МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»
Кафедра дискретной математики и информационных технологий

РЕАЛИЗАЦИЯ VPN-СЕРВЕРА НА ОСНОВЕ ОТКРЫТЫХ ТЕХНОЛОГИЙ

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса 421 группы
направления 09.03.01 — Информатика и вычислительная техника
факультета КНиИТ
Погорельцева Дмитрия Витальевича

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

Заведующий кафедрой
доцент, к. ф.-м. н. _____ Л. Б. Тяпаев

Саратов 2023

ВВЕДЕНИЕ

Актуальность темы обеспечения безопасности в сетевом взаимодействии является одним из ключевых вопросов в информационных технологиях. В связи с этим, реализация VPN-сервера является одним из наиболее актуальных направлений развития сетевых технологий с целью обеспечения безопасного и надежного удаленного доступа к информационным ресурсам. Объект и предмет исследования - проектирование и реализация VPN-сервера на основе открытых технологий. Методы исследования включают в себя анализ существующих решений, выбор наиболее оптимальных компонентов, создание конфигураций VPN-сервера с использованием открытых технологий. Цель работы - реализация VPN-сервера на основе открытых технологий с целью обеспечения безопасного удаленного доступа к информационным ресурсам. Задачи работы включают в себя изучение существующих VPN-решений, выбор платформы, выбор необходимых компонентов, создание конфигураций, тестирование и оценку результатов.

Теоретическая и/или практическая значимость бакалаврской работы. Данная бакалаврская работа представляет собой исследование и реализацию комплексной системы VPN с использованием самых современных и открытых технологий, а именно: Ubuntu, WireGuard и Termius.

В работе были сформулированы цели и задачи, связанные с реализацией VPN сервера, были изучены теоретические основы VPN, проведен анализ наиболее популярных технологий в области виртуальных частных сетей. Для решения поставленных задач были использованы технологии и программные продукты, указанные выше, а именно: система Ubuntu для хостинга, WireGuard для организации VPN-туннелей и Termius для удаленного управления сервером.

Была выполнена полная настройка сервера VPN включая подключение клиентских устройств к виртуальной частной сети. Также были проведены эксперименты, которые показали высокую производительность системы VPN на базе WireGuard.

В результате выполнения дипломной работы был создан функциональный и эффективный VPN-сервер на базе открытых технологий, что демонстрирует применимость этих технологий в реальной среде. Результаты данной работы могут быть полезны для специалистов в области информационной

безопасности, а также для всех, кто заинтересован в обеспечении безопасной передачи данных.

Структура и объем работы. Бакалаврская работа состоит из введения, четырех глав, заключения, списка использованных источников. Общий объем работы - 40 страниц, из них 38 страниц - основное содержание, включая 42 рисунка, список использованных источников информации - 20 наименований.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Первый раздел "Теоретические основы" посвящен непосредственно необходимой теории. Определения VPN - VPN — это аббревиатура технологии, которая расшифровывается как Virtual Private Network, то есть - виртуальная частная сеть. Данная технология обеспечивает безопасную и защищенную передачу данных через открытую интернет-сеть или другую сеть, которая не является частной. С VPN-сетью, удаленные пользователи могут получать доступ к внутренним корпоративным ресурсам через зашифрованный канал.

Также рассматривался принцип работы VPN сервера - VPN работает по принципу создания защищенного канала между удаленным клиентом и целевой сетью. Когда пользователь подключается к VPN, его интернет-соединение перенаправляется через VPN-сервер, который шифрует данные и пересылает их через открытый интернет.

Помимо этого были рассмотрены типы VPN, а именно "Удаленный доступ"и "Сайт к сайту". Удаленный доступ - этот тип VPN обеспечивает удаленный доступ к корпоративным ресурсам защищенным туннелем. Это означает, что пользователь (например, сотрудник) должен иметь специальный клиентский софт на своем компьютере, который дает ему возможность подключиться к VPN-серверу. Таким образом, сотрудник может работать из любого места, подключаясь к сети компании и получая доступ к её ресурсам. Недостатком такого типа является потребность временной интеграции, что может быть трудным, если пользователи работают на нескольких устройствах. Сайт-к-сайту - этот тип VPN используется для соединения нескольких локальных сетей в единую общую сеть. Сайт-к-сайту VPN работает, когда сеть одной компании соединяется с другой компанией. Это позволяет обоим компаниям работать с общими ресурсами, выгодно сотрудничать .

Недостатками такого типа являются:

— Большой объем работы по настройке VPN-сервера;

— Общая сеть может быть уязвимой, если обе компании не будут следить за безопасностью.

Также были рассмотрены основные протоколы такие как PPTP,IPsec,OpenVpn, и WireGuard.

И открытые технологии, которые включают в себя:

— OpenVPN

— SoftEther VPN

— WireGuard.

OpenVPN - это открытое программное обеспечение, которое позволяет создавать виртуальные частные сети (VPN), используя протокол SSL/TLS, он обеспечивает высокую степень конфиденциальности и безопасности, защищает данные от кражи, мониторинга и несанкционированного доступа.

OpenVPN поддерживает разные методы аутентификации, включая сертификаты, пароли и ключи.

SoftEther VPN - это бесплатное многоплатформенное программное обеспечение для создания VPN-соединений. SoftEther VPN обеспечивает безопасность передачи данных, как при использовании протоколов SSL/TLS, так и при использовании протоколов L2TP/IPsec и EtherIP.

Одной из главных особенностей SoftEther VPN является высокая скорость передачи данных. Он использует новый протокол VPN, который называется SoftEther VPN Protocol, который предлагает высокую производительность, надежность и безопасность. SoftEther VPN также обеспечивает шифрование данных, поддержку аутентификации и возможность настройки различных параметров.

WireGuard — это новое ядро VPN для Linux, которое использует принципы упрощения и безопасности. В отличие от OpenVPN, WireGuard довольно прост в использовании. Он использует современные шифры и протоколы аутентификации, обеспечивая высокую степень безопасности передачи данных. WireGuard быстрый, легко устанавливаемый, и имеет меньше зависимостей, чем другие VPN-серверы. Благодаря этому он стал очень популярным для создания VPN-туннелей на роутерах и мобильных устройствах

После рассмотрения открытых технологий производился их сравнительный анализ и непосредственно выбор подходящего протокола - WireGuard - это новое ядро VPN для Linux, которое использует принципы упрощения и безопасности. В отличие от наиболее распространенного OpenVPN, WireGuard довольно прост в использовании. Он использует современные шифры и протоколы аутентификации, обеспечивая высокую степень безопасности передачи данных.

Второй раздел "Разработка VPN - сервера" посвящен непосред-

ственно разработке VPN - сервера. В разработке используется виртуальная машина, что позволяет создать отдельную среду для работы с сервером. Это позволяет отделить работу с VPN-сервером от работы на реальном компьютере, а также снизить риск влияния вирусов на сервер. Виртуальная машина позволяет создать изолированную среду, где можно установить операционную систему Ubuntu, а затем использовать ее для разработки и тестирования VPN-сервера. Ubuntu проста и понятна в установке и использовании, именно поэтому выбор пал на эту операционную систему. Для удобства разработки на Ubuntu мы используем Termius – программу для удаленного доступа и управления серверами, которая предоставляет оперативный доступ к виртуальной машине. С помощью Termius можно быстро установить и настроить VPN сервер на Ubuntu. Использование виртуальной машины Ubuntu вместе с Termius дает возможность эффективно разрабатывать и тестировать VPN сервер перед его введением в эксплуатацию. Большинство приложений и утилит, необходимых для разработки VPN, доступны в Ubuntu. Виртуальная машина позволяет получить корректную конфигурацию сервера и отлаженный код программы для работы VPN. В итоге использование виртуальной машины Ubuntu в связке с Termius обеспечивает быструю и удобную разработку VPN-сервера, а также повышает эффективность и надежность работы сервера.

Далее был арендован хост, с помощью которого и будет производиться туннелирование, после чего настраивался Termius - первым шагом хост был внедрен в систему Termius, с помощью данных арендованного сервера, а именно IP адреса, логина, пароля и порта. Далее в целях безопасности, доступ по паролю был изменен на RSA шифрование, в котором используется ассиметричное шифрование, то есть шифрование использующее два разных ключа - приватный и публичный. После изменений проведен перезапуск сервера, с последующим открытием терминала для дальнейшей настройки Ubuntu, а именно использование ряда команд для установки и обновления пакетов системы. После обновления пакетов системы и добавления необходимых инструментов производилась установка и скрипта WireGuard Manager, для последующей автоматизации конфигурации настроек VPN - сервера. Если конфигурация прошла корректно, то по ее окончании разработчик получает QR - код для авторизации на мобильном устройстве и конфиг для

авторизации на компьютере.

В третьем разделе была дана инструкция по авторизации на разных устройствах - мобильного устройства и компьютера. Для авторизации на мобильном устройстве необходимо для начала установить WireGuard, далее в приложении отсканировать QR - код. Авторизация на ПК представляет немного больше сложности. Сначала, нужно перенести файл, путь которого был получен после окончания конфигурации. Для этого нужно перейти на вкладку SFTP - на ней расположены директории ПК - в левом окне и директории сервера - в правом окне. Теперь следует найти нужный файл в директориях сервера. Путь известен, поэтому это не составит много трудностей. После чего нужно перетащить файл в удобную директорию непосредственно на ПК. Далее также, как и на мобильном устройстве нужно установить приложение WireGuard, в нем нажать кнопку "Добавить туннель"и выбрать файл. На этом инструкция по авторизации устройств подходит к концу

В четвертом разделе был проведен эксперимент по сравнению скорости интернета в различных VPN-сервисах, таких как VPN Bucks, TurboVPN и Browsec. Скорость интернета измерялась на гаджетах после подключения к каждому из сервисов после чего было проведено сравнение результатов. Также, проверялась скорость интернета на личном VPN сервере и заключались выводы о том, каким образом работа VPN-сервисов может отличаться от работы личного сервера. В результате эксперимента были получены следующие результаты: скорость интернета в VPN Bucks составила 2.2mbps, в TurboVPN - 1.75 mbps, а в Browsec - 86mbps. Как видно, в Browsec удалось получить наибольшую скорость, что делает его наиболее привлекательным вариантом для использования. Однако, следует отметить, что все VPN-сервисы имеют свои недостатки. Например, у VPN Bucks и TurboVPN скорость очень низкая, что является любопытным фактом для тех кто выбирает VPN-сервисы и хочет минимизировать падение начальной скорости. В то же время, ответственность за работоспособность личного VPNсервера полностью ложится на его владельца. В отличие от VPN-сервисов, где серверы находятся в других частях мира и могут быть перегружены другими пользователями со всего мира, личный VPN сервер обеспечивает более стабильное и быстрое соединение, потому что владелец сервиса знает, сколько пользователей им будут пользоваться и сколько потоков будет обработано. Так, личный VPN сервер

обеспечил скорость интернета в 88mbps, что является лучшим результатом в эксперименте.

ЗАКЛЮЧЕНИЕ

В результате выполнения данной работы был реализован личный VPN сервер на основе протокола WireGuard с использованием программы Termius для дальнейшей настройки сервера. В ходе эксперимента было проведено сравнение скорости личного VPN-сервера с популярными VPN-сервисами (Browsec, TurboVpn, VPN Bucks), в результате которого было установлено, что личный VPN сервер показал лучший результат по скорости. Однако, сервис Browsec был максимально близок по скорости, но уступал по стабильности. В итоге получается, что личный VPN сервер может быть более эффективным в использовании по сравнению с популярными VPN-сервисами. Из выводов следует, что использование личного VPN-сервера может быть более предпочтительным решением для пользователей корпораций, несмотря на наличие бесплатных услуг на рынке. Сервер обеспечивает более высокий уровень безопасности и надежности, а также более быструю скорость передачи данных. В дальнейшем рекомендуется продолжать разработку VPN-сервера, улучшать его производительность и функциональность. Также может быть полезно расширить базу пользователей, предоставив услугу в широком масштабе. В целом, реализация VPN-сервера на протоколе WireGuard является перспективным направлением для создания безопасной и быстрой связи в интернете, и может быть рекомендована для использования как для личных, так и для коммерческих целей.

Основные источники информации:

1 https://teletype.in/@cryptolife/kak-sozdat-svoj-vpn-na-vps-servere

2 https://www.digitalocean.com/community/tutorials/how-to-set-up-andconfigure-an-openvpn-server-on-ubuntu-20-04-ru

3 https://www.digitalocean.com/community/tutorials/how-to-set-up-ssh-keys-onubuntu-20-04

4 https://www.digitalocean.com/community/tutorials/how-to-configure-ssh-keybase authentication-on-a-linux-server

5 Качанов, Н. А. (2017). Протоколы VPN [Электронный ресурс]. – Режим доступа: https://studylib.ru/doc/2566957/protokoly-vpn

6 Shumilov, S. A. (2010). Как установить VPN-сервер на Linux и настроить VPN-клиенты. MGN.BY [Электронный ресурс]. – Режим доступа: https://mgn.by/articles/kak-ustanovit-vpn-server-na-linux-i-nastroit-vpn-klienty

7 Тихомиров, А. (2019). Как быстро и безопасно использовать VPN на Android. Andro News [Электронный ресурс]. – Режим доступа: https://andronew bystro-i-bezopasno-ispolzovat-vpnna-android/

8 Круглов, Д. (2019). Как подключиться к VPN на Windows 10. Red Star IT [Электронный ресурс]. – Режим доступа: https://redstar-it.ru/kakpodklyuchit k-vpn-na-windows-10/

9 Бойченко, А. (2016). Как настроить и использовать VPN в Opera. Интернет-лаборатория [Электронный ресурс]. – Режим доступа: https://ilab.su/2016/07/0 nastroit-i-ispolzovat-vpn-v-opera/

10 Петров, С. (2015). VPN-сервисы в России: реальность и перспективы. Фонтанка.РУ [Электронный ресурс]. – Режим доступа: https://www.fontanka.ru