Практическое занятие № 15. Основы и концепции VPN. Симметричное и ассиметричное шифрование.

Цель работы: изучение принципов работы протоколов и технологий виртуальных частных сетей.

VPN (Virtual Private Network, англ. «виртуальная частная сеть») позволяет защититься от вмешательства третьих лиц в процесс обмена информацией по сети. Изначально технология разрабатывалась для решения задач в корпоративной среде, но позже её преимущества оценили и обычные пользователи.

VPN – это виртуальная частная сеть, которая объединяет несколько устройств, туннелируя их трафик поверх другого сетевого соединения. Если говорить простыми словами, то VPN – технология, позволяющая анонимизировать и обезопасить свою деятельность в Интернете или какой-либо другой сети [3, 12, 23].

Для более глубокого понимания принципа использования технологии, стоит подробнее разобрать составляющие термина виртуальная частная сеть.

«Виртуальная» означает, что VPN создаётся программным способом в виде отдельной прослойки поверх другой сети (например, через Интернет). Для передачи данных используется туннелирование – трафик инкапсулируется в отдельный туннель, который проходит по более низкоуровневому каналу связи. Информация в VPN-туннеле надёжно зашифрована для исключения возможности перехвата данных извне.

«Частная», VPN – внутренняя сеть, в которой находятся только доверенные устройства. Хотя подключение может осуществляться и через внешнюю или общедоступную сеть, оно обособлено от основного канала связи сквозным шифрованием.

«Сеть», соединение происходит между двумя устройствами – клиентом и VPN-сервером, образующими единую сеть.

VPN-подключение создаётся за счёт использования как минимум двух устройств.: сервера и клиента.

Под сервером понимается устройство, на котором расположено основное ПО, прослушивающее определённые порты в ожидании установки соединения с клиентом. Например, VPN-сервис или рабочая сеть.

Под клиентом принято понимать устройство пользователя, с которого совершается подключение к удалённому серверу.

Между сервером и клиентом постоянно передается зашифрованная информация через виртуальный туннель, а все процессы криптографической обработки данных (шифрование и дешифрование) выполняются на самих устройствах. Поэтому в условиях туннелирования, третья сторона не сможет перехватить данные пользователя.

Когда пользователь подключается к VPN-туннелю, все сетевое взаимодействие происходит внутри него, что позволяет создать безопасный канал для обмена данными между удаленными узлами.

Внутри VPN-туннеля данные упаковываются в специальные пакеты и передаются по защищенному каналу, как если бы они перемещались через физическое соединение, например, с помощью Ethernet. Это делает невозможным просмотр и изменение данных при передаче между устройствами. То есть в процессе работы пакеты шифруются, чтобы исключить нелегитимный доступ со стороны злоумышленников.

Есть несколько протоколов туннелирования (например, GRE, ICMP или IPinIP), которые можно использовать для настройки VPN-туннелей. Выбор конкретного зависит от цели, ваших требований к стойкости шифрования и вычислительной сложности.

Кроме того, VPN-туннель может работать в нескольких режимах: «передача данных между двумя сетями» и «защита удаленного доступа к внутренним ресурсам сети».

Передача данных между двумя сетями. Первый режим используют для соединения локальных сетей между собой через интернет. Такой подход

может быть полезен для организации связности между филиалами компании. При этом каждый конец туннеля должен быть настроен для подключения к определенной сети.

Защита удаленного доступа к внутренним ресурсам сети подходит для создания безопасного и шифрованного канала между отдельным устройством (как правило, компьютером или телефоном) и внутренней сетью, к которой обычно нет прямого доступа. Такой подход может быть полезен для удаленной работы, когда сотрудникам нужен доступ к внутренним ресурсам компании, или для подключения к домашней сети из разных мест. В этом режиме удаленный клиент должен быть настроен для подключения к сети через VPN-туннель.

Существует два основных вида туннелирования VPN, каждый из которых выполняет определенные функции в защите данных и настройке соединения: раздельное и полное.

Раздельное туннелирование – метод, при котором VPN-туннель создается только для определенных сетевых соединений, в то время как другие остаются открытыми. Позволяет экономить на пропускной способности сети путем исключения передачи трафика. Однако это менее безопасный метод: информация, которая передается через обычное подключение к интернету, может быть украдена.

При полном туннелировании весь сетевой трафик проходит через VPN-туннель. Этот метод обеспечивает большую степень безопасности, поскольку вся передаваемая информация защищена от внешних угроз. Однако может замедлить скорость соединения и использовать большую пропускную способность сети, чем раздельное туннелирование.

Выбор между раздельным и полным туннелированием зависит от нескольких факторов, включая уровень безопасности, необходимость регулирования пропускной способности сети и ее общую производительность. Если безопасность данных в приоритете, предпочтительнее использовать полное туннелирование. Если же

необходимо сохранить пропускную способность сети и обеспечить безопасность некоторых соединений, лучшим выбором станет раздельное туннелирование.

Когда речь заходит о шифровании в VPN, важно различать алгоритмы шифрования и типы шифров. Фактически, первые относятся к способам передачи данных внутри VPN-туннеля. Сам шифр может быть одним из алгоритмов шифрования, но не наоборот. Давайте подробнее рассмотрим каждую из сущностей.

Одно из главных условий VPN-технологии – качественное и криптостойкое шифрование данных для защиты пользовательской информации во время передачи через интернет. Обычно шифрование разделяют на два класса: симметричное и асимметричное шифрование.

Симметричное шифрование использует один и тот же ключ для шифрования и дешифрования информации. В случае VPN-технологий, клиент и сервер обмениваются одним ключом шифрования, так что все передаваемые данные могут быть зашифрованы и дешифрованы с помощью него. Симметричное шифрование обеспечивает быстрое и эффективное шифрование данных, что делает его наиболее распространенным методом.

Однако симметричное шифрование является менее безопасным, чем асимметричное, поскольку использует один и тот же ключ. Если злоумышленник получит к нему доступ, все данные могут быть легко прочитаны.

Асимметричное шифрование, напротив, использует два ключа – открытый и закрытый. Первый может распространяться свободно и используется для шифрования, в то время как второй – для дешифрования и является конфиденциальным.

Асимметричное шифрование обеспечивает более высокий уровень безопасности, чем симметричное. Однако является менее эффективным и зачастую требует больше ресурсов для шифрования и дешифрования данных.

Наиболее известный алгоритм ассиметричного шифрования – алгоритм Диффи-Хеллмана (DH). Алгоритм Диффи-Хеллмана (DH) — это криптографический протокол, позволяющий двум сторонам безопасно обмениваться ключами по незащищённому каналу связи. Он используется для установления общего секретного ключа, который затем применяется в симметричном шифровании (например, AES).

Алгоритм выполняется в несколько этапов. На первом происходит выбор общих парамтеров. Обе стороны (сервер и клиент) договариваются о двух числах: p – большое простое число и g – сгенерированное случайное число. После этого происходит генерация секретных (приватных или закрытых) ключей: a и b, а переменная p передается между сервером и клиентом.

После этого происходит вычисление и обмен открытыми ключами. Сервер генерирует открытый ключ $A = g^a \bmod p$, а клиент $B = g^b \bmod p$. После чего происходит обмен открытыми ключами шифрования.

На основе полученных открытых ключей, сервер и клиент генерируют общий секретный ключ $K = B^a \bmod p = A^b \bmod p$.

Злоумышленник, перехвативший A и B, не сможет вычислить K, так как для этого нужно решить задачу дискретного логарифмирования (нахождение a или b из $g^x \bmod p$), которая считается вычислительно сложной для больших чисел.

Выбор алгоритма зависит от нужд компании и уровня безопасности, который она хочет обеспечить для своих пользователей. Часто VPN-сервисы комбинируют оба метода. Внутри каждого класса шифрования существует множество алгоритмов и методов, рассмотрим наиболее широко известные реализации.

AES (Advanced Encryption Standard). Это один из наиболее распространенных и надежных алгоритмов симметричного шифрования. Использует один и тот же ключ для шифрования и дешифрования данных и шифрует данные блоками по 128 бит. AES имеет также другие варианты

длины ключа – AES-128, AES-192 и AES-256. Последний считается наиболее надежным и часто используется в VPN-сервисах.

ChaCha20 и Poly1305. ChaCha20 — это относительно новый алгоритм поточного шифрования, который был разработан для обеспечения большей производительности и безопасности туннелирования. В сочетании с MAC-функцией Poly1305, этот метод обеспечивает высокоскоростной и надежный способ шифрования данных. ChaCha20 и Poly1305 используют ключ длиной 256 бит [23-24].

Blowfish и Twofish. Blowfish является симметричным блочным шифром, который был разработан в 1993 году. А Twofish – его наследником, ориентированным на безопасность и производительность. Оба метода используют шифрование с переменной длиной ключа, блоки по 64 бита и различные режимы их шифрования.

3DES (Triple Data Encryption Standard). Этот алгоритм симметричного шифрования, который использует три ключа. Он не считается безопасным и уже устарел, но все еще используется в некоторых VPN-сервисах[25].

RSA (Rivest-Shamir-Adleman) представляет собой алгоритм асимметричного шифрования, который использует два ключа – открытый и закрытый. Он используется для создания зашифрованных туннелей безопасного обмена данными. RSA является более безопасным, но медленным в сравнении с симметричными алгоритмами. Это особенно заметно при использовании ключей большей длины [24-25].

MPPE (Microsoft Point-to-Point Encryption) – алгоритм симметричного шифрования, который был разработан для работы в соединениях PPTP (Point-to-Point Tunneling Protocol). Он использует ключ длиной 40 или 128 бит и шифрует данные.

Большинство современных VPN-сервисов сочетают несколько методов шифрования, чтобы обеспечить максимальную защиту данных и сохранить высокую производительность.

Сценарии использования VPN. Технология VPN популярна среди пользователей, поскольку защищает проходящий через сеть трафик от злоумышленников и делает невозможным расшифровку сообщений. Подобные возможности доступны благодаря маршрутизации трафика через VPN-сервер. Это значит, что отправленные пользователем запросы сначала передаются через туннель от клиента к серверу, а только потом отправляются в Интернет к необходимому веб-ресурсу. Таким образом, возможна пересылка части трафика, защита которой имеет значение через виртуальный туннель, а остального трафика – в открытом виде. Такой селективный отбор трафика для VPN туннеля может быть использован для подключения к сервисам, обрабатывающим конфиденциальную информацию, например к банковскому приложению или личному кабинету пользователя.

В корпоративной сфере VPN используется для объединения или, наоборот, обособления сетей различных отделов. Эта технология позволяет нивелировать локальные ограничения между подключёнными устройствами.

Кроме того, VPN нужен для объединения корпоративных сетей через Интернет между отдалёнными объектами компании: офисами, региональными филиалами, зарубежными представительствами. Это гораздо выгоднее, чем использование физического локального подключения – кабельной или беспроводной связи.

Соединение двух сетей через VPN-туннель. Тип подключения «точка-точка». VPN также даёт сотрудникам возможность подключаться к рабочей сети, находясь вне офиса. Например, дома или в общественном месте. После установки соединения пользователь получает доступ к корпоративным ресурсам и оборудованию. Таким образом, доступно получение удалённого доступа к корпоративной сети (Intranet) с помощью VPN.

Но технология VPN не лишена недостатков, повышение задержки передачи сетевых пакетов, снижение пропускной способности сети. Все это происходит из-за большого количества вычислительных операций при шифровании пользовательского трафика, а также из-за необходимости

инкапсуляции пакета в новую структуру данных, то есть добавление к сообщению избыточной информации. Указанные недостатки наиболее заметны при отсутствии аппаратного ускорения шифрования VPN, когда нагрузка перекладывается на вычислительный процессор оконечного устройства, что нередко снижает скорость передачи данных до 30% от исходной.

Архитектура VPN-сетей строится на базе VPN-протоколов, которые применяются для реализации туннелирования между устройствами. Все они различаются между собой характеристиками, принципом работы и доступностью на разных операционных системах.

OpenVPN. Один из самых безопасных и популярных протоколов, шифрование которого реализуется за счёт использования библиотеки OpenSSL. Программное обеспечение доступно для большинства популярных операционных систем — Windows, macOS, Linux, Android, iOS.

SSTP (Secure Socket Tunneling Protocol). Надёжный протокол, сравнимый по уровню безопасности с OpenVPN. Этот вариант удобен, если предполагается использовать VPN на компьютере под управлением ОС Windows или Linux. Поддержка на других популярных системах, таких как Android или IOS, отсутствует.

L2TP (Layer 2 Tunneling Protocol) / IPSec. По безопасности превосходит предыдущие варианты, благодаря защитным алгоритмам IPSec (Internet Protocol Security). По сравнению с OpenVPN, производительность протокола ниже. Это происходит из-за двойного инкапсулирования данных. Поддерживается всеми распространёнными операционными системами.

IKEv2 (Internet Key Exchange version 2) /IPsec. Безопасность находится на том же уровне, что и у L2TP/IPSec. Протокол производителен и работает быстрее OpenVPN. Поддерживается на большинстве операционных систем. Кроме того, подключение к серверу автоматически восстанавливается в случае обрыва сети. Это делает удобным использование VPN такого типа на мобильных устройствах [26].

WireGuard. Это относительно новый протокол туннелирования, который уже зарекомендовал себя как быстрый и легковесный вариант. WireGuard использует симметричное шифрование и поддерживает различные методы аутентификации и шифрования, включая ChaCha20 и Poly1305. Этот протокол может работать на большинстве современных операционных систем, включая Windows, MacOS, Linux, Android и iOS.

PPTP (Point-to-Point Tunneling Protocol). Устаревший протокол, за разработку которого отвечает Microsoft. Поддерживается всеми системами, имеет максимальную производительность, но слабо защищён.

Выбор протокола зависит от требований к безопасности, производительности и доступности. В большинстве случаев достаточно OpenVPN и IKEv2, так как они обеспечивают высокую безопасность и быстрое соединение.

PPTP и L2TP могут быть незначительно быстрее, но менее безопасны, а IPSec и SSTP имеют больше требований к настройке. WireGuard также можно назвать хорошим вариантом для создания мобильных VPN-туннелей за счет своей скорости.

Контрольные вопросы к материалу П/З № 15:

1. Что такое VPN?
2. Что включает в себя архитектура VPN?
3. Как реализована защита VPN-туннеля?
4. Какие бывают виды туннелирования VPN?
5. Чем похожи и чем отличаются симметричное и ассиметричное шифрование?
6. Какой шифр является симметричным блочным шифром, который был разработан в 1993 году?
7. В чем преимущество использования VPN?
8. Какой протокол является самым оптимальным на данный момент?