

Systemy webowe

SQUID - ACL

Krzysztof Marczyński
226258

23.11.2019

Spis treści

1	Wprowadzenie	3
2	Pliki ACL	3
2.1	Użytkownicy - adresy MAC	3
2.2	Podsieci	4
2.3	Użytkownicy - konta użytkowników	4
2.4	Strony internetowe	4
2.5	Rozszerzenia plików	5
3	squid.conf	11
4	Podsumowanie	13

1 Wprowadzenie

Celem zadania jest przygotowanie filtrów dla środowiska squid z uwzględnieniem następujących reguł:

- Prezes
 - Korzysta z komputerów o adresach MAC 0800278424BF i 080027810873.
 - Nie ma żadnych ograniczeń odnośnie korzystania z sieci.
- Menadżerowie
 - Korzystają z komputerów o adresach MAC 080027E7D537, 0800278259C5, 080027C3BEB8.
 - Nie mają dostępu do stron rozrywkowych w czasie pracy.
 - Nie mają dostępu do stron rozrywkowych w weekendy.
- Projektanci
 - Korzystają z komputerów w podsieci 192.168.2.0.
 - Muszą się logować w celu odróżnienia od Programistów.
 - Nie mają dostępu do stron rozrywkowych przez cały czas.
 - Nie mogą pobierać plików multimedialnych.
 - Nie mogą pobierać programów z wyłączeniem uaktualnień systemu Windows.
- Programiści
 - Korzystają z komputerów w podsieci 192.168.2.0.
 - Muszą się logować w celu odróżnienia od Projektantów.
 - Nie mają dostępu do stron rozrywkowych przez cały czas.
 - Nie mają dostępu do stron prasowych w czasie pracy.
- Administrator
 - Korzystają z komputera o adresie MAC 080027EBD794.
 - Nie ma żadnych ograniczeń w czasie pracy.
 - Nie ma dostępu do stron rozrywkowych poza czasem pracy.
- Sekretarka i Księgowa
 - Korzystają z komputerów w podsieci 192.168.3.0.
 - Nie mają dostępu do stron rozrywkowych w godzinach pracy.
 - Mogą pobierać tylko pliki związane z pracą biurową.

2 Pliki ACL

2.1 Użytkownicy - adresy MAC

Listing 1: ACL - users/boss.acl

```
1 08:00:27:84:24:BF
2 08:00:27:81:08:73
```

Listing 2: ACL - users/managers.acl

```
1 08:00:27:E7:D5:37
2 08:00:27:82:59:C5
3 08:00:27:C3:BE:B8
```

Listing 3: ACL - users/admin.acl

```
1 08:00:27:EB:D7:94
```

2.2 Podsieci

Listing 4: ACL - nets/devs_designers_net.acl

```
1 192.168.2.0/24
```

Listing 5: ACL - nets/office_workers_net.acl

```
1 192.168.3.0/24
```

2.3 Użytkownicy - konta użytkowników

Listing 6: ACL - users/developers.acl

```
1 dev1
2 dev2
3 dev3
4 dev4
5 dev5
6 dev6
```

Listing 7: ACL - users/designers.acl

```
1 des1
2 des2
3 des3
```

2.4 Strony internetowe

Listing 8: ACL - sites/entertainment.acl

```
1 youtube
2 spotify
3 netflix
4 reddit
5 tumblr
6 demotywatory
7 kwejk
```

```

8 | joemonster
9 | wykop
10 | wrzuta
11 | soundcloud
12 | facebook
13 | twitter
14 | instagram
15 | pinterest
16 | 9gag
17 | tinder
18 | snapchat
19 | porn
20 | xxx
21 | redtube
22 | kink
23 | chaturbate

```

Listing 9: ACL - sites/news.acl

```

1 | onet
2 | wp
3 | interia
4 | eska
5 | wyborcza

```

Listing 10: ACL - sites/windows_updates.acl

```

1 | update.microsoft.com

```

2.5 Rozszerzenia plików

Listing 11: ACL - files/apps.acl

```

1 | \.ACTION$
2 | \.APK$
3 | \.APP$
4 | \.BAT$
5 | \.BIN$
6 | \.CMD$
7 | \.COM$
8 | \.COMMAND$
9 | \.CPL$
10 | \.CSH$
11 | \.EXE$
12 | \.GADGET$
13 | \.INF1$
14 | \.INS$
15 | \.INX$
16 | \.IPA$
17 | \.ISU$
18 | \.JOB$
19 | \.JSE$

```

```

20 \.KSH$
21 \.LNK$
22 \.MSC$
23 \.MSI$
24 \.MSP$
25 \.MST$
26 \.OSX$
27 \.OUT$
28 \.PAF$
29 \.PIF$
30 \.PRG$
31 \.PS1$
32 \.REG$
33 \.RGS$
34 \.RUN$
35 \.SCR$
36 \.SCT$
37 \.SHB$
38 \.SHS$
39 \.U3P$
40 \.VB$
41 \.VBE$
42 \.VBS$
43 \.VBSCRIPT$
44 \.WORKFLOW$
45 \.WS$
46 \.WSF$
47 \.WSH$
48 \.torrent$

```

Listing 12: ACL - files/media.acl

```

1 \.3gp$
2 \.3g2$
3 \.asf$
4 \.amv$
5 \.avi$
6 \.drc$
7 \.flv$
8 \.flv$
9 \.f4v$
10 \.f4p$
11 \.f4a$
12 \.f4b$
13 \.flv$
14 \.gif$
15 \.m4v$
16 \.mxf$
17 \.mkv$
18 \.MTS$
19 \.M2TS$
20 \.TS$
21 \.mpg$
22 \.mp2$
23 \.mpeg$

```

24	\.mpe\$
25	\.mpv\$
26	\.mpg\$
27	\.mpeg\$
28	\.m2v\$
29	\.mp4\$
30	\.m4v\$
31	\.mng\$
32	\.nsv\$
33	\.ogv\$
34	\.ogg\$
35	\.mov\$
36	\.qt\$
37	\.yuv\$
38	\.rm\$
39	\.rmvb\$
40	\.roq\$
41	\.svi\$
42	\.gifv\$
43	\.vob\$
44	\.webm\$
45	\.wmv\$
46	\.3gp\$
47	\.aa\$
48	\.aac\$
49	\.aax\$
50	\.act\$
51	\.aiff\$
52	\.alac\$
53	\.amr\$
54	\.ape\$
55	\.au\$
56	\.awb\$
57	\.dct\$
58	\.dss\$
59	\.dvf\$
60	\.flac\$
61	\.gsm\$
62	\.iklax\$
63	\.ivs\$
64	\.m4a\$
65	\.m4b\$
66	\.m4p\$
67	\.mmf\$
68	\.mp3\$
69	\.mpc\$
70	\.msv\$
71	\.nmf\$
72	\.nsf\$
73	\.ogg\$
74	\.oga\$
75	\.mogg\$
76	\.opus\$
77	\.ra\$

```
78 \.rm$
79 \.raw$
80 \.sln$
81 \.tta$
82 \.voc$
83 \.vox$
84 \.wav$
85 \.wma$
86 \.wv$
87 \.webm$
88 \.8svx$
```

Listing 13: ACL - files/office.acl

```
1 \.doc$
2 \.dot$
3 \.xml$
4 \.docx$
5 \.docm$
6 \.dotx$
7 \.dotm$
8 \.doc$
9 \.wpd$
10 \.wps$
11 \.rtf$
12 \.txt$
13 \.csv$
14 \.sdw$
15 \.sgl$
16 \.vor$
17 \.xml$
18 \.uot$
19 \.uof$
20 \.jtd$
21 \.jtt$
22 \.hwp$
23 \.602$
24 \.txt$
25 \.pdb$
26 \.psw$
27 \.xls$
28 \.xlw$
29 \.xlt$
30 \.xls$
31 \.xlw$
32 \.xlt$
33 \.xml$
34 \.xlsx$
35 \.xlsm$
36 \.xltx$
37 \.xltm$
38 \.xlsb$
39 \.wk1$
40 \.wks$
41 \.dif$
```


42	\\.rtf\$
43	\\.csv\$
44	\\.txt\$
45	\\.sdc\$
46	\\.vor\$
47	\\.dbf\$
48	\\.slk\$
49	\\.uos\$
50	\\.uof\$
51	\\.htm\$
52	\\.html\$
53	\\.pxl\$
54	\\.wb2\$
55	\\.ppt\$
56	\\.pps\$
57	\\.pot\$
58	\\.pptx\$
59	\\.pptm\$
60	\\.potx\$
61	\\.potm\$
62	\\.sda\$
63	\\.sdd\$
64	\\.sdp\$
65	\\.vor\$
66	\\.uop\$
67	\\.uof\$
68	\\.cgm\$
69	\\.pdf\$
70	\\.7z\$
71	\\.s7z\$
72	\\.ace\$
73	\\.afa\$
74	\\.alz\$
75	\\.apk\$
76	\\.arc\$
77	\\.ark\$
78	\\.arc\$
79	\\.cdx\$
80	\\.arj\$
81	\\.b1\$
82	\\.b6z\$
83	\\.ba\$
84	\\.bh\$
85	\\.cab\$
86	\\.car\$
87	\\.cfs\$
88	\\.cpt\$
89	\\.dar\$
90	\\.dd\$
91	\\.dgc\$
92	\\.dmg\$
93	\\.ear\$
94	\\.gca\$
95	\\.ha\$

96	\.hki\$
97	\.ice\$
98	\.jar\$
99	\.kgb\$
100	\.lzh\$
101	\.lha\$
102	\.lzx\$
103	\.pak\$
104	\.partimg\$
105	\.paq6\$
106	\.paq7\$
107	\.paq8\$
108	\.pea\$
109	\.pim\$
110	\.pit\$
111	\.qda\$
112	\.rar\$
113	\.rk\$
114	\.sda\$
115	\.sea\$
116	\.sen\$
117	\.sfx\$
118	\.shk\$
119	\.sit\$
120	\.sitx\$
121	\.sqx\$
122	\.tar.gz\$
123	\.tgz\$
124	\.tar.Z\$
125	\.tar.bz2\$
126	\.tbz2\$
127	\.tar.lzma\$
128	\.tlz\$
129	\.tar.xz\$
130	\.txz\$
131	\.uc\$
132	\.uc0\$
133	\.uc2\$
134	\.ucn\$
135	\.ur2\$
136	\.ue2\$
137	\.uca\$
138	\.uha\$
139	\.war\$
140	\.wim\$
141	\.xar\$
142	\.xp3\$
143	\.yz1\$
144	\.zip\$
145	\.zipx\$
146	\.zoo\$
147	\.zpaq\$
148	\.zz\$
149	\.BMP\$

```

150 \.JPEG$
151 \.JPG$
152 \.PCX$
153 \.PSD$
154 \.SGV$
155 \.WMF$
156 \.DXF$
157 \.MET$
158 \.PGM$
159 \.RAS$
160 \.SVM$
161 \.XBM$
162 \.EMF$
163 \.PBM$
164 \.PLT$
165 \.SDA$
166 \.TGA$
167 \.XPM$
168 \.EPS$
169 \.PCD$
170 \.PNG$
171 \.SDD$
172 \.TIF$
173 \.TIFF$
174 \.GIF$
175 \.PCT$
176 \.PPM$
177 \.SGF$
178 \.VOR$

```

Listing 14: ACL - files/windows_update.acl

```

1 \.msu$

```

3 squid.conf

Listing 15: Zmiany w pliku squid.conf

```

1 ##### Authentication setup #####
2 # point to file with users and passwords
3 auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/passwd
4 # max number of sessions
5 auth_param basic children 2
6 # inform web browser about required authentication
7 auth_param basic realm Serwer squid
8 # max session time
9 auth_param basic credentialsttl 2 hours
10
11 ##### CUSTOM ACL #####
12 # users – MAC addresses
13 acl boss      arp      ”/etc/squid/acl/users/boss.acl”

```

```

14 acl managers      arp      "/etc/squid/acl/users/managers.acl"
15 acl admin         arp      "/etc/squid/acl/users/admin.acl"
16
17 # users - subnets
18 acl devs_designers_net      src      "/etc/squid/acl/nets/devs_designers_net.acl"
19 acl office_workers_net      src      "/etc/squid/acl/nets/office_workers_net.acl"
20
21 # require auth for some users
22 acl developers      proxy_auth      "/etc/squid/acl/users/developers.acl"
23 acl designers       proxy_auth      "/etc/squid/acl/users/designers.acl"
24
25 # sites
26 acl entertainment_sites      dstdom_regex      "/etc/squid/acl/sites/
entertainment.acl"
27 acl news_sites              dstdom_regex      "/etc/squid/acl/sites/news.acl"
28 acl windows_updates_sites    dstdom_regex      "/etc/squid/acl/sites/
windows_updates.acl"
29
30 # files
31 acl apps_ext                urlpath_regex      "/etc/squid/acl/files/apps.acl"
32 acl media_ext               urlpath_regex      "/etc/squid/acl/files/media.acl"
33 acl office_ext              urlpath_regex      "/etc/squid/acl/files/office.acl"
34 acl windows_update_ext       urlpath_regex      "/etc/squid/acl/files/
windows_update.acl"
35
36 # time
37 acl working_hours           time      8:00-16:00
38 acl working_days            time      M T W H F
39
40 ##### CUSTOM HTTP_ACCESS #####
41 ### boss ###
42 # Allow everything
43 http_access allow boss
44
45 ### managers ###
46 # Deny access to entertainment sites during working hours
47 http_access deny managers entertainment_sites working_hours working_days
48 # Deny access to entertainment sites during weekends
49 http_access deny managers entertainment_sites !working_days
50
51 http_access allow managers
52
53 ### designers ###
54 # Deny access to entertainment sites
55 http_access deny devs_designers_net designers entertainment_sites
56 # Deny download of media files
57 http_access deny devs_designers_net designers media_ext
58 # Deny download of apps except Windows Update
59 http_access deny devs_designers_net designers apps_ext !windows_update_ext !
windows_updates_sites
60
61 http_access allow devs_designers_net designers
62
63 ### developers ###

```

```
64 # Deny access to entertainment sites
65 http_access deny devs_designers_net designers entertainment_sites
66 # Deny access to news sites during working hours
67 http_access deny devs_designers_net designers news_sites working_hours
   working_days
68
69 http_access allow devs_designers_net developers
70
71 #### admin ####
72 # Allow everything during working hours
73 http_access allow admin working_hours working_days
74 # Deny access to entertainment sites (outside working hours)
75 http_access deny admin entertainment_sites
76
77 http_access allow admin
78
79 #### secretary and accountant ####
80 # Deny access to entertainment sites during working hours
81 http_access deny office_workers_net entertainment_sites working_hours
   working_days
82 # Deny download of files except basic office files
83 http_access deny office_workers_net !office_ext
84
85 http_access allow office_workers_net
```

4 Podsumowanie