SQUID 3.5 – прозрачный прокси

Система:

uname -a
11.1-RELEASE-p8 FreeBSD 11.1-RELEASE-p8 #0: root@amd64-builder.daemonology.net:/usr/obj/usr/src/sys/GENERIC amd64

1. Установка

portsnap fetch update
portmaster www/squid

При выборе опций – мне хватило их по умолчанию, но, на всякий случай, проверяем такие:

В параметрах сборки проверяем, что включена поддержка прозрачного проксирования для используемого брандмауэра (IPFW) и поддержка больших файлов LARGEFILE, ECAP, SSL, SSL_CRTD, а также, если необходима, модификация HTTP-заголовков (использование опций via, request_header_access), включаем LAX_HTTP, для сборки Squid с параметром –enable-http-violations.

lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq squid-3.5.27_3 qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk x
x x+[x] ARP_ACL ARP/MAC/EUI based authentification x x
x x+[x] CACHE_DIGESTS Use cache digests x x
x x+[ ] DEBUG Build with extended debugging support x x
x x+[x] DELAY_POOLS Delay pools (bandwidth limiting) x x
x x+[x] DOCS Build and/or install documentation x x
x x+[x] ECAP Loadable content adaptation modules x x

x x+[ ] ESI ESI support
x x
x x+[x] EXAMPLES Build and/or install examples
x x
x x+[x] FOLLOW_XFF Support for the X-Following-For header
x x
x x+[x] FS_AUFS AUFS (threaded-io) support
x x
x x+[x] FS_DISKD DISKD storage engine controlled by separate
service x x
x x+[x] FS_ROCK ROCK storage engine
x x
x x+[x] HTCP HTCP support
x x
x x+[x] ICAP the ICAP client
x x
x x+[x] ICMP ICMP pinging and network measurement
x x
x x+[x] IDENT Ident lookups (RFC 931)
x x
x x+[x] IPV6 IPv6 protocol support
x x
x x+[x] KQUEUE Kqueue(2) support
x x
x x+[x] LARGEFILE Support large (>2GB) cache and log files
x x
x x+[x] LAX_HTTP Do not enforce strict HTTP compliance
x x
x x+[ ] NETTLE Nettle MD5 algorithm support
x x
x x+[x] PCRE Use Perl Compatible Regular Expressions
x x
x x+[x] SNMP SNMP support
x x
x x+[x] SSL SSL gatewaying support
x x
x x+[x] SSL_CRTD Use ssl_crtd to handle SSL cert requests
x x
x x+[ ] STACKTRACES Enable automatic backtraces on fatal
errors x x
x x+[x] VIA_DB Forward/Via database

```
x x
  x  x+[x]  WCCP  Web  Cache  Coordination  Protocol
x x
 x  x+[x]  WCCPV2  Web  Cache  Coordination  Protocol  v2
x x
 x  xqqqqqqqqqqqqqqqqqqqqqqqq  Authentication  helpers
qqqqqqqqqqqqqqqqqqqqqqqqx x
 x  x+[ ]  AUTH_LDAP  Install  LDAP  authentication  helpers
x x
 x  x+[x]  AUTH_NIS  Install  NIS/YP  authentication  helpers
x x
 x  x+[ ]  AUTH_SASL  Install  SASL  authentication  helpers
x x
  x  x+[  ]  AUTH_SMB  Samba  authentication  helpers
x x
   x   x+[   ]   AUTH_SQL   Install   SQL   based   auth
x x
 x  xqqqqqqqqqqqqqqqqqqqqqqq  GSSAPI  Security  API  support
qqqqqqqqqqqqqqqqqqqqqqx x
   x   x+(   )   GSSAPI_NONE   Disable   GSSAPI   support
x x
 x  x+(*)  GSSAPI_BASE  GSSAPI  support  via  base  system  (needs
Kerberos)          x x
 x  x+( )  GSSAPI_HEIMDAL  GSSAPI  support  via  security/heimdal
x x
 x  x+( )  GSSAPI_MIT  GSSAPI  support  via  security/krb5
x x
    x    xqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq    FW
qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqx x
 x  x+( )  TP_IPF  Transparent  proxying  with  IPFilter
x x
  x  x+(*)  TP_IPFW  Transparent  proxying  with  IPFW
x x
  x  x+(  )  TP_PF  Transparent  proxying  with  PF
x x
                                                        x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
qqqqqqqqqqqqj x
tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
qqqqqqqqqqqqqqqqu
 x                              < OK >         <Cancel>
```

x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
qqqqqqqqqqqqqqqqqqj

2. Настройка

Правим

/usr/local/etc/squid/squid.conf

```
#
# Recommended minimum configuration:
#

visible_hostname squid
dns_nameservers 194.44.219.162 8.8.8.8

# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
#acl localnet src 10.0.0.0/8 # RFC1918 possible internal network
#acl localnet src 172.16.0.0/12 # RFC1918 possible internal network
acl localnet src 192.168.113.0/24 # RFC1918 possible internal network
#acl localnet src fc00::/7 # RFC 4193 local private network range
#acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines

acl SSL_ports port 443
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
```

```
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT

# Добавление в acl списков для users и urls/domain: запрещенные, разрешенные
# и группа расширенного доступа (отключена)
acl denied_users src "/usr/local/etc/squid/denied_users"
acl denied_urls url_regex "/usr/local/etc/squid/denied_urls"
acl allowed_users src "/usr/local/etc/squid/allowed_users"
#acl               allowed_urls              url_regex "/usr/local/etc/squid/allowed_urls"
#acl             extended_access_group            src "/usr/local/etc/squid/extended_access_group"

# Deny requests to certain unsafe ports
http_access deny !Safe_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

## Разрешаем осуществлять коннект к ресурсу, если https
http_access allow localnet CONNECT

## Запрещаем всем доступ на запрещенные сайты
http_access deny denied_users denied_urls
http_access allow allowed_users

## Этим правилом разрешаем всем кто не в группе расширенного доступа ходить только на
# разрешенные сайты
# http_access deny !extended_access_group !allowed_urls

http_access allow localnet
http_access allow localhost
http_access deny all

## Обязательно один из портов должен быть в таком виде и
```

```
являться заглушкой
http_port 3130
http_port 3128 intercept
https_port       3129       intercept       ssl-bump
options=ALL:NO_SSLv3:NO_SSLv2      connection-auth=off
cert=/usr/local/etc/squid/squidCA.pem

always_direct allow all
sslproxy_cert_error allow all
sslproxy_flags DONT_VERIFY_PEER


## Правила доступа для ssl

# правило со списком блокируемых ресурсов (в файле домены вида
.domain.com)
acl           blocked           ssl::server_name_regex
"/usr/local/etc/squid/denied_urls"
acl step1 at_step SslBump1
ssl_bump peek step1

# терминируем соединение, если клиент заходит на запрещенный
ресурс
ssl_bump terminate blocked
ssl_bump splice all

sslcrtd_program /usr/lib/squid/ssl_crtd -s /var/lib/ssl_db -M
4MB

# Uncomment and adjust the following to add a disk cache
directory.
#cache_dir ufs /var/squid/cache 100 16 256

# Leave coredumps in the first cache dir
coredump_dir /var/squid/cache

refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern -i (/cgi-bin/|\?) 0 0% 0
refresh_pattern . 0 20% 4320
```

Создаем файлы:

```
touch /usr/local/etc/squid/denied_urls
cat /usr/local/etc/squid/denied_urls
.pornhub.com
.xxx.com
touch /usr/local/etc/squid/denied_users
cat /usr/local/etc/squid/denied_users
192.168.113.110 # menagers dep
192.168.113.203 #

touch /usr/local/etc/squid/allowed_users
cat /usr/local/etc/squid/allowed_users
192.168.113.0/24 # вся сеть
touch /usr/local/etc/squid/extended_access_group
cat /usr/local/etc/squid/extended_access_group
192.168.0.12 # Masha
192.168.0.15 # Direktor
192.168.0.53 # Sasha
192.168.0.54 # My Note
```

Делаем сертификат

```
cd /usr/local/etc/squid/
openssl req -new -newkey rsa:1024 -days 365 -nodes -x509 -
keyout squidCA.pem -out squidCA.pem
```

Добавляем в /etc/rc.conf

```
squid_enable="YES"
```

Инициализируем кеш:

```
squid -z
```

Добавляем правила в IPFW

```
### LAN
${ipfw} add allow ip from any to any via ${lan}

### SQUID прозрачный
${ipfw} add fwd 127.0.0.1,3128 tcp from table\(0\) to any 80
out via ${wan}
${ipfw} add fwd 127.0.0.1,3129 tcp from table\(0\) to any 443
out via ${wan}
```

Перезапускаем IPFW и стартуем squid:

```
/etc/rc.d/ipfw restart
service squid start
```

Проверяем.

https://www.ew8bak.ru/2017/02/14/

https://wiki.squid-cache.org/ConfigExamples/Intercept/Ipfw