МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

кафедра Компьютерных технологий

«Допущен к защите»
Заведующий кафедрой _____
_____
(Ф.И.О., ученая степень, звание)
_____ «_____»_____20__ г.
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Организация корпоративных сетей в условиях угроз воздействия информационной безопасности.

Специальность 5В070400 - ВТ и П

Выполнил (а) Бахтов В.А (Фамилия и инициалы) ВТ 12-4 группа

Научный руководитель Рахимжанова З.М., ст. преп. (Фамилия и инициалы, ученая степень, звание)

Консультанты:

по экономической части:
Бекмуева А.Ч., к.э.н., доцент (Фамилия и инициалы, ученая степень, звание)
_____ «12» 05 2016 г.
(подпись)

по безопасности жизнедеятельности:
Прокофьева И.Г., д.х.н., профессор (Фамилия и инициалы, ученая степень, звание)
_____ «28» 04 2016 г.
(подпись)

по применению вычислительной техники:
Рахимжанова З.М., ст. преп. (Фамилия и инициалы, ученая степень, звание)
_____ «24» 05 2016 г.
(подпись)

Нормоконтролер: Рахимжанова З.М., ст. преп. (Фамилия и инициалы, ученая степень, звание)
_____ «24» 05 2016 г.
(подпись)

Рецензент: Мукимбеков М.Ж., док. техн. наук (Фамилия и инициалы, ученая степень, звание)
_____ «_____»_____20 16 г.
(подпись)

Алматы 2016 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

Факультет Аэрокосмических технологий, информационных
Специальность 5В070400 - ВТиПО
Кафедра Компьютерных технологий

ЗАДАНИЕ
на выполнение дипломного проекта

Студент Востров Егор Александрович
(фамилия, имя, отчество)

Тема проекта Организация корпоративных сетей в условиях угроз воздействия информационной безопасности.

утверждена приказом ректора № 21 от «10» марта 2016 г.
Срок сдачи законченной работы «___» _____ 20___ г.
Исходные данные к проекту требуемые параметры результатов проектирования (исследования) и исходные данные объекта

Создать виртуальную частную сеть VPN на основе протокола L2TP over IPSec с целью подкл. удал. пользователей к внутренней сети с использованием PFSense-800

Установить и настроить межсетевой экран в существующую сеть таким образом, чтобы разделить ресурсы FTP-сервера и внутренней сети при этом в одном адресном диапазоне.

Перечень подлежащих разработке дипломного проекта вопросов или краткое содержание дипломного проекта:

Перечень графического материала (с точным указанием обязательных чертежей)

Рекомендуемая основная литература

Консультанты по проекту с указанием относящихся к ним разделов

Раздел	Консультант	Сроки	Подпись
БЖД	Приходько И.Г.	01.04 – 28.04.16	
Экон. часть	Бекишева А.О.	06.04 – 12.05.16	

Г Р А Ф И К
подготовки дипломного проекта

№ п/п	Наименование разделов, перечень разрабатываемых вопросов	Сроки представления руководителю	Примечание
I	Анализ безопасности		
II	Аппаратная часть		
III	Расчетная часть		
IV	Безопасность жизнедеятельности		
V	Бизнес план		
1	Основы сетевой безопасности		
1.2	Виды сетевых атак		
1.3	Кадкачение и основные функции		
1.8	Технология межсетевых экранов		
1.9	Обзор межсетевых экранов D-Link		
2			
2.1	Описание Dlink DFL-800		
2.2	Описание D-Link DES-3526		
2.3	Межсетевые экраны		
3			
3.1	расчет степени исп. канала		
3.2	Настройка программного решения		
3.5	Создание VPN - туннеля для орг. L2P		
4	Безопасность жизнедеятельности		
5	Бизнес план		

Дата выдачи задания «___» _____ 2016 г.

Заведующий кафедрой Куралбаев З К _____
(подпись) (Фамилия и инициалы)

Руководитель Рахимжанова З М _____
(подпись) (Фамилия и инициалы)

Задание принял к исполнению
студент Востров Е А _____
(подпись) (Фамилия и инициалы)

АННОТАЦИЯ

Выпускной проект посвящён защите информации корпоративных телекоммуникационных сетей в условиях воздействия угроз информационной безопасности, используя оборудование D – Link DFL – 841.

Просмотрен обзор технологий применимых для организации защиты корпоративных телекоммуникационных сетей, произведены расчеты использования канал и большой скорости передачи информации для отдельно взятого числа компьютеров.

В выпускном проекте произвели анализ вредных и опасных производственных факторов, и защищаемых мероприятий по охране труда.

В выпускном проекте была разработана экономическая часть.

ANNOTATION

Graduation project dedicated to information security of corporate telecommunications networks under the impact of threats to information security, using equipment D – Link DFL–841.

View an overview of the applicable technology for securing corporate telecommunications networks, calculations are made using the channel and high data transfer rate for a specific number of computers.

In the final analysis of the project, produced harmful and hazardous working environments and protected labor protection measures.

In the final part of the project it is economically developed.

АҢДАТПА

Шығарылымның жобасы корпоративтік телекоммуникациялық аудың ақпаратының ығына ара шарттар ақпараттық қауіпсіздіктің айбатының әсерінің арнаулы, жабдығын D – Link DFL–841 пайдалана.

Технологияның шолуы корпоративтік телекоммуникациялық аудың ығының ұйымы үшін қолдан– қара–, игерушілік арна есеп айыр– және ақпараттың берілісінің үлкен жылдамдығына компьютердің оқшау ал– саны үшін.

Шығарылымның жобасында зарарлы және қауіпті өндірістік фактордың және қорға– іс–шараның анализын ша еңбектің күзетінің жасады.

Шығарылымның жобасында әзірле– экономикалық бөлік болды.

Содержание

1 Анализ безопасности

1.1 Основы сетевой безопасности

Разработка всемирной паутины проводилась как публичной системы, целью которой является автономная передача информации. Из–за публичности всемирной паутины множество хакеров угрожают безопасности, осуществляя проникновение в информационную систему различных компаний. С помощью всемирной паутины хакер производит взлом и проникновение в сеть компании, благодаря чему хакер имеет возможность:

– произвести кражу информации;

– получения парольные слова, серверные адреса и другое;

– осуществить вход в ИС фирмы под ранее взломанным пользователем.

Из–за вышесказанных возможностей появляется риск оттока важных клиентов фирмы, а также является недобросовестной конкуренцией.

В сетях фирмы располагаются сервера, на которых хранится важная информация, и осуществляют работу жизненно важные приложения, которые являются целью хакерских атак и, основываясь на этом, необходимо правильно произвести планирование безопасности информации хранилища данных и местной сети.

Правильно сформированные приватные сети гарантируют устойчивость согласования элементов сети и подключений с помощью VPN.

Под «частной виртуальной сетью» подразумевается большое количество методов, с помощью которых гарантируется надежность и прочная связь между большими объединениями пользователей. Проблемы, которые угрожают ИБ, удаётся избежать, использовав для контролирования доступности к местной сети и всемирной паутине таких средств, как брандмауэр, прокси–сервер, роутерами и другими спецсредствами.

Очень часто под «частной виртуальной сетью» подразумевается комплекс методов, гарантирующие защищённость траффика, передающегося между компонентами публичной системы. Под публичной системой подразумевается в большинстве своём случаев всемирная паутина [5].

1.2 Виды сетевых атак

Имеется всевозможное количество способов осуществить взлом и нанести ущерб компании. Среди всех выделю следующие способы:

1) черви, которые делают множество копий самого себя, облегчая доступ хакеру, блокирую разный функционал системы, разрушающие файлы и перегружая сеть;

2) DDOS позволяет осуществить перегрузку сетевого траффика и вывод из работающего состояния различных веб–серверов. Позволяет запрашивать различные данные с сервера, генерируя большое количество траффика, блокируя доступ;

3) атака MID, использующаяся хакерами для получения данных во время передачи по сетевым каналам информации, с помощью анализа траффика. При этом используются уникальные программы. Также можно использовать в качество контроля траффика;

4) spoffing DNS, которые производит подмену записей DNS, ретранслируя траффик на иное имя;

5) social engineering, во время использования которой хакер применяет навыки убеждения, втираясь при этом в доверие и в последствии чего жертва сама не ведая ничего выдаёт секреты;

6) спам является неотъемлемой частью атак, при этом в него встраиваются различные скрипты, которые шифруют данные пользователя, а также могут устанавливать различные сторонние программы, которые осуществляют слежку за пользователем. При этом пользователь не поймёт, что произошли изменения;

7) adware и spyware, которые позволяют осуществлять шпионскую деятельность за действиями пользователя, а также на всём экране появляется назойливая реклама, которая не закрывается [3].

1.3 Назначение и основные функции Интернет–маршрутизаторов

Роутер является компонентом сети, который позволяет объединять различные сети в единую, при этом обрабатывая данные согласно заложенным в него правилам, также перенаправляет пакет, основываясь на свою таблицу маршрутизации.

Роутеры позволяют пользоваться большому количеству работникам единым каналом для доступа в интернет. Дополнительно роутер имеет защиту от взлома.

Основные особенности роутеров:

– обеспечивает связь между несколькими разнородными элементами сети, позволяя осуществлять передачу пакетов;

– наличие таблицы маршрутов, на основе которой роутер читает заголовок пакета и передаёт пакет дальше по выбранному пути, который определяется с учетом выбора протокола маршрутизации.

Функции, которые может выполнять роутер: VPN, IDS, фильтрация траффика, NAT, VS, DHCP и т.д.

DHCP позволяет осуществлять присвоение адресов различным устройствам сети. В качестве параметров задаются маска сети и диапазон адресов. При этому компьютер будет иметь уникальный адрес.

NAT осуществляет трансляцию между сетевыми адресами, когда одному адресу присваивается целый диапазон адресов местной сети. При этом осуществляется замена адреса пакета, когда он проходит через роутер, а также порты.

DMZ осуществляет маршрутизацию, весь трафик переадресовывается на различные порты, которые открыты на роутере, и на основе встроенной таблицы портов осуществляется передача на порт, которые указывается в пакете. Но высока опасность взлома, поэтому необходим брандмауэр.

VPN есть соединение между различными сетями, сетью и компьютером, проходящее через всемирную паутину, гарантируя безопасность соединения. Чтобы создать VPN нет необходимости покупать специальное оборудование, также не обязательно арендовать выделенные каналы. На рисунке 1.1 показано удалённое подключение пользователя. На рисунке 1.2 показано удалённое соединение двух филиалов.

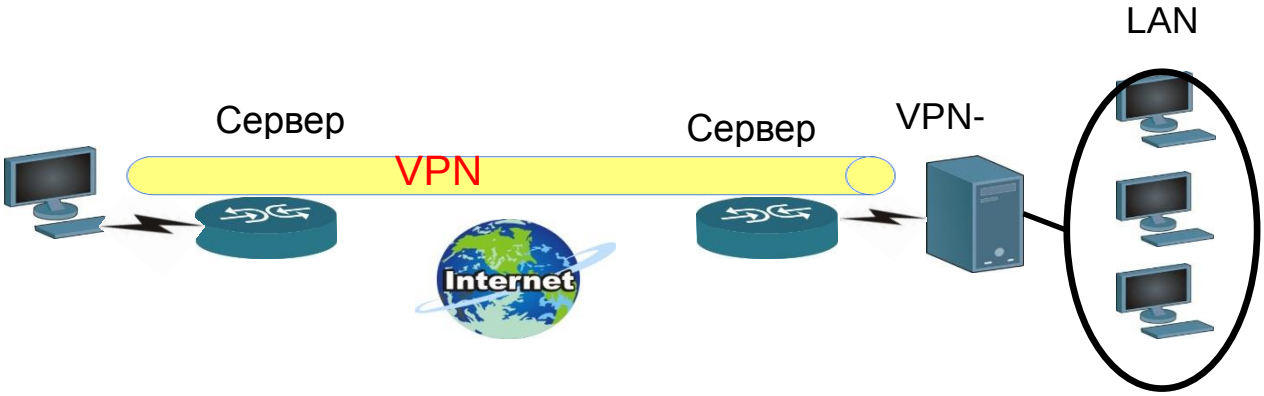

Рисунок 1.1 – VPN для удаленных пользователей

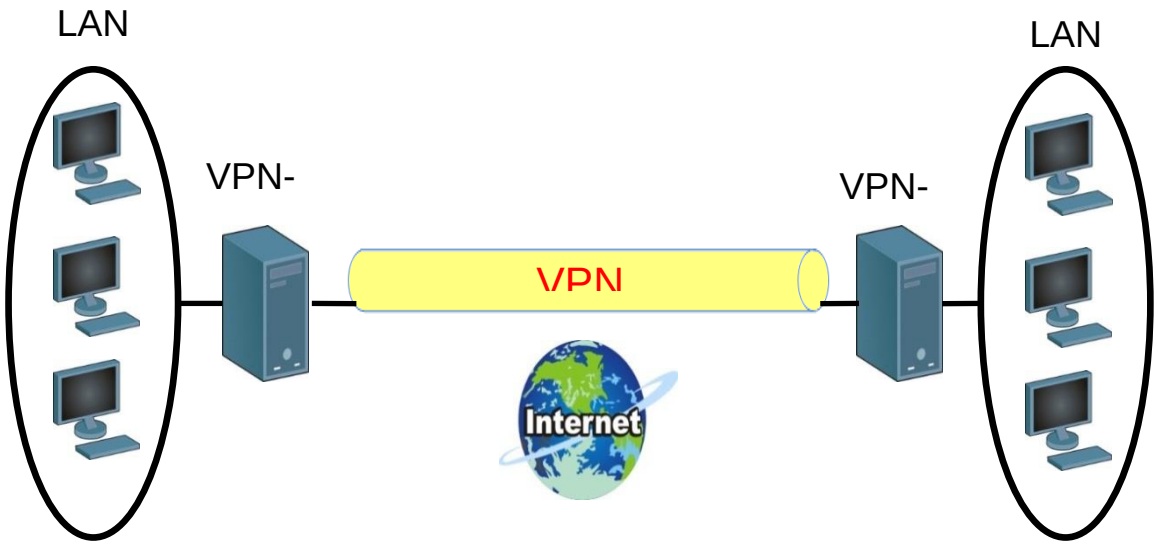

Рисунок 1.2 – VPN для двух офисных сетей

VPN помогает объединять филиалы, которые расположены в разных точках географического пространства. При этом не обязательно, чтобы серверы были в нескольких офисах, что позволяет сделать центральное хранилище данных. Главное, чтобы было постоянное подключение в всемирную паутину. VPN позволяет осуществлять:

– конфиденциальность обеспечивает гарантию сохранности данных, передающихся по общественным каналам, при этом данные не будут просмотрены сторонними людьми;

– целостность данных основывается на том, что данные не будут разрушены, изменены во время передачи;

– доступность заключается в том, что данные всегда будут доступны во время сеанса.

При использовании VPN осуществляется шифрование траффика – это позволяет уберечь данные от просмотра сторонними лицами, также перед использование канала необходимо пройти аутентификацию, ввода запрашиваемы данных, и авторизацию, проверку подлинности ввода данных, что позволяет разграничивать контроль доступа.

Во время открытия сеанса образуется туннель, через который траффик будет проходить. В начале прохождения туннеля происходит инкапсуляция данных, т.е. шифрование, а в конце – декапсуляция, что означает дешифрование данных. С помощью VPN можно осуществлять связь сразу с несколькими пользователями или офисами, создавая несколько туннелей. Такая схема показана на рисунке 1.3.

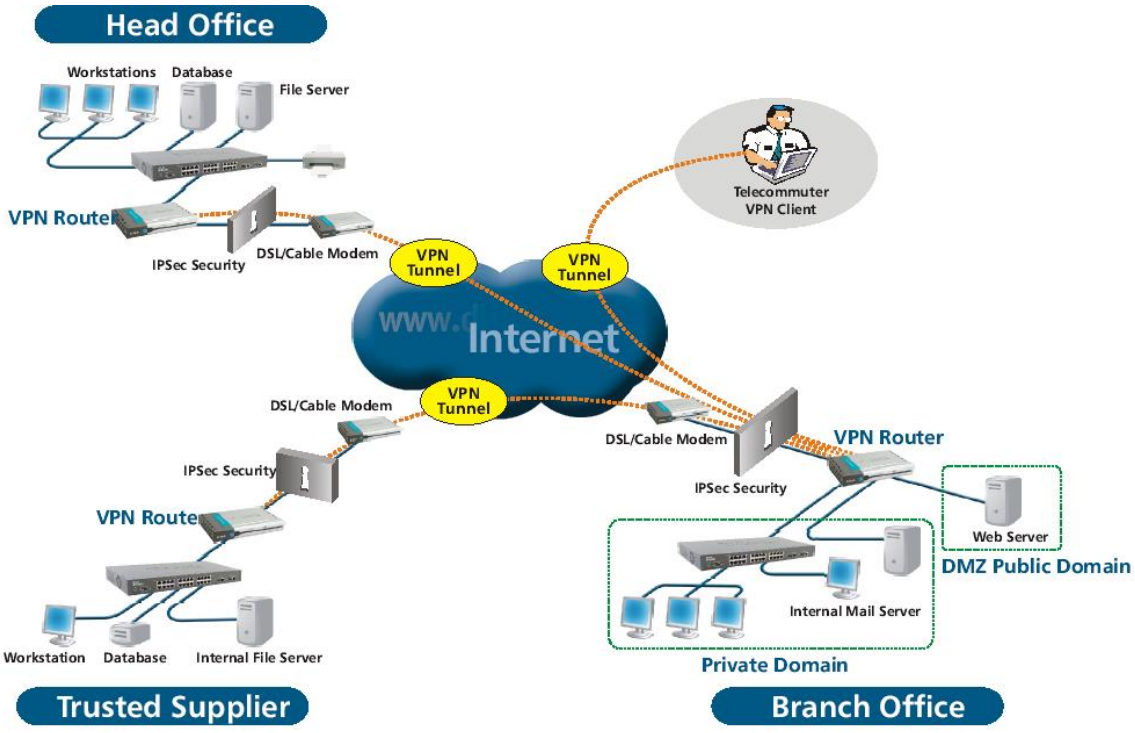

Рисунок 1.3 – Создание VPN–туннелей для нескольких удаленных точек

Перед открытием канала необходимо установить соединение с шлюзом VPN. Стоит учитывать, что внутри приватной сети шифрование отсутствует. Причиной является то, что по умолчанию она считается надёжной и находится под постоянным контролем. Таким образом, шифруется только информация, проходящая сквозь туннель. Существует множество возможностей построить такую сеть. Но самые часто используемые протоколы:

- PPTP используется в ОС Windows;
- L2TP разработан фирмой Cisco, используется вместе с IPSec;
- IPSec создан IETF и используется в большинстве сетях [10].

1.4 PPTP

PPTP используется в приватных виртуальных сетях. Протокол позволяет создавать удалённые подключения, благодаря чему пользователи получают возможность использовать безопасный туннель к корпоративной сети из любой точки мира. Протокол PPP изначально не разрабатывался ля создания туннелей между сетями. PPTP есть расширяет возможности PPP. PPP осуществляет работу на втором уровне модели OSI, главной целью является инкапсуляция данных, т.е. шифрование, и их доставка по типу соединения точка–точка.

PPTP формирует канал, который защищается для обмена данными с помощью различных протоколов. Информация о протоколах, которые поступают во всемирную паутину упакованы в кадры PPP, далее происходит шифрование с помощью PPTP в пакеты IP протокола. В таком виде они передаются через сеть. Принимающий клиент осуществляет дешифрование пакета и далее происходит обработка кадра. Примерным образом PPTP создаёт соединение точка–точка и, основываясь на защищенном канале передаёт по нему сведения. Преимуществом этого является поддержка множества протоколов. Благодаря чему достигается прозрачность защиты для различных протоколов прикладного и сетевого уровней. Из–за чего в местной сети можно использовать любые протоколы. Также PPTP можно использовать для доступа к ISP сетям, которые используются провайдерами для доступа к всемирной паутине.

PPTP использует один из нескольких методов шифрования: RSA, 3DES, RC4 и другие.

Важно разобраться, как осуществляется соединение PPTP. Перед тем как начать передачу пакетов необходимо открыть туннель, через который будет осуществляться их передача. Для этого отправляется запрос серверу для установки соединения. Сервер получает его, обрабатывает и отправляет ответ , который или разрешает установку соединения или запрещает. После чего осуществляется создание туннеля. Весь траффик шифруется и в кадр добавляется сообщение KEEP ALIVE, которое определяет, не отключился ли

сервер, а сервер отправляет ответное сообщение. Если поменялись параметры передачи, то отправляется сервером сообщение на изменение параметров связи. При завершении работы клиент отправляет серверу сообщение, что соединение необходимо закрыть, а сервер в ответ подтверждает его, впоследствии чего туннель перестаёт существовать, а траффик будет идти через всемирную паутину. На рисунке 1.4 показана схема подключения PPTP.

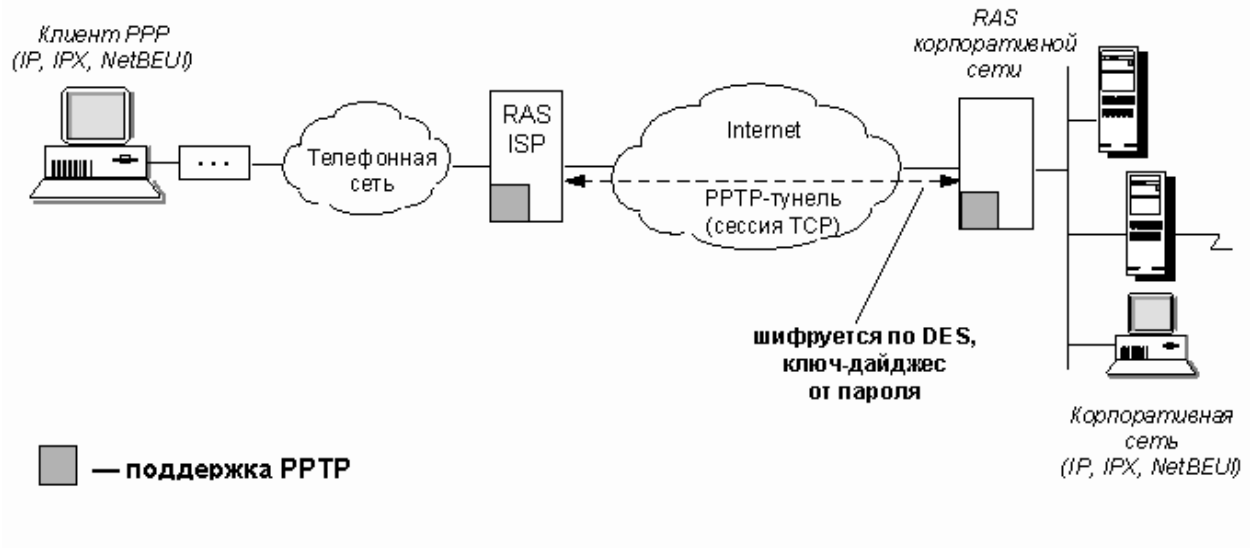

Рисунок 1.4 – Схема подключения с помощью PPTP

При передачи данных по туннелю осуществляется шифрование на стороне клиента, а на стороне сервера – дешифрование. При обратной передаче всё происходит наоборот. PPTP добавляет в кодр PPP–header и trailer. Затем PPP собирается в GRE–пакет, например IP. Но GRE не гарантирует доставку. После чего осуществляется инкапсуляция PPP в кадр с заголовком IP. В заголовок входит адрес получателя и отправителя. В самом конце добавляются окончание кадра. На рисунке 1.4 показана структура данных пакета.

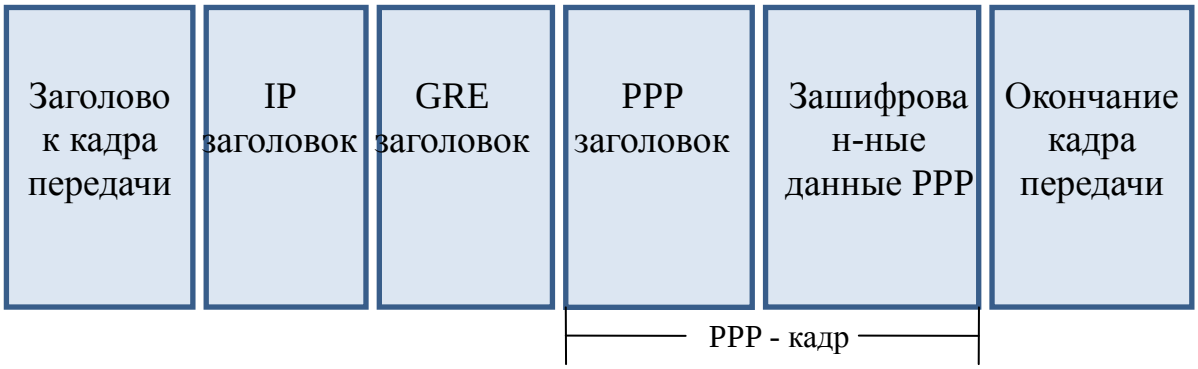

Рисунок 1.5 – Структура данных для пересылки по туннелю PPTP

Чтобы организовать VPN, базирующийся на PPTP, нет необходимости совершать крупные расходы и сложные настройки, для этого необходим настроенный сервер PPTP и клиентские компьютеры с настроенным софтом. Если есть необходимость в соединении филиалов, то необходимо не настраивать на каждом отдельном компьютере, а произвести конфигурацию роутера для подключения удалённого офиса. Такими роутерами является ряд моделей компании D–Link серии DFL.

1.5 L2TP

Протокол L2TP есть группирование двух протоколов разных уровней, PPTP и L2F. Главным преимуществом протокола является то, что можно создавать туннели не в одних только сетях IP, но в frame–relay и т.д. UDP используется в качестве протокола трансфера данных для сетей L2TP. L2PT использует одинаковый размер кадра для управления и отправки данных.

L2PT начинает собирать пакет для передачи данных через туннель с добавления к полю данных PPP названия и L2TP заголовка. Затем UDP инкапсулирует полученный пакет. Добавление к пакету шифрованного уведомления UDP определяется выбранным типом безопасности. После чего осуществляется инкапсуляция в IP. К пакету прибавляется заголовок IP, который содержит адрес получателя и отправителя. И в конце L2TP осуществляет вторую инкапсуляцию PPP, чтобы подготовить информацию к передаче. На рисунке 1.6 показана структура данных пересылки L2TP.

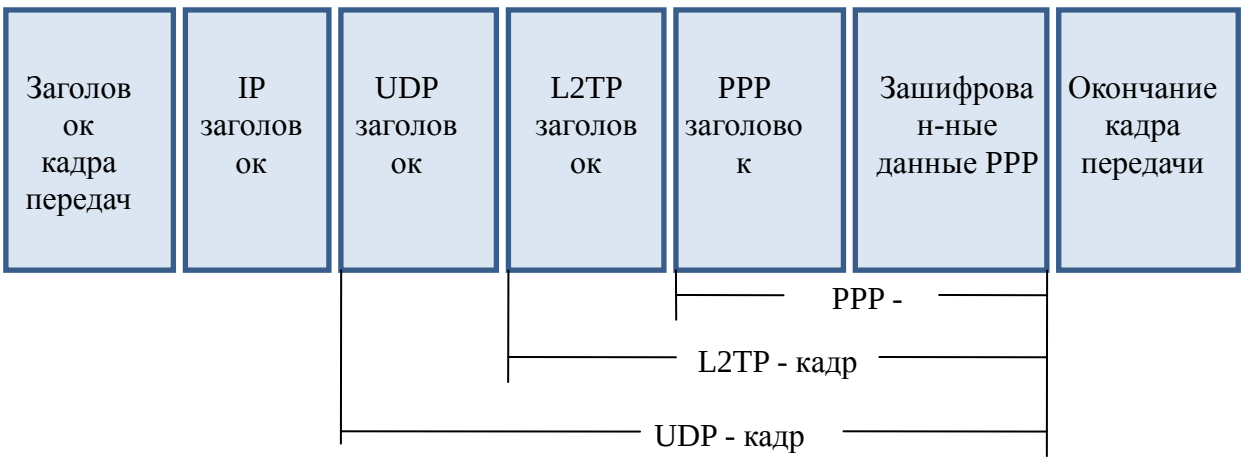

Рисунок 1.6 – Структура данных пересылки L2TP

Обработку принятых данных осуществляет компьютер, производит анализ заголовка и окончания PPP, при этом удаляет IP заголовок. После чего компьютер производит обработку UDP заголовка и для идентификации туннеля используется L2TP заголовок. После данных манипуляций пакет содержит только необходимые сведения, которые переотправляются необходимому адресату [6].

1.6 IPSec

Для усиления защиты протокола IP разрабатывался IPSec. Защита улучшается из–за использования альтернативных протоколов, которые прибавляются к пакету свои заголовки, называемые инкапсуляциями. Задачи, которые IPSec может решить:

– инициализируя защищенный канал производить аутентификацию;

– осуществление шифрования во время передачи информации;

– для работы необходимы секретные ключи, которые в автоматическом режиме передаются клиентам.

IPSec включает такие протоколы, как AH, ESP, IKE. Разберу их. Authentication Header гарантирует не поврежденность информации, контролируя бит чётности пакета. Не обеспечивает конфиденциальность шифрованного маршрута, т.к. при прохождении через NAT меняется и заголовок пакета, т.е. хэш–сумма.

ESP защищает не только целостность и кодирование, но и реализуется защита замены пакетов. Его заголовок располагается между заголовком IP и кодированным пакетом.

IKE позволяет произвести инициализацию защищённого канала, а также позволяет осуществлять взаимообмен ключами между клиентами VPN. Используется протокол UDP с портом №500.

Для кодирования в IPSec применяются различные симметричные методы, которые используют секретные ключи.

IPSec осуществляет работу следующим образом. Взаимодействие протоколов IPSec сделано следующим путем. В начале с поддержки протокола IKE между 2 концами безопасный путь, названный «безопасной ассоциацией» – введено Сопоставление безопасности, SA. Поблизости этот финал признания, который сделает, сделан подделанным, и особенности защиты подобной информации выходят, равно как кодирующий метод, сессионный источник, и т.д. Далее в рамках введенных подделанных запусков работы документ AX или ESP. SA это слово IPSec в целях обозначения конфигурации. Поблизости созданный VPN в целях любого, прикладной протокол, одни несколько SA формируются (т.е. один в целях AH и один в целях ESP).SA, формируется двумя начиная с любого SA – эта односторонняя ассоциация и данные, которые необходимо отправить в 2 установках. Полученный SA пары остается в любом узле.

Т.к. любая секция готова поместить количество тоннелей с другими элементами, любой SA содержит уникальное разрешение, чтобы установить в это или что к узлу кто–то принадлежит. Данный выпуск SPI или индикатор параметра безопасности называют.

SA, который будет сохранен в основании информации (DB) ПЕЧАЛЬНЫХ (База данных Сопоставления безопасности).

Каждый раздел IPSec кроме того содержит 2–ю DB – SPD (База данных Политики безопасности) (политики DB безопасности). Возлюбленный включает построенный в политика отдела. Большая часть VPN заключений позволяет формировать из многих комбинаций подходящих алгоритмов в целях любого отдела с тем, что необходимо определить ассоциацию.

Симметричные методы в целях зашифровывания/расшифровки информации.

Шифровальная ревизия означает в целях контроля единства информации.

Способ идентификации отдела. Самые широко распространенные методы – данный задавал ворота (предварительно разделенные тайны) или свидетельства SA.

Использовать заказ единицы тоннеля или заказ транспорта.

Что использовать категорию Диффи Хеллмен (группа 1 DH (768 битов); группа 2 DH (1 024 бита); группа 5 DH (1 536 битов).

Использовать единицу AX, ESP, или и это и другой совместно.

Использовать единицу PFS.

Формируя политиков, это равно как регулирование, может быть формирование из высоко устроенного списка алгоритмов и Диффи Хеллмена из компаний. Diffie–Hellman (DH) – документ кодирования прикладного в целях униформы определения конфиденциальные ключи в целях IKE, IPsec и PFS. В этом случае это скорее применено 1–е подобранный в двух предоставлениях отделов. Это очень важно, чтобы все в политике безопасности разрешило достигать этого совпадения. Если из–за отказа в политиках Акции все другой встречаются, секции, все одинаково не может определить консолидацию VPN ни в каком случае. Соседняя установка тоннеля VPN между различными способами должна учиться, какие методы сохранены любым дополнительным путем, чтобы была вероятность выбора более безопасных политиков от вероятного.

Пластичность IPSec заключается в целях каждой проблемы предполагается, некоторые методы ее решения и способы, отобранные в целях единой проблемы как правила, не завися от внедрения методов других вопросов ни в каком случае. В это же время рабочая группа IETF определила основной набор поддержанных функций и алгоритмов, который обязан быть, одинаково выполненым во всех продуктах, которые поддерживают IPSec. AX и у механизмов ESP есть все шансы, которые будут применены с различными схемами идентификации и зашифровыванием, некоторые из которых обеспечены обязательные. Например, в IPSec определен, что пакеты заверены или с поддержкой функций MD5, или с поддержкой функций SHA–1. Изготовители товаров, в которых у работ IPSec есть все шансы добавить другие методы идентификации и зашифровывания. Например, некоторые продукты bcgjkmpe.n такие методы криптографии, Иглобрюхих, Бросок, RC5, и т.д. равен как 3DES.

Ограничение IPSec в этом случае, что это поддерживает только информационную передачу на уровне IP протокола.

AX и протоколы ESP работают в двух заказах: транспорт и тоннель.

В данном не защищены все области начального пакета. ESP документа подтверждает подлинность, целостность выполняет контроль и шифры только область информации пакета IP AX, протокол защищает больше областей: в дополнение к информационной области также некоторые области заголовка, за исключением областей изменили переводом, например, области TTL (Время, чтобы жить – время существования пакета информации).

В туннельном заказе начальный пакет расположен в другом IP пакете, и предоставляющая информация сделана в основе заголовка нового пакета IP.

Есть 2 главных схемы использования IPSec расходящаяся во мнениях роль узлов, делающих защищенный канал.

На рисунке 1.7 показано создание канала между двумя точками.

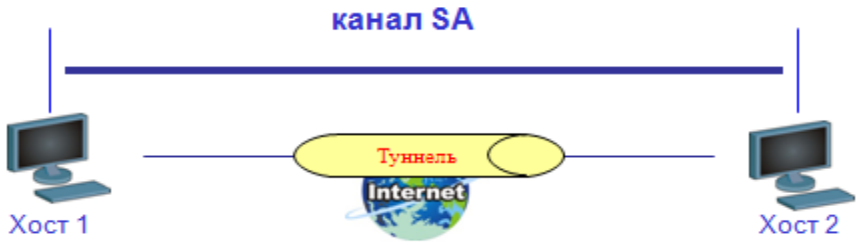

Рисунок 1.7 – Создание канала между двумя точками

Во второй схеме канал инсталлирован между двумя воротами безопасности. Эти ворота принимают данные от заключительных узлов, связанных с сетями, расположенными позади ворот. Заключительные узлы не поддерживают протокол IPSec, движение, посланное в общедоступную сеть, проходит через ворота безопасности, которые выполняют защиту от ее собственного имени. На рисунке 1.8 показано создание канала между двумя шлюзами.

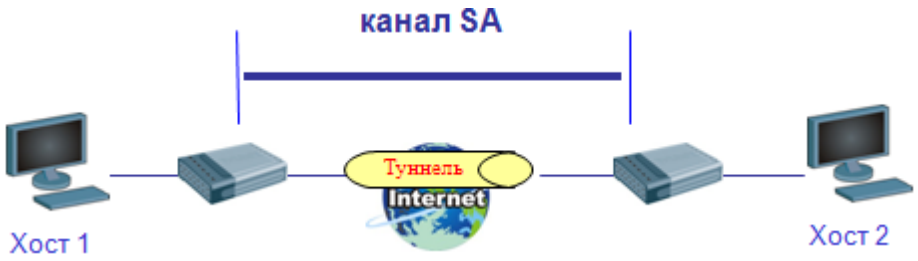

Рисунок 1.8 – Создание канала между двумя шлюзами

Для хостов используются транспортный и туннельный режимы, а для шлюзов – туннельный [6].

1.7 Фаза Один и Фаза Два

Установка связи VPN осуществляется в два этапа. В первой фазе узлы договариваются о способе алгоритме кодирования, идентификации и т.д. Это происходит на основании принятых 3 пакетов (агрессивный способ) или 6 пакетами (обычный способ). После успешной завершении операции формируется SA и процесс переходит в фазу 2.

Во второй фазе происходит генерация сведений о ключах, части договариваются про политику, которую будут использовать. Эти действия называются скоростным режимом, отличаясь от фазы 1, что возможно только устанавливаться в конце последней фазы. Правильный конец фазы 1 приведёт к появлению Фазы 2 и установку тоннеля считают законченной. Сначала к узлу там приходит пакет с адресом получателя другой сети, и узел активирует Фазу 1 узлом, который ответственен за другую сеть. Давайте примем, тоннель между узлами успешно инсталирован и ожидает пакеты. Узлы должны определить перо друг друга и сравнить политику согласно истечению установленной стадии времени. В этот момент в дальнейшем отнесен в целую жизнь Фазы Один или целую жизнь IKE SA. Узлы, кроме того, обязаны изменить источник в целях зашифровывания информации через другой интервал времени, когда в дальнейшем упоминается как время существования Фазы Два или целая жизнь IPSec SA. Фаза Две целых жизни обычно, чем в первой фазе, так как источник должен быть изменен чаща. Типичное время существования Фазы Два – 60 минут для Фазы 1 это равно 24 часам. Самое маленькое различие между Фазой Один и Фазой Два – 5 минут. Необходимо показать подобные особенности времени существования в целях двух устройств. Если не выполнить его, выбор, если первоначально тоннель установлен безопасно, в этом случае вероятен, однако согласно истечению главного нескоординированного периода существования, которое прервет коммуникация. Проблемы появятся случае, если время существования Фазы Каждый – меньше, чем подобный параметр Фазы Два. Если тоннель формировал, ранее висит, в этом случае первое, у которого есть потребность в контроле – данный период существования в двух узлах. Тем не менее необходимо заметить, что поблизости политикам замены в 1 от устройств, изменение займется в силе только поблизости последующим выйти из Фазы Только. Чтобы изменения подняли в силе без задержки, необходимо удалить SA в целях этого тоннеля от основания информации ПЕЧАЛЬНЫХ. Это вызовет обзор соглашения между узлами с новыми вариантами политики доверительных отношений [1].

1.8 Технология межсетевых экранов

Брандмауэры предназначены для противостояния сетевым атакам и угрозам для местной сети. Брандмауэр – это комплекс программных или аппаратных мер, фильтруя траффик, проходящий сквозь него, на основе написанного набора правил. Брандмауэр ставят между всемирной паутиной и местной сетью, хотя иногда их устанавливают внутри самой местной сети, что даёт создать политику внутри компании по защите сети.

Брандмауэром может являться компьютером со специализированным ПО, который анализирует весь проходящий траффик. Любой проходящий пакет проходит проверку на ряд правил, которые ему задали. Если не удовлетворяет пакет правилам, то он блокируется и отбрасывается. В ином случает его пропускают. Данный метод называется фильтрацией.

Брандмауэр может выполнять специальные функции защиты, зависящие от типов используемых портов. Брандмауэр может пропускать траффик по FTP, но не по telnet. Или может работать с протоколами TCP, но не с UDP [3].

1.9 Обзор межсетевых экранов D–Link

У организации D–Link существует линейка брандмауэров NetDefend, которая является комплексом решений для обеспечения безопасности. Линейка NetDefend учитывает все требования, которые прдъявляются безопасности и предотвращению хакерских атак, вирусных угроз и гарантирует конфиденциальность информации. На рисунке 1.9 показана линейка NetDefend. На рисунке 1.10 и 1.11 показано сравнение двух брандмауэров.

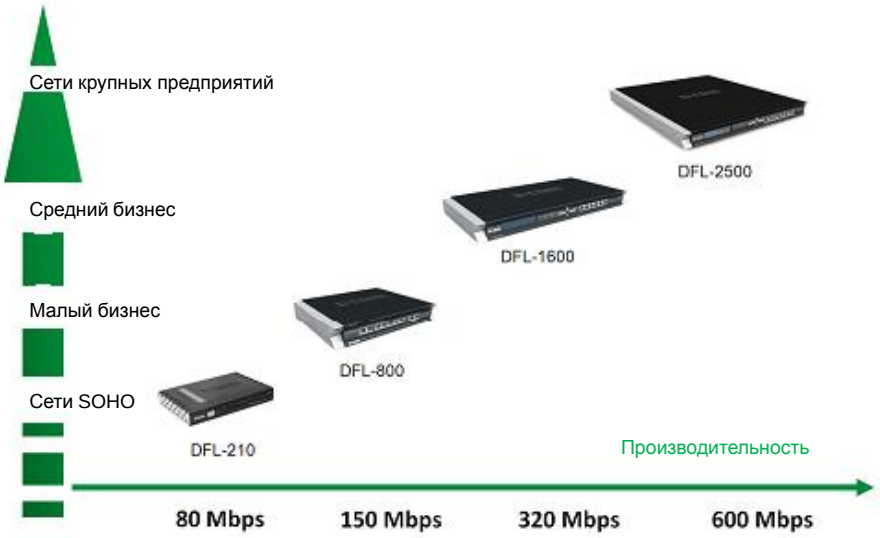

Рисунок 1.9 – Линейка NetDefend

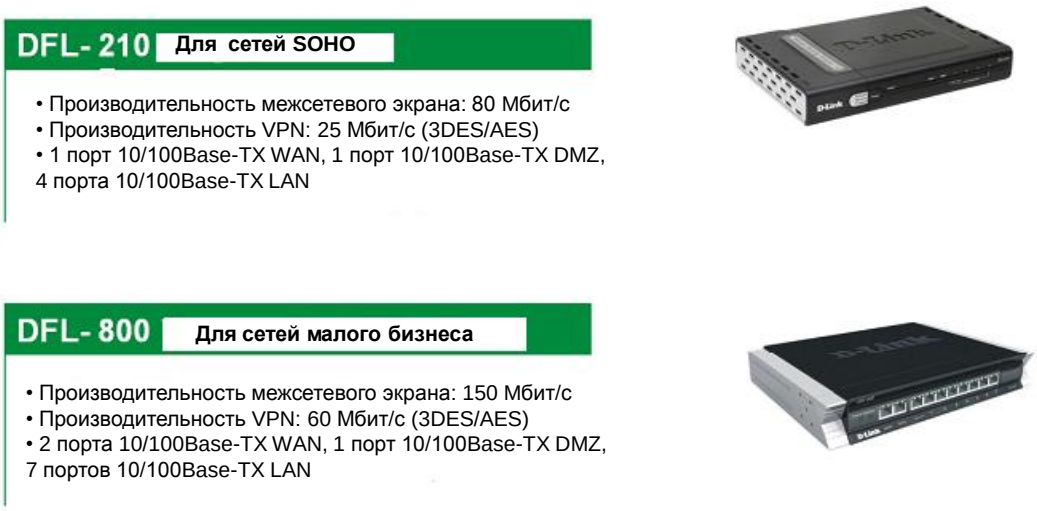

Рисунок 1.10 – Сравнение двух брандмауэров

Рисунок 1.11 – Сравнение брандмауэров

Их особенность – фильтрация входящего и исходящего траффика, основываясь на заголовки IP и TCP, такие как адреса адресата и адресанта и их порты. Реализовать фильтрацию можно многими способами, начиная блокирования определённых адресов и заканчивая портами и протоколами.

Для защиты уязвимых мест, которые присущи фильтрованным пакетам, брандмауэры используют дополнительные программа с целью фильтрации соединений сервисов FTP и других. Такие программы называют прокси, а хост является шлюзом приложения. Это позволяет добиться прямого взаимодействия между внешними хостами и авторизованными клиентами. Шлюз позволяет фильтровать весь траффик на уровне OSI №6.

Преимуществом такого подхода является составлением простых правил фильтрации, организовывая при этом большое количество проверок. Защита на 6 уровне модели OSI позволяет выполнять большое число различных проверок, снижая вероятность использования различных бэкдоров, сетевых атак и т.д.

Но из этого появляются следующие недостатки: маленькая производительность, прокси не может работать с неизвестными ему протоколами.

Брандмауэры могут отслеживать сеансы, установленные приложениями, блокируя пакеты, которые с вероятностью могут нарушить безопасность сети.

При этом брандмауэр не решает все поставленные задачи предотвращения угроз. У брандмауэров нет защиты от бэкдоров. Также нет гарантии защиты от атак внутри сети, ограничивать внутренние сервисы.

В целях решения подобных задач, выполняющих хорошо обдуманный, политика безопасности в том, что отношение между условиями безопасности и потребностями пользователей будет наблюдаться [3].

1.10 Постановка задачи

В данном дипломном проекте рассматривается безопасность корпоративных телекоммуникационных сетей, для этого проводим эксперименты на оборудовании:

− настройка тоннеля канального уровня с использованием оборудования D–LINK DFL–841 и совместным использованием с защищенной сетью:

− создание VPN–туннеля на основе протокола L2TP.

Цель расчета:

− провести расчет степени использования каналов и дать оценку скорости передачи информации для каждого взятого числа компьютеров.

2 Аппаратная часть

2.1 Описание D–Link DFL–810

D–связь DFL–810 – объединенные роутеры связи ряда DFL представляют высокоэффективные решения, которые обеспечивают надёжность сети и предназначенный чтобы удовлетворить растущие требования малого и среднего бизнеса. Поддержка IEEE 802.11n стандарт, осуществленный в роутерах DFL–170N, DFL–150, DFL–510N, DFL–1120N позволяет достигать той же самой работы, как в зашитых сетях, но с наименьшим числом ограничений. Наилучшая защита сети достигнута с помощью организации туннелей виртуальных приватных сетей , поддержка протоколов безопасность IP (IPSec), PPTP, L2TP, GRE Благодаря туннельным торговым представителям VPN, филиалы могут получить удаленный доступ к сети от любого пункта и в любое время без установки клиентского программного обеспечения. На рисунке 2.1 показан роутер D–Link DFL–810.

Рисунок 2.1 – D–Link DFL–810

Основные характеристики:

Интерфейс Ethernet:

- 1 глобальный порт1000 Мбит/с;
- 8 сетевой порт1000 Мбит/с.

Производительность:

- Пропускная способность брандмауэра: 47 Мбит/с;
- Максимальная скорость VPN: 25 Мбит/с;
- Численность сессий: 20 000;
- Численность новых сессий (в секунду): 200;
- Политики брандмауэра: 200.

Виды Интернет–соединения:

- Динамические/Статические IP;
- PPTP/L2TP/PPPoE;

- Multiple PPPoE.

Брандмауэр:

- постоянный маршрут;
- DDNS;
- Маршрутизация VLAN;
- фильтр web.

Сеть:

- клиент/сервер DHCP;
- Relay DHCP;
- IEEE802.1v VLAN;
- Multicast IP;
- IPv6.

Приватная сеть:

- туннель–VPN: 28;
- туннель–IPSec: 12;
- L2TP/PPTP клиенты : 10;
- Traversal NAT IPSec;
- IP Security Encapsulating;
- Header Authentication IP;
- Tunnel VPN Keep Alive.

Осуществляют управление:

- предельной скоростью;
- приоритетом потока;
- QoS.

Можно управлять с помощью:

- пользовательского web–интерфейса;
- CLS.

Брандмауэр:

- статический маршрут;
- DDNS;
- осуществление маршрутизации VLAN;
- PAT, NAT;
- осуществляет фильтрацию web.

Виртуальная приватная сеть:

- туннели VPN: 27;
- туннели IPSec: 13;
- Клиенты L2TP /PPTP: 13;
- GRE: 6;
- IPSec Traversal NAT;
- Нахождение недействующих узлов;
- IP Security Encapsulating;
- IP Header Authentication;

- Tunnel VPN Keep Alive;
- Spoke and Hub.

Управление системой:

- доступ к интерфейсу с помощью HTTPS и HTTP;
- CLI.

2.2 Описание D–Link DES–3551

Серия DES–3527/3551 xStack свитчей включает стекирующие L2 + уровня доступа, обеспечивающего безопасную связь пользователей к сети крупных предприятий и предприятий малого и среднего бизнеса (SMB). Свитчи обеспечивают физическое стекирование, статическое направление, поддержку групп мультиадреса и расширенного оборудования системы безопасности. Основываясь на выше написанном, данное устройство является идеальным решением уровня доступа. Свитчи легко объединяются с свитчами уровня ядра L3 для формирования многоуровневой структуры сети с быстродействующей магистралью и централизованными серверами. На рисунке 2.2 показан D–Link DES–3551.

Рисунок 2.2 – D–Link DES–3551

Свитчи DES–3527/3551 поставляются 24 или 48 Ethernet 10/100 МБит/с портами и поддержкой 4 uplink–портов 1 Гбит Ethernet. Допустим, что пользователям необходимо обеспечение связи таких устройств: телефоны IP , точки доступа и сетевые камеры , возможно использовать DES–3527P или DES–3551P, оборудованными портами на 24 или 48 10/100 Мбит/с, поддерживающими PoE. 8 из этих портов позволяют соединять с устройствами мощностью до 30 ВТ на один порт, в то время как другие порты соответствуют стандартным 802.3, которая обеспечивает мощность 15.4 Вт на порт. Два порта SFP/10/100/1000Base–T на лицевой панели обеспечивают гибкую связь по оптике или меди. Порты 10/100/1000Base–T, которые расположены на тыльной панели, могут использоваться и в качестве портов стекирования с полным полосно–пропускающим рядом из 4 ГБит/с и как медь uplink–порты 1 Гбит Ethernet. Поддержка функции физического стекирования позволяет пользователям объединяться в стеке с 8 устройствами. Свитчи – хорошая альтернатива более дорогим свитчам на основе шасси.

Свитчи ряда DES–3527/3551 xStack обеспечивают широкий набор последнего оборудования системы безопасности, которые включают 802.1X VLAN, ощущающие управление доступностью, основываясь на MAC, и управление доступом, основываясь на WAC. 802.1x VLAN – непрерывное решение безопасности для окончательного пользователя и функция WAC, которая обеспечивает управление доступа с товарищеской встречей пользователю механизма идентификации. Кроме того, выключатель поддерживает обязательную функцию «IP Порт MAC», разрешая администратору создавать связку исходный IP–адрес – исходный Мак адрес – порт адресанта для проверки DHCP информации и блокирования незаконных адресов IP с целью безопасности сети. DES–3527 может определить и расположить по приоритетам пакеты, которые предназначены для центрального процессора с целью предотвращения нарушений функционирования сети из–за вредного движения и защиты выключателя.

Основные характеристики:

Интерфейсы:

- 46 портов 10/100 BASE–X;
- 2 порта 1000 BASE–X;
- 2 порта 100/1000/SFP;
- RS–232;
- 1 ГБит и 100BASE–FX порт SFP.

Производительность:

- максимальная пропускная способность: 18.8 Гбит/с;
- максимальная скорость 64–битных пакетов: 14.1 Mpps.

Виртуальный стек:

- возможность использовать Management Single IP;
- до 30 устройств, которые объединяются в стек.

Функции безопасности:

- SSH v3;
- SSL v2.

Функция Security Port:

- До 60 MAC на порт VLAN;
- Управление одноадресным/многоадресным/широковещательным каналами;
- Server DHCP Screening;
- Защита от атак BPDU.

Управление

- интерфейс WEB;
- CLI;
- Telnet сервер;
- Telnet клиент;
- TFTP клиент.

2.3 Межсетевые экраны

Брандмауэр − такая сложная программное или аппаратное средство, которое даёт шанс осуществить фильтрацию и контроль пакетов, проходящих через него согласно правилам. Это вводится на границе между внутренней и внешней сетями. Главной целью брандмауэра является защита компьютерных сетей или определенных узлов против доступа для преступников. Брандмауэры часто называют фильтрами, который связаны с их главной целью – отфильтровать кадры, которые не подходят по критериями, определенными в конфигурации. На рисунке 2.3 показан принцип работы брандмауэра.

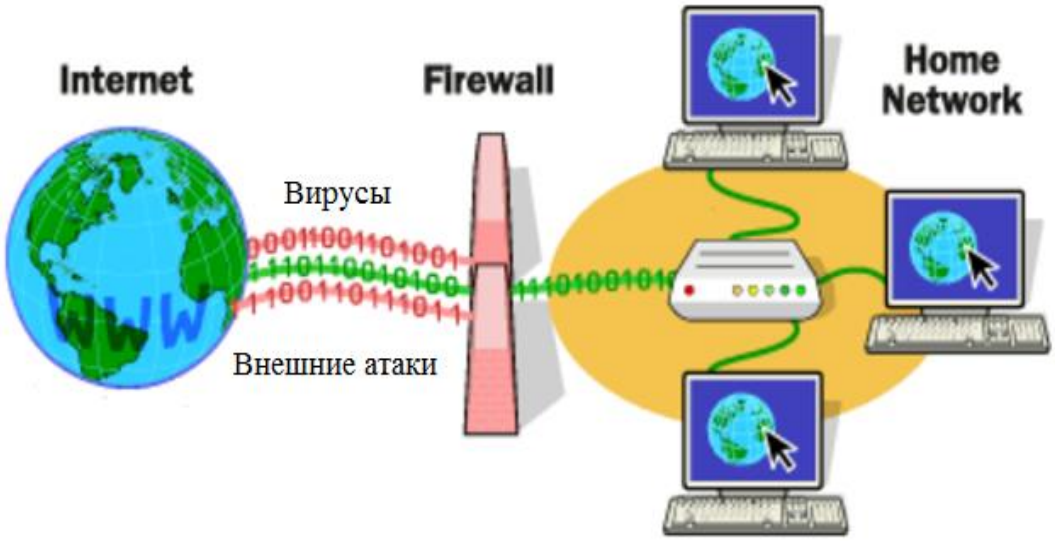

Рисунок 2.3 − Принцип работы брандмауэра

Правильно настроенный брандмауэр – самое важное устройство защиты. Однако, это не будет в состоянии предотвратить нападение через разрешенную линию связи. Брандмауэр не защитит от внутренних пользователей, как они уже находятся в системе. Есть два главныз вида брандмауэров: брандмауэры прикладного уровня и брандмауэры с фильтрацией пакетов. Различные принципы работы лежат в основе их, но при правильной установке оба типа оборудования обеспечивают правильное исполнение системы безопасности, состоящего в блокировании запрещенного траффика. Брандмауэры экраны по доверенности или прикладного уровня , представляют пакеты программ, которые основаны на операционных системах Windows NT и Unix или на платформе аппаратных средств брандмауэров. Брандмауэр обладает несколькими интерфейсами для нескольких сетей, с которыми он связан. Набор правил политик описывает передачу кадров между различными сетями. Если в правиле нет никакого

явного разрешения к допуску данных, брандмауэр отклоняет или отменяет передачу их.

Брандмауэры с фильтрацией кадров могут быть пакетами программ, которые основаны на операционных системах Unix и Windows NT или на платформах аппаратных средств брандмауэров. У брандмауэра есть несколько интерфейсов для каждой сети, с которыми подключается. Подобные брандмауэры прикладного уровня, доставляют пакеты между сетями, которые основываются на правилах. Если правило запретит явно определенный пакет, то соответствующие пакеты будут отменены или отклонены брандмауэром [6].

3 Расчетная часть

3.1 Проводим расчет степени использования канала и оцениваем скорость передачи информации для взятого числа компьютеров

Цель данного расчета:

1) провести расчет степени использования канала;
2) оценить скорость передачи информации для взятого числа компьютеров.

Перед расчётом степени исользования канала сети необходимо в первую очередь определить общий объём информации, который передаётся по локольной сети в течение дня. Предположу, что на предприятии работают 4 категории пользователей:

– которые используют сеть для перессылки документов по электроннной почте;
– которые загружают файлы с FTP;
– которые используют VOIP и телеконференции для переговоров и рабочих совещаний;
– которые работают с удалённой БД.

Данные об объёме данных взяты на основе исследований. Чтобы рассчитать общий объём передаваемых данных по ЛВС, необходимо воспользоваться нижеприведёнными данными. Количество пользователей сети – 50 человек. В таблице 3.1 приведён объём трафика для всех 4–х категорий.

Таблица 3.1 – Объем затрачиваемого трафика

Объем затрачиваемой информации в (Mb)	Вид
500	Пересылка документов по электронной почте
500	Работа с удаленными базами данных
500	Просматривание Web страниц
300	Передача данных мультимедиа
200	Обновление программного обеспечения

Наблюдения показали:

– электронную почту используют 98–100% работников;
– загрузкой файлов с FTP пользуются 45–50% работников;
– работой с удалёнными БД заняты 65–70% работников;

– использованием VOIP и видеоконференций составляет 10–20% работников, с каждым годом количество которых увеличивается.

Объём данных, передающийся за день по ЛВС составляет:

$$Q = 500 + 500 + 500 + 300 + 200 = 2 \text{ Гб} \quad (3.1)$$

Затем переведу данные в байты:

$$Q = 2 \cdot 1024 \cdot 1024 \cdot 1024 = 2.147 \cdot 10^9 \quad (3.2)$$

Чтобы продолжить расчёт необходимо узнать длину кадра. Длина кадра в Ethernet составляет от L_{min}=1000 байт до L_{max}=1500 байт. Служебная информация записывается в кадр TCP с длиной $L_{sl\_TCP/IP}$=48 байт. При этом учту избыточность IPSec. Это зависит от используемых политик и криптографии. Основная длина кадра AH L_{baz_AH}=12 байт, при использовании туннеля длина возрастает до L_{tun_AH}=20. Длина HMAC равна L_{digest_AH}=12 байт. Длина протокола ESP равняется L_{baz_ESP}=10 байт, при использовании туннеля L_{tun_ESP}=20 байт. Когда используется NAT, то L_{NAT}=8 байтю Если используется шифрование DES, то L_{des}=8 байт. Зная эти показатели, рассчитаю длину кадра для AH:

$$L_{sl\_AH} = L_{baz\,AH} + L_{tun\,AH} + L_{digest\,AH} = 12 + 20 + 12 = 44 \text{ байт} \quad (3.3)$$

Рассчитаю длину кадра протокола ESP по формуле:

$$L_{sl\_ESP} = L_{baz\,ESP} + L_{tun\,ESP} + L_{NAT\,ESP} + L_{des\,ESP} = 10 + 20 + 8 + 8 = 46 \quad (3.4)$$

Вычислю длину кадра, передающегося по сети:

$$L_{sl} = L_{sl\,TCP/IP} + L_{sl\,AH} + L_{sl\,ESP} = 48 + 44 + 46 = 138 \text{ байт} \quad (3.5)$$

На основе выше проведённых вычислений определю минимальную длину кадра:

$$L_{info\,min} = L_{min} - L_{sl} = 1000 - 138 = 862 \text{ байт} \quad (3.6)$$

Определю среднюю длину кадра по формуле:

$$L_{info} = \frac{(L_{info\,min} + L_{info\,max})}{2} = \frac{862+1362}{2} = 1112 \text{ байт} \quad (3.7)$$

Чтобы продолжить расчёт нужно задать количество передающихся кадров во время дня. В данной ЛВС используется длина кадров 1150 байт, в числе которых информационными являются 1112 байт.

Чтобы узнать количество кадров, передающих полезную информацию, узнаю по формуле:

$$N_{kadra} = \frac{Q}{L_{kadra}} + 1 \quad (3.8)$$

где Q – объем передаваемой информации, байт;

L_{kadra} – длина информационной (полезной) части одного кадра, байт.

Подставлю значения в формулу (3.8):

$$N_{kadrd} = \frac{2.147 \cdot 10^9}{1112} + 1 = 1.931 \cdot 10^6 \text{ кадр/день}$$

Для вычисления пропускной способности линии связи сети я буду использовать математический аппарат теории массового обслуживания. Информационная часть одного кадра и количество передаваемых кадров являются начальными расчетными данными.

Во время использования выше сказанной теории нужно учитывать соотношение между скоростями обслуживания и поступления кадров.

Скорость поступления кадров определяется в зависимости от трафика по формуле:

$$V_{obsh} = \frac{N_{kadra}}{T \cdot 3600}, \quad (3.9)$$

где N_{kadra} – количество передаваемых кадров в течении рабочего дня;

T – продолжительность рабочего дня, часов.

Для определения скорости поступления кадров учитываем следующие обстоятельства:

– сети, между которыми происходит обмен данными, находятся в одном часовом поясе;

– продолжительность рабочего дня составляет 9 часов.

При данных условиях скорость поступления кадров равна согласно формуле (3.9):

$$V_{obsh} = \frac{1.931 \cdot 10^6}{9 \cdot 3600} = 59.6 \text{ кадр/с}$$

Рассчитаю скорость поступления кадров от одного компьютера:

$$V_{post\ 1\ PK} = \frac{V_{obsh}}{N_{komp}}, \quad (3.10)$$

где N_{komp} – количество компьютеров в рассчитываемой сети.

Подставлю численные значения в формулу (3.10):

$$V_{post\ 1\ PK} = \frac{59.6}{50} = 1.192 \text{ кадр/сек}$$

Для расчета скорости обслуживания зададимся некоторой фиксированной скоростью работы магистрального канала. Время обслуживания одного кадра определяется по формуле:

$$t_{obs\ kadra} = \frac{L_{kadra}}{V_{chan}}, \quad (3.11)$$

где L_{kadra} – длина передаваемого кадра, байт;

V_{chan} – скорость обмена информации в магистральном канале, байт/с.

Подставлю значения в формулу (3.11):

$$t_{obs\ kadra} = \frac{1112}{2.621 \cdot 10^5} = 4.242 \cdot 10^{-3} \text{ с}$$

Время передачи кадра отождествляется с временем обслуживания. Скорость обслуживания является обратной величиной ко времени обслуживания и определяется по формуле:

$$V_{obs\ kadra} = \frac{1}{t_{obs\ kadra}} \quad (3.12)$$

Подставлю численные значения в формулу (3.12):

$$V_{obs\ kadra} = \frac{1}{4.242 \cdot 10^5} = 235.741$$

В результате расчета скорости обслуживания возможны две ситуации:

– скорость обслуживания кадров оказывается больше, чем скорость поступления кадров..

– скорость обслуживания кадров оказывается меньше, чем скорость поступления кадров.

Теперь рассчитаем степень использования канала связи в сети. Для этого воспользуемся формулой:

$$P = \frac{V_{obsh}}{V_{obs\ kadra}}, \quad (3.13)$$

где V_{obsh} – скорость поступления кадров, кадр/с;

$V_{obs\ kadra}$. – скорость обслуживания кадров, кадр/с.

Подставлю значения в формулу (3.13):

$$P = \frac{59.6}{235.741} = 0.253$$

Зная степень использования магистрального канала можно рассчитать вероятность отсутствия кадров в магистральном канале по формуле:

$$P_0 = 1 - P, \quad (3.14)$$

где P – степень использования магистрального канала.

Подставлю полученные значения в формулу (3.14):

$$P_0 = 1 - 0.253 = 0.747$$

Магистральный канал является системой с определенным классом обслуживания. Можно сказать, что магистральный канал является системой обслуживания “с ожиданием”. Следовательно для выбранной оптимальной пропускной способности магистрального канала можно определить такие параметры как:

– среднее число кадров, одновременно находящихся в системе;
– среднее число кадров ожидающих обслуживания в очереди;
– среднее время нахождения кадра в системе;
– среднее время ожидания в очереди.

Среднее число кадров, одновременно находящихся в системе определим по формуле:

$$L = \frac{V_{obsh}}{V_{obs\ kadra} - V_{obsh}}, \quad (3.15)$$

где L – среднее число кадров, одновременно находящихся в системе, кадр;

V_{obsh} – средняя скорость поступления кадров, кадр/с;

$V_{obs\ kadra}$ – средняя скорость обслуживания, кадр/с.

Числено эта величина равна согласно формуле (3.15):

$$\mathrm{L} = \frac{59.6}{235.741 - 59.6} = 0.338 \text{ кадра}$$

Для определения числа кадров, ожидающих обслуживания в очереди, воспользуемся формулой:

$$L_q = P \cdot L, \tag{3.16}$$

где L_q – среднее число кадров, ожидающих обслуживания, кадр;

P – степень использования канала.

L – среднее число кадров, одновременно находящихся в системе, кадр.

Числено число кадров, ожидающих обслуживания равно согласно формуле (3.16):

$$L_q = 0.253 \cdot 0.338 = 0.086 \text{ кадра}$$

Среднее время нахождения кадра в системе представляет собой величину, обратную разнице между скоростью обслуживания и скоростью поступления кадров, т.е. определяется формулой:

$$W = \frac{1}{V_{obs\ kadra} - V_{obsh}}, \tag{3.17}$$

где W – среднее время нахождения кадра в системе, с;

$V_{obs\ kadra.}$ – скорость обслуживания, кадр/с;

V_{obsh} – скорость поступления кадров, кадр/с.

Время нахождения кадра в системе вычисляется по формуле (3.17):

$$W = \frac{1}{235.741 - 59.6} = 5.677 \cdot 10^{-3}\ c$$

Важным параметром, характеризующим очередь, является время ожидания в очереди, которое определяется по формуле:

$$W_q = W \cdot P, \tag{3.18}$$

где W_q – время ожидания в очереди, с;

W – время нахождения кадра в системе, с;

P – степень использования канала связи в сети.

Числено значение времени ожидания в очереди согласно формуле (3.18) равно:

$$W_q = 5.677 \cdot 10^{-3} \cdot 0.253 = 1.435 \cdot 10^{-3} \text{ с}$$

Время нахождения кадра в системе включает в себя время ожидания в очереди. Разность времени нахождения и времени ожидания дает время обслуживания одного кадра магистральным каналом или время передачи по магистральному каналу:

$$T_{chan} = W - W_q \tag{3.19}$$

Получу численное значение по формуле (3.19):

$$T_{chan} = 5.677 \cdot 10^{-3} - 1.435 \cdot 10^{-3} = 4.242 \cdot 10^{-3}\ c$$

Расчет времени использования канала связи производится с помощью электронной таблицы Microsoft Excel. В таблицу 3.1 сведены результаты расчета для скорости работы магистрального канала от 2048 Кбит/с до 512 Кбит/с.

Таблица 3.2 – Результаты расчета скорости обслуживания в магистральном канале

V_{chan}	2048	1024	512
$t_{chan\ IPSec}$	7,361	14,732	29,465
t_{chan}	6,818	13,634	27,267

По результатам расчета строим график времени использования канала связи от скорости канала в соответствии с рисунком 3.1.

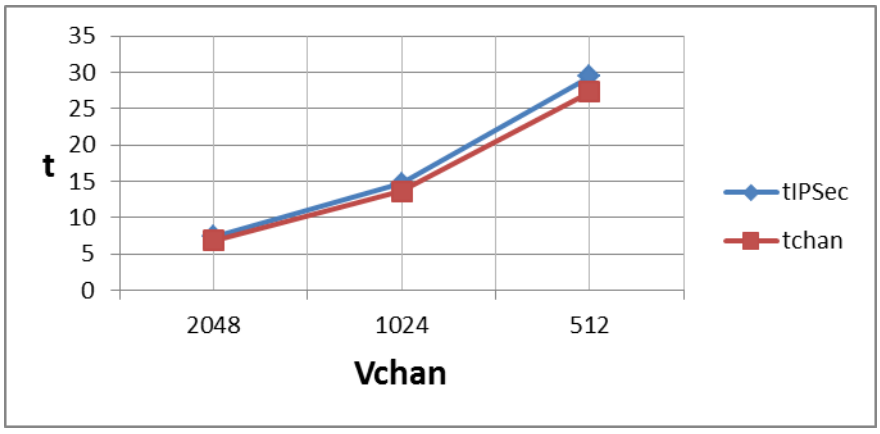

Рисунок 3.1 – График занятости канала связи

Таким образом из проведенного расчета видим, что время обслуживания кадра растет в зависимости от того применяется ли к передаваемой информации шифрование. Так же видно, что при применении протокола IPSec служебная часть кадра увеличивается, а информационная часть кадра уменьшается. За счет этого увеличивается число кадров и увеличивается время передачи информации.

Данный расчет был произведен с использованием программы MathCad.

3.2 Настройка прозрачного режима (Transparent mode) с использованием коммутируемого маршрута Switch Route

Для выполнения необходим брандмауэр DFL–841 и компьютеры в количестве 3 штук.

Цель данной работы заключается в установке и настройке брандмауэра в ЛВС для разделения ресурсов FTP и внутренней сети. Настройка FTP осуществляется на сервере с помощью FTPServ и возможность установить связь с помощью FilшZilla. Стоит учесть то, что во время использования прозрачного режима, брандмауэр работает в режиме свитча уровня 2 и NAT не работает. На рисунке 3.2 показана схема связи оборудования с компьютерами.

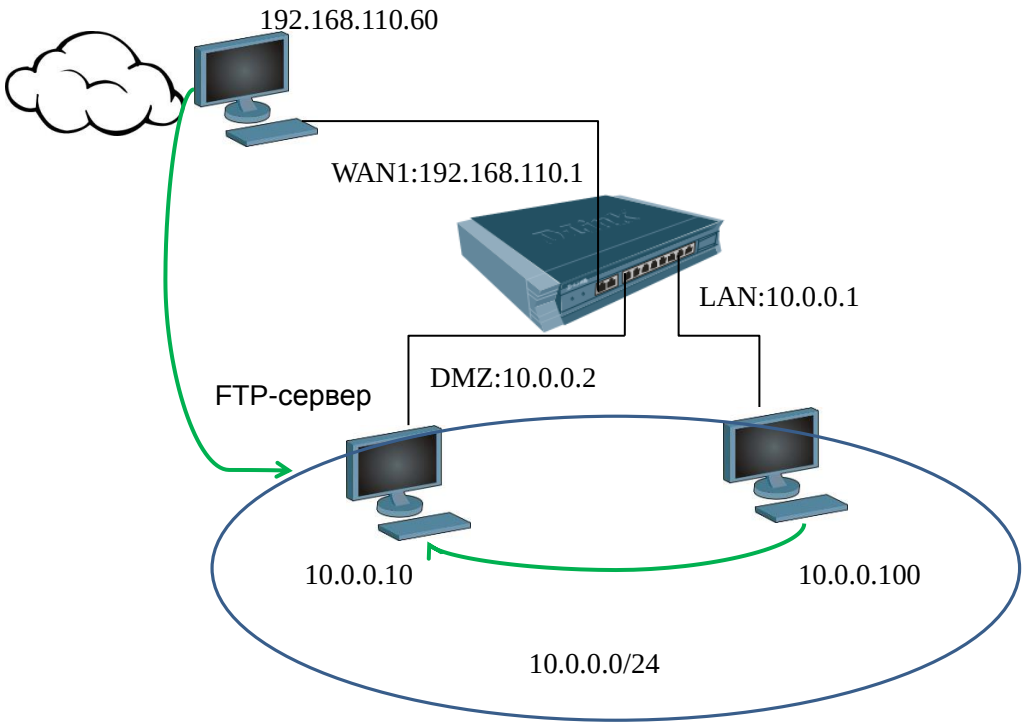

Рисунок 3.2 – Схема связи оборудования с компьютерами

Для настройки брандмауэра проведу следующие шаги:

1) подать питание на брандмауэр;

2) соединить UTP компьютер и брандмауэр;

3) произвести настройку адреса на компьютере, используя «Пуск» → «Настройка» → «Сетевые подключения» → «Подключение по локальной сети» → «Свойства» → «Протокол Интернета TCP/IP» → «Свойства»; Затем

прописать маску 255.255.255.0 и адрес «192.168.1.10». На рисунке 3.3 показана настройка адреса IP;

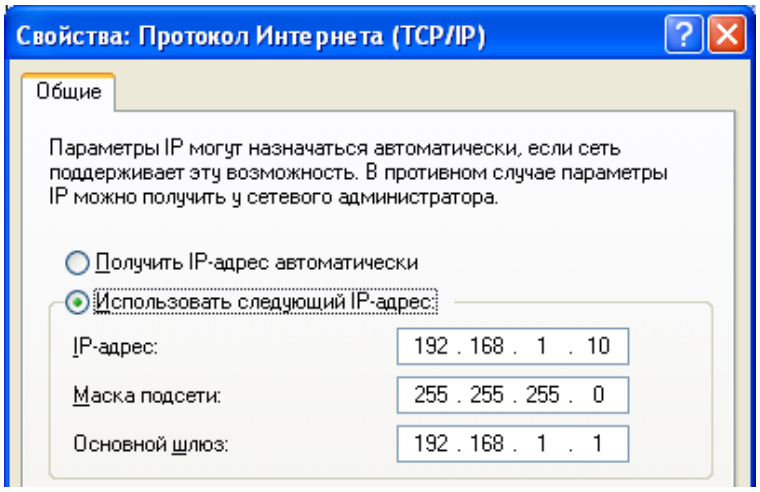

Рисунок 3.3 – Настройка адреса IP

4) с помощью web произвести настройку брандмауэра, используя в адресной строке браузера адрес «192.168.1.1» и стандартные логин с паролем «admin»/«admin»;

5) нажав «+» рядом с вкладкой «interfaces» и выберу «Ethernet» – «wan1». Уберу галку с поля «Enable DHCP Client» и нажму «ОК». На рисунке 3.4 показана настройка «wan1»;

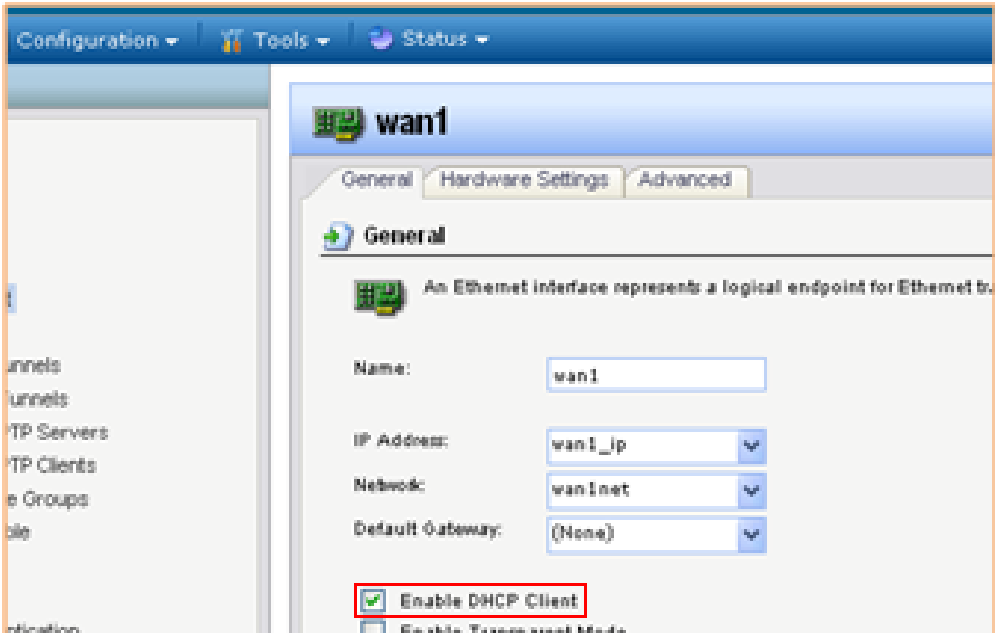

Рисунок 3.4 – Настройка «wan1»

6) затем в вкладке «InterfacesAdresses» произведу настройку согласно таблице 3.3, в которой указаны соответствия адреса и интерфейса;

Таблица 3.3 – Соответствие адреса и интерфейса

Интерфейс	Адрес
Wan1_ip	192.168.110.1
Wan1net	192.168.110.0/24
Wan1_gw	192.168.145.1
Lan_ip	192.168.1.1
Lannet	192.168.1.0/24
Dmznet	192.168.1.0/24
Dmz_ip	192.168.1.254

7) теперь необходимо перейти «Interfaces» → «Ethernet» → «lan». И открыть вкладку «General» и проверить отключен ли «Transparent mode», а в «Advanced» необходимо снять галку с «Add route a interface networks». На рисунке 3.5 показана настройка параметров.

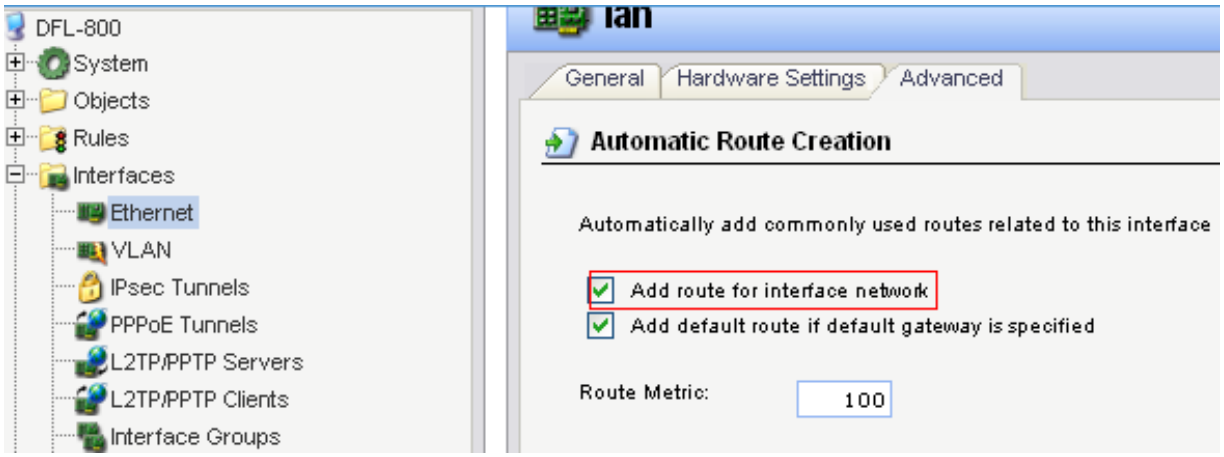

Рисунок 3.5 – Настройка параметров

8) теперь необходимо произвести выше написанное и для вкладки, расположеной «Interfaces» → «Ethernet» → «dmz»;

9) теперь создам группу интерфейсов, перейдя «Interfaces» → «Interfaces Group» и нажму «Ad»d → «Interfaces Group». Затем в поле «Имя» напишу имя группы и выберу lan и dmz. Функцию «Transport/Security» нужно отключить. На рисунках 3.6 и 3.7 показано создание группы интерфейсов.

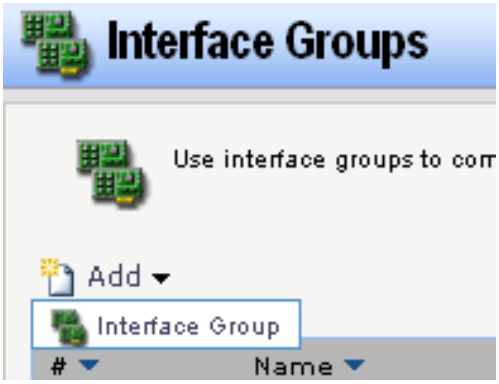

Рисунок 3.6 – Создание «iterfaces groups»

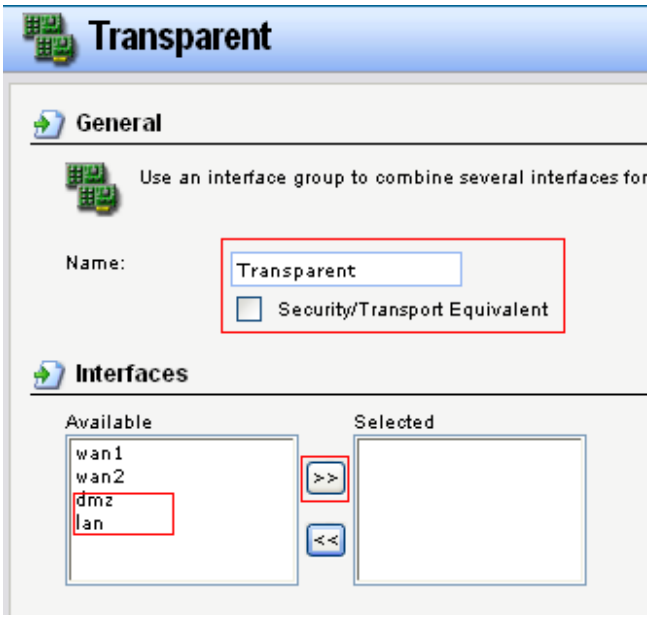

Рисунок 3.7 – Перевод lan, dmz в «selected»

После чего нажму «ОК»;

10) затем необходимо создать «Switchs Route». Открою вкладку «Routing» и выберу «Table Routing» и нажму «Add». Теперь заполню поля «Switched Interfaces» – «TransparGroup», «Network» – «dmz_net», «Metric» – 0 и в последствии нажму «ОК». На рсиунках 3.8 и 3.9 показана настройка «Switchs Route».

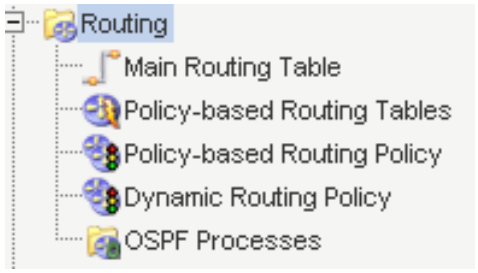

Рисунок 3.8 – Выбираем маршрутизацию

Зайду в «Main Table Routing», нажиму «Add» и выберу «switchs route»;

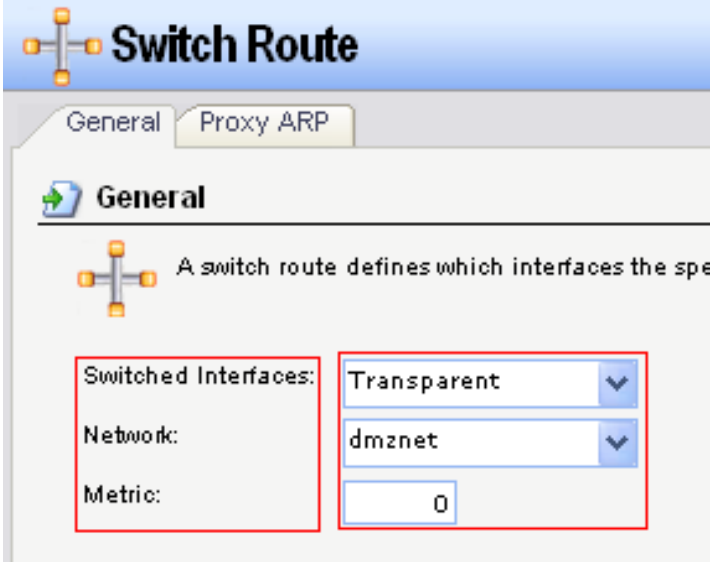

Рисунок 3.9 – Настройка маршрутизации

11) необходимо создать правила для FTP. Раскрою вкладку «Rules» и выберу «Rules IP», который показан на рисунке 3.10

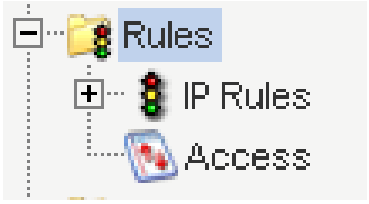

Рисунок 3.10 – Ветка «Rules»

После чего нажму «Add» и укажу «Folder Ip Rule», где в поле «Name» введу «Trasnaparet» и нажму «ОК». На рисунке 3.12 показано создание папки.

Рисунок 3.12 – Создание папки

Первое правило должно разрешать FTP из местной сети. Заполню поля как показано на рисунке 3.13.

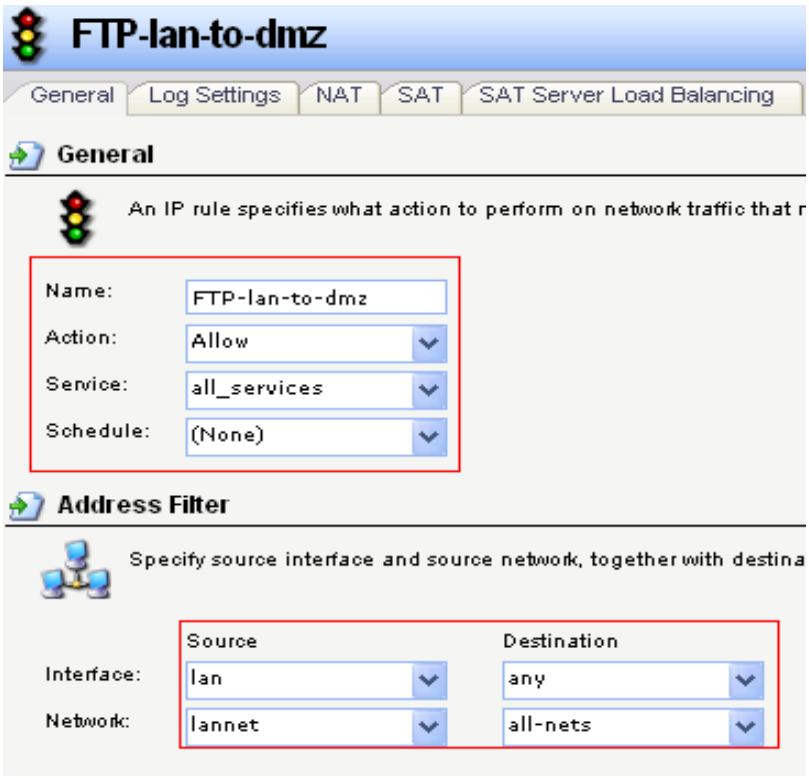

Рисунок 3.13 – Создание правила

В «General» поля «Name» – «FTPlandmz», «Action» – «Allow», «Service» – «all_services».

В «Address Filter» поля «Sources Interface» – «lan», «Sources Network» – «lannet», «Destinations Interfaces» – «any», «Destinations Networks» – «all–nets». После чего нажму «ОК».

Правило №2 разрешает доступ из wan1 к FTP . Заполню поля, показанные на рисунке 3.14.

В «General» заполню поля «Name» – «FTP–wan1–dmz», «Action» – «SAT», «Service» – «ftppassthrough». В «Address Filter» поля «Source Interfaces» – «wan1», «Source Networks» – «all–net», «Destinations Interfaces» – «core», «Destinations Networks» – «wan1_ip».

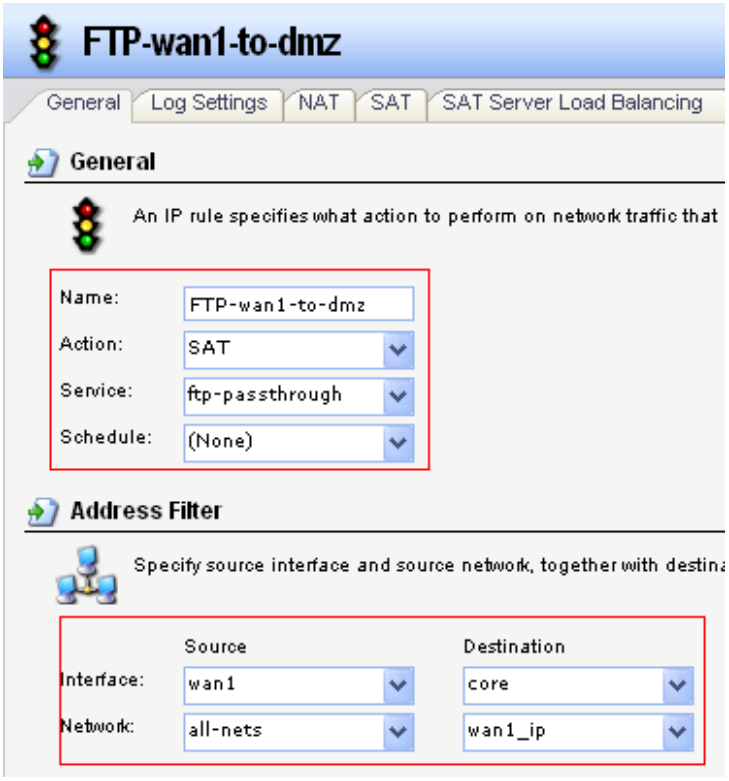

Рисунок 3.14 – Настройка ftp правил

Перейдя в «SAT», выберу «IP Destinations», а в поле «Address IP» выберу «server» и нажму «ОК». На рисунке 3.15 показана настройка «SAT».

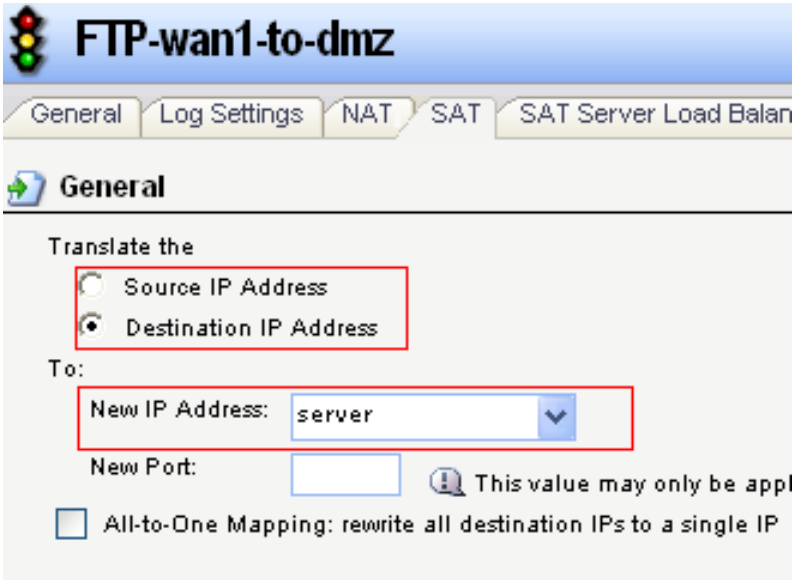

Рисунок 3.15 – Настройка в «SAT»

Для третьего правила заполню младующие поля. В «General» заполню поля «Name» – «FTP–wan1dmz», «Action» – «Allow», «Service» – «all–service». В «Address Filter» заполню «Source Interfaces» – «wan», «Source Networks» – «wan1net», «Destinations Interfaces» – «any», «Destinations

Networks» – «all–nets» и нажму «ОК». Создание правила показано на рисунке 3.16.

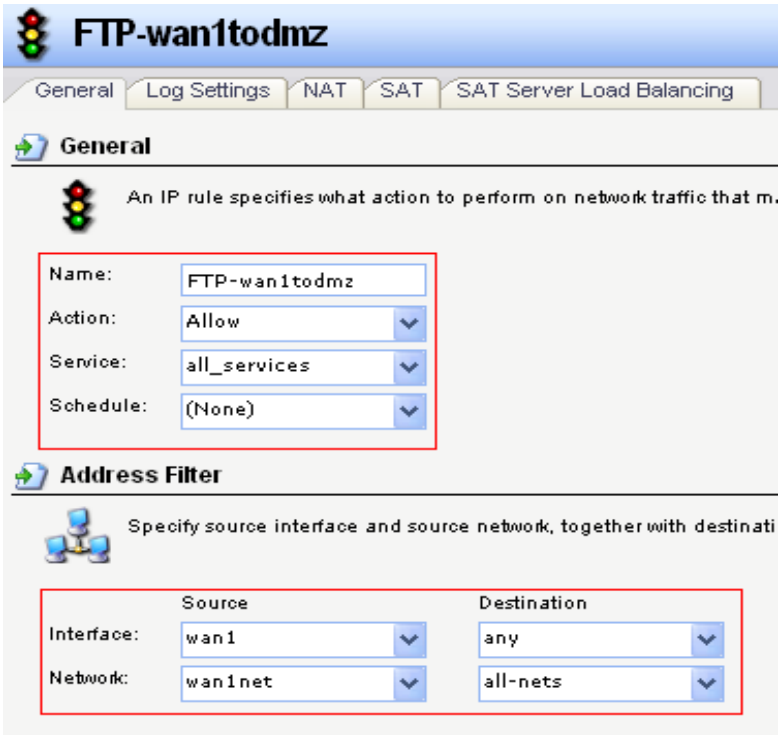

Рисунок 3.16 – Правило три

На рисунке 3.17 показано правило четыре.

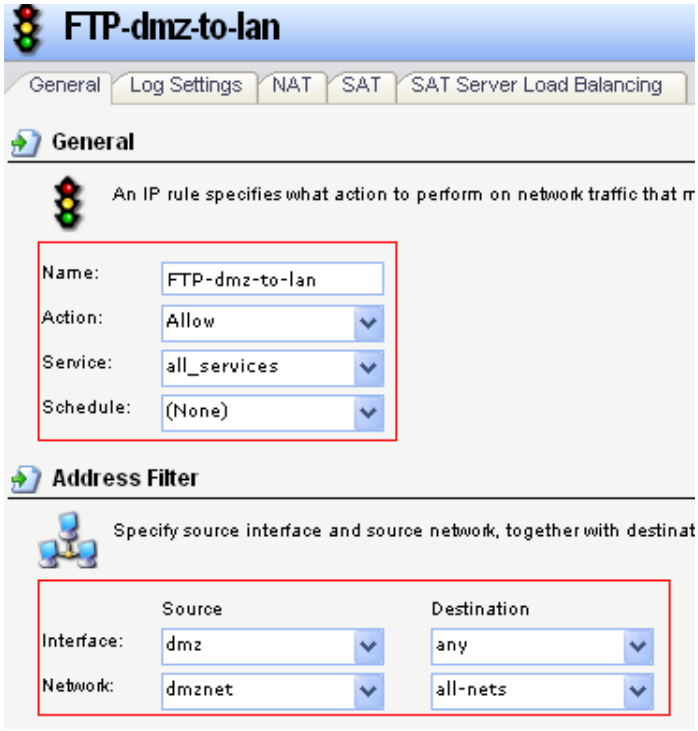

Рисунок 3.17 – Настройка правила четыре

Для четвертого правила заполню младующие поля. В «General» заполню поля «Name» – « FTP–dmz–lan », «Action» – «Allow», «Service» – «all–service». В «Address Filter» заполню «Source Interfaces» – «dmz», «Source Networks» – «dmznet», «Destinations Interfaces» – «any», «Destinations Networks» – «all–nets» и нажму «ОК». После всего применю настройки, нажав «Save and Activates» и нажму «ОК». Теперь необходимо проверить доступ к FTP с ПК, которые находятся в ЛВС, и одного ПК, который находится за брандмауэром.

Для этого воспользуюсь FTPServ. На рисунке 3.18 показана настройка FTPServ.

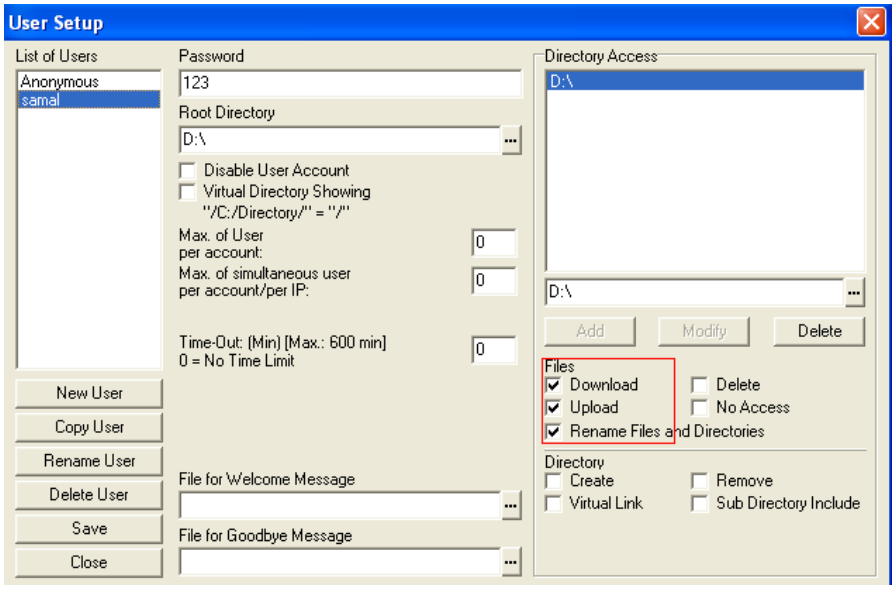

Рисунок 3.18 – Настройки программы FTPserv

На рисунке 3.19 показан пинг внутренней сети.

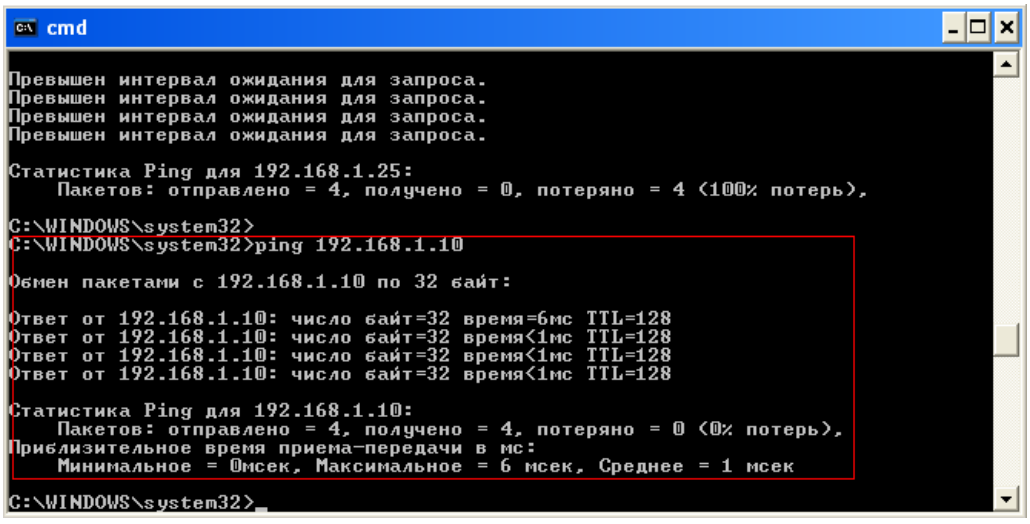

Рисунок 3.19 – Пинг тест

Подключусь с ПК, располагающегося в местной сети. Зайду в программу FiliZilla, пропишу хост, пароль, логин. На рисунке 3.20 показано окно FiliZilla.

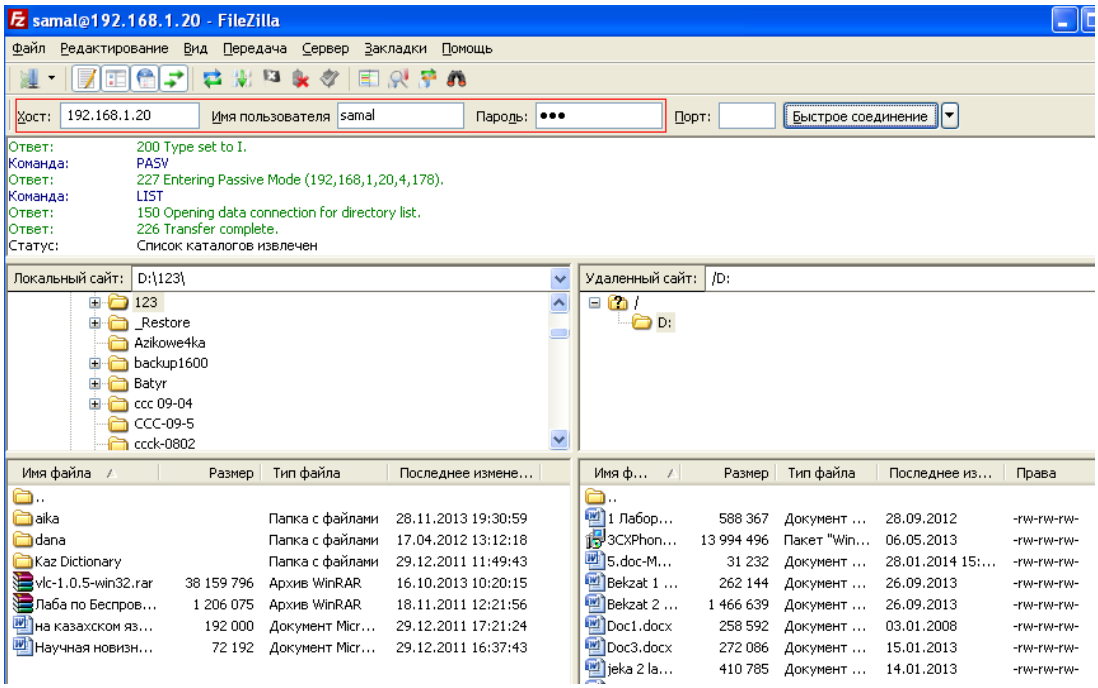

Рисунок 3.20 – Окно FiliZilla

На рисунке 3.21 показан тест пинга.

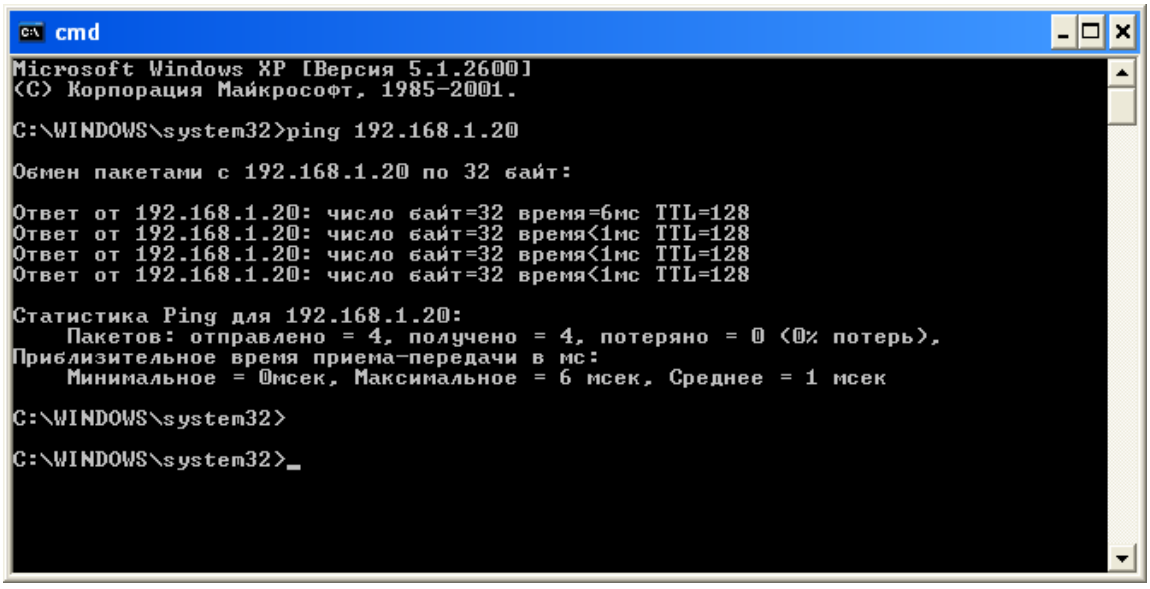

Рисунок 3.21 – Пинг тест

Подключусь к DMZ через внешний компьютер, расположенный в wan1. И также зайду в FiliZilla и пропишу хоста, пароль, логин. На рисунке 3.22 показано окно FiliZilla.

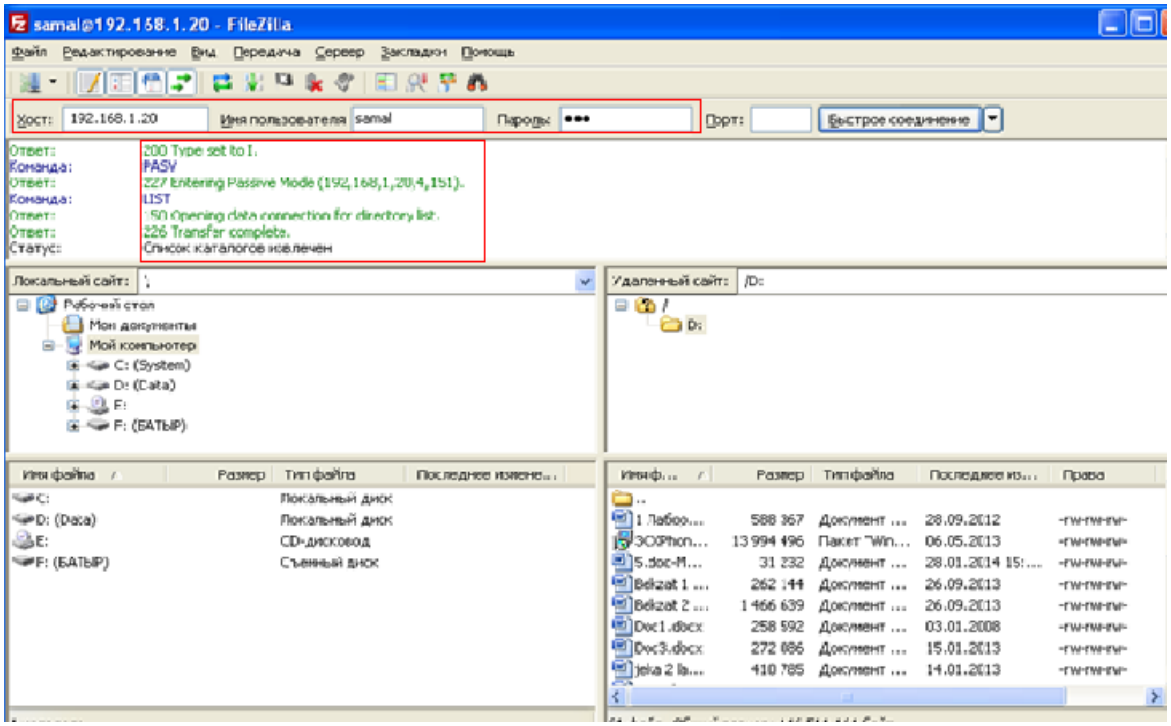

Рисунок 3.22 – Подключение к серверу

На рисунке 3.23 показан тест пинга.

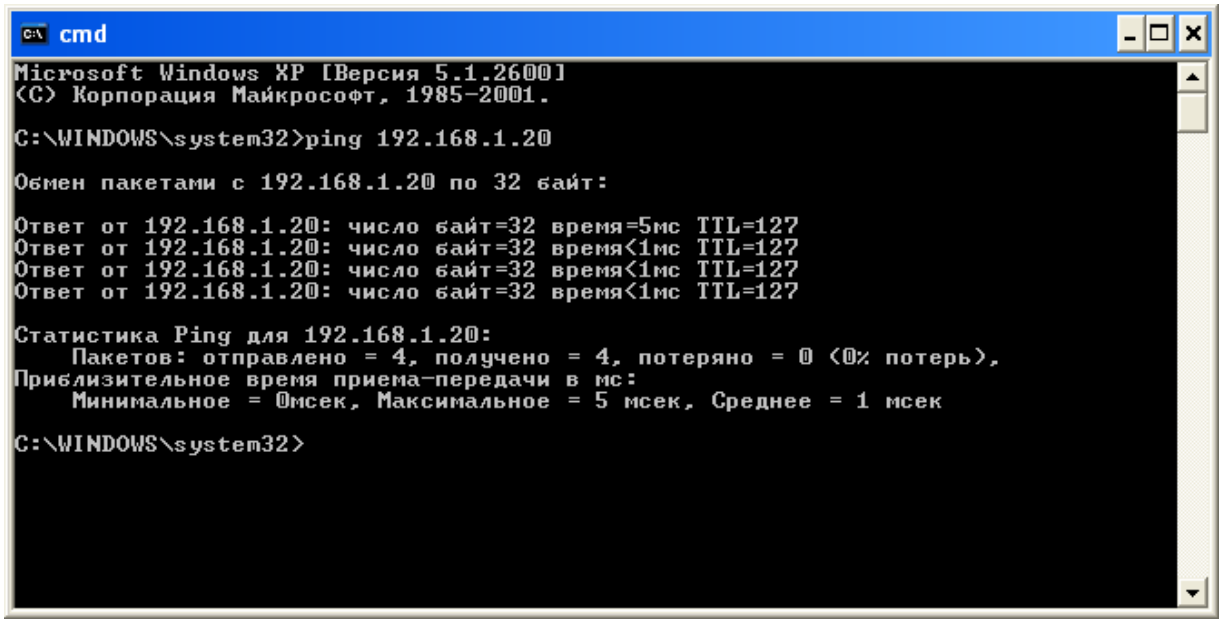

Рисунок 3.23 – Тест пинга

В результате тестов видно, что соединение осуществляется, следовательно всё работает. На основе этого понятно, что связь между сетями DMZ есть.

3.3 Перенаправление портов

Для данной цели понадобится брандмауэр и три компьютера. Целью является выполнение функций перенаправления портов из внешней сети в местную сеть. Схема подключения показана на рисунке 3.24.

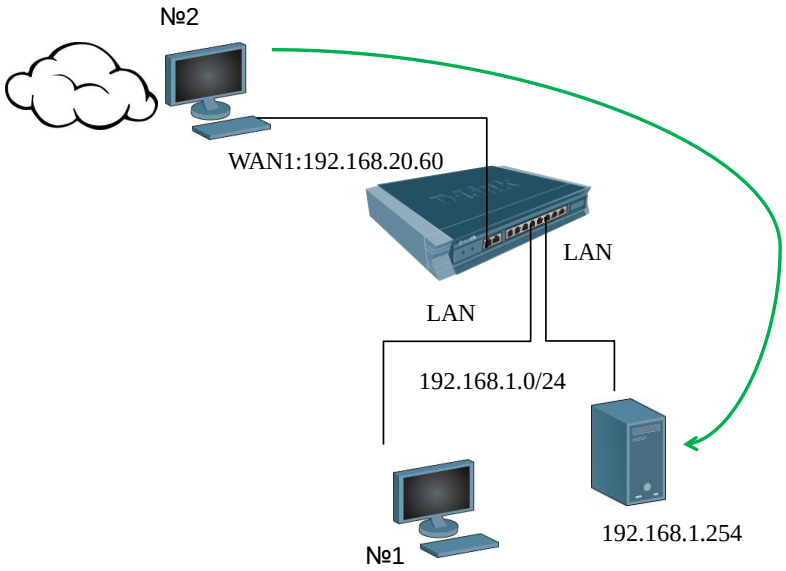

Рисунок 3.24 – Схема подключения брандмауэра

Для этого необходимо настроить IPSec по следующим шагам:

1) подать питание на брандмауэр;

2) соединить UTP компьютер и брандмауэр;

3) произвести настройку адреса на компьютере, используя «Пуск» → «Настройка» → «Сетевые подключения» → «Подключение по локальной сети» → «Свойства» → «Протокол Интернета TCP/IP» → «Свойства»; Затем прописать маску 255.255.255.0 и адрес «192.168.1.xxx». На рисунке 3.3 показана настройка адреса IP;

4) с помощью web произвести настройку брандмауэра, используя в адресной строке браузера адрес «192.168.1.1» и стандартные логин с паролем «admin»/«admin»;

5) после авторизации необходимо указать адреса для двух сетей. Для этого необходимо открыть вкладку «Interfaces» и выбрать «Ethernet», «lan», «wan1» и отключить «Enable Client DHCP» и нажать «ОК». Данная настройка показана на рисунке 3.25.

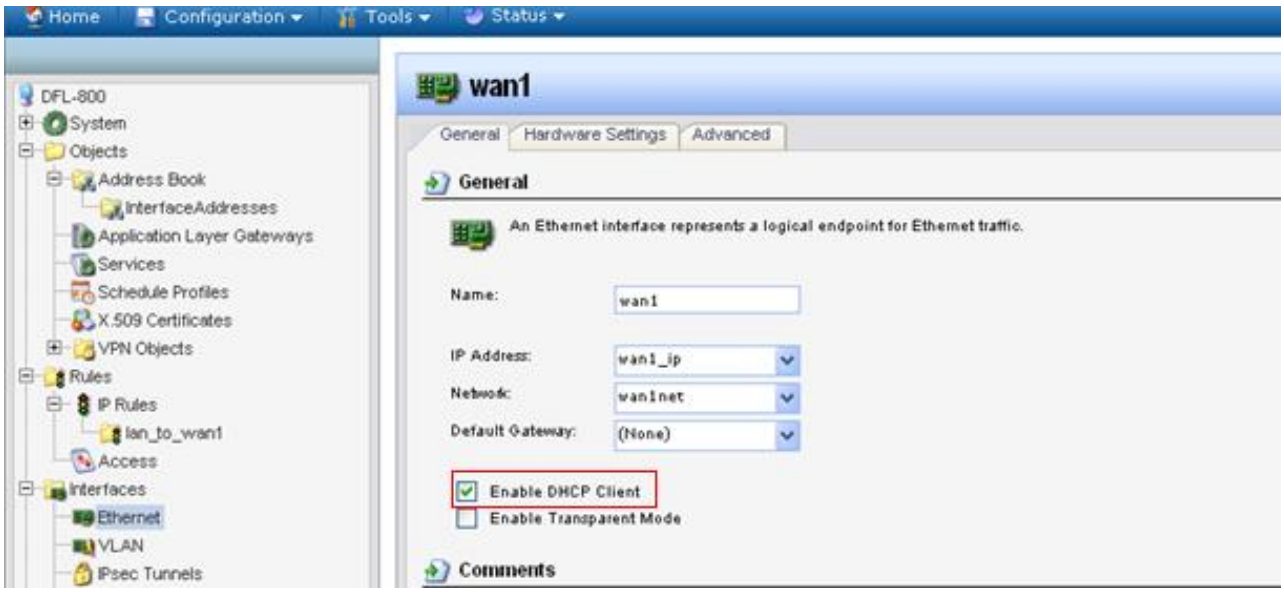

Рисунок 3.25 – Настройка wan

Теперь необходимо развернуть «Objects» и выбрать «Interfaces Addresses». После чего задать адрес для WAN 192.168.20.60, а «wannet» ввести 192.168.20.0/24. Аналогично проведу настройку местной мети, но с параметрами 192.168.1.1 и 192.168.1.0/24. На рисунке 3.26 показана настройка адресов;

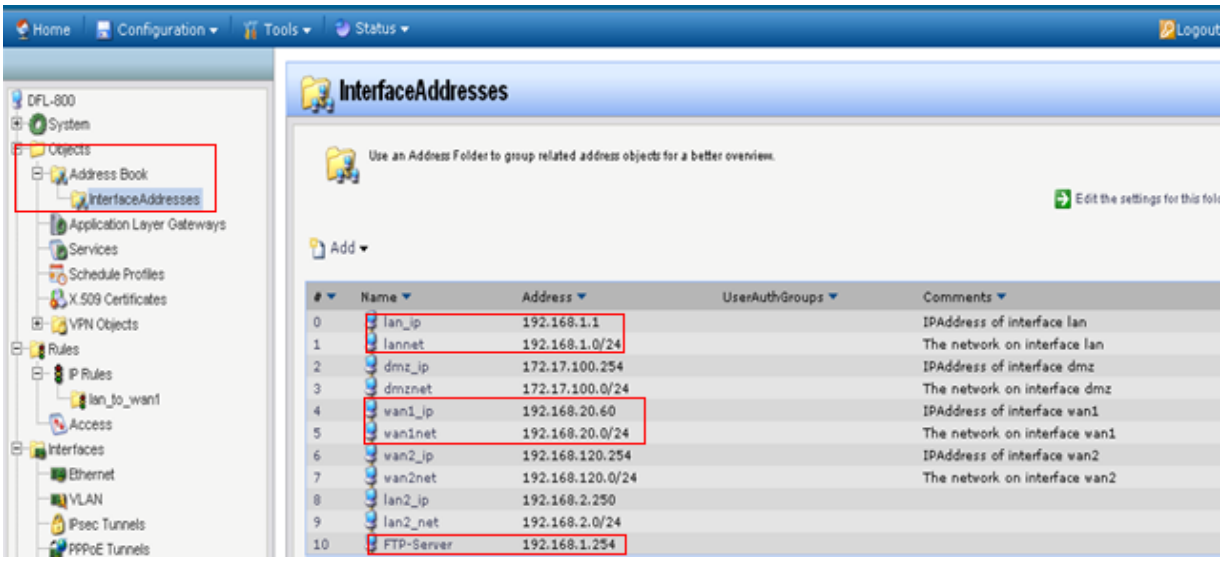

Рисунок 3.26 – Настройка адресов

6) затем добавлю объект в разделе «Objects» выберу «Book Address», нажму «Add» и выберу адрес. Добавлю объект с именем server–FTP с адресом 192.168.1.254 и нажму «ОК».

7) создам правила доступа. Для первого правила заполню следующие поля. В «General» заполню поля «Name» – «ftpserver», «Action» – «SAT», «Service» – «ftpinbound». В «Address Filter» заполню «Source» – « »,

«Networks» – «all–nets», «Interfaces» – «any». В «Destinations» заполню поля « Interface » – «core», «network» – «wan_ip». Во вкладке «SAR» выделю «IP Destinations» и заполню поле «New Address IP» – «Server FTP» и нажму «ОК». На рисунке 3.27 показано правило один.

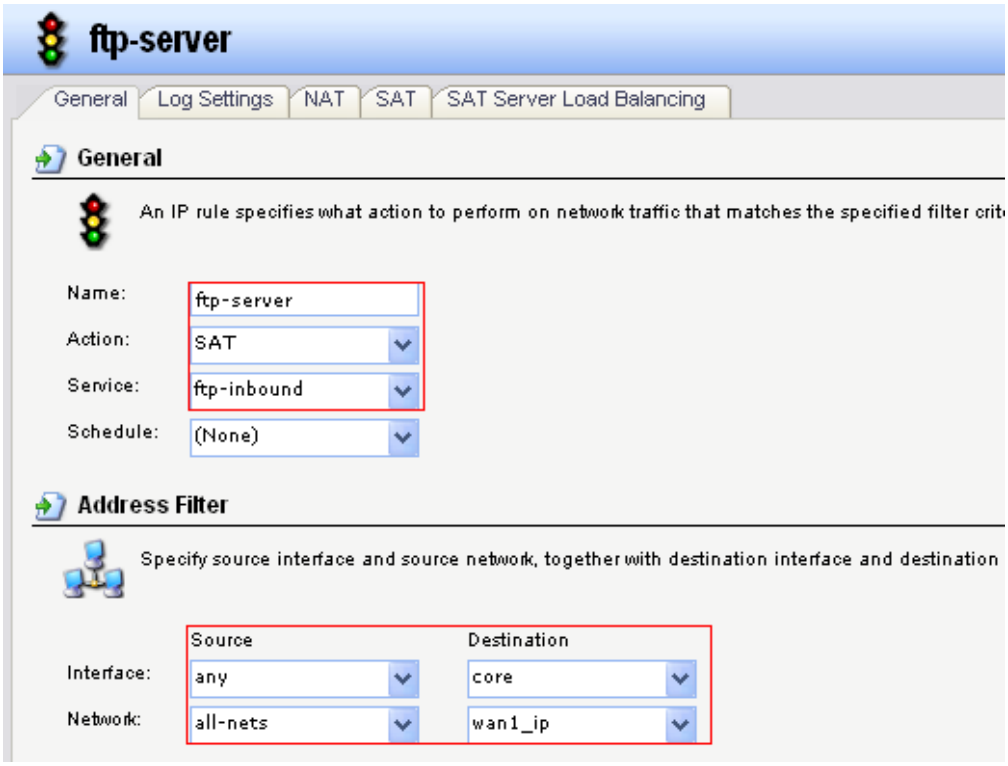

Рисунок 3.27 – Правило один

На рисунке 3.28 показана настройка SAT.

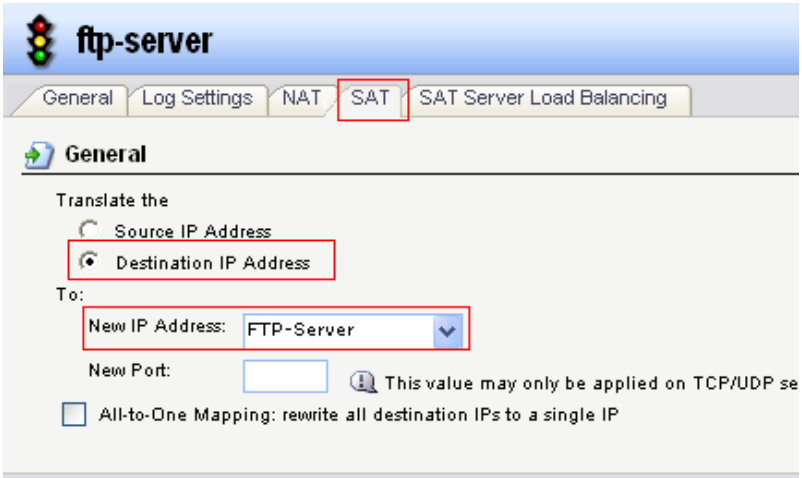

Рисунок 3.28 – Настройка SAT

Для второго правила заполню следующие поля. В «General» заполню поля «Name» – «allowserver », «Action» – «Allow», «Service» – «ftpinbound».

В «Address Filter» заполню «Source» – « », «Networks» – «all–nets», «Interfaces» – «any». В «Destinations» заполню поля «Interface» – «core», «network» – «wan_ip» и нажму «ОК». На рисунке 3.29 показано правило два.

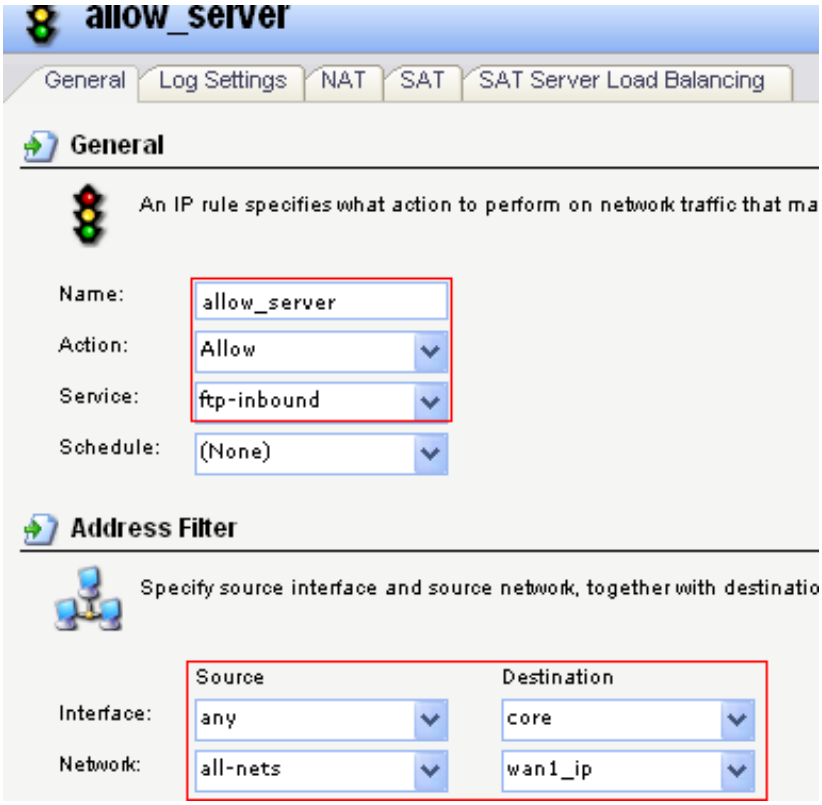

Рисунок 3.29 – Правило для allow server

Теперь необходимо сохранить настройки. Перейду в меню «Configuration» и выберу «Activate and Save» и затем нажму «ОК»;

8) после необходимо настроить ПК. Соединю для этого ПК и брандмауэр;

9) произведу настройку интерфейса. «Пуск» → «Настройка» → «Сетевые подключения» → «Подключение по локальной сети» → «Свойства» → «Протокол Интернета TCP/IP» → «Свойства»; Затем прописать маску 255.255.255.0 и адрес «192.168.20.xxx»;

10) таким же образом настрою сервер, только адрес будет 192.168.1.254 и маска 24;

11) после настройки сети настрою сам сервер с помощью «FTPServ». Открою программу и создам сервер в настройках. После чего зайду с компьютера с адресом 192.168.1.10 с помощью FiliZilla при этом укажу хост, пароль и логин. После чего произведу соединение. А до этого момента создам ещё одно правило в брандмауэре. В «General» заполню поля «Name» – «ping_w_wan1», «Action» – «Allow», «Service» – «pingbound». В «Address Filter» заполню «Source» – « », «Networks» – «all–nets», «Interfaces» – «wan1». В «Destinations» заполню поля «Interface» – «core», «network» – «wan_ip» и нажму «ОК». На рисунке 3.30 показано правило для пинга.

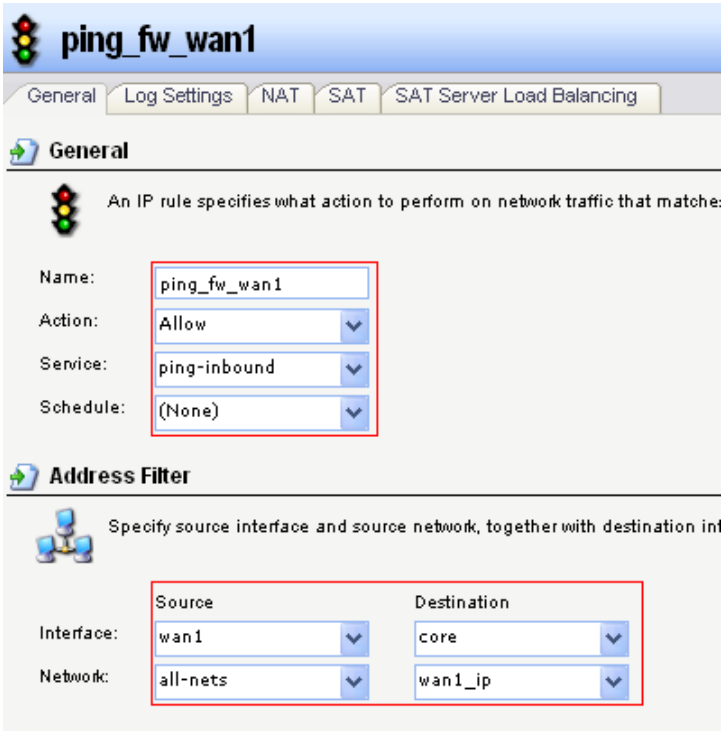

Рисунок 3.30 – Правило для пинга

Теперь применю настройки, нажав «Activate and Save» и нажму «ОК». После чего проведу пинг, который показан на рисунке 3.31.

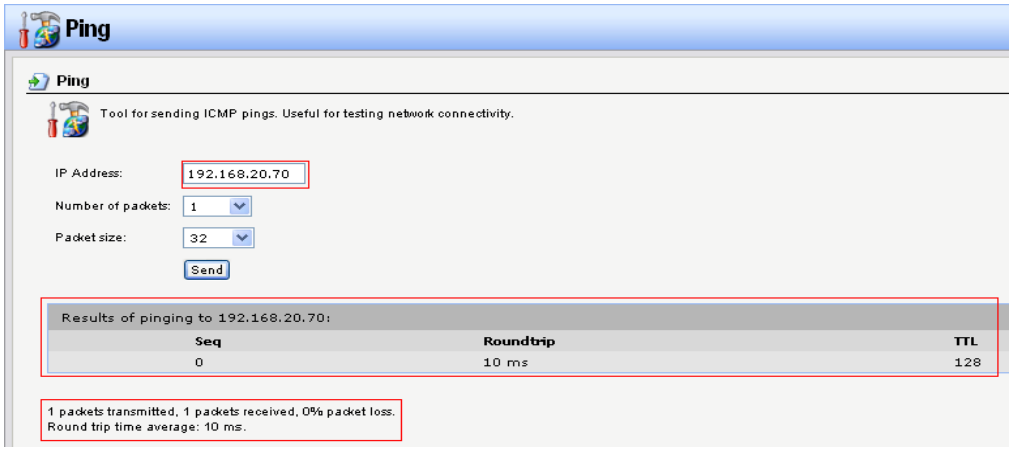

Рисунок 3.31 –Тест пинга

После проверки пинга можно подключаться к серверу. Подключение к серверу показано на рисунке 3.32.

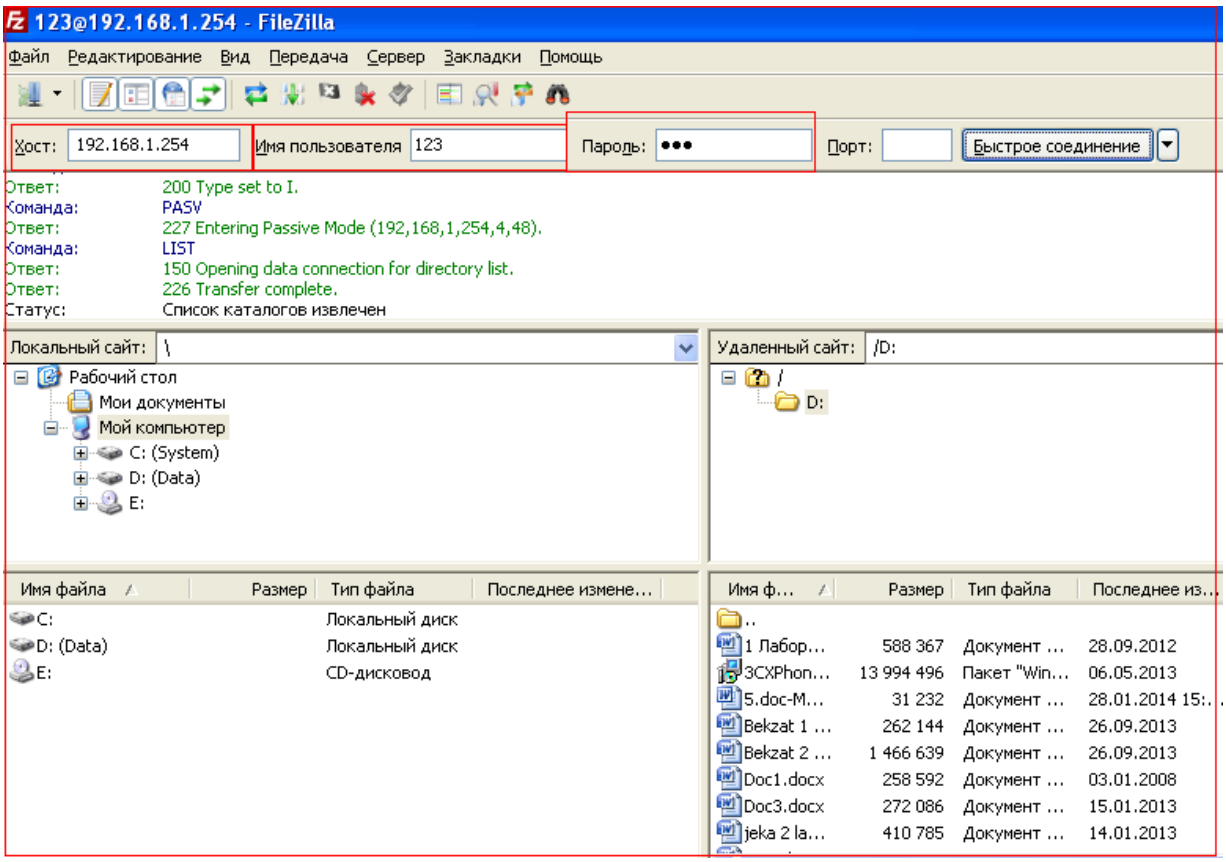

Рисунок 3.35 – Подключение к серверу

3.4 Демонстрация работы DMZ

Для выполнения необходим брандмауэр DFL–841 и компьютеры в количестве 3 штук.

Цель данной работы заключается в настройке отдельной ЛВС, использующей порт DMZ для возможности подключения к серверу FTP всех пользователей. Настройка сервера будет осуществляться с помощью пргаммы Golden Server FTP v4.69.

На рисунке 3.36 показана схема связи оборудования с компьютерами.

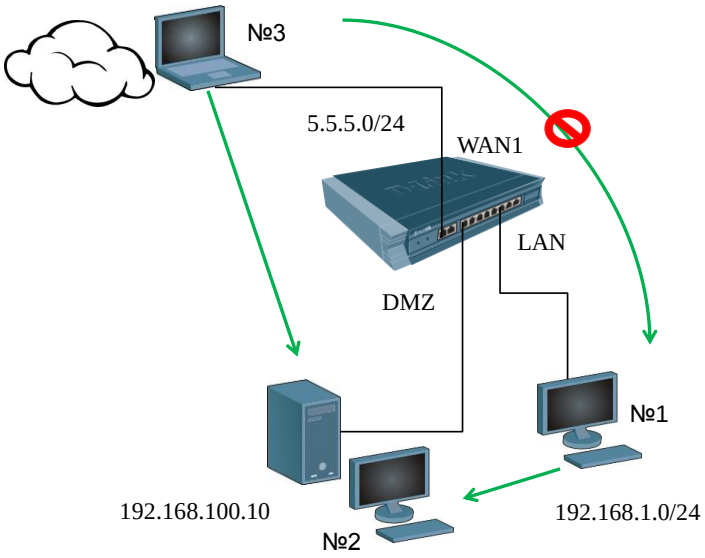

Рисунок 3.36 – Схема связи оборудования с компьютерами

Для настройки брандмауэра проведу следующие шаги:

1) подать питание на брандмауэр;

2) соединить UTP компьютер и брандмауэр;

3) произвести настройку адреса на компьютере, используя «Пуск» → «Настройка» → «Сетевые подключения» → «Подключение по локальной сети» → «Свойства» → «Протокол Интернета TCP/IP» → «Свойства»; Затем прописать маску 255.255.255.0 и адрес «192.168.1.xxx»;

4) с помощью web произвести настройку брандмауэра, используя в адресной строке браузера адрес «192.168.1.1» и стандартные логин с паролем «admin»/«admin»;

5) теперь проведу настройку. Необходимо указать адреса WAN, LAN в DMZ. Для этого необходимо развернуть вкладку «Interfaces» и выбрать «Ethernet», wan и отключить «Enable Client DHCP» и нажать «ОК»;

6) далее разверну вкладку «InterfacAddresses», выберу «wanip» и введу fадрес 5.5.5.1, выберу «wannet» и введу 5.5.5.0/24. Аналогичным образом задам значения «LAN» с адресами 192.168.1/24 и 192.168.1.1, а также «DMZ» с адресами 192.168.100/24 и 192.168.100.1. На рисунке 3.34 показана настройка «InterfacAddresses»;

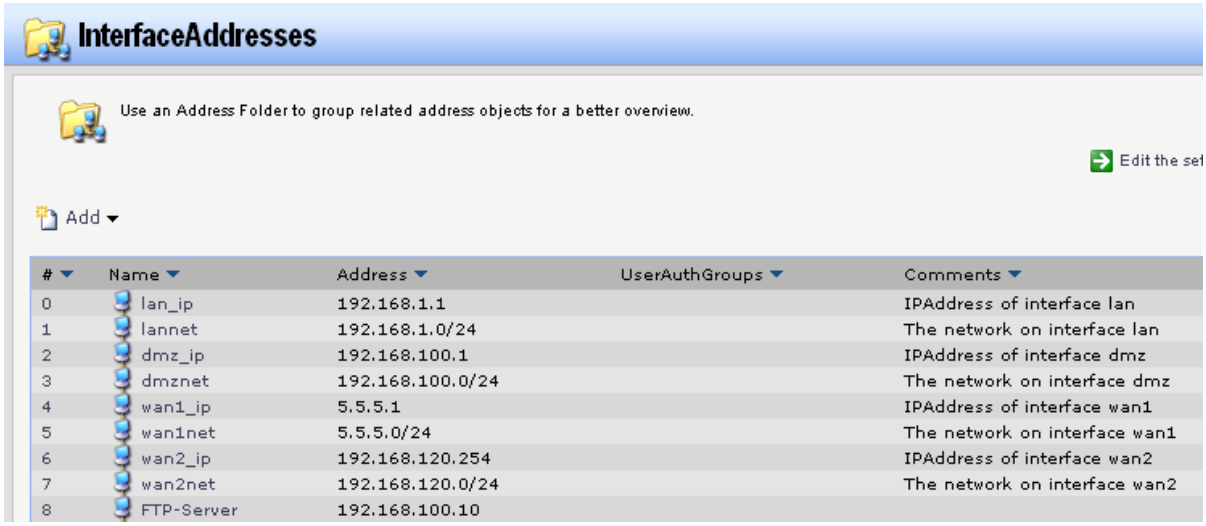

Рисунок 3.34 – Настроенные IP–адресса

7) теперь необходимо произвести создание правил для подключения в «DMZ» из «WAN» и в «DMZ» из «LAN». Для этого разверну вкладку «Rules», выберу «Rules IP» и нажму «Add». Создам первое правило. В «General» заполню поля «Name» – «wantodmz», «Action» – «Allow», «Service» – «ftppassthrough». В «Address Filter» заполню «Source» – « », «Networks» – «wannet», «Interfaces» – «wan1». В «Destinations» заполню поля «Interface» – «dmz», «network» – «Server–FTP» и нажму «ОК». На рисунке 3.35 показано первое правило.

Рисунок 3.35 – Правило первое

Создам второе правило. В «General» заполню поля «Name» – «dmztowan», «Action» – «Allow», «Service» – «ftppassthrough». В «Address Filter» заполню «Source» – « », «Networks» – «server–ftp», «Interfaces» – «dmz». В «Destinations» заполню поля «Interface» – «wan1», «network» – «wannet» и нажму «ОК». На рисунке 3.36 показано второе правило.

Рисунок 3.36 – Правило второе

Создам третье правило. В «General» заполню поля «Name» – «lantodmz», «Action» – «Allow», «Service» – «ftpinbound». В «Address Filter» заполню «Source» – « », «Networks» – «lannet», «Interfaces» – «lan». В «Destinations» заполню поля «Interface» – «dmz», «network» – «dmznet» и нажму «ОК». На рисунке 3.37 показано третье правило.

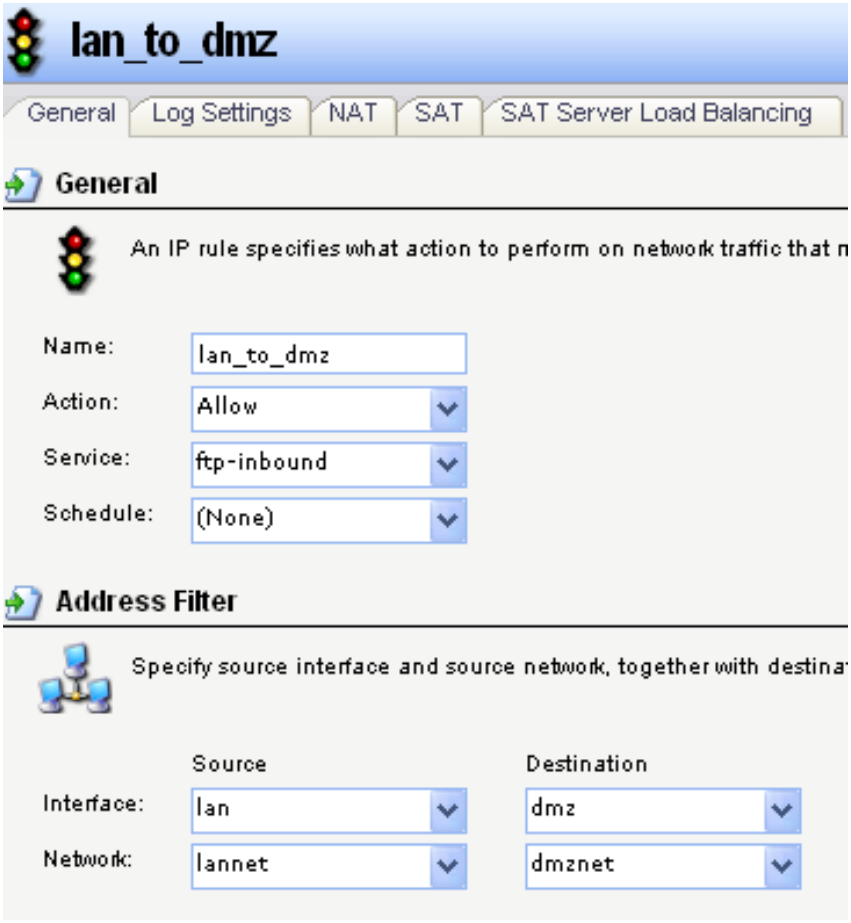

Рисунок 3.37 – Правило третье

Создам четвертое правило. В «General» заполню поля «Name» – «dmztolan», «Action» – «Allow», «Service» – «ftppassthrough». В «Address Filter» заполню «Source» – « », «Networks» – «dmznet», «Interfaces» – «dmz». В «Destinations» заполню поля «Interface» – «lan», «network» – «lannet» и нажму «ОК». На рисунке 3.38 показано третье правило;

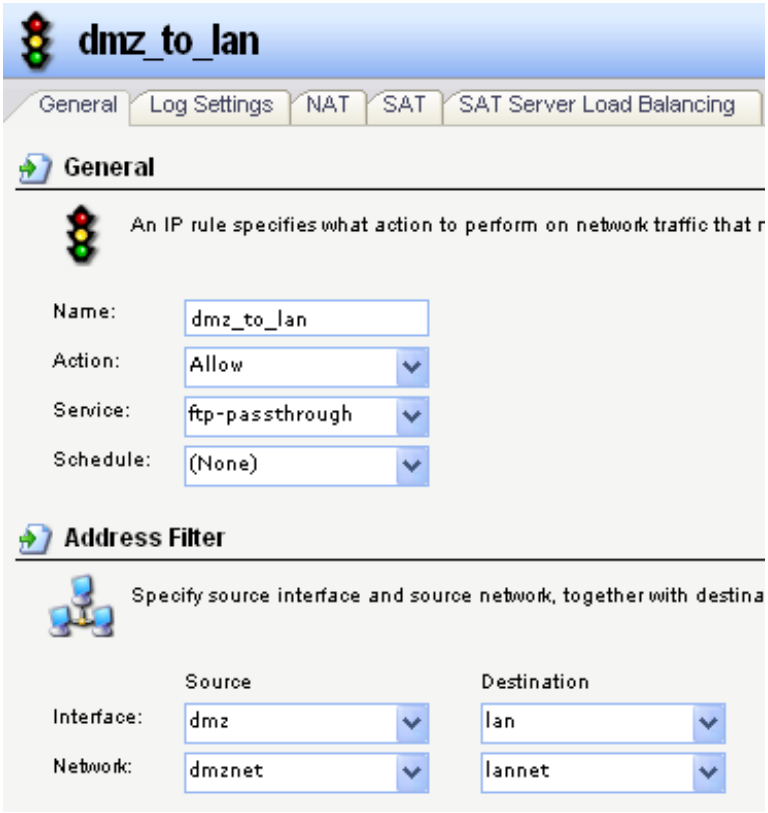

Рисунок 3.38 – Правило четыре

8) теперь необходимо добавить маршрут. Для этого открываю вкладку «Main Table Routing» и нажимаю «Add». На рисунке 3.39 показана настройка маршрутизации wan.

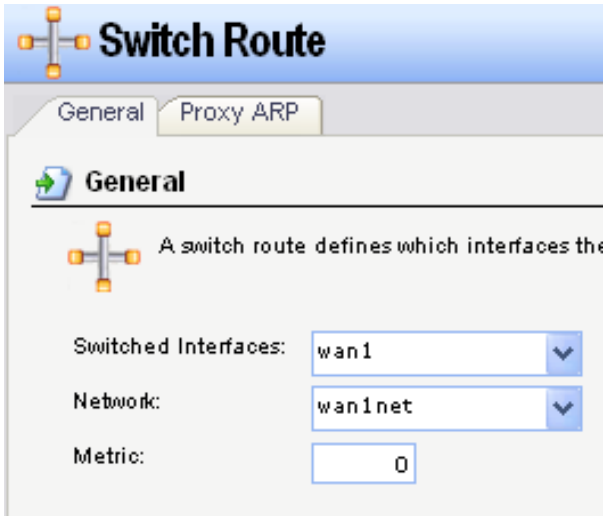

Рисунок 3.39 – Настройка маршрутизации wan

На рисунке 3.40 показана настройка маршрутизации dmz.

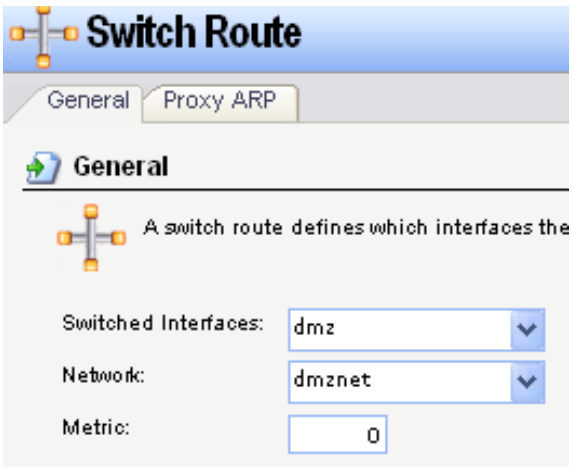

Рисунок 3.40 – Настройка маршрутизации dmz

На рисунке 3.41 показана настройка маршрутизации lan.

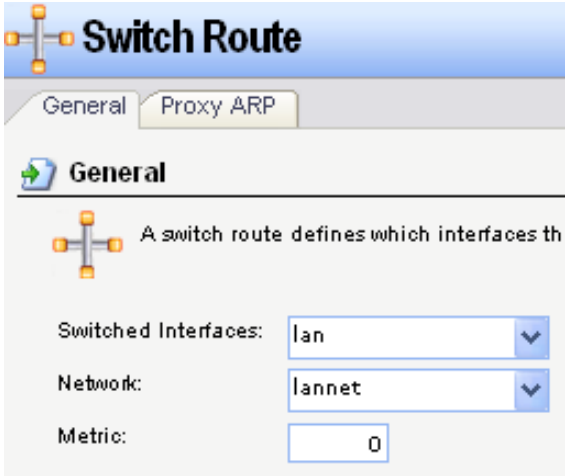

Рисунок 3.41 – Настройка маршрутизации lan

Итоговая таблица маршрутов выглядит следующим образом, как показано на рисунке 3.42;

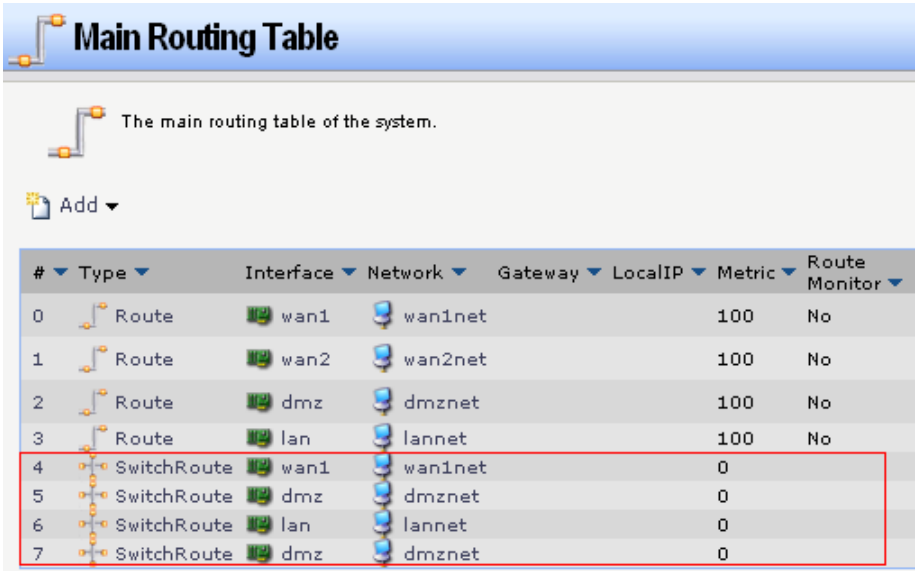

Рисунок 3.42 – Таблица маршрутов

9) после всего произведу сохранение параметров, нажав «Activate and Save».

Теперь необходимо настроить компьютеры. Настрою второй компьютер:

1) соединю UTP брандмауэр (порт DMZ) и компьютер;

2) произведу настройку адреса компьютера, используя «Пуск» → «Настройка» → «Сетевые подключения» → «Подключение по локальной сети» → «Свойства» → «Протокол Интернета TCP/IP» → «Свойства»; Затем прописать маску 255.255.255.0 и адрес «192.168.100.1». На рисунке 3.43 показана настройка адреса компьютера.

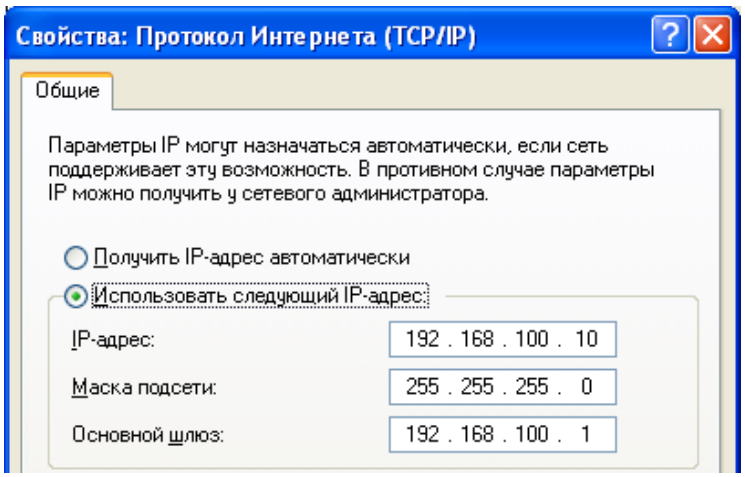

Рисунок 3.43 – Настройка адреса компьютера

Настройка третьего компьютера:

1) соединю UTP брандмауэр (порт WAN) и компьютер;

2) произведу настройку адреса компьютера, используя «Пуск» → «Настройка» → «Сетевые подключения» → «Подключение по локальной сети» → «Свойства» → «Протокол Интернета TCP/IP» → «Свойства»; Затем прописать маску 255.255.255.0 и адрес «5.5.5.xxx». На рисунке 3.43 показана настройка адреса компьютера. На рисунке 3.44 показана настройка адреса компьютера.

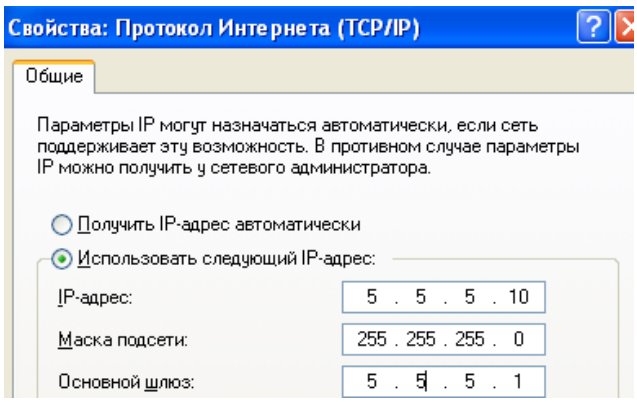

Рисунок 3.44 – Настройка адреса компьютера

Теперь проверю соединение с FTP с двумя компьютерами. Чтобы проверить это открою браузер и в адресной строке напишу ftp://192.168.100.10. Если ответа нет, то сервер не доступен. Но он доступен, поэтому настрою клиент, как показано на рисунке 3.45.

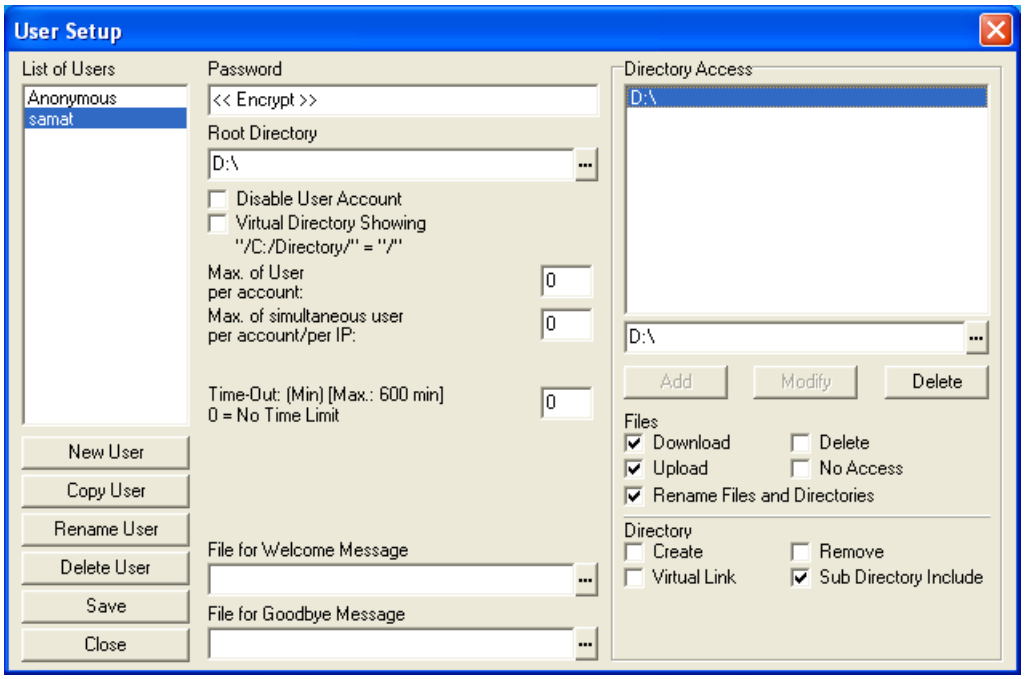

Рисунок 3.45 – Настройка FTPserver

Для настройки понадобится логин, пароль и прописать домашний каталог.

Затем открою проводник и введу ftp://192.168.100.10, введу логин и пароль, затем можно будет передавать и скачивать файлы. На рисунке 3.46 показано окно с подключенным сервером FTP.

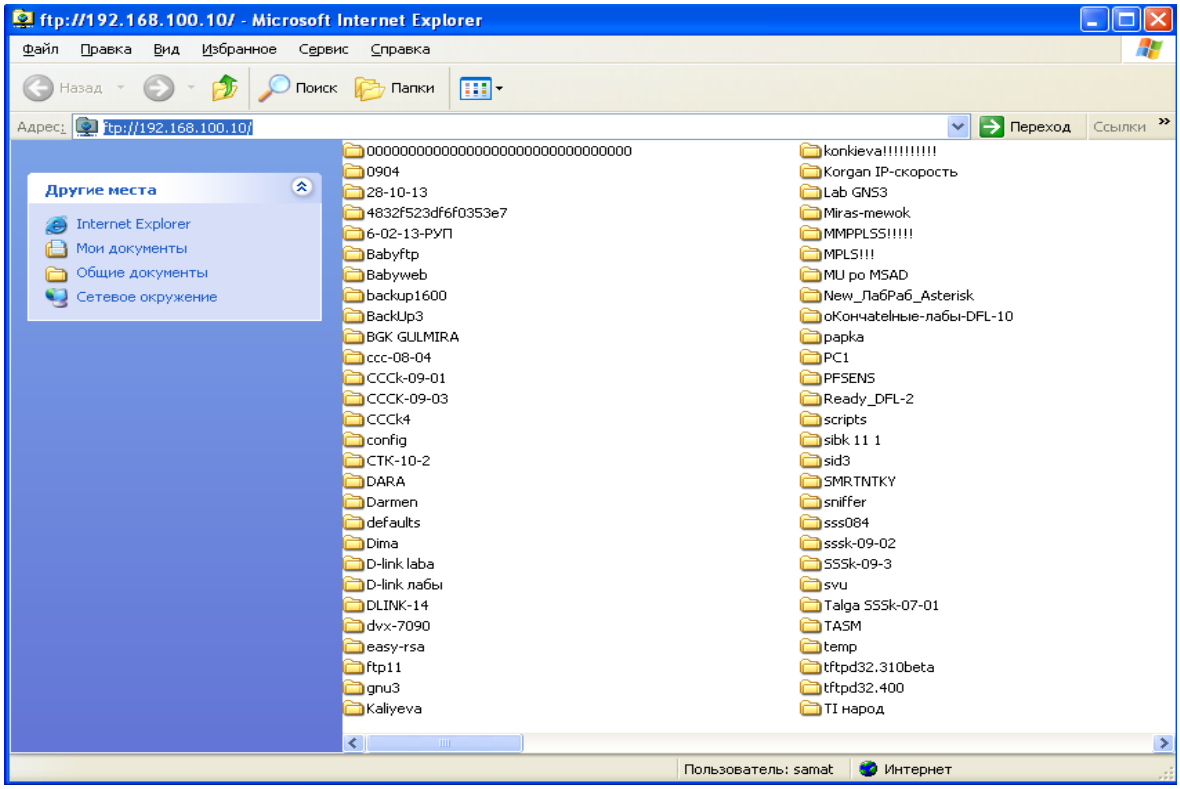

Рисунок 3.46 – Открытый сервер через проводник

Также можно осуществить вход через FiliZila. На рисунке 3.47 показан вход на сервер.

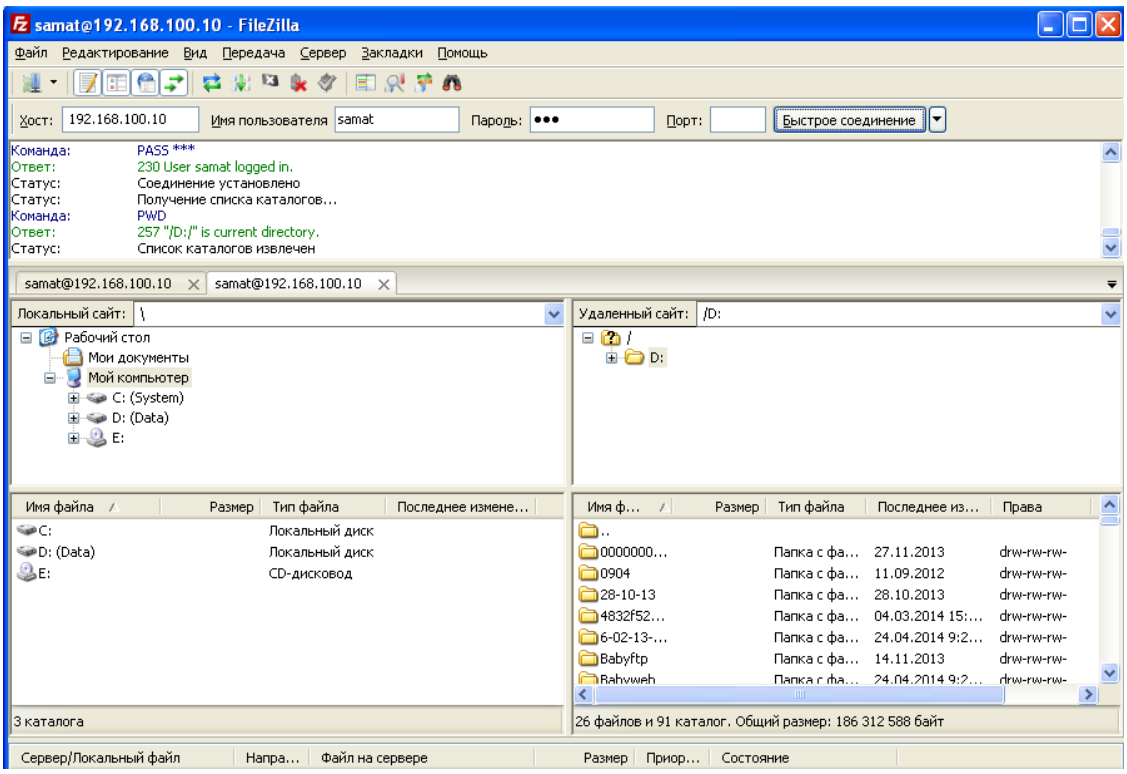

Рисунок 3.47 – Подключение к серверу с помощью FileZilla

Теперь произведу проверку пингом. Пинги будут проходить между wan и lan (рисунок 3.48), а также wan и dmz (рисунок 3.49), а между lan и dmz нет (рисунок 3.50).

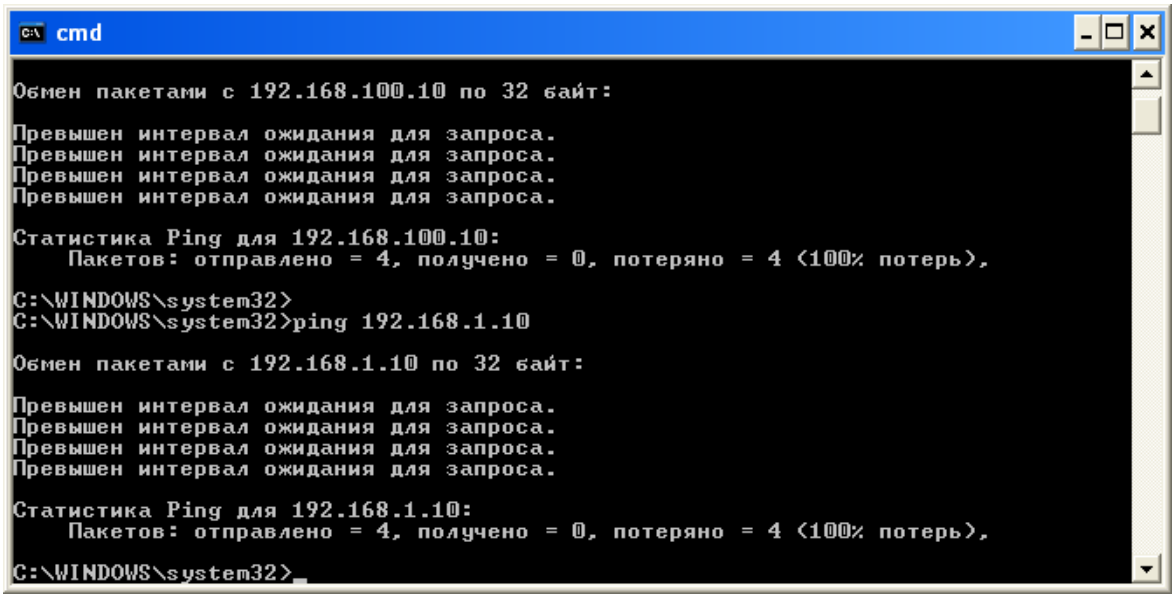

Рисунок 3.48 – Тест пинга между «wan» и «lan»

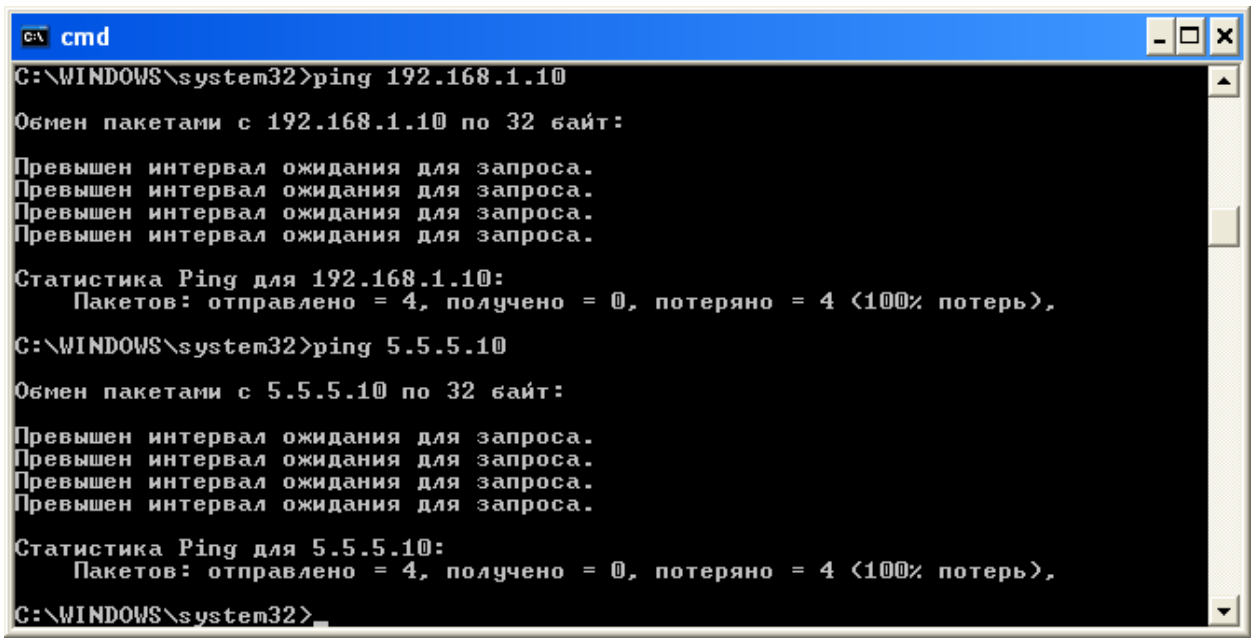

Рисунок 3.49 – Тест пинга между «lan» и «dmz»

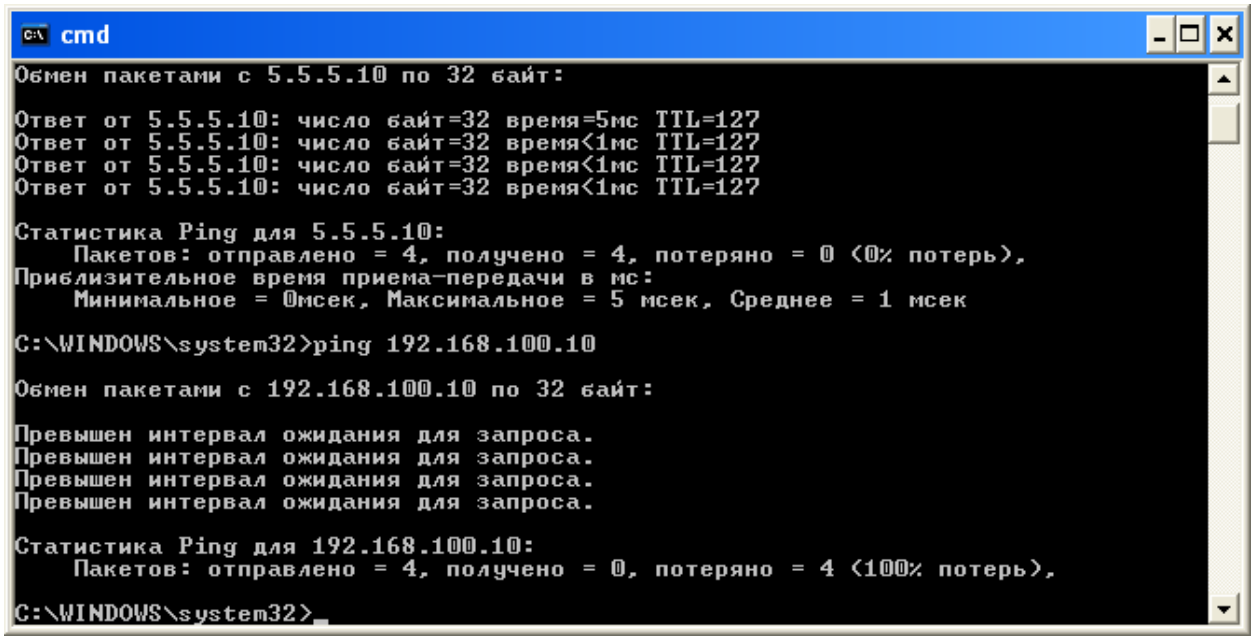

Рисунок 3.50 – Тест пинга между «dmz» и «lan»

На сервер FTP отображаются все события, происходящие в системе. На рисунке 3.51 показано окно с событиями.

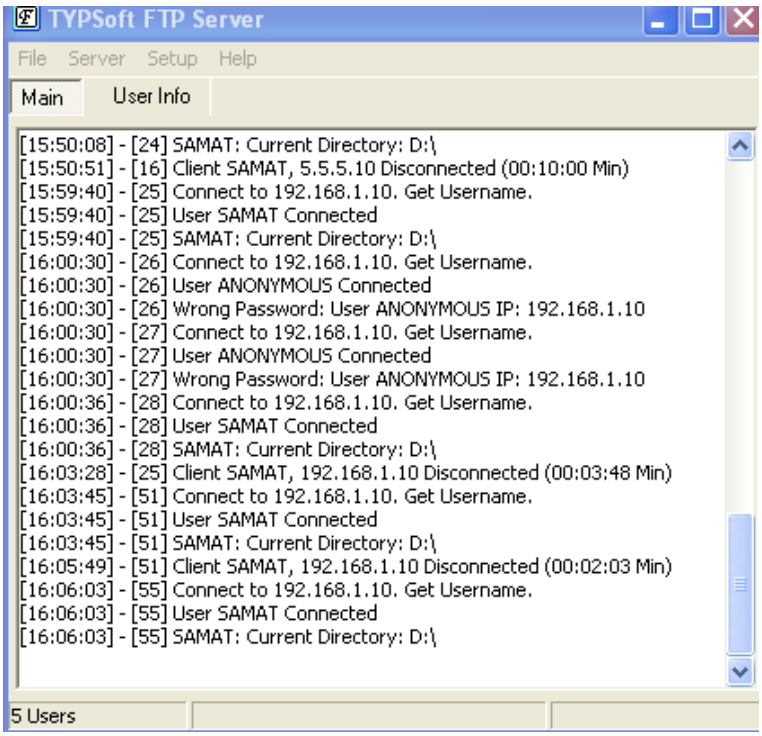

Рисунок 3.51 – Окно с событиями сервера FTP

3.5 Создание VPN–туннеля на основе протокола L2TP

Для создание VPN понадобится два компьютера и брандмауэр.

Целью работы является создание виртуальной приватной сети с использованием протокола L2TP over IPSec для подключения удаленных пользователей с помощью брандмауэра DFL–841.

На рисунке 3.51 показана схема подключения оборудования.

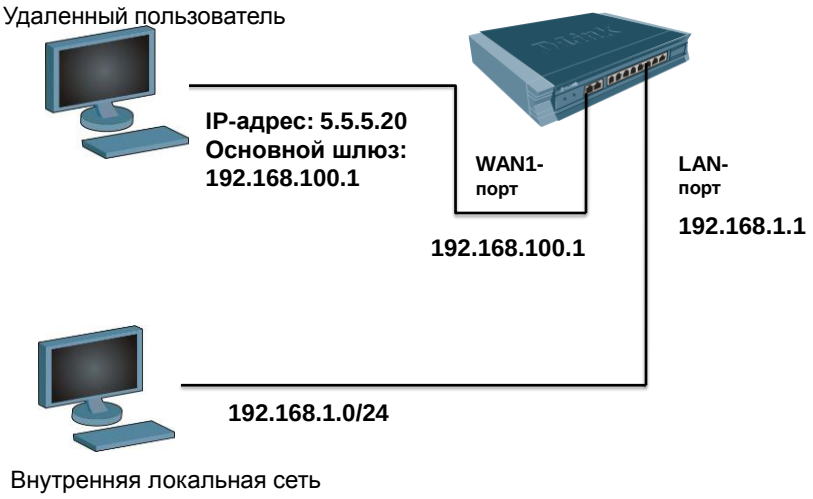

Рисунок 3.51 – Схема подключения оборудования

Настройка L2TP iver IPSec осуществляется оп следующим шагам:

1) подать питание на брандмауэр;

2) соединить UTP компьютер и брандмауэр;

3) произвести настройку адреса на компьютере, используя «Пуск» → «Настройка» → «Сетевые подключения» → «Подключение по локальной сети» → «Свойства» → «Протокол Интернета TCP/IP» → «Свойства»; Затем прописать маску 255.255.255.0 и адрес «192.168.1.xxx»;

4) с помощью web произвести настройку брандмауэра, используя в адресной строке браузера адрес «192.168.1.1» и стандартные логин с паролем «admin»/«admin»;

5) для начала задам адреса lan и wan. Раскрою вкладку «Interfaces» и выберу «Ethernet», при этому брав галку с «Enable Client DHCP» и нажму «ОК»;

6) раскрою вкладку «InterfacAddresses» и добавлю «wan1net» с адресом 192.168.100.0/24. Затем добавлю адрес «wan1» 192.168.100.1. Аналогичным образом добавлю адреса для «lan» 192.168.1.1 и 192.168.1.0/24. На рисунке 3.52 показано окно с адресами сетей;

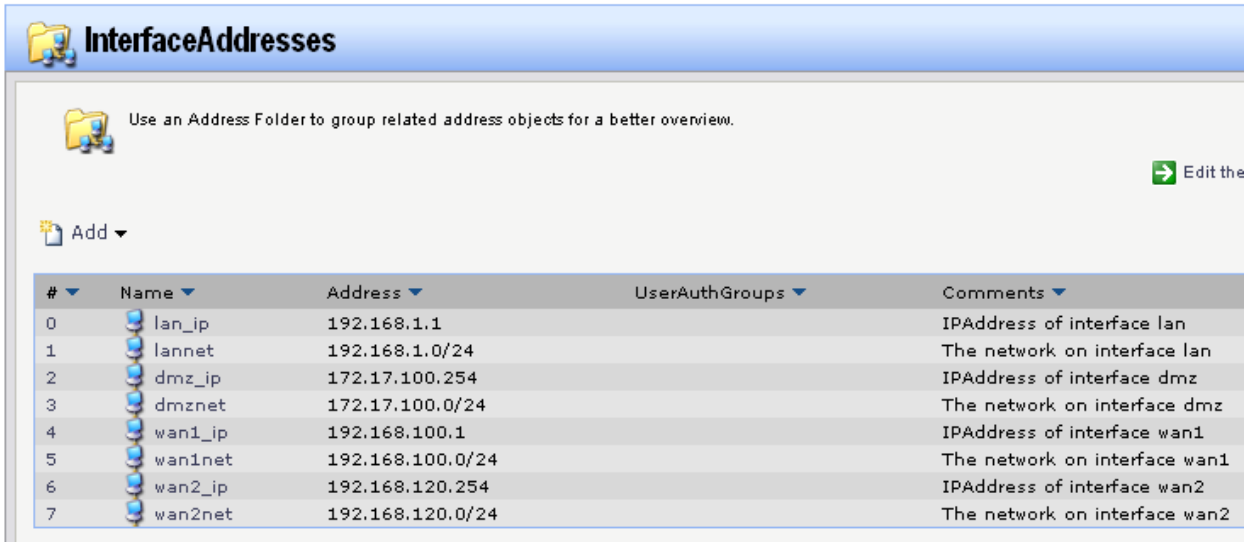

Рисунок 3.52 – Окно с адресами сетей

7) теперь создам пул адресов и назначу их для сервера L2TP. При подключении клиентов им будет выдаваться адрес из назначенного пула. Для этого в вкладке «Address Book» и нажму «Add» и добавлю пулл и сервер. В качестве сервера пропишу адрес 10.0.0.1, а в качестве пула 10.0.0.10–10.0.0.50. Таким образом, пул рассчитан на 50 клиентов. На рисунке 3.53 показан добавленный пул;

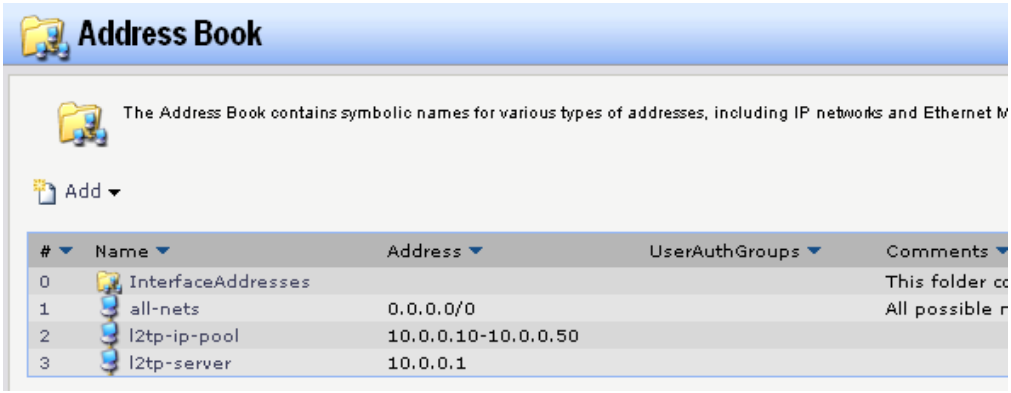

Рисунок 3.53 – Добавленный пул

8) добавлю PSK. Для этого во вкладке «Objects» выберу «Authentication Object», нажму «Add» и выберу PSK. Затем заполню поля «Name» – «ipsec–pre», в «Shared Secret» записывается ключ, в «Confirm Secret» повторно вводится ключ. После чего нажимается «ОК». На рисунке 3.54 показаны настройки IPSec;

]

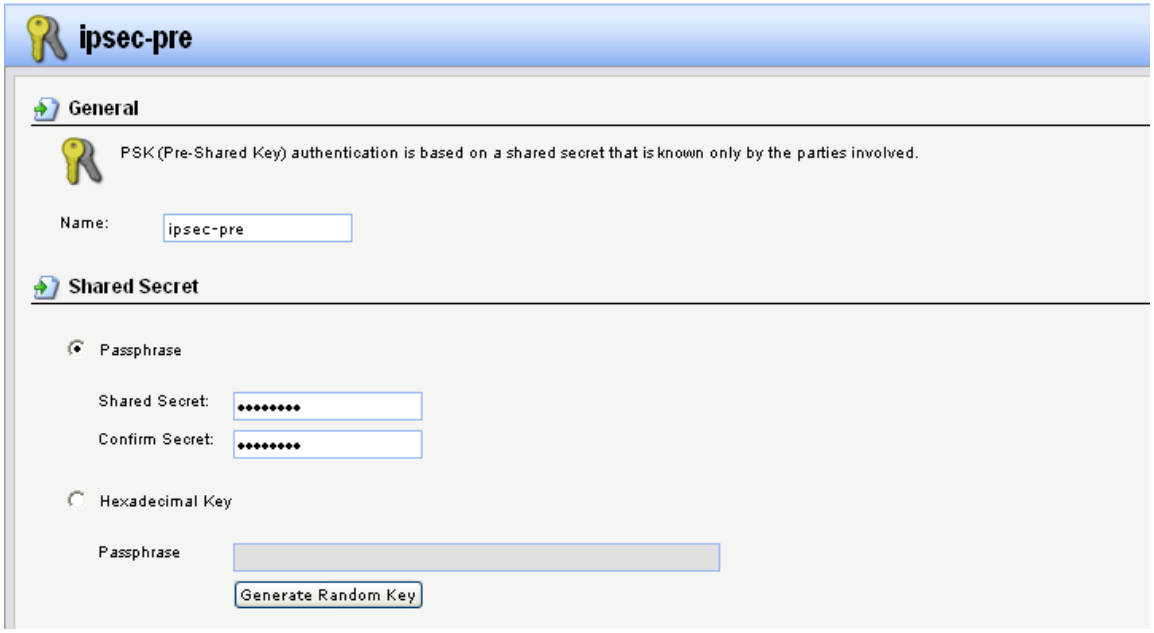

Рисунок 3.54 – Настройки IPSec

9) добавлю IPSec для пользователей в роуминг. В вкладке «Interface» выберу IPSec, нажму «Add» и выберу «Tunnel IPSec». Теперь заполню поля. В «General» поля «Name» – «IPSec_for_roaming», «Local Network» – «all–nets», «Remote Network» – «all–nets», «Remote Endpoint» – «None», «Encapsulation mode» – «Transport». В «Algorithm» заполню поля «IKE Algorithm» – «Medium», «IKE Life Time» – «28800», «IPSec Algorithm» – «Medium», «IPSec Life Time» – «3600». На рисунке 3.55 показаны настройки IPSec.

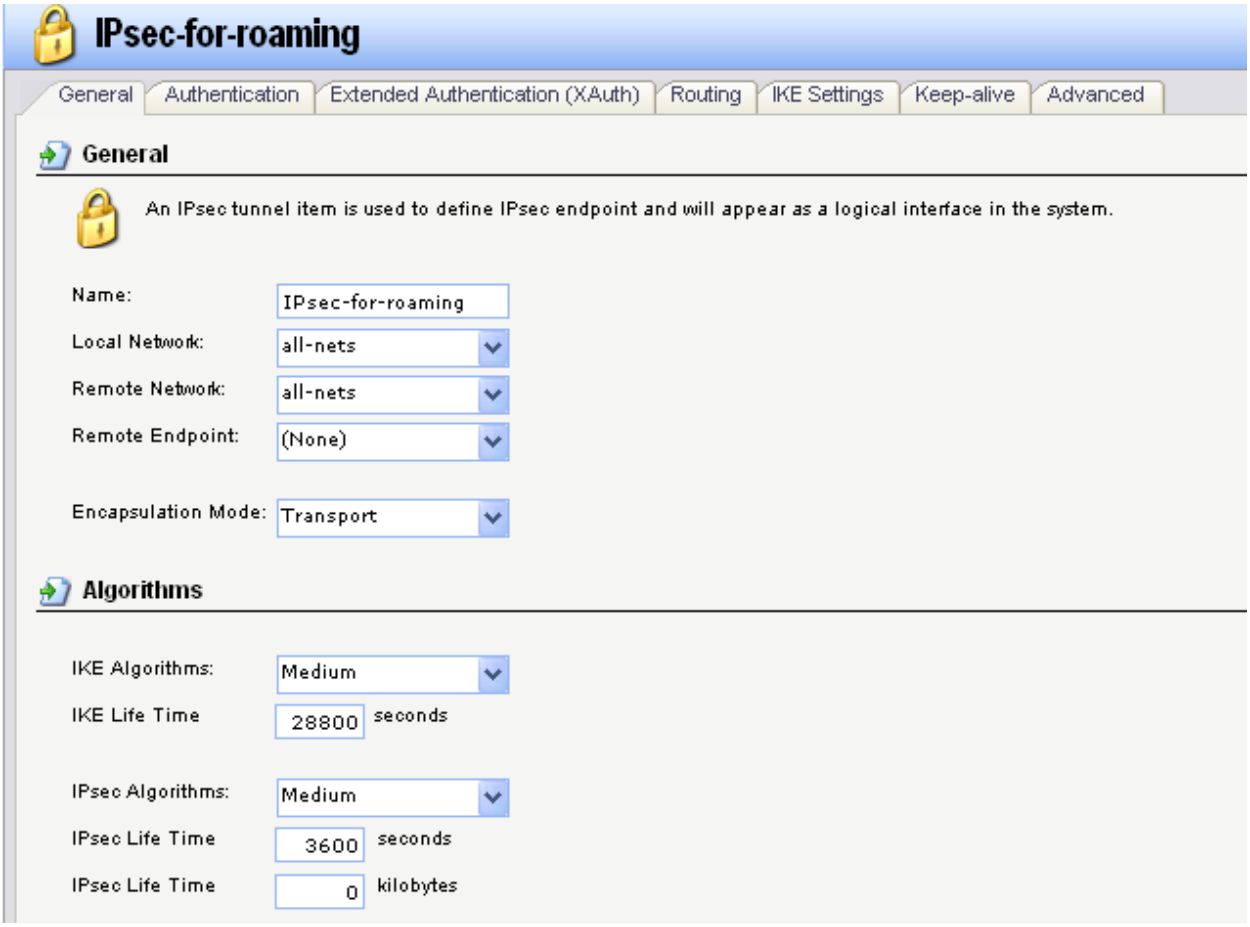

Рисунок 3.55 – Настройки IPSec

Также перейду на вкладку «Authentication» и заполню поле «Pre–shared Key» – «ipsec–pre». В вкладке «XAuth» заполню поле «IKE XAuth» – «Off». После всех действий нажму «ОК»;

10) теперь необходимо добавить серверу L2TP интерфейс. Открою вкладку «Interfaces» и выберу L2TP/PPTP Servers и нажму «Add». Заполню следующие поля в «General» «Name» – «l2tp–if», «Inner Address IP» – «l2tp–server», «Tunnel Protocol» – «L2TP», «Outer interface Filter» – «IPSec–for–roaming», «Server IP» – «wan1_ip». На рисунке 3.56 показано окно с настройками интерфейса;

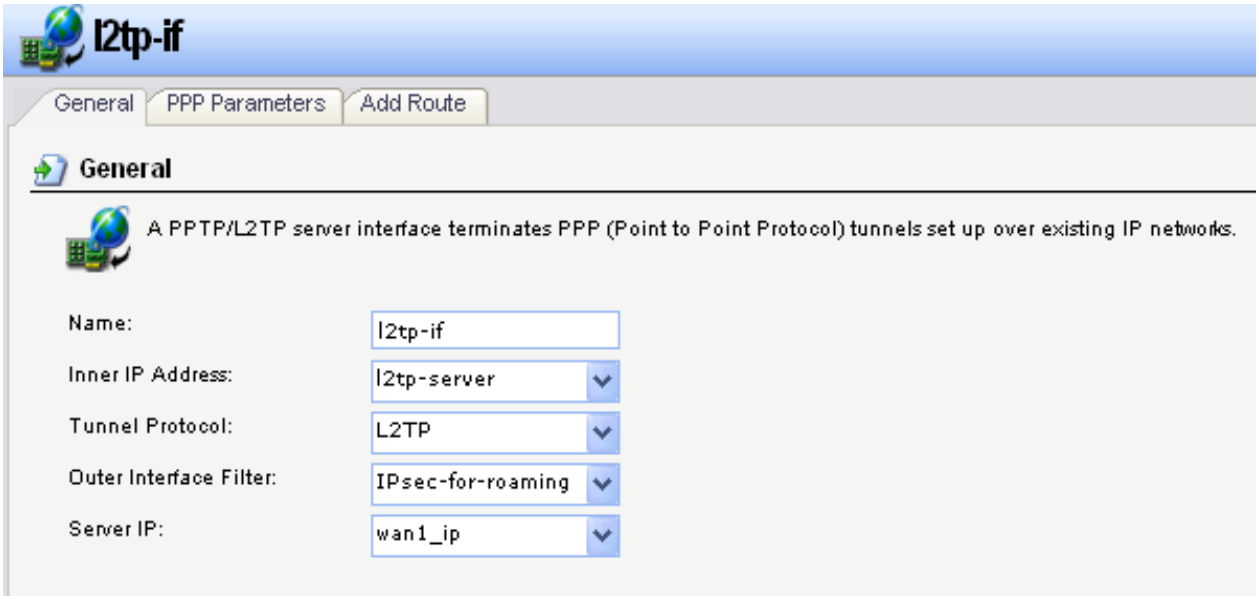

Рисунок 3.56 – Окно с настройками интерфейса

11) добавлю в локальную базу пользователей. В вкладке «User Authentication» выберу «Local User DB» и нажму «Add». Приведу пример создания пользователя. Для начала создам БД с названием «Name» – «l2tp–db». Затем уже в ней создам пользователя с полями «Name» – «test», «Password» – «test», «Confirm password» – «test». На рисунке 3.57 создание пользователя;

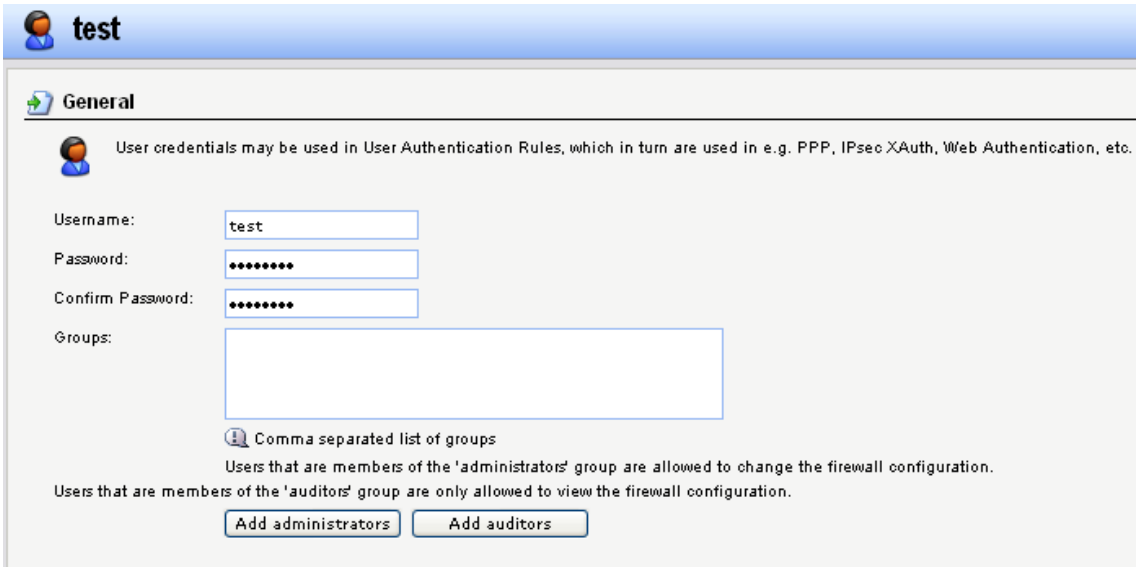

Рисунок 3.57 – Создание пользователя для VPN

12) также необходимо описать правило аутентификации пользователей. Для этого в вкладке «User Authentication» выберу «User Authentication rule» и нажму «Add». Создам правило. Заполню в «General» следующие поля «Name» – «l2tp–auth», «Authentication agent» – «PPP»,

«Authentications Source» – «Local», «Interface» – «l2tp–if», «Originator IP» – «all–nets», «Terminators IP» – «wan1–ip». На рисунке 3.58 показано окно с настройками аутентификации;

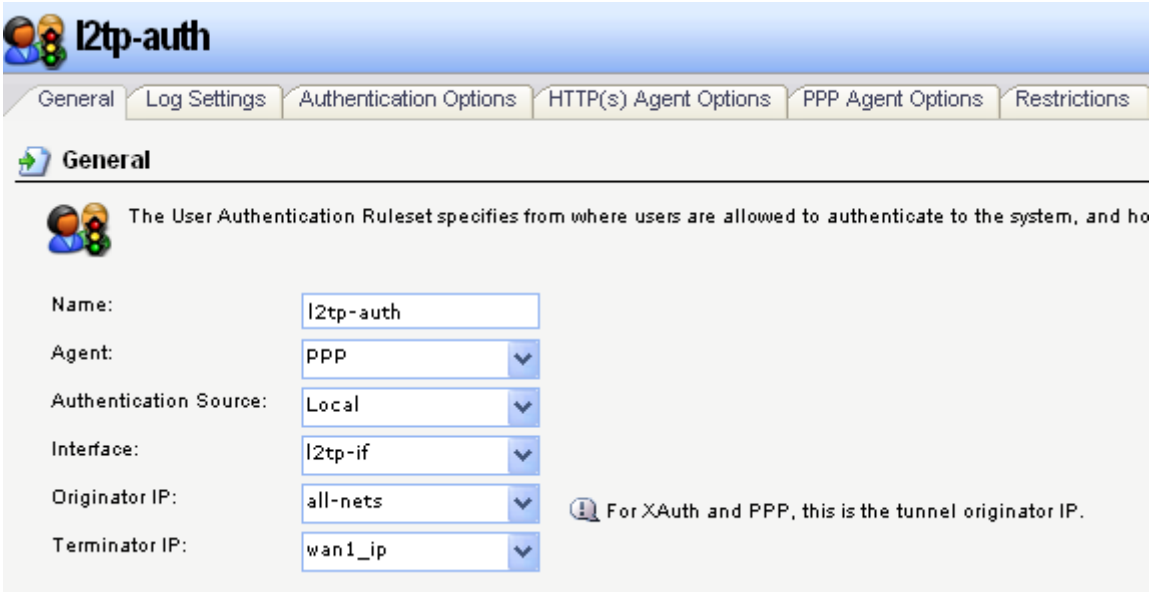

Рисунок 3.58 – Окно с настройками аутентификации

13) продолжу настройку. Перейду на вкладку «Agent Option». В вкладке «General» поставлю галку напротив «MS–CHAP». На рисунке 3.59 показано вкладка «General».

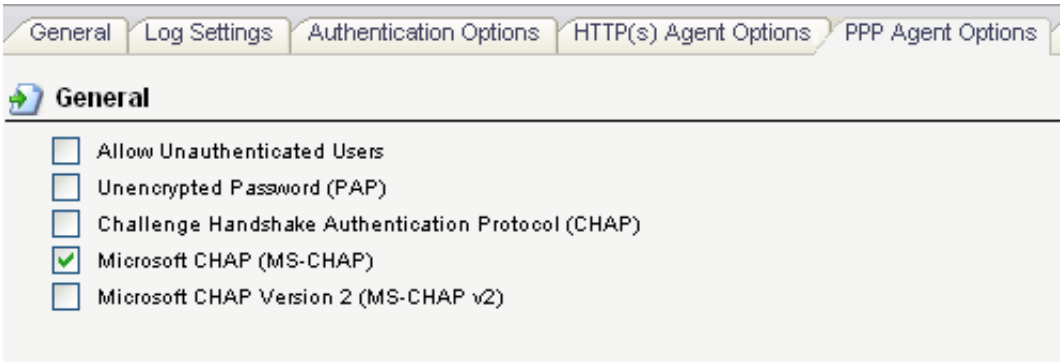

Рисунок 3.59 – Вкладка «General»

В вкладке «Restrictions» выберу «Allow multiple login per username». На рисунке 3.60 показана вкладка «Restriction»;

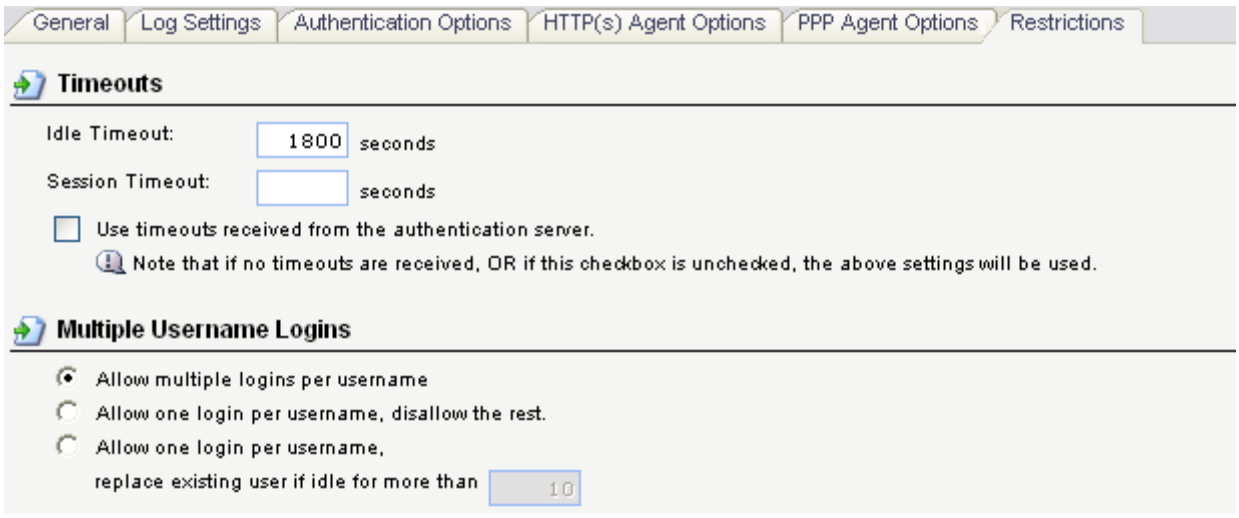

Рисунок 3.60 – Вкладка «Restriction»

14) далее создам правила для разрешения доступа к lan удалённых пользователей и обратно. Для этого необходимо перейти на вкладку «Rules», выбрать раздел «IP Rules» и нажать «Add».

Создам первое правило. В «General» заполню поля «Name» – «allow–l2tplan», «Action» – «Allow», «Service» – «al_service». В «Address Filter» заполню «Source» – « », «Networks» – «all–nets», «Interfaces» – «l2tp–if». В «Destinations» заполню поля «Interface» – «lan», «network» – «lannet» и нажму «ОК». На рисунке 3.61 показано первое правило.

Рисунок 3.61 – Первое правило

Создам второе правило. В «General» заполню поля «Name» – «allow–l2tpwan», «Action» – «Allow», «Service» – «all_service». В «Address Filter» заполню «Source» – « », «Networks» – «lannet», «Interfaces» – «lan». В «Destinations» заполню поля «Interface» – «l2tp–if», «network» – «all–nets» и нажму «ОК». На рисунке 3.62 показано первое правило.

Рисунок 3.62 – Второе правило

Создам третье правило. В «General» заполню поля «Name» – «wantolan», «Action» – «Allow», «Service» – «all_service». В «Address Filter» заполню «Source» – « », «Networks» – «all–nets», «Interfaces» – «wan1». В «Destinations» заполню поля «Interface» – «lan», «network» – «lannet» и нажму «ОК». На рисунке 3.63 показано первое правило.

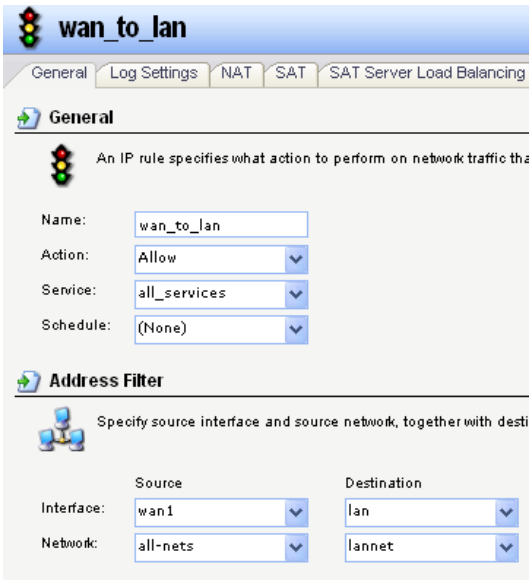

Рисунок 3.63 – Третье правило

Создам четвертое правило. В «General» заполню поля «Name» – «wantolan», «Action» – «Allow», «Service» – «all_service». В «Address Filter» заполню «Source» – « », «Networks» – «lannet», «Interfaces» – «lan». В «Destinations» заполню поля «Interface» – «wan1», «network» – «wannet» и нажму «ОК». На рисунке 3.64 показано первое правило;

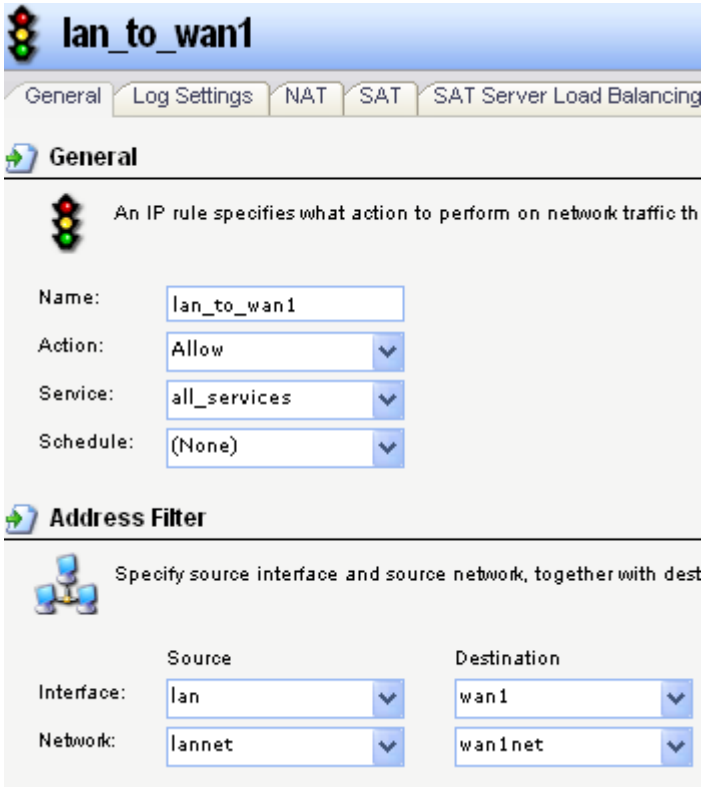

Рисунок 3.64 – Четвёртое правило

15) теперь необходимо настроить маршруты. Для этого открою вкладку «Routing» и открою «Main Table Routing», нажму «Add», выберу «Switch». На рисунке 3.65 и 3.66 показаны настройки маршрутизации.

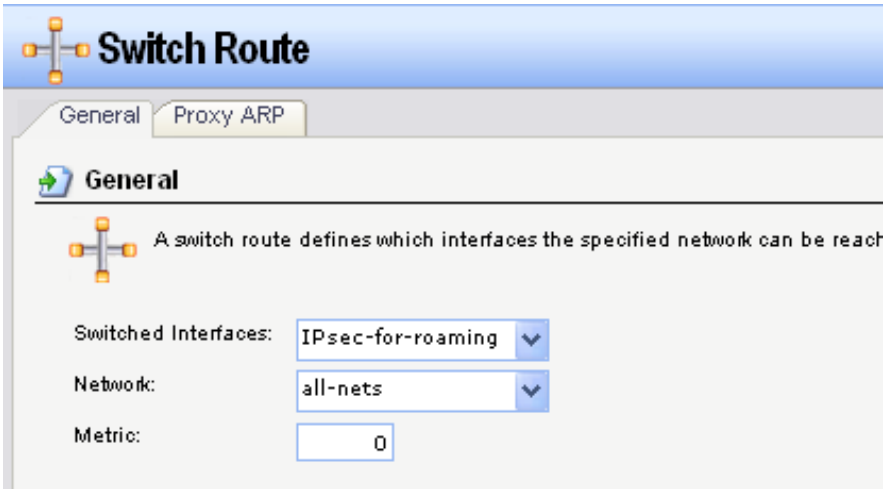

Рисунок 3.65 – Маршрутизация «ipsec for roaming»

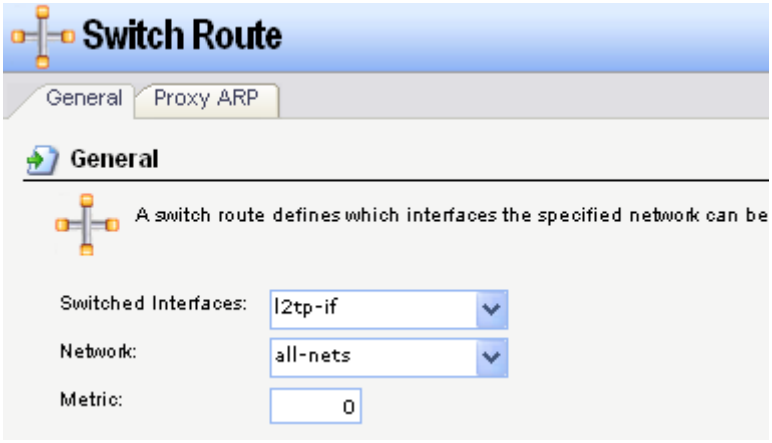

Рисунок 3.66 – Маршрутизация «l2tp–if»

После настройки маршрутизации необходимо сохранить настройки, нажав «Activates and Save».

Для настройки L2TP необходимо выполнить следующие шаги:

1) проверить работу службы IPSec, перейдя «Администрирование» → «Службы»;

2) соединить UTP брандмауэр и компьютер;

3) произвести настройку адреса на компьютере, используя «Пуск» → «Настройка» → «Сетевые подключения» → «Подключение по локальной сети» → «Свойства» → «Протокол Интернета TCP/IP» → «Свойства»; Затем прописать маску 255.255.255.0 и адрес «192.168.100.1»;

4) «Пуск» → «Сетевые подключения» → «Мастер новых подключений» → «Подключить к сети на рабочем месте» → «Подключение к виртуальной частной сети» → «укажите имя создаваемого подключения» → «Не набирать номер для подключения» → «укажу 192.168.100.1» → «введу пользователя и пароль (test и test). Подключение осуществлено.

4 Безопасность жизнедеятельности

4.1 Анализ условий труда оператора

Цель проекта – организация корпоративной сети при угрозах влияния безопасности системы. Эксперименты сделаны в лаборатории кафедры оборудовании DFL–841 к подключенному ПК. DFL–841 – просто развертываемое устройство брандмауэр, разработанное для крупных предприятий, защищающее сеть от нападений.

Главные особенности:

− DRAM: 384 Мб;

− Flash память 128 Мб;

− пропускная способность свыше 300 Мбит/с;

− шифрование 3DES: свыше 38 Мбит/с;

− безопасность: L2TP/PPTP/IPSec;

− алгоритмы аутентификации: SHA–1 и MD5.

Для уверенной работы ПК нужен постоянный ток, который преобразуется в БП. В БП переменный ток преобразуется в постоянный. Мощность БП врьируется в больших пределах и в большинстве случаях используются 400 Вт. Зрительные работы на персональных компьютерах имеют разряд IV (б).

Лаборатория кафедры АУЭС имеет параметры: длину L 8 м, ширину B = 5 м, высоту H = 4 м, также присутствуют четыре окна, различные аппараты, кондиционер и ПК. На рисунке 4.1 показана схема помещения.

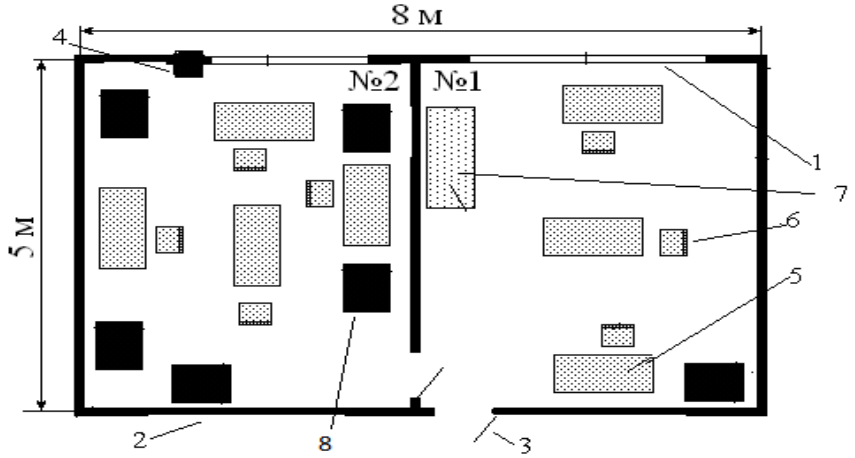

Рисунок 4.1 – Схема аудитории

Для освещения инсталированы газоразрядные люминисцентные лампы мощностью 60 Вт и световым потоком 3110 лм. В лаборатории испольуются

светильники вида КОУ–3х60–2001. Лаборатория оборудована пятью рабочими местами с ПК.

Сильное влияние окзывает окружающая среда, которая сформировалась в помещении, это всё влияет на состояние работников. Организм человека постоянно обменивается теплом с окружающим его миром. На тепловое положение влияют параметры микроклимата, также перегрузки, связанная с трудовой дисциплинной. В отличии от тяжести работы увеличиваются энергозатраты пропорционально, которые состовляют 80–210 Вт. Согласо ГОСТ 12.1.005–88 класс энергозатрат 1а, при которых организм расходует не больше 139 ккал/час, рабочая температура окружающей среды не должна превышать 23 °С, а влажность не более 75%, а скорость воздуха не менее 0.4 м/с. Кондиционер в помещении предназначен для регулирования климата. Кондиционирование позволяет не только осуществлять вентиляцию и отопление, но и воссоздаёт благоприятные условия климата в летнее время года, используя фреонную систему,

Цель обусловить атмосферы развивается в обслуживании подобных особенностей легкой сферы как, какой ряд любой Человек вследствие личной организации автоматической терморегуляции организма Чувствовал бы себя удобно, в этом случае принять не замечало влияния этой сферы ни в каком случае. Организационные трудовые зоны содержат огромный роль в организациях работы. Точное формирование из рабочего места уменьшает подобные трудности одинаково: ранняя усталость, негативное воздействие в теле человека, который портит его здоровье, сокращение выполнения работы.

На рисунке 4.2 показано рабочее место.

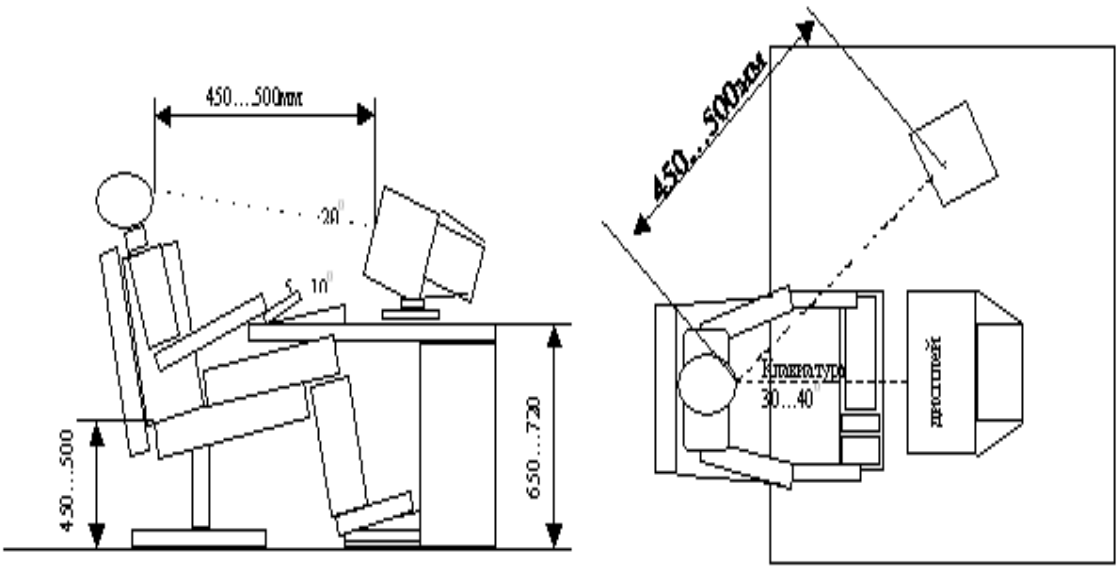

Рисунок 4.2 – Рабочее место

Место работы оснащено представим для отображениях необходимых данны, приспособлениями для управления, где осуществляется рабочая

деятельность человека. Для регулирования правил и номр рабочего места введены СН 245–71, который устанавливает минимальный объём на человека, а также рабочую площадь сотрудника. После анализа рабочих условий в этом разделе решу задачи:

- произвести расчёт освещенности рабочего места;
- разработать рабочее место, учитывая требования энергобезопасности и санитарных норм.

4.2 Анализ условия труда оператора с расчетом освещения на рабочем месте

4.2.1 Расчет природного освещения

Здание должно внутри должно освечиваться внутри естесственным освещением. При перепланировки, переконструировании помещений необходимо учитывать конструктивно природное освещение комнат и других объектов. Для этого необходимо сделать просветы, которые должны обеспечивать необходимый уровень КЕО согласно требованиями СНиП РК 2.04–05–2002 «Естественное и искусственное освещение. Нормы проектирования».

Длина помещения L = 4 м, ширина комнаты B = 5 м, высота комнаты H = 4 м. Высота рабочего стола h_p = 0.75 м. Газоразрядные лампы выступают источниками света. Мощность одной лампы 60 Вт, а световой поток – 3110 лм.

В помещении присутствуют два окна размером 2.2x2.5 м каждое. Окно расположено на высоте 1.5 м от пола. Окна располагаются в одной стороне комнаты. Класс зрительной работы IVб.

Нормированные значения КЕО приводятся для III пояса светового климата формуле:

$$e^{IV} = e^{III} \cdot m \qquad (4.1)$$

где $e^{III}_{н}$ – значение КЕО III пояса;

m – коэффициент светового климата, для IV пояса.

Значение КЕО с учетом коэффициентов m равно согласно формуле (4.1):

$$e^{IV}_{н} = 1.3 \cdot 0.9 = 1.17\ \%$$

Коэффициент естественного освещения рассчитаем по формуле:

$$e_н = \frac{100 \cdot S_0 \cdot \tau_0 \cdot r_1}{S_п \cdot \eta_0 \cdot K_{зд} \cdot K_з} \qquad (4.2)$$

где So – суммарная площадь боковых световых проёмов, равное 3.79 м^2;

$S_п$ – площадь пола помещения, м^2;

$e_н$ – нормированное значение КЕО;

$k_з$ – коэффициент запаса;

$\tau_0 = \tau_1 \cdot \tau_2 \cdot \tau_3 \cdot \tau_4$ – общий коэффициент светопропускания;

η_0 – световая характеристика окон;

r_1 – коэффициент, учитывающий повышение КЕО при боковом освещении благодаря свету, отраженному от поверхностей помещения и подстилающего слоя, прилегающего к зданию;

$k_{зд}$ – коэффициент, учитывающий затенение окон противостоящими зданиями.

Площадь пола помещения:

$$S = L \cdot B = 4 \cdot 5 = 20 \text{ м}^2 \quad (4.3)$$

Рамы из дерева позволяющие увеличить прпоускание света из–за двойного остекления, а в качестве несущей конструкции применяются арки из железобетона. Тогда τ_0 равен:

$$\tau_0 = 0.8 \cdot 0.6 \cdot 0.8 = 0.384 \quad (4.4)$$

Чтобы узнать η_0 нужно определить соотношение длины к глубине. Из–за того, что окна располагаются на одной и той же стороне, то вычислю по данной формуле:

$$\frac{L}{l} = \frac{4}{3} = 1.33 \quad (4.5)$$

Надо рассчитать соотношение l/h_1, где h1 является высотой между верхом окна и рабочей поверхностью:

$$h_1 = h_{ок} + h_{н.ок} – h_{пов} = 2.5 + 1 – 0.75 = 2.75 \text{ м} \quad (4.6)$$

Таким образом, соотношение B/h_1 равно:

$$\frac{B}{h_1} = \frac{4}{2.75} = 1.45 \quad (4.7)$$

Для найденного соотношению определю η_0 равный 10, 5.

Чтобы определить r1 нужно определить l/B , где l является расстоянием между наружной стеной и расчётной точкой. Для этого случая приму l = 3, следовательно соотношение принимает единицу.

Приму за p = 0.5, и найду r1 = 2.1. Учту при этом высоту здания. k определяется с помощью $P/H_{зд}$, которое равно:

$$\frac{\mathbf{P}}{\mathbf{H}} = \frac{30}{18} = 1.525 \tag{4.8}$$

Из соотношения выше k = 1. Теперь подставлю данные в формулу (4.2):

$$e_{\mathbf{н}} = \frac{100 \cdot 3.79 \cdot 0.384 \cdot 2.1}{20 \cdot 10.5 \cdot 1 \cdot 1.2} = 1.2128$$

Произведу сравнение величин $e_н$ и e^{IV}, учитывая его площадь оконного проёма обеспечивает необходимый уровень освещения.

4.3 Технические меры защиты от поражения электрическим током

Все меры можно разделить на группы условно. Меры технической защиты группы один обеспечивают защиту против поражения током персонала в случае касания к находящимся под напряжением частям им беспокойство:

– управление условием изоляции устройств электротехнического назначения и мест сети, подающей их;
– блокирование и защитные меры защиты;
– оптимальное расположение обеспечения оборудования разрывает между находящимися под напряжением частями;
– система сигнализации безопасности (свет, звук), отмечая и предупредительные сообщения;
– защита от высокого напряжения стороне низкого напряжения;
– использование низкой силы 43 и 13 В;
– применение отдельного защитного оборудования изоляции.

Вторая группа обеспечивает защиту против поражения с током при малейшем прикосновении к случаю элеутановок в случае поломки изоляции находящейся под напряжением частей им беспокойство:

– защитное основание;
– защитное обнуление;
– защитное закрытие;
– двойная изоляция;
– использование делящихся трансформаторов.

Электрическая изоляция может быть под напряжением. Ясно, что надежность и длительность эксплуатации электротехнических приборов во многих отношениях зависят от условий электрической изоляции, которые находятся под напряжением. Повреждение изоляции часто бывает основной причиной большинства электрических ран, несчастных случаев и огней. Изоляция – это защитная мера, состоит в ограничении из текущего продолжения на теле человека до безопасного размера.

Надёжность изоляции зависит от большого числа факторов предоставлена применением, его определенный тип (рабочий, усиленный и двойной), соответствующие изоляционные материалы, рациональный дизайн электрического оборудования, нормальные условия рабочей среды и правильная организация предотвращения в использовании.

Оборудование имеет изоляцию, которая поддерживает механическое устройство, тепловые и электрические нагрузки, чрезвычайно возможные под условиями эксплуатации.

Защитное основание является преднамеренной связью с землей не находящиеся под напряжением металлические детали электрического оборудования, оборудования, молниеотводов и оцененных спортсменов. Цель защитного основания – для ослабления до безопасной напряженности размера на случае относительно земли, возникающей на не находящиеся под напряжением части прибора под коротким замыканием на случае (распад на случае) в повреждении изоляции проводников, переносящих рабочий ток электроснабжения оборудования.

Ток, который проходит через тело, может быть понижен, увеличен, сопротивление Rch и R2 или уменьшающий основание сопротивления проводника. Последнее является самым простым, поскольку основание импеданса во многих отношениях зависит от конфигурации и это возможно, изменяя его, чтобы получить любую необходимую ценность сопротивления.

Т.о., в присутствии основания с сопротивлением распространению тока маленькой стоимости, ток, продолжающийся через человека, прикоснувшегося к поврежденному кабелю. Возможно прийти к подобному заключению, рассмотрев ценность основания импеданса корпуса электрического оборудования при электропитании от переменного тока.

4.4 Разработка рабочего места оператора с учетом требований санитарии и электробезопасности

Санитария – данный понятие событий координации и промышленных денег, которые предотвращают или которые сокращают влияние в работниках вредных условий. Представлены ключевыми ужасными и вредными условиями: высокая пыльность и примесь атмосферы области; высокое или дешевое тепло атмосферы области; высокая или дешевая сырость; завышенный градус грохота; завышенный градус пульсации.

Работоспособность и общая производительность, находящейся в зависимости с капиталом – гигиенические обстоятельства. Расположение, ясное, просроченное и Невиновное, полностью отвечает на санитарные и гигиенические стандартные меры.

Согласно GOST 12.1.005–86 SSBT «Пролетарий воздушного пространства области, Универсальные Санитарные и Гигиенические Требования», деятельность маленького жаркого в этой комнате выполняются сидя и не называет существенное усилие ни в каком случае, принадлежат группы I а. Свободно от стадий летних микроклиматических характеристики в закрытом помещении не превосходят определенные возможные значения ни в каком случае: температура летней стадии +24 ^{0}C, температура зимней стадии +22 ^{0}C.

Т а б л и ц а 4.1 – Параметры микроклимата

Нормы	Оптимальные			Допустимые		
Период работы	Темпера–тура воздуха, ºС	относи–тельная влаж – ность, %	скорость движения воздуха, м/с	Темпера–тура воздуха, ºС	относи – тельная влаж – ность, %	скорость движе – ния воздуха, м/с
Холодный	22 – 24	30 – 60	0.1	21 – 25	80	0.1
Теплый	23 – 25	40 – 60	0.1	22 – 28	75	0.1 – 0.2

Кондиционер метод, остающийся в закрытом помещении, более многообещающая, обеспечивающая Точность и обычных атмосфер, т.е., создан синтетический продукт атмосферой с поддержкой единиц создания условий. Поблизости у предавшего гласности пространства, идя в договоренность, есть возможность много требований, чтобы нагреться, лишить работы, расхолодить или быть истощенным.

Нагревание рассматривает стабилизация температуры, должен введенным обычным мерам. Строительство стен отлично показывает мир. Звук от оборудования приближается не к сильному.

Вентиляция представлена главный инструмент, обеспечивающий обычные санитарные и гигиенические обстоятельства комнат. Любимые работы с целью натяжения пыли, газов, бесед, излишков высокой температуры из комнат.

Контроль капитала местного климата в зале позволяет шанс продвинуть обстоятельства работы, которая связана с подходящим, который увеличивает удобство работы и эффективность.

Электробезопасность – понятие событий координации и промышленных денег, котоыре предоставляют вредное и опасное влияние в рабочих от тока, электрической арки, электромагнитной степь и константа электроэнергия. Принципы электробезопасности отрегулированы

промышленными бумагами и законными, стандартным и промышленным основанием. Знание оснований электробезопасности любой ценой в целях персонала, обслужащего установки и электрического оборудования.

Электрический ток – главные причины для поражения человека:

− уносят электрический ток, используя неисправные электрические устройства;

− присоединение к неизолированным элементам электроустановки;

− по ошибке данная напряженность на рабочем месте;

− появление напряженности на случае оборудования, которое не находится в возбужденных нормальных условиях;

− уносят электрический ток дефектной линии электропередачи.

С несчастными ситуациями существенного числа от ущерба от гальванического тока соединяют интерфейсом с этой целью, что изоляция электроустановок повреждается. В целях защиты маленького жаркого от гальванического тока потерь соседний дефект изоляции это обязано быть им, используется, это согласовывает последнее на критерий, один с последующих сторон безопасности: земля, обнуление, выключающая безопасность, преобразователь, маленькая интенсивность, двойная изоляция, согласование потенциалов.

Все электрические предметы: компьютер или мобильный телефон, соединение специально намеченной защитой распределены и кабели обладают сильной изоляцией и продолжиться через места, недоступные лицу. В каждом подразделении помещения электроэнергии обязан остаться перед непрерывным управлением специально преподававшие отвечающие лица. Это правило вызывается с этой целью, которые помимо токов в электрооборудовании имеют шансы появиться и очень ненужный (поток короткого короткого замыкания, когда поток перегрузки и потери. В последствии оборудование поворачивается из режима, существует аннулирование огня, общество получено электрическими травмами.

В большинстве зданиях применено гальваническое проведение, которое не обладает единственным основанием кабеля. Соединение персонального компьютера к таким облигациям опасно появлением в случае и сокетах целого блока потенциалов отличных от нуля, которые имеют возможность стать причиной для выхода оборудования от режима соседнее соединение и отсоединение сокетов, но также и к вероятному гальваническому току удара поблизости контакт металлических деталей организации. Точно объявляя, работа персонального компьютера без основания не позволяется, и это представлено, грубая патология стандартных мер защиты работы, но сотрудниках практики учреждений очень Часто ограничиваются проектом сокетов с контактом заземления, который практически не основывается всегда.

Средство электрозащиты – средство от поражения током намеревалось гарантировать электробезопасность. Изоляция оборудование разделяет на основном и дополнительный:

От методов установки нуля защиты корпуса устройства представлен одному. Проблема аннулирования – немедленно, чтобы выключить устройство о коротком замыкании связей одного (два) фазы в теле поблизости. Обеспечить безопасность легкого человек к аннулированному телу во время полуразрушенного периода.

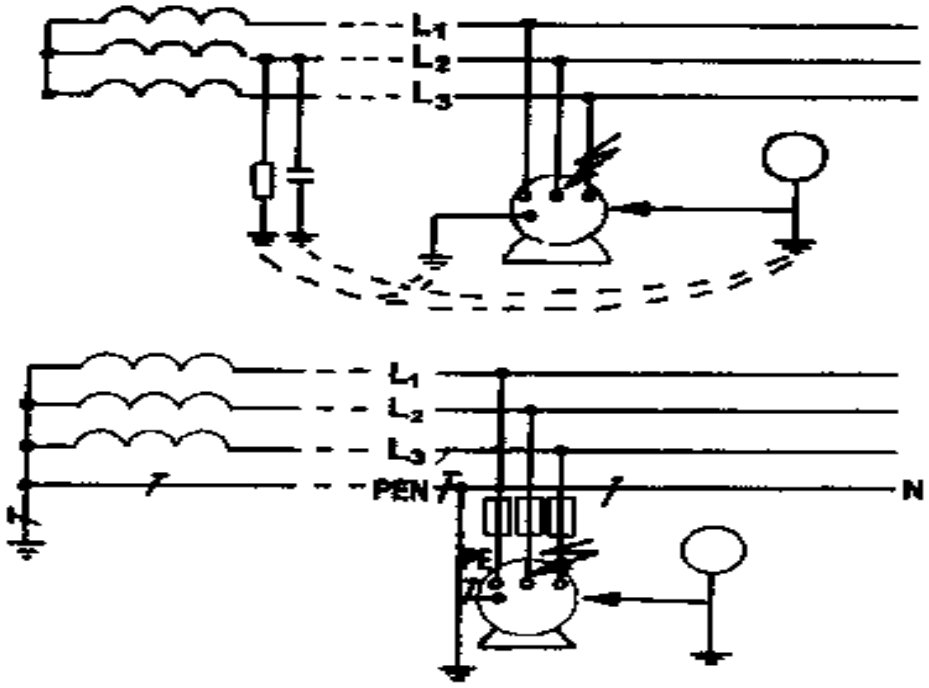

Рисунок 4.4 – Защитное заземление и зануление

В лаборатории условия по электробезопасности исполняются. Напряжение 220В подается на люминисцентные лампы, на кондиционер, на компьютеры, на оборудование. Все электрические объекты подключены через специальный щит распределения и кабели имеют надежную изоляцию.

5 Бизнес план

5.1 Преимущества PPTP

В работе дан обзор создания безопасной ЛВС, основываясь на протоколае PPTP.

Данная услуга позволяет компаниям произвести организацию своей сети на основе оборудования и линий связи, беря на себя контроль за осуществление распределения приоритетов, прав и номеров.

Плюсы данной технологии

- быстрое подключение;
- качественная линия связи;
- не нужно оплачивать выделенные линии;
- безопасное, надёжное и экономичное решение.

Технология позволит сократить затраты на:

- настройку, монтаж и покупку удалённых серверов;
- клиентское ПО;
- удалённый трафик;
- число сисадминов;
- линиях связи.

Единождые затрыты

- оплата доступа сети;
- плата за порт ежемесячная.

5.2 Чем полезны PPTP

Скоростное развитие Интернета, которое наблюдаем в течение прошлых нескольких лет, позволяют каждому владельцу компьютерного доступа с без лимитным объемам информации. Вследствие этой возможности отдельного и общего сетевого доступа связи в разное время суток превращается в неизменное условие рабочего мира. Некоторые компании превращены представлением технологий, позволяющие использовать работу, расположенную на любых географических углах. У сотрудников, которые взяли командировки, есть возможность ввести корпоративную сеть связи непосредственно из гостиничных номеров и тех, кто работает дома, может сохранить в контакте с основными офисами компаний в режиме реального времени. Направляя к улучшенному сотрудничеству с поставщиками и партнерами, компании открывают для них отдельные области сети, преимуществами являются для него время, уезжая на введении нового производства сокращено и качество увеличений обслуживания клиентов.

Изменение в объемах информационных технологий это сопровождается изменением фундаментальной сетевой инфраструктуры. PPTP – туннельный протокол взгляда точка–точка, разработанное Microsoft, позволяя компьютеру установить резервируемое соединение с серверами вследствие создается специальный туннель в стандарте, незащищенная сеть прибывает в замену к классическому методу установления соединения между интернет–пользователями. PPTP может также использоваться для организации туннеля между двумя локальными сетями.

5.3 Организация защищенной сети

К важнейшей основой бизнес–плана относится план организации сети. В проекте производится расчёт затрат доставки, покупки, установки и старта оборудования для защиты ЛВС на базе оборудования DFL–841. Выбор данного оборудования обусловлен тем, что фирма выпускает надёжное функциональное гибко настраивающееся оборудование. Для постойки защищённой сети можно использовать брандмауэры, которые бывают:

– программные брандмауэры. Комплекс устанавливается на сервер и сервер выполняет функции аппаратного брандмауэра, защищающий сеть от взлома;

– аппаратный брандмауэр. Является готовым оборудованием, которому не нужен сервер для контроля проходящего траффика через него.

5.4 Межсетевой экран (firewall)

Для построения сети выбран брандмауэр DFL–841. Он является аппаратным брандмауэром линейки NetDefend, который предназначен для работы с огромными вычислительными мощностями, огромными БД, а также для ускорения работы сети, позволяющий обрабатывать параллельно неимоверное количество кадров. В устройстве есть возможность устанавливать модули SFTP, оптические каналы, также 8 портов стандарта «Gigabit Ethernet», позволяющий использовать саму начинку на максимальных возможностях, избегая при этом узкие места, где скорости канала может не хватить. Также есть возможность объединять их в группы.

Для выполнения проекта нужно произвести установку четырёх брандмауэров в компании.

Таблица 5.1 – Наименование и стоимость оборудования для построения сети

Наименование	Кол–во	Цена, тенге	Стоимость, тенге
ПО OSS	1	25735	25735
DFL–841	4	157000	628000
Лицензия	4	12500	50000

UTP Cat.5E 305м	1	11945	11945
Итого:	10	207180	715680

Общая стоимость оборудования составляет 715680 тенге.

5.5 Финансовый план построения сети

Финансовый план – это часть бизнес–плана, включающая расчёт затрат, эксплуатационных расходов, прибыли, рентабельности, сроков окупаемости.

Цель – максимальная прибыль проекта, при этом надо минимизировать затраты, но также увеличить качество услуг, учитывая цену.

Ниже рассчитывается стоимость внедрения, срок эксплуатации и экономическая эффективность.

5.5.1 Капитальные затраты

Капитальные затраты определим по формуле:

$$К = Ц + К_м + Ку, \quad (5.1)$$

где Ц – цена оборудования сети, тг;

$К_М$ – стоимость рабочих мест в год, тг;

$К_У$ – стоимость монтажа и установки оборудования (5% от стоимости оборудования), тг.

Стоимость оборудования сети составит: Ц = 715680 тенге.

Т а б л и ц а 5.2 – Расчет затрат на организацию рабочего места

Наименование	Цена, тенге	Кол–во	Стоимость, тенге
Компьютер	30537	10	305370
Компьютерный стол	7000	10	70000
Стул	2300	10	23000
Шкаф	11000	2	22000
Итого:	50837	32	420370

Общая стоимость организации рабочего места: 420370 тенге.

Т а б л и ц а 5.3 – Капитальные затраты

Наименование затрат	Стоимость, тенге	Удельный вес, %
Стоимость оборудования,	715680	65,54
Стоимость рабочих мест	420370	33,13

Установка и монтаж оборудования	64529	3,33
Итого	1 200 579	100

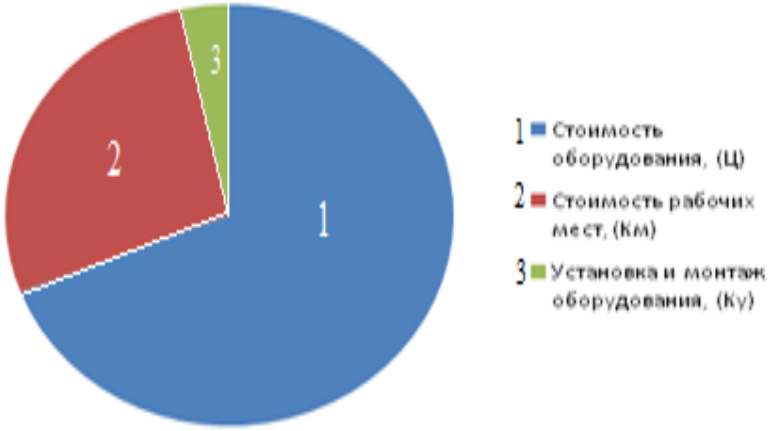

Рисунок 5.1 – Структура капитальных затрат

Рассчитаем капитальные затраты по формуле (5.1):

К =715680 + 420370 + 64529 = 1 200 579 тенге.

5.5.2 Расчет годовых эксплуатационных расходов

Эксплуатационные расходы определим по формуле:

$$Э = ЗП + А + М + С_{ЭЛ} + С_{АДМ}, \quad (5.2)$$

где ЗП – основная и дополнительная заработная плата персонала с отчислением на социальное страхование, пенсионный фонд, тг;

А – амортизационные отчисления, тг;

М – затраты на материалы и запасные части, тг;

$С_{ЭЛ}$ – электроэнергия со стороны производственных нужд, тг;

$С_{АДМ}$– прочие административные управленческие и эксплуатационные расходы, тг.

Для выявления заработной платы в таблице 5.4 приведем среднемесячные оклады обслуживающего персонала.

В годовой фонд заработной платы включается дополнительная заработная плата (работа в праздничные дни, сверхурочные и т.д.) в размере 30% от основной заработной платы.

Т а б л и ц а 5.4 – Среднемесячные оклады обслуживающего персонала

Список персонала	Количество	Ежемесячная з.пл, тенге	З.пл в год, тенге	Всего, тенге

Сетевой админ.	1	40000	480000	480000
Препод.	1	70000	840000	840000
Итого	2	110000	1320000	1320000

Дополнительная заработная плата рассчитывается по формуле:

$$ЗП_{ДОП} = ЗП_{ОСН} \cdot 0.3, \quad (5.3)$$

где $ЗП_{ОСН}$ – годовой фонд основной заработной платы, тенге.

Подставлю значения в (5.3) найдем годовой фонд дополнительной заработной платы:

$$ЗП_{ДОП} = 1320000 \cdot 0.3 = 396000 \text{ тенге}$$

При расчете фонда заработной платы следует учесть премии (15%):

$$П = ЗП_{ОСН} \cdot 0.15 = 1320000 \cdot 0.15 = 198000 \text{ тенге} \quad (5.4)$$

Фонд оплаты труда складывается из основной, дополнительной заработной платы, а также с учетом премий:

$$ФОТ = ЗП_{ОСН} + ЗП_{ДОП} + П \quad (5.5)$$

Определим фонд оплаты труда по формуле (5.5):

$$ФОТ = 1320000 + 396000 + 198000 = 1914000 \text{ тенге.}$$

Социальный налог:

$$Сн = 0.11 \cdot (ФОТ – ФОТ \cdot 0.1) = 0.11 \cdot (1914000 – 1914000 \cdot 0.1) = 189486 \text{ тенге} \quad (5.6)$$

Суммарная заработная плата с учетом отчислений на социальный налог:

$$ЗП = ФОТ + Сн = 1914000 + 189486 = 2103486 \text{ тенге} \quad (5.7)$$

Сумма амортизационных отчислений начисляется по единым нормам, которые устанавливаются в процентах от стоимости основных фондов по формуле:

$$A_0 = \frac{ф \cdot Н_A}{100\%} \quad (5.7)$$

где ф – балансовая стоимость основных фондов, тг;

$Н_А$ – норма амортизационных отчислений.

Найду амортизационные отчисления для оборудования, компьютеров и офисной мебели из (5.7).

Для оборудования для построения сети амортизация составляет 25% от цены оборудования:

$$А_1 = 715680 \cdot 0.25 = 178920 \text{ тенге} \quad (5.8)$$

Амортизация компьютеров составляет 40% от цены:

$$А_2 = 305\,370 \cdot 0.4 = 122148 \text{ тенге} \quad (5.9)$$

Рассчитаю полную амортизацию всех материальных вещей:

$$А = А_1 + А_2 + А_3 = 178920 + 122148 + 20850 = 321918 \text{ тенге} \quad (5.10)$$

Затраты на электроэнергию рассчитаем по следующей формуле:

$$С_{ЭЛ.} = W \cdot Т \cdot S, \quad (5.11)$$

где W– потребляемая мощность, кВт;

Т – количество часов работы, ч/год;

S – стоимость киловатт–часа электроэнергии, тг / квт–час.

Рассчитаем затраты на электроэнергию по формуле (5.11):

$$С_{ЭЛ} = 1.720 \cdot 8760 \cdot 27.05 = 407567 \text{ тенге}$$

Электрическая энергия, потребляемая на прочие нужды, берется в размере 5% от электрической энергии, потребляемой основным оборудованием. Стоимость электроэнергии, потребляемой на прочие нужды по формуле (5.11):

$$С_{ЭЛ.пр} = 407567 \cdot 0{,}05 = 20378 \text{ тенге}$$

Общие затраты на электроэнергию:

$$С_{эл.общ} = С_{эл} + С_{ЭЛ.пр} = 407567 + 20378 = 427945 \text{ тенге} \quad (5.12)$$

Затраты на материалы и запасные части принимают в размере 5% от стоимости системы:

$$М = 715680 \cdot 0.05 = 35784 \text{ тенге} \quad (5.13)$$

Стоимость административных расходов составляет 10% от ФОТ:

$$С_{АДМ} = ФОТ \cdot 10\% = 1914000 \cdot 0.10 = 191400 \text{ тенге} \quad (5.14)$$

Таким образом, эксплуатационные расходы составят:

$$Э = 2103486 + 521643 + 35784 + 427945 + 191400 = 3\,280\,258 \text{ тенге} \quad (5.15)$$

Сведем данные по эксплуатационным расходам в таблицу 5.5 и определим удельный вес каждой статьи расходов.

Т а б л и ц а 5.5 – Эксплуатационные расходы

Статьи эксплуатационных затрат	Стоимость, тенге	Удельный вес, %
Заработная плата персонала	2103486	67.99
Социальные отчисления	521643	16.86
Затраты на материалы и запасные части	35784	1.09
Затраты на электроэнергию	212785	6.88
Административные расходы	191400	6.18
Итого:	3280258	100

5.5.3 Расчет прибыли от внедрения технологии

Внедрение осуществлялось для защиты ЛВС кафедры и проведения коммерческих курсов наладке и эксплуатации устройств линейки NetDefend. Расчёты показали, что реализация является высоко окупаемой.

В будущем планируется ввести платные ежемесячные курсы по эксплуатации оборудования фирмы «D–Link», стоимостью 40 000 тенге со студента. Учитывая, что в одном потоке 8 студентов и в году 12 месяцев, годовой доход от внедрения курсов составит Д = 40 000 · 8 · 12 =3840000 тенге. Кроме того, мы усматриваем дополнительный доход от внедрения нашего проекта в размере 1 000 000 тенге. Всего доход в год составляет 4840000 тенге.

5.5.4 Расчет прибыли и срока окупаемости инвестиций

От прибыли компании также отчисляется подоходный налог, который в РК равен 20%.

Прибыль предприятия до налогообложения.

Доход от основной деятельности определим по формуле:

$$ЧД = Д – Э, \quad (5.16)$$

где Д – годовой доход, тг;

Э – эксплуатационные расходы, тг.

Подставлю значения в формулу (5.16):

$$ЧД = 3\ 880\ 000 – 3\ 280\ 258 = 599742 \text{ тенге}$$

Сумма, отчисляемая на корпоративный подоходный налог с прибыли составит:

$$Н = ЧД \cdot 20\% = 599742 \cdot 0{,}2 = 119948 \text{ тенге} \quad (5.17)$$

Сумма прибыли после налогообложения составит:

$$П = ЧД – Н, \quad (5.18)$$

где Н – корпоративный налог в размере 20% от суммы чистого дохода.

Подставлю значения в формулу (5.18):

$$П = 599742 – 119948 = 479794 \text{ тенге}$$

Определим фонд накопления:

$$ФН = 0.75 \cdot П = = 0{,}75 \cdot 479794 = 359845 \text{ тенге} \quad (5.19)$$

Ожидаемые чистые потоки денежных средств:

$$ОЧПДС = ФН + А = 359845 + 321918 = 681763 \text{ тенге} \quad (5.20)$$

Рентабельность проекта составит:

$$Р = \frac{ОЧПДС}{К} = \frac{681763}{1200579} \cdot 100\% = 56.7\% \quad (5.21)$$

Срок окупаемости – это величина, которая показывает, за какой период будет осуществлён возврат денег, которые были потрачены на организацию предприятия. Срок окупаемости выведем как использование капитальных затрат к чистой прибыли предприятия:

$$T = \frac{К}{ОЧПДС} = \frac{1200579}{681763} = 1.7 \text{ года} \quad (5.22)$$

Таким образом, средства, выложенные в проектирование защищенной корпоративной сети на базе протокола PPTP на канальном уровне, компания вернет вложенные деньги за 1 года и 7 месяцев.

Все экономические показатели по проекту осуществления сети на базе технологии сведем в таблицу 5.6.

Т а б л и ц а 5.6 – Показатели экономической эффективности проекта «Защищенная локальная сеть на базе протокола PPTP канального уровня»

Показатели	Сумма, тенге
Капитальные затраты, тенге	1 200 579
Доход, тенге	3 880 000
Эксплуатационные расходы, тенге	3 280 258
Прибыль до налогообложения, тенге	786157
Коэффициент экономической эффективности (Е)	0.51
Срок окупаемости (Т), мт	1.7

Заключение

В данной дипломной работе рассмотрел протоколы L2TP, PPTP, которые создают тоннель для защиты информации во время передачи между устройствами. Я рассмотрел принципы работы технологий.

Протокол PPTP используется любым оборудованием. Компьютеры, которые функционируют основываня на протоколе PPTP, приобретают высокую скорость, благодаря уменьшению нагрузки на центральыний процессор. PPTP обеспечивает высокую устойчивость к сочетанию с сервером. PPTP является наиболее важным в плане безопасности, т.к. перед передачей данных клиенту необходимо сначала осуществить соединение.

Брандмауэры являются комплексными пакетами для решения задач по предотвращению нелегального доступа, искажения или воровства данных, или другого плохого воздействия, что оказывает воздействие на работоспособность ЛВС.

Все выполненные работы прошли тесты на кафедре и рекомендуются в качестве лабораторных работ.

Вопрос защиты информации в всемирной паутине ставится и, с той или другой степенью действенности, принимается решение с момента появления сетей. Замечаемый в последние годы взрывной прогресс популярности Internet и сопряжённых с ней коммерческих проектов стал толчком с целью формирования технологий защиты информации. К тому же в случае если прежде, главной проблемой защиты в Internet существовало сохранение ресурсов преимущественно от хакерских атак, в таком случае в настоящее время актуальной становится цель защиты коммерческих данных.

Таким способом из проделанного расчета видим, что в период обслуживания кадра увеличивается в зависимости от того используется ли к передаваемой информации шифровка. Так же видно, что при применении протокола PPTP служебный участок кадра возрастает, а информационный участок кадра убавляется. За счет данного повышается численность кадров и повышается время передачи данных.

В разделе безопасность жизнедеятельности проведён анализ условий труда операторов. Сделан расчёт освещения, а так же учтены все требования санитарии и электрической безопасности. В экономической части проделан расчет абсолютнейшей экономической эффективности капитальных вкладов и определён срок окупаемости проекта.

Список литературы

1 Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: 2001.

2 Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3–е изд. – СПб.: Питер, 2011.

3 Сайт http://www.dlink.ru/ru/products/1/1054.html

4 Сайт http://www.wikipedia.org/wiki/l2tp.html

5 Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. 2–е изд. – М: Радио и связь, 2009.

6 Кульгин М. Технологии корпоративных сетей. Энциклопедия. – СПб.: Питер, 2013.

7 Сайт http://www.google.ru/mac.html

8 Сайт http://www.your private network.ru/l2f.html

9 Назаров А.Н., Симонов М.В. Технология высокоскоростных сетей. – М.: Эко–Трендз, 2004.

10 Петренко С.В. Защищенная виртуальная частная сеть: современный взгляд на защиту конфиденциальных данных // Мир Internet. – 2001. – № 2.

11 Левин Л.С., Плотник М.А. Цифровые системы передачи информации.–М.:Радио и связь, 2007.

12 Дюсебаев М. К., Бегимбетова А. С. Методические указания к выпускной работе для студентов всех форм обучения специальностей 050719 – Радиотехника, электроника и телекоммуникации, Алматы: АУЭС, 2008.

13 Маринченко А.В. Безопасность жизнедеятельности: Учебное пособие. – 2–е изд., доп. и перераб. – М.: Издательско–торговая корпорация «Дашков и К», 2007.

14 Кошулько Л.П., Суляева Н.П, Генбач А.А. Производственное освещение. Методические указания к выполнению раздела "Охрана труда" в дипломном проекте. – Алматы, 2011.

15 Базылов К. Б., Алибаева С. А., Бабич А. А. Методические указания по выполнению экономического раздела выпускной работы бакалавров для студентов всех форм обучения специальности 050719 – Радиотехника, электроника и телекоммуникации – Алматы: АУЭС, 2013.

Приложение А

Аутентификация на основе MAC–адресов

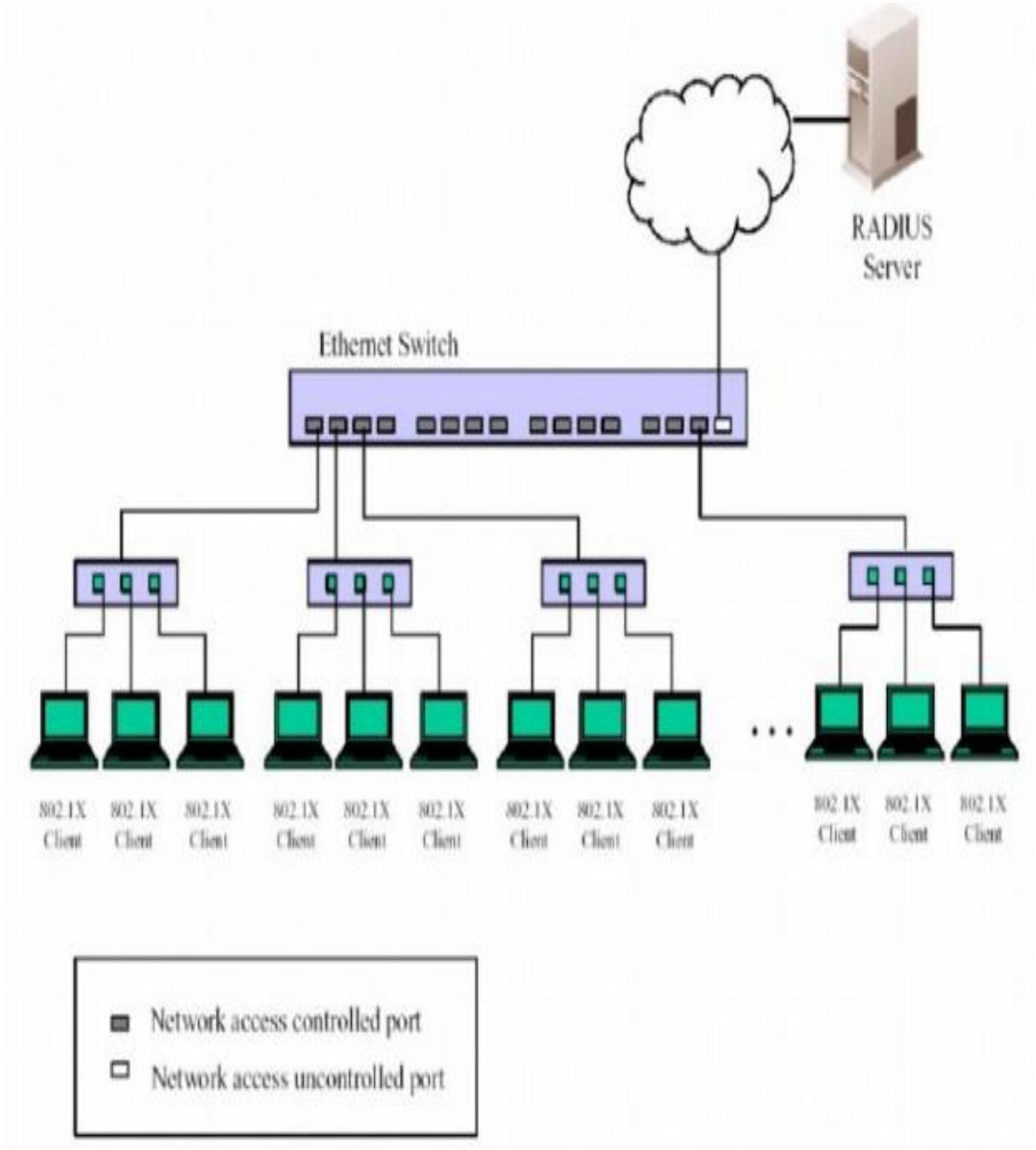

Рисунок А.1 – Схема аутентификации на основе MAC–адресов

Приложение Б

Расчет с помощью программы Mathcad

1. Средняя длина кадра

$Linfomin := 862$ (байт)

$Linfomax := 1362$ (байт)

$$Lkadra := \frac{(Linfomin + Linfomax)}{2}$$

$Lkadra = 1.112 \times 10^{3}$ (байт)

2. Число кадров передоваемых за 1 день

$Q := 4.295 \cdot 10^{9}$ (байт) объем передоваемой информации

$$Nkadrd := \frac{Q}{Lkadra} + 1$$

$$Nkadrd = 3.862 \times 10^{6} \left(\frac{кадр}{день}\right)$$

3. Скорость поступления кадров

$T := 8$ (часов) продолжительность рабочего дня

$$Vobsh := \frac{Nkadrd}{T \cdot 3600}$$

$$Vobsh = 134.111 \left(\frac{кадр}{с}\right)$$

4. Скорость обслуживания кадра

$tobskadra := 4.242 \cdot 10^{-3}$ (с)

$$Vobskadra := \frac{1}{tobskadra}$$

$$Vobskadra = 235.738 \left(\frac{кадр}{с}\right)$$

5. Степень использования канала связи в сети

$$P := \frac{Vobsh}{Vobskadra}$$

$P = 0.569$