING 1030
44. ACPF_REASON_FAIL_WANOPT_NO_VPN 1031
45. ACPF_REASON_FAIL_SSL_ERROR 1032
46. ACPF_REASON_FAIL_SSL_SELF 1033
47. ACPF_REASON_FAIL_SSL_ISSUER 1034
48. ACPF_REASON_FAIL_SSL_REVOKED 1035
49. ACPF_REASON_FAIL_SSL_EXPIRED 1036
50. ACPF_REASON_FAIL_SSL_INVALID 1037
51. ACPF_REASON_FAIL_SSL_REV_FAILED 1038
52. ACPF_REASON_FAIL_FLEX_TIMEOUT 1039
53. ACPF_REASON_FAIL_FLEX_ERROR 1040
ACPF_REASON_FAIL_MEM_FAIL_CLOSE 1041

54. Terminated (2000 - 2999)

55. ACPF_REASON_TERM_TIMEOUT_SESSION 2000
56. ACPF_REASON_TERM_TIMEOUT_BALANCED 2001
57. ACPF_REASON_TERM_TIMEOUT_LASTACK 2002
58. ACPF_REASON_TERM_TIMEOUT_RETRANS 2003
59. ACPF_REASON_TERM_TIMEOUT_HALFSIDE 2004
60. ACPF_REASON_TERM_TIMEOUT_UNREACHABLE 2005
61. ACPF_REASON_TERM_CONN_CLOSE 2006
62. ACPF_REASON_TERM_CONN_RESET_SRC 2007
63. ACPF_REASON_TERM_CONN_RESET_DST 2008
64. ACPF_REASON_TERM_ADMIN_TERMINATE 2009
65. ACPF_REASON_TERM_TIME_MISMATCH 2010
66. ACPF_REASON_TERM_RULE_BLOCK 2011
67. ACPF_REASON_TERM_DYN_RULE_EXPIRED 2012
68. ACPF_REASON_TERM_CONTENT 2013
69. ACPF_REASON_TERM_IS_LOCAL 2014
70. ACPF_REASON_TERM_PASSIVE_SYNC 2015
71. ACPF_REASON_TERM_DEVICE_DOWN 2016
72. ACPF_REASON_TERM_DYN_SERVICE 2017
73. ACPF_REASON_TERM_DURATION 2018
74. ACPF_REASON_TERM_P2P 2019
75. ACPF_REASON_TERM_PROTO_DETECT 2020
76. ACPF_REASON_TERM_IPS_DETECT 2021
77. ACPF_REASON_TERM_WANOPT_FAIL 2022
78. ACPF_REASON_TERM_PROTO_DETECT_UNKNOWN 2023
79. ACPF_REASON_TERM_DYNAMIC_MESH 2024
80. ACPF_REASON_TERM_SSL_ERROR 2025
81. ACPF_REASON_TERM_SSL_SELF 2026

82. ACPF_REASON_TERM_SSL_ISSUER 2027
83. ACPF_REASON_TERM_SSL_REVOKED 2028
84. ACPF_REASON_TERM_SSL_NOVALIDATE 2029
85. ACPF_REASON_TERM_NO_LOCAL_SOCK 2030
86. ACPF_REASON_TERM_MEM_FAIL_CLOSE 2031
87.

88. Packet Dropped (3000 - 3999)

89. ACPF_REASON_DROP_MISMATCH_MAC 3000
90. ACPF_REASON_DROP_MISMATCH_IF 3001
91. ACPF_REASON_DROP_SOURCE_MC 3002
92. ACPF_REASON_DROP_SOURCE_BC 3003
93. ACPF_REASON_DROP_SOURCE_BADCLASS 3004
94. ACPF_REASON_DROP_SOURCE_LOOPBACK 3005
95. ACPF_REASON_DROP_SOURCE_LOCAL 3006
96. ACPF_REASON_DROP_IPHDR_INCOMPLETE 3007
97. ACPF_REASON_DROP_IPHDR_VERSION 3008
98. ACPF_REASON_DROP_IPHDR_CHECKSUM 3009
99. ACPF_REASON_DROP_IPHDR_INVOPT 3010
100. ACPF_REASON_DROP_SOURCE_ROUTE 3011
101. ACPF_REASON_DROP_PKT_INCOMPLETE 3012
102. ACPF_REASON_DROP_TCP_HDR_INCOMPLETE 3013
103. ACPF_REASON_DROP_TCP_HDR_CHECKSUM 3014
104. ACPF_REASON_DROP_TCP_INVALID_COOKIE 3015
105. ACPF_REASON_DROP_TCP_INVALID_SEQ 3016
106. ACPF_REASON_DROP_TCP_INVALID_ACK 3017
107. ACPF_REASON_DROP_TCP_INVALID_OPT 3018
108. ACPF_REASON_DROP_TCP_INVALID_FLAGS 3019
109. ACPF_REASON_DROP_TCP_NO_SESSION 3020
110. ACPF_REASON_DROP_UDP_HDR_INCOMPLETE 3021
111. ACPF_REASON_DROP_UDP_HDR_CHECKSUM 3022
112. ACPF_REASON_DROP_ICMP_HDR_INCOMPLETE 3023
113. ACPF_REASON_DROP_ICMP_HDR_CHECKSUM 3024
114. ACPF_REASON_DROP_ICMP_HDR_INV_TYPE 3025
115. ACPF_REASON_DROP_ICMP_NO_REQUEST 3026
116. ACPF_REASON_DROP_NO_SOCKET 3027
117. ACPF_REASON_DROP_NO_FWD 3028
118. ACPF_REASON_DROP_NO_DEVICE 3029
119. ACPF_REASON_DROP_ARP_DEVICE_MISMATCH 3030
120. ACPF_REASON_DROP_ARP_MULTIPLE 3031
121. ACPF_REASON_DROP_LIMIT_SIZE 3032
122. ACPF_REASON_DROP_LIMIT_RATE 3033
123. ACPF_REASON_DROP_TTL_EXPIRED 3034
124. ACPF_REASON_DROP_ARP_INV_OP 3035

125. ACPF_REASON_DROP_ICMP_NO_SESSION 3036
126. ACPF_REASON_DROP_ICMP_IGNORE 3037
127. ACPF_REASON_DROP_ICMP_RULE_DROP 3038
128. ACPF_REASON_DROP_HIPROTO_HDR_INCOMPLETE 3039
129. ACPF_REASON_DROP_HIPROTO_HDR_INVALID 3040
130. ACPF_REASON_DROP_HIPROTO_HDR_VERSION 3041
131. ACPF_REASON_DROP_HIPROTO_PKT_INCOMPLETE 3042
132. ACPF_REASON_DROP_HIPROTO_PKT_INVALID 3043
133. ACPF_REASON_DROP_MISMATCH_MAC_SRC 3044
134. ACPF_REASON_DROP_MISMATCH_MAC_DST 3045
135. ACPF_REASON_DROP_BRIDGE_ACL 3046
136. ACPF_REASON_DROP_ARP_BURST 3047
137. ACPF_REASON_DROP_STATIC_BARP 3048
138. ACPF_REASON_DROP_LOCKED_BARP 3049
139. ACPF_REASON_DROP_BRIDGE_MAC_SPOOFING 3050
140. ACPF_REASON_DROP_BRIDGE_NO_NEXTHOP 3051
141. ACPF_REASON_DROP_DECOMPRESS_FAIL 3052
142. ACPF_REASON_DROP_SESSION_LOAD_EXCEEDED 3053
143. ACPF_REASON_DROP_QARP_UPDATE_FAILED 3054
144. ACPF_REASON_DROP_QARP_ROUTE_LOOKUP_FAILED 3055
145. ACPF_REASON_DROP_QARP_GROUP_MISMATCH 3056
146. ACPF_REASON_DROP_QARP_MISMATCH 3057
147. ACPF_REASON_DROP_TCP_GUESSED_RST 3058
148. ACPF_REASON_DROP_TCP_INVALID_SYN 3059
149. ACPF_REASON_DROP_EXCEED_MTU 3060
150. ACPF_REASON_DROP_SRA_FUTURE_ACK 3061
151. ACPF_REASON_DROP_IPV6_UNSUPPORTED_HDR 3062
152. ACPF_REASON_DROP_NO_RULESET 3063
153. ACPF_REASON_DROP_SRC_BARP_UNKNOWN 3064
154. ACPF_REASON_DROP_SRCDST_BARP_SAME_DEV 3065
155. ACPF_REASON_DROP_OTHERHOST 3066
156. ACPF_REASON_DROP_NOT_ACTIVE 3067
157. ACPF_REASON_DROP_LINEARIZATION_FAILED 3068
158. ACPF_REASON_DROP_REEVALUATION_FAILED 3069
159. ACPF_REASON_DROP_UNKNOWN_FRAGMENT 3070
160. ACPF_REASON_DROP_BRIDGE_LOOP 3071
161. ACPF_REASON_DROP_RSTP_DISCARD 3072
162. ACPF_REASON_DROP_SYN_WITH_PAYLOAD 3073
ACPF_REASON_DROP_INVALID_URG_PTR 3074

163. Blocked (4000 - 4999) and Application Blocked (7000 - 7999)

164. ACPF_REASON_BLOCK_UNKNOWN 4000
165. ACPF_REASON_BLOCK_NO_FWD 4001
166. ACPF_REASON_BLOCK_RULE_EXPLICIT 4002

167. ACPF_REASON_BLOCK_RULE_NOMATCH 4003 // permanent
168. ACPF_REASON_BLOCK_RULE_SRC_MISMATCH 4004 // permanent
169. ACPF_REASON_BLOCK_RULE_DST_MISMATCH 4005 // permanent
170. ACPF_REASON_BLOCK_RULE_SRV_MISMATCH 4006 // permanent
171. ACPF_REASON_BLOCK_RULE_TIME_MISMATCH 4007 // permanent
172. ACPF_REASON_BLOCK_RULE_IF_MISMATCH 4008 // permanent
173. ACPF_REASON_BLOCK_RULE_LOCAL_LOOP 4009 // permanent
174. ACPF_REASON_BLOCK_RULE_ACL 4010 // adjust ACPF_REASON_BLOCK_RULE_ACL when inserting
175. ACPF_REASON_BLOCK_LIMIT_RULE 4011
176. ACPF_REASON_BLOCK_LIMIT_SRC 4012
177. ACPF_REASON_BLOCK_LIMIT_PENDING 4013
178. ACPF_REASON_BLOCK_LIMIT_SIZE 4014
179. ACPF_REASON_BLOCK_DYN_RULE 4015
180. ACPF_REASON_BLOCK_NO_NAT 4016
181. ACPF_REASON_BLOCK_BROADCAST 4017
182. ACPF_REASON_BLOCK_MULTICAST 4018
183. ACPF_REASON_BLOCK_LIMIT_ALL_SRC 4019
184. ACPF_REASON_BLOCK_LIMIT_UDP 4020
185. ACPF_REASON_BLOCK_LIMIT_UDP_SRC 4021
186. ACPF_REASON_BLOCK_LIMIT_ECHO 4022
187. ACPF_REASON_BLOCK_LIMIT_ECHO_SRC 4023
188. ACPF_REASON_BLOCK_LIMIT_OTHER 4024
189. ACPF_REASON_BLOCK_LIMIT_OTHER_SRC 4025
190. ACPF_REASON_BLOCK_LIMIT_TOTAL 4026
191. ACPF_REASON_BLOCK_NO_ROUTE 4027
192. ACPF_REASON_BLOCK_INVALID_PROTO 4028
193. ACPF_REASON_BLOCK_LIMIT_LICENSE 4029
194. ACPF_REASON_BLOCK_NO_DEVICE 4030
195. ACPF_REASON_BLOCK_RULE_USER_MISMATCH 4031
196. ACPF_REASON_BLOCK_BRIDGE_NO_BARP 4032
197. ACPF_REASON_BLOCK_RULE_MAC_MISMATCH 4033
198. ACPF_REASON_BLOCK_AUTH_REQUIRED 4034
199. ACPF_REASON_BLOCK_NO_LOCAL_ADDRESS 4035
200. ACPF_REASON_BLOCK_REDIR_TO_LOCAL_ADDR 4036
201. ACPF_REASON_BLOCK_SLOT_CREATE_FAILED 4037
202. ACPF_REASON_BLOCK_RULE_QCLASS_MISMATCH 4038
203. ACPF_REASON_BLOCK_V6_LOCAL_BLOCKED 4039
204. ACPF_REASON_BLOCK_WANOPT_MISMACTH 4040
205. ACPF_REASON_BLOCK_RULE_APP_MISMATCH 4041
206. ACPF_REASON_BLOCK_URLCAT_NA_POLICY 4042
207. ACPF_REASON_BLOCK_URLCAT_BLOCK_CUSTOM 4043
208. ACPF_REASON_BLOCK_URLCAT_BLOCK_WHITE 4044
209. ACPF_REASON_BLOCK_URLCAT_BLOCK_BLACK 4045
210. ACPF_REASON_BLOCK_ATD_RULE 4046
211. ACPF_REASON_BLOCK_ATD_ASYNC_HASH 4047

```
212. ACPF_REASON_BLOCK_URLCAT_WARN_NA_POLICY 4048
213. ACPF_REASON_BLOCK_URLCAT_WARN 4049
214. ACPF_REASON_BLOCK_URLCAT_WARN_CUSTOM 4050
215. ACPF_REASON_BLOCK_URLCAT_OVERRIDE 4051
216. ACPF_REASON_BLOCK_CONTENT 4052
217. ACPF_REASON_BLOCK_AGENT 4053
218. ACPF_REASON_BLOCK_SSL_SELF 4054
219. ACPF_REASON_BLOCK_SSL_ISSUER 4055
220. ACPF_REASON_BLOCK_SSL_REVOKED 4056
221. ACPF_REASON_BLOCK_SSL_EXPIRED 4057
222. ACPF_REASON_BLOCK_SSL_INVALID 4058
223. ACPF_REASON_BLOCK_SSL_REV_FAILED 4059
224. ACPF_REASON_BLOCK_UNKNOWN_VRF 4060
225.
226. ACPF_REASON_APPBLOCK_UNKNOWN 7000
... identical to ACPF_REASON_BLOCK ...
```

227. Denied (5000 - 5999)

```
228. ACPF_REASON_DENY_UNKNOWN 5000
229. ACPF_REASON_DENY_RULE_EXPLICIT 5001
230. ACPF_REASON_DENY_RULE_SRC_MISMATCH 5002 // permanent
231. ACPF_REASON_DENY_RULE_DST_MISMATCH 5003 // permanent
232. ACPF_REASON_DENY_RULE_SRV_MISMATCH 5004 // permanent
233. ACPF_REASON_DENY_RULE_TIME_MISMATCH 5005 // permanent
234. ACPF_REASON_DENY_RULE_LOCAL_LOOP 5006 // permanent
235. ACPF_REASON_DENY_RULE_ACL 5007 // permanent
236. ACPF_REASON_DENY_DYN_RULE 5008
ACPF_REASON_DENY_NO_NAT 5009
```

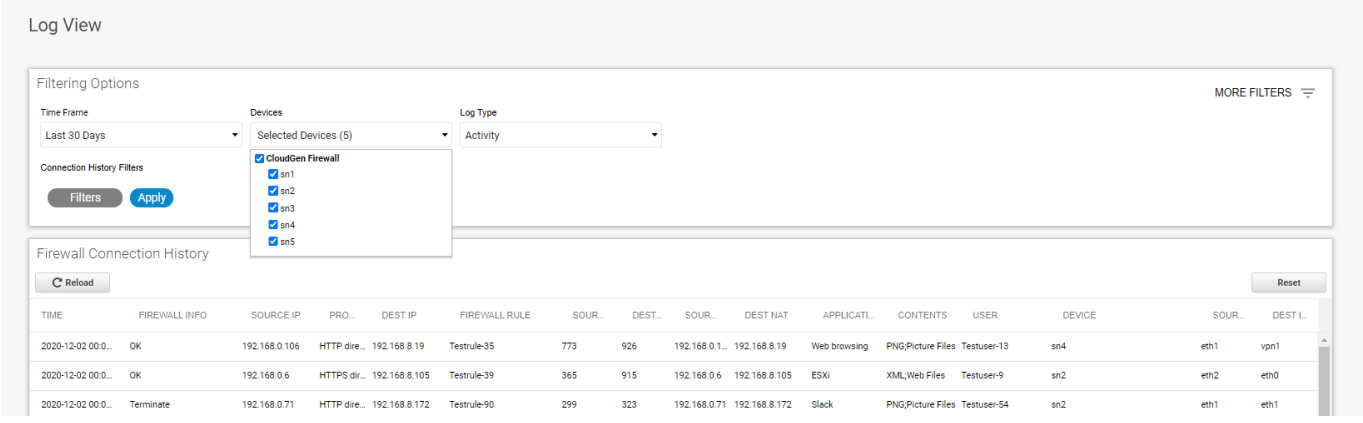
237. Scanned (6000 - 6999)

```
238. ACPF_REASON_SCAN_UNKNOWN 6000
239. ACPF_REASON_SCAN_PATTERN_TERM 6001
240. ACPF_REASON_SCAN_PATTERN_LOG 6002
241. ACPF_REASON_SCAN_P2P_LOG 6003
242. ACPF_REASON_SCAN_P2P_DROP 6004
243. ACPF_REASON_SCAN_P2P_SHAPE 6005
244. ACPF_REASON_SCAN_PROTO_LOG 6006
245. ACPF_REASON_SCAN_PROTO_RESET 6007
246. ACPF_REASON_SCAN_PROTO_DROP 6008
247. ACPF_REASON_SCAN_IPS_LOG 6009
248. ACPF_REASON_SCAN_IPS_LOG_WARN 6010
249. ACPF_REASON_SCAN_IPS_LOG_ALERT 6011
250. ACPF_REASON_SCAN_IPS_DROP 6012
```

```
251. ACPF_REASON_SCAN_IPS_DROP_WARN 6013
252. ACPF_REASON_SCAN_IPS_DROP_ALERT 6014
253. ACPF_REASON_SCAN_WEB_ACCESS 6015
254. ACPF_REASON_SCAN_APP_DETECT 6016
255. ACPF_REASON_SCAN_APP_WARN 6017
256. ACPF_REASON_SCAN_APP_ALERT 6018
257. ACPF_REASON_SCAN_APP_DROP 6019
258. ACPF_REASON_SCAN_APP_DROP_WARN 6020
259. ACPF_REASON_SCAN_APP_DROP_ALERT 6021
260. ACPF_REASON_SCAN_URLCAT_DETECT 6022
261. ACPF_REASON_SCAN_URLCAT_WARN 6023
262. ACPF_REASON_SCAN_URLCAT_ALERT 6024
263. ACPF_REASON_SCAN_URLCAT_DROP 6025
264. ACPF_REASON_SCAN_URLCAT_DROP_WARN 6026
265. ACPF_REASON_SCAN_URLCAT_DROP_ALERT 6027
266. ACPF_REASON_SCAN_VIRUS_DETECT 6028
267. ACPF_REASON_SCAN_VIRUS_DETECT_ATD 6029
268. ACPF_REASON_SCAN_NOT_POSSIBLE_CLOSE 6030
269. ACPF_REASON_SCAN_NOT_POSSIBLE_OPEN 6031
270. ACPF_REASON_SCAN_ERROR_CLOSE 6032
271. ACPF_REASON_SCAN_ERROR_OPEN 6033
272. ACPF_REASON_SCAN_VIRUS_DETECT_ATD_DELIVERED 6034
273. ACPF_REASON_SCAN_REPU_DNS_REQ 6035
274. ACPF_REASON_SCAN_REPU_SINKHOLE_ACCESS 6036
275. ACPF_REASON_SCAN_REPU_HOSTNAME_ACCESS 6037
276.
```

Display the Information Using Filters

To show events, go to **LOG VIEW**, and click **MORE FILTERS** on the top right.



The following filters are available:

- **Time Frame** – Either choose a time frame from the drop-down menu to specify the time frame you want to show the data for, or specify a custom time frame. For a custom time frame, choose **Custom** from the drop-down menu, and enter the start and end date next to **Start** and **End**.
- **Devices** – Select the devices you want to show the logs for.
- **Log Type** – Choose between **Threats / Webfilter** and **Firewall Connection History** from the drop-down menu.

Additional Filters

Use the additional filters to narrow down the selection according to different criteria such as source, destination, protocol, and/or extended box descriptors. Filters are case insensitive and dependent on the field type. Wildcards are supported for all filter operators except **IP Protocol**, which only supports the equals (=) and not equals (≠) operators.

String/Text Fields

String/text fields (e.g., Firewall Rule, User, etc.) are case insensitive and dependent on the field type. Wildcards are supported for all operators. * or % indicates any quantity of bytes (including zero characters), so, in principle, 0-n characters. ? or _ indicates any one byte., in other words, exactly one character.

Examples:

- ex*e will match 'Example', as does e%m%
- examp?e will match 'Example', but ex_le will not match 'Example'

When you choose the equals operator (=) and enter `Null` as filter value, the field is not checked for the string 'Null', but if the field is Null.
For example, if you choose `Firewall Rule = NULL` as filter, it is checked if fw_rule IS NULL.
You can also choose the 'not equals' operator (≠) and enter `Null` (or `null`) as filter value. In this case, it is checked if the field is not null (e.g., fw_rule IS NOT NULL).

For string fields, the supported filters are as follows:

Filter	Description
equals (=)	Value must exactly match the filter (when no wildcards are used).
not equals (≠)	Value does not exactly match the filter (when no wildcards are used).
contains	Value contains the filter, e.g., 'example' contains the string 'xam'.

not contains	Value does not contain the filter, e.g., 'example' does not contain the string 'hello'.
starts with	Value must start with the filter, e.g., 'example' starts with 'exam'. This can also be achieved when using the equals operator with the * wildcard, e.g., `exam*`.
ends with	Value must end with the filter, e.g., 'example' ends with 'mple'. This can also be achieved when using the equals operator with the * wildcard, e.g., `*mple`.

Number Fields

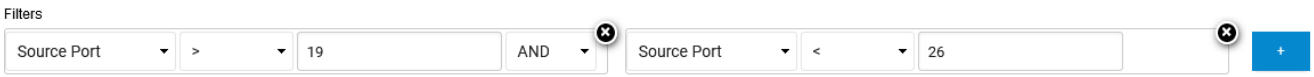
Number fields (e.g., Port, Threat Severity, etc.) support only positive integer values, such as '1', '73', '8323', etc, but not '-12' or '7.3' or '8,2'. No wild cards are allowed. Checking for NULL/IS NOT NULL is possible when using the equals or not equals operator (see above section).

For number fields, the supporting filters are as follows:

Filter	Description
equals (=)	Value must exactly match the filter.
not equals (≠)	Value does not exactly match the filter.
greater than (>)	Value is greater than the filter.
less than (<)	Value is less than the filter.

A 'between' can be put into effect when using 'greater than' and 'less than' connected with an 'AND' conjunction (and one or two equals if you want the edge values to be shown).

Example:



The log window displays the filtered information in columns. Note that extended box descriptors must be configured on the corresponding firewall to be available for selection. For more information, see: How to Configure Custom Box Descriptors and Filter Managed Firewalls in Different Data Views in the CloudGen Firewall documentation.

> This feature requires Barracuda CloudGen Firewall and Control Center version 8.3.1 or higher.

Click **Reload** to reload the logs displayed after you make changes to the filters above.

Figures

1. log_view_tab.png
2. log_filter.png
3. filter_btw.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.