# 1 БЕЗОПАСНЫЕ СЕТЕВЫЕ СОЕДИНЕНИЯ. VPN

## 1.1 Общая информация

Для защиты сети многие используют виртуальную частную сеть для решения личных или корпоративных задач, так что существует большое количество VPN реализаций, и у каждой реализации есть свои плюсы и минусы.

Технология виртуальной частной сети или от английского Virtual Private Network, VPN, дает возможность создать одно или несколько соединений над другой сетью, а с помощью средств шифрования можно достичь максимальной защиты передаваемой информации.

VPN часто реализуется не выше сетевого уровня модели OSI, так как именно на этих уровнях есть возможность применения зашифровки данных, не затрагивая протоколы транспортного уровня. Соответственно эта технология является защищенным соединением поверх существующей сети, реализуемым с помощью инкапсуляции данных.

Задачи, которые решает VPN:

- Шифрование трафика;
- Адресация пакетов, которые предназначены определенным клиентам;
- Аутентификация пользователей при подключении к сети;
- Защита сети от попадания чужих пакетов и узлов при помощи проверки источников данных.

Существует несколько реализаций данной технологии:

- Point-to-Point tunneling protocol, или PPTP;
- IP Security или IPSec;
- Layer 2 Tunneling Protocol или L2TP;
- Secure Socket Tunneling Protocol или SSTP;
- OpenVPN.

### 1.2 Реализации виртуальной частной сети

#### 1.2.1 Протокол туннелирования PPTP

PPTP или от английского Point-to-point transfer protocol – протокол для соединения типа “точка-точка”. Он использует TCP для установления подключения и протокол MPPE, который служит для шифрования трафика. Аутентификация клиентов обычно обеспечивается с помощью MS-CHAPv2 механизма.

Microsoft Point-to-Point Encryption или MPPE — протокол для шифрования данных, который используется поверх соединений PPP. Применяет RSA RC4 алгоритм для обеспечения конфиденциальности данных. MPPE поддерживает 40- и 128-битные ключи, меняющиеся во время соединения.

MS-CHAP (от английского Microsoft Challenge Handshake Authentication Protocol) - это протокол, проверяющий подлинность соединения между клиентом и сервером без передачи пароля.

Он реализован при помощи протокола CHAP, в котором есть механизм возвращения информации об ошибках аутентификации, и можно изменить пароль пользователя, также он предоставляет возможность создания ключей шифрования для протокола MPPE.

PPTP VPN стал распространен благодаря простой настройке, кроссплатформенности и поддержке по умолчанию на большинстве современных операционных систем. Также он популярен из-за своей стабильности, высокой скорости работы и минимальной нагрузки на устройство. Но у этой технологии есть множество уязвимых мест в безопасности, как в устройстве протокола MMPE, так и в аутентификации MS-CHAP. Несмотря на то, что последнюю проблему можно решить изменением системы аутентификации на PEAP, компания Microsoft все равно рекомендует использовать L2TP или SSTP.

Процесс соединения с помощью протокола PPTP состоит из ввода IP-адреса, после которого инициируется передача запроса серверу для начала сеанса. Клиент ждет от сервера подтверждения данных для авторизации, а

также ответа о установленном соединении. В это время PPTP канал запускается, и клиент получает возможность начать туннелирование трафика серверу.

### 1.2.2 Защита трафика сети IPSec

IPSec или от английского IP Security - это стек протоколов, которые обеспечивают секретность трафика, передаваемого трафика через сети, путем отслеживания целостности, подлинности и кодирования пакетов. Он способен работать в транспортном режиме, когда используется шифрование данных пересылаемого пакета, а исходный заголовок сохраняется. Также может работать в туннельном режиме, в нем кодируется весь передаваемый трафик, который потом инкапсулируется в поле данных нового IP-пакета. Но IPSec не создает в системе виртуальный сетевой адаптер, а использует внешний интерфейс, что отдаляет его от виртуальных частных сетей и показывает просто его относительное отношение к ним.

У протокола IPSec также есть уязвимость, из-за которой он может повергаться атакам, направленным на протокол, который используется для первичной настройки соединения и аутентификации конечных узлов. Также обмена секретными ключами, кроме этого при работе IPSec в режиме отсутствия заголовков, злоумышленник может добавить собственные данные в транслируемые пакеты, что показывает брешь в безопасности. Также есть способ, при котором заменяется маршрут передачи пакетов.

### 1.2.3 Протокол туннелирования второго уровня L2TP

L2TP от английского Layer 2 tunneling protocol – протокол, который применяется для туннелирования в виртуальных частных сетях. Он использует сообщения двух видов: информационный и управляющие сообщения. Информационные сообщения применяются для инкапсулирования кадров PPP, которые передаются по туннелю, если пакет теряется, он заново не передается. Управляющие сообщения нужны для установки, поддержания и завершения

туннелей и вызовов, для гарантии доставки они применяют безопасный канал управления, который входит в протокол L2TP.

По структуре протокола понятно описание передачи кадров PPP и координирующих сообщений по каналу управления информации протокола L2TP. Кадры PPP пересылаются по сомнительному каналу, заранее пополняясь заголовком L2TP, далее идут на транспортный уровень для передачи пакетов. Сообщения управления пересылаются по безопасному управляющему каналу L2TP с дальнейшей передачей по этому же транспорту для переправки пакетов. Любые управляющие сообщения содержат порядковые номера, которые нужны, чтобы обеспечить безопасную доставку по каналу, а информационные сообщения используют эти номера для организации пакетов и показа потерь.

### 1.2.4 Протокол безопасного туннелирования сокетов SSTP

SSTP от английского Secure socket tunneling protocol или протокол безопасного туннелирования сокетов – это протокол прикладного уровня, который был спроектирован для создания одновременного взаимодействия при коллективном обмене информацией. Из-за этого протокола появилась возможность создания нескольких подключений между узлами по одному соединению, в следствие чего становится возможным высокоэффективное применение доступных ресурсов сети. Протокол безопасного туннелирования основан на SSL и используется для передачи трафика 443 порт. Благодаря протоколу SSL v.3, который поддерживает SSTP, есть возможность работы без настройки межсетевого экрана, а еще стабильная работа обеспечивается благодаря его интеграции в операционную систему. Из-за того, что SSTP соединяется по протоколу HTTPS, клиентам предоставляется защищенный доступ к сетям за маршрутизаторами NAT, веб прокси и брандмауэрами.

Осуществление SSTP соединения основанного на VPN:

1) Протокол безопасного туннелирования проверяет наличие интернет соединения у клиента, и после того как было подтверждено наличие

сети, начинает устанавливаться TCP соединение с сервером по 443 порту;

2) Потом происходит SSL согласование с устанавливаемым соединением, в соответствии с чем проверяется сертификат сервера и если сертификат верный, то соединение устанавливается, в обратном случае обрывается;
3) Далее клиент отправляет HTTPS запрос на сервер в зашифрованной SSL сессии;
4) Теперь клиент отправляет контрольные SSTP пакеты внутри HTTPS сессии, что приводит к установке SSTP состояния на обеих машинах;
5) Следующим шагом совершается PPP согласование SSSTP по HTTPS на обоих устройствах, после чего клиент проходит аутентификацию на сервере;
6) Затем сессия привязывается в IP интерфейсу на обеих машинах и IP адрес назначается для маршрутизации трафика.;
7) В итоге установлено взаимодействие для любого трафика.

Из-за такого типа соединения блокировка удаленного доступа и проблемы NAT остаются в прошлом. Эта технология достаточно стабильна и хорошо документирована, что показывает насколько это хороший продукт.

### 1.2.5 Система виртуальной частной сети OpenVPN

OpenVPN – открытая реализация виртуальной частной сети, которая предназначена для создания зашифрованных соединений типа “точка-точка” или “сервер-клиенты”. В этой технологии безопасность обеспечивается при помощи библиотеки OpenSSL, которая предоставляет множество инструментов шифрования, и еще используется пакетная аутентификация HMAC, что делает еще сильнее защиту. Также выбранный алгоритм шифрования может замедлить процессы OpenVPN, но чаще всего эта технология работает быстрее и использует меньше ресурсов, в сравнении с L2TP и IPSec, еще в отличие от

этих реализаций у OpenVPN есть встроенный инструмент сжимающий данные, который называется LZO.

Главным плюсом OpenVPN является возможность установки соединения между устройствами, которые находятся за NET, без надобности в изменении настроек при помощи стандартного TCP 443 порта для HTTPS, из-за SSL или TLS инкапсуляции. Также TCP протокол предоставляет лучшую защиту данных, но он работает медленнее относительно UDP, который быстрее благодаря отсутствию подтверждения доставки пакетов, еще UDP установлен по умолчанию.

Именно по этой причине обычно предпочтительнее использовать UDP, потому что через туннель проходят пакеты сетевого уровня и выше по OSI, если применяется режим соединения TUN, или сетевой трафик канального уровня и выше по OSI, если применяется режим TAP. Это означает, что для клиента OpenVPN выступает протоколом канального или даже физического уровня, соответственно защищенность передачи информации возможна при помощи вышестоящих уровней по модели OSI, если это будет необходимо.

Если все-таки настроить туннель на работу по TCP, то сервер в обычном режиме будет получать TCP-сегменты OpenVPN, которые будут содержать другие TCP-сегменты от клиента. В итоге в цепи получится двойная верификация на невредимость данных, что не имеет практической ценности, так как надежность не увеличивается, а пинг и скорость соединения снижаются. Еще есть возможность работы через большую часть прокси серверов, включая HTTP, SOCKS, через NAT и сетевые фильтры. Также сервер можно настроить на нужные сетевые настройки клиенту.

Благодаря широким возможностям настройки и поддержке большинство операционных систем OpenVPN очень много где используется. Данная технология позволяет использовать несколько видов аутентификации:

- Заранее установленный ключ, который является самым простым методом;

- Сертификационная аутентификация, является самым гибким для настроек методом;
- Аутентификации при помощи логина и пароля, есть возможность использования без создания клиентского сертификата, но при наличии серверного.

**2. Заключение**

Подводя итоги, можно выделить следующее:

PPTP прост в настройке и поддерживается на множестве операционных систем, но у него много уязвимых мест.

IPSec хоть и способен пользоваться различными алгоритмами зашифровки данных и аутентификации для VPN, но он использует внешний интерфейс, а не виртуальный сетевой адаптер. L2TP вместе с IPSec может повести себя хорошо со стороны безопасности и совместимости, но двойная инкапсуляция приводит к нестабильной работе туннеля.

SSTP хоть и достаточно удобный, стабильный и довольно защищен, но также является детищем Microsoft, из-за чего его работа сильно связана с операционной системой Windows, в других системах способности SSTP чаще всего оказываются урезанными.

OpenVPN есть причины считать самым осмысленным выбором из-за сбалансированности всех его показателей, в том числе:

- Скорость;
- Кроссплатформенность;
- Стабильность, чаще всего работая через TCP, не применяя сжатие;
- Гибкость настроек;
- Безопасность из-за использования инструментов библиотеки OpenSSL.