ИССЛЕДОВАНИЕ ПРИНЦИПОВ РАБОТЫ VPN, РАЗРАБОТКА ПОЛИТИКИ БЕЗОПАСНОСТИ VPN. ИСПОЛЬЗОВАНИЕ АНОНИМАЙЗЕРОВ

Волохов В.В. Email: Volokhov1146@scientifictext.ru

Волохов Владислав Владиславович - студент,
кафедра компьютерной и информационной безопасности, факультет кибернетики,
Московский технологический университет, г. Москва

Аннотация: *виртуальная частная сеть (VPN - VirtualPrivateNetwork) создается на базе общедоступной сети Интернет. И если связь через Интернет имеет свои недостатки, главным из которых является то, что она подвержена потенциальным нарушениям защиты и конфиденциальности, то VPN могут гарантировать, что направляемый через Интернет трафик так же защищен, как и передача внутри локальной сети. В тоже время виртуальные сети обеспечивают существенную экономию затрат по сравнению с содержанием собственной сети глобального масштаба. В данной статье анализируются как различные методы организации защищенной сети, так и атаки, используемые злоумышленниками.*
Ключевые слова: *интернет, угрозы, безопасность.*

STUDY OF THE PRINCIPLES OF VPN OPERATION, DEVELOPMENT OF VPN SECURITY POLICY. USING ANONYMIZERS

Volokhov V.V.

Volokhov Vladislav Vladislavovich - Student,
COMPUTER AND INFORMATION SECURITY DEPARTMENT, FACULTY OF CYBERNETICS,
MOSCOW TECHNOLOGICAL UNIVERSITY, MOSCOW

Abstract: *Virtual private network (VPN - VirtualPrivateNetwork) is created on the basis of the public Internet. And if the communication through the Internet has its drawbacks, the main one being that it is subject to potential breaches of protection and confidentiality, then VPN can guarantee that the traffic sent via the Internet is as secure as the transmission within the local network. At the same time, virtual networks provide significant cost savings compared to the content of their own global network. In this article, we analyze both the various methods for organizing a secure network, and the attacks used by attackers.*
Keywords*: Internet, threats, security.*

УДК 004.9

Современное развитие информационных технологий и, в частности, сети Internet, приводит к необходимости защиты информации, передаваемой в рамках распределенной корпоративной сети, использующей сети открытого доступа. При использовании своих собственных физических каналов доступа эта проблема так остро не стоит, так как в эту сеть не имеет доступа никто из посторонних. Однако стоимость таких каналов высока, поэтому не каждая компания позволит себе использовать их. В связи с этим Internet является наиболее доступным. Internet является незащищенной сетью, поэтому приходиться изобретать способы защиты конфиденциальных данных, передаваемых по незащищенной сети.

VPN - это технология, которая объединяет доверенные сети, узлы и пользователей через открытые сети, которым нет доверия. Технология, которая получает все большее распространение среди не только технических специалистов, но и среди рядовых пользователей, которым также требуется защищать свою информацию (например, пользователи Internet-банков или Internet-порталов).[1]

Специалисты в области технологии VPN используют сугубо технические понятия, такие как «используемый алгоритм криптографического преобразования», «туннелирование», «сервер сертификатов» и т.д. Но для конечных пользователей эта терминология ничего не скажет. Скорее их интересует несколько иная интерпретация вопросов - сколько лет можно не беспокоиться за сохранность своей информации и насколько медленнее будет работать сеть, защищенная с помощью VPN-устройства.

В зависимости от цели использования VPN, можно выделить следующие основные угрозы.

Man-in-the-middle (MITM) — «шпион посредине». Это атака на VPN, при которой злоумышленник вклинивается в канал шифрования между отправителем и получателем, создавая два отдельных шифрованных соединения. Обычно такая атака осуществляется в момент обмена ключами шифрования: злоумышленник перехватывает их и навязывает обеим общающимся сторонам свои ключи. При использовании SSL и сертификатов ему достаточно встроиться в цепочку доверия браузера.[3]

Man-in-the-browser (MITB) — «шпион в браузере». Это вариант атаки MITM, при котором перехват шифрованного соединения происходит в браузере отправителя или получателя. Строго говоря, информация перехватывается еще до шифрования с помощью вредоносных компонент, написанных на

JavaScript, NET или других языках, с использованием которых создаются модули расширения для браузеров. Эта атака характерна в основном для SSL VPN, организуемой посредством браузера, и браузерного модуля Tor.[2]

IdentityTheft — кража личности. В организациях, где VPN используется для защиты доступа к корпоративным ресурсам, у злоумышленников появляется возможность проникновения внутрь сети с помощью аутентификационной информации легальных пользователей. Ее можно получить путем перехвата паролей в результате атаки MITM или MITB. Подключившись к корпоративному шлюзу и создав защищенное соединение, злоумышленник может действовать от имени сотрудника компании и получить расширенные полномочия и доступ к внутренней структуре сети, которая не всегда сегментирована и дополнительно укреплена.

Проанализировав протоколы организации VPN можем прийти к выводу что самый безопасный протокол VPN — это OpenVPN[4], соответственно провайдерам нужно расширять сферу его применения.

PPTP — очень небезопасный протокол. Его взломали спецслужбы и даже Microsoft отказались от его поддержки, так что на сегодня следует его избегать. И хотя вас может привлечь удобство настройки или кросс-платформенная совместимость, помните, что практически те же преимущества предлагает L2TP/IPSec, однако у него еще и более высокий уровень защиты.

Если речь не идет о действительно важных данных, L2TP/IPSec — это то, что вам нужно, хотя этот протокол и ослаблен и скомпрометирован. Однако, если вы ищете быстрый и удобный в настройке VPN, который не требует установки дополнительного ПО, он прекрасно подойдет, особенно с учетом того, что VPN для мобильных устройств поддерживается не лучшим образом.

Несмотря на то, что вам нужно будет устанавливать сторонние приложения, OpenVPN — лучший протокол в любом случае. Он работает быстро, надежно, и, хотя его настройка может занять немало времени, она того стоит.

IKEv2 тоже работает быстро и безопасно, и если он используется в сочетании с другими средствами обеспечения безопасности, он может прекрасно подойти для пользователей мобильных устройств, в частности благодаря автоматическому возобновлению подключения. Кроме того, это один из немногих протоколов с поддержкой устройств Blackberry.

SSTP предлагает практически те же преимущества, что и OpenVPN, однако он работает только на платформе Windows. С другой стороны, он куда лучше совместим с этой системой, чем другие протоколы. Однако, поддержка провайдеров ограничена, во-первых, из-за поддержки систем, во-вторых, из-за того, что компания Microsoft известна давним сотрудничеством с Агентством национальной безопасности, так что мы бы не советовали доверять этому протоколу.

Если подытожить - при возможности используйте OpenVPN, для мобильных устройств подойдет IKEv2. L2TP — этого протокола достаточно для быстрых решений, однако с учетом расширения поддержки OpenVPN для разных устройств.

Сервисы-анонимайзеры скрывают данные о компьютере или пользователе в локальной сети от удаленного сервера. Это очень удобно, если сайты для развлечения или общения заблокированы от сотрудников компании, где они работают, по инициативе руководства. Или же пользователь просто не хочет, чтобы его «вычислили» и заметает таким образом следы, предотвращая передачу данных о себе компетентным органам.

Список литературы / References

1. «Виртуальные частные сети VPN» Александр Росляков Телеком, 2009. 320 с.
2. Столлингс В. «Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards» - М.: «Вильямс», 2012. С. 432. ISBN 0-13-016093-8.
3. [Электронный ресурс]. Режим доступа: http://www.cisco.com/web/RU/products/sw/netmgtsw/ps2327/index.html/ (дата обращения: 21.05.2018).
4. [Электронный ресурс]. Режим доступа: https://losst.ru/prostaya-nastrojka-openvpn-linux/ (дата обращения: 21.05.2018).