ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ VPN ВИДА СЕТЬ-СЕТЬ

Игнатьев Александр Андреевич

студент, Лесосибирский Педагогический Институт — филиал Сибирского Федерального Университета, РФ, Лесосибирск

Киргизова Елена Викторовна

научный руководитель, канд. пед.наук, доцент кафедры высшей математики, информатики и естествознания, Лесосибирский Педагогический Институт — филиал Сибирского Федерального Университета, РФ, Лесосибирск

Румянцев Максим Валерьевич

научный руководитель, канд. филос. наук, доцент, Сибирский Федеральный Университет, РФ, Красноярск

Обеспечение безопасности передаваемых данных через публичный канал связи(Internet) является одной из основных задач функционирования корпоративной сети. Исторически сложилось так, что протокол IPv4 не имеет встроенного функционала для шифрования данных и механизма проверки их целостности(контрольная сумма высчитывается только для заголовка, не для поля данных). По этой причине были разработанны средства, обеспечивающих безопасность передачи данных, методом инкапсуляции передаваемых данных в протоколы различных уровней модели OSI. Стоит отметить, что использование тех или иных механизмов всегда определяется конкретной поставленной задачей, таким образом невозможно выработать единый алгоритм использования применимый ко всем случаям. Кроме того, при выборе используемого решения нобходимо обратить внимание на основные качества — криптостойкость и простоту эксплуатации. В рамках данной статьи рассмотрим существующие протоколы, проведем анализ и выделим наиболее подходящие для VPN вида сеть-сеть.

Понятие VPN.

Virtual Private Network — это способ использования открытых или частных сетей таким образом, чтобы пользователи VPN были отделены от других пользователей и могли взаимодействовать между собой, как если бы находились в единой закрытой(выделенной) сети [2]. То есть VPN обеспечивает целостность и недоступнойсть передаваемой информации по публичным каналам связи. По этой причине чаще всего VPN тесно связан с понятием туннелирования. Туннелирование в компьютерных сетях — процесс, в ходе которого создается защищенное логическое соединение между двумя конечными точками посредством инкапсуляции различных протоколов. Инкапсулируемый протокол относится к тому же или более низкому уровню OSI, чем используемый в качестве тоннеля. Упрощенно это выглядит так: приложение - отправитель формирует запрос, этот запрос «заворачивается» в выбранный протокол VPN, попутно шифруется, если функционал реализован в протоколе, а затем передается по сети как некоторые данные. При поступлении на хост-получатель, «разворачивается» принимающей стороной, дешифруется(при наличии ключа) и обрабатывается приложением — получателем.

При этом передающие протоколы ничего не знают о содержимом, а содержимое ничего не знает о передающих протоколах, что и называется туннелем. Об особенностях реализации и

видах виртуальных частных сетей ниже.

Виды VPN.

Весьма очевиден тот факт, что вопрос о безопасности передаваемых данных стал чрезвычайно актуален ровно в тот момент, когда Интернет, в текущем его виде, вырвался из лабороторных стен и грянул в массы. Как следствие, возможных реализаций(устаревших и не очень) разработано изрядное количество. В данной статье рассмотрим наиболее известные и актуальные:

Канальный уровень:

1. PPTP

2. L2TP

Сетевой уровень:

1. GRE/IPIP

2. IPsec

Транспортный уровень:

1. SSL/TLS

2. OpenVPN

Остановимся на каждом из них.

VPN канального уровня.

PPTP (Point-to-Point Tunneling Protocol) - туннельный протокол типа точка-точка, позволяющий компьютеру устанавливать защищённое соединение с сервером за счёт создания специального туннеля в стандартной, незащищённой сети. Протокол PPTP позволяет инкапсулировать (упаковывать или скрыть от использования) пакеты PPP в пакеты протокола Internet Protocol (IP) и передавать их по сетям IP (в том числе и Интернет). Транспортом PPP в данном случае служит протокол GRE, также для управления GRE используется дополнительный порт TCP 1723. Поддерживает протокол MPPE для защиты данных и различные механизмы авторизации клиентов, среди которых MSCHAPv2 и EAP-TLS.

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 организовывать VPN с заданными приоритетами доступа, однако не содержит в себе средств для защиты данных и механизмов аутентификации. В случае необходимости используется IPsec.

VPN сетевого уровня.

GRE (generic routing encapsulation — общая инкапсуляция маршрутов) — разработанный CISCO протокол туннелирования сетевых пакетов. Основное назначение — инкапсуляция пакетов сетевого уровня модели OSI в IP-пакеты. Номер протокола в IP — 47. Протокол не поддерживает никаких режимов аутентификации или шифрования, его задача — доставка пакетов. В случае необходимости используется IPsec.

IPsec был разработан с целью повышения безопасности IP протокола. Следует отметить, что IPsec предлагает набор алгоритмов и механизмов, а не готовое решение, задача настройщика выбрать нужное и применить в зависимости от поставленных целей. Представлены возможности шифрования, аутентификации и функции для сохранности целостности сообщения. Поддерживается два режима работы — транспортный и туннельный.

Транспортный режим используется только для шифрования и аутентификации данных, исходные заголовки IP не аутентифицируются и остаются прежними. В туннельном режиме аутентифицируются и шифруются в том числе и исходные заголовки IP, поверх них создаются новые заголовки, что позволяет полностью скрыть информацию, передающуюся по сети, включая сетевой уровень модели OSI от злоумышленника.

VPN транспортного уровня.

SSL/TLS. Изначально SSL разрабатывался как средство защиты TCP-соединения, ни UDP ни ICMP протоколы не поддерживались, что сказалось на архитектуре SSL. После стандартизации IETF (Internet Engineering Task Force) он был переименован в TLS. Фактически, SSL и TLS — названия взаимозаменяемые, отличаются они версиями протокола. Поддерживают аунетнификацию, шифрование и функции сохранения целостности сообщений. SSL VPN делится на два класса:

1) Веб-VPN. Примером может служить применяемый почти повсеместно протокол HTTPS. Соединение устанавливается в браузере в момент обращения к веб-серверу, клиентом выступает не отдельный хост, а конкретный браузер. Весь остальной трафик, помимо конкретного сайта передается незашифрованным.

2) Инкапсуляция пакетов в SSL/TLS. Более подходящий под определение VPN механизм работы. Заключается он в том, что весь IP трафик перехватывается на шлюзе и инкапсулируется в TCP соединение, которое и защищается про помощи протокола SSL/TLS. Недостатком данного решения является тот факт, что способ инкапсуляции IP в TCP не стандартизирован, что не обеспечивает совместимость оборудования разных производителей.

OpenVPN — свободная реализация технологии виртуальной частной сети (VPN) с открытым исходным кодом для создания зашифрованных каналов типа точка-точка или сервер-клиенты между компьютерами. Частный случай использования инкапсуляции пакетов в SSL/TLS, особенность которой в собственной разработке серверной и клиентской частей, что обеспечивает программную совместимость для различных производителей оборудования. Транспортом может быть как TCP так и UDP.

VPN сеть-сеть

Рассмотрим представленные выше протоколы в ключе организации VPN вида сеть-сеть. Оговорюсь, что в данной статье не рассмартиваются протоколы динамической маршрутизации, в том случае, если у вас большое количество офисов. При использовании динамической маршрутизации требования к протоколам отличаются от текущих. С учетом того факта, что большинство из протоколов поддерживают относительно одинаковые параметры безопасности, хоть и различными методами, отталкиваться будем от криптоустойчивости таковых и удобства управления трафиком.

PPTP. Использует жесткое разделение клиент-сервер. Один туннель будет обеспечивать доступ в одну сеть, соответсвенно для двухстороннего обмена потребуется второй туннель. Аутентификация по логину-паролю, рекомендуемый протокол - MS-CHAP v2, шифрование MPPE. На текущий момент времени ни один ни второй протокол не является безопасным, так, в 2012 году был представлен сервис, способный подобрать пароль MS-CHAP v2 за 23 часа, а MPPE уязвим к атаке, подменяющей биты. Также шифруется только пользовательский трафик, все остальные данные передаются в открытом виде. Можно использовать в связке с IPsec, но в таком случае нет необходимости использовать непосредственно PPTP. Не рекомендуется использовать при передаче по публичным каналам связи.

L2TP + IPsec. Главная особенность в том, что используются кадры PPP. То есть в нашей работающей сети будет использоваться дополнительная инкапсуляция, имеющая смысл только если мы пользуемся встроенным в протокол функционалом, например приоритезации трафика или в случае использования не только IP-сетей. При этом функционал VPN осуществляет IPsec.

IPsec. Шифруется исходный IP пакет целиком при использовании туннельного режима. При

использовании транспортного режима шифруется только содержимое пакета. Как следствие, злоумышленник ничего не сможет узнать о трафике, кроме отправителя и получателя пакета. Главный минус использования IPsec в чистом виде — большие затраты времени на настройку. Для того, чтобы обеспечить связь сеть-сеть придется прописывать параметры маршрутизации и политики безопасности для каждой сети. Как следствие, значительно увеличевается время на диагностику проблем.

GRE + IPsec. Решить вышеописанную проблему позволяет протокол GRE. Настройка сводится к организации туннеля GRE и настроек политики безопасности(IPsec) только для него. Для всех необходимых сетей GRE интерфейс указывается шлюзом, через который в дальнейшем будет происходить передача данных между нашими офисами, а функционал VPN будет накладываться при любой активности GRE интерфейса.

OpenVPN. Является весьма конкурентноспособным с GRE + IPsec и по обеспечению безопасности и по удобству настройки. Кроме того, может быть использован на любом TCP и UDP порту, что позволяет произвести настройку, если существует проблема на уровне провайдера с другими протоколами. Тем не менее, в отличии от остальных протоколов, реализованных на уровне ядра, OpenVPN является приложением, что может замедлять работу. Также рекомендуется использование протокола UDP, так как использование TCP может заметно сказаться на скорости передачи данных.

Список литературы:

1. «Виды VPN-соединений (PPTP, L2TP, IPSec, SSL)» — [Электронный ресурс] — режим доступа. — URL: https://kb.zyxel.ru/hc/ru/articles/115002573033-%D0%92%D0%B8%D0%B4%D1%8B-VPN-%D1%81%D0%BE%D0%B5%D0%B4%D0%B8%D0%BD%D0%B5%D0%BD%D0%B8%D0%B9-PPTP-L2TP-IPSec-SSL-

2. «Калейдоскоп VPN-технологий» — [Электронный ресурс] — режим доступа. — URL: https://cyberleninka.ru/article/v/kaleydoskop-vpn-tehnologiy

3. «Методическое пособие. IPSec» — [Электронный ресурс] — режим доступа. — URL: http://dfe.karelia.ru/koi/posob/security/index.html

4. «OpenVPN. Documentation» — [Электронный ресурс] — режим доступа. —URL: https://openvpn.net/index.php/open-source/documentation.html