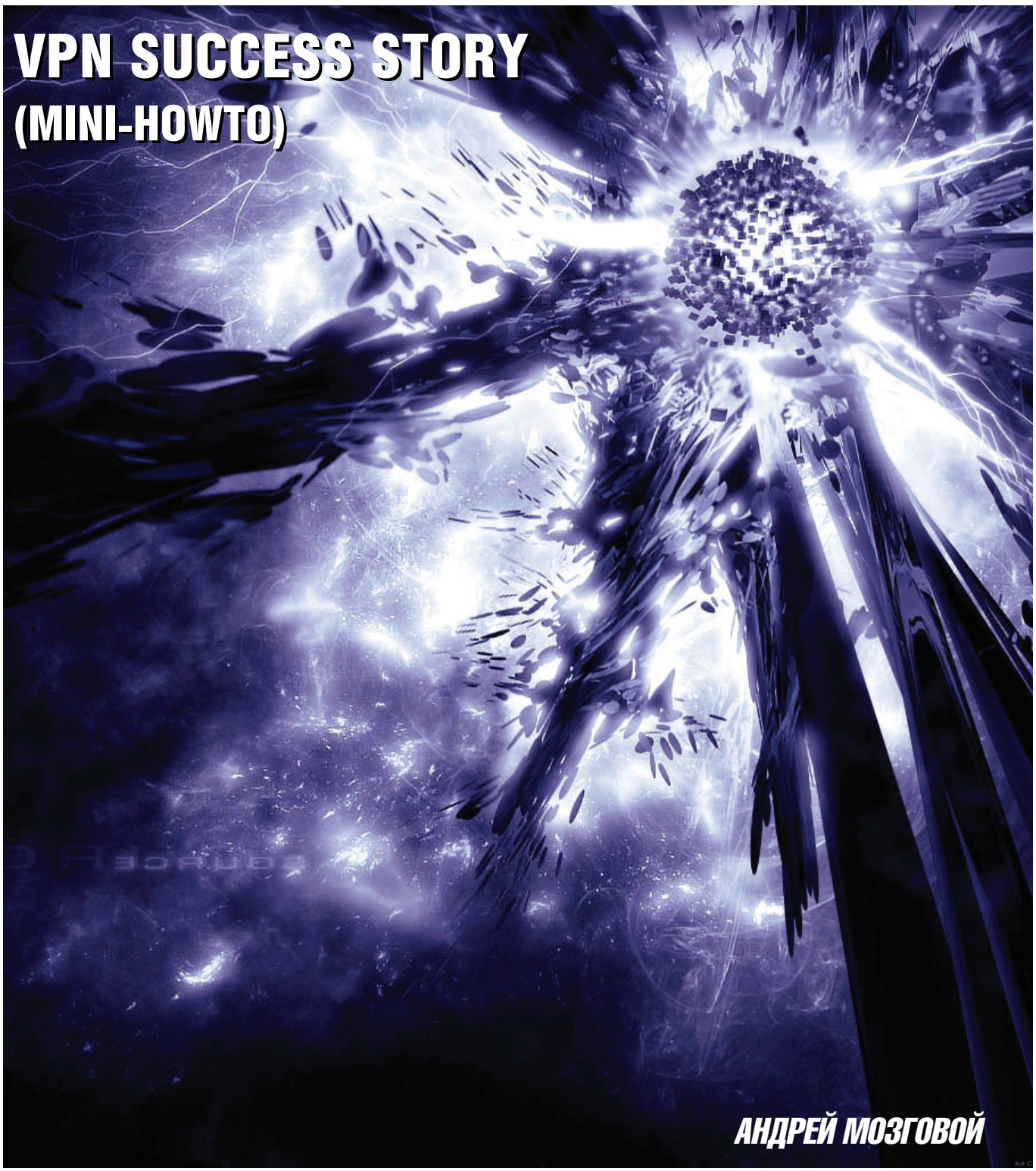
VPN SUCCESS STORY (MINI-HOWTO)



АНДРЕЙ МОЗГОВОЙ

Хочу рассказать вам о благополучном поднятии VPN в локальной сети. Учтите, пожалуйста, что VPN был организован не для соединения удаленных сетей, а для решения проблемы «подмены IP- и MAC-адресов пользователями локальной сети».

Для аутентификации будем использовать протокол MS-CHAP-v2. Для шифрования трафика используется MPPE (Microsoft Point-to-Point Encryption). MPPE – это протокол, разработанный специально для передачи зашифрованных дейтаграмм по соединению точка-точка (point-to-point).

Дистрибутив Slackware 9.1. Ядро Linux-2.4.24.

Вам так же понадобятся ppp-2.4.2b3 и poptop-1.1.4-b4. Желательно использовать последний ppp-cvs, так как в его дереве уже имеется скрипт, который вносит в ядро необходимые изменения.

Poptop – это VPN-сервер, к которому подключаются клиенты.

Замечание: во время редактирования настоящей статьи вышел релиз ppp-2.4.2. Автор уже проверил его работоспособность – все в порядке.

- Собираем pppd:

```
./configure
make
make install
```

- Скриптом mppeinstall.sh из ppp-2.4.2b3/linux/mppe патчим ядро. Хотя в ppp-2.4.2b3 нет патча для ядра linux-2.4.24, к ядру удачно применяется патч для linux-2.2.20.
- Заходим в конфигурацию ядра. Нам нужен раздел «Network device support». В нем включаем поддержку протокола PPP, несколько дополнительных модулей и новую опцию MPPE-шифрования (по возможности включайте опции модулями). В «make menuconfig» конфигурация должна выглядеть примерно так:

```
<M>   PPP (point-to-point protocol) support
[*]   PPP multilink support (EXPERIMENTAL)
[*]   PPP filtering
<M>   PPP support for async serial ports
<M>   PPP support for sync tty ports
<M>   PPP Deflate compression
<M>   PPP BSD-Compress compression
<M>   PPP MPPE compression (encryption)
<M>   PPP over Ethernet (EXPERIMENTAL)
```

В разделе «Cryptographic options» включите «Cryptographic API», в нем обязательно включите «SHA1 digest algorithm» и «ARCFOUR» (ARCFOUR сказано включить в документации, но такого в linux-2.4.24 нет. Предполагаю, что еще необходимо включить «HMAC support» и «MD5 digest algorithm», остальные – на ваше усмотрение). Сохраняем изменения, пересобираем ядро и модули.

- Собираем poptop:

```
./configure --with-pppd-ip-alloc.
/* дополнительная опция для снятия ограничения
* на количество сессий и еще кое-что полезное с
* выделением IP-адресов.
*/
make
make install
```

Настройка:

```
Файл /etc/ppp/options
lock

Файл /etc/ppp/options.pptpd
#debug
ipparam PoPToP
lock
mtu 1490
mru 1490
ms-dns <your dns ip addr>
proxyarp
auth
refuse-pap
refuse-chap
refuse-mschap
require-mschap-v2
require-mppe
require-mppe-128
ipcp-accept-local
ipcp-accept-remote
lcp-echo-failure 30
lcp-echo-interval 5
deflate 0
```

Замечание: как сказано выше, для аутентификации используем только ms-chap-v2. Чтобы узнать больше о параметрах и их значениях, загляните в man 8 pppd.

```
Файл /etc/pptpd.conf
#debug
speed 115200
option /etc/ppp/options.pptpd
#localip 10.0.0.1
#remoteip 10.0.0.2-254
```

Замечание: последние две строки не имеют особого смысла, если poptop собирался с параметром «--with-pppd-ip-alloc».

Запускается все следующим скриптом:

```
Файл /etc/rc.d/rc.pptpd
#!/bin/sh
#
# /etc/rc.d/rc.pptpd
#
# description: control pptp server
#

case "$1" in
start)
     modprobe ppp_async
     modprobe ppp_generic
     modprobe ppp_mppe
     modprobe slhc
     if /usr/local/sbin/pptpd; then
         touch /var/lock/subsys/pptpd
     fi
     ;;
stop)
     killall -TERM pptpd
     rm -f /var/lock/subsys/pptpd
     ;;
restart)
     killall pptpd
     if /usr/local/sbin/pptpd; then
         touch /var/lock/subsys/pptpd
     fi
     ;;
status)
     ifconfig
     ;;
*)
     echo "Usage: $0 {start|stop|restart|status}"
     ;;
esac
```

Пользователи прописываются в /etc/ppp/chap-secrets. Формат файла и пример заполнения:

```
# Secrets for authentication using CHAP
# client          server secret               IP addresses
  test            *      test                 192.168.1.5
```

Все мелкие детали, надеюсь, додумаете сами.

А трафик считать – милое дело! (man pppd, раздел SCRIPTS). Есть такие файлы /etc/ppp/ip-up и /etc/ppp/ip-down, которые pppd запускает в начале и в конце соединения соответственно. А им (этим файлам) передаются такие интересные параметры, как, например, логин, время на линии, скорость, сколько получено и отослано байт и т. д.

Как настроить клиентов, почитайте тут: http://poptop.sourceforge.net/dox/.

Замечание: администраторам, которые решили реализовать в своей сети VPN-доступ, поможет DHCP-сервис. Предварительно, до установки VPN-соединения, адреса в сети можно раздавать с помощью DHCP, из какой-нибудь внутренней сети (192.168.1.0/24) без выхода в Интернет, главное, чтобы VPN-шлюз был доступен. Доступ в Интернет у пользователей будет появляться только после установления VPN-соединения.

Отдельное спасибо Дмитрию Коптеву за помощь в организации соединения и Андрею Бешкову за критику.