ЧТО ТАКОЕ VPN И ТУННЕЛИРОВАНИЕ?

**VPN** ***(virtual private network – виртуальные частные сети)***и **туннелирование** являются методами, позволяющими шифровать информационное соединение между вашим компьютером и другим компьютером сети. Другой компьютер может принадлежать вашей организации, доверенному лицу или коммерческому VPN сервису. Туннелирование скрывает информацию отдельных информационных потоков внутри зашифрованного протокола, таким образом, превращая весь проходящий через туннель трафик нечитабельным для посторонних, на всем своем пути. Виртуальные частные сети очень часто используются корпорациями для обеспечения сотрудников, которым необходим доступ к конфиденциальной финансовой или другой информации, подключением к компьютерным сетям компании из дома или других отдаленных мест через сеть Интернет.

Использование VPN или других разновидностей туннелирования с целью шифрования вашей информации может быть очень хорошим способом обеспечения её закрытости для всех, кроме вас и тех людей, которым вы доверяете. У этого способа есть еще один дополнительный эффект, который заключается в том, что различные виды трафика выглядят для «подслушивающего» одинаково, это также касается систем, пытающихся блокировать отдельные ресурсы в сети Интернет. Учитывая, что многие международные организации используют технологию VPN, очень маловероятно, что она будет заблокирована.

Эти методы создают туннель от вашего компьютера до другого компьютера в сети Интернет. Ваша информация может сначала проходить через этот туннель, а затем продолжить путь до пункта назначения во всемирной паутине. Сохранность и конфиденциальность трафика внутри туннеля защищаются шифрованием.



Если туннель заканчивается вне территории, где Интернет подвергается фильтрации, это может быть эффективный метод обхода Интернет цензуры, так как фильтрующая единица/сервер видит только шифрованные данные и не имеет возможности узнать, какая информация проходит через туннель.

Важно заметить, что данные шифруются только до конца туннеля и затем перемещаются в незашифрованном виде до пункта назначения. Так, например, если вы установили туннель с коммерческим провайдером VPN. И затем запросили веб страницу [news.bbc.co.uk](http://www.sesawe.net/news.bbc.co.uk) через этот туннель, данные будут передаваться в зашифрованном виде только от вашего компьютера до компьютера провайдера VPN, находящегося на другом конце соединения, но после него данные не будут зашифрованы для серверов, управляемых BBC, также как и любой другой Интернет трафик. Это означает, что VPN провайдер, BBC и люди, контролирующие систему между этими двумя серверами, теоретически могут видеть, какую информацию вы запросили.

Туннелирование

Главным различием между VPN соединением и туннелем является то, что система VPNподразумевает шифрование всех данных между вашим компьютером и Интернетом, в то время как при использовании **туннеля** кодируется только трафик, обрабатываемый отдельными приложениями. Шифрование при этом основывается либо на **номерах портов**, используемых этими приложениями, либо программа запрашивает у вас информацию о том, какой туннель использовать для каждого приложения. В отличие от VPN, при использовании туннелей требуется отдельно настраивать все приложения, которые должны использовать шифрованный туннель (веб браузер, клиент электронной почты или программа службы обмена мгновенными сообщениями) на работу через него. Интересным фактом является то, что не все приложения способны работать через распространенные типы туннелей. Например, большинство VoIP систем используют протокол **UDP**, который не поддерживается большей частью систем туннелирования. Также некоторые популярные приложения, такие как веб браузер Opera, не имеют встроенной поддержки для **прокси-серверов типа SOCKS**, которые являются самым распространенным типом прокси-серверов в программном обеспечении для туннелирования. В случаях возникновения подобных проблем вам придется использовать дополнительное приложение, такое как FreeCap для операционных систем Windows (<http://www.freecap.ru/eng/>) или tsocks для Linux (<http://tsocks.sourceforge.net/>).

После создания туннеля и настройки приложений, коммуникация этих приложений с сетью Интернет будет проходить через шифрованный туннель, идущий до компьютера с установленным программным обеспечением туннелирования, который напрямую передает запросы пользователей и ответы серверов сети. Пользователи, у которых есть знакомые в странах без Интернет цензуры, могут установить частные сервисы туннелирования, в то время как остальные могут воспользоваться аналогичными коммерческими сервисами. Обычно стоимость подобных сервисов составляет примерно 5 долларов США в месяц (чаще всего для оплаты требуется наличие кредитной карты).

Существуют также различные бесплатные сервисы туннелирования. При использовании бесплатных сервисов пользователи должны знать, что последние часто включают рекламу. Рекламные запросы иногда осуществляются посредством незашифрованных **HTTP открытых текстовых запросов**, которые могут перехватываться посредниками (Интернет сервис провайдер). Последние на этом основании могут определить, что пользователь использует сервис туннелирования. Более того, многие сервисы туннелирования основываются на использовании прокси-серверов типа SOCKS, при использовании которых возможна утечка запросов **доменных имен**. Названия некоторых коммерческих систем туннелирования, которые также предоставляют бесплатный сервис (медленный) приведены ниже:

•      <http://www.http-tunnel.com/>

•      <http://www.hopster.com/>

•      <http://www.htthost.com/>

VPN

В отличие от туннелей системы VPN передают все данные через шифрованную сеть, включая**Voice over IP** (VoIP) и информационный обмен с приложениями, не поддерживающими SOCKS. Установленные VPN системы являются более разносторонними инструментами, чем туннели, но их установка и настройка является более сложной по сравнению с большинством приложений туннелирования.

Существует несколько различных стандартов установки VPN сетей, включая **IPSec**, **SSL/TLS**и**PPTP**, которые различаются по своей сложности, по обеспечиваемому уровню безопасности и по совместимости с отдельными операционными системами. Естественно существует также множество различий в реализации каждого стандарта на уровне программного обеспечения, которое имеет различные свойства.

•    Хоть и считается, что PPTP использует более слабое шифрование, по сравнению с IPSec и SSL/TLS, но этот стандарт может быть очень удобен для обхода Интернет блокирования и его клиентское программное обеспечение встроено в большинство версий Microsoft Windows.

•    VPN системы, созданные на основе SSL/TLS, довольно просты в настройке и обеспечивают высокий уровень безопасности.

•    IPSec работает на уровне сети Интернет, который ответственен за передачу пакетов данных в Интернет архитектуре, в то время как другие стандарты используют уровень приложений. Этот факт говорит о том, что IPSec является более гибким инструментом, так как он может быть использован для защиты всех остальных протоколов, находящихся на более высоких уровнях. Кроме того, приложения не должны быть разработаны специально для использования IPSec, в то время как функции SSL/TLS или других протоколов высокого уровня должны быть встроены в приложение.

**Виртуальные Частные Сети** часто используются компаниями и организациями в качестве частных каналов коммуникации для обеспечения безопасного подключения через сеть Интернет. В связи с их популярностью существует множество коммерческих провайдеров услугVPN, которые позволяют вам получить доступ к сервису VPN за определенную плату. Использование подобного сервиса требует от вас доверия к его владельцам, при этом обеспечивая простой и удобный метод обхода Интернет фильтрации за месячную плату в размере около 5-10 долларов США. Список коммерческих провайдеров VPN услуг доступен здесь: <http://en.cship.org/wiki/VPN>.

В качестве альтернативы платным коммерческим VPN сервисам, пользователи, имеющие знакомых, живущих в странах, где отсутствует Интернет цензура, могут попросить их скачать и установить программное обеспечение, которое создаст частный VPN сервис. Это требует существенно более высокого уровня технических знаний, но после установки будет работать бесплатно. Помимо прочего частная природа таких установок обуславливает меньшую вероятность их блокирования, чем в случае с коммерческими сервисами, которые были доступны в течение продолжительного времени. Одной из наиболее распространенных, бесплатных программ с открытым кодом, позволяющих установить подобные частные VPN сети, является OpenVPN (<http://openvpn.net/>). Программа может устанавливаться на Linux, MacOS, Windows и многие другие операционные системы.

Преимущества

Приложения туннелирования и виртуальных частных сетей обеспечивают шифрованную передачу ваших данных. Как правило, они способны безопасно выполнять различные функции удаленного компьютера, не только передавать веб трафик. Так что их использование является одним из наиболее безопасных способов обхода Интернет цензуры. После настройки программного обеспечения, использовать его очень просто.

Приложения туннелирования и виртуальных частных сетей больше всего подходят технически грамотным пользователям, которым необходим безопасный сервис обхода Интернет цензуры более чем только для получения веб трафика, и которые имеют доступ в Интернет со своих собственных компьютеров, так что они могут установить на них дополнительной программное обеспечение. Коммерческие сервисы туннелирования являются идеальным ресурсом для пользователей в странах с Интернет цензурой, у которых нет надежных знакомых, имеющих свободный доступ в сеть Интернет. Виртуальные частные сети (VPN) являются распространенным бизнес приложением, которое, скорее всего, не будет заблокировано.

Некоторые, но не все, коммерческие туннели и VPN сервисы заявляют, что могут обеспечить уровень конфиденциальности, который не может быть достигнут при использовании частных сервисов. Эта защита конфиденциальности может быть действительно эффективной. Но только в том случае, если коммерческий провайдер виртуальных частных сетей или туннелирования является надежным.

Недостатки и риски

Коммерческие сервисы туннелирования и коммерческие виртуальные частные сети (VPN) официально опубликованы и могут уже быть подвержены фильтрации. Они, как правило, не могут быть использованы в местах публичного доступа (таких как Интернет кафе или библиотеки), где пользователи не могут установить дополнительное программное обеспечение. Использование приложений туннелирования и особенно виртуальных частных сетей требует наличия более высокого уровня технической грамотности, чем в случае использования других методов обхода Интернет цензуры.

Сетевой оператор может раскрыть факт использования VPN и определить кто является провайдером виртуальной частной сети. Сетевой оператор не должен иметь возможности просматривать содержание информационного обмена, осуществляемого через VPN, за исключением тех случаев, когда VPN установлена неправильно.

Оператор VPN или туннеля (также как и оператор прокси сервиса) может отслеживать ваши действия, если только вы не используете дополнительное шифрование для ваших коммуникаций. Если вы его не используете, вам придется доверять оператору VPN или туннеля и надеяться, что он не злоупотребит этим доступом.