УДК 004.057.4

ВЫБОР СРЕДСТВ ДЛЯ СКРЫТИЯ IP АДРЕСА ПРИ РАБОТЕ В ГЛОБАЛЬНОЙ СЕТИ (СРАВНЕНИЕ PROXY, SSH И VPN)

Хожевец О.А., аспирант БГУИР

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Аннотация. В статье анализируется проблема использования различных средств для изменения IP адреса пользователя при работе в глобальной сети. В работе проводится анализ эффективности применения проксификаторов, сравнение их функциональных возможностей.

Ключевые слова. Анонимность, модель OSI, прокси, протоколы.

За непродолжительное время в системах защиты и в системах обхода систем защиты многое поменялось, но одна вещь так и не изменилась, извечный спор: "Что лучше? Прокси? ВПН? SSH туннель?".

Сколько людей - столько и мнений. Различные сообщества время от времени пытаются решить данную проблему и найти лучшее решение.

Зачем нужны проксификаторы?

Основной целью использования Проксификаторов, является изменение IP адреса пользователя. Чтобы создать новую личность и выглядеть в глазах систем идентификации(защиты) новым пользователем необходимо сменить IP и многие на этом и останавливаются, однако те ресурсы, которые помогают сменить IP, могут и навредить.

Пользователи часто путают понятия "Анонимность" и "Безопасность" и в следствии неправильного использования сетевых ресурсов наблюдается "Эффект страуса". Пользователь думает, что он сменил IP и теперь его никто не узнает, но в это же время у него наблюдаются утечки его реального IP адреса сразу в нескольких местах - то есть хоть голова и в земле, а туловище все равно снаружи именно по причине неправильного использования сетевых ресурсов и происходит деанонимизация пользователя системами идентификации пользователей.

Первое с чего необходимо начать - это с фундамента, необходимо определить какие именно сетевые ресурсы необходимы, и в этом поможет Модель OSI на рисунке 1.

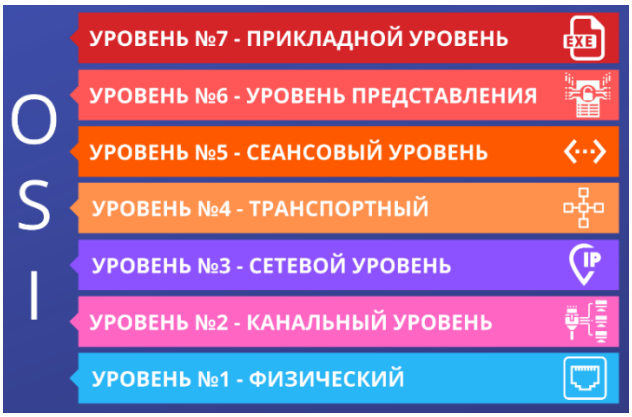

Рисунок 1 — Модель OSI [1]

Есть семь основных этапов сетевого соединения, и каждый из этих этапов (далее - уровни) характеризуется различным уровнем прав, доступа и архитектуры в зависимости от того, на каком из уровней необходимо работать и будет зависеть выбор Проксификатора, потому что в некоторых случаях хватит прокси в браузере (Уровень 7) а иногда придется опустится ниже, например при проксификации всей операционной системы с помощью ВПН (Уровень 2)

Какие ресурсы принято использовать для изменения IP адреса при обходе систем идентификации пользователей?

Proxy сервера. Proxy сервера (Прокси) - сервер посредник - он получает пакеты пользователя при соединении и "носит" их от пользователя к целевому веб ресурсу.

Прокси может быть настроен на сервере, домашнем ПК, роутере, телефоне, кофеварке и практически любом другом доступном сетевом ресурсе.

Прокси бывают нескольких видов:

CGI - или по-другому web прокси. Это веб страница, на которой предлагается ввести адрес сайта, и он откроется в этой же странице с другим IP. Браузерный вариант.

HTTP - Простой прокси для HTTP запросов. Бесполезное решение в нашем случае.

Ко всему прочему HTTP делятся еще на три условные группы:

Прозрачные прокси - Сообщат всем веб ресурсам реальный IP пользователя. Пример - заголовок x-forwarded-for.

Анонимные прокси - Скроют IP пользователя, но сообщат о том, что используется прокси. Бесполезно.

Элитные прокси - Скроют IP пользователя, не сообщат о том, что используется прокси, ну и на этом все.

HTTPS - Тот же прокси HTTP но уже +S - а это значит, что он поддерживает шифрование, то есть у пользователя будут проксифицировать вебстранички https - формы авторизации, ввод и передача чувствительной информации и т.д. Но этот прокси все равно издалека виден системам идентификации, плюс ко всему еще и может модифицировать пакеты пользователя.

Socks 4 - Первый пригодный для работы протокол Прокси. Пытается скрыть проксификацию, не модифицирует пакеты и в целом неплох, но имеет свои минусы.

Socks 5 - Практически идеальный вариант, то же что и Socks 4, но добавилась нужная поддержка UDP протокола, и соответственно возможность подмены DNS и IPv6.

ShadowSocks - Китайское опенсорс изобретение, которое по функционалу лидирует среди всех конкурентов.

Proxy является самой многочисленной группой и самым популярным средством изменения IP адреса при работе с различными системами защиты и идентификации пользователя. В таблице 1 приведено сравнение самых популярных Proxy протоколов.

Таблица 1– Сравнение протоколов прокси

	HTTP	HTTPS	SOCKS 4	SOCKS 5	SHADOWSOCKS
Скрывает реальный IP	+	+	+	+	+
Поддержка SSL шифрования	-	+	+	+	+
Скрывает факт проксификации	-	-	+	+	+
Не изменяет заголовок пакета	-	-	+	+	+
Проксификация всех пакетов	-	-	+	+	+
Работа за фаерволом	-	-	+	+	+
Проксификация DNS запросов	-	-	-	+	+
Адресация IP6	-	-	-	+	+
Расширенные протоколы шифрования	-	-	-	-	+
Маскировка трафика	-	-	-	-	+
Защита от DPI	-	-	-	-	+

После изучения таблицы не остается вопросов с каким проксификатором лучше работать. Разница между протоколами Proxy впечатляющая, и при этом каждый пункт функционала, указанный в этой таблице, может использоваться системами идентификации пользователей.Именно эта разница в функционале делает HTTP, HTTPS, SOCKS 4 протоколы бесполезными, потому что отсутствие поддержки UDP протокола и плюс к этому отсутвие проксирования DNS запросов будут аномальными и выделят пользователя среди массы других реальных пользователей.

Варианты Socks 5 и ShadowSocks являются единственными, которые могут помочь в маскировке личности пользователя при работе с системами идентификации пользователей. Но есть не только Proxy, рассмотрим другие технологии.

SSH туннели. Вторая по популярности после Proxy технология. Удаленный сервер, который по принуждению пользователя стал сервером посредником. Работает это следующим образом - при

соединении SSH-клиента и SSH-сервера со стороны SSH-клиента поднимается SOCKS-прокси, например, на localhost'е, на который можно указывать приложениям с поддержкой SOCKS. Само проксирование будет через SSH-сервер, с которым соединяется пользователь. В сумме - Интернет будет видеть пользователя от имени SSH-сервера, соединение между SSH-клиентом и SSH-сервером зашифровано, так что не видно вложенных данных приложения, а для приложения все выглядит как обращение к обычному SOCKS-прокси.

VPN. VPN - Виртуальная Частная Сеть - технология позволяющая создать зашифрованное соединение в незашифрованных сетях. Пришла из телефонных сетей и насчитывает более 10 разновидностей, на практике же, при всех своих достоинствах имеет серьезный недостаток в работе - слабую возможность маскировки использования технологии VPN. В дальнейшем сравнении возьмем усредненную рыночную конфигурацию VPN. Ввиду того, что на рынке присутствует большое разнообразие VPN сервисов, и у каждого свои особенности рассмотрим их в общем.

TOR. Когда речь заходит о смене личности некоторые люди воспринимают TOR как панацею. Но в TOPе есть проблемы:

1. TOP Браузер не изменяет отпечатки цифровой личности.
2. TOP Браузер имеет свои уникальные особенности, которые выдают пользоватея.
3. Всем известно что сеть TOP официально выступает за интернет без цензуры, по факту его используют для противоправных действий. Ни одна уважающая себя система защиты не позволит ничего сделать с IP адреса входящего в сеть выходных узлов сети TOP. Поэтому сеть TOP не пригодна для работы.

По результатам, среди всех популярных технологий, по смене IP адреса можно выделить четыре технологии пригодные для работы: Socks 5, ShadowSocks, SSH туннели, VPN.

Признаются непригодными для работы: CGI Proxy, HTTP Proxy, HTTPS Proxy, Socks 4 Proxy, TOR.

Результатом анализа технологии по смене IP необходимо выделить лучшую из всех, при сведении полученных результатов в таблицу 2 получается:

Таблица 2. Сравнение протоколов анонимайзеров.

	SSH тунель	VPN	SOCKS 5	SHADOWSOCKS
Скрывает реальный IP	+	+	+	+
Поддержка SSL шифрования	+	+	+	+
Скрывает факт проксификации	+	-	+	+
Не изменяет заголовок пакета	+	+	+	+
Проксификация всех пакетов	+	+	+	+
Работа за фаерволом	+	+	+	+
Поддержка UDP протокола	-	+	+	+
Проксификация DNS запросов	+	+		
Адресация IP6	-	+	+	+
Расширенные протоколы шифрования	-	+	-	+
Маскировка трафика	-	-	-	+
Защита от DPI	-	-	-	+

Технология ShadowSocks является лидирующей.

Место №1 – ShadowSocks. Технология, которая единственная из анализируемых создавалась именно для маскировки личности, в то время как остальные были созданы либо для обеспечения безопасности передаваемой информации, либо как часть сетевой архитектуры. В этом и кроется секрет успеха ShadowSocks т.к. Анонимность была причиной его появления, но никак не следствием.

Место №2 - Socks 5. Имея свои явные недостатки протокол Socks 5 все равно остается надежным решением по смене личности при работе с системами идентификации пользователей. Да, он не маскирует трафик, не устойчив против Deep Packet Inspection - но такие технологии на данный момент встречаются довольно редко, поэтому работать возможно, хоть время и неумолимо летит вперед, и ситуация по актуальности использования Socks 5 скоро изменится не в лучшую сторону.

Место №3 - VPN и SSH. На третьем месте разместились сразу две технологии способные изменить IP адрес, и они в целом тождественные - они могут использоваться в работе, но их выявление является в большинстве случаев очень простой задачей, поэтому рассчитывать на данные технологии в работе не лучший выбор. Вариантов определения использования VPN и SSH довольно много и фактически все из них уже используются системами идентификации

Список использованных источников:

1. *Филимонов А.Ю. Построение мультисервисных сетей Ethernet. — М.: BHV, 2007.*
2. *Shadowsocks. Почему лучше, чем обычный SOCKS, и практика использования. [Электронный ресурс]. — Режим доступа: https://netwhood.online/2018/12/17/shadowsocks/*
3. *Ачилов Р.Н. Построение защищенных корпоративных сетей. — М.: ДМК Пресс, 2013. -250 с.*

UDC 004.057.4

SELECTING MEANS TO HIDE IP ADDRESS WHEN WORKING IN THE GLOBAL NETWORK (COMPARISON OF PROXY, SSH AND VPN)

Khozhevets O.A.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Annotation. The article analyzes the problem of using various tools to change the user's IP address when working in the global network. The paper analyzes the effectiveness of the use of proxifiers, compares their functionality.

Keywords. Anonymity, OSI model, proxies, protocols.