Systemy webowe
SQUID - ACL

Krzysztof Marczyński
226258

23.11.2019

Spis treści

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
  - Korzystaja 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 Zewnętrzne pliki ACL

Podczas definiowania filtrów dla środowiska squid wykorzystano zewnętrzne pliki ACL podzielone na następujące kategorie:

- Użytkownicy: adresy MAC - definicje adresów fizycznych komputerów szefa, menadżerów i administratora
- Użytkownicy: konta użytkowników - nazwy kont programistów i projektantów

- Podsieci - podsieci z których korzystają programiści i projektanci oraz pracownicy biurowi (sekretarka i księgowa)
- Strony internetowe - fragmenty nazw domen stron rozrywkowych (społecznościowe, dotyczące memów, filmów, muzyki i pornografii), informacyjnych i zawierających aktualizacje systemu Windows
- Rozszerzenia plików - definicje rozszerzeń plików programów, mediów (muzyka i filmy), biurowych (dokumenty, arkusze kalkulacyjne, prezentacje, pliki skompresowane, graficzne i tekstowe) oraz aktualizacji systemu Windows

2.1 Użytkownicy: adresy MAC

Listing 1: ACL - adresy MAC komputerów szefa - users/boss.acl

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

Listing 2: ACL - adresy MAC komputerów menadżerów - 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 - adresy MAC komputerów administratora - users/admin.acl

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

2.2 Użytkownicy: konta użytkowników

Listing 4: ACL - nazwy kont programistów - users/developers.acl

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

Listing 5: ACL - nazwy kont projektantów - users/designers.acl

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

2.3 Podsieci

Listing 6: ACL - podsieć z której korzystają programiści i projektanci - nets/devs_designers_net.acl

```
1 192.168.2.0/24
```

Listing 7: ACL - podsieć z której korzystają sekretarka i księgowa - nets/office_workers_net.acl

```
192.168.3.0/24
```

2.4 Strony internetowe

Listing 8: ACL - strony rozrywkowe - sites/entertainment.acl

```
youtube
spotify
netflix
reddit
tumblr
demotywatory
kwejk
joemonster
wykop
wrzuta
soundcloud
facebook
twitter
instagram
pinterest
9gag
tinder
snapchat
porn
xxx
redtube
kink
chaturbate
```

Listing 9: ACL - strony informacyjne - sites/news.acl

```
onet
wp
interia
eska
wyborcza
```

Listing 10: ACL - strony z aktualizacjami systemu Windows - sites/windows_updates.acl

```
update.microsoft.com
```

2.5 Rozszerzenia plików

Listing 11: ACL - rozszerzenia plików programów - files/apps.acl

```
\.ACTION$
\.APK$
```

```
\.APP$
\.BAT$
\.BIN$
\.CMD$
\.COM$
\.COMMAND$
\.CPL$
\.CSH$
\.EXE$
\.GADGET$
\.INF1$
\.INS$
\.INX$
\.IPA$
\.ISU$
\.JOB$
\.JSE$
\.KSH$
\.LNK$
\.MSC$
\.MSI$
\.MSP$
\.MST$
\.OSX$
\.OUT$
\.PAF$
\.PIF$
\.PRG$
\.PS1$
\.REG$
\.RGS$
\.RUN$
\.SCR$
\.SCT$
\.SHB$
\.SHS$
\.U3P$
\.VB$
\.VBE$
\.VBS$
\.VBSCRIPT$
\.WORKFLOW$
\.WS$
\.WSF$
\.WSH$
\.torrent$
```

Listing 12: ACL - rozszerzenia plików mediów - files/media.acl

```
\.3gp$
\.3g2$
\.asf$
\.amv$
\.avi$
\.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$
```

```
\.gsm$
\.iklax$
\.ivs$
\.m4a$
\.m4b$
\.m4p$
\.mmf$
\.mp3$
\.mpc$
\.msv$
\.nmf$
\.nsf$
\.ogg$
\.oga$
\.mogg$
\.opus$
\.ra$
\.rm$
\.raw$
\.sln$
\.tta$
\.voc$
\.vox$
\.wav$
\.wma$
\.wv$
\.webm$
\.8svx$
```

Listing 13: ACL - rozszerzenia plików biurowych - files/office.acl

```
\.doc$
\.dot$
\.xml$
\.docx$
\.docm$
\.dotx$
\.dotm$
\.doc$
\.wpd$
\.wps$
\.rtf$
\.txt$
\.csv$
\.sdw$
\.sgl$
\.vor$
\.xml$
\.uot$
\.uof$
\.jtd$
\.jtt$
\.hwp$
\.602$
\.txt$
```

```
\.pdb$
\.psw$
\.xls$
\.xlw$
\.xlt$
\.xls$
\.xlw$
\.xlt$
\.xml$
\.xlsx$
\.xlsm$
\.xltx$
\.xltm$
\.xlsb$
\.wk1$
\.wks$
\.dif$
\.rtf$
\.csv$
\.txt$
\.sdc$
\.vor$
\.dbf$
\.slk$
\.uos$
\.uof$
\.htm$
\.html$
\.pxl$
\.wb2$
\.ppt$
\.pps$
\.pot$
\.pptx$
\.pptm$
\.potx$
\.potm$
\.sda$
\.sdd$
\.sdp$
\.vor$
\.uop$
\.uof$
\.cgm$
\.pdf$
\.7z$
\.s7z$
\.ace$
\.afa$
\.alz$
\.apk$
\.arc$
\.ark$
\.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$
```

```
\.uc2$
\.ucn$
\.ur2$
\.ue2$
\.uca$
\.uha$
\.war$
\.wim$
\.xar$
\.xp3$
\.yz1$
\.zip$
\.zipx$
\.zoo$
\.zpaq$
\.zz$
\.BMP$
\.JPEG$
\.JPG$
\.PCX$
\.PSD$
\.SGV$
\.WMF$
\.DXF$
\.MET$
\.PGM$
\.RAS$
\.SVM$
\.XBM$
\.EMF$
\.PBM$
\.PLT$
\.SDA$
\.TGA$
\.XPM$
\.EPS$
\.PCD$
\.PNG$
\.SDD$
\.TIF$
\.TIFF$
\.GIF$
\.PCT$
\.PPM$
\.SGF$
\.VOR$
```

Listing 14: ACL - rozszerzenia plików aktualizacji systemu Windows - files/windows_update.acl

```
\.msu$
```

3 Zmiany w konfiguracji

Konfigurację oparto na pliku squid.conf udostępnionym na eportalu. W celu realizacji zadania dopisano konfigurację przedstawioną na listingu 15. Żeby jednoznacznie określić jak reguły dostępu odzwierciedlają reguły biznesowe kod opisano odpowiednimi komentarzami.

Nową konfigurację dopisano do pliku squid.conf pomiędzy następującymi wyrażeniami:

- http_access deny CONNECT !SSL_ports
- http_access allow localhost

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 -i     "/etc/squid/acl/sites/
       entertainment.acl"
27 acl news_sites                dstdom_regex -i     "/etc/squid/acl/sites/news.acl
       "
28 acl windows_updates_sites     dstdom_regex -i     "/etc/squid/acl/sites/
       windows_updates.acl"
29
30 # files
31 acl apps_ext               urlpath_regex -i     "/etc/squid/acl/files/apps.acl"
32 acl media_ext              urlpath_regex -i     "/etc/squid/acl/files/media.acl"
33 acl office_ext             urlpath_regex -i     "/etc/squid/acl/files/office.acl
       "
34 acl windows_update_ext     urlpath_regex -i     "/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 developers entertainment_sites
66 # Deny access to news sites during working hours
67 http_access deny devs_designers_net developers 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 Testy

Na potrzeby testów przygotowano konfigurację Docker Compose przedstawioną na listingu 16 i Dockerfile przedstawioną na listingu 17

Listing 16: Konfiguracja Docker Compose

```
version: '2'
services:
  corpo_proxy:
    container_name: corpo_proxy
    build: .
    volumes:
      - ./proxy/squid.conf:/etc/squid/squid.conf
      - ./proxy/log:/var/log/squid
      - ./proxy/acl/:/etc/squid/acl/
    networks:
      - network_outer
      - devs_designers_net
      - office_workers_net
    ports:
      - 3128:3128

  boss:
    container_name: boss
    build: .
    mac_address: 08:00:27:84:24:BF
    networks:
      - network_outer

  manager:
    container_name: manager
    build: .
    mac_address: 08:00:27:C3:BE:B8
    networks:
      - network_outer

  admin:
    container_name: admin
    build: .
    mac_address: 08:00:27:EB:D7:94
    networks:
      - network_outer

  dev_designer:
    container_name: dev_designer
    build: .
    networks:
      - devs_designers_net

  office_worker:
    container_name: office_worker
    build: .
    networks:
```

```
48        - office_workers_net
49
50  networks:
51    network_outer:
52      driver: bridge
53      ipam:
54        config:
55          - subnet: 10.1.1.0/24
56
57    devs_designers_net:
58      driver: bridge
59      ipam:
60        config:
61          - subnet: 192.168.2.0/24
62
63    office_workers_net:
64      driver: bridge
65      ipam:
66        config:
67          - subnet: 192.168.3.0/24
```

Listing 17: Konfiguracja Dockerfile

```
1  FROM sameersbn/squid:3.5.27-2
2  RUN apt-get update && \
3      apt-get install -y iputils-ping curl net-tools apache2-utils iproute2 wget
           && \
4      htpasswd -bmc /etc/squid/passwd dev1 pass && \
5      htpasswd -bm /etc/squid/passwd dev2 pass && \
6      htpasswd -bm /etc/squid/passwd dev3 pass && \
7      htpasswd -bm /etc/squid/passwd dev4 pass && \
8      htpasswd -bm /etc/squid/passwd dev5 pass && \
9      htpasswd -bm /etc/squid/passwd dev6 pass && \
10     htpasswd -bm /etc/squid/passwd des1 pass && \
11     htpasswd -bm /etc/squid/passwd des2 pass && \
12     htpasswd -bm /etc/squid/passwd des3 pass && \
13     chmod o+r /etc/squid/passwd
```

W celu przeprowadzenia testów należało połączyć się z wybranym kontenerem Dockera, a następnie wykonać zapytania curl lub wget ze wskazaniem serwera proxy i, jeśli to konieczne, paremetrów uwierzytelniania użytkownika. Przykład pokazano na listingu 18.

Listing 18: Przykładowy test

```
1  docker exec -it dev_designer bash
2  curl -x des1:pass@corpo_proxy:3128 https://9gag.com
3  wget https://download.ted.com/talks/PaoloCardini_2012G-480p.mp4 -e use_proxy=
       yes -e https_proxy=http://des1:pass@corpo_proxy:3128
```

W przypadku jeśli dany zasób był zabroniony otrzymywano następujące komunikaty:

- curl: (56) Received HTTP code 403 from proxy after CONNECT
- wget: Proxy tunneling failed: ForbiddenUnable to establish SSL connection.

W wyniku przeprowadzonych testów stwierdzono, że wszystkie reguły i związane z nimi filtry squid działają w oczekiwany sposób.

5 Podsumowanie

Celem zadania było ograniczenie dostępu do określonych treści użytkownikom pewnej firmy. Serwer proxy squid i reguły ACL pozwalają w prosty sposób tego dokonać, a poprzez składanie wielu prostych reguł ACL w pojedynczej definicji dostępu http_access można zdefiniować skomplikowane warunki zależące od wielu czynników.

Jednakże na potrzeby tego zadania listy rozszerzeń plików i listy stron były definiowane ręcznie, co może skutkować tym, że wiele nieporządancyh stron czy plików nadal będzie dostępne dla użytkowników. O ile rozszerzenia plików są zbiorem względnie możliwym do zdefiniowania przy pewnym nakładzie pracy, to ogromna liczba istniejących stron rozrywkowych wyklucza możliwość zablokowania dostępu do wszystkich. Częściowym rozwiązaniem tego problemu mogłoby być wykupienie takich list od firm, które specjalizują się w komercyjnym ich tworzeniu i ciągłym poszerzaniu.