УДК 004.738.2

ТЕХНОЛОГИИ VPN ДЛЯ КОРПОРАТИВНЫХ СЕТЕЙ

Кучинский П.С., студент гр.763102

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Давыдова Н.С. – канд. тех. наук., доцент

Аннотация. В работе представлен анализ возможных реализаций сети предприятия на базе технологий VPN.

Ключевые слова. Виртуальная частная сеть, VPN, VPN-шлюз, VPN-клиент, VPN-сервер, Site-to-Site VPN, Remote Access VPN.

VPN (Virtual Private Network) – это логическая сеть на базе виртуальных туннелей, создаваемая поверх другой коммуникационной сети. При этом, даже если коммуникации осуществляются по публичным сетям с использованием небезопасных протоколов, то за счёт шифрования создаются закрытые от посторонних каналы обмена информации и обеспечивается конфиденциальность и целостность данных. Доступ к такому виртуальному туннелю должен быть чрезвычайно затруднен всем возможным активным и пассивным внешним наблюдателям. VPN позволяет объединить, например, несколько офисов организации в единую сеть с безопасной передачей информации через Интернет [1].

Для создания виртуальной частной сети крупного предприятия нужны VPN-шлюзы, VPN-серверы и VPN-клиенты. VPN-шлюзы целесообразно использовать для защиты локальных сетей предприятия, VPN-серверы и VPN-клиенты используют для организации защищенных соединений удаленных и мобильных пользователей с корпоративной сетью через Интернет.

VPN-клиент представляет собой программный или программно-аппаратный комплекс, выполняемый обычно на базе персонального компьютера. Его сетевое программное обеспечение модифицируется для выполнения шифрования и аутентификации трафика, которым это устройство обменивается с другими VPN-клиентами, VPN-серверами или шлюзами безопасности VPN.

VPN-сервер представляет собой программный или программно-аппаратный комплекс, выполняющий функции сервера. VPN-сервер обеспечивает защиту серверов от несанкционированного доступа из внешних сетей, а также организацию защищенных соединений с отдельными компьютерами и с компьютерами из сегментов локальных сетей, защищенных соответствующими VPN-продуктами.

Шлюз безопасности VPN – это сетевое устройство, подключаемое к двум сетям и выполняющее функции шифрования и аутентификации для многочисленных хостов, расположенных за ним. Шлюз безопасности VPN должен быть размещен так, чтобы через него проходил весь трафик, предназначенный для внутренней корпоративной сети.

Классифицировать VPN решения можно по нескольким основным параметрам [2]:

– по типу используемой среды:

1 Защищённые VPN сети. Наиболее распространённый вариант приватных частных сетей. С его помощью возможно создать надежную и защищенную подсеть на основе ненадёжной сети, как правило, Интернета. Примером защищённых VPN являются: IPSec, OpenVPN и PPTP.

2 Доверительные VPN сети. Используются в случаях, когда передающую среду можно считать надёжной и необходимо решить лишь задачу создания виртуальной подсети в рамках большей сети. Вопросы обеспечения безопасности становятся неактуальными. Примерами подобных VPN решении являются: MPLS и L2TP. Эти протоколы перекладывают задачу обеспечения безопасности на другие, например L2TP, который как правило, используется в паре с IPSec.

– по способу реализации:

1 VPN сети в виде специального программно-аппаратного обеспечения. Реализация VPN сети осуществляется при помощи специального комплекса программно-аппаратных средств. Такая реализация обеспечивает высокую производительность и, как правило, высокую степень защищённости.

2 VPN сети в виде программного решения. Используют персональный компьютер со специальным программным обеспечением, обеспечивающим функциональность VPN.

3 VPN сети с интегрированным решением. Функциональность VPN обеспечивает комплекс, решающий также задачи фильтрации сетевого трафика, организации сетевого экрана и обеспечения качества обслуживания.

– по назначению: Site-to-Site VPN, Remote Access VPN

Соединение «точка-точка» (Site-to-Site) применяется для подключения всей локальной сети в одной локации к локальной сети в другой. Стандартный сценарий – подключение удаленных филиалов к центральному офису или дата-центру компании. При этом не требуется установка VPN-клиентов на устройства пользователей, так как соединение обрабатывает VPN-шлюз, и передача данных между устройствами в разных сетях происходит прозрачно. При использовании VPN типа Site-to-Site шлюз VPN одной удаленной локальной сети взаимодействует со шлюзом другой локальной сети для создания безопасного туннеля. Удаленным устройствам не нужен VPN-клиент, они отправляют обычный трафик через шлюзы VPN. Схема VPN-соединения Site-to-Site представлена на рисунке 1.

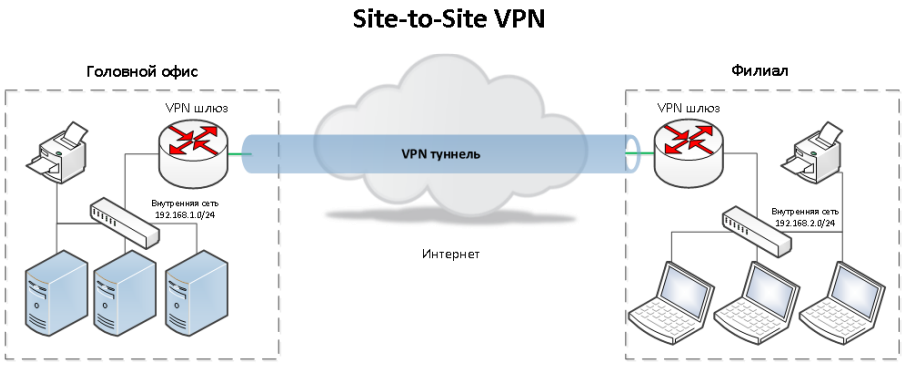

Рисунок 1 – Схема VPN-соединения Site-to-Site

VPN удаленного доступа (Remote access VPN) используется для предоставления сотрудникам компании безопасного доступа к корпоративной сети и ее ресурсам через публичную сеть Интернет. Это особенно актуально, когда для подключения к Интернету используется общественная точка доступа Wi-Fi или другие небезопасные способы подключения. Для Remote access VPN также необходимо, чтобы на устройстве было установлено клиентское программное обеспечение. Это программное обеспечение VPN-клиента взаимодействует со шлюзом VPN, на котором производится аутентификация и авторизация пользователя и создает защищенный «виртуальный» туннель между локальной сетью и шлюзом. После успешного прохождения этой процедуры пользователь получает доступ к внутренним сетевым ресурсам (файловый сервер, базы данных, принтеры и другие) так, будто он подключен к локальной сети. Схема VPN-соединения Remote access представлена на рисунке 2.

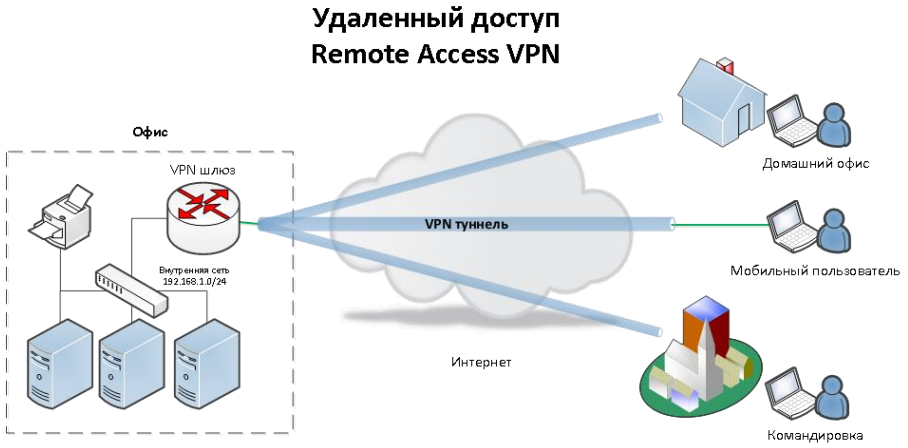

Рисунок 2 – Схема VPN-соединения Remote access

Стоит так же учитывать, что VPN можно различать по средствам реализации:

– VPN на базе сетевой ОС;

– VPN на базе программного обеспечения;

– VPN на базе маршрутизаторов;

– VPN на базе брандмауэров;

- VPN на базе аппаратных средств.

К средствам VPN, выполненным в виде автономного ПО относятся и VPN-шлюзы, и VPN-клиенты. Многие компании-производители аппаратных шлюзов дополняют линейку своих продуктов чисто программной реализацией VPN-клиента, который рассчитан на работу в среде стандартной ОС. Что касается программных шлюзов (иногда они называются также «сервера защищенных каналов»), то производители как правило нагружают их некоторыми

дополнительными функциями по защите данных, например: функциями по фильтрации траффика и контролю доступа, свойственными брандмауэру. Поэтому граница между брандмауэрами со встроенными функциями VPN и программными VPN-шлюзами очень размыта. Например, таким продуктом является RRAS (Routing and Remote Access Service). RRAS включает в себя усовершенствованный программный многопротокольный маршрутизатор, который поддерживает протоколы маршрутизации RIP и OSPF из TCP/IP. RRAS может быть использован как VPN-шлюз при взаимодействии «сеть-сеть» [3].

VPN на базе сетевой ОС. Примером являются системы Windows. Для создания VPN используется протокол PPTP, который интегрирован в систему Windows [4]. Данное решение очень привлекательно для организаций, использующих Windows в качестве корпоративной операционной системы. Необходимо отметить, что стоимость такого решения значительно ниже стоимости прочих решений. В работе VPN на базе Windows используется база пользователей NT, хранящаяся на Primary Domain Controller (главный контроллер домена) (PDC). При подключении к PPTP-серверу пользователь аутентифицируется по протоколам PAP, CHAP или MS-CHAP. Передаваемые пакеты инкапсулируются в пакеты GRE/PPTP. Для шифрования пакетов используется нестандартный протокол от Microsoft Point-to-Point Encryption с 40 или 128 битным ключом, получаемым в момент установки соединения. Недостатками данной системы являются отсутствие проверки целостности данных и невозможность смены ключей во время соединения. Положительными моментами являются легкость интеграции с Windows и низкая стоимость.

VPN на базе маршрутизаторов применяется для создания защищенных каналов маршрутизаторов. Так как вся информация, исходящая из локальной сети, проходит через маршрутизатор, то на маршрутизатор можно возложить и задачи шифрования. Примером оборудования для построения VPN на маршрутизаторах является оборудование компании «Cisco». Начиная с версии программного обеспечения IOS 11.3, маршрутизаторы Cisco поддерживают протоколы L2TP и IPSec. Помимо простого шифрования проходящей информации Cisco поддерживает и другие функции VPN, такие как идентификация при установлении туннельного соединения и обмен ключами.

VPN на базе брандмауэров. Брандмауэры большинства производителей поддерживают туннелирование и шифрование данных. К программному обеспечению брандмауэра добавляется модуль шифрования. Недостатком этого метода можно назвать зависимость производительности от аппаратного обеспечения, на котором работает брандмауэр. При использовании брандмауэров на базе ПК надо помнить, что подобное решение можно применять только для небольших сетей с небольшим объемом передаваемой информации.

Вариант построения VPN на специальных устройствах может быть использован в сетях, требующих высокой производительности. Выделенные аппаратные шлюзы реализованы в виде отдельного аппаратного устройства, основная функция которого – высокопроизводительное шифрование траффика. VPN-устройства являются фактическими лидерами практически по всем показателям, кроме одного – стоимости. Аппаратные шлюзы высшего класса обязательно поддерживают IPsec, причем со многими расширениями в виде новых и мощных в криптографическом отношении алгоритмов. Обладают высокой производительностью за счет аппаратной поддержки операций шифрования. По удобству и простоте инсталляции, аппаратные шлюзы обычно намного превосходят программные шлюзы и такие комбинированные решения, как шлюзы на основе брандмауэров и маршрутизаторов. Аппаратное устройство уже при включении готово работать, ему не надо проходить громоздкий процесс инсталляции в среде какой-либо ОС, как это требуется для большинства программных или комбинированных продуктов, а для работы необходимо только задать значения конкретных адресов и, может быть, ключей для установления тоннелей.

Описанная выше классификация позволяет реализовывать VPN сети различными способами, каждый из которых имеет свои преимущества и недостатки в зависимости от требований к сети. При выборе решения требуется учитывать факторы производительности средств построения VPN. Для построения VPN лучше всего использовать специализированное оборудование, однако если имеется ограничение в средствах, то можно обратить внимание на чисто программное решение [5].

Таким образом, основными достоинствами использования VPN-технологий для защиты информации в распределенных корпоративных сетях являются:

1 Возможность защиты всей корпоративной сети.

2 Масштабируемость системы защиты.

3 Использование ресурсов открытых сетей в качестве отдельных коммуникационных звеньев корпоративной сети; все угрозы, возникающие при использовании сетей общего пользования, будут компенсироваться средствами защиты информации.

4 Обеспечение подконтрольности работы сети и достоверная идентификация всех источников информации.

5 Сегментация информационных систем и организация безопасной эксплуатации системы, обрабатывающей информацию различных уровней конфиденциальности, программными и программно-аппаратными средствами защиты информации.

Список использованных источников:

1. Scott C., Wolfe P., Erwin M. Virtual private networks. – O'Reilly Media Inc., 1999. P. – 225.

2. Николахин А. Ю., Использование технологии vpn для обеспечения информационной безопасности //Экономика и качество систем связи. – 2018. – №. 3.

3. Казиева Г. С., Мухамеджанова А. Д. НЕКОТОРЫЕ АСПЕКТЫ ТЕХНИЧЕСКОЙ РЕАЛИЗАЦИИ VPN //Научно-Технического Общества «КАХАК». – 1998. – С. 88.

4. VPN на базе аппаратных средств [Электронный ресурс]. – Режим доступа: https://helpiks.org/4-69912.html.

5. Березин А., Петренко С. Построение корпоративных защищенных виртуальных частных сетей //Сетевой журнал. – 2001. – №. 1.