MPD - настройка собственного VPN-сервера

Опубликовано muff в Втр, 2010-05-25 01:40

В связи с просьбой одного из сотрудников в реализации доступа к серверам офисной сети из дома (согласно требованиям безопасности, доступ к ним из сети Internet ограничен), возникла необходимость в настройке VPN-сервера. Реализовывать будем на базе MPD - основанная на netgraph реализация ppp-протокола мультисвязи для FreeBSD. Еще одним плюсом в сторону MPD есть то, что он совместим с Microsoft, тоесть подключиться к нашему серверу пользователи ОС Windows смогут пользуясь стандартными средствами ОС.

В более ранних версиях, для работы MPD необходима была поддержка ядром NETGRAPH, однако, начиная с FreeBSD6.0, это необязательно. Поскольку офисный маршрутизатор работает под FreeBSD 8.0, пересобирать ядро с поддержкой NETGRAPH не будем:

```
# uname -a
FreeBSD office.company.net 8.0-STABLE FreeBSD 8.0-STABLE #1: Thu Jan 14 17:33:25 EET 2010
muff [at] office [dot] company [dot] net:/usr/obj/usr/src/sys/Office i386
```

Исходные данные:

- Адресация локальной сети - **192.168.192.0/24**
- IP-адресс VPN-сервера, "смотрящий" в локальную сеть - **192.168.192.55**
- IP-адресс VPN-сервера, "смотрящий" в Internet - **193.227.206.45**
- IP-адреса клиентам выдавать из этой же подсети - **192.168.192.0/24**
- Разрешить доступ в Internet

Приступаем к установке:

```
# cd /usr/ports/net/mpd5/ && make install clean && rehash
```

Итак, после установки переходим в каталог /usr/local/etc/mpd5/, поскольку все конфигурационные файлы MPD находятся в этом каталоге:

```
# cd /usr/local/etc/mpd5 && ls -la


total 58drwxr-xr-x 2 root wheel 512 25 ??? 02:01 .drwxr-xr-x 7 root wheel 512 25 ???
 02:01 ..-r--r--r-- 1 root wheel 11856 25 ??? 02:01 mpd.conf.sample-r--r--r-- 1 root
 wheel 39541 25 ??? 02:01 mpd.script.sample-r--r--r-- 1 root wheel 834 25 ??? 02:01
mpd.secret.sample
```

А теперь приступаем непосредственно к настройке. Я буду настраивать сервер на поддержку 3 одновременных подключений (количество пользователей). Думаю, что настройка на большее количество подключениий проблем не вызовет - просто добавляем еще одну строку с логином и паролем пользователя в mpd.secret. Первый конфигурационный файл - mpd.conf. С примерами разнообразных настроек можно ознакомиться в mpd.conf.sample. Забыл в начале описать, что настраивать будем по протоколу PPTP. В результате нехитрых манипуляций получаем следующий mpd.conf:

```
# cat mpd.conf

startup:
        # Определяем пользователей
        set user username username_pass admin
```

```
        set user username1 userpass1
        # Конфигурация консоли
        set console self 127.0.0.1 5005
        set console open
        # Конфигурация веб-сервера
        set web self 0.0.0.0 5006
        set web open

default:
        load pptp_server

pptp_server:
# Определяем, какой адресный пул использовать
        set ippool add pool1 192.168.192.150 192.168.192.175
# Создаем клонируемый шаблон B
        create bundle template B
# Разрешаем на интерфейсе проксирование MAC-адресов
        set iface enable proxy-arp
# Задаем время простоя
        set iface idle 1800
# Исправлять ошибки с определением MSS
        set iface enable tcpmssfix
# Включаем сжатие данных
        set ipcp yes vjcomp
# Конкретизируем адресный пул для динамического присвоения параметров
        set ipcp ranges 192.168.192.55/32 ippool pool1
# Указываем, какие адреса DNS-серверов присваивать клиентам
        set ipcp dns 8.8.8.8 8.8.4.4
# Эти строки необходимы для поддрежки Microsoft Point-to-Point шифрования
        set bundle enable compression
        set ccp yes mppc
        set mppc yes e40
        set mppc yes e128
        set mppc yes stateless
# Создаем клонируемый шаблон L
        create link template L pptp
# Указываем, какой шаблон использовать
        set link action bundle B
# Запрещаем режим мультилинк
        set link disable multilink
        set link yes acfcomp protocomp
# Требуем chap авторизацию
        set link no pap chap eap
        set link enable chap
# Уменьшение размера mtu для избежания фрагментации
        set link mtu 1400
# Задаем адрес для входящих сообщений
        set pptp self 193.227.206.45
# Разрешаем входящие подключения
        set link enable incoming
```

Дальше необходимо создать файл mpd.secret, где будем хранить логины и пароли (при необходимости указываем и IP-адрес, который нужно присвоить клиенту, иначе берется из пула заданных адресов) VPN-пользователей. Пример mpd.secret:

```
# cat mpd.secret
muff muffpasswd 192.168.192.150
user1 user1pass 192.168.192.151
user2 user2pass 192.168.192.152
```

Добавляем загрузку MPD при старте системы:

```
# echo '# VPN PPTP Server' >> /etc/rc.conf
# echo 'mpd_enable="YES"' >> /etc/rc.conf
```

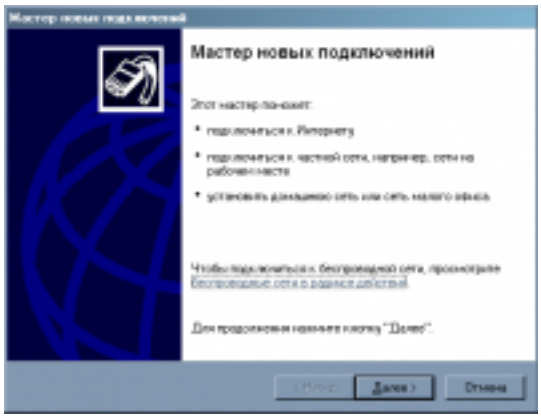
Даем команду запуска:

```
# sh /usr/local/etc/rc.d/mpd5 start
Starting mpd5.
```

Как оговаривалось раньше, поддержка NETGRAPH на уровне ядра не обязательна, NETGRAPH подгружается в виде модулей:

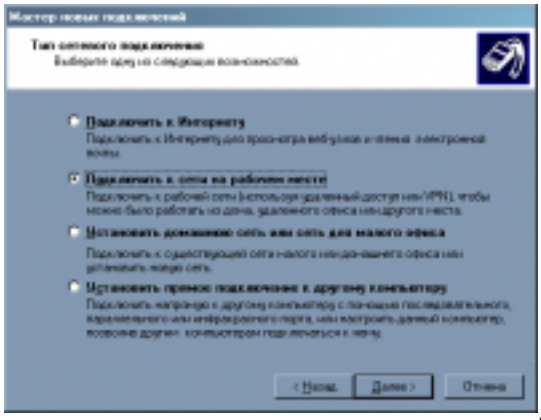
```
# kldstat


Id Refs Address Size Name1 26 0xc0400000 4992e8 kernel2 1 0xc1b5a000 35000 ipl.ko3 1
 0xc1c65000 2000 warp_saver.ko4 1 0xc2b57000 4000 ng_socket.ko5 8 0xc2c3a000 b000 ne
tgraph.ko6 1 0xc2bd2000 4000 ng_mppc.ko7 1 0xc2bdd000 2000 rc4.ko8 1 0xc2be3000 3000
 ng_tee.ko9 1 0xc2be9000 4000 ng_pptpgre.ko10 1 0xc2c45000 5000 ng_ksocket.ko11 1 0x
c2bf9000 3000 ng_iface.ko12 1 0xc2c4a000 7000 ng_ppp.ko13 1 0xc2c35000 3000 ng_tcpms
s.ko
```

Теперь попробуем настроить VPN-клиента под Windows XP. В "Панели управления" переходим в "Сетевые подключения" и жмем "Создание нового подключения". В результате запускается мастер новых подключений:



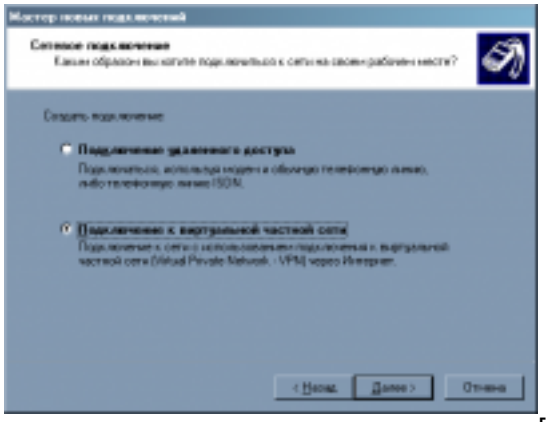
[1]

После нажатия "Далее" выбираем тип сетевого подключения "Подключить к сети на рабочем месте":



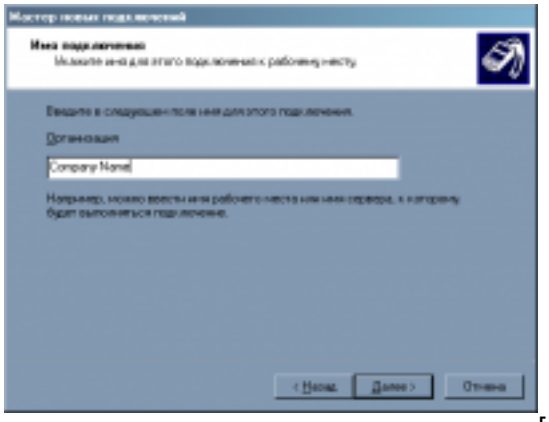
[2]

Потом уточняем, что это будет подключение к виртуальной частной сети:



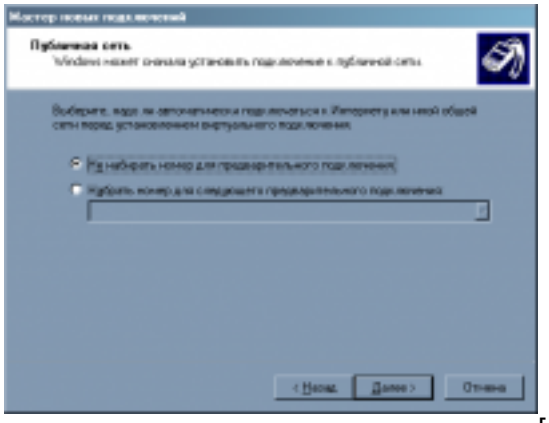
[3]

Далее задаем название подключения, чтобы идентифицировать его среди других подключений:



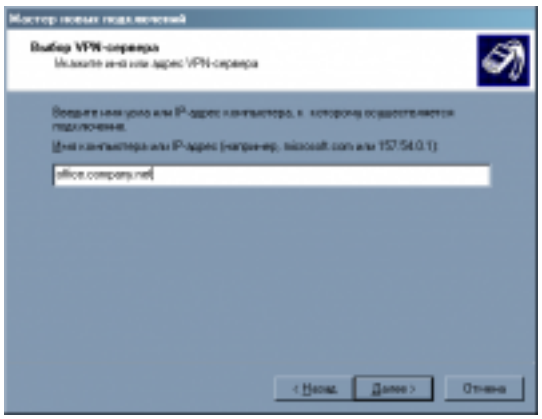
[4]

При необходимости указываем, набирать предварительное подключение, или нет:



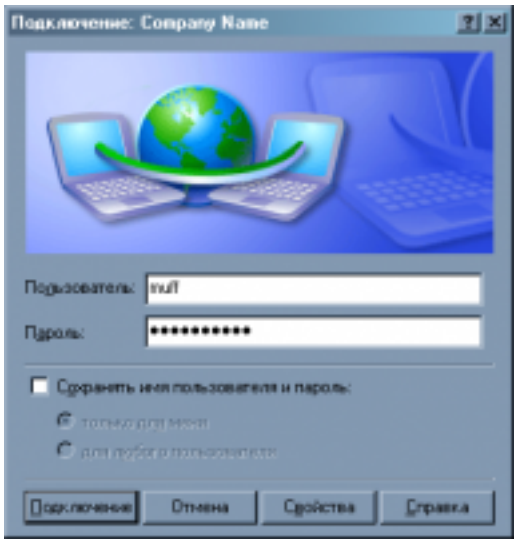
[5]

Следующим шагом указываем адрес сервера, к которому будем подключаться:



[6]

Потом остается только нажать кнопку "Готово". Ну а дальше заполняем поля логина и пароля и жмем "Подключиться":



[7]

В результате подключения на сервере автоматически создается интерфейс ng0:

```
ng0: flags=88d1<UP,POINTOPOINT,RUNNING,NOARP,SIMPLEX,MULTICAST> metric 0 mtu 1396ine
t 192.168.192.55 --> 192.168.192.150 netmask 0xffffffff
```

И на стороне клиента тоже:

```
Company Name - PPP ???????:

DNS-??????? ????? ??????????  . . : ???????? . . . . . . . . . . . . . : WAN (PPP/SLIP
) Interface ?????????? ?????. . . . . . . . . : 00-53-45-00-00-00 Dhcp ???????. . .
. . . . . . . . : ??? IP-????? . . . . . . . . . . . . . : 192.168.192.150 ????? ?????
?? . . . . . . . . . . . : 255.255.255.255 ???????? ???? . . . . . . . . . . . : 192.168
.192.150 DNS-??????? . . . . . . . . . . . : 8.8.8.8 8.8.4.4
```

После подключения стали доступна локальная сеть офиса. На этом статью можно заканчивать. Опишу еще несколько полезных моментов.

Настройка логирования и ротации логов

```
# echo '\!mpd' >> /etc/syslog.conf
# echo '*.* /var/log/mpd.log' >> /etc/syslog.conf
# touch /var/log/mpd.log
# sh /etc/rc.d/syslogd restart
# echo '/var/log/mpd.log 640 7 * $W6D0 JC' >> /etc/newsyslog.conf
```

Подключение к командной строке

 # telnet 127.0.0.1 5005

```
Trying 127.0.0.1...Connected to localhost.Escape character is '^]'.Multi-link PPP da
emon for FreeBSD

Username: muffPassword:

Welcome!Mpd pid 58159, version 5.5 (root [at] office [dot] company [dot] net
 01:59 25-May-2010)[] helpAvailable commands:authname : Choose link by auth name   bundle : Ch
oose/list bundlesclose : Close a layer                create : Create new itemdestroy : Destroy item
      exit : Exit consoleiface : Choose bundle by iface       help : Help on any commandlink : Choose li
nk                load : Read from config filelog : Set/view log options          msession : Ch. bundle by
msession-idopen : Open a layer                quit : Quit programrepeater : Choose/list repeaters      se
ssion : Choose link by session-idset : Set parameters                show : Show status[] show sessions
ng0 192.168.192.150 B-1 4755068-B-1 L-1 1 4755068-L-1 muff 195.3.159.250
```

Подключение к web-интерфейсу

[8]

Источник (получено *2025-03-28 22:30*):
http://muff.kiev.ua/content/mpd-nastroika-sobstvennogo-vpn-servera

Ссылки:
[1] http://muff.kiev.ua/files/imagepicker/1/mpd0.png
[2] http://muff.kiev.ua/files/imagepicker/1/mpd1.png
[3] http://muff.kiev.ua/files/imagepicker/1/mpd2.png
[4] http://muff.kiev.ua/files/imagepicker/1/mpd3.png
[5] http://muff.kiev.ua/files/imagepicker/1/mpd4.png
[6] http://muff.kiev.ua/files/imagepicker/1/mpd5.png
[7] http://muff.kiev.ua/files/imagepicker/1/mpd6.png
[8] http://muff.kiev.ua/files/imagepicker/1/mpd7.png