



ТЕХНОЛОГИЯ VPN

Пасько Виталий Витальевич

Сахненко Максим Сергеевич

студенты

научный руководитель: **Аверченко Артём Павлович**

ст. преподаватель

Омский государственный технический университет, г. Омск

Введение

VPN, она же «виртуальная частная сеть» — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети, например Интернет. Несмотря на то, что для коммуникации используются сети с меньшим или неизвестным уровнем доверия например, публичные сети, уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств шифрования, аутентификации, инфраструктуры открытых ключей, средств защиты от повторов и изменений передаваемых по логической сети сообщений.

В зависимости от применяемых протоколов и назначения VPN может обеспечивать соединения трёх видов: узел-узел, узел-сеть и сеть-сеть.

Структура VPN

VPN состоит из двух частей: "внутренней" (управляемой) сети, которых может быть несколько, и "внешней" сети, через которую проходит инкапсулированное соединение (обычно используется Интернет).

Также возможно подключение отдельного компьютера к виртуальной сети.

Удаленный пользователь подключается к VPN через сервер доступа, который подключен как к внутренней, так и к внешней (публичной) сети. При подключении удаленного пользователя (или установлении соединения с другой защищенной сетью) сервер доступа требует выполнения процесса идентификации, а затем процесса аутентификации. После успешного завершения обоих процессов удаленный пользователь (удаленная сеть) получает право работать в сети, то есть происходит процесс авторизации.

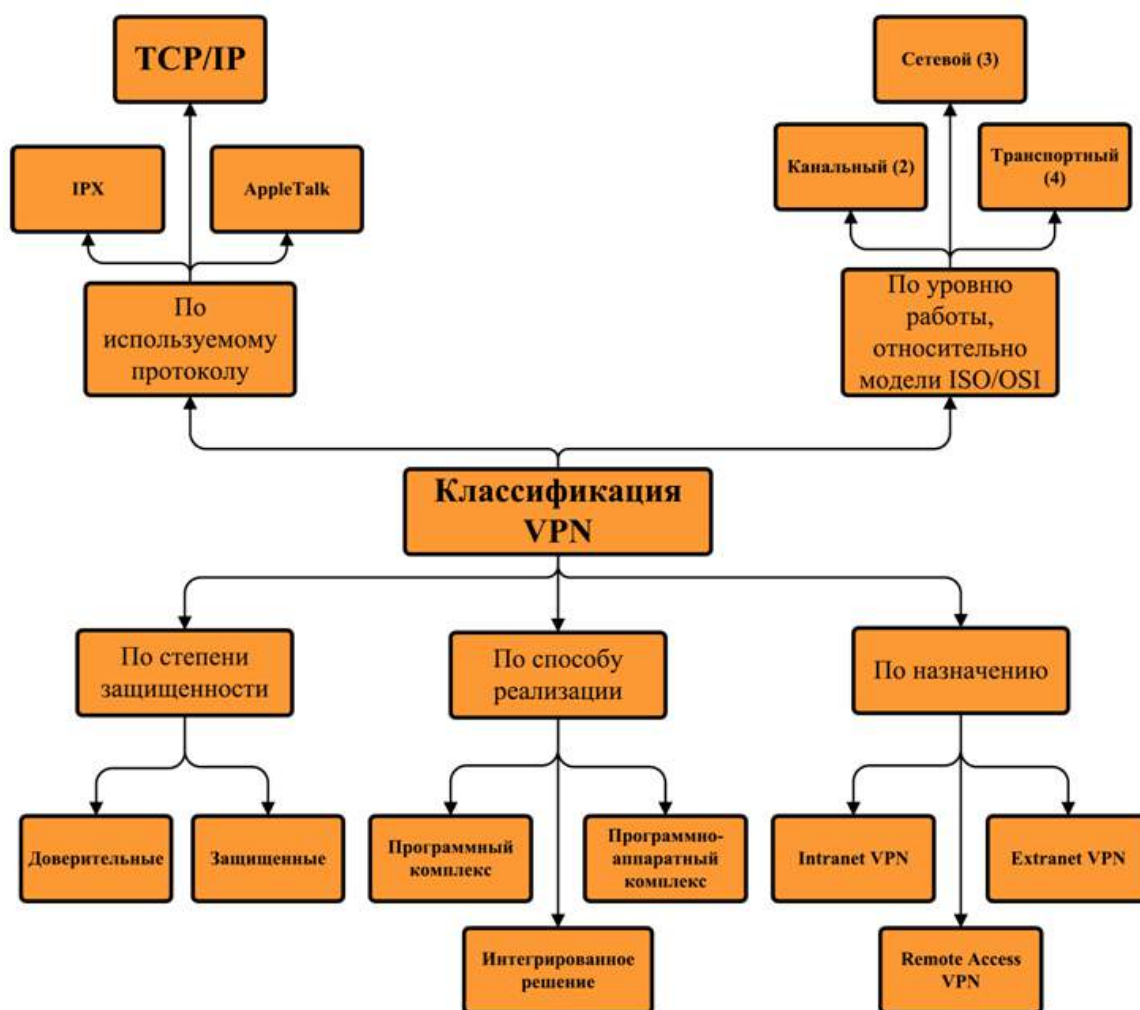
Виды VPN



VPN шифрует данные с помощью протоколов.

- OpenVPN
- L2TP/IPSec
- IKEv2
- PPTP
- WireGuard
- SSTP

Классификации VPN



По используемому протоколу

Протокол TCP/IP



Наборы правил, или протоколы, используются для организации обмена данными между компьютерами. В настоящее время наиболее широко используется набор протоколов, получивший общее название TCP/IP. (Напомним, что во многих европейских странах используется протокол X.25). Основными функциями семейства протоколов TCP/IP являются электронная почта, передача файлов между компьютерами и удаленный вход в систему.

Команда пользователя mail, команды пользователя обработки сообщений (MH) и команда сервера sendmail могут использовать TCP/IP для передачи сообщений между системами, а базовые сетевые утилиты (BNU) могут использовать TCP/IP для передачи файлов и команд между системами.

TCP/IP - это набор протоколов, который устанавливает стандарты для связи между компьютерами и содержит подробные соглашения о маршрутизации и межсетевом взаимодействии. TCP/IP широко используется в Интернете, поэтому пользователи из научно-исследовательских институтов, школ, университетов, государственных учреждений и промышленных предприятий могут использовать его для связи.

TCP/IP обеспечивает связь между компьютерами, подключенными к сети, обычно называемыми хостами. Любая сеть может быть подключена к другой сети и общаться с ее хостами. Хотя существуют различные сетевые технологии, многие из которых основаны на коммутации пакетов и потоковой передаче данных, набор протоколов TCP/IP имеет одно важное преимущество: он обеспечивает аппаратную независимость.

"Примечание: TCP/IP обеспечивает только базовые функции управления сетью. По сравнению с TCP/IP, SimpleNetworkManagementProtocol (SNMP) предоставляет более широкий набор команд и функций управления."

По способу реализации

Программное решение. Для функционирования VPN используется ПК со специализированным ПО.

Программно-аппаратное решение. Для реализации VPN используется комплекс специальных программно-аппаратных средств. За счет такого подхода обеспечиваются высокая производительность и защищенность.

Интегрированное решение. Реализацию VPN обеспечивает программно-аппаратный комплекс, попутно решающий задачи организации сетевого экрана, фильтрации трафика и т.д.

По степени защищенности

Доверительные. Реализуются при необходимости создания виртуальной подсети в составе большой сети. Передающая среда при этом считается доверительной, а проблемы безопасности — неактуальными.



Защищенные. Это самый популярный вид VPN, с помощью которого создаются защищенные и надежные сети на базе ненадежных сетей, например, Интернета.

По назначению

Extranet VPN. Виртуальные сети, в которые могут подключаться «внешние» пользователи — клиенты или заказчики. Так как они пользуются меньшим доверием, нежели сотрудники компании, существует необходимость создания определенных правил, ограничивающих доступ «внешних» пользователей к конфиденциальной или коммерческой информации.

RemoteAccess VPN. Реализуется для обеспечения защищенного канала между корпоративной сетью и пользователем, подключенным к защищенной сети извне, например, с домашнего ПК.

Internet VPN. Реализуется провайдерами для предоставления доступа клиентам, подключающимся по одному физическому каналу.

Intranet VPN. Объединяет в защищенную сеть ряд филиалов одной компании, распределенных географически, для обмена информацией по открытым каналам.

Client/Server VPN. Защищает данные, передаваемые между узлами корпоративной сети (но не сетями). Обычно реализуется для узлов, находящихся в одном сетевом сегменте, например, клиентской машиной и сервером. Этот вариант применяется для разделения одной физической сети на несколько логических.

Вывод

Тенденции рынка программного обеспечения VPN

Проблема Интернета в наши дни заключается в том, что правительства, провайдеры, рекламодатели и хакеры все лучше и лучше вторгаются в частную жизнь пользователей. Даже онлайн-продавцы теперь отслеживают активность на основе IP-адресов.

Поскольку в современном мире безопасность Интернета приобрела первостепенное значение, все больше компаний устанавливают программное обеспечение VPN, главным образом для защиты частной жизни, блокировки рекламы и доступа к заблокированным веб-сайтам. Ожидается, что к концу 2022 года мировой рынок VPN вырастет в среднем на 13% и достигнет 106 миллиардов долларов. Считается, что этот рост обусловлен развитием сектора кибербезопасности, увеличением числа инцидентов, связанных с безопасностью, ростом промышленности и увеличением использования мобильных устройств. Однако высокие затраты на развертывание и отсутствие технических навыков могут помешать этим прогнозам.

Список литературы:



1. «MPLS and VPN Architectures», **Том 2. Авторы:** Jim Guichard, Ivan Pepelnjak, Jeff Apcar-
https://books.google.ru/books?id=1ov-2vEyFCUC&hl=ru&source=gbs_navlinks_s
2. Egyptian Informatics Journal Volume 23, Issue 4, December 2022-
<https://www.sciencedirect.com/science/article/pii/S1110866522000482>
3. «Что такое VPN?»-<https://nordvpn.com/ru/what-is-a-vpn/>