TOR - обеспечиваем анонимность в сети{jcomments on}

Tor (сокр. от англ. **The Onion Router**) — свободное программное обеспечение для реализации так называемой « **луковой маршрутизации** ». С помощью Tor пользователи могут сохранять анонимность при посещении веб-сайтов, отправке сообщений и при работе с другими приложениями, использующими протокол TCP. Безопасность трафика обеспечивается за счёт использования распределённой сети серверов (нод — «узлов»), называемых «многослойными маршрутизаторами» (onion routers).
Система Tor была создана в исследовательской лаборатории Военно-морских сил США по федеральному заказу. В 2002 году эту разработку решили рассекретить, а исходные коды были переданы независимым разработчикам, которые создали клиентское программное обеспечение и опубликовали исходный код под свободной лицензией.

Пользователи сети Tor запускают «луковый» прокси-сервер на своей машине, данное программное обеспечение подключается к серверам Tor, периодически образуя цепочку сквозь сеть Tor, которая использует криптографию многоуровневым способом. Каждый пакет, попадающий в систему, проходит через три различных прокси-сервера (нода), которые выбираются случайным образом. Перед отправлением пакет последовательно шифруется тремя ключами: сначала для третьего узла, потом для второго, и, в конце концов, для первого. Когда первый узел получает пакет, он расшифровывает «верхний» слой шифра (аналогия с тем, как чистят луковицу) и узнает, куда отправить пакет дальше. Второй и третий сервер поступают аналогичным образом. В то же время, программное обеспечение «лукового» прокси предоставляет SOCKS-интерфейс. Программы, работающие по SOCKS-интерфейсу, могут быть настроены на работу через сеть Tor, который, мультиплексируя трафик, направляет его через виртуальную цепочку Tor. Что в конечном итоге позволяет обеспечивать анонимный серфинг в сети.
Внутри сети Tor трафик перенаправляется от одного маршрутизатора к другому и окончательно достигает точки выхода, из которой чистый (нешифрованный) пакет уже доходит до изначального адреса получателя (сервера). Трафик от получателя (сервера)

обратно направляется в точку выхода сети Tor.

Добавляем репозитарий:

apt-add-repository ppa:ubun-tor/ppa

apt-get update

Ставим:

apt-get install tor privoxy

Запускаем:

/etc/init.d/tor start

Он будет использовать следующую конфигурацию:

Protocol: socks5

Port: 9050

Т.е нужно прописать в настройках приложений использование прокси сервера.

Плагин для firefox можно скачать **здесь**