VPN по протоколу PPTP на PoPToP.

Автор: lissyara.
Оригинал: http://www.lissyara.su/articles/freebsd/security/poptop/

Подкинули халтуру - надо организовать, чтобы люди могли из дома ходить в рабочую сетку, терминально работать с 1с, и прочие прелести :) Копание инета дало - форточки много чего поддерживают, но для данного случая подходил только протокол PPTP (мне не хотелось замутов с ключами, да и настройка виндовой части там сложней - а инструктировать тётеньку-заказчика не было никакого желания, т.к. она малость подтормаживала :))
PPTP (Point-to-Point Tunneling Protocol) — туннельный протокол типа точка-точка. Не самый удачный выбор, т.к. спецификация на него не была ратифицированна - он не считается настолько же безопастным протоколом как другие VPN протоколы - IPSec, например...
Первым делом проверяем наличие псевдо-устройства tun и ppp в ядре - без них работать не будет.pseudo-device ppp 1 # Kernel PPP
pseudo-device tun # Packet tunnel.

Если они закомментированы - раскомментируем и пересобираем ядро. Затем обновляем порты и устанавливаем PoPToP: /root/>cd /usr/ports/
/usr/ports/>make search name='poptop'
Port: poptop-1.2.3
Path: /usr/ports/net/poptop
Info: Windows 9x compatible PPTP (VPN) server
Maint: olmi@rentech.ru
B-deps: expat-1.95.8_3 gettext-0.14.5 gmake-3.80_2 libiconv-1.9.2_1
R-deps: rc_subr-1.31_1
WWW: http://www.poptop.org/

/usr/ports/>cd /usr/ports/net/poptop
/usr/ports/net/poptop/>make && make install && make clean

После инсталляции правим конфиг PoPToP до такого состояния:
/usr/local/etc/pptpd.confoptions /etc/ppp/options.pptpd
debug
noipparam

debug - это только на время отладки, потом можно закомментровать. И не забудте noipparam - без неё работать не будет, сам наступил на эти грабли, ковырялся два дня, ползал по инету в поисках ответов на вопрос - что за ругань в логах на Warning: Label

ipparam rejected -direct connection: Configuration label not found

а кончилось всё как всегда - надо было прочесть man на pptpd.conf :)
Затем создаём/радактируем следующие файлы:
/etc/ppp/ppp.confpptp:

```
 enable proxy                # для работы внутри локальной сети
 # (позволяет делать запрося ARP, но только
 # в случае, если выдаваемый клиенту адрес
 # принадлежит этой сети)
 set dns 213.85.16.7          # адрес DNS
 set ifaddr 192.168.20.240     # внутренний адрес
 set timeout 300              # таймаут простоя до разрыва соединения
 # если 0 - то не рвётся вообще
 enable MSChapV2              # протокол по которому шифруемся
 set nbns 192.168.20.254       # WINS
```

/etc/ppp/options.pptpdproxyarp

```
+MSChap-V2 mppe-128 mppe-stateless
```

/etc/ppp/ppp.secret# файлик с именами пользователей, паролями и IP адресами выдваемыми пользователям

```
# User_Name User_Password User_IP_address
lissyara          123     192.168.20.230
liss2             123     192.168.20.235
```

Собственно всё - добавляем строку в /etc/rc.conf и запускаем PoPToP:/etc/ppp/>echo 'pptpd_enable="YES"' >> /etc/rc.conf

```
/etc/ppp/>/usr/local/etc/rc.d/pptpd.sh start
Starting pptpd.
/etc/ppp/>ps -axl | grep pptpd
 0  4448   1  25 2  0   936  524 select Ss  ??  0:00.02 /usr/local/sbin/pptpd
/etc/ppp/>sockstat | grep pptpd
root     pptpd     4448    6 tcp4   *:1723                *:*
root     pptpd     4448    5 dgram  syslogd[120]:3
/etc/ppp/>
```

После чего надо разрешить порт 1723 в файрволле, траффик по интерфейсу tun0 и протокол GRE:allow tcp from any to me 1723

```
allow gre from any to any
allow ip from any to any via tun0
```

Правила добавляем гдень-ть вверху файрволла. (НО! Если через машину ходит траффик изнутри сети - т.е. это шлюз, добавлять надо после NAT - иначе ничё не заработает, т.к. пакеты выпадут до трансляции адресов :))
Пробуем что получилось, для контроля смотрим логи, для чего расскомметируем строку в файле /etc/syslog.conf*.* /var/log/all.log

После чего создаём этот файл и перезапускаем syslogd:/root/>touch /var/log/all.log
/root/>killall -1 syslogd
/root/>tail -f /var/log/all.log
Dec 4 13:53:45 lissyara syslogd: restart

Там и смотрим происходящее во время подключения. Не забудте после настройки закомментировать строку в syslog.conf и перезапустить syslogd.
Настройка форточек проста до безобразия: Создаём новое соединение мастером, выбираем подключаться к сети на рабочем месте, вводим логин, пароль, IP или имя сервака и всё...