Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Космических и информационных технологий
институт

Вычислительная техника
кафедра

УТВЕРЖДАЮ
Заведующий кафедрой
_____ О. В. Непомнящий
подпись инициалы, фамилия
« ___ » ____ 20 __ г.

БАКАЛАВАРСКАЯ РАБОТА

09.03.01 Информатика и вычислительная техника
код и наименование направления

Система удаленного доступа в сеть предприятия
тема

Пояснительная записка

Руководитель	_____	доцент, канд.физ-мат.наук	К. В. Коршун
	подпись, дата	должность, ученая степень	инициалы, фамилия
Выпускник	_____		С. В. Занин
	подпись, дата		инициалы, фамилия
Нормоконтролер	_____	доцент, канд.физ-мат.наук	К. В. Коршун
	подпись, дата	должность, ученая степень	инициалы, фамилия

Красноярск 2021

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Космических и информационных технологий
институт

Вычислительная техника
кафедра

УТВЕРЖДАЮ
Заведующий кафедрой
_____ О. В. Непомнящий
подпись инициалы, фамилия
« ___ »_____ 20 __ г.

ЗАДАНИЕ
НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ
в форме бакалаврской работы

Студенту Занину Сергею Владимировичу
фамилия, имя, отчество

Группа КИ17-07Б Направление (специальность) 09.03.01
номер код

Информатика и вычислительная техника
наименование

Тема выпускной квалификационной работы Система удаленного доступа в сеть предприятия

Утверждена приказом по университету №_____ от _____

Руководитель ВКР К. В. Коршун, доцент, канд.физ-мат.наук
инициалы, фамилия, должность, учёное звание и место работы

Исходные данные для ВКР: Спроектировать систему удаленного доступа в сеть предприятия, изучить существующие технологии VPN, разработать общую архитектуру системы, выбрать аппаратное и программное обеспечение системы, разработать конфигурацию аппаратного и программного обеспечения, разработать и реализовать прототип системы, провести тестирование работоспособности.

Перечень разделов ВКР: Аналитическая часть, разработка общей архитектуры системы, разработка системы удаленного доступа, проверка работоспособности системы.

Перечень графического материала: презентация в формате Power Point.

Руководитель ВКР _____ К. В. Коршун
Подпись инициалы, фамилия

Задание принял к исполнению _____ С. В. Занин
Подпись инициалы, фамилия

«___»_____2020

РЕФЕРАТ

Выпускная квалификационная работа по теме « Система удаленного доступа в сеть предприятия » содержит 35 страниц текстового документа, 30 изображений, 11 использованных источников.

Актуальность.

С началом коронавирусной проблемы в нашей стране, удаленный доступ пользуется актуальностью как никогда ранее.

Целью бакалаврской работы является проектирование и реализация системы удаленного доступа в сеть предприятия.

Основные задачи:

- Изучить существующие технологии VPN;
- Разработать общую архитектуру системы;
- Выбрать аппаратное и программное обеспечение системы;
- Разработать конфигурацию аппаратного и программного обеспечения;
- Разработать и реализовать прототип системы, провести тестирование работоспособности.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В настоящее время работа, связанная с обработкой информации, невозможна без использования компьютерных сетей. Однако не всегда возможна физическая реализация локальной сети. Часто возникает ситуация, когда работники находятся не в помещение офиса, а работают с клиентами на местах, выезжают в командировки. В этом случае важно организовать работу таким образом, чтобы, находясь в отдалении от локальной сети организации, они, тем не менее, могли подключиться к ней. Обеспечить доступ к локальной сети при отсутствии непосредственного подключения к ней, можно с помощью средств удаленного доступа к сети. Они используются для связи удаленного компьютера с сетью. Также обеспечивают передачу данных на различные расстояния.

Одним из основных факторов, влияющих на выбор, является размер организации. Исходя из ее потребностей и возможностей определяются необходимые для удаленного доступа программно-аппаратные средства. Подбор оборудования и методики организации удаленного доступа, должны решать данные проблемы. Задача, решаемая данной работой связана с решением обозначенной выше проблемы и может быть сформулирована следующим образом:

Изучить существующие технологии организации удаленного доступа, спроектировать и реализовать систему удаленного доступа.

На основании этого были поставлены следующие задачи выпускной квалификационной работы:

1.Ознакомление с технологиями VPN, выбор технологии для использования в системе;

2. Разработка общей архитектуры системы;

3. Разработка конфигурации аппаратного и программного обеспечения;

4. Реализация прототипа системы удаленного доступа.

1 Аналитическая часть

1.1 Описание предметной области

Удалённый доступ – это обширное понятие, которое включает в себя множество типов и вариантов взаимодействия компьютеров, сетей и приложений. Если рассматривать различные схемы взаимодействия, которые обычно относятся к удаленному доступу, то им присуще глобальное использование каналов взаимодействия или сетей. Для удаленного доступа, как правило, характерен вид взаимодействия, когда, с одной стороны, имеется центральная часть большой сети или компьютер, а с другой, с удаленного терминала, компьютера или малой сети, желающие получить доступ к другим сетевым ресурсам. Количество удаленных от центральной сети узлов и сетей, которым необходим этот доступ, постоянно растет, поэтому современные средства удаленного доступа рассчитаны на большое количество клиентов.

1.2 VPN Виртуальные частные сети

VPN создает локальную сеть между несколькими компьютерами в сегментах сети. Машины могут находиться как в одной локальной сети, так и могут быть удалены на большом расстоянии друг от друга и подключены через Интернет. VPN поставляется с дополнительной защитой, чтобы сделать виртуальную сеть частной. Сетевой трафик проходящий через VPN часто называют внутренним туннелем по сравнению с другими трафиками, которые находятся за пределами туннеля.

На рис 1.1 сетевой трафик показан так, как традиционно проходит через сегменты сети и Интернета. Здесь этот трафик относительно открыт для проверки и анализа, но защищенные протоколы такие как HTTPS и SSH менее уязвимы для злоумышленников.

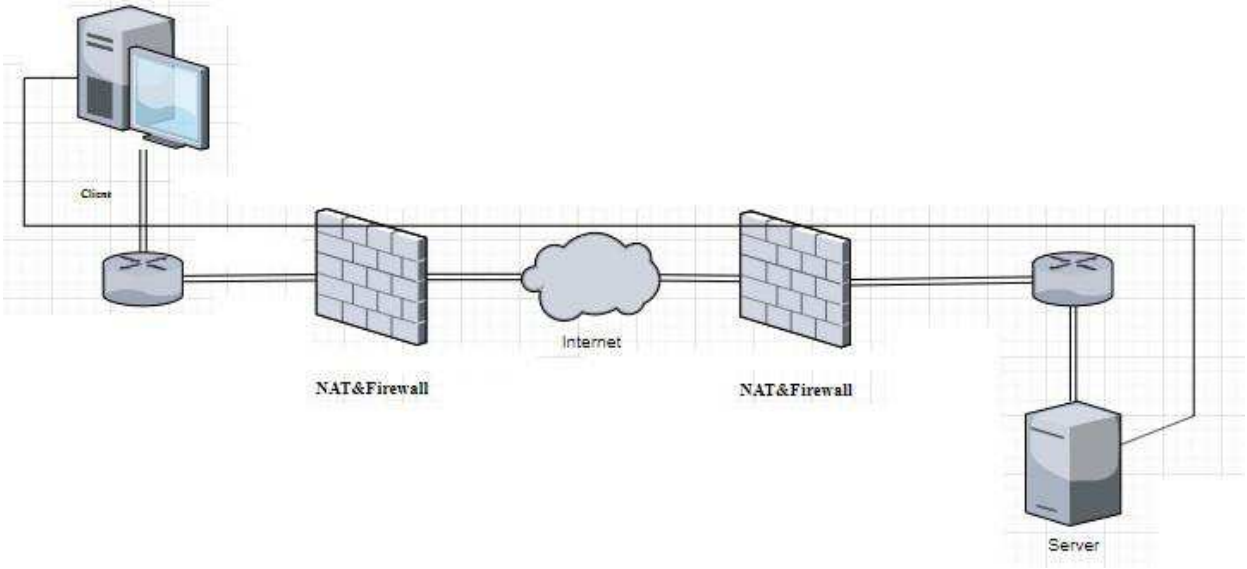

Рисунок 1 – Сетевой трафик

Здесь злоумышленники по-прежнему могут видеть из какого типа соединения какой компьютер к какому серверу подключён [4].

Когда используется VPN, трафик внутри туннеля больше не может быть идентифицирован. Трафик внутри VPN может быть любым, что бы не отправлялось по локальной или глобальной сети. В то время как сама VPN маршрутизируется через Интернет, как на рис 1 , устройства по сетевому пути могут видеть только трафик VPN; эти устройства не знают о том, что происходит или передается внутри частного туннеля. Защищенные протоколы такие как HTTPS и SSH защищены внутри туннеля от других пользователей VPN, но будет дополнительно неопознаваемый трафик снаружи туннеля. VPN не только производит шифрование трафика внутри туннеля, но и также он скрывает и защищает отдельные потоки данных от тех, кто находится за пределами туннеля [2].

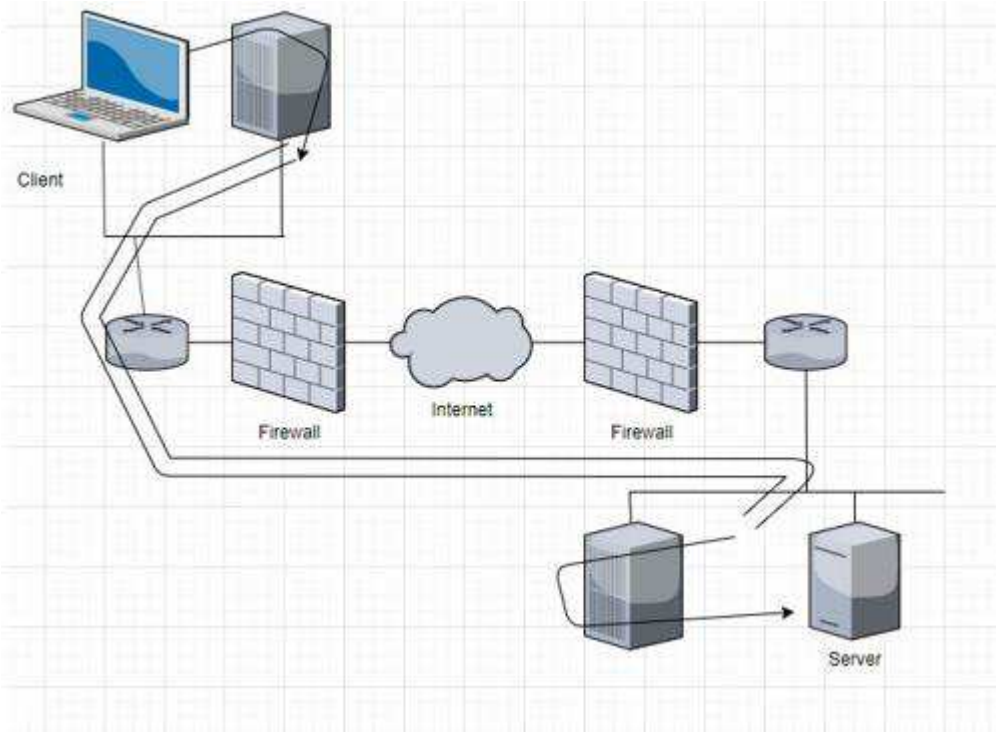

Рисунок 2 – VPN-туннель

На рисунке 2 показаны как сильные стороны, так и одна самая большая угроза технологий VPN. VPN-туннель проникает через роутеры и брандмауэры с обеих сторон. Таким образом весь сетевой трафик, который проходит через VPN-туннель, обходит обычную защиту сети, если только не предпринимаются особые меры для контроля VPN трафика [11].

Большинство реализаций VPN используют некоторую форму шифрования и аутентификацию. Шифрование VPN гарантирует что другие стороны, которые отслеживают трафик между системами, не смогут декодировать и в дальнейшем проанализировать конфиденциальные данные. Аутентификация состоит из двух компонентов:

Первый, аутентификация пользователя и системы, которая предоставляет подключение к авторизованному серверу. Этот тип аутентификации в форме сертификата или сочетании имени пользователя и пароля. Конкретные правила данных пользователей можно согласовать, например, правила о конкретных маршрутах, правила брандмауэра или других скриптов и утилитах. Как правило они уникальны для каждого экземпляра, но для каждого из них можно провести

настройку если используется OpenVPN.

Второй компонент аутентификации – это дополнительная защита для потока связи. В этом случае способ подписи каждого отправленного пакета является установленным. Каждая система проверяет правильно ли подписаны полученные VPN-пакеты до расшифровки данных. Путем аутентификации пакетов, которые уже находятся в зашифрованном виде, система может сэкономить время обработки даже не расшифровывая пакеты, которые не соответствуют правилам аутентификации. Такая аутентификация мешает потенциальным атакам типа “Denial of Service” (DoS), а также предотвращает “Man in the Middle” (MITM) при условии, что ключи подписи хранятся в безопасном месте [3].

1.3 Технологии VPN

Множество продуктов VPN, доступны на рынке как коммерческие, так и с открытым исходным кодом. Все продукты VPN делится на четыре категории:

- VPN на основе PPTP-протокола;
- VPN на основе протокола IPSec;
- VPN на основе SSL;
- OpenVPN.

OpenVPN тоже является VPN на основе SSL поскольку использует SSL или TLS-подобный протокол для установления безопасного соединения. Тем не менее создана отдельная категория для OpenVPN, так как он отличается от другой SSL на основе VPN-решения [10].

1.3.1 PPTP

Одним из протоколов VPN является протокол точка-точка (PPTP) разработан Microsoft и Ascend в 1999 году. Протокол PPTP официально зарегистрирован как RFC263 также PPTP клиент был включен в Windows с 1995

года и до сих пор включен в большинство операционных систем.

В настоящее время протокол PPTP считается небезопасным, так как надежность защищенного соединения напрямую связана с надежностью самого соединения. Пример: аутентификация (пароль). Таким образом ненадежный пароль приводит к небезопасному VPN-соединению. Большинство установок PPTP использует MSCHAPv2 протокол для шифрования паролей. Безопасность протокола PPTP использует сертификаты " X. 50 " для защищенного PPTP-соединения, что обеспечивает довольно безопасное соединение. Но все клиенты PPTP поддерживают EAP-TLS, которая необходима для разрешения использования сертификатов " X. 509 ".

Два канала PPTP:

- канал управления для настройки соединения;
- канал для передачи данных.

Канал управления устанавливается через TCP-порт. Канал данных использует общую инкапсуляцию маршрутизации (GRE) протокола, который является IP-протоколом.

PPTP-клиенты доступны практически на всех операционных системах начиная от Windows до Linux и Unix и также для устройств Android и Ios [7].

1.3.2 IPSec

IPSec – официальный стандарт IEEE/IETF для IP - безопасности. Официально зарегистрирован как RFC 2411. IPSec встроен в стандарт IPv6. IPSec работает на уровне второй и третьей модели OSI сетевой сети. У IPSec есть политика безопасности, что делает ее чрезвычайно гибкой и мощной, но и трудно настраиваемой и отлаживаемой. Безопасность политики разрешает администратору шифроватьтрафик между двумя конечными точками на основе параметров, таких как IP-адрес источника и IP-адрес назначения, а также между исходным и конечными портами TCP или UDP. Возможна настройка IPSec на использование предварительно разделенных ключей или сертификатов для защиты подключения VPN. К тому же он использует сертификаты “X.509”, одноразовые пароли, протоколы имен пользователя или пароль для аутентификации VPN-соединения. В IPSec присутствует 2 режима работы: транспортный режим и туннельный режим.

Транспортный режим используется чаще всего в сочетании с туннелированием второго уровня (L2TP). L2TP протокол выполняет аутентификацию пользователя. Клиенты IPSec встроенные в операционные системы обычно выполняют IPSec с L2TP, также возможно настроить подключение только по протоколу IPSec.

IPSec VPN-клиент, встроенный в Microsoft Windows, по умолчанию использует протокол IPSec с L2TP, но его можно отключить или обойти.

IPSec использует два канала:

- Канал управления для настройки соединение и один для передачи данных. Канал управления инициируется через UDP.
- Канал данных использует инкапсулированную полезную нагрузку безопасности (ESP), протокол который является IP- протоколом.

Целостность IPSec пакетов обеспечивается с помощью проверки подлинностисообщения (HMAC). Недостаток IPSec – расширение к стандарту, которое делает его более сложным для того чтобы соединить две конечные точки

IPSec от разных поставщиков. Программное обеспечение IPSec входит в состав операционных систем, а также брандмауэры, маршрутизаторы и микропрограммное обеспечение [8].

1.3.3 VPN на основе SSL

VPN на основе SSL использует протоколы SSL и TLS. VPN на основе SSL чаще называют web-VPN или безлимитным VPN. Есть поставщики, которые предоставляют отдельное клиентское программное обеспечение такое как Cisco AnyConnect. VPN с основой SSL используют такой же сетевой протокол, что и для (HTTPS). OpenVPN же использует пользовательские алгоритмы для шифрования и подписи данных трафика. Это основная причина, по которой OpenVPN указан как отдельная VPN категория. Не существует четкого определенного стандарта для VPN на основе SSL, но большинство используют протоколы SSL и TLS для настройки и защитного соединения. В большинстве случаев соединение защищается с помощью сертификатов с одноразовым паролем или протоколами имени пользователя и пароля для аутентификации соединения. На основе SSL, VPN очень похожи на соединения, используемые для защиты веб-сайтов (HTTPS) также часто используется один и тот же протокол и канал (TCP и порт 443). Несмотря на то, что VPN на основе SSL часто называют веб или клиентскими, там есть довольно много поставщиков которые используют плагин браузера или элемент управления ActiveX чтобы улучшить VPN-соединение.

Это делает VPN несовместимыми с неподдерживаемыми браузерами или операционными системами [9].

1.3.4 OpenVPN

OpenVPN это VPN на основе SSL так как он использует протоколы SSL и TLS для защищённого соединения. Однако OpenVPN также использует

HMAC в сочетании алгоритма хеширования для обеспечения целостности пакетов. OpenVPN можно настроить для использования предварительно разделенных ключей, а также сертификатов. Данные функции не доступны другим VPN на основе SSL. Кроме того, OpenVPN использует виртуальный сетевой адаптер, устройство tun или tap в качестве интерфейса между пользовательским программным обеспечением OpenVPN и ОС.

OpenVPN может работать с операционными системами поддерживающими устройство tun или tap. В настоящее время это Linux, Free / Open / NetBSD, Solaris, AIX, Windows и Mac OS, а также устройства iOS и Android. Для всех этих платформклиентское программное обеспечение должно быть установлено что отличает OpenVPN от client-less или веб-VPN. Протокол OpenVPN не определен встандарте RFC, но протокол является общедоступным, потому что OpenVPN – это часть программного обеспечения с открытым исходным кодом. Факт, того что он является открытым исходным кодом, практически делает OpenVPN более безопасным чем closed source VPN так как код постоянно проверяется разными людьми.

Также существует очень мало шансов что секретные бэкдоры будут встроены в OpenVPN. OpenVPN имеет канал управления и канал передачи данных. Они шифруются и защищаются по-разному. Весь трафик проходит через одно соединение TCP или UDP. Канал управления шифруется и защищается с помощью SSL и TLS каналов, также данные шифруется с помощью пользовательского протокола шифрования. Протокол и порт по умолчанию для OpenVPN это UDP и порт 1194 [6].

1.4 Анализ VPN сетей

1.4.1 Преимущества и недостатки PPTP

Преимущество VPN на основе PPTP – программное обеспечение для клиентов VPN встроено в большинство операционных систем. Время запуска

для настройки и инициализация PPTP VPN- соединения происходит очень быстро.

Недостатками VPN на основе PPTP являются отсутствие безопасности и параметры конфигурации как на стороне клиента, так и на стороне сервера. Кроме того, EAP-TLS расширение которое позволяет использовать сертификаты “X.509”, полностью поддерживается только в Microsoft Windows, но существует patch для pppd с открытым исходным кодом. Patch pppd включен в почти каждый дистрибутив Linux. Кроме того, если необходимо прибегнуть к использованию EAP-TLS, то простота настройки PPTP VPN значительно снижается. Это потому, что EAP-TLS требуется настроить инфраструктуру открытых ключей, как IPSec и OpenVPN. Серьезным недостатком PPTP является использование протокола GRE,который делает его несовместимым с устройствами за пределами NAT.

1.4.2 Преимущества и недостатки IPSec

Преимущества протокола IPSec в его безопасности, хорошей поддержки со стороны поставщиков и различных платформ включая маршрутизаторы xDSL и Wi-Fi, а также возможность использования Fine-Grained политик безопасности для управления потоком трафика. Недостатками IPSec является то, что его, как известно трудно настроить и отладить. Различные реализации IPSec от поставщиков не воспроизводятся хорошо вместе, и IPSec не интегрируется хорошо с сетями NAT. Наиболее примечательно, что не рекомендуется, а иногда даже невозможно запускать сервер IPSec, который находится внутри сети NAT.

1.4.3 Преимущества и недостатки VPN на основе SSL

VPN на основе SSL или веб-VPN имеют преимущество в отсутствии или очень малого программного обеспечения для клиентов. Это делает установку и инициализацию на стороне клиента очень простой. Недостатком веб-VPN можно назвать то, что он часто не является полноценным VPN и позволяет получить

доступ к одному серверу или набору серверов. Кроме того, это усложняет возможность поделиться локальными данными с удаленного сайта или сервера.

1.4.4 Преимущества и недостатки OpenVPN

Преимуществами OpenVPN является простота установки конфигурациии возможность установки в ограниченных сетях, включая сети NAT. Кроме того OpenVPN включает в себя функции безопасности, которые так же сильны, как и у VPN на основе IPSec, включая аппаратную маркерную защитуи поддержку для различных пользователей механизм аутентификации.

Недостатки OpenVPN находятся в отсутствии масштабируемости и ее зависимость в установке клиентского программного обеспечения. Еще одним недостатком является отсутствие графического интерфейса для настройки и управления. В частности, драйвер интерфейса tap для Microsoft Windows часто вызывала проблемы развертывания, когда выпускалась новая версия Windows.

1.5 Внутренние компоненты OpenVPN

Одним из основных блоков OpenVPN является драйвер tun и tap. Концепция драйвера tun и tap происходит из Unix и Linux, где они часто доступны как часть операционной системы. Это виртуальные сетевые адаптеры, которые рассматривается операционной системой как двухточечный адаптер (в стиле tun) для трафика IP или в качестве полноценного виртуального адаптера Ethernet для всех типов трафиков(в стиле tap). На внутренней стороне этих адаптеров находится такое приложение как OpenVPN, которое обрабатывает входящий и исходящий трафик. Linux, Free / Open / NetBSD, Solaris и Mac OS включают в себя драйвер ядра tun.

Для Microsoft Windows был написан James Yonan специальный драйвер NDIS, называется адаптером TAP-WIN32. На данный момент версии NDIS5 и NDIS6 драйвера доступны, поддерживая Windows XP через Windows 8.1.

Разработка этого адаптера теперь официально отделена от основного OpenVPN развития, но OpenVPN продолжает сильно полагаться на него.

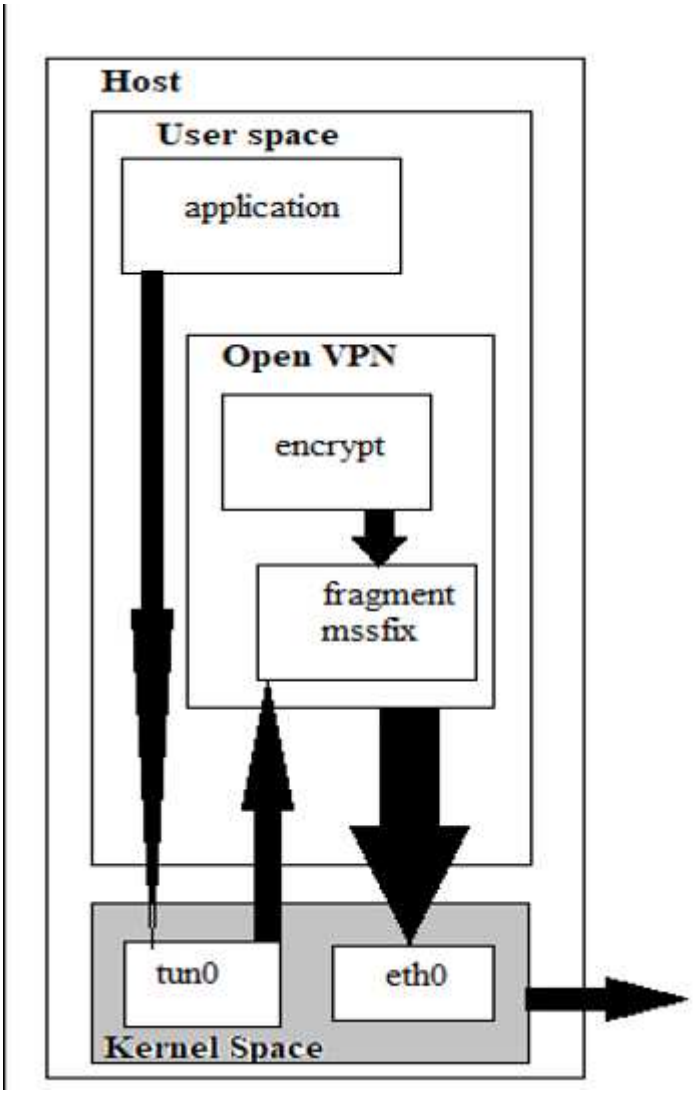

Рисунок 3 – Поток трафика из пользовательского приложения через OpenVPN

Пример: Поток трафика из пользовательского приложения через OpenVPN изображен на Рис 3. приложение отправляет трафик на адрес, доступный через туннель OpenVPN в несколько шагов:

- Приложение передает пакет операционной системе;
- ОС решает использовать обычные правила маршрутизации (пакет должен маршрутизироваться через VPN);
- Пакет пересылается на устройство настройки ядра;
- Устройство настройки ядра пересылает пакет в процесс OpenVPN (в

пользовательском пространстве);

• Процесс OpenVPN шифрует и подписывает пакет и фрагментирует его при необходимости, а также снова передает его к ядру (чтобы отправить его на адрес удаленной конечной точки VPN);

• Ядро забирает зашифрованный пакет и пересылает его на удаленную конечную точку VPN, где происходит обратный процесс.

На этой диаграмме видно, что производительность OpenVPN всегда будет ниже, чем у обычного сетевого подключения. Для большинства приложений, потеря производительности минимальна. Однако дляскоростей, превышающих 1 Гбит/с, существует слабое место в производительности как с точки зрения пропускной способности так и с задержки. Следует отметить что производительность драйвера Windows намного ниже чем производительность встроенных адаптеров tun и tap в других операционных системах. Это верно даже для самой реализации драйвера TAP-Win32 в NDIS6. Для одного клиента OpenVPN воздействие довольно мало. Для крупномасштабного сервера OpenVPN, который обслуживает много клиентов, это может легко вызвать проблемы с производительностью. Это одна из главных причин того, что сообщество разработчиков открытого исходного кода обычно рекомендует использовать хост на основе Unix или Linux в качестве сервера OpenVPN [9].

1.6 Режимы UDP и TCP

OpenVPN поддерживает два способа связи между конечными точками, используя UDP или TCP. UDP - это протокол без установленного соединения или с потерями протокола. Если пакет теряется при передаче, то сетевое соединения незаметно это исправит. TCP - это протокол ориентированный на соединение. Пакеты отправляются и доставляются по протоколу handshake, обеспечивая доставку каждого пакета на другую сторону. Оба способа связи имеют свои преимущества и недостатки. Это на самом деле зависит от типа трафика, который отправляется через VPN-туннель.

Пример: Использование приложения на основе TCP через VPN может привести к двойной потере производительности особенно если имеется плохое подключение к сети. В этом случае повторяется передача потерянных пакетов, потерянных как внутри, так и снаружи туннеля, что приводит к снижению производительности. Однако аналогичным образом можно утверждать, что отправка пакетов через UDP, также не является отличной идеей. Если приложение использует UDP протокол для своего трафика, восприимчивого к атакам удаления или переупорядочения, то базовое зашифрованное TCP соединение повысит безопасность таких приложений даже больше чем базовый VPN на основе UDP. Если большая часть трафика через VPN основана на UDP, тогда лучше использовать TCP-соединение между конечными точками VPN.

При выборе между транспортом UDP или TCP, общее правило таково: если у вас работает UDP (mode udp), то используйте его; если нет, то попробуйте TCP (режим tcp-сервера и режим tcp - клиента). Некоторые коммутаторы и маршрутизаторы неправильно пересылают трафик UDP, что может быть проблемой, особенно если несколько клиентов OpenVPN подключены к одному коммутатору или маршрутизатору.

Точно так же на производительность OpenVPN через TCP может сильно повлиять выбор Интернет-провайдеров (ISP), некоторые провайдеры используют странные размеры MTU или пакеты, с фрагментированными правилами, что приводит к крайне низкой производительности OpenVPN-overTCP по сравнению с незашифрованным TCP-трафиком.

1.7 Протокол шифрования

OpenVPN реализует TLS через UDP, но способ OpenVPN использования TLS отличается от способа веб-браузера, использующего TLS. Таким образом, когда OpenVPN запускается через TCP, то трафик отличается от обычного трафика TLS. Брандмауэр, использующий глубокую проверку пакетов (DPI), может легко отфильтровать трафик OpenVPN. Основное различие между

OpenVPN-TLS и browser-TLS заключается в подписи пакетов. OpenVPN предлагает функции для защиты от DoS-атак с помощью подписания пакетов канала управления с помощью специального статического ключа (--tls- authta.key 0|1). Пакеты канала передачи данных, которые передаются по тому же UDP или TCP соединению, подписываются совершенно по-разному и очень легко различаются от трафика HTTPS. Это также является основной причиной, почему port-sharing, где OpenVPN и безопасный веб-сервер могут использовать один и тот же IP-адрес, и номер порта может фактически работать.

1.8 Режим клиент - сервер с tun и tap устройствами

Модель развертывания OpenVPN – это один сервер с несколькими удаленными клиентами, способными маршрутизировать трафик.

Основное различие между режимом tun и tap - это тип используемого адаптера. Tap адаптер обеспечивает полный виртуальный интерфейс Ethernet (второго уровня), в то время как адаптер tun рассматривается как адаптер точка-точка (третьего уровня) большинством операционных систем. Компьютеры, подключенные с помощью (виртуальных) адаптеров Ethernet, могут образовывать единый широковещательный домен, который необходим для определенных приложений. С точка-точка адаптерами этого невозможно. Кроме того, не все операционные системы поддерживают tap адаптеры. Например: iOS и Android поддерживают только устройства tun. Кроме того, режим tap позволяет настроить мост, где обычная сеть адаптера соединена мостом с виртуальным адаптером tap.

2 Общая архитектура системы

Система удаленного доступа разрабатывается для организации, которая имеет небольшую сеть. Сеть состоит из нескольких компьютеров,сервера, маршрутизатора и коммутатора. Сервер выполняет задачи, такие как обмен файлами и совмесной работы. Маршрутизатор представляет собой обычный роутер. С его помощью компьютеры выходят в сеть интернет.

Поставлена задача: получить удаленный доступ в сеть организации. То есть: человек, работающий дистанционно, должен иметь доступ к внутреннему серверу. Например, для обмена файлами или совместной работы с другими сотрудниками.

Для того чтобы реализовать данную систему необходимо несколько компонентов.

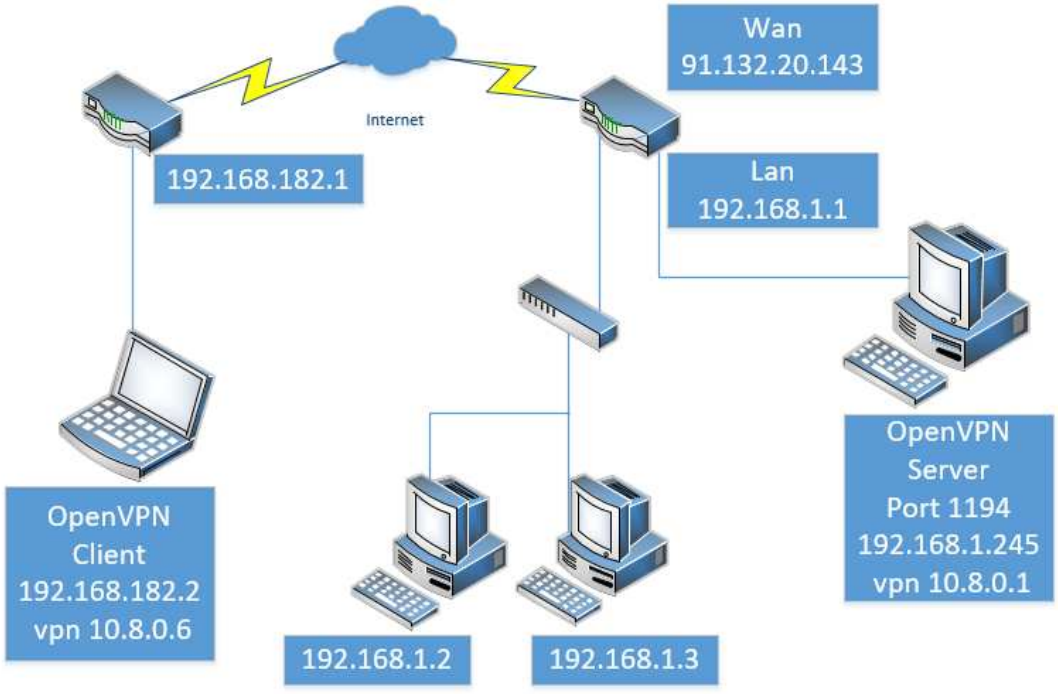

Рисунок 4 – Общая архитектура системы

Во-первых, сервер VPN. Выше рассмотрены существующие VPN технологии. Они имеют различные преимущества и недостатки. В качестве технологии для использования в системе была выбрана технология OpenVPN.

Во-вторых, сам сервер. В организации нет лишнего оборудования, на котором можно запустить OpenVPN сервер. Кроме того, сеть небольшая и предполагается невысокая нагрузка на OpenVPN сервер. Поэтому задействовуем существующий в организации сервер. На него, дополнительно в нагрузку установим OpenVPN сервер.

Маршрутизатор, через который происходит выход в интернет. Он представляет собой обычный роутер. Данная организация для своих целей ранее приобрела выделенный ip-адрес (Рис. 4). Для того чтобы VPN клиенты, находясь за пределами сети, могли подключаться к VPN серверу, который находится во внутренней сети организации, на маршрутизаторе необходимо настроить перенаправление портов.

Последним компонентом системы является VPN клиент. VPN клиент запускается на личном оборудовании дистанционно работающего сотрудника.

3 Разработка системы удаленного доступа

3.1 Установка и настройка сервера OpenVPN

Для создания ключей и сертификатов сервера необходимо сделать следующие:

Открыть папку “easy-rsa”, которая находится по адресу “C:\OpenVPN\easy-rsa” . Найти файл vars.bat.sample. Переименовать его в vars.bat и открыть его любым текстовым редактором .(Рис 5).

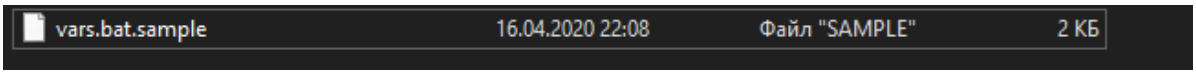

Рисунок 5 – Файл vars.bat

Указать путь к папке “easy-rsa” на “C:\OpenVPN\easy-rsa”

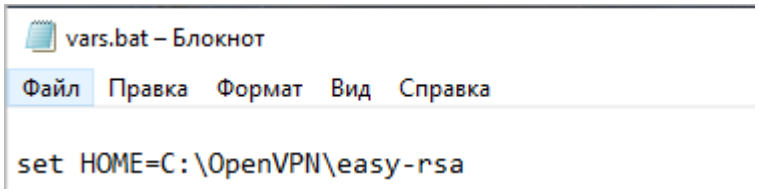

Рисунок 6 – Путь к папке

Следующие параметры оставить без изменений.

set key dir = “папка где будут создаваться ключи”

set DH key size =” Размер ключа DH”

set KEY_SIZE=” Размер ключа”

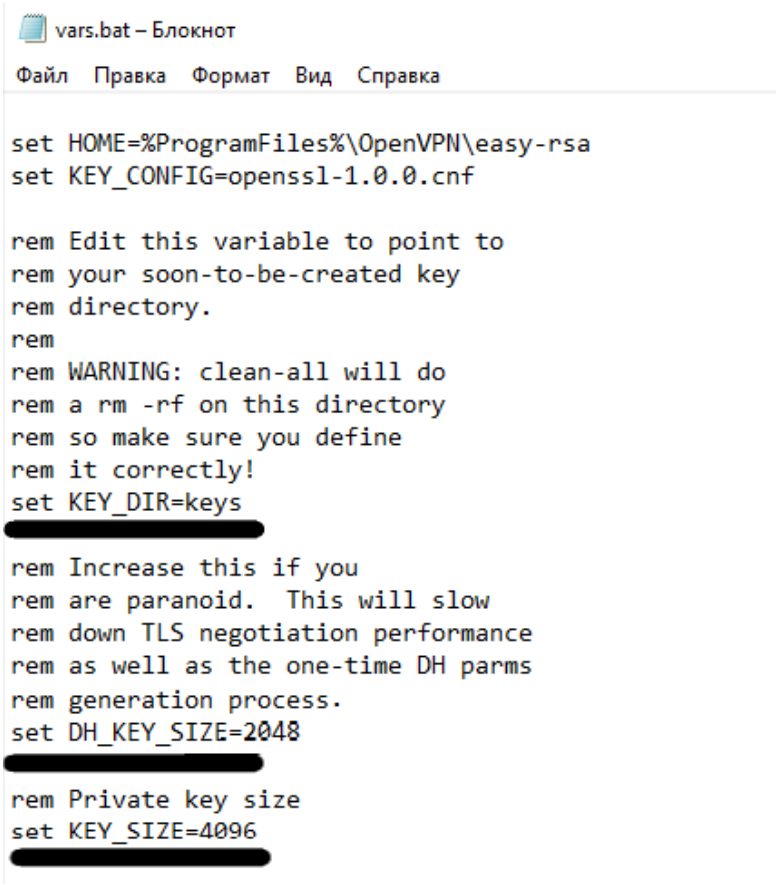

Рисунок 7 – Неизменные параметры

Остальные строки заполнить произвольно.

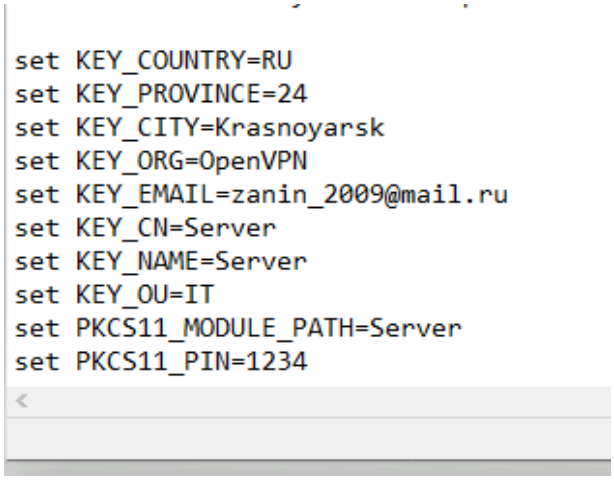

Рисунок 8 – Заполнение параметров

Изменить файлы: build-ca.bat, build-dh.bat, build-key.bat, build-key-pass.bat, build-key-pkcs12.bat и build-key-server.bat. Они представлены на рисунке 9.

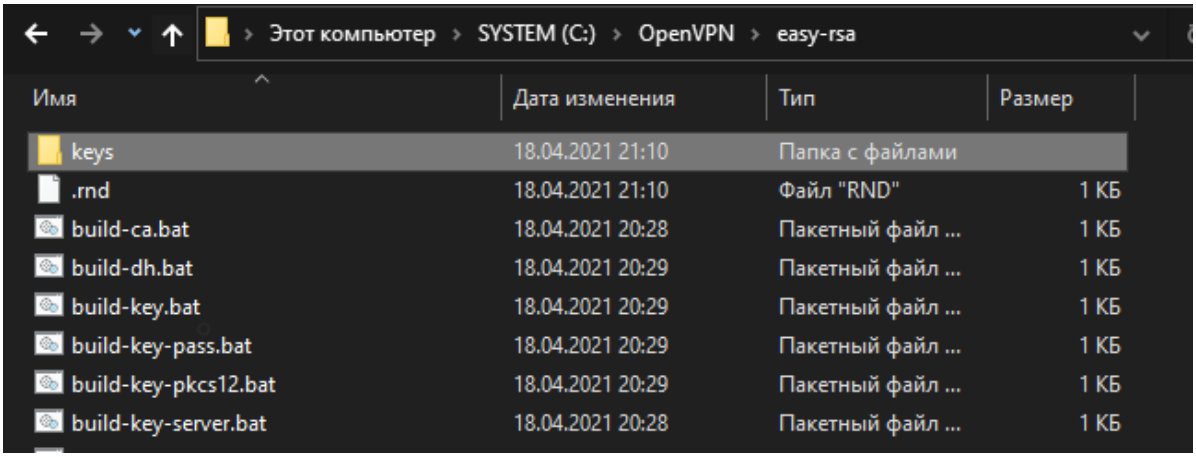

Рисунок 9 – Редактируемые файлы

В них отредактировать команду openssl на полный путь к соответствующему ей файлу “openssl.exe.”

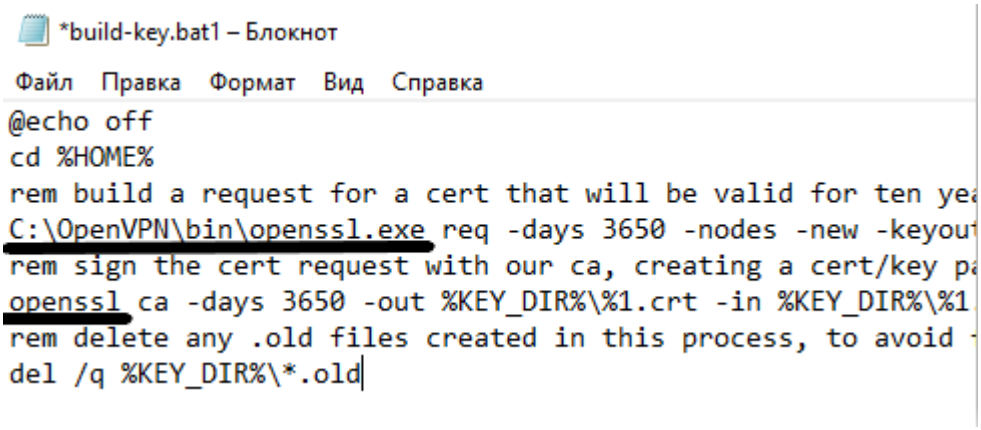

Рисунок 10 – Редактирование команды

Запустить командную строку и перейти в целевой каталог.

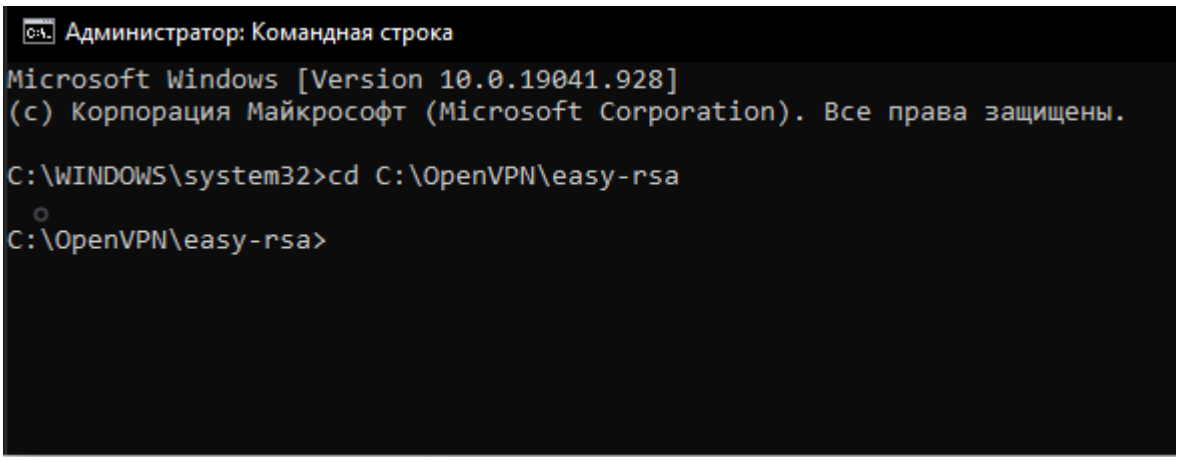

Рисунок 11 – Запуск командной строки

Ввести команду “vars.bat” и нажать ENTER.

Ввести команду clean-all.bat.

Повторить, первую команду “vars.bat”.

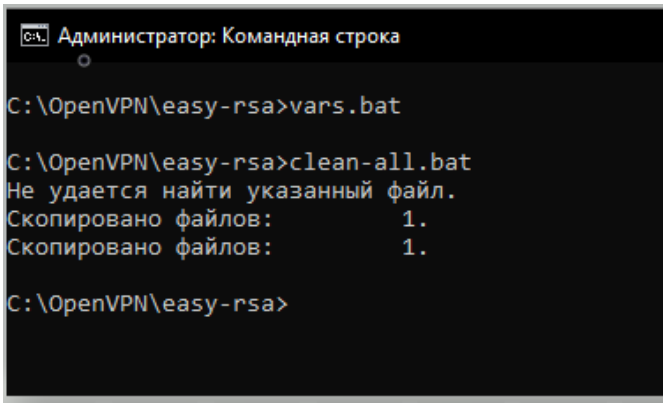

Рисунок 12 – Команда vars.bat

Создать файлы, необходимые для работы. Для этого использовать команду “build- ca.bat”. После выполнения команды ,подтвердить данные, которые вносились в файл vars.bat. Несколько раз нажать ENTER, пока не появится исходная строка.

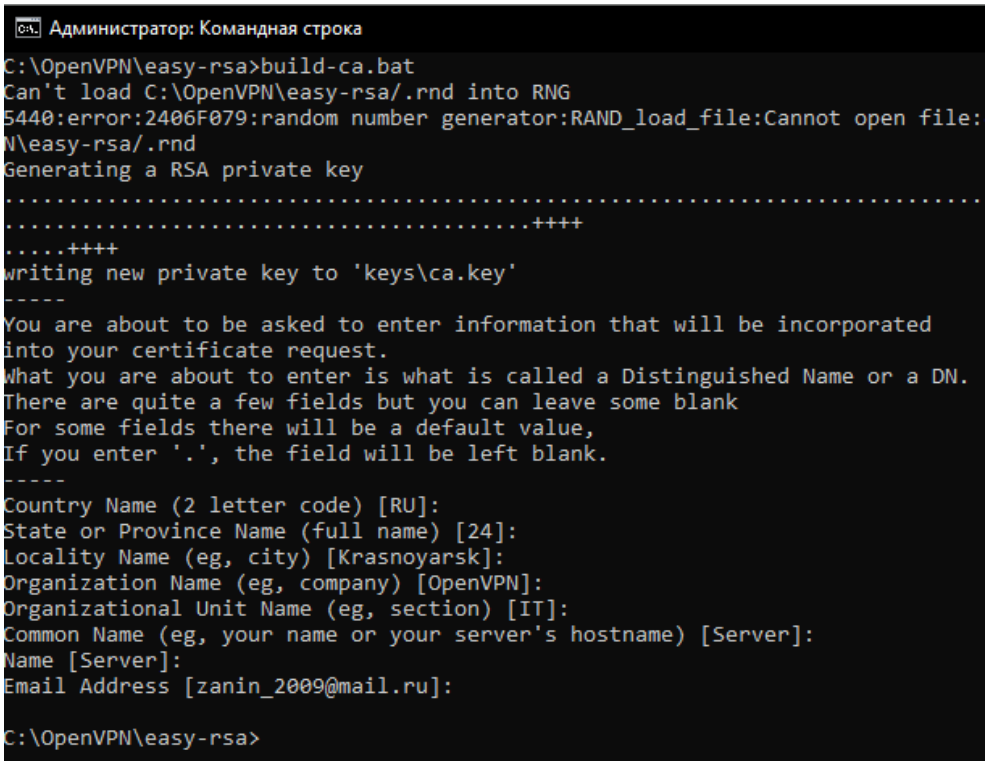

Рисунок 13 – Команда build-ca.bat

Создать DH-ключ с помощью запуска файла через команду “build- dh.bat”

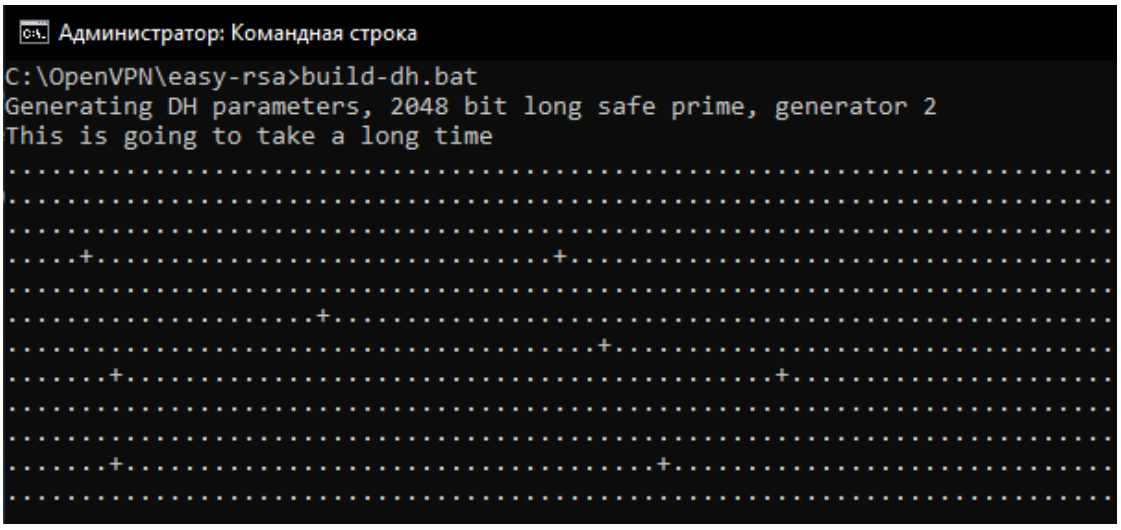

Рисунок 14 – Создание DH-ключа

Приготовить сертификат для серверной части. Ему присвоить то имя, которое прописано в vars.bat в строке “KEY_NAME” это Server. Команда выглядит так: build-key-server.bat Server. Подтвердить данные: для этого нажать ENTER, ввести букву “y”(yes). Командную строку закрыть [5].

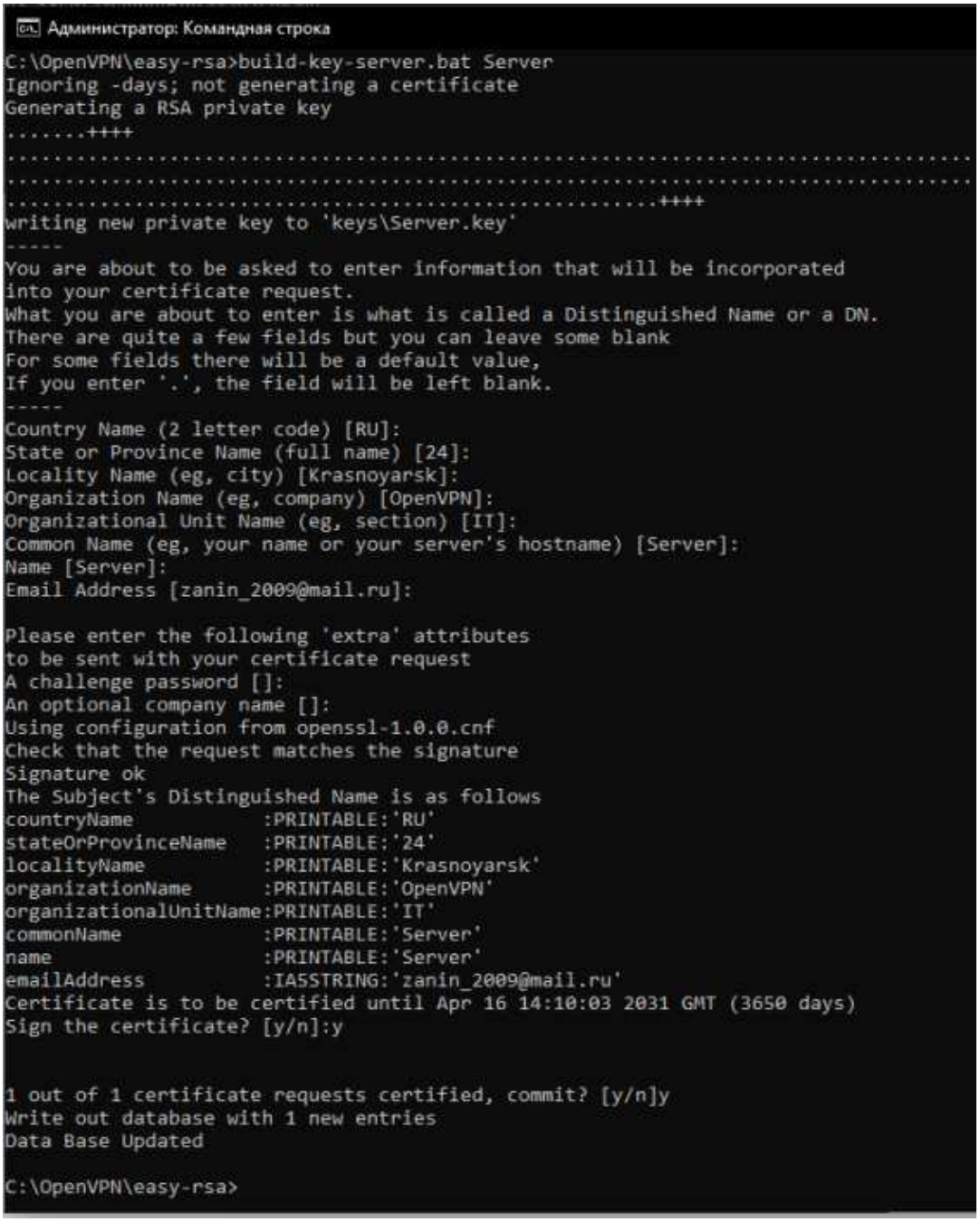

Рисунок 15 – Сертификат для серверной части

В папке “easy-rsa” появится новая папка с названием “keys”

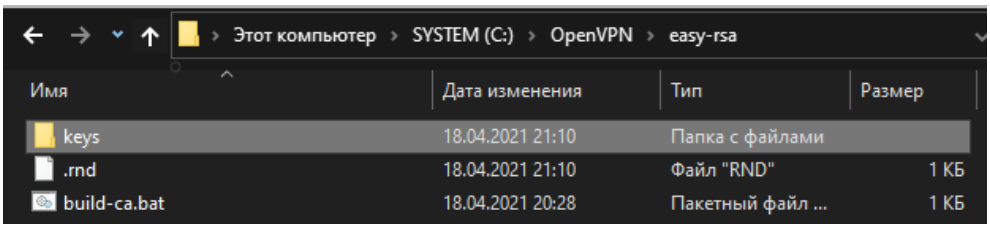

Рисунок 16 – Папка keys

Содержимое папки “keys”. скопировать в папку “ssl”, которую нужно создать в корневом каталоге программы.

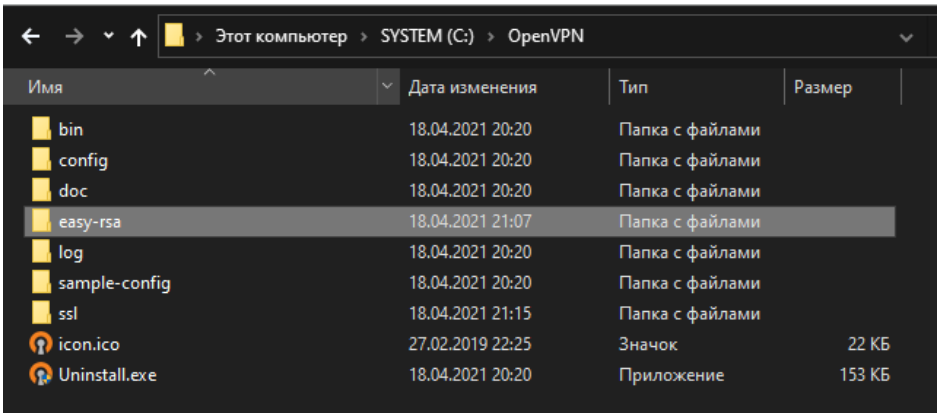

Рисунок 17 – Создание папки ssl

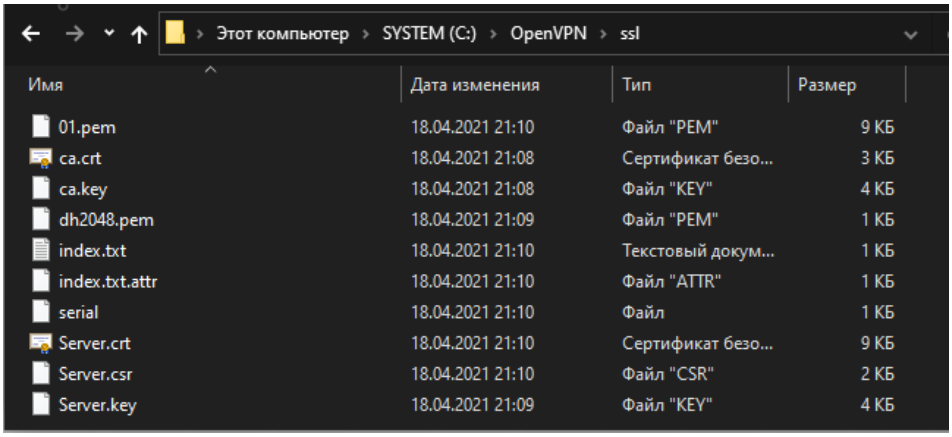

Рисунок 18 – Содержимое папки ssl

Открыть каталог “C:\OpenVPN\config”. Создать текстовый документ, переименовать его в “server.ovpn” и открыть. Ввести следующий код:

port 1194 – порт, через который будет производиться подключение

proto udp – протокол подключения

dev tun – виртуальный сетевой драйвер

dev-node "Server" – устанавливает имя виртуального интерфейса

dh C:\\OpenVPN\\ssl\\dh2048.pem – путь к DH ключу

ca C:\\OpenVPN\\ssl\\ca.crt – путь к сертификату

cert C:\\OpenVPN\\ssl\\Server.crt – путь к сертификату

key C:\\OpenVPN\\ssl\\Server.key – путь к ключу

server 10.8.0.0 255.255.255.0 – ip сервера

max-clients 32 – максимальное количество клиентов

keepalive 10 120 – совмещенная команда ping и ping-restart. Использует сразу два параметра в секундах, перечисленных через пробел.

client-to-client – с помощью этой команды клиенты видят друг друга в сети.

comp-lzo – параметр сжатия трафика

persist-key – не перечитывать ключи при перезапуске туннеля.

persist-tun – команда оставляет без изменения устройства tun или tap при перезапуске OpenVPN.

cipher AES-256-CBC – алгоритм шифрования

status C:\\OpenVPN\\log\\status.log – указываем статус-файл

log C:\\OpenVPN\\log\\openvpn.log – указываем лог-файл

verb4 – устанавливает уровень информативности отладочных сообщений

mute 20 – количество сообщений логов из одной категории

Для работы виртуального адаптера нужно сделать следующие:

Открыть панель управления – центр управления сетями – изменение параметров адаптера. Найти подключение, осуществляемое через “TAP-Windows Adapter V9”. Переименовать его в “Server”. Это название совпадает с параметром “dev-node”в файле server.ovpn.

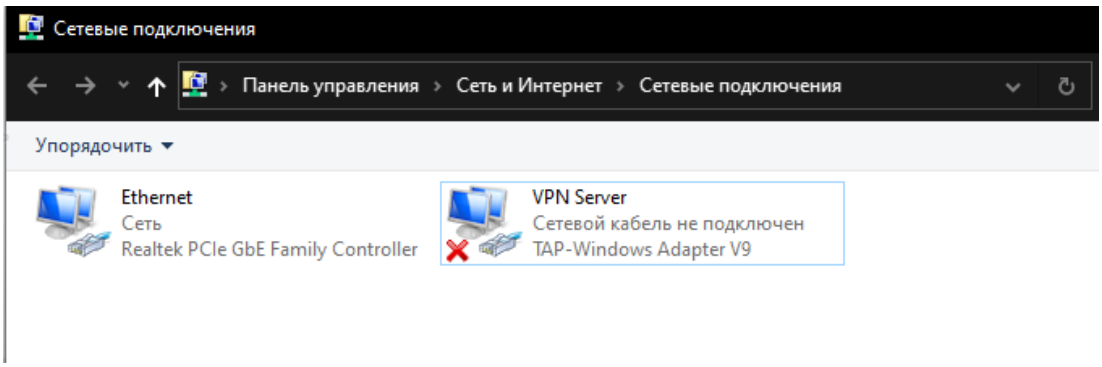

Рисунок 19 – TAP-Windows Adapter V9

Запустить службу нажатием сочетание клавиш Win+R, ведя в строку “services.msc” и нажать ENTER. Найти сервис с названием “OpenVpnService”, кликнув правой кнопкумышки и открыть его свойства. Тип запуска поменять на “Автоматически” запустить службу и нажать“Применить” [1].

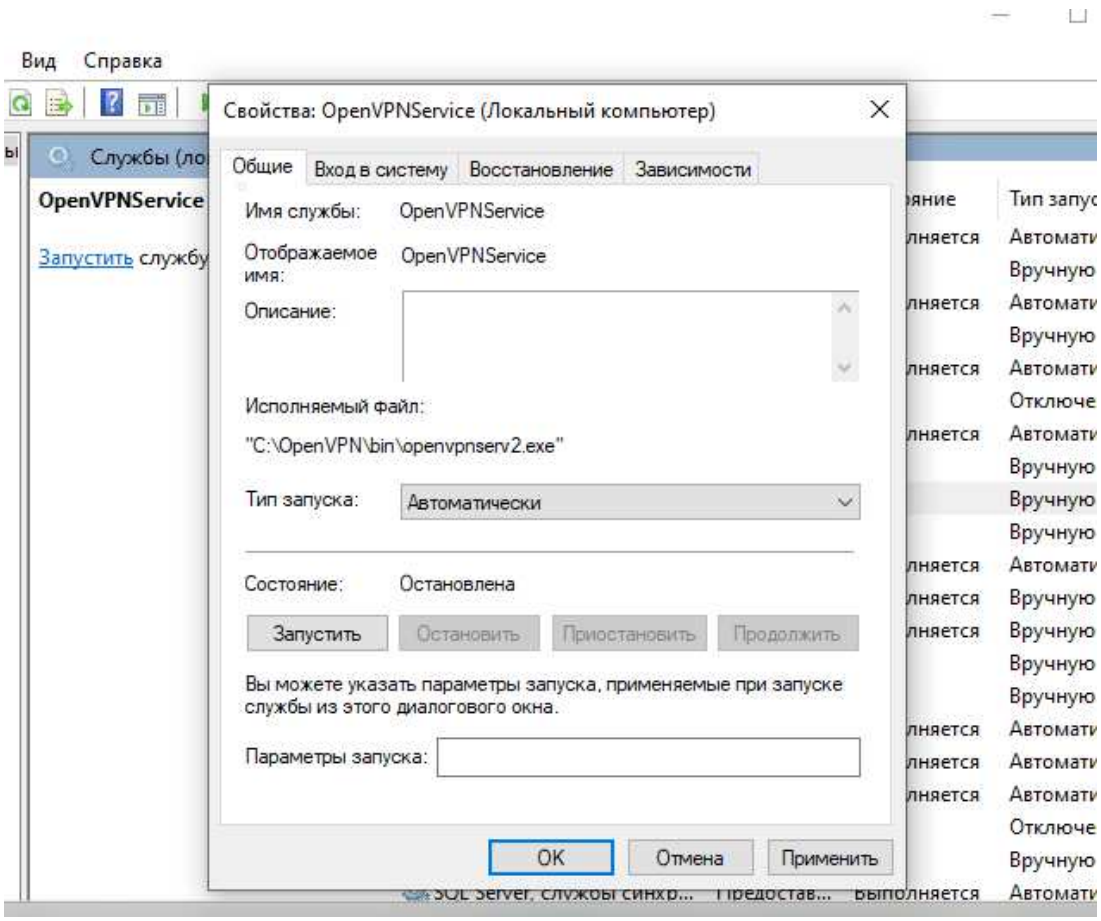

Рисунок 20 – Запуск службы OpenVPNService

3.2 Установка и настройка клиента OpenVPN

Для создания клиентских сертификатов и ключей нужно:

Открыть папку “keys”. Удалить все содержимое файла “index.txt”, сохранить файл.

Запустить командную строку. Ввести команду vars.bat, а затем создать клиентский сертификат с названием “Client” командой “build-key-server.bat Client”.

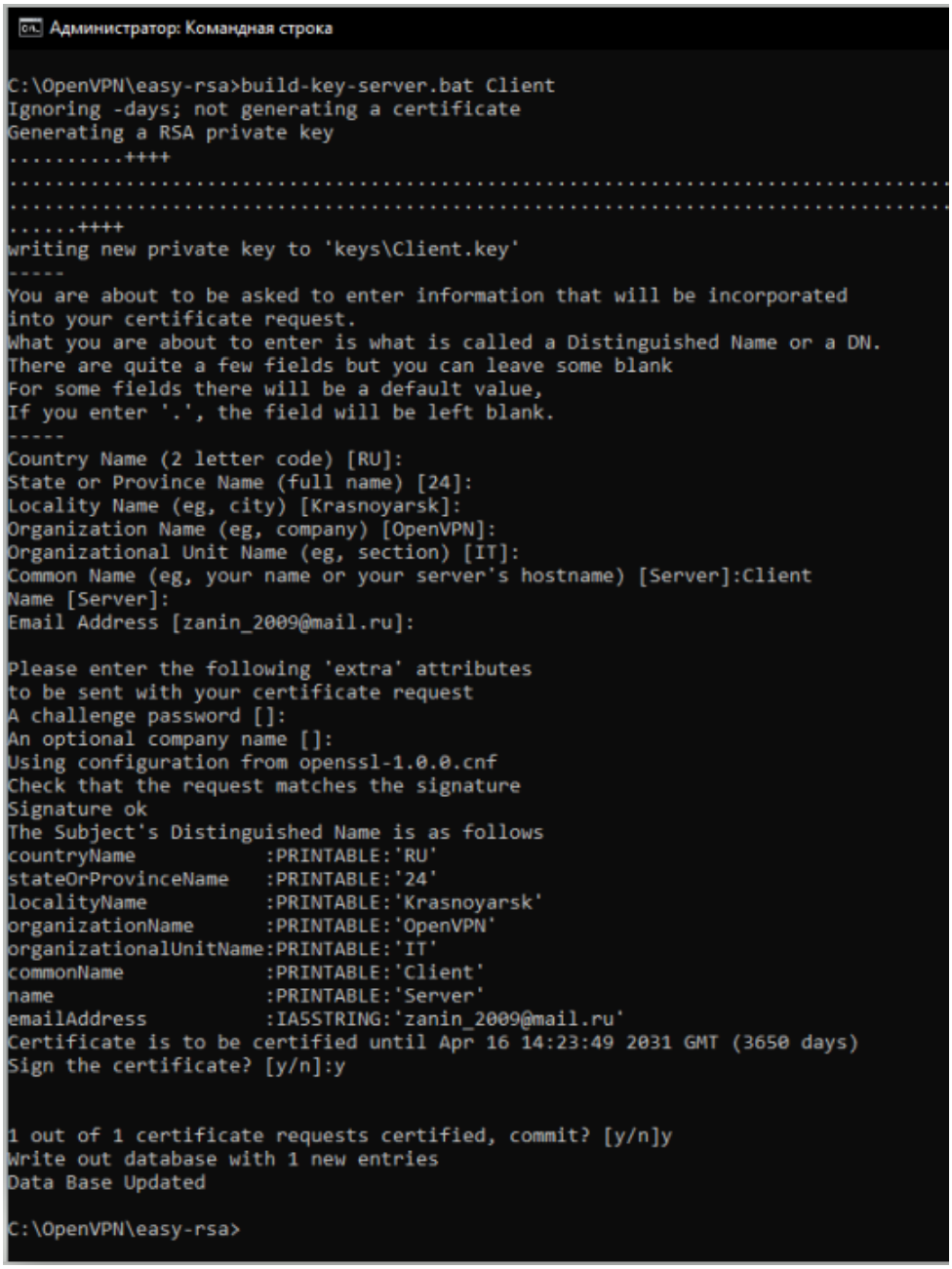

Рисунок 21 – Создание клиентского сертификата

В целях безопасности, для каждого клиента можно сгенерировать свои файлы.Но их названия должно отличаться, например, “Client1” и так далее. В этом случае необходимо будет повторять все действия, начиная с очистки index.txt.

Создать конфигурациооный файл для клиента “Client.ovpn”. Для этого нужно открыть каталог “C:\OpenVPN\config”. Создать текстовый документ, переименовать его в “Client.ovpn” и открыть. Вести следующий код:

client – имя клиента

remote 192.168.1.245 – ip удалённого доступа.

proto udp – протокол.

ca ca.crt – файл сертификата для CA.

cert Client.crt – файл сертификат клиента.

key Client.key – файл ключ клиента.

dh dh2048.pem – файл dh.

cipher AES-256-CBC – алгоритм шифрования.

comp-lzo – параметр сжатия трафика.

3.3 Настройка маршрутизатора

Для того чтобы VPN клиенты, находясь за пределами сети, могли подключаться к VPN серверу, который находится во внутренней сети организации, на маршрутизаторе было настроено перенаправление портов.

Резервироваине ip-адреса за сервером.

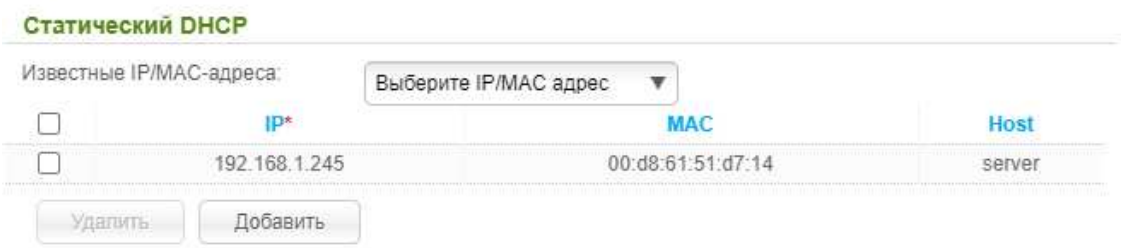

Рисунок 23 – Резервирование ip-адреса

Виртуальные серверы

	Имя	Интерфейс	Протокол	Внешний порт	Внутренний порт	Внутренний IP	Удаленный IP
☐	port1194	<Все>	UDP	1194	1194	192.168.1.245	

Добавить | Удалить | Удалить все

Рисунок 24 – Перенаправление порта 1194

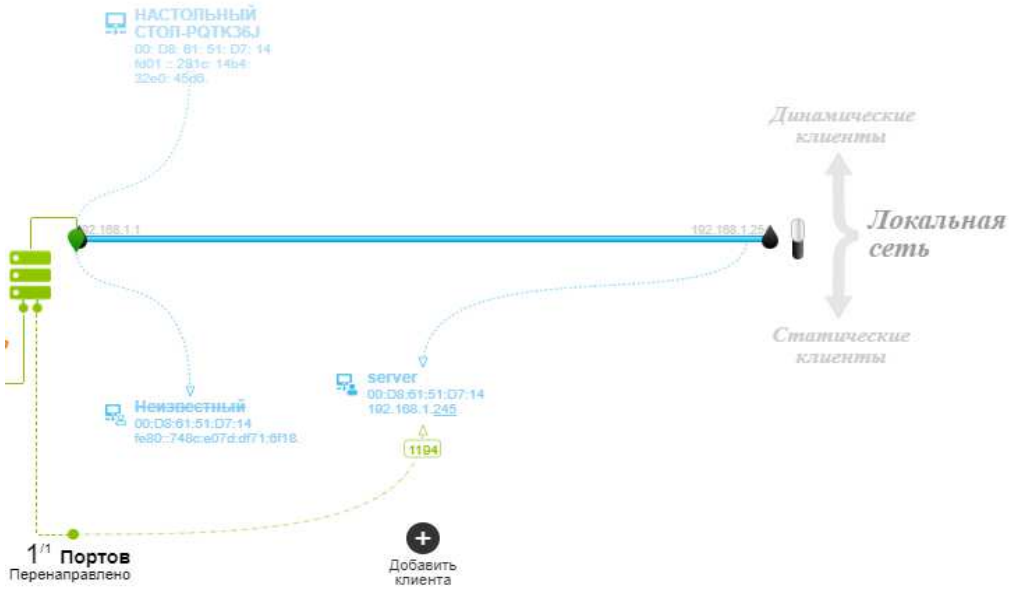

Рисунок 25 – Перенаправление порта 1194

Статус / Сетевая статистика

Имя	IP - Шлюз	MAC	Rx/Tx	Длительность, мин	
WIFI	-	90:8D:78:F9:3F:C6	156.71 МБайт / 2.17 ГБайт	-	›
dynamic_Internet_2	91.132.20.143/24 - 91.132.20.1	90:8D:78:F9:3F:C5	2.96 ГБайт / 3.85 ГБайт	21.3	›
LAN	192.168.1.1/24 - -	90:8D:78:F9:3F:C6	60.96 МБайт / 156.33 МБайт	-	›

Рисунок 26 –Настройка WAN

4 Тестирование системы

Установливаем OpenVPN обычным способом на компьютер. Запускаем файл конфигурацию Client.ovpn. Подключаемся к серверу.

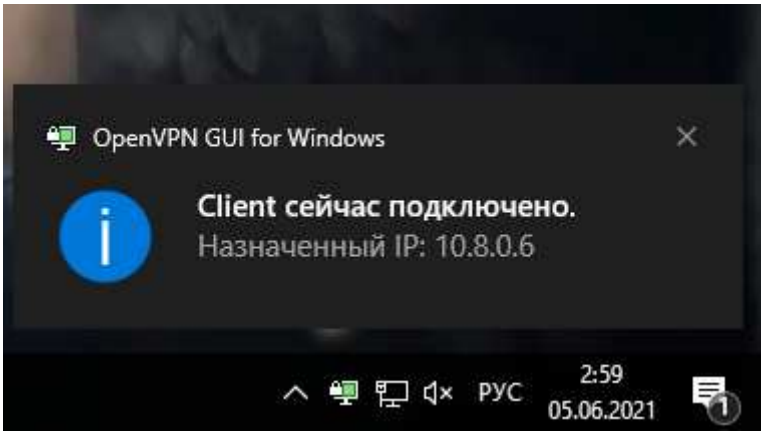

Рисунок 27 – Подключение клиента к серверу

Проверка подключения клиента к серверу организации. Для этого прописать локальный IP компьютера (через двойной обратный слеш ”\\”) организации на который есть доступ в локальной сети предприятия.

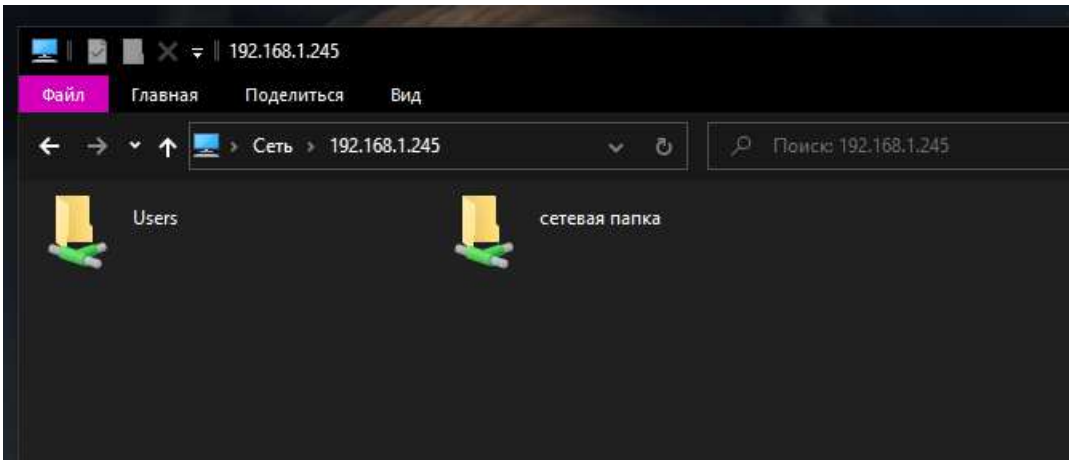

Рисунок 28 – Подключение клиента к серверу

Проверка подключения сервера организации к клиенту. Для этого необходимо прописать локальный IP компьютера (через двойной обратный слеш”\\”) сети клиента.

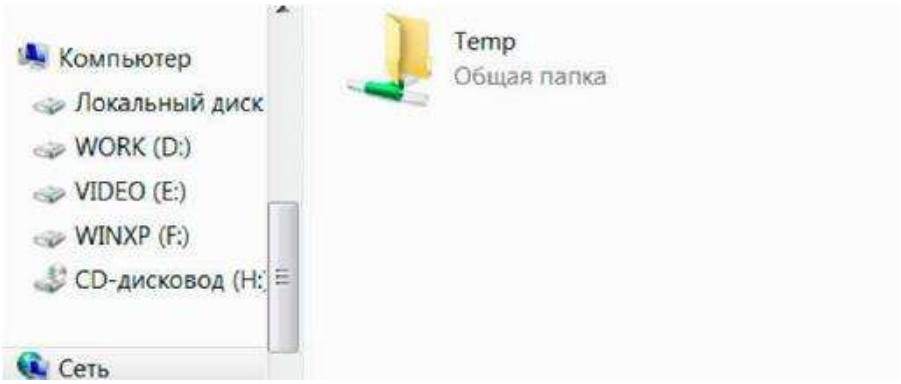

Рисунок 29 – Подключение сервера к клиенту

Проверка сетевого окружения. Для этого необходимо зайти в папку сеть с клиента.

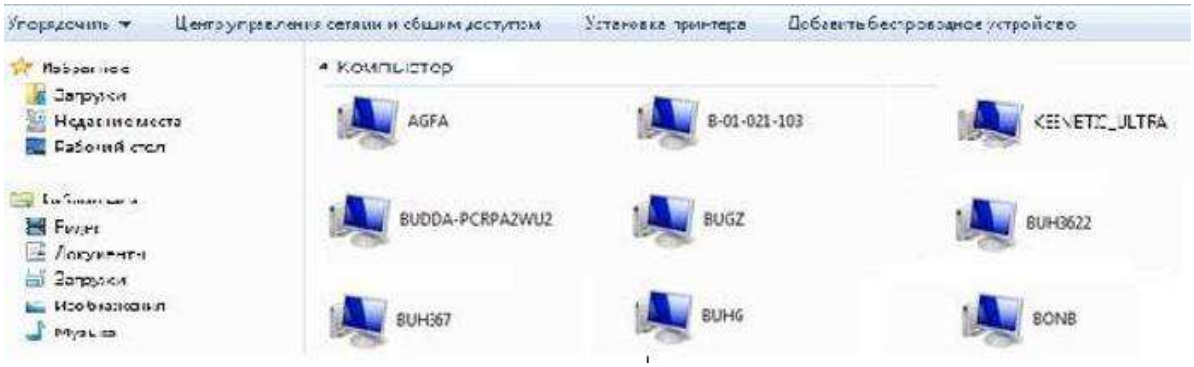

Рисунок 30 – Сетевое окружение

5 Заключение

OpenVPN - свободная реализация технологии виртуальной частной сети (VPN) с открытым исходным кодом для создания зашифрованных каналов типа точка-точка или сервер-клиенты между компьютерами. Она позволяет устанавливать соединения между компьютерами, находящимися за NAT и сетевым экраном, без необходимости изменения их настроек.

Теоретическая часть диплома описывает аспекты и термины, а также определение и состав: VPN, протоколы (TCP и UDP), протоколы шифрованияи OpenVPN.

Практическая часть диплома описывает разработку системы удаленного доступа для организации, основные идеи и концепции. Был организован удалённый доступ к локальной сети через Open VPN. Реализована лёгкая конфигурация для клиента, где не требуется никаких настроек на своем компьютере, а просто запуск файла конфигурации.

В данной работе были подробно рассмотрены и проанализированы: VPN, протоколы (TCP и UDP), протоколы шифрования и OpenVPN.

Перед началом работы была поставлена цель работы:

- Разработать систему удалённого доступа в сеть предприятия.

Для досижения этой цели были выполнены следующие задачи:

- Изучить технологии VPN, выбрать технологию для использования в системе;
- Разработать общую архитектуру системы;
- Разработать конфигурации аппаратного и программного обеспечения;
- Реализавать прототип системы удаленного доступа.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Настройка VPN - соединения для Windows. [ссылка]. [просмотрено 21.04.2021] http://www.tomtel.ru/tariffsandconnection/vpn/vpnconf7.html
2. Построение безопасных сетей на основе VPN. [ссылка]. [просмотрено 22.14.2021] http://www.aitishnik.ru/seti/postroenie-bezopasnich- setey-na-osnove-vpn.html
3. Построение виртуальных частных сетей OpenVPN [ссылка]. [просмотрено 22.04.2021] https://lvee.org/ru/articles/149
4. Организация VPN-каналов [ссылка]. [просмотрено 21.04.2021] http://interface31.ru/tech_it/2011/09/organizaciya-vpn-kanalov-mezhdu-ofisami.html
5. Руководство по настройке и установке OpenVPN [ссылка]. [просмотрено 17.04.2021] http://habrahabr.ru/post/233971/
6. OpenVPN, краткое описание [ссылка]. [просмотрено 20.04.2021] https://7d3.ru/wiki/166
7. PPTP [ссылка]. [просмотрено 21.04.2021] https://ru.wikipedia.org/wiki/PPTP
8. IPsec [ссылка]. [просмотрено 21.04.2021] https://ru.wikipedia.org/wiki/IPsec
9. Википедия – Open VPN. [ссылка]. [просмотрено 19.04.2021] https://ru.wikipedia.org/wiki/OpenVPN
10. VPN. [ссылка]. [просмотрено 21.04.2021] http://www.cisco.com/web/RU/products/sw/netmgtsw/ps2327/index.html
11. Туннельные протоколы VPN. [ссылка]. [просмотрено 19.04.2021] https://technet.microsoft.com/ru-ru/library/cc771298%28=ws.10%29.apx

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Космических и информационных технологий
институт

Вычислительная техника
кафедра

УТВЕРЖДАЮ
Заведующий кафедрой
_____ О. В. Непомнящий
подпись инициалы, фамилия
« 25 » 06 2021 г.

БАКАЛАВАРСКАЯ РАБОТА

09.03.01 Информатика и вычислительная техника
код и наименование направления

Система удаленного доступа в сеть предприятия
тема

Пояснительная записка

Руководитель	Коршун 05.06.21	доцент, канд.физ-мат.наук	К. В. Коршун
	подпись, дата	должность, ученая степень	инициалы, фамилия
Выпускник	05.06.21		С. В. Занин
	подпись, дата		инициалы, фамилия
Нормоконтролер	Коршун 05.06.21	доцент, канд.физ-мат.наук	К. В. Коршун
	подпись, дата	должность, ученая степень	инициалы, фамилия

Красноярск 2021