УДК 330.4:330.46

СОВРЕМЕННЫЕ VPN – СЕТИ

В.В. МАЙОРОВ

Кубанский государственный технологический университет,
350002, Российская Федерация, г. Краснодар, ул. Московская, 2;
электронная почта: mayorovvladislav@outlook.com

Статья посвящена современным VPN - сетям. Данная проблема очень актуальна в настоящее время. Это связано главным образом с обеспечением безопасности в сети Интернет. Меры безопасности используют как компании, так и обычные пользователи. Это позволяет персоналу работать удаленно и пользоваться данными фирмы без опасений утечки информации. Степени защищенности VPN – сетей различны, что означает различную направленность на потребление данной виртуальной сети. При использовании шифрования VPN – соединения, можно защититься от несанкционированного доступа к передаваемой информации. В последнее время все чаще поднимается вопрос анонимности в сети интернет. В статье дается краткий анализ наиболее значимых протоколов VPN – соединений. В связи с этим информация, отражённая в рецензируемой статье, своевременна и актуальна.
Ключевые слова: VPN – сеть, PPTP, L2TP, IPSec, Open VPN, глобальная сеть Internet.

На сегодняшний день в сфере сетей и телекоммуникаций актуальной задачей является защищенная передача информации на большое расстояние. Разрабатываются различные сетевые протоколы, которые направлены на решение определенных задач [1-3].

Самыми известными являются TCP (transmission control protocol) и UDP (user datagram protocol). Данные протоколы решают проблему отправки и принятия информации через сеть. Основной идеей данных протоколов было взаимодействие компьютеров в сети, что дало толчок для развития других протоколов, например, шифрования данных для передачи сообщений.

Производилось объединение локальных сетей с помощью кабеля. Это позволило на небольшом расстоянии создавать локальную сеть, в которой могли бы взаимодействовать различные люди и техника. Например, взаимодействие работников в офисе с базой данных на сервере.

Но в ближайшее время часто поднимается вопрос о расширении локальной сети и её доступности на удаленном расстоянии через интернет. Это

побудило к разработке VPN – сетей. Главной задачей VPN – протоколов было создание удаленной локальной сети между компьютерами на производстве.

Поэтому были разработаны различные протоколы VPN – сетей. Существуют VPN – сети, которые представляют собой технологии, позволяющие обеспечить одно или несколько сетевых соединений. Они очень эффективны, так как позволяют создавать виртуальные сети поверх других небезопасных сетей, благодаря использованию средств криптографии (аутентификации, шифрования, средств для защиты от повторов и изменений).

VPN – сеть позволяет создавать соединение с узлом сервера, в последствии который может выдавать IP адрес из пула локальных IP адресов сервера, что дает возможность получение и отправку информации через провайдера данного сервера. Это позволяет условно менять местонахождение устройства. Также, при использовании шифрования VPN – соединения, можно защититься от несанкционированного доступа к передаваемой информации.

VPN представляет собой объединение отдельных машин или локальных сетей в виртуальную сеть, которая обеспечивает целостность и безопасность передаваемых данных. Она обладает свойствами выделенной частной сети и позволяет передавать данные между двумя компьютерами через промежуточную сеть (internetwork), например, Internet. [3, 4]

VPN имеет некоторое преимущество перед другими удаленными соединениями. Основным фактором является экономичность. Это позволяет не покупать выделенную линию у провайдера, предоставляющего доступ в интернет. И еще одним фактом является обращение пользователей к корпоративной сети без использования коммутируемого соединения.

VPN состоит из двух частей: «внутренняя» (подконтрольная) сеть, которых может быть несколько, и «внешняя» сеть, по которой проходит инкапсулированное соединение (обычно используется Интернет) [3, 4].

Существует различные виды VPN-сетей:

- ***VPN*** (***Virtual Private Network*** – виртуальная частная сеть) – обобщённое название технологий, позволяющих обеспечить одно или

несколько сетевых соединений IPSec (IP security) – часто используется поверх IPv4.

- ***PPTP*** (***point-to-point tunnel in g protocol***) – разрабатывался совместными усилиями нескольких компаний, включая Microsoft.
- ***PPPoE*** (***PPP*** (***Point-to-Point Protocol***) over Ethernet)
- ***L2TP*** (***Layer 2 Tunnelling Protocol***) – используется в продуктах компаний Microsoft и Cisco.
- ***Open VPN SSL VPN*** с открытым исходным кодом, поддерживаетрежимы PPP, bridge, point-to-point, multi-client server

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) [5].

Протокол PPTP обеспечивает безопасную передачу данных от удаленного клиента к отдельному серверу предприятия путем создания в сети TCP/IP частной виртуальной сети. Он может также использоваться для организации туннеля между двумя локальными сетями. Этот протокол работает, устанавливая обычную PPP-сессию с противоположной стороной с помощью протокола Generic Routing Encapsulation (GRE). Второе соединение на TCP порта 1723 используется для инициации и управления GRE-соединением. Для защиты данных PPTP-траффика может быть использован ещё один протокол MPPE.

Ещё один протокол L2TP (Layer 2 Tunneling Protocol) – это протокол канального уровня, который осуществляет туннелирование. Он 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 [6].

Протокол L2TP использует сообщения двух типов: управляющие и информационные сообщения. 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 [6].

Структура этого протокола описывает передачу кадров PPP и управляющих сообщений по управляющему каналу и каналу данных протокола L2TP. Кадры PPP передаются по ненадежному каналу данных, предварительно дополняясь заголовком L2TP, а затем – по транспорту для передачи пакетов, такому как Frame Relay, ATM и т.п. Управляющие сообщения передаются по надежному управляющему каналу L2TP с последующей передачей по тому же транспорту для пересылки пакетов [6].

Все управляющие сообщения должны содержать порядковые номера, используемые для обеспечения надежной доставки по управляющему каналу. Информационные сообщения могут использовать порядковые номера для упорядочивания пакетов и выявления утерянных пакетов [6].

Существует ещё набор протоколов IPSec (IP Security), которые касаются 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, то есть на третьем уровне модели OSI [6].

Internet-протокол (IP) не имеет средств защиты передаваемых данных. Он даже не может гарантировать, что отправитель является именно тем, за кого он себя выдает. Протокол IPSec представляет собой «попытку» исправить ситуацию. При его использовании весь передаваемый трафик может быть защищен перед передачей по сети. При использовании IPSec получатель сообщения может отслеживать 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 может повторять ее снова). 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. Необходимо обеспечить невозможность повторной передачи такого трафика [6].

Open VPN является достаточно новой технологией с открытым кодом, которая использует библиотеку Open SSL и протоколы SSLv3/TLSv1, наряду с множеством других технологий для обеспечения надежного VPN-решения. Одним из его главных преимуществ является то, что Open VPN очень гибок в настройках. Этот протокол может быть настроен на работу на любом порту, в том числе на 443 TCP-порту, что позволяет маскировать трафик внутри Open VPN под обычный HTTPS (который использует, например, Gmail) и поэтому его трудно заблокировать [7].

Open VPN стал технологией «номер один» при использовании VPN, и хотя он изначально не поддерживается операционными системами, этот протокол широко поддерживается через стороннее программное обеспечение.

В результате проведённого автором обзора по VPN - сетям, была составлена их классификация по следующим исследованным свойствам, которые отражены на рисунке 1 [4].

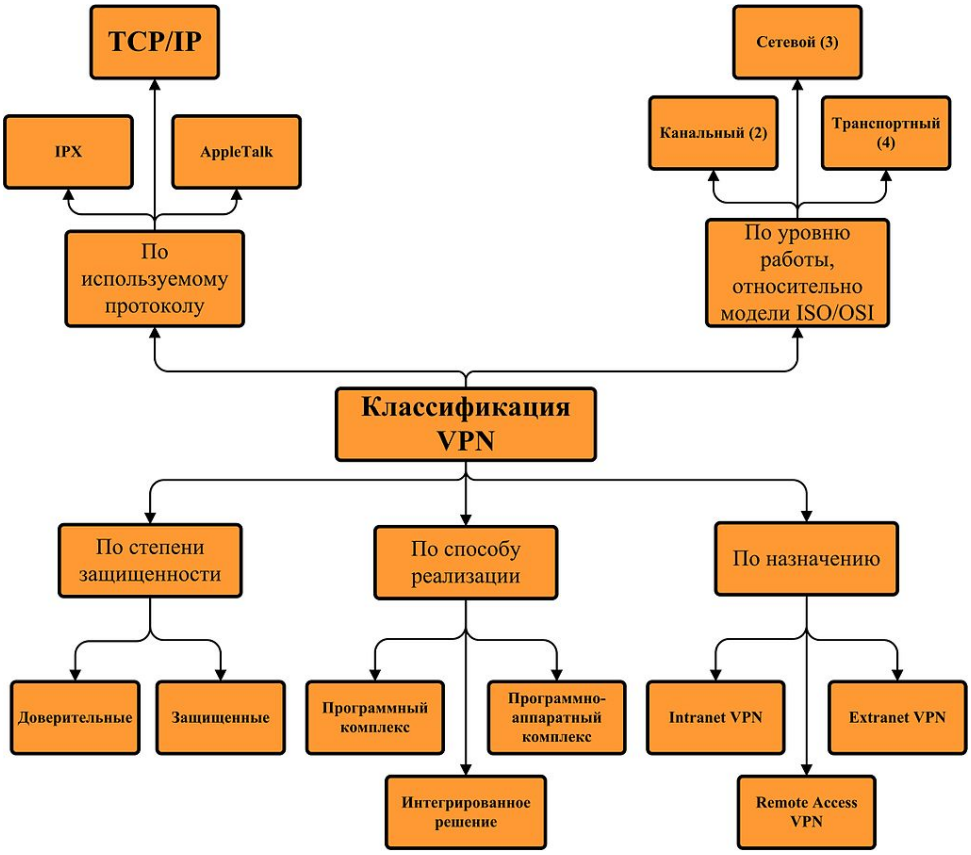

Рисунок 1 – Классификация современных VPN-сетей

Исходя из видов VPN – сетей, пользователь может выбирать конкретный протокол для решения поставленной задачи. Для среднестатистического пользователя можно рассматривать такие протоколы как ***PPTP*** и ***L2TP***. Они очень схожи между собой, но протокол ***L2TP*** более требователен к вычислительным ресурсам пользователя. Оба протокола по умолчанию не предполагают шифрования и обычно используются совместно с протоколом IPSec.

Но для создания максимально быстрого VPN-соединения можно использовать протокол ***PPTP*** для подключения к локальной сети через интернет для различных нужд, например, для получения доступа к сетевому диску или принтеру, что сохранит коммерческие и личные данные от несанкционированного копирования.

ЛИТЕРАТУРА

1. Попова О.Б. База данных раздела «Вычислительные системы» курса лекций «Вычислительные системы, сети и телекоммуникации» // Программы для ЭВМ. Базы данных. Топологии интегральных микросхем. 2015. №9. С. 88.

2. Попова О.Б. База данных раздела «Телекоммуникации» курса лекций «Вычислительные системы, сети и телекоммуникации» // Программы для ЭВМ. Базы данных. Топологии интегральных микросхем. 2015. №9. С. 72.

3. Попова О.Б. База данных раздела «Сети» курса лекций «Вычислительные системы, сети и телекоммуникации» // Программы для ЭВМ. Базы данных. Топологии интегральных микросхем. 2015. №9. С. 87.

4. WikipediaVPN - [Электронный ресурс] – Режим доступа: http://ru.wikipedia.org/wiki/VPN

5. Что такое VPN технология - [Электронный ресурс] – Режим доступа: http://setkrugom.narod.ru/index3.html

6. Виды VPN-соединений (PPTP, L2TP, IPSec, SSL) - [Электронный ресурс] – Режим доступа: http://https://zyxel.ru/kb/1638/

7. PPTPvsL2TPvsOpenVPNvsSSTP - [Электронный ресурс] – Режим доступа: http://habrahabr.ru/post/191874/

REFERENCES

1. Popova O.B. Baza dannykh razdela «Vychislitelnye sistemy» kursa lektsiy «Vychislitelnye sistemy, seti i telekommunikatsii» // Programmy dlya EVM. Bazy dannykh. Topologii integralnykh mikroskhem. 2015. №9. S. 88.

2. Popova O.B. Baza dannykh razdela «Telekommunikatsii» kursa lektsiy «Vychislitelnye sistemy, seti i telekommunikatsii» // Programmy dlya EVM. Bazy dannykh. Topologii integralnykh mikroskhem. 2015. №9. S. 72.

3. Popova O.B. Baza dannykh razdela «Seti» kursa lektsiy «Vychislitelnye sistemy, seti i telekommunikatsii» // Programmy dlya EVM. Bazy dannykh. Topologii integralnykh mikroskhem. 2015. №9. S. 87.

4. WikipediaVPN - [Elektronnyy resurs] – Rezhim dostupa: http://ru.wikipedia.org/wiki/VPN

5. Chto takoe VPN tekhnologiya - [Elektronnyy resurs] – Rezhim dostupa: http://setkrugom.narod.ru/index3.html

6. Vidy VPN-soedineniy (PPTP, L2TP, IPSec, SSL) - [Elektronnyy resurs] – Rezhim dostupa: http://https://zyxel.ru/kb/1638/

7. PPTPvsL2TPvsOpenVPNvsSSTP - [Elektronnyy resurs] – Rezhim dostupa: http://habrahabr.ru/post/191874/

MODERN VPN – NETWORKS

V.V. MAYOROV

Kuban State Technological University,
2, Moskovskaya st., Krasnodar, Russian Federation, 350002;
e-mail: mayorovvladislav@outlook.com

The article is devoted to modern VPN – networks. This issue is very topical at the moment. This is mainly due to security on the Internet. These security measures are used as a company, as well as ordinary users. This allows staff to work remotely and use the company's data. Degrees of VPN security – different networks, which means a different focus on the consumption of the virtual network. When using encryption VPN - connection, you can protect yourself from unauthorized access to the transmitted information. In recent years, increasingly raised the issue of anonymity on the Internet. The article provides a brief analysis of the most important protocols VPN - connections. In this regard, the information reflected in the peer-reviewed article, timely and relevant.

Key words: VPN - Network, PPTP, L2TP, IPSec, OpenVPN, the global Internet.