УДК 004.7

Плетеный Д.С.
студент магистратуры
2 курс, факультет «Отдел магистратуры»
Поволжский государственный университет телекоммуникаций и информатики
Россия, г. Самара
Аленченко В.В.
студент магистратуры
2 курс, факультет «Отдел магистратуры»
Поволжский государственный университет телекоммуникаций и информатики
Россия, г. Самара
Научный руководитель: Кузнецов Михаил Владимирович

СРАВНЕНИЕ VPN - СОЕДИНЕНИЙ ДЛЯ ПРИМЕНЕНИЯ В ЗАЩИЩЕННЫХ КОРПОРАТИВНЫХ СЕТЯХ

Аннотация: *в статье рассматриваются современные протоколы для построения VPN – туннелей для применения в корпоративных сетях, перечисляются достоинства и недостатки по отношению к защищенности внутренней сети предприятия.*

Ключевые слова: *VPN, сеть, предприятие, защита, протокол, построение, безопасность, соединение, тоннель, Интернет.*

Annotation: *the article discusses modern protocols for building VPN tunnels for use in corporate networks, lists the advantages and disadvantages with respect to the security of the enterprise's internal network.*

Key words: *VPN, network, enterprise, protection, protocol, construction, security, connection, tunnel, Internet.*

Для передачи защищенной информации в открытых каналах связи существуют технологии и программные продукты, предназначенных для создания VPN-соединения в соответствии с международными стандартами IPSec. Для небольших предприятий такие решения являются хорошей альтернативой выделенным корпоративным сетям, и при этом имеют свои преимущества: надежность, простота настройки и масштабирования, изменяемая топология, мониторинг событий в сети, невысокая стоимость аренды каналов и телекоммуникационного оборудования.

При выходе из локальной сети в Интернет возникают такие угрозы, как несанкционированный доступ к информации во время передачи по открытой сети и несанкционированный доступ к внутренним ресурсам корпоративной сети предприятия. Информационная безопасность в таких соединениях обеспечивается следующими мерами: прямое и обратное криптографическое преобразование данных, аутентификация сторон, проверка достоверности и целостности данных. Технология виртуального тоннеля позволяет исключить несанкционированный доступ к передаваемой информации по открытым сетям, при этом ее реализация достаточно проста и относительно недорогая.

Основные протоколы для построения VPN-туннеля:

PPTP

L2TP

IPSec

SSL

PPTP (Point-to-Point Tunneling Protocol) - протокол «точка-точка». Компьютер устанавливает защищённое соединение с сервером за счёт создания специального туннеля в незащищённой сети. PPTP позволяет инкапсулировать пакеты PPP в пакеты IP и передавать их по сетям IP.

PPTP можно также применить для создания туннеля между двумя удаленными локальными сетями. PPTP работает, устанавливая обычную PPP-сессию с противоположной стороной с помощью протокола Generic Routing

Encapsulation (GRE). Второе соединение на TCP порту 1723 используется для инициации и управления GRE-соединением.

Для защиты PPTP-трафика может быть применен протокол MPPE. Для аутентификации клиентов могут применяться различные механизмы, безопасные из которых — MSCHAPv2 и EAP-TLS.

Для обеспечения работы клиента по протоколу PPTP необходимо установить IP-соединение с туннельным сервером PPTP. Вся передаваемая по такому соединению информация может быть защищена и сжата. По PPTP могут передаваться данные различных протоколов сетевого уровня (TCP/IP, NetBEUI и IPX).

Перечислим преимущества PPTP протокола.

- Использование частного IP-адреса. Пространство IP-адресов частной сети не должно координироваться с пространством глобальных (внешних) адресов.

- Поддержка множества протоколов. Есть возможность осуществлять доступ к частным сетям, использующим различные комбинации TCP/IP или IPX протоколов.

- Безопасная передачи информации. Для предотвращения несанкционированного доступа прieняются протоколы и политики обеспечения безопасности сервера удаленного доступа.

- Возможность применения аутентификации и защиты данных при передаче пакетов через Интернет.

L2TP (Layer 2 Tunneling Protocol) - протокол туннелирования уровня 2 (канального уровня). Объединяет протокол L2F (Layer 2 Forwarding), разработанный компанией Cisco, и протокол PPTP корпорации Microsoft. Позволяет организовать VPN с заданными приоритетами доступа, однако не содержит в себе средства для защиты информации и механизмов аутентификации.

L2TP использует сообщения двух типов: управляющие и информационные.

Управляющие сообщения используются для установления, поддержания и ликвидации туннелей и вызовов. Для обеспечения доставки ими используется надежный управляющий канал протокола L2TP. Информационные сообщения используются для инкапсулирования кадров PPP, передаваемых по туннелю. При потере пакета он не передается повторно.

Структура протокола описывает передачу кадров PPP и управляющих сообщений по управляющему каналу и каналу данных протокола L2TP. Кадры PPP передаются по ненадежному каналу, предварительно дополняясь заголовком L2TP, а затем - по транспорту для передачи пакетов, такому как Frame Relay, ATM и тому подобные. Управляющие сообщения передаются по надежному управляющему каналу L2TP с последующей передачей по тому же транспорту для пересылки пакетов данных.

Все управляющие сообщения должны содержать порядковые номера, используемые для обеспечения надежной доставки информации по управляющему каналу. Информационные сообщения используют порядковые номера для упорядочивания пакетов и выявления утерянных пакетов.

Преимущества L2TP:

- Разнообразие протоколов. Так как используется кадрирование PPP, удаленные пользователи могут использовать для доступа к корпоративному узлу большое количество различных протоколов, таких как IP, IPX и т.д.

- Создание туннелей в различных сетях. L2TP может работать как в сетях IP, так и в сетях ATM, Frame Relay и других.

- Безопасность передачи данных. При этом пользователь не должен иметь никакого специального программного обеспечения.

- Возможность аутентификации пользователей.

IPSec (IP Security) - набор протоколов, касающихся вопросов обеспечения защиты данных при транспортировке IP-пакетов. IPSec также включает в себя протоколы для защищённого обмена ключами в сети Интернет. Протоколы IPSec работают на сетевом уровне (уровень 3 модели OSI).

IP не имеет средств защиты данных и не может гарантировать, что отправитель является именно тем, за кого он себя выдает. При использовании IPSec весь передаваемый трафик может быть защищен перед передачей по сети. При использовании IPSec получатель может отследить источник полученных пакетов и удостовериться в целостности данных. Необходимо быть уверенным в том, что транзакция может осуществляться только один раз (за исключением случая, когда пользователь уполномочен повторять ее). Это означает, что не должно существовать возможности записи транзакции и последующего ее повторения в записи с целью создания у пользователя впечатления об осуществлении нескольких транзакций. Представьте себе, что мошенник получил информацию о трафике и знает, что передача такого трафика может дать ему какие-то преимущества (например, в результате на его счет будут переведены деньги). Необходимо обеспечить невозможность повторной передачи такого трафика.

IPSec VPN оптимален для объединения сетей разных офисов через Интернет.

Преимущества для пользователей SMB/SOHO (Малый бизнес/Малый офис/Домашний офис):

- Экономическая эффективность
- Законченное решение для коммерческого использования

Для дистанционных пользователей:

- Интегрированное безопасное решение
- Нет необходимости в дополнительном программном обеспечении
- Простота конфигурирования

Для коллективных пользователей:

- Экономически эффективное решение для дистанционных пользователей и филиалов
- Совместимость с решениями большинства поставщиков решений для виртуальных частных сетей.

Существует две разновидности протокола IPSec: ESP (Encapsulation Security Payload, инкапсуляция защищенных данных) и AH (Authentication Header, Аутентифицирующий заголовок). ESP и AH - новые протоколы IP. О том, что пакет является пакетом ESP, говорит значение в поле протокола заголовка IP, равное 50, а для пакета AH - равное 51.

В пакетах ESP и AH между заголовком IP (IP header) и данными протокола верхнего уровня вставляется заголовок ESP/AH (ESP/AH header). ESP может обеспечивать как защиту данных, так и аутентификацию, а также возможен вариант протокола ESP без использования защиты данных или без аутентификации. Однако, невозможно использовать протокол ESP одновременно без защиты данных и без аутентификации, поскольку в данном случае безопасность не обеспечивается. При осуществлении защиты передаваемых данных заголовок ESP не защищен, но защищены данные протокола верхнего уровня и часть трейлера ESP.
А в случае аутентификации производится аутентификация заголовка ESP, данных протокола верхнего уровня и части трейлера ESP.
Хотя протокол AH может обеспечивать только аутентификацию, она выполняется не только для заголовка AH и данных протокола верхнего уровня, но также и для заголовка IP.

Протоколы семейства IPSec могут использоваться для защиты либо всех полезных данных IP-пакета, либо данных протоколов верхнего уровня в поле полезных данных IP-пакета. Это различие определяется выбором двух различных режимов протокола IPSec: транспортного режима или туннельного режима.

Транспортный режим в основном используется хостом IP для защиты генерируемых им самим данных, а туннельный режим используется шлюзом безопасности для предоставления услуги IPSec другим машинам, не имеющим функций IPSec. Однако функции хоста IPSec и шлюза безопасности могут выполняться одной и той же машиной. Оба протокола IPSec, AH и ESP, могут выполняться в транспортном или туннельном режиме.

SSL VPN

SSL (Secure Socket Layer) это протокол защищенных сокетов, обеспечивающий безопасную передачу данных по сети Интернет. При использовании данного протокола создается защищенное соединение между сервером и клиентом.

Протокол SSL использует защиту данных с открытым ключом для подтверждения подлинности отправителя и получателя. Поддерживает надёжность передачи данных за счёт использования корректирующих кодов и безопасных хэш-функций.

SSL использует такие алгоритмы защиты, как RC4, MD5, RSA и т.п. SSL использует два ключа - открытый ключ и закрытый (он же частный ключ, который известен только получателю).

На данный момент, в Интернете возможно встретить множество сайтов, в которых используется протокол SSL для обеспечения безопасности персональных данных (в качестве примера можно представить веб-сайты, предоставляющие коммерческие и банковские услуги). Все современные браузеры, почтовые клиенты и интернет-приложения поддерживают работу с протоколом SSL. Для доступа к страницам, защищённым протоколом SSL, в строке URL вместо стандартного префикса «http» применяется префикс «https» (порт 443), который указывает на то, что будет применяться SSL-соединение. SSL также может обеспечить защиту протоколов прикладного уровня модели OSI, таких как POP3 или FTP. Для работы протокола SSL требуется, чтобы на сервере присутствовал SSL-сертификат. Защищенное соединение клиент-сервер при использовании SSL выполняет две функции - аутентификацию и защиту данных.

Протокол SSL состоит из двух уровней. На нижних уровнях (уровни 4-5) многоуровневого транспортного протокола (например, TCP) он является протоколом записи и используется для инкапсуляции различных протоколов. Для каждого инкапсулированного протокола он обеспечивает условия, при

которых сервер и клиент могут подтверждать друг другу свою подлинность, выполнять защиту передаваемых данных и производить обмен ключами, прежде чем протокол программы начнет передавать и получать данные. Ниже перечислены преимущества протокола SSL:

- Простота использования
- Нет необходимости в дополнительном программном обеспечении
- Безопасный удаленный доступ
- SSL VPN оптимален для подключения удаленных пользователей к ресурсам локальной сети офиса через Интернет.

Использованные источники:

1. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях: учебное пособие. - М.: ДМК Пресс, 2012. - 592 с.
2. Калашников С.К. История «болезней» VPN // Журнал сетевых решений, 2013. - № 11.
3. Блог Cisco в России и СНГ [Электронный ресурс]. URL: https://gblogs.cisco.com/ru/
4. Отчет Cisco по информационной безопасности за 2018 год [Электронный ресурс]. URL: https://www.cisco.com/c/dam/global/ru_ru/assets/offers/assets/cisco_2018_acr_ru.pdf
5. Threat Hunting Report [Электронный ресурс]. URL: https://www.cisco.com/c/dam/global/ru_ru/assets/pdfs/cybersecurity-series-2019-threat-hunting-ru.pdf