МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет
имени К.И. Сатпаева

Институт информационных и телекоммуникационных технологий

Кафедра «Электроника, телекоммуникации и космические технологии»

Рсалімова Мадина Батырқызы

Анализ технологии VPN и ее построение

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
к дипломному проекту

специальность 5В071900 – Радиотехника, электроника и телекоммуникация

Алматы 2019

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет
имени К.И. Сатпаева

Институт информационных и телекоммуникационных технологий

Кафедра «Электроника, телекоммуникации и космические технологии»

ДОПУЩЕН К ЗАЩИТЕ
Заведующий кафедрой ЭТиКТ
канд.техн.наук
_____ Е. Таштай
“ 13 ” 05 2019г

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
к дипломному проекту

На тему: Анализ технологии VPN и ее построение

по специальности 5В071900 – Радиотехника, электроника и телекоммуникации

Выполнила Рсалимова М.Б.

Рецензент
канд. техн. наук, профессор АУЭС
_____ А.С. Байкенов
_____ 2019г.

Научный руководитель
маг-р техн. наук, лектор
_____ Г.М. Байкенова
“ 6 ” 05 2019г.

Алматы 2019

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет имени К.И. Сатпаева

Институт информационных и телекоммуникационных технологий

Кафедра «Электроника, телекоммуникации и космические технологии»

5В071900 – Радиотехника, электроника и телекоммуникации

УТВЕРЖДАЮ
Заведующий кафедрой ЭТиКТ
канд.техн.наук
_____Е. Таштай
"02" "02" 2019 г.

ЗАДАНИЕ
на выполнение дипломного проекта

Обучающемуся *Ресалімовой Мадине Батырқызы*
Тема *Анализ технологии VPN и ее построение*
Утверждена *приказом Ректора Университета* № 1162-б от " 16 " 10 2018г.
Срок сдачи законченного проекта " 16 " мая 2019г.
Исходные данные к дипломному проекту: *Схема корпоративной сети компании в городе Нур-Султан. Общая схема организации сети. Оборудование от компании Cisco. Программа моделирования Cisco Packet Tracer.*
Перечень подлежащих разработке в дипломном проекте вопросов:
а) *Анализ виртуальных частных сетей (VPN)*
б) *Построение сети с применением технологии виртуальных частных сетей*
в) *Необходимые технические расчеты для реализации проекта*
Перечень графического материала (с точным указанием обязательных чертежей): *Отличие частной сети от виртуальной частной сети, передача данных сквозь туннель, установление IP-соединения с туннельным сервером PPTP, соединение IPSec, принцип подключения протокола SSL VPN.*

Рекомендуемая основная литература: *1) Денисова Т.Б. «Надежность и безопасность услуги VPN»; 2) С. В. Запечников, Н. Г. Милославская, А.И. Толстой. Основы построения виртуальных частных сетей. – М: Горячая линия – Телеком, 2003.*

ГРАФИК

подготовки дипломной работы (проекта)

Наименования разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю и консультантам	Примечание
Анализ виртуальных частных сетей	8.02.2019	выполнено
Проектирование корпоративной сети по технологии VPN	22.03.2019	выполнено
Модель виртуальной частной сети для предприятия	21.04.2019	выполнено

Подписи

консультантов и нормоконтролера на законченную дипломную работу (проект) с указанием относящихся к ним разделов работы (проекта)

Наименования разделов	Консультанты, И.О.Ф. (уч. степень, звание)	Дата подписания	Подпись
Нормоконтролер	доктор PhD Тайсариева К.Н	6.05.19	

Научный руководитель _____Г.М. Байкенова
(подпись)

Задание принял к исполнению обучающийся _____М.Б. Рсалімова
(подпись)

Дата "__16__"___10_____2018г.

АННОТАЦИЯ

Современная корпоративная инфраструктура включает территориально-распределенные подразделения. Для их интегрирования в единую сеть нужны технологии, которые передают трафик в защищенном режиме. Концепция создания виртуальных частных сетей (VPN) активно развивается, чтобы обеспечить эффективное и безопасное использование сетевых атак в открытых сетях.

В дипломном проекте дается анализ виртуальной частной сети, ее сущность. Рассматриваются различные технологии, концепции построения, протоколы VPN. Показан пример построения корпоративной сети с VPN, а также настройка оборудования с использованием программы Cisco Packet Tracer .

АҢДАТПА

Қазіргі корпоративтік инфрақұрылым географиялық бөлінген бірліктерді қамтиды. Оларды бірыңғай желіге біріктіру үшін бізге трафикті қауіпсіз режимге жіберетін технологиялар қажет. Виртуалды жеке желілерді (VPN) құру тұжырымдамасы ашық желілерде желілік шабуылдарды тиімді және қауіпсіз пайдалануды қамтамасыз ету үшін белсенді түрде дамып келеді.

Дипломдық жобада виртуалды жеке желінің талдауы, оның мәні. Түрлі технологиялар, құрылыстық ұғымдар, VPN хаттамалары қарастырылады. VPN корпоративтік желісін құрудың үлгісі, сондай-ақ Cisco Packet Tracer көмегімен жабдықты орнату мысалы көрсетілген.

ANNOTATION

Modern corporate infrastructure includes geographically distributed units. To integrate them into a single network, we need technologies that transmit traffic in a secure mode. The concept of creating virtual private networks (VPN) is being actively developed to ensure the effective and secure use of network attacks in open networks.

In the thesis project provides an analysis of the virtual private network, its essence. Various technologies, building concepts, VPN protocols are considered. Shown is an example of building a corporate network with a VPN, as well as setting up equipment using Cisco Packet Tracer.

СОДЕРЖАНИЕ

Введение		9
1	Анализ виртуальных частных сетей	10
1.1	Глобальные сети и технология виртуальных частных сетей	10
1.2	Различные технологии VPN	11
1.3	Сущность технологии VPN	12
1.3.1	Концепция построения виртуальных защищенных сетей VPN	12
1.3.2	Разновидности протоколов для построения VPN	14
1.4	Постановка задачи	19
2	Проектирование корпоративной сети по технологии VPN.	23
2.1	Способы построенияVPN	23
2.2	Сеть на базе Dinamic Multipoint VPN	26
2.3	Выбор необходимых технических средств	28
2.3.1	Выбор кабеля	28
2.3.2	Выбор коммутатора	30
2.3.3	Выбор маршрутизатора	32
3	Расчетная часть	35
Заключение		
Перечень принятых сокращений, терминов		
Список использованной литературы		

ВВЕДЕНИЕ

Современное развитие информационных технологий и, в частности, Интернета, требует защиты информации, предоставляемой в выделенной корпоративной сети с использованием сетей открытого доступа.

До появления «всемирной паутины» – Интернета – не всякая компания могла позволить себе пользоваться закрытыми сетями, охватывающими большие территории, когда доступ к ее ресурсам могли получить только пользователи этой сети, так как каналы связи были очень дорогими. В настоящее время, с развитием сети Интернет, появилась новая тенденция – использование для конструирования всеобщей корпоративной связи в основном недорогого и доступного (если сравнить с выделенными каналами) транспорта: IP сетей всеобщего пользования (внешние сети). Однако Интернет – это незащищенная сеть, поэтому приходиться изобретать способы защиты конфиденциальных данных, передающихся через незащищенную сеть.

Для корпоративных сетей важны такие особенности, как скорость и качество обслуживания клиентов, предоставление заданного набора услуг и гарантий, которые редко обеспечишь во внешних сетях. Чтобы решить все эти проблемы можно использовать технологию виртуальных частных сетей (VPN). VPN – технология, объединяющая защищенные сети, узлы и пользователей с ненадежными открытыми сетями. Это одна из самых распространенных технологий не только для технических специалистов, но и для простых пользователей. Информация должна быть защищена (например, интернет-банкинг или пользователи интернет-портала).

Одними из ключевых отличительных особенностей больших регионально-рассредоточенных корпоративных сетей считаются: использование глобальных связей и соединение внутренних частных сетей разных филиалов компаний и компьютеров его отдаленных работников с централизованной частной сетью; техобслуживание огромной численности разных клиентов. Эти функции к тому же демонстрируют оптимальность создания сетей с использованием технологии VPN, которые дают возможность совместить правила безопасности к разрешаемым услугам системы. Однако ради продуктивного ее использования нужно решить ряд главных задач, которые связаны с выбором построения сети, формированием работы клиентов и сетей, гарантированием необходимого уровня безопасности информаций и нужных параметров отправки и принятий данных.

Мой дипломный проект посвящен анализу работы и способу организации VPN для объединения территориально-рассредоточенных офисов корпоративной сети.

1 Анализ виртуальных частных сетей

1.1 Глобальные сети и технология виртуальных частных сетей

WAN (Wide Area Network) – глобальная сеть, покрывающая большие географические регионы, включающие в себя как локальные сети, так и прочие телекоммуникационные сети и устройства (рисунок 1.1).

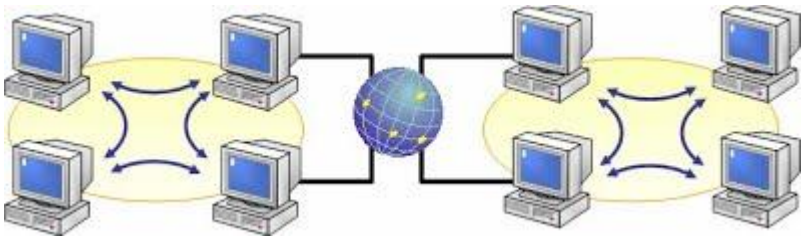

Рисунок 1.1 – Глобальная сеть

На сегодняшний день внедрение виртуальных частных сетей на основе Интернет протокола (IP) стало основным способом организации корпоративных территориально-разнесенных сетей с использованием выделенных линий, Frame Relay и других традиционных технологий для глобальных сетей.

Ранее для безопасной передачи данных требовалась необходимость в выделенной линии, связывающей два пункта. Стоимость организации таких сетей довольно высока.

Виртуальная частная сеть предоставляет пользователям безопасный способ доступа к ресурсам корпоративной сети через Интернет или другие публичные или частные сети без необходимости подключения к сети.

Рисунок 1.2 – Отличие частной сети от виртуальной частной сети

Безопасные частные виртуальные сети – это набор технологий / сервисов для туннелирования, аутентификации, контроля доступа и управления, используемых для защиты данных и передачи трафика через Интернет.

Суть виртуальных частных сетей (Virtual Private Network, VPN) проста: она может быть аналогом частной сети (определенного ресурса) в публичной

сети (общего ресурса) и может быть Интернетом или инфраструктурой последнего или определенного оператора.

Этот метод давно используется со времен сетей X.25 и Frame Relay. Новые технологии, особенно MPLS, теперь расширяют возможности VPN, такие как распределенный соединитель Ethernet (L2 VPN) или IP-сеть (L3 VPN).

1.2 Различные технологии VPN

Различные технологии VPN означают другую «глубину» связи с оператором. Например, связь между удаленными офисами в небольших компаниях часто достигается путем организации туннелей через Интернет с использованием протокола IPSec. В этом случае взаимодействие с оператором очень низкое: подключение к Интернету должно обеспечиваться через канал с необходимой пропускной способностью, а задача создания VPN решается специалистами компании или ее партнером по интеграции.

Основными преимуществами этого подхода являются его низкая стоимость, а также возможность быстрой настройки VPN в любом месте - не нужно связываться с конкретным оператором для подключения к определенным услугам, и сегодня доступ к Интернету практически одинаков. Закрытые туннели IPSec можно организовать не только между офисом, но и между офисом и компьютером, клиентом или командировкой домашнего сотрудника.

Для этих целей могут использоваться и другие протоколы VPN, функционирующие по схеме «пользователь — шлюз»: SSL/TLS, PPTP, L2TP.

Популярность IPSec VPN во многом зависит от доступности соответствующих устройств. При всех своих преимуществах технология IPSec VPN имеет массу недостатков.

Криптотуннели через Интернет обычно используются для предоставления несущественной информации для организации резервных каналов связи в случае задержки или отказа основного канала. Этот недостаток IPSec VPN создает иллюзию независимости от операторов связи, поскольку отсутствует поддержание параметров связи между удаленными подразделениями предприятия.

IPSec VPN — классический пример виртуальной частной сети, построенной по так называемой наложенной модели (Overlay), когда оборудование сервис-провайдера не задействуется в процессе маршрутизации клиентского трафика, а его сеть предоставляет лишь «прозрачное» соединение между площадками предприятия.

Другая модель организации VPN — одноранговая (Peer) — подразумевает взаимодействие устройств (маршрутизаторов/коммутаторов) клиента с оборудованием сервис-провайдера, которое задействуется для маршрутизации клиентского трафика. В идеале клиенту предоставляется

отдельный выделенный маршрутизатор — в настоящее время это, как правило, виртуальный маршрутизатор с поддержкой IP/MPLS. Сетевая безопасность при этом обеспечивается дополнительными административно-техническими методами, такими как фильтрация пакетов и маршрутов.

1.3 Сущность технологии VPN

Задача создания корпоративной компьютерной сети в одном здании может быть относительно легко решаемой. Однако современная корпоративная инфраструктура включает территориально распределенные подразделения, партнеров, клиентов и поставщиков. Поэтому было гораздо сложнее построить корпоративную сеть.

В связи с быстрым развитием Интернета и сетей доступа сообщества произошел качественный шаг к распространению информации и доступу к ней. Пользователи получили дешевые и доступные интернет-каналы. Предприятия пытаются использовать такие каналы для предоставления такой коммерческой и управленческой информации.

Для эффективного противодействия сетевым атакам и обеспечения возможности активного и безопасного использования в бизнесе открытых сетей в начале 1990-х гг. родилась и активно развивается концепция построения виртуальных частных сетей — VPN (Virtual Private Network).

Сущность виртуальных частных сетей заключается в использовании публичной телекоммуникационной и/или сетевой инфраструктуры (например, Интернет) для обеспечения безопасного доступа удаленных филиалов и сотрудников к основной сети организации (Remote Access VPN) или для объединения географически удаленных локальных сетей (LAN-to-LAN VPN).

1.3.1 Концепция построения виртуальных защищенных сетей VPN

Интернет стал неотъемлемой частью нашей жизни. Достоинства Интернета на основе протокола TCP/IP бесспорны: это мощная, хорошо продуманная и надежная сеть, обеспечивающая уверенную передачу данных; адресное пространство, хоть и не беспредельно, но очень велико.

Сегодня Интернет резко вырос и стал практически неисчерпаемым источником информации различными способами. Кроме того, это быстрый и надежный способ общения. Но, к сожалению, преимущества Интернета – это его недостатки. Таким образом, прозрачность сети для подключения новых компьютеров и доступа к информации, представленной в сетевых пакетах, не защищена данными пользователей Интернета.

Это было особенно важно из-за развития электронной коммерции, частого использования услуг интернет-платежей и интенсивного взаимодействия между людьми в разных частях сети.

Концепция виртуальной VPN основана на простой идее: если в глобальной сети есть два узла для обмена информацией, необходимо построить виртуальный безопасный туннель между двумя узлами, чтобы обеспечить конфиденциальность и целостность информации, передаваемой через открытые узлы, получая доступ к виртуальному туннелю всех активных и пассивных внешних это должно быть очень трудно для наблюдателей.

В настоящее время VPN конкурирует с глобальными сетями WAN (Wide Area Network). VPN успешно интегрируют инфраструктуру удаленного офиса в единую корпоративную сеть онлайн, что сводит к минимуму стоимость корпоративной сети. Кроме того, при доступе к Интернету любой сотрудник компании может без проблем подключиться к своей корпоративной сети из любой точки мира.

Наиболее универсальным способом построения VPN является использование технологии инкапсуляции, или туннелирования. В общем случае туннелирование применяется для того, чтобы передавать пакеты одной сети (первичной) по каналам связи другой (вторичной), протоколы которых не совместимы. Для этого пакет первичной сети (данные и протоколы) инкапсулируется в пакет вторичной сети и становятся видны как данные. Таким образом, пакет продвигается маршрутизаторами ядра сети только на основании внешнего заголовка, без инспекции содержимого оригинального пакета. Это иллюстрирует рисунок 1.3, на котором показана передача данных от A к B по туннелю между X и Z. Промежуточный узел Y не знает адреса получателя B, а передает данные по туннелю только узлу Z. В этом сценарии узел X называется входом в туннель, а узел Z – выходом.

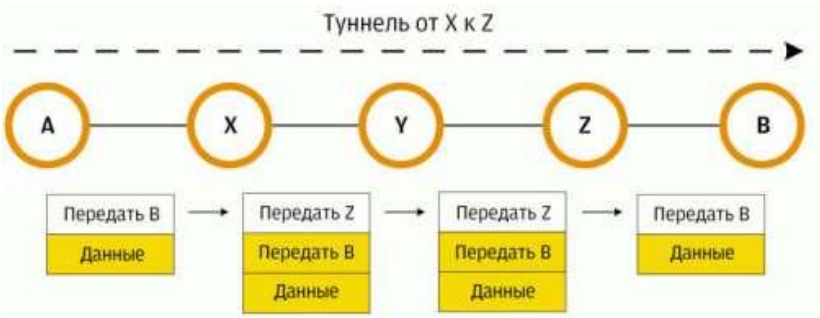

Рисунок. 1.3 – Передача данных сквозь туннель

Как правило, инкапсуляция не включает кодирование. Если нужно повысить уровень безопасности, это делается через частную сеть перед процедурой инкапсуляции. Функционально туннель можно представить как сквозной виртуальный канал, имеющий начальную точку (вход, инициатор туннеля) и одну или более конечных (выходов, терминаторов туннелей).

1.3.2 Разновидности протоколов для построения VPN

Известно, что существует «слабое место» в зависимости от структуры протокола IP сетей, использующих протокол IP. IP-разработчики не предоставляют каких-либо функций безопасности в области IP, а гибкость IP позволяет максимально использовать преимущества этого протокола для преодоления контроля трафика, контроля доступа и других мер безопасности. Поэтому сетевые данные, использующие протокол IP, могут быть легко подделаны и перехвачены.

Когда туннелирование передается в пакетной сети с сетевым протоколом, они внедряются или инкапсулируются в пакеты протокола в другой сети. Это обеспечивает безопасность при передаче данных.

PPTP.

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).

Рисунок 1.4 – Место протокола PPTP в модели OSI

PPTP обеспечивает безопасную передачу данных на один корпоративный сервер, создавая отдельную виртуальную сеть в сети TCP/IP с удаленного клиента. PPTP также можно использовать для установки туннеля между двумя локальными сетями. PPTP работает, устанавливая обычную PPP-сессию с противоположной стороной с помощью протокола Generic Routing Encapsulation (GRE). Второе соединение на TCP порту 1723 используется для инициации и управления GRE-соединением. Протоколы MPPE могут использоваться для защиты данных трафика PPTP. Для аутентификация клиентов могут использоваться различные механизмы, наиболее безопасные из них – MSCHAPv2 и EAP-TLS.

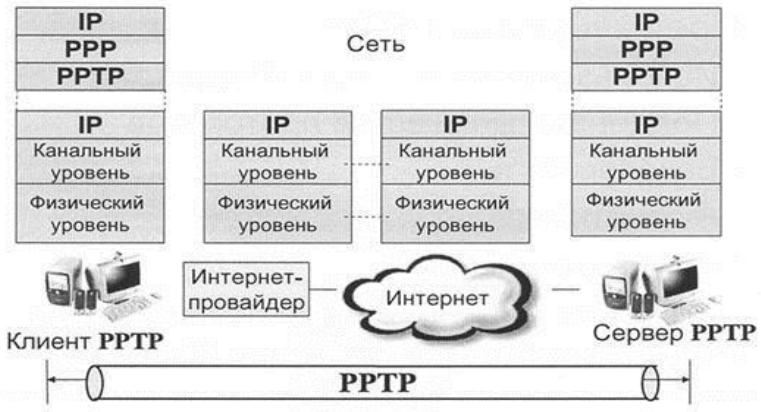

Рисунок 1.5 – Установление IP-соединения с туннельным сервером PPTP

Чтобы работать с клиентским протоколом PPTP, необходимо установить IP-соединение с сервером туннелирования PPTP (рисунок 1.5). Все данные, передаваемые через это соединение, могут быть защищены и сжаты. Туннель PPTP может передавать данные из разных сетевых протоколов (TCP / IP, NetBEUI и IPX).

L2TP.

L2TP (Layer 2 Tunneling Protocol) – протокол туннелирования уровня 2 (канального уровня). 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.

Протокол L2TP использует сообщения двух типов: управляющие и информационные сообщения (рисунок 1.6). Управляющие сообщения используются для установки, обслуживания и удаления туннелей и вызовов. Они используют доверенный канал управления протоколом L2TP, чтобы обеспечить их доставку. Информационные сообщения используются для инкапсуляции изображений PPP, передаваемых через туннель. При потере пакета он не передается повторно.

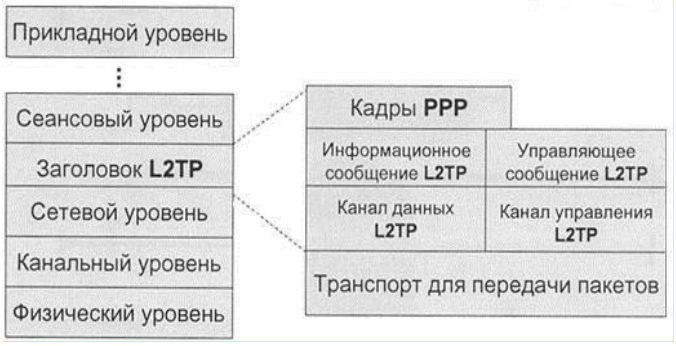

Рисунок 1.6 – Место протокола L2TP в модели OSI

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.

IPSec

IPSec (IP Security) – набор протоколов, касающихся 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 3 модели OSI (рисунок 1.7).

Рисунок 1.7– Место протокола IPSec в модели OSI

Internet-протокол (IP) не имеет средств защиты передаваемых данных. Он даже не может гарантировать, что отправитель является именно тем, за кого он себя выдает. IPSec представляет собой попытку исправить ситуацию. При использовании IPSec весь передаваемый трафик может быть защищен перед передачей по сети (рисунок 1.8). С помощью IPSec получатель сообщения может отслеживать источник полученных пакетов и может проверять целостность данных. Необходимо убедиться, что транзакция выполняется только один раз (за исключением случая, когда пользователь уполномочен повторять ее). 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. Представьте себе, что мошенник получил информацию о трафике и знает, что передача такого трафика может дать ему какие-то преимущества (например, в результате на его счет будут переведены деньги). Необходимо обеспечить невозможность повторной передачи такого трафика.

Рисунок 1.8 – Соединение IPSec

IPSec VPN оптимален для объединения сетей разных офисов через Интернет (рисунок 1.9).

Рисунок 1.9 – VPN соединение с использованием протокола IPSec.

IPSec VPN создает определенные преимущества для пользователей SMB/SOHO (Малый бизнес/Малый офис/Домашний офис):

- экономическая эффективность;
- законченное решение для коммерческого использования.

Для дистанционных пользователей:

- интегрированное безопасное решение;
- нет необходимости в дополнительном программном обеспечении;
- простота конфигурирования.

Для коллективных пользователей:

- экономически эффективное решение для дистанционных пользователей и филиалов;
- совместимость с решениями большинства поставщиков решений для виртуальных частных сетей.

SSL(Secure Socket Layer) VPN.

SSL (Secure Socket Layer) – протокол защищенных сокетов, обеспечивающий безопасную передачу данных по сети Интернет. При его использовании создается защищенное соединение между клиентом и сервером.

SSL использует защиту данных с открытым ключом для аутентификации передатчика и получателя. Он поддерживает надежность передачи данных, обеспечивая исправление кодов и хэшей.

SSL использует два ключа для защиты данных – открытый ключ и закрытый или частный ключ, известный получателю сообщения.

Сегодня существует множество веб-сайтов, которые используют SSL для защиты данных онлайн-пользователей (например, коммерческие и банковские услуги).

Все популярные браузеры, почтовые клиенты и интернет-приложения поддерживают использование SSL.

Для доступа к страницам, защищенным с помощью SSL, обычно вместо префикса http используется префикс https (порт 443), что указывает на использование соединения SSL.

SSL также может обеспечить защиту протоколов прикладного уровня (уровень 7 модели OSI), например, таких как POP3 или FTP. Для работы SSL требуется, чтобы на сервере имелся SSL-сертификат.

Защищенная связь между клиентом и сервером через SSL выполняет две функции - аутентификацию и защиту данных.

SSL состоит из двух уровней. Многоуровневый транспортный протокол (TCP) используется для шифрования протоколов и кодирования протоколов на более низких уровнях (уровни 4-5) (то есть генерация пакетов).

Для каждого инкапсулированного протокола он обеспечивает условия, при которых сервер и клиент аутентифицируют друг друга, защищают передаваемые данные и заменяют ключи друг на друга перед отправкой и получением данных.

SSL VPN оптимален для подключения удаленных пользователей к ресурсам локальной сети офиса через Интернет (рисунок 1.10).

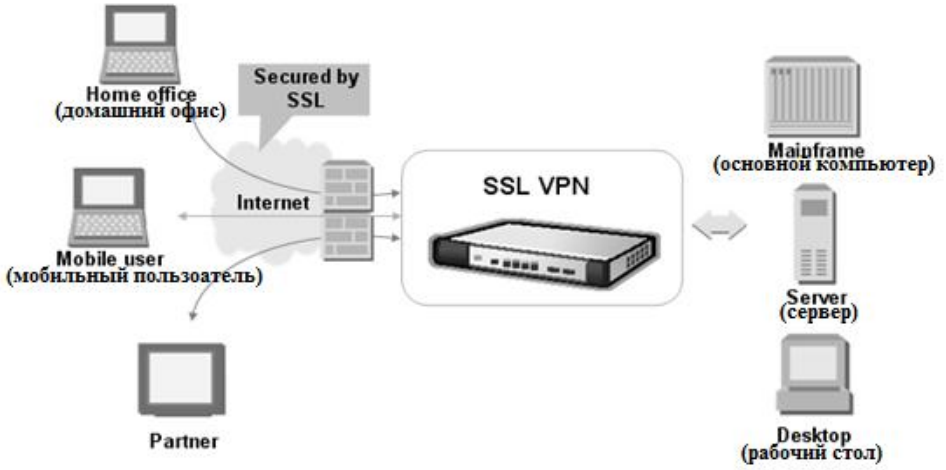

Рисунок 1.10 – Принцип подключения протокола SSL VPN

SSTP (англ. Secure Socket Tunneling Protocol) – протокол безопасного туннелирования сокетов. Протокол VPN от Microsoft, основанный на SSL и включённый в состав их ОС начиная с Windows 2008 и Windows Vista SP1. Соединение проходит с помощью HTTPS по 44.3 порту. Для шифрования используется SSL, для аутентификации — SSL и PPP.

GRE (англ. Generic Routing Encapsulation) общая инкапсуляция маршрутов – протокол туннелирования сетевых пакетов, разработанный компанией Cisco Systems. Протокол GRE обеспечивает механизм инкапсуляции произвольных пакетов в произвольный транспортный протокол.

1.4 Постановка задачи

Эффективное использование информационных технологий является важным стратегическим фактором повышения конкурентоспособности современных предприятий и организаций.

Технология виртуальной частной сети VPN обеспечивает связь между сетями, а также решение различных проблем через защищенный канал Интернет (туннель) между удаленным пользователем и корпоративной сетью.

Достоинства использования VPN-технологий для защиты информации в распределенных сетевых информационных системах масштаба предприятия:

- способность защищать всю корпоративную сеть - от широкого спектра локальных офисов до отдельных рабочих мест. Используя аутентификацию, получатель сообщения, являющийся пользователем виртуальной частной сети, может отслеживать происхождение пакетов и обеспечивать целостность данных;
- средства защиты данных в виртуальных частных сетях обеспечивают конфиденциальность данных первичного пользователя. Защита может быть распространена на все коммуникации из сети - от сегментов локальной сети до каналов связи глобальной сети, включая отключенные и отключенные сети;
- масштабируемость системы защиты, то есть использование сложного программного, аппаратного/программного обеспечения с точки зрения сложности, производительности и затрат для защиты объектов различной сложности и производительности;
- использование открытых сетевых ресурсов в качестве отдельной сети корпоративной сети; все риски, связанные с использованием публичных сетей, компенсируются защитой информации;
- управление сетью и надежная идентификация всех источников информации. Аутентификация трафика при необходимости может быть на уровне отдельных пользователей;

- сегментация ИС и организация безопасной эксплуатации системы, обрабатывающей информацию различных уровней конфиденциальности, программными и программно-аппаратными средствами защиты информации.

Виртуальные частные сети похожи на логические комбинации локальных сетей, которые создаются на разных уровнях с помощью разных протоколов, таких как PPTP, IPsec, GRE, L2TP, LCP, OpenVPN, MPLS и т. д.

Не все технические средства читают и поддерживают эти протоколы, следовательно, надо для начала узнать, какие устройства участвуют в структуре локальной сети, какие из них поддерживают нужные нам протоколы для создания нашей VPN сети.

Для проектирования VPN в работе для примера выбрана корпоративная сеть, главный офис которой находится в г. Нур-Султан. Я буду использовать оборудование от компании Cisco.

Компания имеет три филиала. Офисы расположены в трех разных регионах страны: Нур-Султан, Кокшетау, Павлодар.

Главный офис организации находится в г. Нур-Султан, главный сервер с большой базой данных расположен в этом же месте. На рисунке 1.11 представлена схема сети в г. Нур-Султан.

Услуга Интернет предоставляется хост-провайдером АО «Казахтелеком». Сеть организации подключена к сети хост-провайдера через оптоволоконные кабели через граничный маршрутизатор Cisco 2901.

За степень доступа в сети организации отвечают три оборудования второго уровня «Cisco 2901», соединенные с пограничным маршрутизатором, предоставляющие доступ к сети сотрудникам. Внутренние сети включают маршрутизацию, при которой уникальные IP-адреса компании (DHCP) динамически регистрируются и передаются внутри и наоборот (NAT).

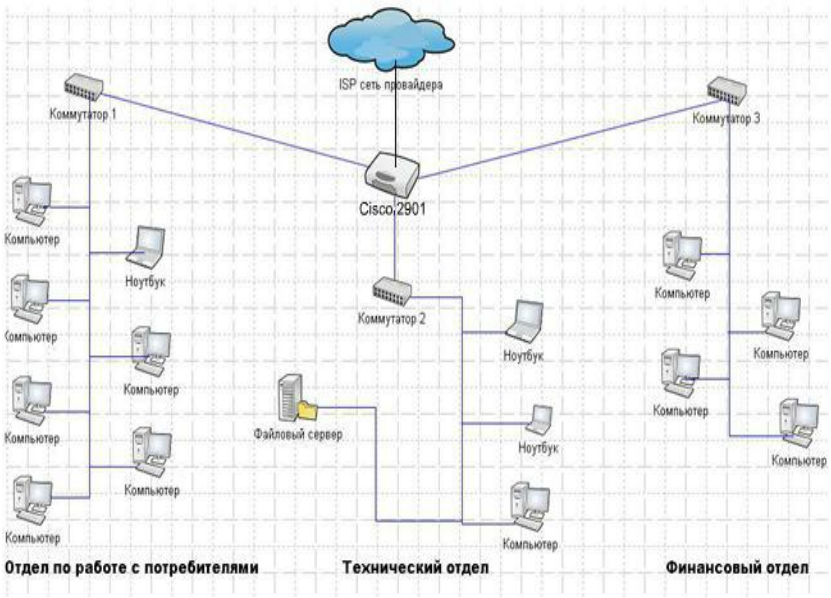

Рисунок 1.11 – Схема корпоративной сети компании в городе Нур-Султан

Протокол динамического назначения IP (DHCP) - это стандарт, который позволяет хостам получать IP-адреса из различных конфигураций, таких как DHCP и сеть.

Этот стандарт представлен в виде «абонент-сервер». Для самонастройки во время установки сетевого оборудования принимающий абонент отправляет запрос на DHCP-сервер, а DHCP-сервер отвечает на эти запросы, назначая хосту уникальный IP-адрес

В эпизоде с нашей организацией сервером является роутер «Cisco 2901».

Трансляция сетевых адресов (NAT) – это функция, которая позволяет маршрутизатору изменять IP-адреса транзитных пакетов для работы в автономном режиме. После получения пакета локального отправителя маршрутизатор может просмотреть заголовок пакета и область информации. Если в заголовке пакета есть адрес локального адреса, сообщение перенаправляется на локальное целевое устройство. Однако при отсутствии локального адреса субъекта пакет следует перенаправить во внешнюю сеть. Для этого маршрутизатор заменяет физический (внутренний) адрес пакета на внешний IP-адрес, который будет использоваться для доступа в Интернет, и заменяет нумерацию портов (если необходимо идентифицировать магистральные пакеты, отправленные абонентам подсети). Маршрутизатор запишет IP-адреса, необходимые для получения обратного пакета, и сохранит его в течение некоторого времени. Через некоторое время, если клиент завершит передачу пакетов с клиентом, маршрутизатор отформатирует записи в таблице маршрутизации в формате порта, включая обмен. Маршрутизатор локализует широковещательные пакеты и делит абонентов на три группы, за счет функции, с помощью которой маршрутизатор может создать виртуальные локальные сети: «отдел по работе с потребителями», «технический отдел», «финансовый отдел».

В городах Кокшетау и Павлодар сетевые линии настраиваются аналогичным образом, за исключением расположения файлового сервера, поскольку график проектирования сети не изменяется.

На рисунке 1.12 представлена общая схема корпоративной сети компании.

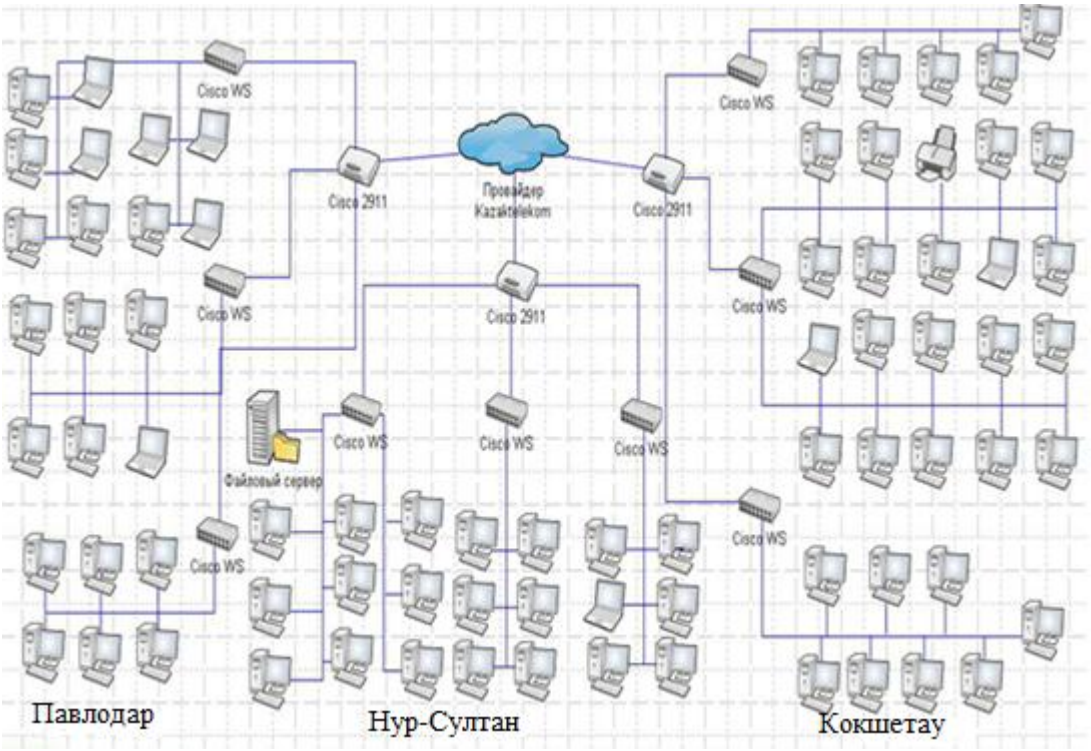

Рисунок 1.12 – Общая схема организации сети

Целью работы является объединение трех филиалов организации, которые расположены в трех разных местах, в одну безопасную приватную сеть по технологии VPN. Для решения данной задачи следует выполнить:

1) подобрать оборудование по результатам расчета;

2) создать туннель IP Sec Site to Site;

3)настроить динамическую маршрутизацию. Для этого можно использовать протоколы OSPF, EIGRP, BGP.

Для улучшения и расширения каждой организации я использую DMVPN. Это логическая частная сеть, которая может автоматически создавать туннельный канал. Поэтому нужно только настроить этот узел для добавления нового узла в виртуальную частную сеть.

2 Проектирование корпоративной сети по технологии VPN

2.1 Способы построения VPN

Реализация в последние годы. VPN в основном осуществляется крупными организациями, банковскими учреждениями и государственными учреждениями. Такие факторы интереса позволяют виртуальным частным сетям не только значительно снизить стоимость создания новых информационных каналов с удаленными ветвями, но и повысить безопасность при передаче и приеме данных.

Эта реализация сети осуществляется определенным образом в зависимости от планов и условий виртуальной отдельной сети. Компоненты и настройки персональной сети почти всегда отмечены типом оборудования, используемого для виртуальных частных сетей

По методу технического построения виртуальные приватные сети строятся на базе:

- роутеров;
- брандмауэров;
- программных решений;
-специальных оборудований с внедренными процессорами для шифрования.

VPN на базе роутеров.

Этот метод реализаций виртуальных частных сетей обуславливает использование роутеров для построения безопасных каналов, потому что почти все сообщения, исходящие из внутренней сети, проходят сквозь роутер, следовательно, совершенно правильно доверить ему и шифрование. Роутеры, разработанные компанией«CiscoSystems», оснащены поддержкой стандартов L2TP и IPSec Не имея подключения простого шифрования проходящих сообщений Cisco поддерживает другие функции виртуальной частной сети, такие как туннелирование Cisco и аутентификация по паролю.

Изображение на рисунке 2.1 иллюстрирует метод построения виртуальной частной сети с использованием роутеров.

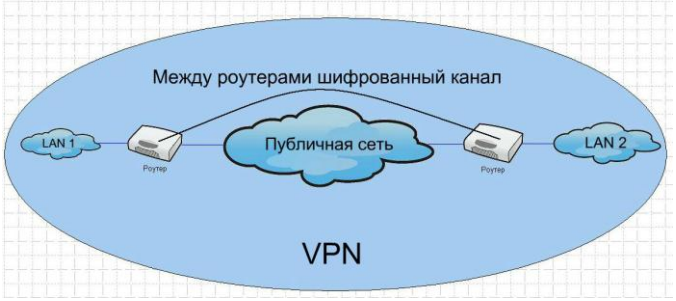

Рисунок 2.1 – VPN на базе роутеров

В целях реализаций виртуальных приватных сетей «CiscoSystems» применяет защищенный логический канал с шифровкой каждого IP-пакета.

Виртуальные частные сети на базе брандмауэров.

Межсетевые экраны всех производителей поддерживают разные стандарты туннелирования и кодирования данных. При использовании брандмауэров персональных компьютеров это решение следует принимать во внимание, когда небольшие объемы используются только для передачи небольших данных.

Недостатками данного способа является большая дороговизна в расчете на одну вакансию и зависимое положение эффективности от возможности аппаратуры, на котором работает брандмауэр.

В качестве примера построения на основе межсетевых экранов можно привести Barracuda Web Application Firewall компании «Barracuda». Barracuda Web Application Firewall применяет для проектирования виртуальных частных сетей простой метод на основе протокола IPSec. Поток пакетов, проходящий через межсетевой экран, декодируется, затем к нему реализуются обычные нормы контроля доступом. Barracuda Web Application Firewall под контролем операционных систем Windows.

Изображение на рисунке 2.2 иллюстрирует случай построения VPN .канала при помощи брандмауэра.

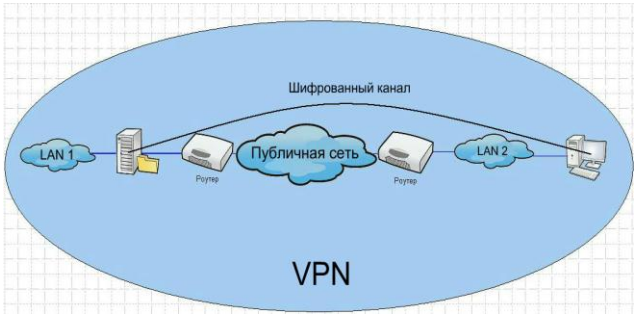

Рисунок 2.2 – Виртуальная приватная сеть на базе брандмауэра

VPN на базе программного обеспечения (ПО).

Виртуальные частные сети, реализованные на основе программного обеспечения, по эффективности ниже узкоспециализированных устройств, но, тем не менее, имеют большую мощность для построения виртуальных частных сетей. Нужно иметь в виду, что при случаях удаленной работы требования к нужному каналу невелики.

Исходя из этого понимается, что исключительно программные средства с легкостью дают производительность, которая хватает для удаленной работы.

В качестве примера данной реализаций будет выступать ПО Cyber Ghost VPN компании «Cyber Ghost». При использовании этого программного обеспечения, пользователь подключается к серверу, проходит процесс аутентификации и меняет пароли. Затем зашифрованная информация

передается другим IP-пакетам, которые отправляются на файловый сервер в процессе инкапсуляции. Во время передачи туннель анализирует информацию о целостности.

Виртуальные частные сети на базе специализированного оборудования.

Преимущество этих виртуальных частных сетей состоит в том, что они очень эффективны, потому что они имеют высокую работоспособность благодаря специально кодированным чипам.

Использование виртуальных частных сетей в специализированном оборудовании может использоваться в сетях, требующих высокой производительности. В качестве примера можно представить продукт CERTEX VPN SB компаний«CERTEX VPN». Изображение на рисунке 2.3 иллюстрирует способ построения виртуальных приватных сетей на базе узкоспециализированных аппаратных продуктов.

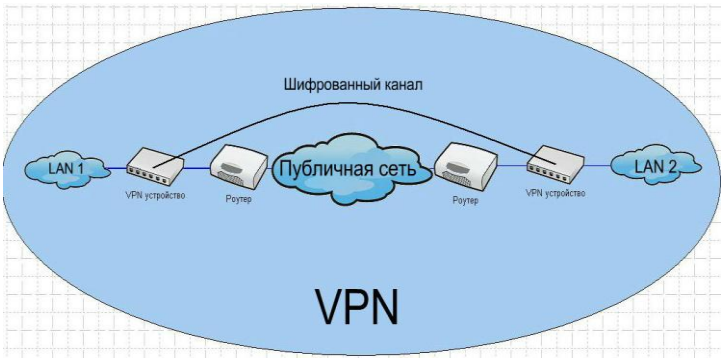

Рисунок 2.3 –VPN на основе аппаратных продуктов

Представленное аппаратное средство применяет аппаратное кодирование отправляемых данных. CERTEX VPN SB использует протокол IPSec.

Кроме того, есть много протоколов для логических соединений регионально разделенных сетей:

- Generic Routing Encapsulation
- IPSecurity (при туннельном режиме)
- Generic Routing Encapsulation IP Security
- Dynamic Multipoint VPN

Первый протокол имеет недостатки:

- слабая защищенность. Информация, упакованная в протокол инкапсуляций GRE, отправляется все-таки в незащищенном виде;
- плохо работает с протоколом трансляций адресов;
.- офисы друг с другом не могут взаимодействовать напрямую, взаимодействие осуществляется через централизованный узел.

Второй способ также имеет недостатки: при использований туннельного режима информация кодируется заодно с ip заголовком, следовательно, нельзя использовать динамическую маршрутизацию

При использовании третьего способа пакету назначается идентификация с помощью GRE, а вся информация кроме заголовка кодируется IPSecurity. Также возможен случай использования динамической маршрутизации, остается проблема масштабирования, которую может решить Dynamic Multipoint VPN

Среди всех протоколов для логических соединений регионально разделенных сетей я выбрала протокол Dynamic Multipoint VPN.

2.2 Сеть на базе Dinamic Multipoint VPN

Наша компания и три его офиса работают в трех разных городах, которые должны быть объединены в одну сеть, головной офис которого находится в Нур-Султан.

Предприятие для связи между офисами может позволить себе только арендованные каналы. Это может быть сеть одного конкретного провайдера или Интернет, не имеет значения. Важно, что предприятию выделили IP-адреса, маршрутизируемые в этой сети, и можно с их использованием объединять сети. DMVPN отлично подходит для этой задачи, поэтому мы рассмотрим конфигурацию сети на основе этой технологии.

Dynamic Multipoint Virtual Private Network – динамическая многопртовая виртуальная частная сеть, технология объединения частных сетей через общественные сети. Для объединения частных сетей, как правило, используется проектирование туннелей через публичные сети.

Суть технологии заключается в том, что на каждом узле сети настраивается только один туннельный интерфейс, который и организует затем необходимое количество туннелей автоматически, преобразуя топологию сети из «звезды» в полносвязную. Несмотря на то, что эта технология все еще предусматривает центральный узел, конечные узлы организуют туннели между собой.

В конечном счете, даже после того, как он накопил такую сеть, даже центральный узел не играет такой важной роли, даже если он построен с использованием звездной технологии. Разбивка конечных узлов может продолжать взаимодействовать с существующими туннелями (если, конечно же, сеть провайдера позволяет).

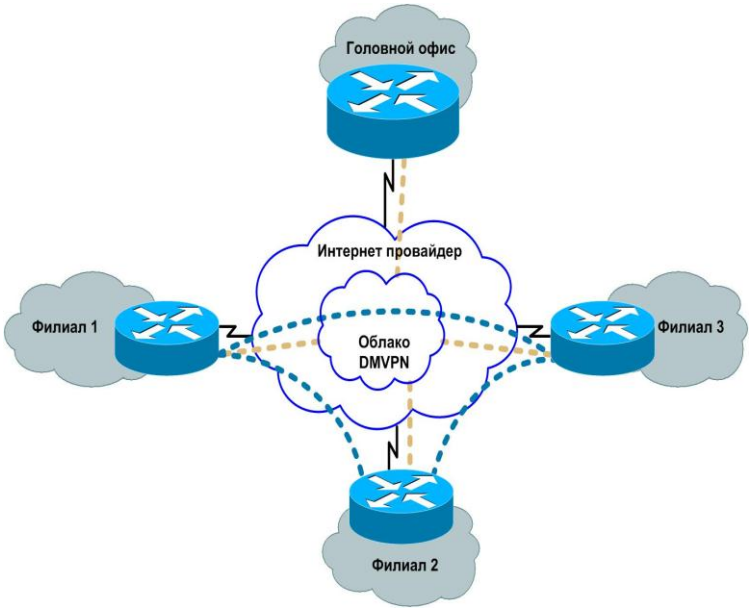

Рисунок 2.4 – Топология сети на основе DMVPN

Dynamic Multipoint Virtual Private Network – виртуальная частная сеть, позволяющая построить соединение по схеме «Звезда», с возможностью динамического создания туннелей между удаленными филиалами. При этом важно отметить, что удаленные части могут использовать динамически-назначаемые IP адреса, что часто встречается при подключении удаленных филиалов через сеть Internet .

Технология DMVPN обеспечивает безопасное соединение между удаленными подразделениями более широким способом, чем составление двухточечных контактов между всеми финансовыми организациями и объединение их в полностью интегрированную топологию, и имеет следующие преимущества:

- при добавлении новых филиалов в существующую сеть, необходимо настроить только новый маршрутизатор, изменений на уже существующих маршрутизаторах не требуется;
- DMVPN позволяет использовать динамические IP-адреса на spoke-маршрутизаторах (маршрутизаторах филиалов);
- если двум spoke-маршрутизаторам необходимо установить туннель напрямую, то он устанавливается динамически.

Технология DMVPN позволяет оптимизировать производительность, минимизировать задержку для приложений реального времени и динамически настраивать.

В результате облегчается обслуживание и настройка концентраторов и обеспечивается эффективное использование системы управления качеством обслуживания (QoS) для приоритезации маркированных сетей и приложений, работающих в режиме реального времени. Наложение архитектуры системы балансировки нагрузки на сервере концентрации DMVPN увеличит пропускную способность.

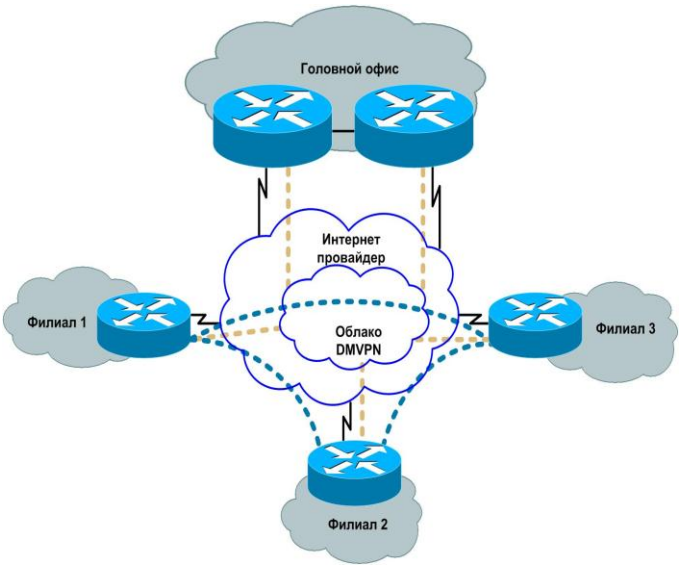

Рисунок 2.5 – Сеть DMVPN с резервированием центрального маршрутизатора

Начиная строить свою собственную сеть, необходимо рассчитать варианты ее развития и обеспечьте рост сети, и, следовательно, выбрать правильное оборудование, отвечающее всем требованиям.

2.3 Выбор необходимых технических средств

2.3.1 Выбор кабеля

При проектировании компьютерной сети витая пара, безусловно, самая популярная. Ее может быть несколько видов, в зависимости от условий парной передачи, объема, скорости передачи и многих других факторов. Чтобы выбрать кабель, нужны настройки передачи данных и стоимость кабеля.

Различают несколько видов витой пары:

- UTP без защитного экрана;
- FTP с одним экраном, который сделан из фольги;
- STP с защитой каждой пары, а также одним общим экраном с видом сетки;
- U/STP без внешней защиты, но каждая пара находится в экране из фольги;
- S/FTP – одна общая оплетка из меди и каждая пара находится в экране из фольги.

Конструкция FTP – это тот же кабель UTP, слой фольги под алюминиевой стороной защитного покрытия (или алюминиевой полимерной пленки), плюс дренажный проводник вдоль этой стороны. UTP кабель не требует проводника.

Соответственно, благодаря дополнительному слою материала, кабель FTP может быть шире и менее гибким, в зависимости от толщины экрана. Отличие кабеля UTP и FTP можно увидеть на рисунке 2.4 ниже.

Рисунок 2.6 – Кабели вида UTP и FTP

Также разница кабелей витая пара – это категория. В настоящее время существует семь категорий, которые классифицируются как CAT1-CAT7.

Категории определяют эффективную полосу пропускания. Кроме того, чем выше категории кабелей, тем больше пар и общая длина кабеля. Ниже приведены категории и их характеристики.

Категории кабеля витая пара:

- CAT1 – одна пара, данную категорию применяют при включении телефонной связи. Частотная полоса - 0.1 МГц;

- CAT2 – устаревший тип кабеля, отличается низкой скоростью передачи сигнала (до 4 Мбит/сек). Может быть применимым для телефонных сетей. Частотная полоса 1 МГц;

- CAT3 – состоит из двух пар, раньше применялся для построения сетей 10BASE-T, Token Ring (скорость до 10 Мбит/сек). Частотная полоса - 16 МГц;

- CAT4 – кабель из четырех пар, который ранее эксплуатировался при конструировании Token Ring сетей, 10BASE-T, 10BASE-T4. Отличается лимитом скорости передачи - 16 Мбит/сек. Частотная полоса - 20 МГц;

- CAT5 – насчитывает четыре пары. Во время эксплуатации двух пар, скорость передачи будет - 100 Мбит/сек. Частотная полоса - 100 МГц;

- CAT5e – наиболее используемый вид кабеля, насчитывает четыре пары, применяется при конструировании сетей 100/1000 Мбит/сек. Во время задействования двух пар, скорость передачи - 100Мбит/с, если задействуют все четыре пары – 1000Мбит/с. Частотная полоса - 100 МГц;

- CAT6 – находит применение в сетях Fast Ethernet (100 Мбит/сек), Gigabit Ethernet (1000 Мбит/сек), передает сигнал на скорости до 10 Гбит/сек. Частотная полоса - 250 МГц;

Также существует подкатегория - CAT6a - с частотой полосой до 500 МГц.

- CAT7 – во время работы на частоте до 600 МГц, скорость передачи доходит до 10 Гбит/сек. Максимальная длина передачи сигнала обеспечивается двойным экранированием кабеля.

В настоящее время на практике повсеместно для построения локальных сетей и Интернет применяется lan-кабель витых пар категории CAT5. В таблицах 2.1 - 2.3 приведены характеристики кабеля FTP 5 CAT.

Таблица 2.1 - Механические характеристики кабеля FTP 5 CAT

Наименование	Характеристики	
Механические характеристики	Монтаж	Эксплуатация
Максимальное растягивающее усилие	400Н	50Н
Минимальный радиус изгиба	8 диаметров	4 диаметра
Разрывное усилие оболочки не менее	70 кгс/кв.см	

Таблица 2.2 - Массогабаритные характеристики кабеля FTP 5 CAT

Наименование	Параметры							
Количество пар	1	2	4	8	10	25	50	100
Внешний диаметр, мм	3.5	5	6.4	10.2	10.7	14.8	18.4	22.5
Масса, кг/км	12	21	38	87	92	178	324	605

Таблица 2.3 - Электрические характеристики кабеля FTP 5 CAT

Наименование	Характеристики
Электрические характеристики	
Волновое сопротивление	100±15 Ом
Искажение, не более (100 МГц)	45 нс/км
Электрическое сопротивление жил не более	9,5 Ом/100м
Асимметрии жил рабочей пары не более	3%
Электрическая емкость цепи не более	5,2 нФ/.100м
Сопротивление изоляции жил не менее	5000 мОм*км
Пробивное напряжение между проводниками, а также между проводом. и экраном в течение 1 мин	
При постоянном токе	750 В
При переменном токе частотой 50 Гц	500В

2.3.2 Выбор коммутатора

На уровне доступа необходим управляемый коммутатор, который будет поддерживать настройку виртуальных локальных сетей VLAN. Для

распределения нагрузки и удобства подключения были выбраны три 8 портовых коммутаторов от компании Cisco WS-C2960C-8TC-S, которые будут осуществлять доступ от оконечного оборудования к пограничному маршрутизатору.

Таблица 2.4 – Характеристики коммутатора Cisco WS-C2960C-8TC-S

Общие характеристики	
Тип устройства	Коммутатор (switch)
Количество слотов для дополнительных интерфейсов	1
Объем оперативной памяти	128 Мб
Объем флеш-памяти	64 Мб
LAN	
Количество портов коммутатора	8 x Ethernet 10/100 Мбит/сек
Количество uplink/стек/SFP-портов и модулей	2
Максимальная. скорость uplink/SFP-портов	10/100/1000 Мбит/сек
Внутренняя пропускная способность	10 Гбит/сек
Размер таблицы MAC ад.ресов	8192
Управление	
Web-интерфейс	Есть
Поддержка Telnet	Есть
Тип управления	уровень 2
Поддержка SNMP	Есть
Дополнительно	
Поддержка IPv6	Есть
Поддержка стандартов	Auto MDI/MDIX, Jumbo Frame, IEEE 802.1p (Priority tags), IEEE 80.2.1q (VLAN), IEEE 802.1d (Spanning Tree), IEEE 802.1s (Mult.iple Spanning Tree), Link Aggregation Control Protocol (LACP)
Размеры (ШхВхГ)	269 x 44 x 213 мм
Вес	1.27 кг

Коммутаторы Cisco WS-C2960C-8TC-S входят в линейку управляемых коммутаторов Cisco 2 уровня, предназначенную для корпоративных сетей. Коммутаторы этой серии оснащены 8/16/24/48 портами 10/100 Мбит/с FastEthernet, а также 1/2/4 комбо-портами GigabitEthernet/SFP.

На рисунке 2.7 показан коммутатор Cisco «WS-C2960C-8TC-S».

Рисунок 2.7 - Cisco «WS-C2960C-8TC-S»

2.3.3 Выбор маршрутизатора

Сегодня на рынке представлено множество моделей маршрутизаторов, стоимость которых в десять раз дороже, поэтому часто возникает проблема с выбором наилучшего варианта.

Чтобы выполнить этот проект, необходимо соответствующее оборудование для создания определенных настроек, выполнение определенных задач - в данном случае реализация VPN-связи.

Для настройки параметров VPN в качестве граничного маршрутизатора каждого офиса требуется маршрутизатор для создания надежной высококачественной сети, поддерживающей следующие протоколы:

- поддерживающий протокол динамического туннелирования mGRE;
- протокол обеспечения безопасности Ipsec;
- протоколы динамической маршрутизации OSPF и DHCP;
- протокол преобразования адресов NAT;
- который обеспечивает пропускную способность в размере не менее 26 Мбит/с.

Поскольку на этом узле будет держаться вся внутренняя сеть офиса, не желательно экономить на этой точке, поэтому было принято решение о приобретении продукции Cisco надежного качества.

Просмотрев технические характеристики, а также стоимость на оборудование, сделали выбор. Маршрутизаторы компании Cisco поддерживающие протоколы туннелирования и безопасности начинаются от 1900 серии. Пропускная способность этих маршрутизаторов свыше 2.6 Мбит/с начинается лишь с 2900 серии. Поэтому маршрутизатор, соответствующий моим требованиям - серии 2900 - «Cisco 2911».

Cisco ISR 2900 – серийные маршрутизаторы с интеграцией сервисов, разработанные на основании многолетнего опыта Cisco в области инноваций и реализаций передовых решений. Архитектура новых платформ будет поддерживать следующий этап работы филиалов организации, что позволит значительно сократить эксплуатационные расходы за счет перевода средств мультимедийной совместной работы и средств виртуализации на отраслевой уровень.

Платформы второго поколения для Cisco ISR разрешают не только нынешние задачи, но и будущие задачи, поскольку они используют многоядерные процессоры для поддержки высокопроизводительных сигнальных процессоров для расширения перспективных возможностей передачи видео, используются мощные сервисные модули с повышенной доступностью, средства коммутации Gigabit Ethernet с поддержкой расширенной спецификации POE, а также новые возможности управления и мониторинга потребления энергии.

На рис. 2.8 изображен маршрутизатор Cisco 2911.

Рисунок 2.8 – Маршрутизатор Cisco 2911

Модульный маршрутизатор Cisco 2911/K9 – это устройство нового поколения, относящееся к семейству ISR G2. Модель позволяет настроить безопасное широкополосное соединение с сетью, использовать мультимедийные данные, видео, беспроводную связь, а также множество дополнительных функций с минимальными затратами на приобретение и обслуживание.

Cisco 2911/K9 со встроенными сетевыми сервисами на 3 порта идеально подходит для создания сетей малых и средних организаций и предприятий. Модель имеет 512 МБ встроенной и 526 МБ флеш-памяти, возможность поддержки PoE на портах 10/100/1000 Ethernet, помимо этого поддержку протокола VPN и туннелирования для осуществления надежной и безопасной передачи при построении удаленных VPN сетей.

В таблице 2.5 представлены основные характеристики данного устройства.

Таблица 2.5 – Характеристики Cisco 2911

Серия	Cisco 2900 Series ISR
Рекомендуемая замена	ISR4331 Cisco LAN маршрутизатор модульный 3 x GE, 3 x NIM, 1 x ISC, 1 x SM, IP Base
WAN порты Ethernet	3 x GE
LAN порты Ethernet	Совмещаются с WAN
Слоты интерфейсных карт	4 слота
Память FLASH	256 Мб
Память FLASH максимум	4 Гб\
Объем ОЗУ	512 Мб
Память ОЗУ максимум	2 Гб
Гарантия	90 дней Cisco Limited Warranty

Продолжение таблицы 2.5

Серия	Cisco 2900 Series ISR
Потребляемая мощность номинальная/максимальная	50/210 Ватт
Тип питания	AC 100-240В
Типы поддерживаемых карт	4 слота EHWIC
Слоты DSP ресурсов	2 слота PVDM
Высота RM UNIT	1U
Внутренний сервисный слот	1 слот ISM
Тип установки	Стоечное/настольное
Порты консольные	RJ-45 (RS232), AUX RJ-45(RS232), USB, mini-USB
Сетевой слот NM/SM	1 слот SM
Порты USB	2 x USB 2.0
Размер	88,9мм x 438,2мм x 469,9мм
Вес	13.2 кг
Протоколы	IPv4, IPv6, Static Routes, Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol (IGMPv3) Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), Distance Vector Multicast Routing Protocol (DVMRP), IPSec, Generic Routing Encapsulation (GRE), Bi-Directional Forwarding Detection (BVD), IPv4-to-IPv6 Multicast, MPLS, L2TPv3, 802.1ag, 802.3ah, L2 и L3 VPN.

3 Модель виртуальной частной сети для предприятия

3.1 Настройка VPN соединения с использованием программы Cisco Packet Tracer

Предприятие состоит из 3 филиалов. Задачей данного проекта является создание виртуальной частной сети (VPN) с целью соединения сетей различных территориально-разделенных филиалов одной организации в одну безопасную корпоративную защищенную сеть с целью доступа к единой базе данных. VPN преобразует соединения в IP сетях всеобщего пользования в так называемые туннели, то есть в защищенные каналы с заранее известной полосой пропускания, гарантируя защищенность и большое количество услуг при разумной цене установленных каналов. Вследствие чего эта технология имеет большой спрос у большого количества организаций, которые не имеют свои сетевые ресурсы, в связи с тем, что она экономична, доступна и безопасна.

Необходимо организовать удаленный доступ к серверам в центральном офисе.

Для этого есть 3 способа:

- Static Nat способ, когда пользователи будут обращаться на белый публичный адрес нашего роутера, автоматически будут попадать на сервера филиала;

- DMZ способ, когда настраиваются публичные адреса;

-VPN виртуальная частная сеть, организация локальной сети через Интернет. Логичное соединение с помощью туннеля между офисами.

Есть два вида соединения VPN:

– IP Sec Site to Site – соединение нескольких пользователей;

– IP Sec RA VPNS- соединение только одного пользователя.

В данном проекте мы рассмотрим IP Sec Site to Site.

Построение VPN состоит из 2х фаз:

- установка SA (Security Association) и ISAKMP Tunnel (Internet Security Association and Key Management Protocol);

- Ip Sec Tunnel.

В программе Cisco Packet Tracer создаем предприятие состоящее из центрального офиса и филиала в каждом из которых имеется роутер, компьютеры (ПК) и шлюз.

Для начала нужно настроить связь через VPN от центрального офиса к филиалу и наоборот (рисунок 3.1).

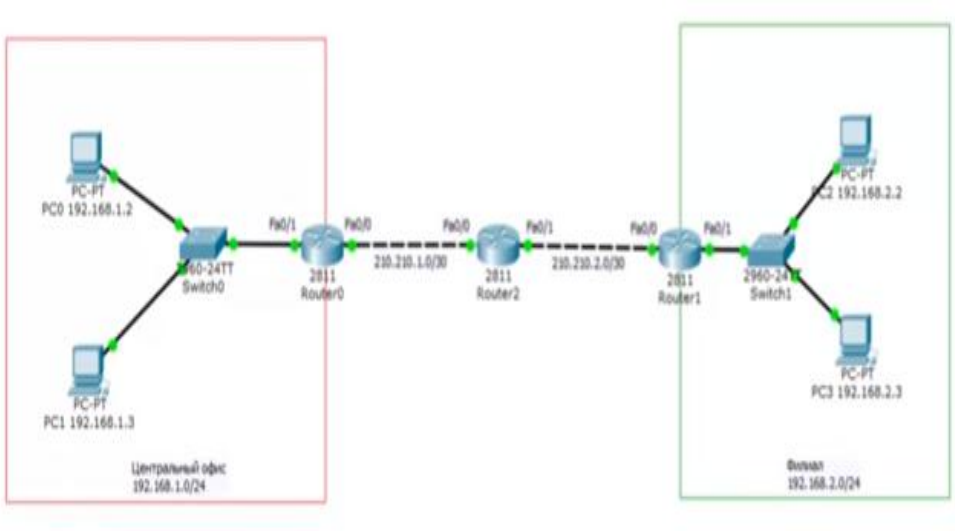

Рисунок 3.1- Проект предприятия

Для этого необходимо настроить в роутере центрального офиса два IP адреса. Начать нужно с NAT – обеспечить доступ в Интернет (рисунок 3.2).

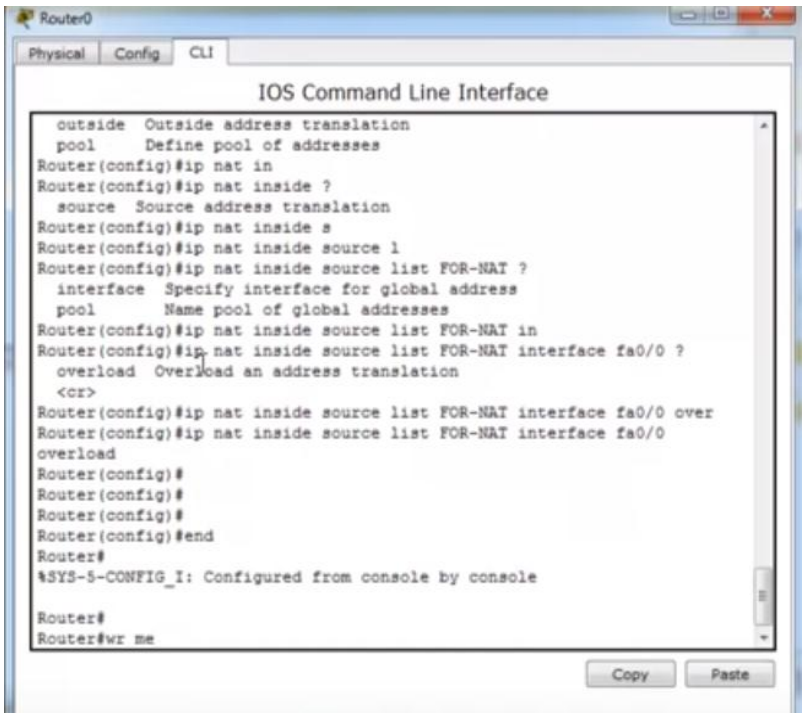

Рисунок 3.2 – Настройка роутера центрального офиса

После заполнения IP адресов и обеспечения доступа в Интернет, проверим Ping (доступ) с компьютера центрального офиса до интерфейса Интернет провайдера (рисунок 3.3).

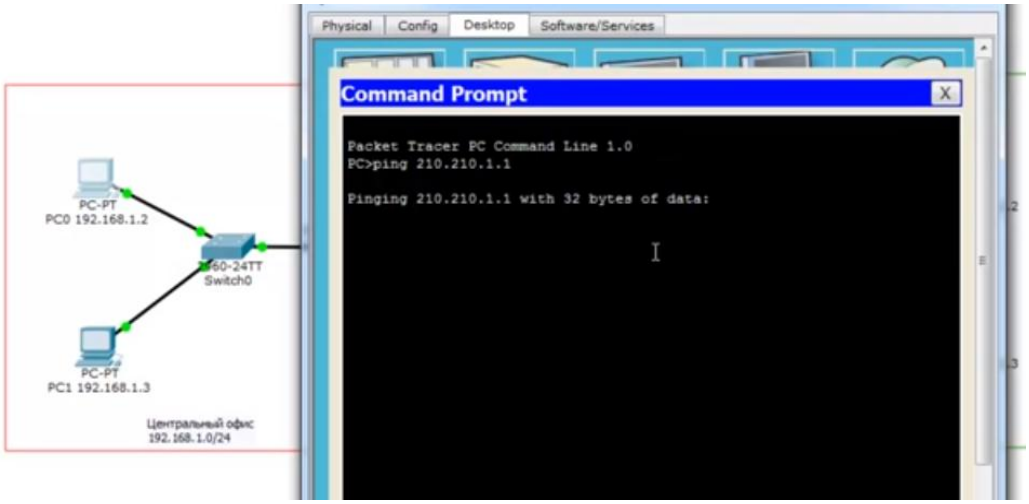

Рисунок 3.3 – Ping компютера центрального офиса

Ping пошел все сделано верно, после этого тоже самое нужно провести на роутере филиала.

Теперь перейдем к настройке VPN.

Первым делом необходимо настроить первую фазу. Создается политика, где мы указываем алгоритм шифрования, это параметры необходимые для построения туннеля ISAKMP через которые будут передаваться параметры основного IP Sec туннеля.

В роутере центрального офиса указываем:

-алгоритм шифрования encryption 3des;

- алгоритм хэширования hash mds;

- тип аутентификации authentication pre share Group 2.

Также не забываем про настройку ключа аутентификации и пира – crypto isakmp key cisco address 210.210.2.2. Адрес пира – это адрес внешнего интерфейса роутера на филиале. На рисунке 3.4 видно, как правильно настраивать первую фазу.

На этом настройка первой фазы заканчивается.

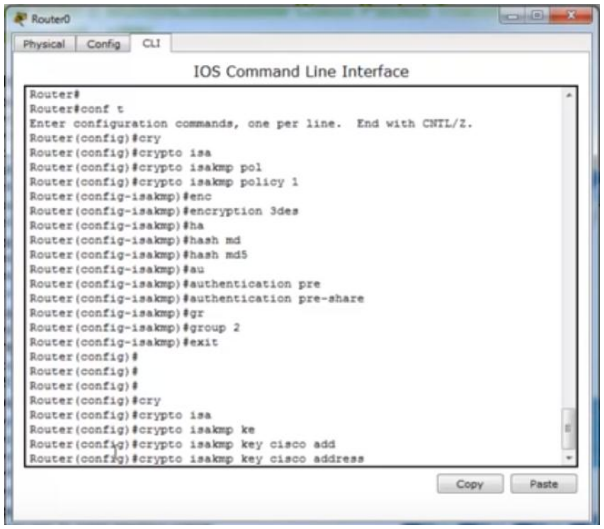

Рис 3.4 -Настройка первой фазы VPN

Настройка второй фазы VPN.

Во второй фазе в роутере центрального офиса указываем параметры для построения IP Sec туннеля – crypto ip sec transform-set TS:

-алгоритм шифрования encryption 3des;

- алгоритм хэширования encruption-md5-hmac.

Далее необходимо создать access list , то есть определить какой трафик мы будем заворачивать в VPN туннель.

Трафик шифрования:

- Ip access-list extended FOR VPN;

- Permit ip 192.168.1.0.0.0.0.25 \ 192.168.2.0.0.0.0.255.

После этого создаем криптокарту (рисунок 3.5). Указываем IP адрес-crypto map CMAP 10 ipsec-isakmp. Параметры IP Sec туннеля - set peer 210.210.2.2 \ set transform-set TS. Указываем, какой трафик нужно шифровать-match address FOR VPN. Производим привязку к интерфейсу - interface FastEthernet 0/0 crypto map CMAP.

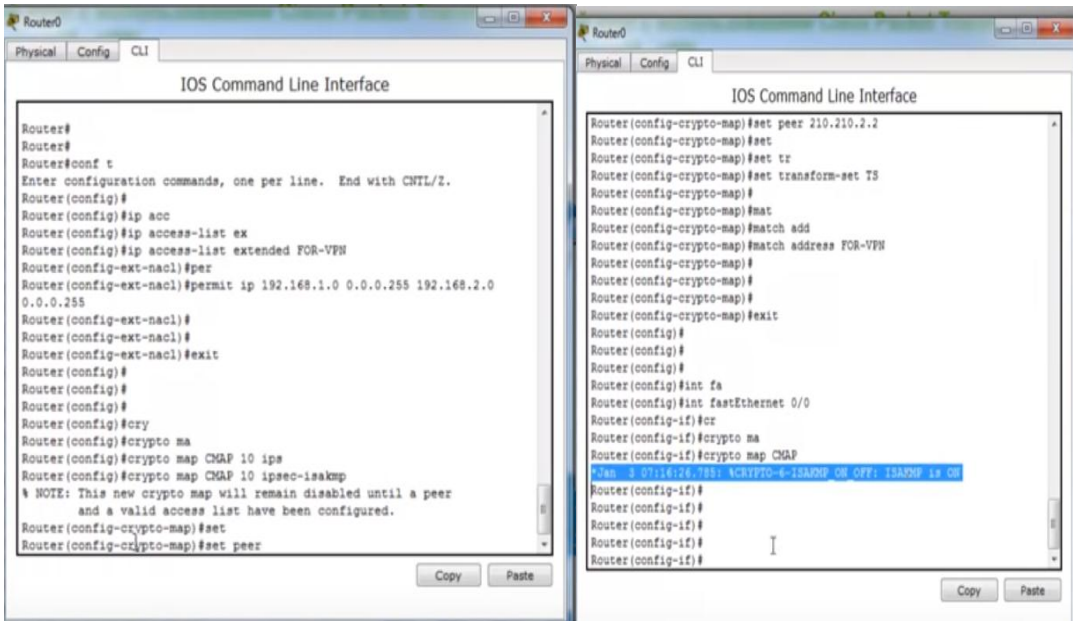

Рисунок 3.5 – Создание криптокарты и привязка к интерфейсу в роутере центрального офиса

На этом настройка второй фазы заканчивается, все нужно сохранить и провести такую же настройку на роутере филиала, отличаться будут только IP адреса.

Теперь, чтобы мы смогли пропинговать с центрального офис компьютер в филиале, нам нужно изменить Access List для NATa .Для этого нужно указать трафик с source локальной сети с distanaition локальной сети филиала. Удаляем существующий access list и создаем расширенный access list не забываем указать запрещенный трафик.

После создания расширенного Access list также проводим такие же настройки на роутере (маршрутизаторе) филиала.Пингованием проверим соединение центрального офиса компьютерами в филиале и наоборот. По

программе Ping пошел все верно, то есть мы только что построили VPN соединение между центральным офисом и филиалом. После этого на роутере центрального офиса проверим, построился ли технологический туннель. На рис 3.6 видно , что технологический туннель построен.

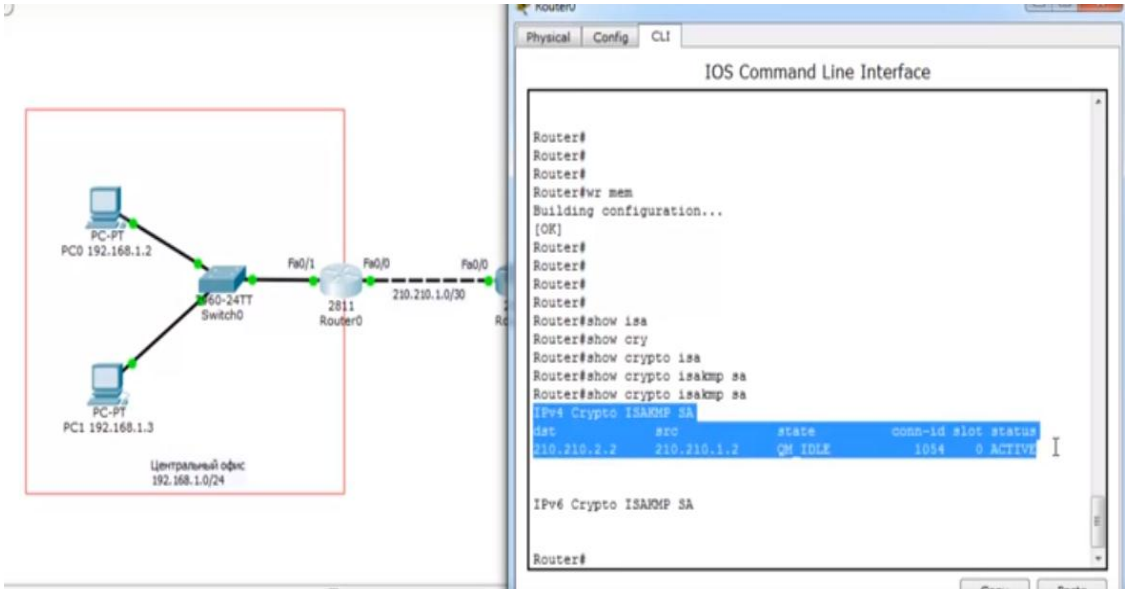

Рисунок 3.6 –Проверка построения технологического туннеля

Здесь же проверяем, построился ли IPSec туннель, на рисунке 3.7 видны все необходимые данные.

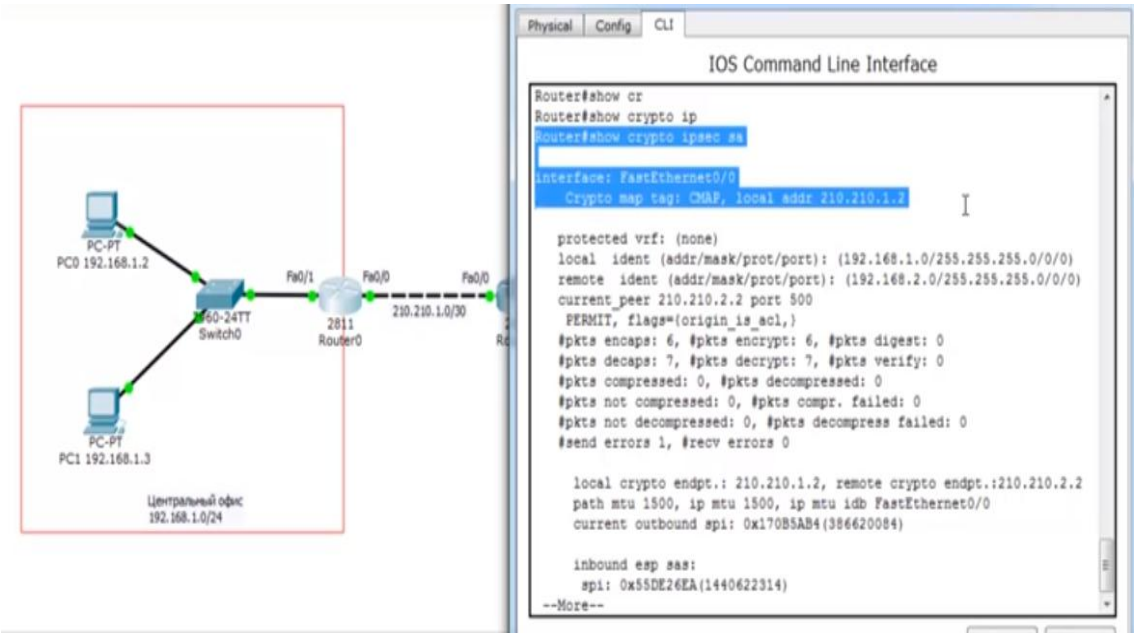

Рис 3.7- Проверка IP Sec туннеля

На рис 3.8 можно увидеть сколько пакетов зашифровалось и сколько расшифровалось.

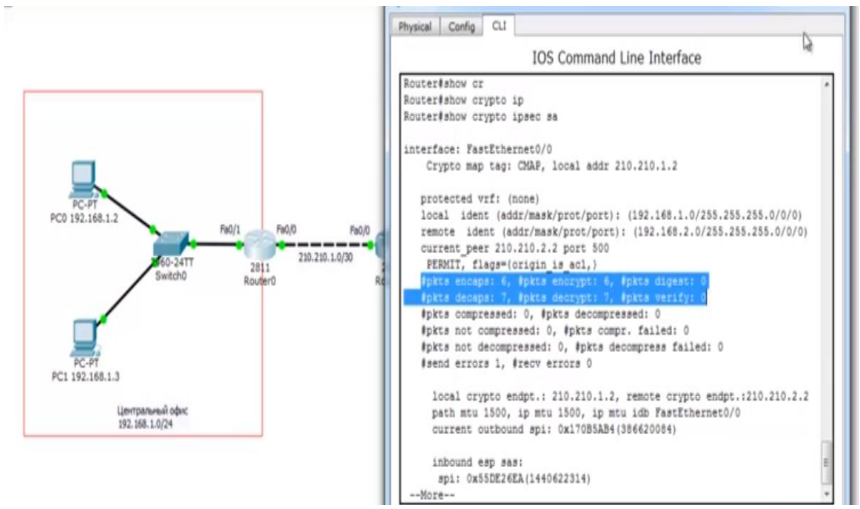

Рис 3.8- Проверка IP Sec туннеля, количество расшифрованных и зашифрованных пакетов

На этом настройка VPN соединения закончена. Мы построили туннель от центрального офиса к филиалу.

3.2 Анализ производительности сети VPN

Производительность сети является очень важным параметром, и любой инструмент, который ее снижает, в любой организации смотрят с подозрением. Не являются исключением и средства построения VPN, которые добавляют дополнительные задержки, связанные с обработкой трафика, проходящего через VPN-устройство. Все задержки, вызванные криптографическим трафиком, можно разделить на три типа:

- задержки при установлении защищенного соединения между VPN-устройствами;
- задержки, связанные с зашифрованием и расшифрованием защищаемых данных, а также преобразованиями, необходимыми для контроля их целостности;
- задержки, связанные с добавлением нового заголовка к передаваемым пакетам.

Реализация самых распространенных версий построения VPN включает установление защищенных соединений не между абонентами сети, а только между VPN-устройствами. С учетом криптографической стойкости используемых алгоритмов смена ключа возможна через длительный промежуток времени. Вследствие этого задержки типа 1, на скорость обмена данными при использовании средств построения VPN почти не влияют. Разумеется, этот тезис имеет стойкие алгоритмы шифрования, использующие ключи не менее 128 бит (Triple DES, ГОСТ 28147-89 и т.д.). Устройства, использующие бывший стандарт DES, могут вносить определенные задержки в работу сети. Задержки типа 2 начинают играть роль только при передаче

данных по высокоскоростным каналам (от 10 Мбит/сек). В других случаях скорость программных или аппаратных алгоритмов, выбранных алгоритмами шифрования и контроля целостности, обычно высока, и в цепочке операций «зашифрованием пакета - передача пакета в сеть» и «прием пакетов из сети - расшифрованием пакета» время зашифрования (расшифрования) значительно меньше времени, необходимого для передачи данного пакета в сеть. Основная проблема заключается в добавлении дополнительного заголовка к каждому пакету, проходящему через VPN. Давайте рассмотрим пример системы диспетчерского управления, которая обменивается данными в режиме реального времени между удаленными станциями и центральными точками. Допустим размер передаваемых данных - не более 25 байтов. Интенсивность передаваемых данных - 50-100 переменных в секунду. Функциональная совместимость между узлами осуществляется по каналам с пропускной способностью 64 кбит / с.Пакет со значением одной переменной процесса имеет длину 25 байтов (имя переменной - 16 байт, значение переменной - 8 байт, служебный заголовок - 1 байт). IP-протокол добавляет к длине пакета еще 24 байта (заголовок IP-пакета). При использовании LMI FRMI Frame Relay в качестве среды передачи добавляются еще 10 байтов FR. Итого:

$$L_{всего} = L_{имя} + L_{знач.} + L_{сл.заг.} = 16+8+1+24 = 59 \text{ байт} = 472 \text{ бит}.$$

Для передачи 750 значений переменных процесса за 10 секунд (75 пакетов в секунду) необходима полоса пропускания:

$$ПП = 75 \cdot 472 = 34{,}5 \text{ Кбит/с}.$$

Значение результата означает, что мы соблюдаем ограничения на скорости 64 Кбит/ с. Рассмотрим, как ведет себя сеть при включении в нее средства построения VPN. Первый пример основан на забытом протоколе SKIP. Добавляет 59 байтов данных на 112 байтов (для ГОСТ 28148-89).

$$L_{по\ сети} = L_{всего} + L_{доп.} = 59+112 = 171 \text{ байт (1368 бит)},$$

$$ПП = 75 \cdot 1368 = 102{,}6 \text{ Кбит/с}.$$

То есть на 60% превышает максимальную пропускную способность имеющегося канала связи. Протокол IPSec и пропускная способность для вышеуказанных параметров будет превышать 6% (67,8 кбит / с).Это при условии, что дополнительный заголовок для алгоритма ГОСТ 28147-89 составит 54 байта. Кроме того, плагин, который подключен к каждому пакету разных производителей всего по 36 байт (или 26 в зависимости от режима работы), что не приводит к снижению пропускной способности (57 кбит / с и 51 кбит / с соответственно).

ЗАКЛЮЧЕНИЕ

В дипломном проекте были рассмотрены различные технологии VPN, разновидности протоколов для построения VPN, сущность технологии VPN.

Основной задачей являлось построение виртуальной частной сети, где в качестве примера было предложено объединение филиалов компании, находящихся в трех разных городах. Для этого был произведен подбор оборудования, в Cisco Packet tracer были созданы настройки виртуальной частной сети, проектирование туннеля IP Sec Site to Site.

Эффективное использование информационных технологий является важным стратегическим фактором повышения конкурентоспособности современных предприятий и организаций. Технология виртуальной частной сети VPN обеспечивает связь между сетями, а также решение различных проблем через защищенный канал Интернет (туннель) между удаленным пользователем и корпоративной сетью.

Исходя из проделанной работы можно отметить, что основная цель дипломного проекта – анализ и проектирование виртуальной частной сети выполнена.

Перечень принятых сокращений, терминов

BGP (*Border Gateway Protocol*) — протокол граничного шлюза;

DHCP (Dynamic Host Configuration Protocol — протокол динамической настройки узла;

DMVPN (Dynamic Multipoint Virtual Private Network)– динамическая многопртовая виртуальная частная сеть;

DMZ (*Demilitarized Zone*)— демилитаризованная зона;

EIGRP (Enhanced Interior Gateway Routing Protocol) — усовершенствованный дистанционно-векторный протокол;

GRE (Generic Routing Encapsulation) – общая инкапсуляция маршрутов;

IPSec (Internet Protocol Security)- набор протоколов обеспечения защиты данных;

ISAKMP Tunnel (Internet Security Association and Key Management Protocol) – ассоциация Безопасности Интернета и Протокол Управления Ключами;

LAN (Local Area Network) – локальная вычислительная сеть;

L2TP (Layer 2 Tunneling Protocol) – протокол туннелирования уровня 2 (канального уровня);

MPLS (multiprotocol label switching)— многопротокольная коммутация по меткам;

NAT (Network Address Translation) — преобразование сетевых адресов;

OSPF (Open Shortest Path First) — протокол динамической маршрутизации;

PPTP (Point-to-Point Tunneling Protocol) – туннельный протокол типа точка-точка;

SA (Security Association) – ассоциация безопасности;

SSL (Secure Socket Layer) – протокол защищенных сокетов;

SSTP (Secure Socket Tunneling Protocol) – протокол безопасного туннелирования сокетов;

VLAN(Virtual Local Area Network) – виртуальная локальная сеть;

VPN (Virtual Private Network) – виртуальная частная сеть;

WAN (Wide Area Network) – глобальная сеть.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1 Амато Вито. Основы организации сетей Cisco, том 1. М.: Издательский дом "Вильяме", 2004. – 512с.

2 Гучард Б. Архитектура MPLS и VPN. – Индианаполис: Cisco Press, 2006. –504 с.

3 С. В. Запечников, Н. Г. Милославская, А.И. Толстой. Основы построения виртуальных частных сетей. – М: Горячая линия – Телеком, 2003.

4 Сериков И. Виртуальные частные сети PC Magazine RE. – 1999.

5Сущность технологии VPN. Электронный ресурс (https://studref.com/325308/informatika/tehnologiya_virtualnyh_chastnyh_setey)

6 Виртуализация сетей. Электронный ресурс https://www.intuit.ru/studies/courses/2324/624/lecture/13588

7 Алибаева С.А. Методические указания по дипломному проектированию (для студентов всех форм обучения направления 652400 – Радиоэлектроника и телекоммуникации). – Алматы: , 2001. - 17 с.

8 Л.Г. Мордухович, А.П.Степанов. Системы Радиосвязи. Курсовое проектирование. Учебное пособие. Москва «Радио и связь» 1987 г.

9 Романец Ю. В., Тимофеев П. А., В. Ф. Шаньгин. Защита информации в компьютерных системах и сетях. 2-е изд. М.: Радио и связь, 2001.

10 Щеглов А.Ю. «Компьютерная безопасность. Корпоративная VPN. Требования к построению и подходы к упрощению администрирования».

11 Вишневский В.М. Теоретические основы проектирования компьютерных сетей, Москва, 2003. – 506с.

12 Денисова Т.Б. «Надежность и безопасность услуги VPN».

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
СӘТБАЕВ УНИВЕРСИТЕТІ

ОТЗЫВ

НАУЧНОГО РУКОВОДИТЕЛЯ

на дипломный проект

Рсалімовой Мадины Батырқызы

5В071900 – Радиотехника, электроника и телекоммуникации

Тема: Анализ технологии VPN и ее построение

Одними из ключевых отличительных особенностей больших регионально-рассредоточенных корпоративных сетей считаются: использование глобальных связей и соединение внутренних частных сетей разных филиалов компаний и компьютеров его отдаленных работников с централизованной частной сетью. На сегодняшний день одной из самых распространенных технологий, которая позволяет связывать между собой территориально-рассредоточенные сети и при этом быть достаточно защищенной, является технология VPN, технология виртуальных частных сетей.

Данный дипломный проект Рсалімовой Мадины посвящен анализу работы технологии VPN и ее построению на примере корпоративной сети.

В первой главе дается анализ виртуальной частной сети, ее сущность, показаны различные технологии , протоколы VPN.

Во второй главе рассматривается концепция построения виртуальной частной сети.

В третьей главе в программе Cisco Packet Tracer показана модель виртуальной частной сети для предприятия, проектирование туннеля IP Sec Site to Site.

Считаю, что дипломная работа выполнена на 95/А/«отлично», а дипломант, Рсалімова Мадина Батырқызы, заслуживает присвоения академической степени бакалавра техники и технологии по специальности 5В071900-Радиотехника, электроника и телекоммуникации.

Научный руководитель
маг-р техн. наук, лектор
_____Г.М. Байкенова
“6” 05 2019г.

Ф КазНИТУ 706-16. Отзыв научного руководителя

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
СӘТБАЕВ УНИВЕРСИТЕТІ

РЕЦЕНЗИЯ

на дипломный проект

Рсалімовой Мадины Батырқызы

5В071900 – Радиотехника, электроника и телекоммуникации

На тему: Анализ технологии VPN и ее построение

Выполнено:
а) графическая часть на 10 листах
б) пояснительная записка на 43 страницах

ЗАМЕЧАНИЯ К РАБОТЕ

В настоящее время, с развитием сети Интернет, появилась новая тенденция – использование для конструирования всеобщей корпоративной связи в основном недорогого и доступного (если сравнить с выделенными каналами) транспорта: IP сетей всеобщего пользования (внешние сети). Однако Интернет – это незащищенная сеть, поэтому приходиться изобретать способы защиты конфиденциальных данных, передающихся через незащищенную сеть. Концепция создания виртуальных частных сетей (VPN) активно развивается, чтобы обеспечить эффективное и безопасное использование сетевых атак в открытых сетях.

Дипломный проект Рсалімовой М.Б. посвящен анализу работы и способу организации VPN для объединения территориально-рассредоточенных офисов корпоративной сети.

В первой главе проведен анализ виртуальной частной сети, рассмотрены различные технологии, протоколы VPN, показано различие глобальных сетей от технологии виртуальных частных сетей.

Во второй главе рассмотрены способы построения виртуальной частной сети, проведен выбор необходимых технических средств, кабеля, маршрутизатора, коммутатора путем сравнения нескольких видов.

Третья глава посвящена моделированию виртуальной частной сети для предприятия, проектирование туннеля IP Sec Site to Site с помощью программы Cisco Packet Tracer.

Оценка работы

Считаю, что дипломная работа выполнена на 95/А/«отлично», а дипломант, Рсалімова Мадина Батырқызы, заслуживает присвоения академической степени бакалавра техники и технологии по специальности 5В071900-Радиотехника, электроника и телекоммуникации.

Рецензент
канд. техн. наук, профессор АУЭС
_____ А.С. Байкенов
“____”_____2019г.

Ф КазНИТУ 706-17. Рецензия

Протокол анализа Отчета подобия Научным руководителем

Заявляю, что я ознакомился(-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Рсалимова Мадина

Название: Анализ технологии VPN и ее построение

Координатор:Гулжан Байкенова

Коэффициент подобия 1:40,9

Коэффициент подобия 2:13,5

Тревога:9

После анализа Отчета подобия констатирую следующее:

☐ обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, признаю работу самостоятельной и допускаю ее к защите;

☐ обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;

☐ обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, не допускаю работу к защите.

Обоснование:

.....
.....
.....
.....
.....
.....

13.05.2019 .....

Дата *Подпись Научного руководителя*

Протокол анализа Отчета подобия

заведующего кафедрой / начальника структурного подразделения

Заведующий кафедрой / начальник структурного подразделения заявляет, что ознакомился(-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Рсалимова Мадина

Название: Анализ технологии VPN и ее построение

Координатор: Гулжан Байкенова

Коэффициент подобия 1:40,9

Коэффициент подобия 2:13,5

Тревога:9

После анализа отчета подобия заведующий кафедрой / начальник структурного подразделения констатирует следующее:

☐ обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, работа признается самостоятельной и допускается к защите;
☐ обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;
☐ обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, работа не допускается к защите.

Обоснование:

.....
.....
.....
.....
.....

30.04.2019 .....

Дата

Подпись заведующего кафедрой /

начальника структурного подразделения