

*Бежик Антон Александрович, студент бакалавриата 2 курс,
МИРЭА-Российский технологический университет (РТУ МИРЭА),
Россия, г. Москва, Институт информационных технологий
Россия, г. Москва*

*Свищёв Андрей Владимирович, старший преподаватель кафедры
практической и прикладной информатики
МИРЭА-Российский технологический университет (РТУ МИРЭА),
Россия, г. Москва, Институт информационных технологий
Россия, г. Москва*

СЕРВИСЫ VPN: ЧТО ЭТО ТАКОЕ, ПРИЧИНЫ ВОЗНИКНОВЕНИЯ, ЦЕЛЬ СУЩЕСТВОВАНИЯ, НЕОБХОДИМОСТЬ ИСПОЛЬЗОВАНИЯ И ВОЗМОЖНЫЕ АЛЬТЕРНАТИВЫ

Аннотация: С развитием сетевых технологий, безопасность в Интернете стала одним из важных факторов его использования. Большинство соединений в Интернете трудно назвать безопасными, их просмотр может быть осуществлен как другими пользователями, так и интернет провайдером. Для того чтобы обезопасить данные пользователя от просмотра и хищения сторонними лицами, был разработан новый вид подключения - VPN.

Ключевые слова: VPN, Виртуальная Приватная Сеть, разновидности VPN подключений, что такое VPN.

Abstract: With the development of network technologies, Internet security has become one of the important factors in its use. Most Internet connections can hardly be called secure, their viewing can be carried out both by other users and by an Internet provider. In order to protect user data from being viewed and stolen by third parties, a new type of connection has been developed - VPN.

Keywords: VPN, Virtual Private Network, types of VPN connections, what is VPN.

Настоящая статья посвящена теме возникновения технологии VPN, описанию её развития и выделения главных сервисов на рынке.

Технология VPN в данный момент времени являлась одним из главных сетевых трендов. Благодаря технологии VPN человек получает возможность обойти большинство региональных барьеров, установленных на потребляемый контент.

Целью исследования является выяснение что такое технология VPN, причины её возникновения и показ главных представителей данной услуги.

Объектом исследования является возникновение технологии и путь развития VPN.

Предмет исследования

Есть ли смысл в предоставлении услуг VPN или существуют более удобные и дешевые средства, предоставляющие аналогичные услуги.

Практическая значимость исследования

Проведение анализа технологии VPN и составления мнения о её заменяемости и нахождение главных представителей рынка, для обозначения качественных сервисов по предоставлению услуги.

Что такое VPN и зачем его используют

VPN или Virtual Private Network - это защищенный поток данных (туннель) между пользовательским устройством и сетью Интернет. Подключение VPN позволяет сберечь ваши данные передаваемые куда либо от стороннего влияния, а именно прослушивания или вмешательства в них. Сами по себе сервисы VPN являются наиболее простым способом по защите своих данных и сокрытия своих личных данных в сети Интернет [1].

Обычные пользователи используют VPN подключение для того чтобы свободно использовать Интернет в тайне от других пользователей и для обхода региональных ограничений.

Крупные компании используют VPN соединения для создания безопасного соединения наподобие локального при подключении сотрудника извне. Корпоративные VPN сервисы не настолько гибкие и предоставляют меньше возможностей пользователю, поскольку их задача состоит в основном только из предоставления безопасного подключения между сотрудниками.

Преимущества использования VPN сервисов

Как мы выяснили выше, сервисы VPN занимаются предоставлением защищенного канала данных для передачи данных [2], однако какими плюсами помимо этого они обладают. Вот несколько из таковых:

- Изменение местоположения;
- Защита конфиденциальности;
- Повышения безопасности;
- Доступ к web-страницам.

Рассмотрим каждое преимущество поподробнее.

Изменение местоположения

Если вы используете сервис VPN, то для защиты ваших данных он производит смену вашего IP-адреса на уникальный номер. По данному номеру легко определить ваше новое местоположение и личность. Благодаря этому, при помощи этого специального номера вы можете свободно пользоваться интернетом как-будто вы находитесь в Англии, США, России, Японии или в любой стране имеющие у себя на территории VPN сервера.

Защита конфиденциальности

Благодаря смене IP адреса можно легко защитить вашу личность и местоположение от нежелательных наблюдателей вашей активности в интернете, сайтов, приложений и сервисов или других пользователей. Также благодаря VPN сервисам ваш провайдер или оператор сотовой связи также не может получить доступ к вашему трафику.

Повышения безопасности

Благодаря VPN подключения вы также повышаете свою безопасность в публичных сетях. Использование VPN предотвращает сниффинг пакетов, атаки

через посреднические сети Wi-Fi и обезопасивает от подключений к поддельным сетям. Это очень удобно при работе вне дома, либо при нахождении в командировке, так как в поездке нельзя быть уверенным в безопасности всех сетей, к которым производится подключение.

Доступ к web-страницам

При нахождении в странах с ограничениями по доступу к популярным ресурсам, например, в Китае, VPN сервисы позволяют свободно использовать любые заблокированные интернет-ресурсы на территории страны. Так же подключение к VPN позволяет обойти практически любой FireWall установленный в публичных или корпоративных сетях.

Как работают сервисы VPN

Установления VPN подключения

При подключении к сети интернет при помощи сервиса VPN между вашим устройством (VPN клиентом) и VPN сервером устанавливается безопасное подключение. Ваш данные все ещё проходят через провайдера, однако он уже не в состоянии распознать что в них находится или понять куда они направляются. Все веб страницы перестают видеть ваш оригинальный IP-адрес и начинают видеть адрес VPN сервера. Этот адрес совместно используется множеством пользователей и меняется в течении некоего промежутка времени.

Также соединение VPN подразделяется на несколько видов подключений. Самые функциональные и популярные из них:

- Проксирование;
- Аутентификация;
- Туннелирование;
- Шифрование.

Рассмотрим эти соединения подробнее.

Проксирование

Чаще всего сервисы VPN работают также, как и прокси-сервера. Прокси-сервер является посредником для всего вашего взаимодействия с сетью. Вместо вашего IP-адреса и вашего местоположения всем виден IP-адрес прокси-сервера,

через которое произведено ваше VPN соединение. Благодаря этому VPN является одним из самых безопасных способов подключений в интернете.

Аутентификация

Для создание безопасных соединений требуются сложные математические методы и выражения. Для того чтобы справиться с данной задачей был придуман метод аутентификации. После выполнения аутентификации, VPN-сервер и VPN-клиент полностью завершают своё сопряжение.

Туннелирование

Туннелирование и шифрование - это методы защиты соединения между клиентом и сервером VPN. При туннелировании каждый пакет данных перемещается в другой пакет с данными. Благодаря этому сторонним пользователям сложнее получить доступ к передаваемой информации во время её перемещения.

Шифрование

Шифрование - это способ сокрытия данных от сторонних лиц, с возможностью расшифровки получателем. Благодаря этому пользователь может скрыть свой трафик от провайдера [3].

VPN Протоколы

VPN протоколы [4] - это способы, с помощью которых устройство клиента соединяется с сервером VPN. у каждого из протоколов есть свои преимущества и недостатки. Какое-то из соединений позволяет обеспечить быструю передачу данных, а какое-то имеет повышенную безопасность. Самые популярные VPN протоколы:

- ***OpenVPN*** - протокол с открытым исходным кодом, является одним из самых безопасных.
- ***IKEv2*** - один из новейших протоколов, главным преимуществом которого является скорость передачи.
- ***L2TP / IPsec*** - виртуальный туннельный протокол, использующийся в частных локальных сетях.
- ***PPTP*** - туннельный протокол точечного типа, устанавливающий

соединение в виртуальных частных сетях.

- **WireGuard** - протокол с открытым исходным кодом, конкурент протоколов IPsec и OpenVPN.
- **SSTP** - это форма виртуальной частной сети, обеспечивающая безопасную связь.

Альтернатива VPN сервисам

Хотя полноценной альтернативы VPN с точки зрения безопасности, анонимности и скорости в интернете найти невозможно, есть варианты с похожими услугами, чей функционал урезан по сравнению с VPN [5].

Tor (The Onion Router)

Это бесплатный сервис, предоставляющий доступ к сети сервером, который рандомизированным способом перенаправляет интернет трафик, таким образом определения источника данных становится невозможным (см. Рисунок 1).

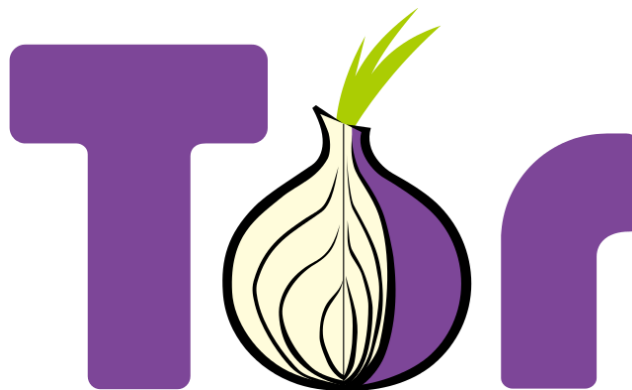


Рисунок 1 – Tor

Часто использование Tor совмещают с использованием VPN, так как их методы безопасности работают по-разному и в совокупности дают очень высокий уровень безопасности.

Главным же недостатком Tor браузера является медленная скорость передачи данных. Это происходит из-за передачи трафика между серверами, которая происходит множество раз перед тем как достигнуть пользователя. Из-за этого работать с большими файлами внутри Tor становится неудобно.

Прокси-сервисы

Это посредник между клиентским устройством и сетью Интернет. Однако практически все Прокси-сервисы предоставляют довольно медленную скорость передачи пакетов, а преимущество в конфиденциальности и безопасности в этих соединениях отсутствует напрочь. Работу прокси сервера можно посмотреть на рисунке 2.

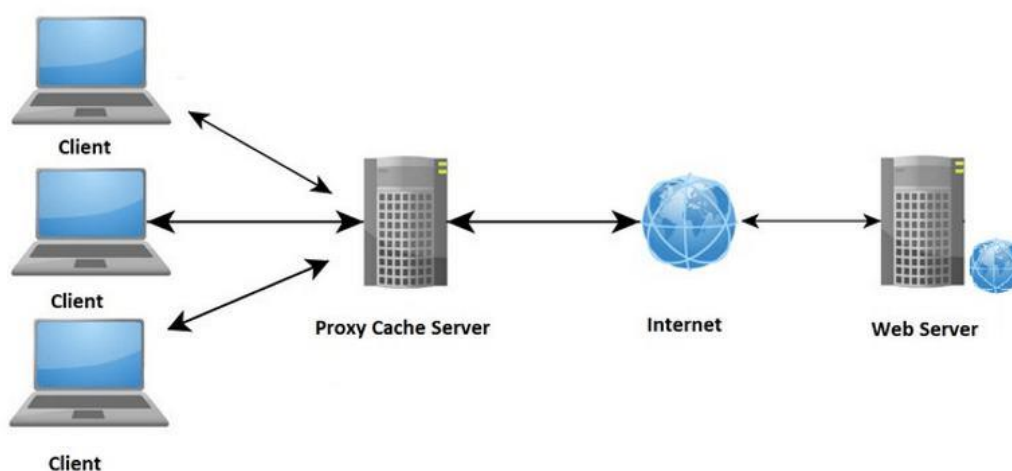


Рисунок 2 - Работа прокси сервера

Сущность вышеизложенного сводится к тому, что VPN сервисы являются необходимой и удобной технологией. Имеется множество протоколов VPN сервисом под разные типовые задачи, у каждого из них есть свои достоинства и недостатки. Сама по себе технология VPN на данный момент уникальная и не имеет аналогов предоставляющий такой же широкий и вместе с тем направленный спектр цифровых услуг.

Библиографический список:

1. kasperskiy //Антивирус, Режим доступа: свободный [Электронный ресурс] - URL -<https://www.kaspersky.ru/blog/vpn-explained/10635/> (Дата обращения: 18.11.2021).
2. РБК //Новостной портал, Режим доступа: свободный [Электронный ресурс] - URL - <https://trends.rbc.ru/trends/industry/604f0a309a79477d332569e3>(Дата обращения: 20.11.2021).

3. Настоящее время //Информационный ресурс, Режим доступа: свободный [Электронный ресурс] - URL - <https://www.currenttime.tv/a/internet-bezopasnost-vpn/31145192.html> (Дата обращения 15.11.2021).

4. Le-VPN //Дистрибьютор VPN сервисов, Режим доступа: свободный [Электронный ресурс] - <https://le-vpn.com/ru/15-reasons-use-vpn-service/> (Дата обращения 21.11.2021).

5. КОМЬЮНИТИ //Информационный ресурс, Режим доступа: свободный [Электронный ресурс] - URL - <https://timeweb.com/ru/community/articles/chto-takoe-vpn-i-zachem-on-nuzhen> (Дата обращения 22.11.2021).