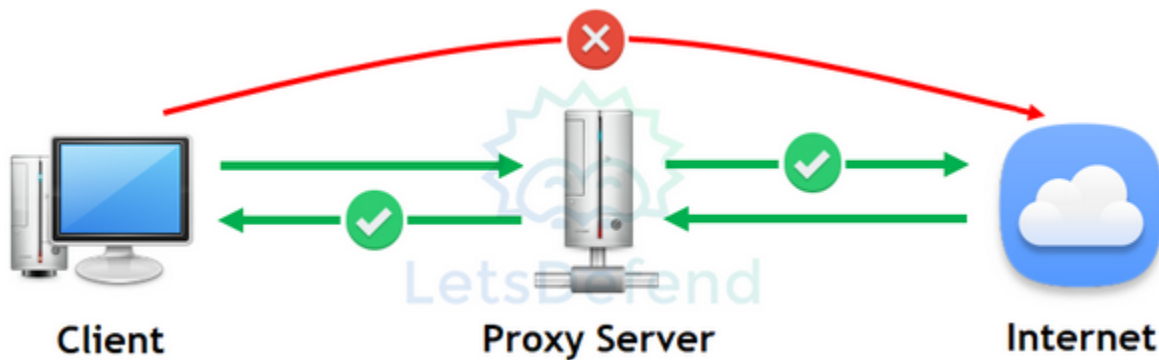




Proxy Server Analysis Questions

By: Ryan Stewart



Question: According to the given **Squid Web Proxy Server** log, how many different web addresses are there to send HTTP GET method requests? (Check the web addresses of the requests using the HTTP GET method)

The screenshot shows a log file with columns for time, IP, and request details. A search window is open with the text 'GET' entered. The search results show 5 matches in the entire file.

Line	Time	IP	Request
1	1667829869.002	127.0.0.1	TCP_TUNNEL/200 39 CONNECT letsdefend.io:443 - HIER_DIRECT/104.26.1
2	1667829869.515	127.0.0.1	TCP_TUNNEL/200 39 CONNECT letsdefend.io:443 - HIER_DIRECT/104.26.1
3	1667829869.552	127.0.0.1	TCP_TUNNEL/200 39 CONNECT letsdefend.io:443 - HIER_DIRECT/104.26.1
4	1667829869.668	127.0.0.1	TCP_TUNNEL/200 39 CONNECT fonts.googleapis.com:443 - HIER_DIRECT/1
5	1667829869.743	127.0.0.1	TCP_TUNNEL/200 39 CONNECT fonts.googleapis.com:443 - HIER_DIRECT/1
6	1667829869.803	127.0.0.1	TCP_TUNNEL/200 39 CONNECT letsdefend.io:443 - HIER_DIRECT/104.26.1
7	1667829869.808	127.0.0.1	TCP_TUNNEL/200 39 CONNECT www.googleadsmanager.com:443 - HIER_DIRE
8	1667829869.852	127.0.0.1	TCP_TUNNEL/200 39 CONNECT www.googleadsmanager.com:443 - HIER_DIRE
9	1667829870.054	127.0.0.1	TCP_TUNNEL/200 39 CONNECT www.googleadsmanager.com:443 - HIER_DIRE
10	1667829872.180	127.0.0.1	TCP_TUNNEL/200 39 CONNECT www.googleadsmanager.com:443 - HIER_DIRE
11	1667829872.296	127.0.0.1	TCP_TUNNEL/200 39 CONNECT www.googleadsmanager.com:443 - HIER_DIRE
12	1667829913.545	127.0.0.1	TCP_TUNNEL/200 39 CONNECT www.googleadsmanager.com:443 - HIER_DIRE
13	1667830015.593	127.0.0.1	TCP_TUNNEL/200 39 CONNECT www.googleadsmanager.com:443 - HIER_DIRE
14	1667830050.820	127.0.0.1	TCP_TUNNEL/200 39 CONNECT www.googleadsmanager.com:443 - HIER_DIRE
15	1667830091.823	127.0.0.1	TCP_TUNNEL/200 39 CONNECT www.googleadsmanager.com:443 - HIER_DIRE
16	1667830106.856	127.0.0.1	TCP_TUNNEL/200 39 CONNECT www.googleadsmanager.com:443 - HIER_DIRE
17	1667830133.807	127.0.0.1	TCP_TUNNEL/200 39 CONNECT www.googleadsmanager.com:443 - HIER_DIRE
18	1667830179.248	127.0.0.1	TCP_TUNNEL/200 39 CONNECT www.googleadsmanager.com:443 - HIER_DIRE
19	1667830266.590	127.0.0.1	TCP_TUNNEL/200 39 CONNECT www.googleadsmanager.com:443 - HIER_DIRE
20	1667830278.603	127.0.0.1	TCP_TUNNEL/200 39 CONNECT www.googleadsmanager.com:443 - HIER_DIRE
21	1667830350.399	127.0.0.1	TCP_TUNNEL/200 39 CONNECT www.googleadsmanager.com:443 - HIER_DIRE
22	1667830356.536	127.0.0.1	TCP_TUNNEL/200 39 CONNECT www.googleadsmanager.com:443 - HIER_DIRE
23	1667830366.016	127.0.0.1	TCP_TUNNEL/200 39 CONNECT www.googleadsmanager.com:443 - HIER_DIRE
24	1667830374.671	127.0.0.1	TCP_TUNNEL/200 39 CONNECT www.googleadsmanager.com:443 - HIER_DIRE
25	1667830429.666	127.0.0.1	TCP_TUNNEL/200 39 CONNECT www.googleadsmanager.com:443 - HIER_DIRE

```

1667829913.545      289 127.0.0.1 TCP_MISS/302 352 GET http://virustotal.com/ - HIER_DIRECT/216.239.3
1667830015.593      680 127.0.0.1 TCP_MISS/301 459 GET http://amazon.com/ - HIER_DIRECT/52.94.236.248
1667830050.820      87696 127.0.0.1 TCP_TUNNEL/200 302638 CONNECT urlscan.io:443 - HIER_DIRECT/49.12.22
1667830091.823      177512 127.0.0.1 TCP_TUNNEL/200 1758578 CONNECT www.virustotal.com:443 - HIER_DIRECT
1667830106.856      170930 127.0.0.1 TCP_TUNNEL/200 8213 CONNECT youtube.com:443 - HIER_DIRECT/172.217.1
1667830133.807      118056 127.0.0.1 TCP_TUNNEL/200 6093 CONNECT amazon.com:443 - HIER_DIRECT/52.94.236.
1667830179.248      186421 127.0.0.1 TCP_TUNNEL/200 279445 CONNECT www.abuseipdb.com:443 - HIER_DIRECT/1
1667830266.590      7016 127.0.0.1 TCP_TUNNEL/200 35168 CONNECT www.hackread.com:443 - HIER_DIRECT/64.
1667830278.603      171061 127.0.0.1 TCP_TUNNEL/200 4941 CONNECT reddit.com:443 - HIER_DIRECT/151.101.12
1667830350.399      220057 127.0.0.1 TCP_TUNNEL/200 74505 CONNECT github.com:443 - HIER_DIRECT/140.82.12
1667830356.536      203041 127.0.0.1 TCP_TUNNEL/200 7392 CONNECT gitlab.com:443 - HIER_DIRECT/172.65.251
1667830366.016      2202 127.0.0.1 TCP_MISS/301 471 GET http://bleepingcomputer.com/ - HIER_DIRECT/104
1667830374.671      347 127.0.0.1 TCP_MISS/301 945 GET http://darkreading.com/ - HIER_DIRECT/104.17.1
1667830429.666      144 127.0.0.1 TCP_MISS/301 805 GET http://thehackernews.com/ - HIER_DIRECT/172.67

```

Question: According to the given **Squid Web Proxy Server** log, to which port of the "letsdefend.io" address was the request sent?

```

aws-waf.log x  aws-loadbalancer.log x  squid-proxy.log x
4      1667829869.668      40 127.0.0.1 TCP_TUNNEL/200 39 CONNECT fonts.googleapis.com:443 - HIER_DIRECT/1
5      1667829869.743      23 127.0.0.1 TCP_TUNNEL/200 39 CONNECT fonts.googleapis.com:443 - HIER_DIRECT/1
6      1667829869.803      15 127.0.0.1 TCP_TUNNEL/200 39 CONNECT letsdefend.io:443 - HIER_DIRECT/104.26.1
7      1667829869.808      42 127.0.0.1 TCP_TUNNEL/200 39 CONNECT www.googletagmanager.com:443 - HIER_DIRE
8      1667829869.852      15 127.0.0.1 TCP_TUNNEL/200 39 CONNECT letsdefend.io:443 - HIER_DIRECT/104.26.1
9      1667829870.054      252 127.0.0.1 TCP_TUNNEL/200 39 CONNECT embed.typeform.com:443 - HIER_DIRECT/18.
10     1667829872.180      43 127.0.0.1 TCP_TUNNEL/200 39 CONNECT fonts.gstatic.com:443 - HIER_DIRECT/216.
11     1667829872.296      16 127.0.0.1 TCP_TUNNEL/200 39 CONNECT letsdefend.io:443 - HIER_DIRECT/104.26.1
12     1667829913.545      289 127.0.0.1 TCP_MISS/302 352 GET http://virustotal.com/ - HIER_DIRECT/216.239.
13     1667830015.593      680 127.0.0.1 TCP_MISS/301 459 GET http://amazon.com/ - HIER_DIRECT/52.94.236.24
14     1667830050.820      87696 127.0.0.1 TCP_TUNNEL/200 302638 CONNECT urlscan.io:443 - HIER_DIRECT/49.12.2
15     1667830091.823      177512 127.0.0.1 TCP_TUNNEL/200 1758578 CONNECT www.virustotal.com:443 - HIER_DIREC
16     1667830106.856      170930 127.0.0.1 TCP_TUNNEL/200 8213 CONNECT youtube.com:443 - HIER_DIRECT/172.217.
17     1667830133.807      118056 127.0.0.1 TCP_TUNNEL/200 6093 CONNECT amazon.com:443 - HIER_DIRECT/52.94.236
18     1667830179.248      186421 127.0.0.1 TCP_TUNNEL/200 279445 CONNECT www.abuseipdb.com:443 - HIER_DIRECT/
19     1667830266.590      7016 127.0.0.1 TCP_TUNNEL/200 35168 CONNECT www.hackread.com:443 - HIER_DIRECT/64
20     1667830278.603      171061 127.0.0.1 TCP_TUNNEL/200 4941 CONNECT reddit.com:443 - HIER_DIRECT/151.101.1
21     1667830350.399      220057 127.0.0.1 TCP_TUNNEL/200 74505 CONNECT github.com:443 - HIER_DIRECT/140.82.1
22     1667830356.536      203041 127.0.0.1 TCP_TUNNEL/200 7392 CONNECT gitlab.com:443 - HIER_DIRECT/172.65.25
23     1667830366.016      2202 127.0.0.1 TCP_MISS/301 471 GET http://bleepingcomputer.com/ - HIER_DIRECT/10
24     1667830374.671      347 127.0.0.1 TCP_MISS/301 945 GET http://darkreading.com/ - HIER_DIRECT/104.17.
25     1667830429.666      144 127.0.0.1 TCP_MISS/301 805 GET http://thehackernews.com/ - HIER_DIRECT/172.6

```