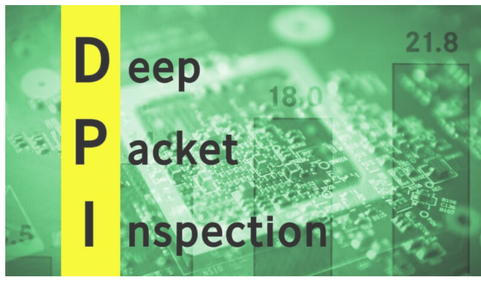
Автономный способ обхода DPI и эффективный способ обхода блокировок сайтов по IP-адресу. GoodbyeDPI и ReQrypt

Admin • September 22, 2017



Провайдеры Российской Федерации, в большинстве своем, применяют системы глубокого анализа трафика (DPI, Deep Packet Inspection) для блокировки сайтов, внесенных в реестр запрещенных.

Не существует единого стандарта на DPI, есть большое количество реализации от разных поставщиков DPI-решений, отличающихся по типу подключения и типу работы.

Существует два распространенных типа подключения DPI: пассивный и активный.

Пассивный DPI:

Пассивный DPI — DPI, подключенный в провайдерскую сеть параллельно (не в разрез) либо через пассивный оптический сплиттер, либо с использованием зеркалирования исходящего от пользователей трафика. Такое подключение не замедляет скорость работы сети провайдера в случае недостаточной производительности DPI, из-за чего применяется у крупных провайдеров. DPI с таким типом подключения технически может только выявлять попытку запроса запрещенного контента, но не пресекать ее. Чтобы обойти это ограничение и заблокировать доступ на запрещенный сайт, DPI отправляет пользователю, запрашивающему заблокированный URL, специально сформированный HTTP-пакет с перенаправлением на страницу-заглушку провайдера, словно такой ответ прислал сам запрашиваемый ресурс (подделывается IP-адрес отправителя и TCP sequence). Из-за того, что DPI физически расположен ближе к пользователю, чем запрашиваемый сайт, подделанный ответ доходит до устройства пользователя быстрее, чем настоящий ответ от сайта.

Активный DPI:

Активный DPI — DPI, подключенный в сеть провайдера привычным образом, как и любое другое сетевое устройство. Провайдер настраивает маршрутизацию так, чтобы DPI получал трафик от пользователей к заблокированным IP-адресам или доменам, а DPI уже принимает решение о пропуске или блокировке трафика. Активный DPI может проверять как исходящий, так и входящий трафик, однако, если провайдер применяет DPI только для блокирования сайтов из реестра, чаще всего его настраивают на проверку только исходящего трафика.

Системы DPI разработаны таким образом, чтобы обрабатывать трафик с максимально возможной скоростью, исследуя только самые популярные и игнорируя нетипичные запросы, даже если они полностью соответствуют стандарту.

Программа для обхода DPI

Я написал программу для обхода DPI под Windows: GoodbyeDPI.

Она умеет блокировать пакеты с перенаправлением от пассивного DPI, заменять Host на hoSt, удалять пробел между двоеточием и значением хоста в заголовке Host, «фрагментировать» HTTP и HTTPS-пакеты (устанавливать TCP Window Size), и добавлять дополнительный пробел между HTTP-методом и путем.

Преимущество этого метода обхода в том, что он полностью автономный: нет внешних серверов, которые могут заблокировать.

По умолчанию активированы опции, нацеленные на максимальную совместимость с провайдерами, но не на скорость работы. Запустите программу следующим образом:

> *goodbyedpi.exe -1 -a*

Если заблокированные сайты стали открываться, DPI вашего провайдера можно обойти.

Попробуйте запустить программу с параметром -2 и зайти на заблокированный HTTPS-сайт. Если все продолжает работать, попробуйте режим -3 и -4 (наиболее быстрый).

Некоторые провайдеры, например, Мегафон и Yota, не пропускают фрагментированные пакеты по HTTP, и сайты перестают открываться вообще. С такими провайдерами используйте опцию -3 -a

Эффективное проксирование для обхода блокировок по IP

В случае блокировок по IP-адресу, провайдеры фильтруют только исходящие запросы на IP-адреса из реестра, но не входящие пакеты с этих адресов.

Программа ReQrypt работает как эффективный прокси-сервер: исходящие от клиента пакеты отправляются на сервер ReQrypt в зашифрованном виде, сервер ReQrypt пересылает их серверу назначения **с подменой исходящего IP-адреса на клиентский**, сервер назначения отвечает клиенту напрямую, минуя ReQrypt.

Если наш компьютер находится за NAT, мы не можем просто отправить запрос на сервер ReQrypt и ожидать ответа от сайта. Ответ не дойдет, т.к. в таблице NAT не создана запись для этого IP-адреса.

Для «пробива» NAT, ReQrypt отправляет первый пакет в TCP-соединении напрямую сайту, но с TTL = 3. Он добавляет запись в NAT-таблицу роутера, но не доходит до сайта назначения.

Долгое время разработка была заморожена из-за того, что автор не мог найти сервер с возможностью спуфинга. Спуфинг IP-адресов часто используется для амплификации атак через DNS, NNTP и другие протоколы, из-за чего он запрещен у подавляющего большинства провайдеров. Но сервер все-таки был найден, хоть и не самый удачный. Разработка продолжается.

Заключение и TL;DR

GoodbyeDPI — программа под Windows, позволяющая обходить пассивные и активные DPI. Просто скачайте и запустите ее, и заблокированные сайты станут снова доступны.

Для Linux есть аналогичная программа — zapret.

Используйте кроссплатформенную программу ReQrypt, если ваш провайдер блокирует сайты по IP-адресу.

Определить тип блокировки сайтов можно программой Blockcheck. Если в тестах DPI вы видите, что сайты открываются, или видите строку «обнаружен пассивный DPI», то GoodbyeDPI вам поможет. Если нет, используйте ReQrypt.

Полная инструкция и дополнительные материалы доступны у нас на форуме.