Безопасный OpenVPN на VPS за несколько минут

@PhoenixGruppe • August 16, 2017

https://habrahabr.ru/post/335516/

Введение

В связи с последними событиями и возможной блокировкой публичных VPN сервисов созрела идея облегчить жизнь людям и сделать скрипт для быстрой установки OpenVPN со всеми настройками и легким выпуском сертификатов.

Скрипт позволяет одной командой создать работающий сервер и создать файлы конфигурации для клиентов в unified формате (то есть с сертификатами, включёнными в файл конфигурации). Кстати, эти файлы подходят для мобильных устройств.

Скрипт создавался для машин с CentOS 7.x или Ubuntu Server 17.x, использование на Ubuntu 16.x. возможно, но там OpenVPN 2.3.x в репозиториях. При необходимости можно добавить другие дистрибутивы, но обычно при покупке VPS можно выбрать систему и это не так важно.

Скрипт написан на bash за пару часов, возможны ошибки и наверняка что-то можно было реализовать проще и лучше.

Запускайте скрипт на свежей машине, он перезаписывает правила iptables и конфигурацию OpenVPN. И да, в правилах iptables разрешен порт ssh 22, если вы поменяли его на другой, не забудьте поменять порт в скрипте.

Особенности

1. По умолчанию рекомендуется cipher AES-256-GCM (что достаточно безопасно на данный момент);
2. По умолчанию используется auth SHA256 (вместо дефолтного SHA1);
3. По умолчанию для OpenVPN 2.4.x используется tls-crypt (что усложняет обнаружение трафика OpenVPN);
4. По умолчанию использует Google DNS и блокировку локальных DNS (setenv opt block-outside-dns) для предотвращения DNS Leak;
5. Создаются все нужные правила в iptables и ip6tables;
6. Есть поддержка IPv6.

Как пользоваться

Использовать скрипт очень просто, скачайте файл openvpnsetup.sh на ваш VPS, дайте ему права на запуск chmod +x openvpnsetup.sh и запустите ./openvpnsetup.sh. В результате вы получаете настроенный сервер, готовый к работе на выбранном вами порту.

В папке /etc/openvpn создается скрипт newclient.sh, который нужен для создания файлов конфигурации клиентской части, использовать его так же просто — ./newclient.sh clientname. Результатом будет файл /etc/openvpn/bundles/clientname.ovpn, который сразу можно использовать на клиенте, просто положите его в папку config (в случае использования на Windows) на вашей машине.

Если вы захотите пересоздать сервер, просто удалите все из папки /etc/openvpn и запустите скрипт заново (естественно, клиентские сертификаты надо будет перевыпустить).

Советы по выбору VPS для OpenVPN

1. В первую очередь смотрим на цену, можно найти предложения за $3-4 в месяц, что дешевле многих VPN сервисов;
2. Выбирайте VPS ближе к вам географически, если хотите иметь приемлемую скорость через VPN. Чем меньше пинг от вас до VPS, тем лучше скорость;
3. Выбирайте минимальную конфигурацию. OpenVPN не использует больше одного ядра и может работать на 256MB памяти. Минимального дискового пространства в 3-5GB так же вполне достаточно;
4. Некоторые VPS ограничены по трафику, но обычно это 1TB в месяц, если вы планируете использовать больше, рассмотрите другие тарифные планы;
5. Перед тем как оформить заказ на VPS, уточните разрешена ли загрузка торрентов (при условии, что они вам нужны, конечно);
6. Так же можно уточнить включены ли TUN/TAP устройства в системе. В скрипте есть проверка на это, но лучше уточнить до покупки, возможно их и нельзя будет включить через поддержку провайдера VPS;
7. Наличие IPv6 адреса, скрипт позволяет настроить сервер с поддержкой IPv6 и возможно вы захотите иметь возможность посещать IPv6 ресурсы через VPN.

Скрипт доступен на GitHub.

Бонус: результат проверки анонимности на 2ip.ru:

Проверка анонимности

Все сайты, куда бы вы не заходили, определяют ваши данные как:

ваш адрес: France
ваш IP адрес: 51.[redacted]
ваш провайдер: UK Government Department for Work and Pensions

Мы можем проверить точность этой информации, на самом ли деле она соответствует действительности, не используете ли вы прокси, анонимайзер, VPN сервер, Tor или другие средства анонимизации..

Метод проверки	Результат
Заголовки HTTP proxy	нет
Открытые порты HTTP proxy	нет
Открытые порты web proxy	нет
Открытые порты VPN	нет
Подозрительное название хоста	нет
Разница во временных зонах (браузера и IP)	IP: 2017-08-11 22:29 (Europe/Paris) браузер: 2017-08-11 22:29
Принадлежность IP к сети Tor	нет
Режим браузера Turbo	нет
Принадлежность IP хостинг провайдеру	нет
Определение web proxy (JS метод)	нет
Утечка IP через Flash	нет
Определение туннеля (двусторонний пинг)	высокая анонимизация (не можем проверить)
Утечка DNS	вы используете публичные DNS Google (74.125.47.136, 74.125.73.88)
VPN fingerprint	нет
Утечка IP через WebRTC	нет

Мы не обнаружили средств анонимизации, ничего подозрительного.

Вероятность использования средств анонимизации:

0 %

Проверка на [redacted]:

witch.valdikss.org.ru

```
First seen     = 2017/08/11 22:54:46
Last update    = 2017/08/11 23:34:02
Total flows    = 10
Detected OS    = Windows 7 or 8
HTTP software = ???
MTU            = 1500
Network link   = Ethernet or modem
Language       = Russian
Distance       = 11
PTR            = [redacted]

PTR test       = Probably server user
Fingerprint and OS match. No proxy detected (this test does not include headers detection).
No OpenVPN detected.

No NTLM hash is leaked. Try to manually copy&paste
file://witch.valdikss.org.ru/a to the address bar (Windows with IE/Edge/Chrome) or
\\witch.valdikss.org.ru\a (Windows with Firefox).
```

Проверка на DNS Leak:

DNS leak test.com — What is a DNS leak? — What are transparent DNS proxies? — How to fix a DNS leak

Test complete

```
Query round Progress... Servers found
  1         ......              6
```

Sponsored by IVPN — Ultimate IP leak Protection

IP	Hostname	ISP	Country
74.125.181.5	none	Google	Belgium
74.125.181.11	none	Google	Belgium
74.125.73.84	none	Google	Belgium
74.125.73.77	none	Google	Belgium
74.125.47.12	none	Google	Belgium
74.125.47.138	none	Google	Belgium

https://t.me/PhoenixTrading