УДК 004.9

Авласевич Д.В., студент,
4 курс, Институт финансов, экономики и управления,
Тольяттинский государственный университет,
Тольятти (Россия)
Дмитриев Н.А., студент,
4 курс, Институт финансов, экономики и управления,
Тольяттинский Государственный Университет,
Тольятти (Россия)
Кириллов А.А., студент,
4 курс, Институт финансов, экономики и управления,
Тольяттинский Государственный Университет,
Тольятти (Россия)
Бачинский А.Г. магистрант
1 курс, Институт машиностроения,
Тольяттинский государственный университет,
Тольятти (Россия)
Avlasevich DV, student,
4th year, Institute of Finance, Economics and Management,
Tolyatti State University,
Tolyatti (Russia)
Dmitriev NA, student,
4th year, Institute of Finance, Economics and Management,
Tolyatti State University,
Tolyatti (Russia)
Kirillov AA, student,
4th year, Institute of Finance, Economics and Management,
Tolyatti State University,
Tolyatti (Russia)
Bachinsky A.G. undergraduate

1 year, Institute of Mechanical Engineering,
Togliatti State University,
Tolyatti (Russia)

ИССЛЕДОВАНИЕ ПРИНЦИПОВ РАБОТЫ VPN, РАЗРАБОТКА ПОЛИТИКИ БЕЗОПАСНОСТИ VPN. АНОНИМАЙЗЕРЫ И ИХ ПРИМЕНЕНИЕ.

Аннотация: Виртуальная частная сеть (VPN – VirtualPrivateNetwork) формируется на базе общедоступной сети Интернет. Коммуникация через сеть-интернет имеет свои минусы, а самый главный недостаток заключается в том, что она постоянно подвергается всевозможными нарушениям защиты и конфиденциальных данных, в таком случае, VPN может гарантировать, что трафик, который направляется через Интернет находится под защитой таким же образом, как и передача внутри локальной сети. В это же время виртуальные сети гарантируют значительную экономию затрат в сравнении с содержанием своей сети глобального масштаба. В данной статье проводится анализ различных методов организаций защищенной сети, а также атаки, которые используют злоумышленники.

Ключевые слова: VPN; интернет; угрозы; безопасность; интернет-защита.

Research of principles of vpn operation, development of vpn security policy. Anonymisers and thier application.

Annotation: A virtual private network (VPN – VirtualPrivateNetwork) is formed on the basis of the public internet. Communication over the network has its drawbacks, and this case, it is constantly exposed to all kinds of security breaches and confidential data, which may be associated with a VPN inside the local

networks guarantee significant cost savings. This article analyzes the various methods of organizing a secure network.

Keywords: VPN; Internet; threats; security; internet protection.

Создание и становление нынешних технологий получения данных, в том числе, сети Internet, заставляет нас прибегнуть к защите собственных данных, которые в свою очередность, поступают в рамках распределенной коллективной сети, которая применяет сети прямого использования. Если использовать свои собственные физические каналы доступа, то эта проблема не стоит так остро, поскольку в эту сеть никто из посторонних не имеет доступа. Но цена за такие каналы высокая и не каждая компания сможет себе позволить такую роскошь. Исходя из этого сеть Internet является наиболее доступной. Internet – это незащищенная сеть, поэтому приходится создавать способы защиты конфиденциальности, которые передаются по сети без защиты. [1]

VPN считается технологией, соединяющая проверенные сети, участки и пользователей посредством открытия сети, у которых отсутствует доверие. Методика, получающая большую огласку среди промышленных экспертов, а также среди простых юзеров, которые также имеют необходимость в охране своих сведений (например, юзеры Internet-банков либо Internet-порталов).

Эксперты, которые находятся в сфере научно-технических процессов VPN используют только промышленные определения, разберем к примеру «используемый метод шифровального преобразования», «туннелирование», «сервер сертификатов» и т.д. Но для обычных пользователей подобные определения мало что значат. Больше всего им интересна несколько иная интерпретация задач, к примеру, как долго можно не беспокоиться за безопасность своих данных и как долго способна функционировать сеть, защищенная VPN-устройством.

Все зависит с какой целью использовать VPN, исходя из этого, можно выделить следующие основные опасения:

- Man-in-the-middle (MITM) — «человек посредине». Это явление - своего рода ddos на VPN, с помощью которого преступник способен пробраться в канал шифра в цепочке отправителя или получателя, генерируя при этом единичные шифрованные объединения. Чаще всего атака подобного вида совершается при обмене ключами кодирования: взломщик перехватывает данные источники и заставляет использовать двух собеседников собственные ключи. С поддержкой SSL и сертификатов ему нужно только пробраться в цепочку доверия браузера. [2]
- Man-in-the-browser (MITB) — «человек в браузере». Такого рода способ атаки MITM, используется в случае если информация перехватывается с помощью шифров в браузере от отправителя либо получателя. Проще говоря, злоумышленник приобретает информацию еще до начала кодирования при поддержке вредоносных компонентов, прописанных в JavaScript, NET либо иных языках программирования, благодаря которым формируются модули расширений для браузеров. Атака такого плана свойственна чаще всего для SSL VPN, которая создана с помощью браузера, и браузерного модуля Tor.
- IdentityTheft — кража личности. В фирмах, где VPN применяется в случае охраны доступа к коллективным ресурсам, злоумышленник приобретает возможность пробраться внутрь сети при поддержке аутентификационных данных, приобретенных от честных юзеров. Такую информацию возможно приобрести с помощью перехвата паролей в следствии атаки MITM либо MITB. При подсоединении к коллективному шлюзу и формировании secure connection, правонарушитель может осуществлять действия от имени работника фирмы т.е. приобрести расширенные полномочия, и, кроме того,

полный допуск к внутренней структуре сети, которая может быть не всегда дополнительно укреплена и разделена.

Проведя анализ протоколов организации VPN можно сделать вывод о том, что самый безопасный протокол VPN — это OpenVPN, в соответствии с этим провайдерам нужно увеличивать сферу его использования.

PPTP — достаточно опасный протокол. Его взломали спецслужбы и даже Microsoft отказались его поддерживать, поэтому на сегодняшний момент следует его не использовать. Хоть вас и может завлечь удобство настроек или кросс-платформенная совместимость, запомните, что почти такие же преимущества предоставляет L2TP/IPSec, но при этом он имеет еще более высокий и эффективный уровень защиты. [3]

В случае если разговор не идет о действительно значимых данных, L2TP/IPSec — это то, что подойдет для вас, несмотря на то что данный протокол и ослаблен, и скомпрометирован. Но, если вы ищете быстрый и простой в настройке VPN, которому не требуется установка дополнительного ПО, этот вариант отлично подойдет, тем более, учитывая, что VPN для мобильных девайсов имеет не лучшую поддержку. [3]

Учитывая то, что вам придется устанавливать сторонние приложения, OpenVPN является лучшим протоколом в любом случае. Он надежно и быстро работает, хоть и его настройка способна занять огромное количество времени, но не напрасно.

IKEv2 так же работает безопасно и достаточно быстро, при использовании его в сочетании с другими средствами обеспечения безопасности, он способен отлично использоваться на мобильных устройствах, в частности из-за автоматического возобновления подключения. Помимо этого, является так же одним из немногих протоколов с поддержкой устройств Blackberry. [3]

SSTP предоставляет почти такие же преимущества, как и OpenVPN, но все же он совместим только при работе на платформе Windows. В то же время, он намного лучше сочетается с этой системой, чем другие протоколы. Но стоит помнить, что поддержка провайдеров ограничена, прежде всего, из-за поддержки систем, а также, из-за того, что компания Microsoft давно сотрудничает с Агентством национальной безопасности, поэтому мы бы не стали рекомендовать данный протокол. [3]

Подводя итоги, можно сказать следующее: по возможности используйте OpenVPN, а для мобильных версий подойдет IKEv2. L2TP, его вполне достаточно для быстрых решений, но стоит помнить, что расширения поддержки OpenVPN учитываются для разных устройств.

Сервисы-анонимайзеры скрывают данные пользователя или компьютера в локальной сети от удаленного сервера. Это достаточно удобно, в случае если веб-сайты для общения или развлечения могут заблокированы от сотрудников компании, в месте их работы, исходя из инициативы руководства. А также если пользователь не хочет, чтобы его «вычислили» и прячет таким образом следы, которые предотвращают передачу сведений о себе каким-либо осведомленным органам. [4]

Список используемой литературы:

1. С. А. Петренко, В. А. Курбатов Политики безопасности компании при работе в интернет.
2. Cisco Systems, Решения компании Cisco Systems по обеспечению безопасности корпоративных сетей (издание II)
3. С. И. Макаренко, Информационная безопасность: учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009г.
4. В. В. Платонов, Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: учеб.

пособие для студ. высш. учеб. заведений/ В.В. Платонов. — М.: Издательский центр «Академия», 2006г.