Squid

оригинал

Прокси (кеширующий) сервер.

http://www.squid-cache.org

Фильтр содержимого	Режик
Администрирование доступа пользователей	SQUID Account Management System
Генератор отчетов	SARG

Установка

```
apt install squid
```

Настройка

Fix Me!

Места для вставки соответствующих параметров выделены следующими символами ###

/etc/squid/squid.conf

```
#debug_options ALL,1 28,9

http_port 10.0.0.1:3128
http_port 10.0.0.11:3128
tcp_outgoing_address 10.0.0.1

maximum_object_size 131072 KB
# minimum_object_size 0 KB
maximum_object_size_in_memory 32 KB

#cache_dir null /null
#cache_dir ufs /usr/local/squid/cache 8192 16 256
#cache_log /dev/null

cache_dir null /tmp
```

```
cache_log /var/log/squid/cache.log
cache_replacement_policy heap LFUDA

### Протокол ###
# Включить
#access_log /var/log/squid/access.log
#cache_store_log /var/log/squid/store.log
# Отключить
access_log none
cache_store_log none

# Отключение /var/log/squid/netdb.state
netdb_filename none

ftp_user anonymous@domain.ru
visible_hostname HTTP Proxy
cache_mgr webmaster@domain.ru

### Использование авторизации basic ###
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

### Фильтр содержимого ###
#redirect_program /opt/rejik/redirector /opt/rejik/redirector.conf

# Запрет больших файлов
#request_body_max_size 1 MB
#reply_body_max_size 1 MB

acl NOQ1 urlpath_regex cgi-bin \?
no_cache deny NOQ1

# ACL: ALL
acl ALL src 0.0.0.0/0.0.0.0

# Not cache!
no_cache deny all

### Списки доступа по URL/IP ###
include /usr/local/etc/squid/urls-lists.conf

acl ftp proto FTP
#always_direct allow FTP
http_access allow ftp

#acl manager proto cache_object
acl SSL_ports port 443 563
acl Safe_ports port 80          # http
acl Safe_ports port 81          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443 563     # https, snews
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
http_access allow manager localhost

# ACL: Deny ALL
```

```
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access deny ALL
http_reply_access deny ALL
icp_access deny ALL


cache_effective_user proxy
cache_effective_group proxy

logfile_rotate 7
# minimum_retry_timeout 5 seconds
# maximum_single_addr_tries 3

#coredump_dir /usr/local/squid/cache
coredump_dir /var/log/squid

# Скрывать внутренний IP адрес клиента
forwarded_for off
via off

#header_access X-Forwarded-For deny all
#header_access Via deny all

### Выпуск трафика с разных IP-адресов ###
```

Использование авторизации basic

Добавление пользователя для авторизации:

```
htpasswd /etc/squid/passwd ПОЛЬЗОВАТЕЛЬ
```

Параметры для файла `squid.conf`:

```
auth_param basic program /usr/lib/squid3/basic_ncsa_auth /etc/squid/passwd
auth_param basic children 3
auth_param basic realm proxy
authenticate_ttl 600 seconds
authenticate_ip_ttl 10 seconds
auth_param basic credentialsttl 2 hours
```

Протокол (Log)

Для включения/отключения протокола нужно внести соответствующие изменения в файл `squid.conf`:

- Отключить

```
access_log none
cache_store_log none
cache_log /dev/null
```

- Включить:

```
access_log /var/log/squid/access.log
cache_store_log /var/log/squid/store.log
```

Выпуск трафика с разных IP-адресов

Пример выпуска трафика из разных сетей/адресов с разных внешних IP-адресов:

- Для сети `net1` использовать `ВНЕШНИЙ_IP_1`
- Для сети `net2` использовать `ВНЕШНИЙ_IP_2`
- Для адреса `net3` использовать `ВНЕШНИЙ_IP_3`
- Для остальных использовать `ВНЕШНИЙ_IP_4`

squid.conf

```
acl net1 src 10.1.1.0/24
acl net2 src 10.1.2.0/24
acl net3 src 10.1.3.1/32
tcp_outgoing_address ВНЕШНИЙ_IP_1 net1
tcp_outgoing_address ВНЕШНИЙ_IP_2 net2
tcp_outgoing_address ВНЕШНИЙ_IP_3 net3
tcp_outgoing_address ВНЕШНИЙ_IP_4
```

Ограничение доступа по IP/URL

Fix Me!

Используется для:

- Debian
- MS Windows
- ClamAV
- SpamAssassin
- Discord
- Telegram

Файлы с расширением `.allow` и `.deny` содержат список IP–адресов и/или их масок, одна строка — один адрес/маска.

Примеры:

1. Разрешить доступ к обновлению SpamAssassin:

   /usr/local/etc/squid/SpamAssassin.allow

   ```
   10.1.10.11
   10.1.10.12
   10.1.10.13
   ```

2. Запретить доступ для следующих IP:

   /usr/local/etc/squid/Deny.deny

   ```
   10.1.10.0/24
   ```

   к URL по списку

   ```
   windowsupdate.com
   detectportal.firefox.com
   ```

Пример готового файла `urls-lists.conf`:

/usr/local/etc/squid/urls-lists.conf

```
### MS Windows ###
acl MS_Windows.urls url_regex "/usr/local/etc/squid/MS_Windows.urls"
acl MS_Windows.allow src "/usr/local/etc/squid/MS_Windows.allow"
http_access allow MS_Windows.allow MS_Windows.urls
http_reply_access allow MS_Windows.allow MS_Windows.urls

### Deny ###
acl Deny.urls url_regex "/usr/local/etc/squid/Deny.urls"
acl Deny.deny src "/usr/local/etc/squid/Deny.deny"
http_access deny Deny.deny Deny.urls

# ACL: ExtlRerorts
acl ExtRerorts.urls url_regex "/usr/local/etc/squid/ExtRerorts.urls"
acl ExtRerorts.allow src "/usr/local/etc/squid/ExtRerorts.allow"
http_access allow ExtRerorts.allow ExtRerorts.urls
http_reply_access allow ExtRerorts.allow ExtRerorts.urls

### ClamAV ###
acl ClamAV.urls url_regex "/usr/local/etc/squid/ClamAV.urls"
acl ClamAV.allow src "/usr/local/etc/squid/ClamAV.allow"
http_access allow ClamAV.allow ClamAV.urls
http_reply_access allow ClamAV.allow ClamAV.urls

### SpamAssassin ###
acl SpamAssassin.urls url_regex "/usr/local/etc/squid/SpamAssassin.urls"
acl SpamAssassin.allow src "/usr/local/etc/squid/SpamAssassin.allow"
http_access allow SpamAssassin.allow SpamAssassin.urls
http_reply_access allow SpamAssassin.allow SpamAssassin.urls

# ACL: SBIS
acl SBIS.urls url_regex "/usr/local/etc/squid/SBIS.urls"
acl SBIS.allow src "/usr/local/etc/squid/SBIS.allow"
acl SBIS.ports port 80 443 8585
http_access allow SBIS.allow SBIS.urls SBIS.ports
http_reply_access allow SBIS.allow SBIS.urls SBIS.ports

# ACL: SBIS-online
acl SBIS-online.urls url_regex "/usr/local/etc/squid/SBIS-online.urls"
acl SBIS-online.allow src "/usr/local/etc/squid/SBIS-online.allow"
acl SBIS-online.ports port 80 443 53 3478
http_access allow SBIS-online.allow SBIS-online.urls SBIS-online.ports
http_reply_access allow SBIS-online.allow SBIS-online.urls SBIS-online.ports

# ACL: Maps
acl Maps.urls url_regex "/usr/local/etc/squid/Maps.urls"
acl Maps.allow src "/usr/local/etc/squid/Maps.allow"
http_access allow Maps.allow Maps.urls
http_reply_access allow Maps.allow Maps.urls

### Debian ###
acl Debian.urls url_regex "/usr/local/etc/squid/Debian.urls"
acl Debian.allow src "/usr/local/etc/squid/Debian.allow"
http_access allow Debian.allow Debian.urls
http_reply_access allow Debian.allow Debian.urls

# ACL: iBank2
acl iBank2.ports port 33333 9091 80 443
#acl CONNECT method CONNECT
acl iBank2.allow src "/usr/local/etc/squid/iBank2.allow"
acl iBank2.urls url_regex url_regex "/usr/local/etc/squid/iBank2.urls"
```

```
http_access allow iBank2.allow iBank2.urls iBank2.ports
http_reply_access allow iBank2.allow iBank2.urls iBank2.ports

# ACL: Сбербанк
acl SberBank.ports port 80 443 9443 444
acl SberBank.allow src "/usr/local/etc/squid/SberBank.allow"
acl SberBank.urls url_regex url_regex "/usr/local/etc/squid/SberBank.urls"
http_access allow SberBank.allow SberBank.urls SberBank.ports
http_reply_access allow SberBank.allow SberBank.urls SberBank.ports

# ACL: Внешние отчёты
#acl ExternalRerorts.urls url_regex "/usr/local/etc/squid/ExternalRerorts.urls"
#acl ExternalRerorts.allow src "/usr/local/etc/squid/ExternalRerorts.allow"
#http_access allow ExternalRerorts.allow ExternalRerorts.urls
#http_reply_access allow ExternalRerorts.allow ExternalRerorts.urls

# ACL: All
acl All.urls url_regex "/usr/local/etc/squid/All.urls"
acl All.allow src "/usr/local/etc/squid/All.allow"
http_access allow All.allow All.urls
http_reply_access allow All.allow All.urls

# ACL: 1C
acl 1C.urls url_regex "/usr/local/etc/squid/1C.urls"
acl 1C.allow src "/usr/local/etc/squid/1C.allow"
http_access allow 1C.allow 1C.urls
http_reply_access allow 1C.allow 1C.urls

### Discord ###
acl Discord.urls url_regex "/usr/local/etc/squid/Discord.urls"
acl Discord.allow src "/usr/local/etc/squid/Discord.allow"
http_access allow Discord.allow Discord.urls
http_reply_access allow Discord.allow Discord.urls

### ACL: Telegram ###
acl Telegram.urls url_regex "/usr/local/etc/squid/Telegram.urls"
acl Telegram.allow src "/usr/local/etc/squid/Telegram.allow"
http_access allow Telegram.allow Telegram.urls
http_reply_access allow Telegram.allow Telegram.urls
```

Перезапуск

```
service squid reload
```

Тестирование

Видимость в сети:

```
netstat -tulpn |grep 3128
```

Для тестирования удобно использовать браузер Links.

Преобразование штампа даты времени из файла access.log

Примеры:

```
cat access.log | perl -p -e 's/^([0-9]*)/"[".localtime($1)."]"/e'
```

или

```
echo 1464578711.398 | perl -p -e 's/^([0-9]*)/"[".localtime($1)."]"/e'
```

logrotate

Fix Me!

Настройка ротации протокола с помощью logrotate:

/etc/logrotate.d/squid3

```
#
#   Logrotate fragment for squid3.
#
/var/log/squid3/*.log {
    monthly
    compress
    delaycompress
    rotate 2
    missingok
    nocreate
    sharedscripts
    prerotate
        test ! -x /usr/sbin/sarg-reports || /usr/sbin/sarg-reports monthly
        endscript
    postrotate
        test ! -e /var/run/squid3.pid || /usr/sbin/squid3 -k rotate
    endscript
}
```

Ссылки

Squid Log Files

Can I make Squid proxy only, without caching anything?

Sonar — Web Interface for Squid

wiki.rsu.edu.ru: Настройка proxy-сервера

Convert squid timestamps

Squid configuration directive tcp_outgoing_address

Squid на практике. Использование нескольких интерфейсов для выхода в Интернет

Директивы(TAG) Squid. tcp_outgoing_address

http://sysadminmosaic.ru/squid/squid

2021-07-07 13:11