OpenVPN - построение тунеля

Опубликовано muff в Втр, 2009-08-18 17:54

Для начала немного общей информации.

OpenVPN – надежное и гибкое решение для VPN, позволяющее большинству платформам семейства Unix/Linux, Windows 2000/XP, и Mac OSX безопасно устанавливать зашифрованные каналы связи между собой.
OpenVPN — свободная реализация технологии Виртуальной Частной Сети (VPN) с открытым исходным кодом для создания зашифрованных каналов типа точка-точка или сервер-клиенты между компьютерами. Она позволяет устанавливать соединения между компьютерами находящимися за NAT-firewall без необходимости изменения его настроек. OpenVPN была создана Джеймсом Йонан (James Yonan) и распространяется под лицензией GNU GPL.

Создание VPN-тунеля с помощью OpenVPN подразумевает под собой создание псевдоустройства tun. Проверьте, пожалуйста, присутствует ли у вас в конфигурационном файле ядра такая строка:

```
device          tun             # Packet tunnel.
```

Если данное устройсво исключено из ядра, необходимо пересобрать ядро с данной опцией, или же подгрузить модуль для данного устройства.

Тем, кто будет пересобирать ядро - сюда [1] (рекомендую именно этот вариант, если планируете долгосрочное использование тунеля). Мы же подгрузим модуль для устройства tun, поскольку на данный момент только тестируем тунель.

```
# kldstat
Id Refs Address Size Name
1 3 0xffffffff80100000 525b50 kernel
2 1 0xffffffff80822000 56e snake_saver.ko
# kldload /boot/kernel/if_tun.ko
# kldstat
 Id Refs Address Size Name
1 4 0xffffffff80100000 525b50 kernel
2 1 0xffffffff80822000 56e snake_saver.ko
3 1 0xffffffff80823000 26de if_tun.ko
```

Модуль подгрузился. Не помешало бы, чтобы этот модуль подгружался и на этапе загрузки системы:

```
# echo 'if_tun_load="YES"' >> /boot/loader.conf
```

Итак, продолжим.

На данный момент между **Router 1** и **Router 2** есть 1 хоп при трассировке (пока тестируем достаточно и этого, все равно количество промежуточных хопов ни на что не влияет).

Схема построения:

IP интерфейсов, что смотрят в Internet на маршрутизаторах:

Router 1: 195.3.159.250

Router2: 193.227.207.94

Трассировка с **Router 1** к **Router2**:

```
# traceroute -n 193.227.207.94
 traceroute to 193.227.207.94 (193.227.207.94), 64 hops max, 52 byte packets
 1  195.3.159.249  0.182 ms  0.210 ms  0.112 ms
 2  193.227.207.94  1.109 ms  1.078 ms  1.046 ms
```

Настраиваем **Router 1**. Поищем пакет openvpn в портах:

```
# cd /usr/ports/
# make search name='openvpn'
 Port: openvpn-2.0.6_9
Path: /usr/ports/security/openvpn
Info: Secure IP/Ethernet tunnel daemon
Maint: matthias [dot] andree [at] gmx [dot] de
B-deps: lzo2-2.03_2
R-deps: lzo2-2.03_2
WWW: http://openvpn.net/ [2]

Port: openvpn-admin-1.9.4_2
Path: /usr/ports/security/openvpn-admin
Info: GUI frontend to openvpn
Maint: ports [at] FreeBSD [dot] org
B-deps: atk-1.26.0 bitstream-vera-1.10_4 cairo-1.8.8,1 compositeproto-0.4 damageproto-1.1.0_2
encodings-1.0.2,1 expat-2.0.1 fixesproto-4.0 font-bh-ttf-1.0.0 font-misc-ethiopic-1.0.0
font-misc-meltho-1.0.0_1 font-util-1.0.1 fontconfig-2.6.0,1 freetype2-2.3.9_1 gamin-0.1.10_3
gettext-0.17_1 gio-fam-backend-2.20.4 glib-2.20.4 gmake-3.81_3 gtk-2.16.5_1 gtk-sharp-2.12.9_1
hicolor-icon-theme-0.10_2 inputproto-1.5.0 intltool-0.40.6 jasper-1.900.1_8 jpeg-7 kbproto-1.0.3
libX11-1.2.1_1,1 libXau-1.0.4 libXcomposite-0.4.0,1 libXcursor-1.1.9_1 libXdamage-1.1.1
libXdmcp-1.0.2_1 libXext-1.0.5,1 libXfixes-4.0.3_1 libXft-2.1.13 libXi-1.2.1,1 libXinerama-1.0.3,1
libXrandr-1.3.0 libXrender-0.9.4_1 libfontenc-1.0.4 libglade2-2.6.4_1 libiconv-1.13.1
libpthread-stubs-0.1 libxcb-1.4 libxml2-2.7.3 mkfontdir-1.0.4 mkfontscale-1.0.6 mono-2.4.2.3_1
p5-XML-LibXML-1.69,1 p5-XML-LibXML-Common-0.13 p5-XML-NamespaceSupport-1.10
p5-XML-Parser-2.36_1 p5-XML-SAX-0.96 pango-1.24.5 pcre-7.9 perl-threaded-5.8.9_3 pixman-0.15.4
pkg-config-0.23_1 png-1.2.38 python26-2.6.2_2 randrproto-1.3.0 renderproto-0.9.3
shared-mime-info-0.60_1 tiff-3.8.2_4 xcb-proto-1.5 xcb-util-0.3.5 xextproto-7.0.5
xineramaproto-1.1.2 xmlcatmgr-2.2 xorg-fonts-truetype-7.4 xproto-7.0.15
R-deps: atk-1.26.0 bitstream-vera-1.10_4 cairo-1.8.8,1 compositeproto-0.4 damageproto-1.1.0_2
encodings-1.0.2,1 expat-2.0.1 fixesproto-4.0 font-bh-ttf-1.0.0 font-misc-ethiopic-1.0.0
font-misc-meltho-1.0.0_1 font-util-1.0.1 fontconfig-2.6.0,1 freetype2-2.3.9_1 gamin-0.1.10_3
gettext-0.17_1 gio-fam-backend-2.20.4 glib-2.20.4 gtk-2.16.5_1 gtk-sharp-2.12.9_1
hicolor-icon-theme-0.10_2 inputproto-1.5.0 jasper-1.900.1_8 jpeg-7 kbproto-1.0.3 libX11-1.2.1_1,1
libXau-1.0.4 libXcomposite-0.4.0,1 libXcursor-1.1.9_1 libXdamage-1.1.1 libXdmcp-1.0.2_1
libXext-1.0.5,1 libXfixes-4.0.3_1 libXft-2.1.13 libXi-1.2.1,1 libXinerama-1.0.3,1 libXrandr-1.3.0
libXrender-0.9.4_1 libfontenc-1.0.4 libglade2-2.6.4_1 libiconv-1.13.1 libpthread-stubs-0.1 libxcb-1.4
```

libxml2-2.7.3 lzo2-2.03_2 mkfontdir-1.0.4 mkfontscale-1.0.6 mono-2.4.2.3_1 openvpn-2.0.6_9 p5-XML-LibXML-1.69,1 p5-XML-LibXML-Common-0.13 p5-XML-NamespaceSupport-1.10 p5-XML-SAX-0.96 pango-1.24.5 pcre-7.9 perl-threaded-5.8.9_3 pixman-0.15.4 pkg-config-0.23_1 png-1.2.38 python26-2.6.2_2 randrproto-1.3.0 renderproto-0.9.3 shared-mime-info-0.60_1 tiff-3.8.2_4 xcb-proto-1.5 xcb-util-0.3.5 xextproto-7.0.5 xineramaproto-1.1.2 xmlcatmgr-2.2 xorg-fonts-truetype-7.4 xproto-7.0.15
WWW: http://sourceforge.net/projects/openvpn-admin [3]

Port: openvpn-auth-ldap-2.0.3_1
Path: /usr/ports/security/openvpn-auth-ldap
Info: LDAP authentication plugin for OpenVPN
Maint: snb [at] FreeBSD [dot] org
B-deps: lzo2-2.03_2 openldap-client-2.4.17 openvpn-2.0.6_9 re2c-0.13.5
R-deps: openldap-client-2.4.17
WWW: http://dpw.threerings.net/projects/openvpn-auth-ldap/ [4]

Port: openvpn-devel-2.1.r19
Path: /usr/ports/security/openvpn-devel
Info: Secure IP/Ethernet tunnel daemon
Maint: matthias [dot] andree [at] gmx [dot] de
B-deps: lzo2-2.03_2
R-deps: lzo2-2.03_2
WWW: http://openvpn.net/ [2]

Найдено 4 порта. Нам нужен

Port: openvpn-2.0.6_9
Path: /usr/ports/security/openvpn
Info: Secure IP/Ethernet tunnel daemon
Maint: matthias [dot] andree [at] gmx [dot] de
B-deps: lzo2-2.03_2
R-deps: lzo2-2.03_2
WWW: http://openvpn.net/ [2]

Приступаем к установке:

```
# cd /usr/ports/security/openvpn
 # make install clean
```

Опции установки оставляем по умолчанию:

```
Options for openvpn 2.0.6_9


[ ] PW_SAVE Interactive passwords may be read from a file
```

После установки не забываем обновить пути. Создаем каталог, где будут лежать конфигурационные файлы.

```
# rehash
# mkdir /usr/local/etc/openvpn
 # cd /usr/local/etc/openvpn
```

Создаем файл с ключем шифрования тунеля.

```
# openvpn --genkey --secret /usr/local/etc/openvpn/tun0.key
```

Посмотрим результат команды:

```
# cat /usr/local/etc/openvpn/tun0.key
```

```
## 2048 bit OpenVPN static key#-----BEGIN OpenVPN Static key V1-----f85bf8204f9e4744
6e497d166f2f1aa21980cd79f2fe7ce2d5054003a87dae0872b331532fe4da258e2e1fbf1fedbf849b91
85d573ee908955975a6f8eef6f4ef43195b7eafcf73b1a45392991be61ca756926c59899b689f127b998
eb9369bd52eab3791708d0215dd6a59f226d8c91aa523b288c715284ddcaa4f4df2f7a9375794c875fd2
8c2f14d351d92a1c62195926866b44b72941eaec67e20495d54992f38c01fa22521f681ab50d71e3379e
64fd253f10b929a6f27dc884e158b3b37b2eb1e7ce0d4047618b59cae6b5ea785fbf9c9fafdb70168c36
b8f21b3e898ea28dae707fe1995a1f6f5d153ea361fc31794c1fc8ef89000790e28d36444767-----END
 OpenVPN Static key V1-----
```

Вот этим ключем и будем шифровать наш канал :)

Создадим конфигурационный файл /usr/local/etc/openvpn/openvpn.conf . Листинг конфигурационного файла:

```
# Создаем устройство типа tun
dev tun0

# IP-адресс удаленного пира
remote 193.227.207.94

# 91.196.102.190 - это IP-адресс локальной конечной точки VPN
# 91.196.102.189 - это IP-адресс удаленной конечной точки VPN
ifconfig 91.196.102.190 91.196.102.189

# Указываем ключ шифрования для тунеля
secret /usr/local/etc/openvpn/tun0.key
```

Добавляем опции загрузки в /etc/rc.conf:

```
# echo '#OpenVPN' >> /etc/rc.conf
 # echo 'openvpn_enable="YES"' >> /etc/rc.conf
 # echo 'openvpn_configfile="/usr/local/etc/openvpn/openvpn.conf"' >>  /etc/rc.conf
 # echo 'openvpn_dir="/usr/local/etc/openvpn"'  >> /etc/rc.conf
```

Запускаем тунель:

```
# sh /usr/local/etc/rc.d/openvpn start
```

Проверяем, создался ли туннель:

```
# ifconfig tun0
tun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> metric 0 mtu 1500
inet 91.196.102.190 --> 91.196.102.189 netmask 0xffffffff
Opened by PID 673
```

Все гуд. Приступаем к конфигурированию **Router2**.

По аналогии установим из портов openvpn. Потом создадим каталог для конфигурационных файлов и создадим такой же ключ шифрования, как и на **Router1** (должен совпадать на обеих маршрутизаторах):

```
# mkdir /usr/local/etc/openvpn
 # touch /usr/local/etc/openvpn/tun0.key
 # chmod 600 /usr/local/etc/openvpn/tun0.key
```

Заливаем туда содержимое /usr/local/etc/openvpn/tun0.key с **Router1**.

Создаем конфигурационный файл. Листинг /usr/local/etc/openvpn/openvpn.conf:

```
# cat /usr/local/etc/openvpn/openvpn.conf

# Создаем устройство типа tun
dev tun

# IP-адресс удаленного пира
remote 195.3.159.250

# 91.196.102.189 - это IP-адресс локальной конечной точки VPN
# 91.196.102.190 - это IP-адресс удаленной конечной точки VPN
ifconfig 91.196.102.189 91.196.102.190

# Указываем ключ шифрования для тунеля
secret /usr/local/etc/openvpn/tun0.key
```

Добавляем опции загрузки в /etc/rc.conf:

```
# echo '#OpenVPN' >> /etc/rc.conf
 # echo 'openvpn_enable="YES"' >> /etc/rc.conf
 # echo 'openvpn_configfile="/usr/local/etc/openvpn/openvpn.conf"' >>  /etc/rc.conf
 # echo 'openvpn_dir="/usr/local/etc/openvpn"'  >> /etc/rc.conf
```

Запускаем тунель:

```
# sh /usr/local/etc/rc.d/openvpn start
```

Проверяем, создался ли туннель:

```
# ifconfig tun0
tun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> metric 0 mtu 1500
inet 91.196.102.189 --> 91.196.102.190 netmask 0xffffffff
Opened by PID 37668
```

Все ок... Проверяем с **Router2** доступность "другой" стороны тунеля:

```
# ping 91.196.102.190
PING 91.196.102.190 (91.196.102.190): 56 data bytes
64 bytes from 91.196.102.190: icmp_seq=0 ttl=64 time=1.512 ms
64 bytes from 91.196.102.190: icmp_seq=1 ttl=64 time=1.390 ms
64 bytes from 91.196.102.190: icmp_seq=2 ttl=64 time=1.226 ms
^C
--- 91.196.102.190 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.226/1.376/1.512/0.117 ms
```

Все ok. На этом построение тунеля завершено.

Дальше дело за маршрутизацией... Уже вам решать что в этот тунель заворачивать.

Источник (получено *2024-09-19 02:17*):
http://muff.kiev.ua/content/openvpn-postroenie-tunelya

Ссылки:
[1] http://muff.kiev.ua/node/16
[2] http://openvpn.net/
[3] http://sourceforge.net/projects/openvpn-admin
[4] http://dpw.threerings.net/projects/openvpn-auth-ldap/