Автор:
08.09.11 11:17 - Последнее обновление 08.09.11 11:26

Настройка OpenVPN на маршрутизаторе dd-wrt и Windows клиентах

Для создания безопасного тоннеля к своей домашней сети остановил выбор на OpenVPN . Во-первых, данный сервис поддерживается dd-wrt и можно скачать уже готовую прошивку для маршрутизатора (не все модели). Во-вторых, данный сервер поддерживает VPN через http (https) прокси.

Как установить прошивку уже писалось , теперь настроим безопасное соединение с нашей сетью и возможность использовать безгранично интернет из любого места мира через своего провайдера.

Небольшое отступление. Вопрос это мне в голову не приходил до определенного времени, а именно рабочий интернет начали ограничивать мне, из-за постоянного забивания мною канала скачиванием полновесных документов, каталогов, необходимого ПО и прочее. Меня просто поставили в очередь пользователей, жаль что не в первых рядах;) Скорость в связи с этим упала до обидных 0,5 Мбит. Что меня очень не устраивало, особенно когда тебе надо скачать новый каталог от производителей размером 200 МБ и ждать скачки этого каталога необходимо час, а то и два.

Хоть провайдеры предоставляющие интернет у меня дома и на работе разные, но дружат, таким образом основные пулы у них объединены отдельным оптическим каналом который никак не ограничен. Разумеется и у нас в очередях в серверной это никак не прописано и я могу подключаться к своему маршрутизатору даже не подключая интернет. Так же свою роль сыграл мой киевский друг (привет тебе, Вадим), у которого в офисе стоял жесткий (резали почти всё) прокси с авторизацией с неограниченным украинским трафиком и очень ограниченным мировым.

Теперь собственно перейдем к настройке всего этого дела.

1. Установка OpenVPN. Качаем сборку с официального сайта , самая свежая на момент написания 2.1.4 и устанавливаем всё по умолчанию.

2. Сборка ключей и сертификатов для сервера/клиентов. Запускаем консоль Windows - "Пуск - Строка поиска - cmd".

Выполняем команду, которая создаст папку для наших ключей и сертификатов, а также скопирует в неё файлы serial.start и index.txt.start без суффикса .start:

```
cd "c:Program FilesOpenVPNeasy-rsa" && mkdir keys && copy serial.start keysserial && copy index.txt.start keysindex.txt
```

Теперь надо скопировать vars.bat.sample и openssl.cnf.sample в vars.bat и openssl.cnf следующей командой:

cd "c:Program FilesOpenVPNeasy-rsa" && init-config.bat

Теперь необходимо создать Diffie-Hellman key:

C:Program FilesOpenVPNeasy-rsa>build-dh.bat

В результате в каталоге C:Program FilesOpenVPNeasy-rsakeys появится файл dh1024.pem.
Создаем Certificate Authority, с помощью команды в консоли "build-ca.bat":
C:Program FilesOpenVPNeasy-rsa>build-ca.bat Так в каталоге keys было создано два файла ca.crt и ca.key. При нижеследующих запросах я отвечал "по-совести":

Country Name (2 letter code) [US]:
State or Province Name (full name) [CA]:
Locality Name (eg, city) [SanFrancisco]:
Organization Name (eg, company) [OpenVPN]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:
Email Address [mail@host.domain]:
Далее генерируем ключи для сервера пакетным файлом "build-key-server.bat" как имя сервера указываем ddwrt:
C:Program FilesOpenVPNeasy-rsa>build-key-server.bat ddwrt На эти вопросы так же отвечал:

A challenge password []:
An optional company name []:
Затем для клиентов, я создавал для 3-х (себя, друга и на всякий случай, соответственно user1, user2, user3):
C:Program FilesOpenVPNeasy-rsa>build-key.bat user1 В итоге у нас в папке C:Program FilesOpenVPNeasy-rsakeys множество нам нужных ключей и сертификатов.

3. Настройка маршрутизатора. Заходим на веб-интерфейс нашего маршрутизатора во вкладку "Службы - PPTP". Включаем кнопку Start OpenVPN Daemon и раскрывается доступ к настройкам нашего сервера.
"Публичный серт.сервера" - извлекаем из "C:Program FilesOpenVPNeasy-rsakeysca.crt" с помощью блокнота, причем ключ должен быть помещен полностью начиная с "-----BEGIN

CERTIFICATE-----" и заканчивая "-----END CERTIFICATE-----".
"Публичный серт.клиента" - из файла "C:Program FilesOpenVPNeasy-rsakeysddwrt.crt".
"Личный ключ пользователя" - файл "C:Program FilesOpenVPNeasy-rsakeysddwrt.key".
"DH PEM" - "C:Program FilesOpenVPNeasy-rsakeysdh1024.pem".
Пример моего конфигурационного файла:

```
mode server
tls-server
daemon
server 192.168.66.0 255.255.255.0
port 443
proto tcp-server
dev tun0
ca /tmp/openvpn/ca.crt
cert /tmp/openvpn/cert.pem
key /tmp/openvpn/key.pem
dh /tmp/openvpn/dh.pem
push "redirect-gateway def1"
push "dhcp-option DNS 192.168.66.1"
push "dhcp-option WINS 192.168.66.1"
keepalive 10 120
client-to-client
persist-key
persist-tun
verb 3
```

Нажимаем сохранить и применить.
Так же надо подправить наш брандмауэр, чтобы он пропускал подключения к нашему серверу. Делается это во вкладке "Техобслуживание - Команды" и вводим команду:

```
iptables -I INPUT 1 -p tcp --dport 443 -j ACCEPT
iptables -I FORWARD 1 --source 192.168.66.0/24 -j ACCEPT
```

Нажимаем кнопку снизу "Сохр.брандмауэр".

4. Теперь необходимо настроить клиентов. Для пользователей которые будут пользоваться моим сервером, необходимо установка OpenVPN, и сохранение в папке "C:Program FilesOpenVPNeasy-rsa" папочки "keys" со следующими файлами - ca.crt, user1.crt, user1.key (разумеется каждому отдельному клиенту необходимы уникальные user1.crt, user1.key из тех что мы создавали с различными названиями).
Редактируем с помощью блокнота "C:Program FilesOpenVPNsample-configclient.ovpn". Мой конфиг:

```
client
dev tun
proto tcp-client
remote myIP 443
resolv-retry infinite
nobind
persist-key
persist-tun
```

ca "C:\Program Files\OpenVPN\easy-rsa\keys\ca.crt"
cert "C:\Program Files\OpenVPN\easy-rsa\keys\user1.crt"
key "C:\Program Files\OpenVPN\easy-rsa\keys\user1.key"
verb 3
Вместо "myIP" прописан мой реальный IP-адрес (можно использовать имя службы DDNS, для динамических адресов на вкладке "Установка - DDNS"), так же для каждого клиента будут пути к ключам и сертификатам с их именами. Сохраняем файл в папку "C:Program FilesOpenVPNconfig". Запускаем OpenVPN GUI, он появляется значком в панели задач, щелкаем правой кнопкой мыши на нём и кликаем "Connect". После вывода логов значок светится зеленым светом - мы подключились.

Конфигурация для прокси с авторизацией:
client
dev tun
proto tcp-client
http-proxy proxy 3128 user.pas basic
remote myIP 443
resolv-retry infinite
nobind
persist-key
persist-tun
ca "C:\Program Files\OpenVPN\easy-rsa\keys\ca.crt"
cert "C:\Program Files\OpenVPN\easy-rsa\keys\user1.crt"
key "C:\Program Files\OpenVPN\easy-rsa\keys\user1.key"
verb 3 Где proxy это IP-адрес прокси-сервера, а user.pas это файл состоящий из двух строк - первая логин, вторая пароль, находящийся здесь "C:Program FilesOpenVPNconfig", это при стандартной авторизацией пользователей, при необходимости авторизации через http, строка будет выглядеть следующем образом:
http-proxy proxy 3128 user.pas ntlm

Теперь есть доступ в домашнюю сеть из любой точки мира, главное чтобы был доступ к ключам и конфигурациям, в моем случае я использовал архив с паролем загруженный на Документы Google. Загрузка маршрутизатора при одном подключении составляет порядка 30% процессорной мощности, следовательно не рекомендую подключать более двух пользователей одновременно.

оригинал: http://kharlashkin.blogspot.com/2011/04/openvpn-dd-wrt-windows.html ссылка на статью:
http://thin.kiev.ua/index.php?option=com_content&view=article&id=410:453345345&catid=71:dir-320-&Itemid=87

{jcomments on}