Министерство образования и науки Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ
Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра дискретной математики и
информационных технологий

Реализация и обеспечение безопасности VPN в корпоративной среде

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса 421 группы
направления 09.03.01 «Информатика и вычислительная техника»
факультета компьютерных наук и информационных технологий
Егорова Олега Вадимовича

Научный руководитель
к. ф.-м.н., доцент _____ В.А. Поздняков
подпись, дата

Зав. кафедрой
к. ф.-м.н., доцент _____ Л.Б. Тяпаев
подпись, дата

Саратов 2017

ВВЕДЕНИЕ

В настоящее время технологии построения виртуальных защищенных частных сетей (VPN) активно используются различных компаниях (банков, ведомств, крупных государственных структур и т. д.). Причина такого интереса заключается в том, что VPN-технологии действительно дают возможность не только существенно сократить расходы на содержание выделенных каналов связи с удаленными филиалами, но и повысить конфиденциальность обмена информацией без необходимости выделения отдельных каналов связи.

Кроме того, если людям потребуется доступ к своей информации, хранящейся на их домашнем компьютере, или на компьютере фирмы. Эту проблему можно решить, организовав удалённый доступ к нему с помощью VPN. Преимущества технологии VPN в том, что организация удалённого доступа делается не через телефонную линию, а через Internet, что намного дешевле и безопаснее. И потому VPN представляют интерес для крупных компаний и весьма актуальны в настоящее время.

Целью бакалаврской работы является практическая реализация VPN в корпоративной среде и обеспечение её безопасности. Для достижения этой цели были сформулированы следующие задачи:

1. Изучить различные способы реализации VPN
2. Сделать сравнительный обзор технологий VPN и выбрать оптимальную
3. Реализовать выбранную технологию
4. Обеспечить безопасность VPN

Работа состоит из введения, четырёх глав, заключения и списка использованных источников.

Во введении бакалаврской работы приводятся общие сведения, актуальность темы, цели и задачи работы. В первой главе даются основные определения VPN (виртуальной частной сети) и рассказывается про компоненты её формирующие. Во второй главе приведен сравнительный обзор технологий VPN и выбрана оптимальная. В третей главе находится постановка задачи для практики и первая часть практики (развёртывание OpenVPN сервера). В

четвертой главе описана вторая часть практики и представлены использованные на практике дополнительные возможности OpenVPN для обеспечения безопасности виртуальной частной сети. В заключении сделаны выводы о проделанной работе. Список использованной литературы содержит источники, на которые приводятся ссылки в работе.

Основное содержание работы

1 Технология VPN и её компоненты

Термин “виртуальные частные сети” (VPN, Virtual Private Networks) возник в начале 1997 г. Базисной технологией, используемой в виртуальных частных сетях, является стек протоколов TCP/IP, который был разработан в 60-х годах.

VPN – это зашифрованный или инкапсулированный процесс коммуникации, который безопасным образом передает данные из одной точки в другую; безопасность этих данных обеспечена устойчивой технологией шифрования, и передаваемые данные проходят через открытую, незащищенную, маршрутизируемую сеть.

Замечательным свойством технологии VPN является её масштабируемость. По мере того как провайдеры сетевых услуг увеличивают полосу пропускания на своих магистралях, VPN тоже могут расти, чтобы пользоваться этой полосой. Так как VPN не зависят от платформы и не опираются на определённую операционную систему, почти любое устройство в компании может функционировать либо как VPN клиент, либо как сервер. VPN также предоставят пространство для собственного роста, большинство устройств VPN смогут управлять любыми службами, размещенными на них. Они позволяют по запросу создавать туннели или сквозную передачу с шифрованием. Создавать туннели к другим узлам, например, туннель между корпоративным центральным офисом и основными офисами сбыта, а позже дополнительные туннели для других офисов.

Сеть VPN состоит из пяти ключевых компонентов:

- Сервер VPN
- VPN-клиент
- Алгоритмы шифрования
- Система аутентификации
- Протокол VPN

Эти компоненты реализуют соответствие требованиям по безопасности, производительности и способности к взаимодействию.

2 Сравнительный обзор технологий VPN

Сравнительный обзор выполнен для следующих технологий:

- PPTP (Point-to-Point tunneling protocol)
- IPSec (IP Security)
- L2TP (Layer 2 Tunneling Protocol) и L2TP+IPSec
- SSTP (Secure Socket Tunneling Protocol)
- OpenVPN

Подробнее плюсах и минусах каждой технологии написано в дипломе. Я же выбрал OpenVPN поскольку его можно назвать оптимальным выбором для большинства стандартных пользовательских задач поскольку в этой реализации сбалансированы:

- Скорость: за счет сжатия LZO и возможности работы по протоколу UDP
- Стабильность: особенно при работе через TCP
- Гибкость конфигурации: предусмотрены дополнительные опции, например, балансировка нагрузки, различные типы аутентификации
- Кроссплатформенность: наличие клиентских приложений для большинства современных ОС, в т.ч. мобильных
- Безопасность: благодаря работе со всеми инструментами библиотеки openssl

Сами перечисленные выше широкие возможности порождают и недостаток OpenVPN – первичная конфигурация может оказаться сложнее, чем в случае с другими реализациями.

Так или иначе, реализация OpenVPN является самым сбалансированным решением, хотя с точки зрения безопасности она, возможно, может конкурировать с IPsec/L2TP.

3 Развертывание OpenVPN сервера

Задача в данном случае сводиться к тому, чтобы компьютеры PC1 и PC2 на рисунке 1 могли совместно использовать свои сетевые ресурсы в обе стороны через VPN туннель. То есть как за сервером, так и за клиентом сеть должна быть видна.

На рисунке 1 представлена схема сети:

WinServ – сервер главного офиса, ОС Windows Server 2012 r2

WinClient – сервер филиала, ОС Windows Server 2012 r2

PC1/PC2 – ОС Windows 7

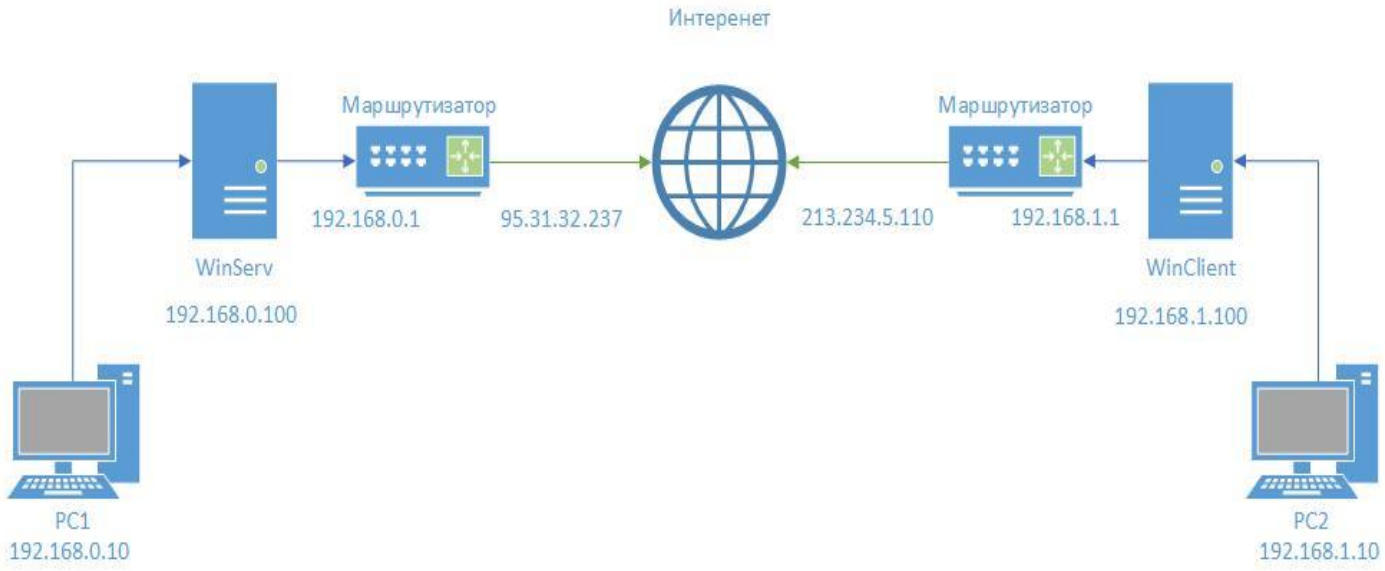

Рисунок 1 – Схема сети

В таблице 1 представлено описание схемы сети:

Таблица 1 – Описание схемы сети

Имя	WinServ	Router1	WinClient	Router2
Внешний ip		95.31.32.237		213.234.5.110
Локальный ip	192.168.1.100	192.168.0.1	192.168.1.100	192.168.1.1
Комментарий	Сервер OpenVPN	Шлюз	Клиент OpenVPN	Шлюз

Для решения данной задачи была выбрана технология OpenVPN.

Процесс развертывания OpenVPN-сети состоял из следующих этапов:

- определение диапазона адресного пространства и правил адресации узлов сети;
- предварительная настройка серверов;
- установка программного пакета OpenVPN на серверы;

- генерирование сертификатов и ключей сервера и клиента;
- формирование файла конфигурации сервера OpenVPN;
- формирование набора файлов конфигурации клиентов;
- настройка шлюзов;
- запуск сервера OpenVPN;
- настройка OpenVPN-клиента;
- проверка подключения настроенного клиента к серверу OpenVPN.

Результат работы VPN со стороны сервера представлен на рисунке 2, со стороны клиента на рисунке 3.

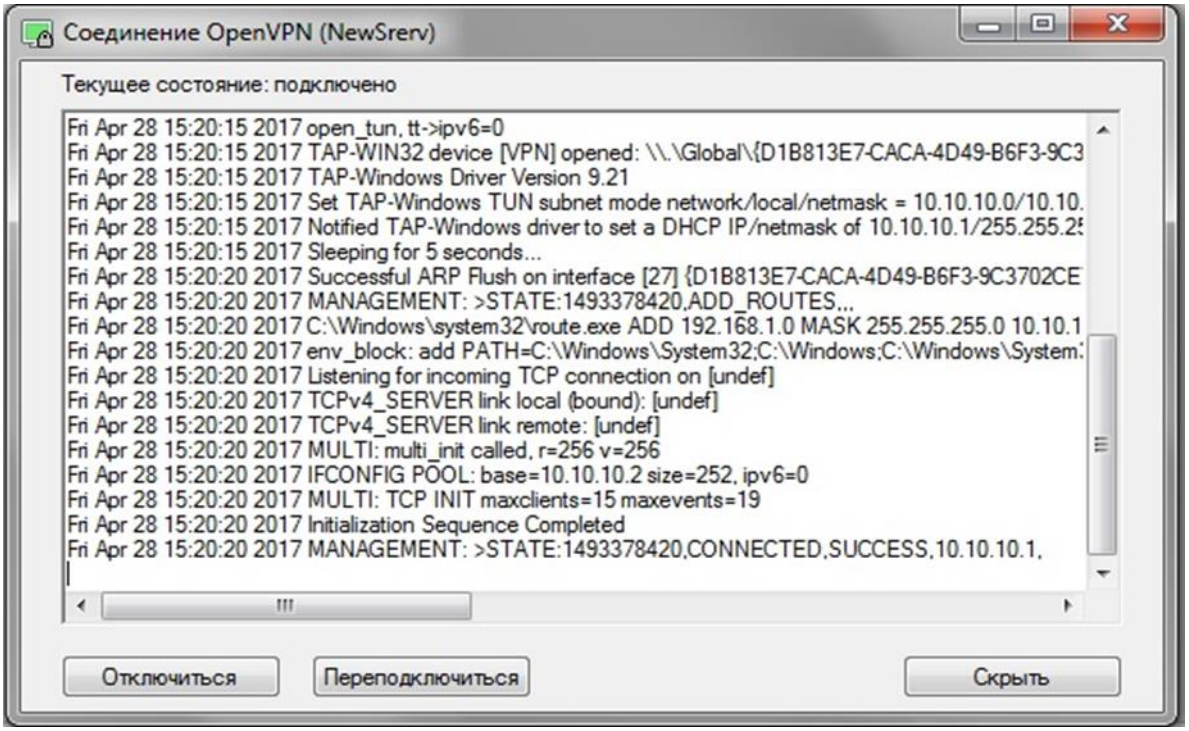

Рисунок 2 – Успешный запуск сервера OpenVPN

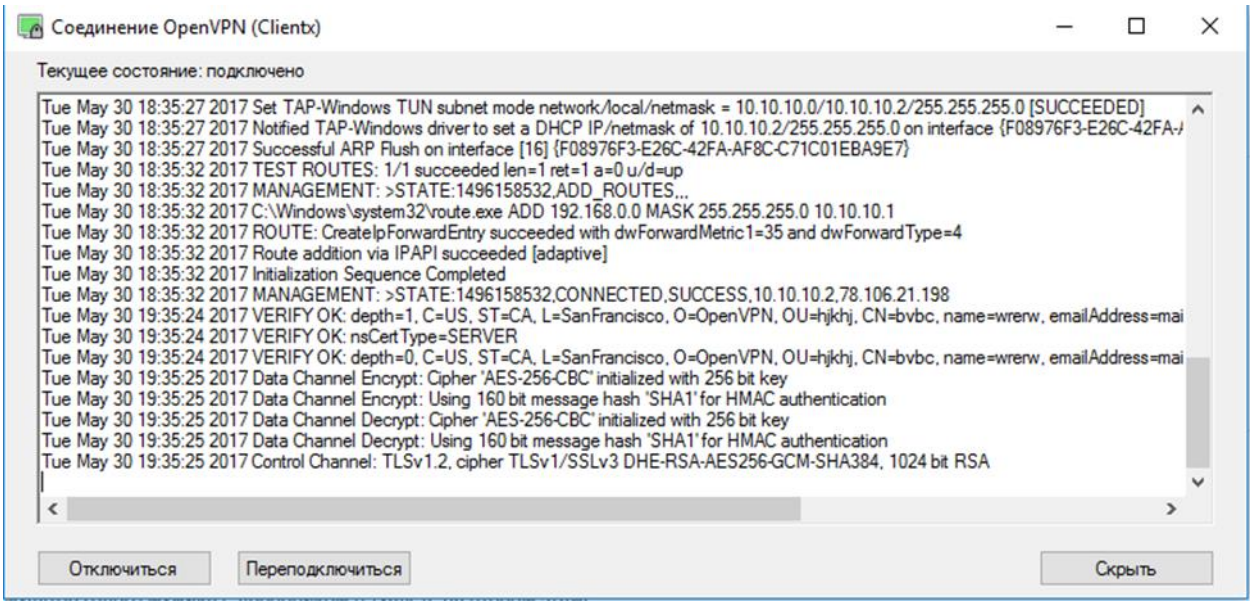

Рисунок 3 – Успешное подключение клиента к серверу

Таким образом была успешно установлена связь между сетью главного офиса и его филиалом при помощи технологии OpenVPN.

4 Обеспечение безопасности VPN

После того как сервер OpenVPN был настроен. Можно приступить к обеспечению его безопасности.

В OpenVPN присутствуют дополнительные инструменты для обеспечения безопасности. Ниже приведен список основных использованных опций.

- HMAC (hash-based message authentication code)
- Увеличение размера RSA-ключа
- Увеличение размера симметричных ключей
- Хранение закрытого ключа CA на отдельной машине
- Отзыв сертификатов
- Валидация серверного сертификата

Перечисленные выше инструменты были использованы для повышения уровня безопасности виртуальной частной сети, однако следует так же обращать внимание на сохранность других элементов: используемых каналов передачи ключей и сертификатов, физическую сохранность узлов сети VPN.

ЗАКЛЮЧЕНИЕ

За время выполнения бакалаврской работы, была изучена специальная литература, сделан обзор основных технологии VPN. Описаны основные понятия, использующиеся в данной работе. В соответствии с планом, было реализовано VPN соединение между главным офисом и его филиалом, с помощью технологии OpenVPN и обеспечена безопасность VPN с помощью дополнительных инструментов. Что и являлось основной целью бакалаврской работы.

Таким образом, все поставленные задачи были в полном объеме решены.