Автор:
13.05.14 21:27 -

Автор: admin.

SecurityKISS - ещё один бесплатный *VPN* сервис, обеспечивающий виртуальную частную сеть, своего рода индивидуальный шлюз или туннель, называйте как хотите, между вашим компьютером и конечной точкой посещения. Это всё-равно, если вы едете на автомобиле по многополосной дороге, с большим количеством участников движения, но по собственной, индивидуальной полосе движения, на которую остальные участники, заезжать не имеют право, или же ещё, что более надёжно, по собственному туннелю, куда другие, даже если б и захотели, а попасть не могут.

Если скажем - *ZenMate* , работает только с *Chrome*-образными браузерами, то *Security KISS* - совместим с любым типом браузеров, т.к., первый - использует специальный плагин, а второй - полнофункциональное соедениение через *VPN* , настройку которого, мы рассмотрим ниже. На бесплатном аккаунте, имеются ограниченния на трафик - 300 МБдень, не густо конечно, но для простого серфинга, вполне может хватить. Вся частная сеть там, реализована на основе *OpenVPN, PPTP, L2TP* - типов соединений. Что это такое?

1) ***PPTP*** - встроен почти во все операционные системы, очень прост в настройке, очень быстрый, много ещё где используется, небезопасен в плане протокола аутентификации ***MS-CHAP v.2*** .

2) ***L2TP*** - вообще данный тип, сам по себе, не обеспечивает шифрования трафика, для этого необходим ***L2TPIPsec***, о котором на сайте нечего не сказано, если я правильно всё понимаю. При рассмотрении ***L2TP*** на уровне ***L2TPIPsec*** , можно отметить очень хорошую безопасность, лёгкую настраивоимость, доступность во многих операционных системах, но, при его использовании, может понадобится

дополнительная настройка роутера и скорость работы, несколько медленее, чем у ***PPTP***
и
OpenVPN
.

3) ***OpenVPN*** - на мой взгляд, из выше представленных, будет лучшим, особенно для домашних компьютеров. Гибкие настройки, очень безопасен, может работать сквозь файрволлы, обладает широкими возможностями шифрования. При этом - требуется установка дополнительного программного обеспечения, может оказаться не очень удобным в плане настройки и не полная поддержка портативными устройствами.

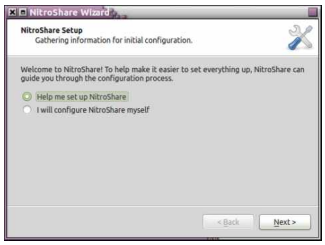
Далее, предлагаю использовать третий тип: ***OpenVPN***, как наболее удачный по множеству параметров. Заходим на сайт:
http://www.securitykiss.com/
. Данная инструкция годится для
Ubuntu
: с 11.10 по 14.04 версии, включительно.

Регистрация.

1) Кнопка **1** (на снимке) - там расположены флаги стран для выбора языка отображения, русский тоже есть - выбираем его.
2) Кнопка **2** (на снимке) - здесь показывается ваш текущий *IP*-адрес и страна.
3) Кнопка **3** (на снимке) - "зона клиента", кликаем сюда для регистрации.

Должно появиться вот такое окно, думаю, что здесь всё понятно без объяснений.

Здесь, наверное тоже объяснять особо нечего.



После этих действий, на ваш *E-Mail* придёт письмо с данными, там будет - ***Client ID: XXXXXX*** , ***Password: XXXXXX*** и другое.

Заходим в аккаунт и скачиваем файлы настроек.

На главной странице сайта, жмём на кнопочку - **"Зона клиента"** (первый снимок, кнопка **3**). В появившимся окне, заполняем данные, которые пришли вам на ***E-Mail*** . Это: ***Client ID*** и ***Password*** , затем жмём кнопочку: **"** ***Login*** **"** .

После этого, вы попадёте в такое же окошко, только это будет, как бы ваш внутренний аккаунт с данными. Там, в верхнем меню, переходите на вкладку: **"*Downloads*"**, потом ещё одна вкладка:
"
Linux
"
и в разделе:
"
Linux Network Manager Configuration
"
- нажимаете кнопочку:
"
Downloads
"
. Вам будет предложено два варианта:
"архив.
tar
"
или
"архив.
zip
"
. Выбираете любой и скачиваете его к себе на компьютер. Затем, распаковываете его и распакованую папку с файлами, помещаете в любое место в домашней директории.

Проверяем, разрешена ли отправка IP в Linux.

Открываем терминал и выполняем:

cat /proc/sys/net/ipv4/ip_forward

Если ответ будет **"1"** (еденица), то всё норамально, а если **"0"** (ноль), то нужно проделать следующее. Дело в том, что для разных версий
Ubuntu
, подразумевается своё действие, их всего два, а что бы сработало сразу и наверняка, просто выполните их оба (по-возможности), независимо от версии
Ubuntu
. Откройте терминал и выполните:

sudo su
echo 1 > /proc/sys/net/ipv4/ip_forward
gedit /etc/sysctl.conf

В открывшимся файле, найдите и раскоментируйте (убрать заначок решётки **#**) строчку: **net.ipv4.i**
p_forward = 1
. Сохраните изменения и перезагрузите систему. После перезагрузки, ещё раз проверьте разрешение:

cat /proc/sys/net/ipv4/ip_forward

На выходе должна быть **"1"** (еденица).

Вытаскиваем нужные нам данные.

Здесь всё очень просто, вы помните, что мы скачали архив с файлами, распаковали его и распакованную папку поместили в домашнюю директорию. Заходим в эту папку, там будут находится четыре файла, сейчас нам нужен файл: ***README.txt***. Открываем его и смотрим представленный список прокси, нам нужно выбрать любой понравившийся с параметром: **"*udp*"**
в графе:
"
Proto
"
. Вот маленький отрезок текста из файла:

Country	City	IP Address	Proto	Port
FR	Paris	37.59.65.55	udp	123
FR	Paris	37.59.65.55	tcp	443

В данном случае, из имеющегося мы выберем:

Франция, Париж, 37.59.65.55 udp 123

Записываем эти данные и идём дальше.

Автор:
13.05.14 21:27 -

Устанавливаем дополнительное "ПО".

Окрываем "центр приложений" и вводим в строку поиска: ***network-manager-openvpn***. Если этот плагин установлен, а вы это увидите, то всё "OK", если нет, то установите его.

Настраиваем VPN (OpenVPN-соединение).

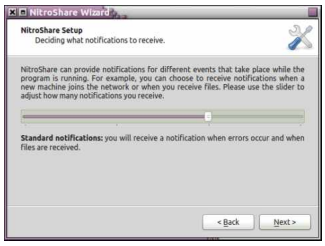
Кликаем по значку сетевого соединения в трее и выбираем: **Соединения *VPN* Натроить *VPN***.

Настройка VPN через значок в трее.

Добаляем новый тип соединения.

Выбираем тип соединения.

Из выпадающего меню выбираем тип соединения ***OpenVPN*** и жмём на кнопочку: **"Создать"** .

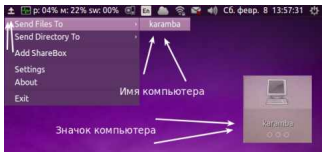


Настройки параметров.

1) Кнопка **1** - Название соединения, можете прописать любое.
2) Кнопка **2** - Просто выбираете эту вкладку.
3) Кнопка **3** - Шлюз, здесь вписываете *IP*-адрес, который мы с вами брали из файла: ***README.txt***
.
4) Кнопка **4** - Сертификаты (*TLS*) - выставлено по-умолчанию.
5) Кнопка **5** - Указываете путь до файла: ***client.crt***, в папке, которую мы скачали.
6) Кнопка **6** - Тоже, что и **п.5**, только файл: ***ca.crt***.
7) Кнопка **7** - Тоже, что и **п.5,6,** только файл: ***client.key***.
8) Кнопка **8** - Кликаете сюда для продолжения.

Дополнительные настройки.

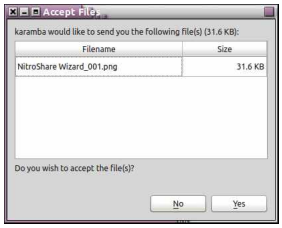
Здесь, поставьте две галочки, как показано на снимке и в позиции: "Использовать другой порт шлюза", впишите номер порта **123** - это номер из нашего файла ***README.txt***.



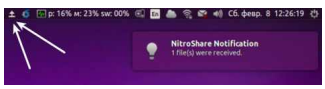
Теперь, нажмите: "OK", потом: "Сохранить", потом: "Закрыть".

Подключаемся к VPN.

Кликните по значку "Сетвых соединений" в трее и выбирите, только что созданное соединение:



Системное сообщение об удачном подключении к *VPN*.



Всё, вы подключены к собственному *VPN*-туннелю. Для пущей убедительности, можете зайти на сервис 2ip.ru и проверить свой *IP*-адрес и всё остальное. Теперь, вы можете одним кликом, устанавливать *VPN*-соединение и отключаться от него (октлючается также, через значок в трее).

Положительные характеристики *SecurityKISS*:

- Полноценное обеспечение безопасного соединения с Интернетом.

Отрицательные характеристики *SecutiryKISS*:

- Относительно небольшой дневной лимит трафика.

Параметры:

Язык интерфейса: английский русский
Лицензия: бесплатно
Домашняя страница: securitykiss.com

Проверялось на *«Ubuntu» 14.04 LTS, Unity (64-bit.).*

Автор:
13.05.14 21:27 -

Read more http://www.linux-info.ru/securitykiss.html