

## Настройка проксирующего режима squid

### Цели занятия

показать возможности конфигурирования SQUID как безопасного прокси-сервера (шлюза в Интернет) для корпоративной сети

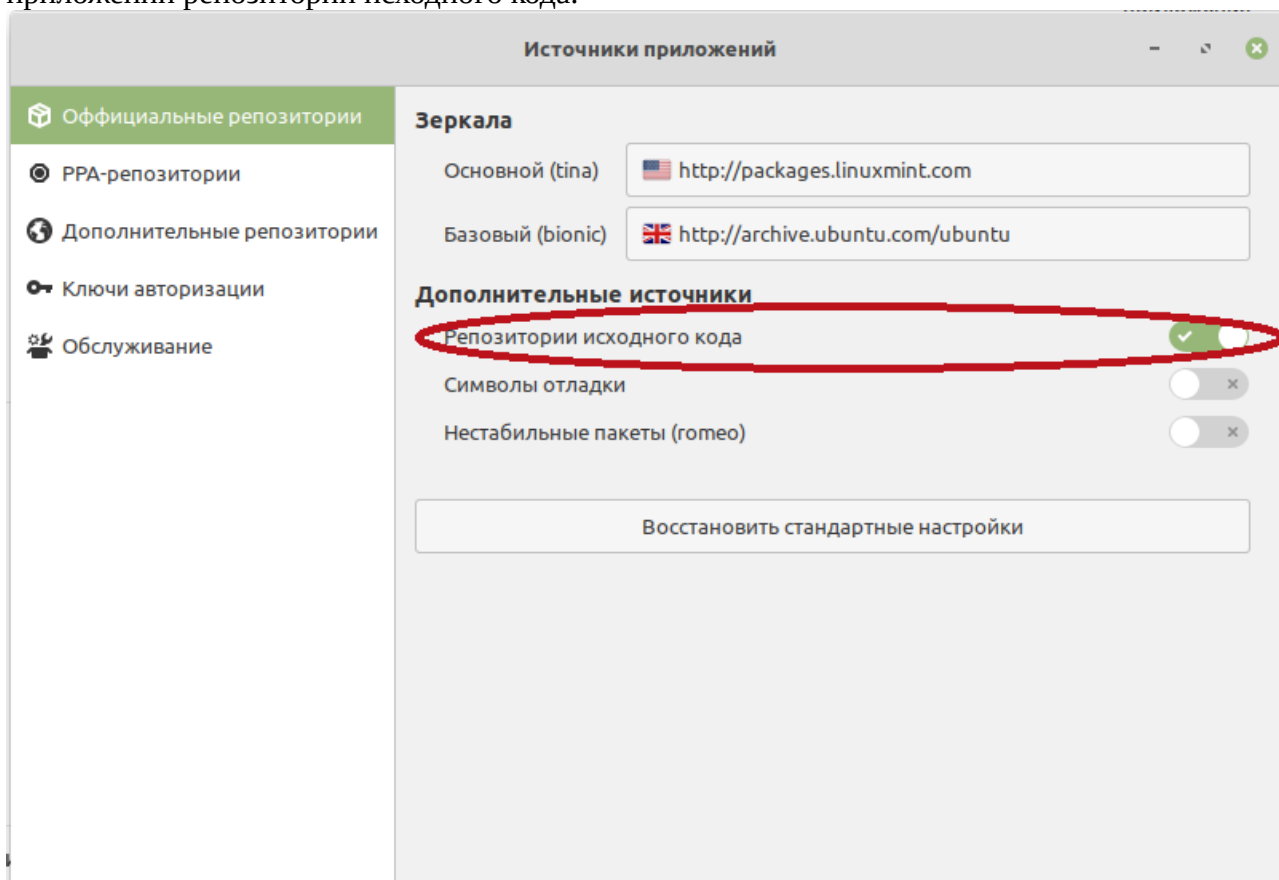
Сконфигурировать правила доступа пользователей в сеть Интернет на **прокси-сервере SQUID**

**1. Подготовительный(начальный) этап:** установка необходимых инструментов для сборки из исходников(сорцов) подходящей нам версии Squid.

```
$ sudo apt install dpkg-dev libldap2-dev libpam0g-dev libdb-dev cdb libsas12-dev debhelper libcppunit-dev libkrb5-dev comerr-dev libcap2-dev libcap3-dev libexpat1-dev
```

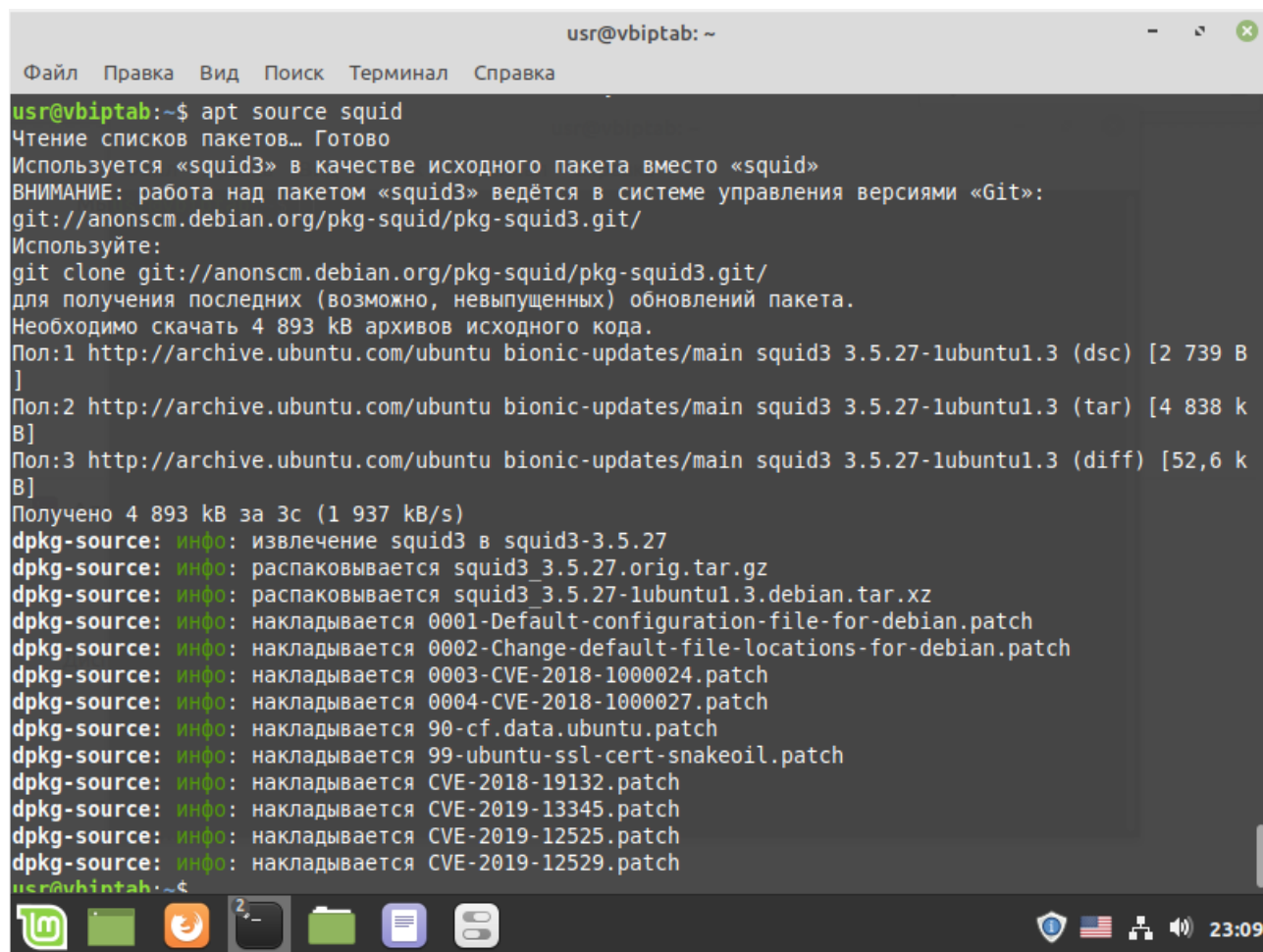
```
$ sudo apt install libxml2-dev autotools-dev libltdl-dev pkg-config libnetfilter-conntrack-dev nettle-dev libgnutls28-dev libssl1.0-dev
```

Далее для скачивания необходимых нам файлов сорцов, разрешаем в источниках приложений репозитории исходного кода:



скачиваем исходники следующей командой:

*\$ apt source squid*



```
usr@vbipatb:~$ apt source squid
Чтение списков пакетов... Готово
Используется «squid3» в качестве исходного пакета вместо «squid»
ВНИМАНИЕ: работа над пакетом «squid3» ведётся в системе управления версиями «Git»:
git://anonscm.debian.org/pkg-squid/pkg-squid3.git/
Используйте:
git clone git://anonscm.debian.org/pkg-squid/pkg-squid3.git/
для получения последних (возможно, невыпущенных) обновлений пакета.
Необходимо скачать 4 893 kB архивов исходного кода.
Пол:1 http://archive.ubuntu.com/ubuntu bionic-updates/main squid3 3.5.27-1ubuntu1.3 (dsc) [2 739 B
]
Пол:2 http://archive.ubuntu.com/ubuntu bionic-updates/main squid3 3.5.27-1ubuntu1.3 (tar) [4 838 k
B]
Пол:3 http://archive.ubuntu.com/ubuntu bionic-updates/main squid3 3.5.27-1ubuntu1.3 (diff) [52,6 k
B]
Получено 4 893 kB за 3с (1 937 kB/s)
dpkg-source: инфo: извлечение squid3 в squid3-3.5.27
dpkg-source: инфo: распаковывается squid3_3.5.27.orig.tar.gz
dpkg-source: инфo: распаковывается squid3_3.5.27-1ubuntu1.3.debian.tar.xz
dpkg-source: инфo: накладывается 0001-Default-configuration-file-for-debian.patch
dpkg-source: инфo: накладывается 0002-Change-default-file-locations-for-debian.patch
dpkg-source: инфo: накладывается 0003-CVE-2018-1000024.patch
dpkg-source: инфo: накладывается 0004-CVE-2018-1000027.patch
dpkg-source: инфo: накладывается 90-cf.data.ubuntu.patch
dpkg-source: инфo: накладывается 99-ubuntu-ssl-cert-snakeoil.patch
dpkg-source: инфo: накладывается CVE-2018-19132.patch
dpkg-source: инфo: накладывается CVE-2019-13345.patch
dpkg-source: инфo: накладывается CVE-2019-12525.patch
dpkg-source: инфo: накладывается CVE-2019-12529.patch
usr@vbipatb:~$
```

переходим в директорию `~/squid3-3.5.27/` и правим файл

*\$ vim debian/rules*

Ищем строку “`—enable-ecap \`” и ниже добавляем следующее:

```
usr@vbipat: ~/squid3-3.5.27
Файл  Правка  Вид  Поиск  Терминал  Справка

--enable-auth-digest="file,LDAP" \
--enable-auth-negotiate="kerberos,wrapper" \
--enable-auth-ntlm="fake,smb_lm" \
--enable-external-acl-helpers="file_userip,kerberos_ldap_group,LDAP_group,session,
SQL_session,time_quota,unix_group,wbinfo_group" \
--enable-url-rewrite-helpers="fake" \
--enable-eui \
--enable-esi \
--enable-icmp \
--enable-zph-qos \
--enable-ecap \
--enable-ssl --enable-ssl-crtld --with-openssl \
--disable-translation \
--with-swapdir=/var/spool/squid \
--with-logdir=/var/log/squid \
--with-pidfile=/var/run/squid.pid \
--with-filedescriptors=65536 \
--with-large-files \
--with-default-user=proxy

BUILDINFO := $(shell lsb_release -si 2>/dev/null)

DEB_CONFIGURE_EXTRA_FLAGS += --enable-build-info="$(BUILDINFO) $(DEB_HOST_ARCH_OS)"

ifeq ($(DEB_HOST_ARCH_OS), kfreebsd)
    DEB_CONFIGURE_EXTRA_FLAGS += --enable-kqueue
endif
ifeq ($(DEB_HOST_ARCH_OS), linux)
```

Далее в редакторе vi в файл debian/control  
\$ vi debian/control

подключаем **libssl1.0-dev**:

```
usr@vbipat: ~/squid3-3.5.27
Файл  Правка  Вид  Поиск  Терминал  Справка

Source: squid3
Section: web
Priority: optional
Maintainer: Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
XSBC-Original-Maintainer: Luigi Gangitano <luigi@debian.org>
Uploaders: Santiago Garcia Mantinan <manty@debian.org>
Homepage: http://www.squid-cache.org
Standards-Version: 3.9.8
Vcs-Git: git://anonscm.debian.org/pkg-squid/pkg-squid3.git/
Vcs-Browser: https://anonscm.debian.org/git/pkg-squid/pkg-squid3.git/
Build-Depends: libldap2-dev, libpam0g-dev, libdb-dev, cdb, libssl-dev, debhelper (>=10), libcpp
unit-dev, libkrb5-dev, comerr-dev, libcap2-dev [linux-any], libcap3-dev (>= 1.0.1-2), libexpat1-d
ev, libxml2-dev, libltdl-dev, dpkg-dev (>= 1.16.1~), pkg-config, libnetfilter-conntrack-dev [linux
-any], nettle-dev, libgnutls28-dev, lsb-release, dh-apparmor, dh-autoreconf, libssl1.0-dev
XS-Testsuite: autopkgtest

Package: squid3
Architecture: all
Section: oldlibs
Priority: optional
Pre-Depends: squid (>= ${source:Version})
Depends: ${shlibs:Depends}, ${misc:Depends}, lsb-base
Description: Transitional package
  Squid is a high-performance proxy caching server for web clients, supporting
  FTP, gopher, ICY and HTTP data objects.
.
  This is a transitional package used to migrate from squid3 to squid.

Type :qa! and press <Enter> to abandon all changes and exit Vim
```

чтобы в процессе сборки избежать проблем с зависимостями устанавливаем пакет:

```
$ sudo apt-get install dh-apparmor
```

и запускаем процесс сборки командой:

```
usr@vbipatb:~/squid3-3.5.27$ dpkg-buildpackage -rfakeroot -b
```

**Примечание:** лог сборки достаточно объёмный, поэтому выложу его отдельным файлом, чтобы не испортить красоту оформления.

```
usr@vbipatb: ~
Файл  Правка  Вид  Поиск  Терминал  Справка
Распаковывается devscripts (2.17.12ubuntu1.1) ...
Настраивается пакет libfile-homedir-perl (1.002-1) ...
Настраивается пакет devscripts (2.17.12ubuntu1.1) ...
Обрабатываются триггеры для man-db (2.8.3-2ubuntu0.1) ...
usr@vbipatb:~/squid3-3.5.27$ cd ..
usr@vbipatb:~$ ls -l
итого 33096
drwxr-xr-x 20 usr usr      4096 окт 21 00:26 squid3-3.5.27
-rw-r--r--  1 usr usr    147620 окт 21 00:25 squid3_3.5.27-1ubuntu1.3_all.deb
-rw-r--r--  1 usr usr    18135 окт 21 00:26 squid3_3.5.27-1ubuntu1.3_amd64.buildinfo
-rw-r--r--  1 usr usr    3783 окт 21 00:26 squid3_3.5.27-1ubuntu1.3_amd64.changes
-rw-r--r--  1 usr usr   52640 июл 18 22:34 squid3_3.5.27-1ubuntu1.3.debian.tar.xz
-rw-r--r--  1 usr usr    2739 июл 18 22:34 squid3_3.5.27-1ubuntu1.3.dsc
-rw-r--r--  1 usr usr  4837850 фев 27 2018 squid3_3.5.27.orig.tar.gz
-rw-r--r--  1 usr usr  2492396 окт 21 00:26 squid_3.5.27-1ubuntu1.3_amd64.deb
-rw-r--r--  1 usr usr   175620 окт 21 00:26 squid-cgi_3.5.27-1ubuntu1.3_amd64.deb
-rw-r--r--  1 usr usr   178700 окт 21 00:26 squidclient_3.5.27-1ubuntu1.3_amd64.deb
-rw-r--r--  1 usr usr   293452 окт 21 00:25 squid-common_3.5.27-1ubuntu1.3_all.deb
-rw-r--r--  1 usr usr 25463320 окт 21 00:26 squid-dbg_3.5.27-1ubuntu1.3_amd64.deb
-rw-r--r--  1 usr usr   166820 окт 21 00:26 squid-purge_3.5.27-1ubuntu1.3_amd64.deb
drwxr-xr-x  2 usr usr    4096 окт  6 10:47 Видео
drwxr-xr-x  2 usr usr    4096 окт  6 22:10 Документы
drwxr-xr-x  2 usr usr    4096 окт  6 10:47 Загрузки
drwxr-xr-x  2 usr usr    4096 окт 20 23:36 Изображения
drwxr-xr-x  2 usr usr    4096 окт  6 10:47 Музыка
drwxr-xr-x  2 usr usr    4096 окт  6 10:47 Общедоступные
drwxr-xr-x  2 usr usr    4096 окт 21 00:40 'Рабочий стол'
drwxr-xr-x  2 usr usr    4096 окт  6 10:47 Шаблоны
usr@vbipatb:~$
```

После завершения сборки устанавливаем squid командой:

```
usr@vbipatb:~$ sudo dpkg -i *.deb
```

и исправляем проблему зависимостей командой:

```
usr@vbipatb:~$ sudo apt-get -f install
```

Затем переходим в папку с только что установленным squid: `/etc/squid/` и создаём в ней директорию `ssl_cert`, назначаем ей права `chmod 700 ssl_cert/`. Далее будем генерировать сертификаты для **https://** защищённых соединений:

```
root@vbiptab: /etc/squid/ssl_cert
Файл  Правка  Вид  Поиск  Терминал  Справка
usr@vbiptab:~$ sudo -i
root@vbiptab:~# cd /etc/squid
root@vbiptab:/etc/squid# mkdir ssl_cert
root@vbiptab:/etc/squid# chmod 700 ssl_cert/
root@vbiptab:/etc/squid# cd ssl_cert
root@vbiptab:/etc/squid/ssl_cert# openssl req -new -newkey rsa:2048 -sha256 -days 1200 -nodes -x509 -extensions v3_ca -keyout ruCA.pem -out ruCA.pem
Can't load /root/.rnd into RNG
139732392100288:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/rand/randfile.c:88:Filename=/root/.rnd
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'ruCA.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-State]:Orenburg
Locality Name (eg, city) []:Orenburg city
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Tehnoprom
Organizational Unit Name (eg, section) []:it-spec
Common Name (e.g. server FQDN or YOUR name) []:Labuzhskiy
Email Address []:labuzhskiy@ya.ru
root@vbiptab:/etc/squid/ssl_cert#
```

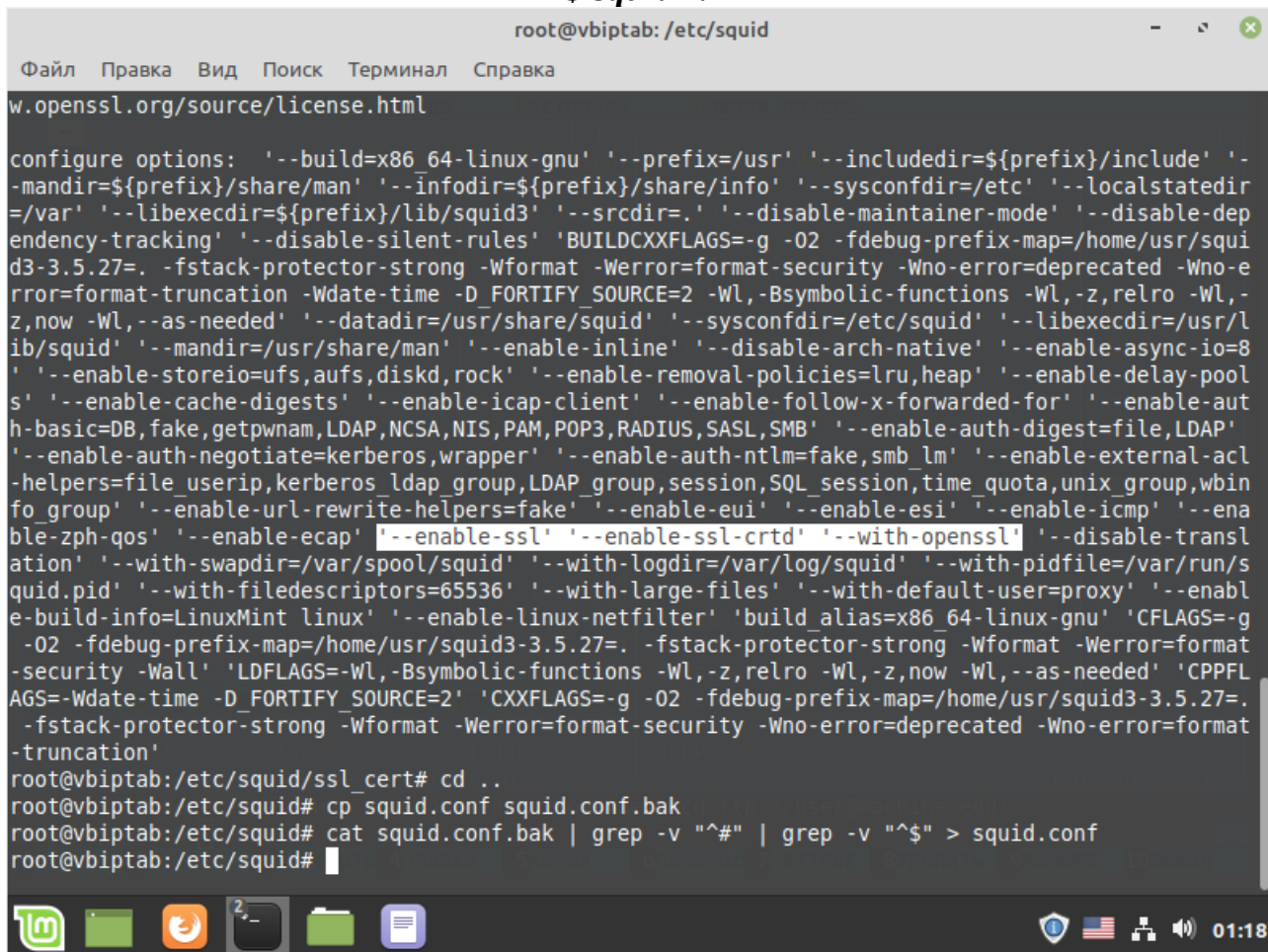
```
root@vbiptab: /etc/squid/ssl_cert
Файл  Правка  Вид  Поиск  Терминал  Справка
.....+++++
.....+++++
writing new private key to 'ruCA.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-State]:Orenburg
Locality Name (eg, city) []:Orenburg city
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Tehnoprom
Organizational Unit Name (eg, section) []:it-spec
Common Name (e.g. server FQDN or YOUR name) []:Labuzhskiy
Email Address []:labuzhskiy@ya.ru
root@vbiptab:/etc/squid/ssl_cert# openssl x509 -in ruCA.pem -outform DER -out ruCA.der
root@vbiptab:/etc/squid/ssl_cert# ll
итого 16
drwx----- 2 root root 4096 окт 21 01:02 ./
drwxr-xr-x 3 root root 4096 окт 21 00:49 ../
-rw-r--r-- 1 root root 1039 окт 21 01:02 ruCA.der
-rw----- 1 root root 3168 окт 21 00:58 ruCA.pem
root@vbiptab:/etc/squid/ssl_cert# /usr/lib/squid/ssl_crted -c -s /var/lib/ssl_db
Initialization SSL db...
Done
root@vbiptab:/etc/squid/ssl_cert#
```



На основе сертификата закрытого ключа, создаём сертификат открытого ключа и генерируем базу данных `ssl_db`.

Убедимся, что в собранной нами версии *Squid* присутствует необходимый набор опций, заявленных перед началом сборки, для этого выполним команду:

**\$ squid -v**



```
root@vbiptab: /etc/squid
Файл Правка Вид Поиск Терминал Справка
w.openssl.org/source/license.html

configure options: '--build=x86_64-linux-gnu' '--prefix=/usr' '--includedir=${prefix}/include' '-
-mandir=${prefix}/share/man' '--infodir=${prefix}/share/info' '--sysconfdir=/etc' '--localstatedir
=/var' '--libexecdir=${prefix}/lib/squid3' '--srcdir=' '--disable-maintainer-mode' '--disable-dep
endency-tracking' '--disable-silent-rules' 'BUILDCXXFLAGS=-g -O2 -fdebug-prefix-map=/home/usr/squi
d3-3.5.27=. -fstack-protector-strong -Wformat -Werror=format-security -Wno-error=deprecated -Wno-e
rror=format-truncation -Wdate-time -D_FORTIFY_SOURCE=2 -Wl,-Bsymbolic-functions -Wl,-z,relro -Wl,-
z,now -Wl,--as-needed' '--datadir=/usr/share/squid' '--sysconfdir=/etc/squid' '--libexecdir=/usr/l
ib/squid' '--mandir=/usr/share/man' '--enable-inline' '--disable-arch-native' '--enable-async-io=8
' '--enable-storeio=ufs,aufs,diskd,rock' '--enable-removal-policies=lru,heap' '--enable-delay-pool
s' '--enable-cache-digests' '--enable-icap-client' '--enable-follow-x-forwarded-for' '--enable-aut
h-basic=DB,fake,getpwnam,LDAP,NCSA,NIS,PAM,POP3,RADIUS,SASL,SMB' '--enable-auth-digest=file,LDAP'
'--enable-auth-negotiate=kerberos,wrapper' '--enable-auth-ntlm=fake,smb_lm' '--enable-external-acl
-helpers=file_userip,kerberos_ldap_group,LDAP_group,session,SQL_session,time_quota,unix_group,wbin
fo_group' '--enable-url-rewrite-helpers=fake' '--enable-eui' '--enable-esi' '--enable-icmp' '--ena
ble-zph-qos' '--enable-ecap' '--enable-ssl' '--enable-ssl-crtid' '--with-openssl' '--disable-transl
ation' '--with-swapdir=/var/spool/squid' '--with-logdir=/var/log/squid' '--with-pidfile=/var/run/s
quid.pid' '--with-filedescriptors=65536' '--with-large-files' '--with-default-user=proxy' '--enabl
e-build-info=LinuxMint linux' '--enable-linux-netfilter' 'build_alias=x86_64-linux-gnu' 'CFLAGS=-g
-O2 -fdebug-prefix-map=/home/usr/squid3-3.5.27=. -fstack-protector-strong -Wformat -Werror=format
-security -Wall' 'LDFLAGS=-Wl,-Bsymbolic-functions -Wl,-z,relro -Wl,-z,now -Wl,--as-needed' 'CPPFL
AGS=-Wdate-time -D_FORTIFY_SOURCE=2' 'CXXFLAGS=-g -O2 -fdebug-prefix-map=/home/usr/squid3-3.5.27=.
-fstack-protector-strong -Wformat -Werror=format-security -Wno-error=deprecated -Wno-error=format
-truncation'
root@vbiptab:/etc/squid/ssl_cert# cd ..
root@vbiptab:/etc/squid# cp squid.conf squid.conf.bak
root@vbiptab:/etc/squid# cat squid.conf.bak | grep -v "^#" | grep -v "$" > squid.conf
root@vbiptab:/etc/squid#
```

Теперь создадим резервную копию файла **squid.conf**, перед началом настройки.

Перезапишем оригинальный конфигурационный файл **squid.conf**, выполнив отбор строк из резервной копии файла с усечением комментариев и строк, содержащих символ «\$»,

затем приведём получившийся конфиг-файл к рабочей версии: для этого укажем параметры нашей ЛВС **localnet**, и параметры сетевого интерфейса, обрабатывающего **http** и **https** запросы в прозрачном режиме; а для случая **https** – ещё и с подстановкой сгенерированного нами сертификата.

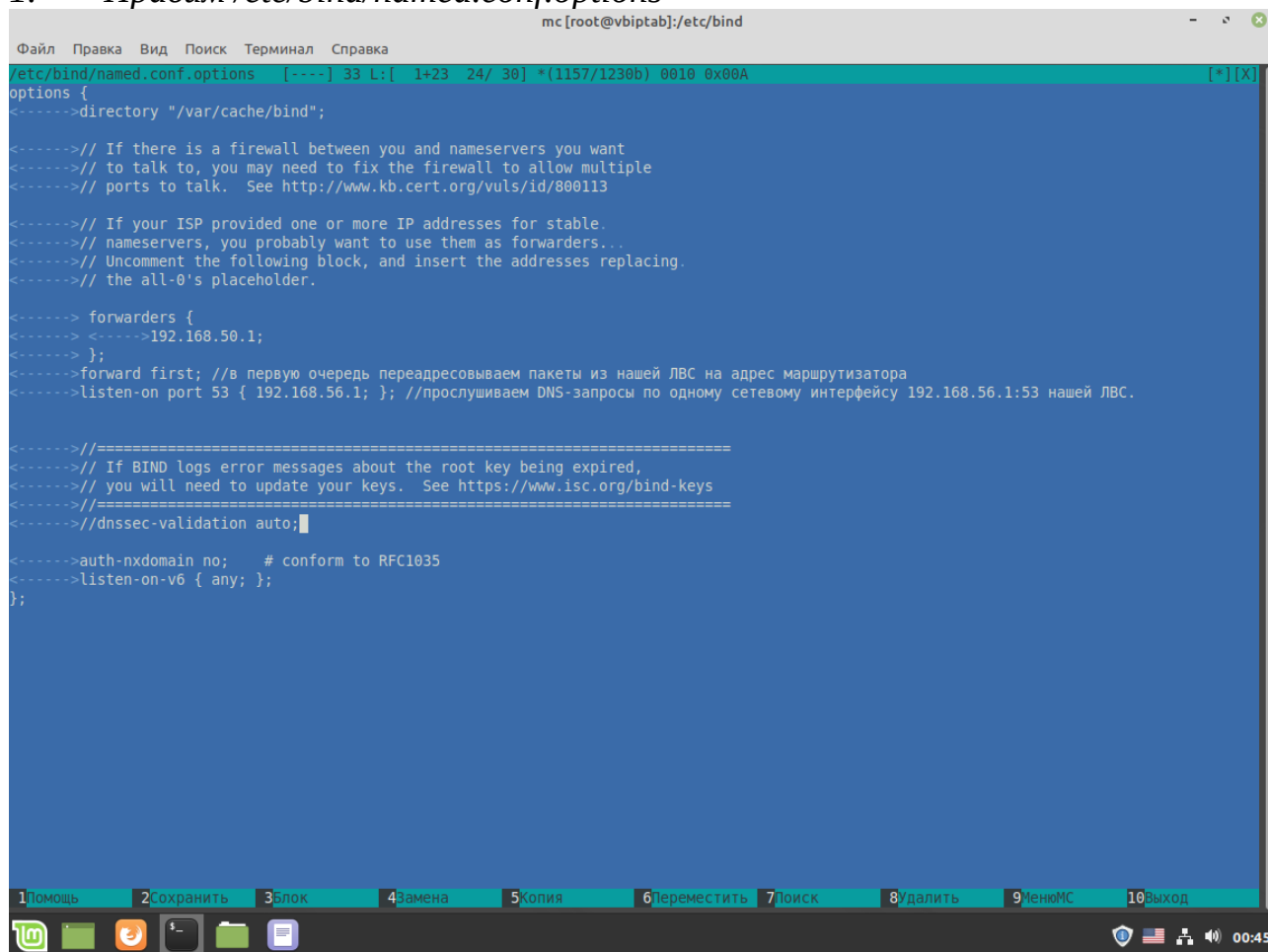
```
mc [root@vbiptab]:/etc/squid
Файл Правка Вид Поиск Терминал Справка
/etc/squid/squid.conf [----] 32 L: [ 1+ 0 1/ 32] *(32 /1117b) 0010 0x00A [*][X]
acl localnet src 192.168.56.0/24
acl SSL_ports port 443
acl Safe_ports port 80<-----># http
acl Safe_ports port 21<-----># ftp
acl Safe_ports port 443<-----># 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
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
http_access allow localhost
http_access allow localnet
http_access deny all
http_port 192.168.56.1:3128 intercept
https_port 192.168.56.1:3129 intercept ssl-bump cert=/etc/squid/ssl_cert/ruCA.pem
ssl_bump peek all
ssl_bump splice all
sslcrtld_program /usr/lib/squid/ssl_crtld -s /var/lib/ssl_db -M 4MB
coredump_dir /var/spool/squid
refresh_pattern ^ftp:<----->1440<---->20%<---->10080
refresh_pattern ^gopher:<----->1440<---->0%<---->1440
refresh_pattern -i (/cgi-bin/|\?) 0<---->0%<---->0
refresh_pattern (Release|Packages|.gz)*$ 0 20% 2880
refresh_pattern .<----->0<----->20%<---->4320
1Помощь 2Сохранить 3Блок 4Замена 5Копия 6Переместить 7Поиск 8Удалить 9МенюМС 10Выход
```

Парсим, получаем следующее:

```
root@vbiptab:~/squid3-3.5.27/debian# squid -k parse
2019/10/24 00:02:07 Startup: Initializing Authentication Schemes ...
2019/10/24 00:02:07 Startup: Initialized Authentication Scheme 'basic'
2019/10/24 00:02:07 Startup: Initialized Authentication Scheme 'digest'
2019/10/24 00:02:07 Startup: Initialized Authentication Scheme 'negotiate'
2019/10/24 00:02:07 Startup: Initialized Authentication Scheme 'ntlm'
2019/10/24 00:02:07 Startup: Initialized Authentication
2019/10/24 00:02:07 Processing Configuration File: /etc/squid/squid.conf (depth 0)
2019/10/24 00:02:07 Processing: acl localnet src 192.168.56.0/24
2019/10/24 00:02:07 Processing: acl SSL_ports port 443
2019/10/24 00:02:07 Processing: acl Safe_ports port 80 # http
2019/10/24 00:02:07 Processing: acl Safe_ports port 21 # ftp
2019/10/24 00:02:07 Processing: acl Safe_ports port 443 # https
2019/10/24 00:02:07 Processing: acl Safe_ports port 70 # gopher
2019/10/24 00:02:07 Processing: acl Safe_ports port 210 # wais
2019/10/24 00:02:07 Processing: acl Safe_ports port 1025-65535 # unregistered ports
2019/10/24 00:02:07 Processing: acl Safe_ports port 280 # http-mgmt
2019/10/24 00:02:07 Processing: acl Safe_ports port 488 # gss-http
2019/10/24 00:02:07 Processing: acl Safe_ports port 591 # filemaker
2019/10/24 00:02:07 Processing: acl Safe_ports port 777 # multiling http
2019/10/24 00:02:07 Processing: acl CONNECT method CONNECT
2019/10/24 00:02:07 Processing: http_access deny !Safe_ports
2019/10/24 00:02:07 Processing: http_access deny CONNECT !SSL_ports
2019/10/24 00:02:07 Processing: http_access allow localhost manager
2019/10/24 00:02:07 Processing: http_access deny manager
2019/10/24 00:02:07 Processing: http_access allow localhost
2019/10/24 00:02:07 Processing: http_access allow localnet
2019/10/24 00:02:07 Processing: http_access deny all
2019/10/24 00:02:07 Processing: http_port 192.168.56.1:3128 intercept
2019/10/24 00:02:07 Starting Authentication on port 192.168.56.1:3128
2019/10/24 00:02:07 Disabling Authentication on port 192.168.56.1:3128 (interception enabled)
2019/10/24 00:02:07 Processing: https_port 192.168.56.1:3129 intercept ssl-bump cert=/etc/squid/ssl_cert/ruCA.pem
2019/10/24 00:02:07 Starting Authentication on port 192.168.56.1:3129
2019/10/24 00:02:07 Disabling Authentication on port 192.168.56.1:3129 (interception enabled)
2019/10/24 00:02:07 Processing: ssl_bump peek all
2019/10/24 00:02:07 Processing: ssl_bump splice all
2019/10/24 00:02:07 Processing: sslcrtld_program /usr/lib/squid/ssl_crtld -s /var/lib/ssl_db -M 4MB
2019/10/24 00:02:07 Processing: coredump_dir /var/spool/squid
2019/10/24 00:02:07 Processing: refresh_pattern ^ftp: 1440 20% 10080
2019/10/24 00:02:07 Processing: refresh_pattern ^gopher: 1440 0% 1440
2019/10/24 00:02:07 Processing: refresh_pattern -i (/cgi-bin/|\?) 0 0% 0
2019/10/24 00:02:07 Processing: refresh_pattern (Release|Packages|.gz)*$ 0 20% 2880
2019/10/24 00:02:07 Processing: refresh_pattern . 0 20% 4320
2019/10/24 00:02:07 Initializing https proxy context
2019/10/24 00:02:07 Initializing https_port 192.168.56.1:3129 SSL context
2019/10/24 00:02:07 Using certificate in /etc/squid/ssl_cert/ruCA.pem
root@vbiptab:~/squid3-3.5.27/debian#
```

Далее нужно выполнить настройку **BIND9** на форвардинг пакетов компьютеров ЛВС на главный маршрутизатор организации и перенастроить **iptables** таким образом, чтобы все наши пакеты проходили через **BIND9**.

## 1. Правим /etc/bind/named.conf.options



```
mc [root@vbipstab]:/etc/bind
Файл  Правка  Вид  Поиск  Терминал  Справка
/etc/bind/named.conf.options  [----] 33 L: 1+23 24/ 30] *(1157/1230b) 0010 0x00A [*][X]
options {
<----->directory "/var/cache/bind";

<----->// If there is a firewall between you and nameservers you want
<----->// to talk to, you may need to fix the firewall to allow multiple
<----->// ports to talk.  See http://www.kb.cert.org/vuls/id/800113

<----->// If your ISP provided one or more IP addresses for stable.
<----->// nameservers, you probably want to use them as forwarders...
<----->// Uncomment the following block, and insert the addresses replacing.
<----->// the all-0's placeholder.

<-----> forwarders {
<-----> <----->192.168.50.1;
<-----> };
<----->forward first; //в первую очередь переадресовываем пакеты из нашей ЛВС на адрес маршрутизатора
<----->listen-on port 53 { 192.168.56.1; }; //прослушиваем DNS-запросы по одному сетевому интерфейсу 192.168.56.1:53 нашей ЛВС.

<----->//=====
<----->// If BIND logs error messages about the root key being expired,
<----->// you will need to update your keys.  See https://www.isc.org/bind-keys
<----->//=====
<----->//dnssec-validation auto;

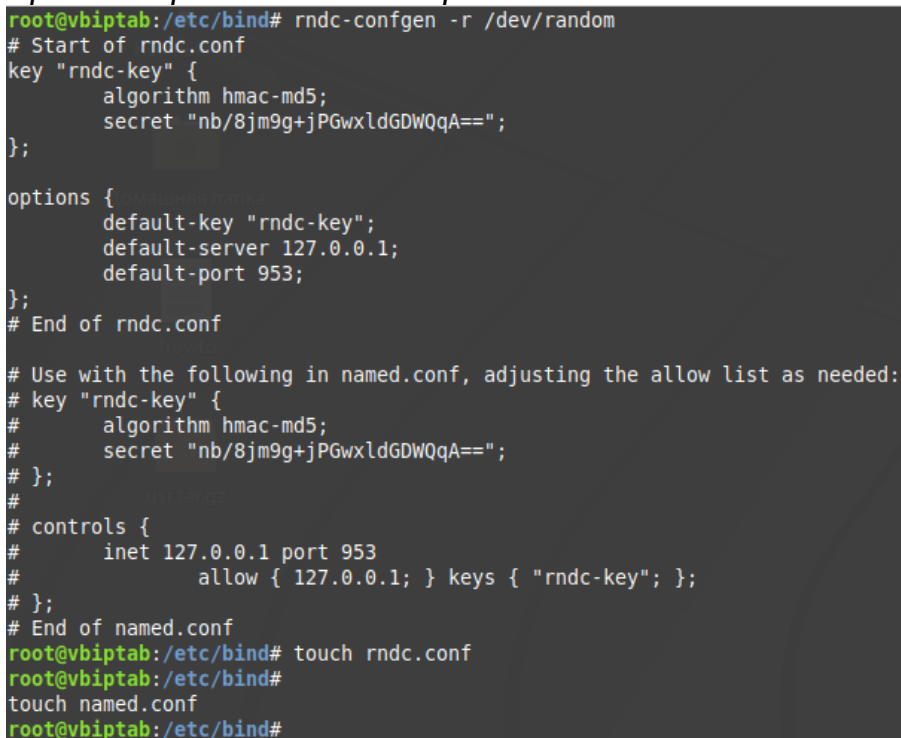
<----->auth-nxdomain no;      # conform to RFC1035
<----->listen-on-v6 { any; };
};

1Помощь  2Сохранить  3Блок  4Замена  5Копия  6Переместить  7Поиск  8Удалить  9МенюМС  10Выход
```

## 2. Выполняем команду

**# rndc-confgen -r /dev/urandom**

а результат выполнения пересохраняем 2-мя файлами: **rndc.conf** и **named.conf**, раскомментировав строки в **named.conf**



```
root@vbipstab:/etc/bind# rndc-confgen -r /dev/random
# Start of rndc.conf
key "rndc-key" {
    algorithm hmac-md5;
    secret "nb/8jm9g+jPGwxldGDWQqA==";
};

options {
    default-key "rndc-key";
    default-server 127.0.0.1;
    default-port 953;
};
# End of rndc.conf

# Use with the following in named.conf, adjusting the allow list as needed:
# key "rndc-key" {
#     algorithm hmac-md5;
#     secret "nb/8jm9g+jPGwxldGDWQqA==";
# };
#
# controls {
#     inet 127.0.0.1 port 953
#     allow { 127.0.0.1; } keys { "rndc-key"; };
# };
# End of named.conf
root@vbipstab:/etc/bind# touch rndc.conf
root@vbipstab:/etc/bind# touch named.conf
root@vbipstab:/etc/bind#
```



mc [root@vbiptab]:/etc/bind

Файл Правка Вид Поиск Терминал Справка

217/217 100%

/etc/bind/rndc.conf

# Start of rndc.conf

key "rndc-key" {

algorithm hmac-md5;

secret "nb/8jm9g+jPGwxldGDWQqA==";

};

options {

default-key "rndc-key";

default-server 127.0.0.1;

default-port 953;

};

# End of rndc.conf

1Помощь 2Разверн 3Выход 4lex 5Перейти 6 7Поиск 8Сходный 9Формат 10Выход

mc [root@vbiptab]:/etc/bind

Файл Правка Вид Поиск Терминал Справка

217/217 100%

/etc/bind/named.conf

[-----] 0 L:[ 1+22 23/ 23] \*(731 / 731b) <EOF>

// This is the primary configuration file for the BIND DNS server named.

//

// Please read /usr/share/doc/bind9/README.Debian.gz for information on the.

// structure of BIND configuration files in Debian, \*BEFORE\* you customize.

// this configuration file.

//

// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";

include "/etc/bind/named.conf.local";

include "/etc/bind/named.conf.default-zones";

# Use with the following in named.conf, adjusting the allow list as needed:

key "rndc-key" {

<----->algorithm hmac-md5;

<----->secret "nb/8jm9g+jPGwxldGDWQqA==";

};

#

controls {

<----->inet 127.0.0.1 port 953

<-----><----->allow { 127.0.0.1; } keys { "rndc-key"; };

};

# End of named.conf

1Помощь 2Сохранить 3Блок 4Замена 5Копия 6Переместить 7Поиск 8Удалить 9МенюМС 10Выход

Т.к. служба **rndc** в настройках «по умолчанию» контролируется через петлевой интерфейс **lo**, **127.0.0.1**, и требует разрешающее правило по порту **953**, закрытому в **iptables**, добавляем → новое разрешающее правило **iptables** вида:

**\$ sudo iptables -A INPUT -i lo -j ACCEPT**

затем убираем лишние правила по **53** порту из цепочки **FORWARD**:

```
root@vbiptab:/etc/bind# iptables -D FORWARD -s 192.168.56.0/24 -p tcp -m multiport --ports 53,80,443 -j ACCEPT
root@vbiptab:/etc/bind# iptables -A FORWARD -s 192.168.56.0/24 -p tcp -m multiport --ports 80,443 -j ACCEPT
root@vbiptab:/etc/bind# iptables -D FORWARD -s 192.168.56.0/24 -p udp -m multiport --ports 53 -j ACCEPT
root@vbiptab:/etc/bind# iptables -A INPUT -s 192.168.56.0/24 -p udp -m multiport --ports 53 -j ACCEPT
root@vbiptab:/etc/bind# iptables -P INPUT DROP
root@vbiptab:/etc/bind# iptables-save
```

и пересоздаём правила для протоколов **tcp** и **udp** по порту **53** в цепочке **INPUT**.

```
root@vbiptab:/etc/bind# iptables -A INPUT -s 192.168.56.0/24 -p tcp -m multiport --ports 53 -j ACCEPT
root@vbiptab:/etc/bind# iptables-save
```

```
# Generated by iptables-save v1.6.1 on Thu Oct 24 01:48:43 2019
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -p tcp -m multiport --ports 2002,8080,8081 -j ACCEPT
-A INPUT -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -s 192.168.56.0/24 -p udp -m multiport --ports 53 -j ACCEPT
-A INPUT -s 192.168.56.0/24 -p tcp -m multiport --ports 53 -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i enp0s3 -p tcp -m tcp --dport 22 -j ACCEPT
-A FORWARD -i enp0s3 -p tcp -m tcp --dport 80 -j ACCEPT
-A FORWARD -i enp0s3 -p tcp -m tcp --dport 443 -j ACCEPT
-A FORWARD -p icmp -j ACCEPT
-A FORWARD -s 192.168.56.0/24 -p tcp -m multiport --ports 80,443 -j ACCEPT
COMMIT
# Completed on Thu Oct 24 01:48:43 2019
# Generated by iptables-save v1.6.1 on Thu Oct 24 01:48:43 2019
*nat
:PREROUTING ACCEPT [872:97441]
:INPUT ACCEPT [856:94950]
:OUTPUT ACCEPT [686:52452]
:POSTROUTING ACCEPT [655:49677]
-A PREROUTING -i enp0s3 -p tcp -m tcp --dport 8080 -j DNAT --to-destination 192.168.56.2:80
-A PREROUTING -i enp0s3 -p tcp -m tcp --dport 8081 -j DNAT --to-destination 192.168.56.2:443
-A PREROUTING -i enp0s3 -p tcp -m tcp --dport 2002 -j DNAT --to-destination 192.168.56.2:22
-A POSTROUTING -s 192.168.56.0/24 -j MASQUERADE
COMMIT
# Completed on Thu Oct 24 01:48:43 2019
root@vbiptab:/etc/bind#
```

И сохраняем настройки:

**\$ sudo dpkg-reconfigure iptables-persistent**

Проверка из Windows-ЛВС с компьютеров пользователей:  
работает.

