Пускаем трафик до сервера через Clouflare

1. Покупаем домен (можно взять бесплатный на Freenom).
2. Привязываем домен к Cloudflare.
3. На своём сервере с Shadowsocks настраиваем simple-obfs в HTTP-режиме, обязательно с фейловером на обычный вебсервер (obfs=http;failover=127.0.0.1:8080;fast-open как пример). Сам Shadowsocks при этом важно направить работать на 80 порту.
4. В панели управления Cloudflare ставим корневую DNS-запись домена на наш Shadowsocks-сервер, проверяем, чтобы трафик шёл через флару (Режим DNS and HTTP proxy). Желательно также на вкладке Firewall перкключить фаерволл в режим Essentially Off.
5. На своей домашней пеке настраиваем Shadowsocks в том же режиме, обязательно прописываем в настройках simple-obfs наш домен для спуфинга (obfs=http;obfs-host=cooldomain.cf;fast-open как пример), и внимание, в качестве сервера указываем любой IP-адрес клаудфлары (https://www.cloudflare.com/ips/).
6. Профит. Теперь соединение с теневыми носками идёт через клаудфлару, провайдеру становится неизвестен IP-адрес конечного сервера, возможно также сервер станет чуточку быстрее из-за прокладываемых фларой маршрутов. Трафик зашифрован самими носками, поэтому через флару пропускать его безопасно. Главное не злоупотреблять и не качать терабайты.
7. К сожалению, какого-то хуя данное решение не работает на Shadowsocks для ведроида, в то время, как на обычном shadowsocks-libev всё нормально. Учитывая то, что ведроноски часто сломаны (с недавних пор, например, отвалилось перенаправление DNS-запросов на локальный DNScrypt-клиент, висящий на локальном порту того же сервера), потеря не велика.
8. Можно, я думаю, также воспользоваться выдаваемыми фларой HTTPS-сертификатами, но это будет сложнее, потребуется заодно настраивать локальный реверс-прокси для расшифровки SSL-трафика и скармливания расшифрованных HTTP-запросов носкам.