РОЛЬ VPN-ТЕХНОЛОГИЙ В ПОВЫШЕНИИ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ ПРЕДПРИЯТИЯ

Ковалько О.А., Кулешов И.С.

гр. 367041

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

Научный руководитель: Хацкевич О.А. – кандидат технических наук, доцент кафедры ИКТ

Аннотация. В статье рассматривается вопрос использования виртуальных частных сетей (VPN) в корпоративных структурах компаний. Анализируются наиболее значимые преимущества внедрения VPN для обеспечения целостности и конфиденциальности информации. Раскрывается процесс подключения к VPN. Исследуются тенденции развития технологий реализации VPN-каналов.

Ключевые слова: VPN, GRE, защита данных, виртуальная частная сеть, сетевой трафик.

Введение. В современном мире информация является одной из наиболее ценных составляющих, и, как любую другую ценность, человек стремится защитить её от несанкционированного доступа и вмешательства. С развитием компьютерных технологий вопрос сохранения и защиты информации приобретает всё большее значение, и проблема информационной безопасности становится чрезвычайно актуальной.

Среди методов, направленных на обеспечение доступности информации, исследователи отмечают использование сочетания различных подходов к контролю, дублированию и резервированию данных. Для обеспечения целостности и конфиденциальности информации в сетях применяются методы построения виртуальных каналов, основанные на использовании криптографических технологий.

В этом контексте, VPN (виртуальная частная сеть или туннелирование) представляет собой технологию, позволяющую установить постоянное защищенное соединение между компьютером и сервером, основанное на передаче данных в виде зашифрованных пакетов GRE. Для шифрования используется современный алгоритм MPPE с 128-битным состоянием, который обеспечивает высокий уровень безопасности.

Основная часть. Актуальность исследования потенциала внедрения виртуальных частных сетей (VPN) в корпоративные структуры компаний обусловлена несколькими ключевыми аспектами:

– VPN-сети обеспечивают высокий уровень безопасности передаваемой информации посредством шифрования, что особенно актуально для защиты конфиденциальных корпоративных данных;

– использование VPN позволяет существенно снизить риски утечки данных, предотвращая несанкционированный доступ к внутренней информации компании;

– с помощью VPN сотрудники получают возможность подключаться к корпоративной сети независимо от своего местоположения, что крайне важно в условиях растущей популярности гибридных и удаленных режимов работы;

– удаленные работники благодаря VPN имеют беспрепятственный доступ ко всем необходимым ресурсам компании, включая внутренние базы данных и приложения;

– при наличии у организации нескольких офисов, VPN обеспечивает безопасное и надежное соединение между ними;

– VPN способствует управлению трафиком и распределению нагрузки между различными узлами сети;

– внедрение VPN-сетей позволяет создать защищённую сеть без необходимости прокладывания физических линий связи, что существенно снижает затраты на развитие инфраструктуры;

– VPN предоставляет возможность централизованного управления доступом и правами пользователей, что упрощает процессы администрирования безопасности и позволяет оперативно реагировать на потенциальные угрозы;

– использование VPN позволяет скрыть реальный IP-адрес пользователей, затрудняя проведение атак на корпоративную сеть и повышая общую безопасность компании.

Процесс подключения к виртуальной частной сети VPN выглядит следующим образом: на компьютере формируется пакет GRE, который затем шифруется с использованием одного из доступных алгоритмов шифрования. После этого зашифрованный пакет отправляется на VPN-сервер, где происходит его расшифровка. Сервер обрабатывает запрос и пересылает его к нужному ресурсу для получения или передачи информации. Ресурс, получив запрос от VPN-сервера, обрабатывает его и отправляет обратно необходимую информацию. Затем сервер VPN вновь формирует зашифрованный пакет GRE и передает его на компьютер пользователя, где происходит расшифровка и отображение запрашиваемого результата.

Такой процесс обеспечивает постоянный защищенный поток зашифрованной информации от компьютера к ресурсам Интернета, что гарантирует безопасность и конфиденциальность передаваемых данных.

Хотя использование данной технологии приводит к некоторой задержке в передаче данных из-за многоэтапного процесса шифрования и расшифровки, это замедление обычно несущественно и не влияет на комфортную работу пользователя [1].

Технология VPN (Virtual Private Network – виртуальная частная сеть) представляет собой один из эффективных способов защиты сетей и данных, которые передаются через них.

Основная концепция технологии VPN заключается в следующем:

– на всех устройствах (в частности, ПК), имеющих доступ к сети Интернет, устанавливается программное обеспечение, реализующее функционал VPN, например, VPN-агент. Это гарантирует, что ни одно устройство конечного пользователя не останется незащищенным;

– VPN-агенты автоматически шифруют всю исходящую информацию и, соответственно, расшифровывают входящие данные. Они также обеспечивают проверку целостности данных, используя электронную цифровую подпись (ЭЦП) или хэш (криптографическая контрольная сумма, рассчитанная на основе ключа шифрования);

– поскольку данные, передаваемые по Интернету, представляют собой совокупность пакетов, сформированных протоколом IP, VPN-агенты работают именно с такими пакетами;

– перед отправкой IP-пакета VPN-агент выполняет следующие действия:

1) по IP-адресу получателя из имеющихся алгоритмов шифрования и ЭЦП выбирается соответствующий алгоритм для защиты пакета, и формируются ключи. Если информация о получателе отсутствует в настройках, передача данных не осуществляется;

2) добавляется ЭЦП отправителя или соответствующий хэш в пакет;

3) происходит полное шифрование пакета, включая его заголовок;

4) выполняется процесс инкапсуляции, при котором создается новый заголовок, указывающий не на конечного получателя, а на его VPN-агент. Эта функция обеспечивает дополнительную защиту, представляя обмен данными между двумя сетями как взаимодействие между двумя компьютерами, оснащенными VPN-агентами, и скрывает внутренние IP-адреса от злоумышленников.

– при получении IP-пакета выполняются следующие обратные операции:

1) если заголовок содержит информацию о VPN-агенте отправителя, который отсутствует в списке разрешенных адресов, пакет просто игнорируется. Аналогичная процедура применяется к пакетам с поврежденными заголовками.

2) в соответствии с настройками выбираются соответствующие алгоритмы шифрования и ЭЦП, а также необходимые ключи;

3) пакет расшифровывается, и проверяется его целостность. В случае неверной ЭЦП, пакет отклоняется;

4) затем пакет в исходном формате передается конечному получателю по внутренней сети.

Все данные операции выполняются в автоматическом режиме. Основная сложность технологии VPN заключается в настройке VPN-агентов, однако опытный пользователь вполне способен справиться с этой задачей.

VPN-агент устанавливается непосредственно на защищенном компьютере, что особенно эффективно для мобильных пользователей, подключающихся к сети Интернет. В этом случае обеспечивается безопасность обмена данными только для устройства, на котором установлен VPN-агент.

Существует возможность объединения функций VPN-агента с маршрутизатором, в этом случае он приобретает название криптографического маршрутизатора IP-пакетов [2].

Основной задачей VPN-агента является создание безопасного канала между защищаемыми сетями, часто называемого «туннелем». Кроме этого, все пакеты данных проходят через процесс «фильтрации» в соответствии с установленными настройками агента. Таким образом, работа VPN-агента сводится к выполнению двух ключевых функций: созданию туннелей и фильтрации передаваемых пакетов.

Набор правил, регулирующих создание туннелей, называется «политикой безопасности» и задается в настройках VPN-агента. После проверки пакетов они либо направляются в определенные туннели, либо отбрасываются на основании следующих критериев: IP-адреса источника (для исходящих пакетов это адрес конкретного компьютера, входящего в защищаемую сеть); IP-адреса назначения; протоколы более высокого уровня, к которым относятся данные пакеты (например, TCP или UDP); номера портов, через которые осуществляется отправка информации (например, 1080).

Таким образом, выделенные механизмы позволяют VPN-агенту эффективно обеспечивать безопасность и контроль передачи данных в корпоративной или частной сети.

В последние годы наблюдается значительное развитие технологий, связанных с внедрением виртуальных частных сетей (VPN). Это обусловлено не только растущей потребностью в защите данных в условиях повсеместной цифровизации, но и стремлением пользователей к более свободному и безопасному доступу к информации.

Одной из основных тенденций является совершенствование криптографических методов, применяемых для шифрования сетевого трафика. Традиционные протоколы, такие как PPTP и L2TP, постепенно уступают место более современным и надежным решениям, таким как OpenVPN и WireGuard. Эти новые протоколы обеспечивают более высокий уровень защиты данных, применяя улучшенные алгоритмы шифрования и аутентификации, что значительно усложняет перехват и расшифровку данных для потенциальных злоумышленников.

Еще одной важной тенденцией является интеграция VPN-технологий с облачными сервисами. Современные VPN-решения позволяют не только создавать защищенные каналы на локальных серверах, но и использовать возможности облачных инфраструктур. Это обеспечивает бизнесу новые возможности в плане гибкости, масштабируемости и доступности VPN-сетей посредством децентрализованных архитектур.

Также, в связи с глобализацией и увеличением количества удаленно работающих сотрудников, наблюдается повышенный интерес к мобильным VPN-решениям. Разработчики активно создают приложения, позволяющие пользователям подключаться к корпоративным сетям из любой точки мира через мобильные устройства. Это требует тщательной оптимизации, как в плане производительности, так и обеспечения безопасности, что способствует разработке новых протоколов и алгоритмов,

адаптированных для мобильных платформ.

Особое внимание уделяется также вопросу конфиденциальности данных. В условиях усиления требований, таких как Общий регламент по защите данных (GDPR) в Европе, компании все чаще внедряют VPN не только для защиты собственной информации, но и для обеспечения конфиденциальности данных клиентов. Прозрачность работы VPN-провайдеров и возможность аудита их политики безопасности становятся ключевыми факторами в этом процессе.

Нельзя не отметить также растущую роль искусственного интеллекта и машинного обучения в развитии VPN-технологий. Эти инструменты все чаще используются для мониторинга сетевого трафика, автоматизации выявления нежелательных действий и оптимизации использования ресурсов. Внедрение ИИ в VPN-системы позволяет создавать более адаптивные и интеллектуальные решения, которые способны прогнозировать и предотвращать потенциальные угрозы [3].

Таким образом, развитие технологий VPN-каналов характеризуется комплексным подходом к вопросам безопасности, приватности и доступности. Эти изменения, происходящие на фоне быстрого развития информационных технологий, формируют новые стандарты и определяют дальнейшее направление развития виртуальных частных сетей.

Заключение. Организация защищенного канала передачи данных является одной из ключевых задач, поскольку информация представляет собой ценный ресурс для любой компании. Корпоративные сети должны обеспечивать высокий уровень безопасности и надежности, что нередко требует использования сложных технологий, таких как VPN. Виртуальные частные сети позволяют создавать зашифрованные каналы для передачи данных, обеспечивая защиту информации от несанкционированного доступа.

В ходе исследования и анализа современных технологий создания сетей VPN было выявлено, что за последние годы технологии виртуальных частных сетей (VPN) значительно эволюционировали. Этот прогресс обусловлен растущей потребностью пользователей в обеспечении безопасности данных и свободном доступе к информации.

Таким образом, учитывая современные тенденции в реализации VPN-технологий, можно заключить, что их грамотное и эффективное применение представляет собой важнейший этап на пути к созданию безопасной и высокодоступной вычислительной среды, способной удовлетворить текущие требования и вызовы времени.

Список использованных источников:

1. *Прокопов, В. VPN. Теория и реальность / В. Прокопов [Электронный ресурс]. – Режим доступа: https://www.solidex.by/wp-content/uploads/2017/07/vpn_-_teoriya_i_realnost.pdf. – Дата доступа: 20.09.2024.*

2. *Олифер, В.Г. Компьютерные сети: Принципы протоколы технологии / В.Г. Олифер, Н.А. Олифер. – 3-е издание. – СПб: Пирер, 2006. – 367 с.*

3. *The Future of VPN Technology: Trends and Innovations to Watch in 2024 [Electronic resource]. – Mode of access: https://neg.by/novosti/otkrytj/risk-slit-dannye-est-li-smysl-ispolzovat-opensorsnye-resheniya-pri-zashchite-kanalov-svyazi/. – Date of access: 20.09.2024.*

THE ROLE OF VPN TECHNOLOGIES IN INCREASING THE SECURITY OF THE ENTERPRISE'S CORPORATE NETWORK

Kovalko O.A, Kuleshov I.S.

gr.367041

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

Khatskevich O.A. – Candidate of Technical Sciences, Associate Professor of the Department of ICT

Annotation. The article examines the issue of using virtual private networks (VPN) in corporate structures of companies. The most significant advantages of implementing VPN to ensure the integrity and confidentiality of information are analyzed. The process of connecting to VPN is disclosed. Trends in the development of technologies for implementing VPN channels are studied.

Keywords: VPN, GRE, data protection, virtual private network, network traffic.