МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»
Институт систем управления и информационных технологий
Кафедра систем информационной безопасности

«ДОПУЩЕН К ЗАЩИТЕ»
Зав. кафедрой к.п.н., доцент Р. Ш. Бердибаев
_____ «_____» _____2019 г.
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Построение безопасной корпоративной сети для компании «AGMACSOURCE»
Специальность: «Системы информационной безопасности»
Выполнил: Султанов Нурали Мухтарович Группа СИБ-15-2
Научный руководитель: ст. пр. Ургенишбаев Камал Махамбетович
Консультанты:
по экономической части:
к.э.н., профессор Аренбаева Кс.Г.
(ученая степень, звание, Ф.И.О)
_____ «22» мая 2019 г.
(подпись)
по безопасности жизнедеятельности:
старший преподаватель Бекбасаров Ш.Ш.
(ученая степень, звание, Ф.И.О)
_____ «22» мая 2019 г.
(подпись)
по применению вычислительной техники:
старший преподаватель Ургенишбаев К.М.
(ученая степень, звание, Ф.И.О)
_____ «22» мая 2019 г.
(подпись)
Нормоконтролер:
Ст. преподаватель каф СИБ Аскарова Н.Б.
(ученая степень, звание, Ф.И.О)
_____ «22» 05 2019 г.
(подпись)
Рецензент:
Умирзаков Сырым Бимуратович, упр. директор АО „Казтелеком"
(ученая степень, звание, Ф.И.О)
_____ «23» май 2019 г.
(подпись)

Алматы 2019

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Институт систем управления и информационных технологий

Кафедра систем информационной безопасности

Специальность «Системы информационной безопасности»

ЗАДАНИЕ
на выполнение дипломного проекта

Студенту Султанову Нурали Мухтаровичу

Тема проекта: Построение безопасной корпоративной сети для компании «AGMACSOURCE»

Утверждена приказом по университету №124 от «26» октября 2018 г.

Срок сдачи законченного проекта «_____» _____2019 г.

Исходные данные к проекту (требуемые параметры результатов исследования (проектирования) и исходные данные объекта): проект предполагает построение безопасной корпоративной сети для предприятия. Помимо построения сети необходимо организовать надежную систему защиты. В качестве системы защиты будут использоваться: разделение подсетей на VLAN, правила в межсетевом экране, парольная политика, IDS, Proxy.

Перечень вопросов, подлежащих разработке в дипломном проекте, или краткое содержание дипломного проекта: дипломный проект состоит из 5 глав, разделенных на подглавы, каждая из которых соответствует определенной тематике, необходимой при проектировании безопасной корпоративной сети.

В первой главе дипломного проекта приведены общие понятия, касаемо корпоративных сетей, основные понятия виртуализации, описан принцип работы VLAN и vSwitch, функционал брандмауэров, а также Proxy, IDS, VPN.

Во второй главе дипломного проекта описаны все средства, необходимые для построения корпоративной сети.

В третей главе подробно описан весь процесс разработки, подкрепленный скриншотами.

Четвертая глава посвящена экономической составляющей дипломного проекта, в которой приведено технико-экономическое обоснование, а также все необходимые расчеты.

Пятая глава посвящена расчетам, необходимым для создания вентиляционных условий в помещении, пригодных к комфортной работе специалистов.

Перечень графического материала (с точным указанием обязательных чертежей):

1 принципы работы необходимых составляющих корпоративной сети;

2 интерфейсы всех необходимых средств;

3 структурная схема сети;

4 скриншоты процесса проектирования;

5 скриншоты работоспособности сети.

Основная рекомендуемая литература:

1 Бекишева А.И. Методические указания к выполнению экономической части дипломной работы для бакалавров специальности 5В0703 - Информационные системы – Алматы: АУЭС; 2013. –24 с

2 Хакимжанов Т.Е. Расчет аспирационных систем. Дипломное проектирование. Для студентов всех форм обучения всех специальностей. – Алматы: АУЭС, 2014 – 30 с

3 Корпоративная сеть – от необходимости до реализации URL: https://compress.ru/article.aspx?id=12025

4 Корпоративные сети URL: http://tsput.ru/res/informat/lekts.htm

5 Что такое виртуализация и как работает виртуальный сервер URL: https://habr.com/ru/company/vps_house/blog/344048/

Конструкции по проекту с указанием относящихся к ним разделов проекта

Раздел	Консультант	Сроки	Подпись
Экономика	Арынбаева Ж.Т.	04.03-22.05	
БЖСД	Бекбасаров Ш.Ш.	05.03-12.05	
Вычислит. техника	Уразбаев К.М.	18.03-22.05	
Нормоконтроль	Искакова К.Ж.	15.04-22.05	
Рецензия	Блещинов С.Б.	06.05-13.05	

График
подготовки дипломного проекта

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Определение актуальности темы	22.10.2018	
Анализ предметной области	12.11.2018	
Теоретический материал о корп. сети ЭВМ	04.02.2019	
Теоретический материал о виртуализации	13.02.2019	
Анализ средств безопасности	22.02.2019	
Определение приемлемых решений	05.03.2019	
Структурная схема сети	12.03.2019	
Установка гипервизора	20.03.2019	
Настройка сетевых интерфейсов	25.03.2019	
Установка и настройка межсетевого экрана	01.04.2019	
Настройка сервера	05.04.2019	
NAT и FW Rules	11.04.2019	
Применение средств безопасности	29.04.2019	
Отладка работы сети	05.05.2019	
Тестирование безопасности	05.05.2019	
Анализ проделанной работы	15.05.2019	

Дата выдачи задания «24» февраля 2019 г.

Заведующий кафедрой _____ (_____)
(Подпись) (Ф.И.О)

Научный руководитель проекта _____ (Уренгимбаев К.М.)
(Подпись) (Ф.И.О)

Задание принял к исполнению студент _____ (Султанов К.М.)
(Подпись) (Ф.И.О)

Аннотация

Данный дипломный проект посвящен проектированию безопасной корпоративной сети для ТОО «AGMACSOURCE». В теоретической части описана методика по построению сетей. В практической части реализована модель сети, с применением защитных средств.

В экономической части произведен расчет возможных затрат при разработке дипломного проекта.

В разделе безопасности жизнедеятельности произведен расчет для системы вентиляции в помещении.

Андатпа

Бұл дипломдық жоба «AGMACSOURCE» ЖШС үшін қауіпсіз корпоративті желіні жобалагауға арналған. Теориялық бөлім желілерді құру әдісін сипаттайды. Тәжірибелік бөлімде желілік модель қорғаныс құралдарын пайдалану арқылы жүзеге асырылады

Экономикалық талдау бөлігінде диплом жобасын әзірлеугі құны есептеледі.

Оңтайлы еңбек жағдайын денсаулық сақтау және қауіпсіздік бөлімінде бөлме желдету жүйесі үшін есептеу жургізілді.

Annotation

This thesis project is dedicated to the design of a secure corporate network for «AGMACSOURCE» LLP. The theoretical part describes the method for constructing networks. In the practical part, the network model is implemented using protective equipment.

In the economic part included the calculation of the possible costs in the development of the graduation project.

In the section of life safety were calculated ventilation system in the room.

Содержание

Введение

В наши дни практически любая сфера человеческой жизнедеятельности тесно сопряжена с информационными технологиями. Процесс обмена информацией непрерывен, в данном потоке участвуют как персональные, так и имеющие определенную ценность корпоративные данные. Бизнес и информация – два тесно связанных понятия на любых уровнях, начиная с трансконтинентальных компаний, заканчивая любым индивидуальным предприятием. Информация, которой обладает компания, имеет материальную ценность и требует наличия определенной информационной системы, задача которой – хранение, обработка и защита корпоративных данных. Процесс деятельности предприятия подразумевает наличие определенного количество сотрудников, имеющих различный уровень доступа к корпоративной информации. Возникает необходимость в безопасной локальной корпоративной сети. Данная сеть служит для обеспечения безопасного организованного обмена информации между сотрудниками компании.

Актуальность данной работы заключается в том, чтобы создать безопасную модель корпоративной сети из Opensource средств, тем самым сделать возможным её реализацию практически для любого предприятия. Так, как многие небольшие предприятия являются достаточно уязвимыми, ввиду чрезмерно дорогих методов безопасности сети, а так же недостатка гражданских специалистов в области ИБ, способных самостоятельно реализовать данную модель.

Целью данного проекта является создание модели безопасной корпоративной сети в виртуальном пространстве ESXI 6.7.

Задачи, поставленные мной для достижения цели:

- установка гипервизора ESXI 6.7 на базе VMware Workstation Pro 15;
- создание всех сегментов сети в виртуальном пространстве;
- обеспечение их безопасности;
- тестирование и исправление ошибок;
- рассмотрение БЖД и экономической части;
- анализ выполненной работы.

1 Анализ предметной области

1.1 Основные понятия и определения корпоративной сети

Говоря о корпоративной сети, следует начать с понятия локальной сети. Локальная сеть – это компьютерная сеть, организовывающая доступ к Интернету для нескольких компьютеров, посредством маршрутизаторов, коммутаторов, сетевых адаптеров (рисунок 1.1).

Рисунок 1.1 – LAN

Локальные сети имеют различные способы классификации, один из основных – по способу администрирования. Таким образом, в зависимости от способа организации сети, она может приобретать характер локальной, распределённой, городской или глобальной. Управление сетью или её сегментом осуществляет сетевой администратор. В сложных сетях работу ведёт целая команда администраторов, с разграничением прав и обязанностей.

Организация сети осуществляется благодаря проводным или беспроводным технологиям. Локальные сети могут быть связаны между собой посредством шлюзов, либо иметь подключение к сети Интернет.

Основной способ построения локальных сетей – Ethernet. Ранее применялись и другие технологии, однако их неактуальность не вызывает необходимости даже для их упоминания [1].

Маршрутизация в сетях бывает либо статической, либо динамической. При статической маршруты явно прописываются в процессе конфигурации роутера без применения различных протоколов маршрутизации. В динамической таблица маршрутизации редактируется при помощи протоколов, таких как RIP.

В локальной сети могут быть организованы рабочие группы, объединяющие несколько конкретных компьютеров.

Ошибочным считается мнение, что в локальной сети применяются все уровни модели OSI. Непосредственно в работе LAN необходимыми являются лишь физический и канальный уровни [2].

Важнейшим понятием в локальной сети является адресация. Так, как в своём дипломном проекте я применяю лишь адресацию посредством протокола IPv4, кратко рассмотрим лишь его.

IP-адрес – уникальный сетевой адрес узла, идентифицирующий его в рамках сети. Данный адрес необходим для обращения к конкретному узлу, объекту сети. Он состоит из номера сети и номера узла и выдается администратором, либо же провайдером, если речь заходит о выходе в глобальную сеть. Протокол IPv4 широко используется с 1981 года и включает в себя 4 294 967 296 уникальных 32-битных адресов. Адрес принято обозначать четырьмя десятичными числами, например – 192.168.1.1. Также через дробь принято указывать маску подсети. Маска подсети нужна для определения адресов подсети и узла, но она не входит в IP-пакет. IP-адреса бывают трех классов: A, B и C (рисунок 1.2).

Классы IP-адресов

Класс адреса	Диапазон 1-го октета (десятичное представление)	Биты 1-го октета (зеленые биты не меняются)	Сетевая (С) и узловая (У) части адреса	Маска подсети по умолчанию (в десятичном и двоичном формате)	Число возможных сетей и узлов для каждой сети
A	1 - 127	00000000 - 01111111	С.У.У.У	255.0.0.0 11111111.00000000.00000000.00000000	126 сетей (2^7-2) 16 777 214 узлов для каждой сети (2^24-2)
B	128 - 191	10000000 - 10111111	С.С.У.У	255.255.0.0 11111111.11111111.00000000.00000000	16 382 сетей (2^14-2) 65 534 узла для каждой сети (2^16-2)
C	192 - 223	11000000 - 11011111	С.С.С.У	255.255.255.0 11111111.11111111.11111111.00000000	2 097 150 сетей (2^21-2) 254 узла для каждой сети (2^8-2)

Рисунок 1.2 – классы IP-адресов

Любое предприятие на определенных этапах развития сталкивается с такой проблемой, как необходимость систематизации имеющейся информации и автоматизации производственных процессов. Для решения этой задачи разрабатываются корпоративные сети и системы, позволяющие упорядочить используемые данные (рисунок 1.3).

Рисунок 1.3 – Корпоративная сеть

Корпоративная сеть – структура, функционирующая в рамках непосредственно определенного предприятия или организации. Участниками процессов в данной сети являются исключительно сотрудники предприятия. Структура сети основывается на масштабах и нуждах компании. Первостепенная задача корпоративной сети – эргономичность, поэтому при её построении необходимой мерой является анализ всех внутренних рабочих процессов предприятия. Необдуманное построение сети приводит к неоправданным расходам, а также к неудобствам в ходе её эксплуатации. Данная структура должна включать в себя всё необходимое для удовлетворения потребностей организации, ни больше, ни меньше [3]. После организации, грамотно выстроенной, корпоративной сети, предприятие может поднимать вопросы о необходимости определенной части технического персонала, тем самым обеспечить серьёзную экономию средств, расходуемых для содержания человеческих ресурсов. Часто бывает, что один специалист способен выполнять объём задач, для которых раньше требовалось несколько сотрудников. Также серьёзно повышается эффективность и скорость выполнения различных задач, за счет параллельного выполнения вычислительных процессов. После объединения множества элементов в единую сеть повышается устойчивость к сбоям отдельных элементов системы. Исключается наличие огромного количества задач, нацеленных на один результат. Но одно из самых важных преимуществ – возможность единовременного контроля всех элементов, что колоссально повышает безопасность системы [4].

1.2 Виртуализация

Ключевым понятием данного дипломного проекта является виртуализация, так как вся работа выполняется именно в виртуальном пространстве, причём на нескольких уровнях.

Виртуализация – это процесс создания программного (или виртуального) представления чего-либо, например виртуальных приложений, серверов, хранилищ и сетей. Это единственный и самый эффективный способ сокращения расходов на ИТ-инфраструктуру при одновременном повышении эффективности и адаптивности для компаний любых размеров. Виртуализация считается одним из самых важных открытий в области информационных технологий за последние пол столетия. Виртуальные машины и гипервизоры получили широкое применение и рационализировали работу во многих сферах IT. Пользуясь виртуализацией, мы заставляем программное обеспечение функционировать как аппаратное обеспечение, со значительными преимуществами в адаптивности, стоимости, масштабируемости, гибкости, производительности. Благодаря виртуализации ИТ-отделы выполняют несколько виртуальных систем на одном сервере, что обеспечивает экономию и повышение эффективности.

Виртуальная машина – это строго изолированный контейнер ПО, который содержит в себе операционную систему или приложения. Отдельная виртуальная машина независима от других. Наличие множества ВМ на одном компьютере организовывает работу нескольких операционных систем и приложений на одном физическом сервере. Гипервизор отделяет виртуальные машины от сервера и при необходимости выделяет вычислительные ресурсы виртуальной машине в динамическом порядке [5].

Виртуальные машины обеспечивают дополнительную безопасность, целостность и удобство, ввиду отсутствия необходимости в больних вычислительных затратах. Также можно расширить возможности виртуальных машин, с добавлением функции эмуляторов для интерпретаторов и функции полных симуляторов.

Главный принцип заключается в том, что программное обеспечение, функционирующее в виртуальных машинах, не знает об этом факте – даже гостевая операционная система, изначально созданная для работы на железе, считает, что это ее «аппаратная» платформа.

Подытожим основные характеристики виртуальных машин:

- выполнение нескольких операционных систем на одном физическом компьютере;
- распределение системных ресурсов между виртуальными машинами;
- изоляция неисправностей и нарушений системы безопасности на аппаратном уровне;
- сохранение уровня производительности с помощью расширенных средств управления ресурсами;
- сохранение состояния виртуальной машины полностью в виде файлов;
- перемещение и копирование виртуальных машин аналогичны операциям с файлами;
- независимость от оборудования;
- инициализация на любом физическом сервере и перенос на любой сервер для всех виртуальных машин.

Также, виртуализацию можно разделить на 2 типа: аппаратную и программную. Следуя названию, аппаратная виртуализация работает при поддержке со стороны процессора. В отличие от программной виртуализации, гостевые ОС управляются гипервизором напрямую. Аппаратная виртуализация считается намного эффективнее программной, поскольку гипервизор, создает минимальные накладные расходы [6].

Виртуальная память является не менее важным понятием, чем виртуальные машины. Виртуальная память организуется благодаря функционалу относительно небольших дополнений к аппаратным средствам и наборам команд для включения частей хранилища, которые называют сегментами. Её концепция привела к созданию облачных хранилищ. Виртуализация и облачные вычисления – тесные, но не взаимозаменяемые понятия. Средства виртуализации – это программное обеспечение, которое делает возможной независимость вычислительных сред от физической

инфраструктуры, а облачные вычисления – это службы, предоставляющие общие вычислительные ресурсы (рисунок 1.4). Эти технологии дополняют друг друга, поэтому организации могут начать виртуализацию серверов и затем перейти к облачным вычислениям для достижения еще большей адаптивности и расширения возможностей самообслуживания. Капитальные затраты, простои из-за сбоев, экономия на физическом пространстве, техническое обслуживание, серьезные проблемы с производительностью и отключениями, трудоемкие затраты на устранение неполадок, а также многие дополнительные затраты могут окупаться сервисными решениями, хранимыми в облаке.

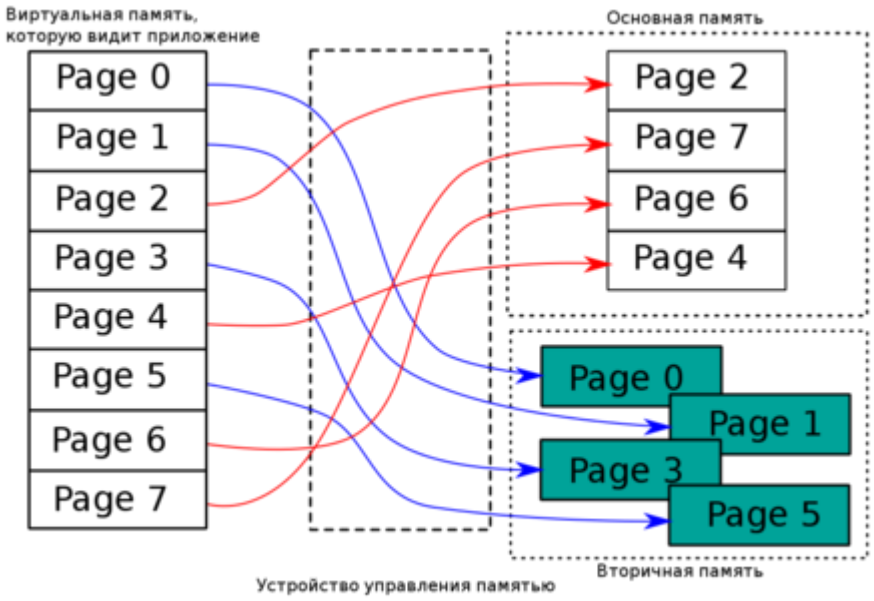


Рисунок 1.4 – Принцип работы виртуальной памяти

1.3 VLAN и vSwitch

VLAN – это функция в роутерах и коммутаторах, позволяющая на одном физическом сетевом интерфейсе создать несколько виртуальных локальных сетей. VLAN используется при создании логической топологии сети, не зависящей от физической топологии. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет узлам группироваться, даже если они не находятся в единой физической сети. Данная процедура может быть выполнена на основе программного обеспечения. VLAN используется при сокращении широковещательного трафика в сети. Широко применяются точки зрения безопасности, например как средство борьбы с переполнением CAM-таблицы.

VLAN необходим для гибкого разделения устройств на группы. Как правило, одному VLAN соответствует одна подсеть. Устройства, находящиеся в разных VLAN, будут находиться в разных подсетях. Но в то же время VLAN не привязан к местоположению устройств и поэтому устройства, находящиеся

на расстоянии друг от друга, все равно могут быть в одном VLAN независимо от местоположения [7].

При передачи трафика в сеть, компьютер даже не догадывается, в каком VLAN'е он находится. В этих целях используется коммутатор (рисунок 1.5). Коммутатор знает, что компьютер, подключенный к определённому порту, находится в соответствующем VLAN'е. Трафик, приходящий на порт определённого VLAN'а, ничем не отличается от трафика из другого VLAN'а. Другими словами, никакой информации о принадлежности трафика к определённому VLAN'у нет. Следовательно, если через порт приходит трафик разных VLAN'ов, коммутатор должен его различать. Для этого каждый кадр трафика должен быть помечен определенным образом. Пометка должна говорить о том, какому VLAN'у трафик принадлежит. Данный процесс называется тегированием трафика VLAN.

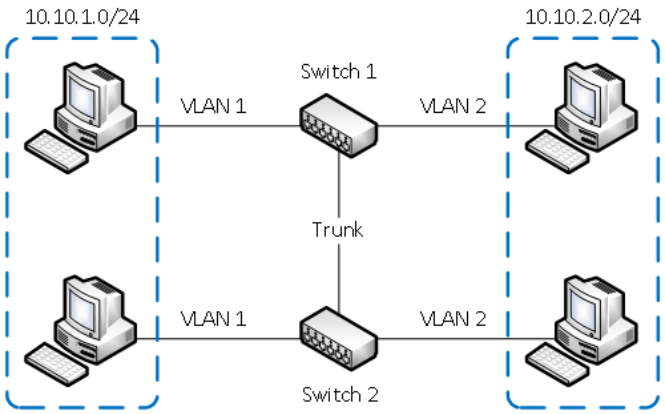


Рисунок 1.5 – Принцип работы VLAN

vSwitch – виртуальный коммутатор, предназначенный для работы в гипервизорах и на компьютерах с виртуальными машинами (рисунок 1.6). vSwitch бывает двух типов – Standard vSwitch, и vNetwork Distributed vSwitch (vDS). Мы будем рассматривать Standard vSwitch. vSwitch работает под управлением гипервизора (vmkernel) и отвечает за все сетевые операции хоста, в том числе он обеспечивает прохождение управляющего трафика. Все сетевые компоненты хоста подключаются к vSwitch посредством портгрупп. В отличие от физического, виртуальный коммутатор не изучает MAC адреса из проходящего трафика и не может создавать сетевую петлю. Виртуальный коммутатор обрабатывает управляющий, сетевой и трафик между вертуальной машиной и сетевыми устройствами.

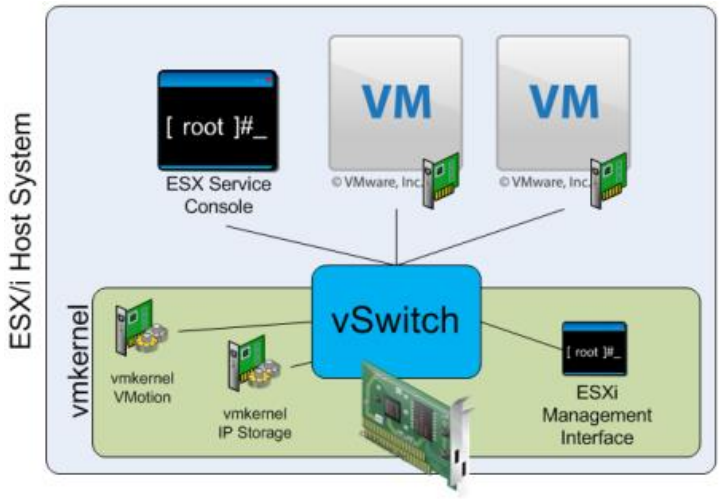


Рисунок 1.6 – принцип работы vSwitch

Допускается возможность использование нескольких коммутаторов для разделения трафика. Виртуальные машины, подключенные к разным виртуальным коммутатором на одном хосте, взаимодействуют через внешнюю сеть. Прямое соединение vSwitch между собой является невозможным, что и предотвращает появление петель. Как и физический, виртуальный коммутатор относится к устройствам второго уровня. Он отвечает за доставку пакетов, но не может организовывать маршрутизацию. Также от физического коммутатора существует отличие в том, что vSwitch обеспечивает отказоустойчивость сетевого соединения. Поддерживается три режима работы с VLAN [8].

Virtual Guest Tagging (VGT) – сетевые пакеты пересылаются виртуальной машине через vSwitch в нетронутом виде, вместе тэгами. Для включения данного режима необходимо указать VLAN ID = 4095 в свойствах портгруппы.

External Switch Tagging (EST) – этот метод наболее распространен в физических сетях. VLAN тэги добавляются и обрезаются при передаче трафика на физическом коммутаторе, поэтому пакет, достигший сервера, уже не будет иметь никакого тэга.

Virtual Switch Tagging (VST) – этот метод распространен в виртуальных инфраструктурах. В режиме VST VLAN тэги обрабатываются на vSwitch, а гостевая ОС работает с нетэгированным трафиком.

1.4 Межсетевой экран

Межсетевой экран (брандмауэр, firewall) – программный или программно-аппаратный комплекс, контролирующий и фильтрующий весь проходящий через него трафик, ссылаясь на заданные правила.

Применяется для защиты отдельных сегментов сети или хостов от возможного несанкционированного проникновения посредством уязвимости

ПО, функционирующего на ПК, или протоколов сети. Функция межсетевого крана заключается в сигнатурном сравнении проходящего трафика.

Наиболее частое расположение фаерволла – граница периметра локальной сети для защиты внутренних узлов (рисунок 1.7). Однако, атаки могут быть реализованы изнутри, поэтому при атаке на элемент той же сети, брандмауэр реагировать не будет. Данный факт привел к тому, что сетевые экраны стали устанавливать не только на границе сети, но и между её сегментами, в целях повышения безопасности [9].

Создание межсетевых экранов началось в 80-х годах, в период отсутствия интернета у большинства пользователей компьютеров. Их функцию выполняли роутеры, занимавшиеся анализом трафика на основе данных из протокола сетевого уровня. После, с развитием сетевых технологий, маршрутизаторы смогли использовать данные уже транспортного уровня. По своей сути, роутер представляет собой первую в мире реализацию программно-аппаратного фаерволла.

Программные межсетевые экраны появились намного позже. Netfilter/iptables, фаерволл экран для Linux, был создан лишь в 1998 году. Это связано с тем, что ранее функцию брандмауэра выполняли антивирусные программы, но с конца 90-х вирусы стали массивнее, и появление межсетевого экрана стало необходимым.

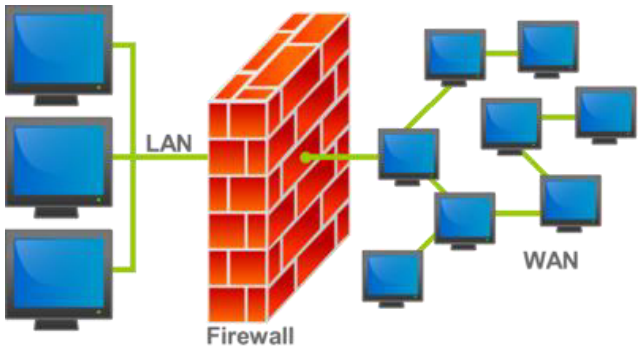


Рисунок 1.7 – Межсетевой экран на границе периметра

Трафик фильтруется в соответствии с заданными правилами – ruleset. По своей сути, фаерволл является последовательностью анализирующих и обрабатываемых трафик фильтров. У каждого фильтра своё назначение; причём, последовательность правил кардинально влияет на работу экрана. Например, большинство межсетевых экранов во время анализа трафика последовательно сравнивают его с сигнатурами – следовательно, наиболее популярные должны располагаться как можно выше.

Принципов, по которым осуществляется обработка входящего трафика, всего два: «всё, что не запрещено – разрешено» и «разрешено только то, что не запрещено».

Фаерволл выполняет две функции: deny, запрет данных – и allow – разрешение на дальнейшую передачу пакета. Некоторые брандмауэры

способны также выполнять функцию reject – запретить трафик, но сообщить отправителю о невозможности действия, чего не возникает при выполнении операции deny, обеспечивающей таким образом повышенную защиту узла.

Межсетевые экраны могут быть либо программно-аппаратными, ибо программными. Первые реализованы в виде отдельного модуля в маршрутизаторе или коммутаторе или специального устройства.

Среди пользователей более распространены программные межсетевые экран, поскольку, для их использования необходима лишь установка специального софта. Однако, требования к машине, предполагаемой под установку фаерволла, довольно высоки.

Именно поэтому в крупных компаниях предпочитают установку специализированных программно-аппаратных комплексов, получивших название «security appliance». Работают они чаще всего на основе систем Linux или же FreeBSD, ограниченных функционалом для выполнения заданной функции. Также, на сегодняшний день существуют Next Generation Firewall`ы, в которых исправлена большая часть недостатков обычных межсетевых экранов [10].

1.5 Proxy, IDS/IPS, VPN

Прокси-сервер – промежуточный сервер в компьютерных сетях, исполняющий роль посредника между хостом и целевым сервером позволяющий клиентам как выполнять запросы, так и получать ответы (рисунок 1.8). Клиент осуществляет подключение к прокси-серверу и отправляет запрос на определенный ресурс, расположенный на другом сервере. Далее прокси-сервер либо запрашивает ресурс у указанного сервера и получает его, либо возвращает ресурс из своего кэша. В некоторых случаях запрос клиента или ответ сервера может быть заменён прокси-сервером в определённых целях. Прокси-сервер помогает защищать компьютер от определенных сетевых атак и помогает сохранять анонимность клиента, но также может использоваться злоумышленниками для скрытия адреса сайта, уличённого в мошенничестве, изменения содержимого целевого сайта (подмена), а также перехвата запросов самого пользователя.

Способы применения прокси-серверов:

- организация доступа компьютеров локальной сети к интернету;
- кэширование данных;
- сжатие данных;.
- защита локальной сети от внешнего доступа;
- ограничение доступа из локальной сети к внешней;
- анонимизация доступа к различным ресурсам;
- обход ограничений доступа.

Прокси сервера бывают двух видов – прозрачные и обратные. При прозрачном прокси нет необходимости использовать различные расширения браузера, или приложения. Достаточно просто прописать маршрут на своём роутере. Обратный прокси перенаправляет клиентские запросы из внешней

сети на внутренние сервера. Используется для снижения нагрузки, безопасности, а иногда и в качестве межсетевого экрана.

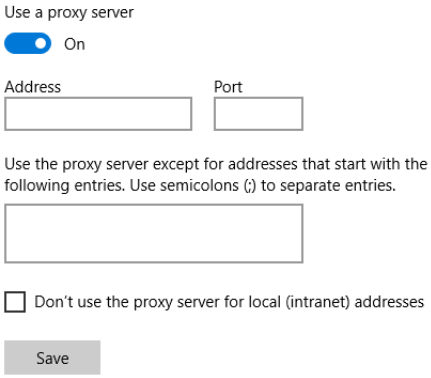


Рисунок 1.8 – Прокси в Windows 10

IDS (Intrusion Detection System) – это программное или программно-аппаратное средство, необходимое для выявления фактов НСД в локальную сеть. IDS анализируют сетевой трафик информационной среды. В случае обнаружения нелегитимных действий, системы обнаружения вторжений осуществляют идентификацию угрозы и оповещение администратора о попытках вторжения. Системы обнаружения вторжений обнаруживают и распознают различные типы вредоносного кода и ПО (трояны, черви, вирусы, сигнатуры атак на уязвимые сервисы и т.д.).

IPS (Intrusion Prevention System) можно считать дополнением к IDS, так как задача обнаружения вторжений сохраняется, однако помимо оповещения администратора, данная система способна сама предотвращать различные типы атак в реальном времени.

Структура IDS/IPS состоит из:

- подсистемы сенсоров, предназначенной для сбора событий на разных участках защищаемой системы;
- подсистемы анализа, предназначенной для выявления и классификации атак и подозрительных действий на основе данных сенсоров;
- хранилища, обеспечивающего накопление первичных событий и результатов анализа;
- консоли управления, позволяющей конфигурировать IDS, наблюдать за состоянием защищаемой системы, просматривать отчеты о выявленных подсистемой анализа инцидентах.

Существует два основных подхода к обнаружению вторжений – сигнатурный и поведенческий.

Сигнатурный анализ трафика в IDS/IPS аналогичен принципу работы многих антивирусов. Сетевой трафик проверяется и сравнивается с базой сигнатур, в которой хранится информация о вредоносном коде, если в трафике обнаруживается соответствие, система срабатывает.

Поведенческий анализ заключается в том, что включенная в сеть IDS/IPS исследует нормальное поведение и функционирование пользователей

и приложений в сети, и затем, на основании построенной модели система обнаруживает некорректное и аномальное поведение пользователей либо приложений.

VPN (Virtual Private Network) – технология, позволяющая обеспечить одно или несколько сетевых соединений поверх другой сети. Проще говоря, становится возможным узлу одной сети приобретать адрес любой другой сети, при наличии соответствующего клиента. В корпоративной сети данная технология крайне необходима для реализации деятельности сотрудником в рабочей сети, в независимости от его местонахождения.

Обычно VPN разворачивают на уровнях не выше сетевого, так как применение криптографии на этих уровнях позволяет использовать в нетронутом виде транспортные протоколы (такие как TCP, UDP).

При определенном уровне реализации и использовании специального ПО, сеть VPN может обеспечивать высокий уровень шифрования передаваемой информации. При должной настройке всех составляющих технология VPN обеспечивает анонимность в Сети (рисунок 1.9).

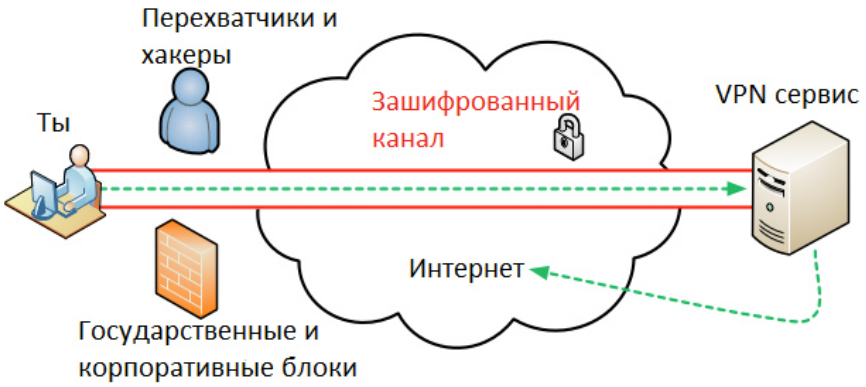


Рисунок 1.9 – Принцип работы VPN

Вывод

В данной главе я рассмотрел основные понятия, касаемые корпоративной сети. Обосновал рациональность и необходимость наличия корпоративной сети на предприятиях/организациях. Описал классификации сетей, способы их организации и преимущества. При построении корпоративной сети необходимо проанализировать потребности конечного предприятия и грамотно подобрать средства для её реализации.

Разумно построить данную модель, пользуясь технологиями виртуализации. Во-первых, нет необходимости в дорогостоящем оборудовании и помещении, для выполнения достаточно лишь одной рабочей станции, обладающей достаточным количеством оперативной памяти. Во-вторых, нет никаких трудностей в случае ошибок в процессе создания, любое действие можно с лёгкостью «откатить».

Говоря о корпоративной сети, невозможно избежать понятия VLAN. Поскольку, в структуре, предполагающей множество компонентов, необходимых для определённого рода группировки, никак не обойтись без подобного разделения, что делает очень удобным мониторинг и управление трафиком между определёнными подсетями.

Для вышеописанных действий в корпоративной сети необходимо наличие межсетевого экрана. Межсетевой экран берёт на себя огромный спектр обязанностей – разделение на подсети, адресация, маршрутизация, доступ к интернету, мониторинг, журналирование, средства безопасности. К необходимым средствам безопасности относятся IDS, Proxy и VPN.

2 Анализ используемых средств и ПО

2.1 VMware Workstation Pro 15 и VMware ESXI 6.7

VMware Workstation – программное обеспечение виртуализации, предназначенное для компьютеров с операционными системами Windows и Linux (рисунок 2.1). Позволяет пользователям устанавливать одну или более виртуальных машин на один физический ПК и запускать их параллельно с ним. На каждую виртуальную машину можно загрузить свою операционную систему. VMware Workstation разработана и продается компанией VMware, подразделением EMC Corporation.

VMware Workstation поддерживает разные типы соединения с сетевым интерфейсом физического компьютера, а также создание общих директорий с виртуальной машиной. ПО может монтировать реальные CD или DVD диски или ISO образы в виртуальные приводы, при этом виртуальная машина будет считать приводы настоящими. Также программа хранит виртуальные жесткие диски в формате .vmdk.

VMware Workstation имеет функцию сохранения текущего состояние виртуальной машины (snapshot). Пользователь может в любой момент вернуться в сохраненное ранее состояние.

VMware Workstation имеет возможность объединять несколько виртуальных машин в группу, которой можно управлять как единым объектом.

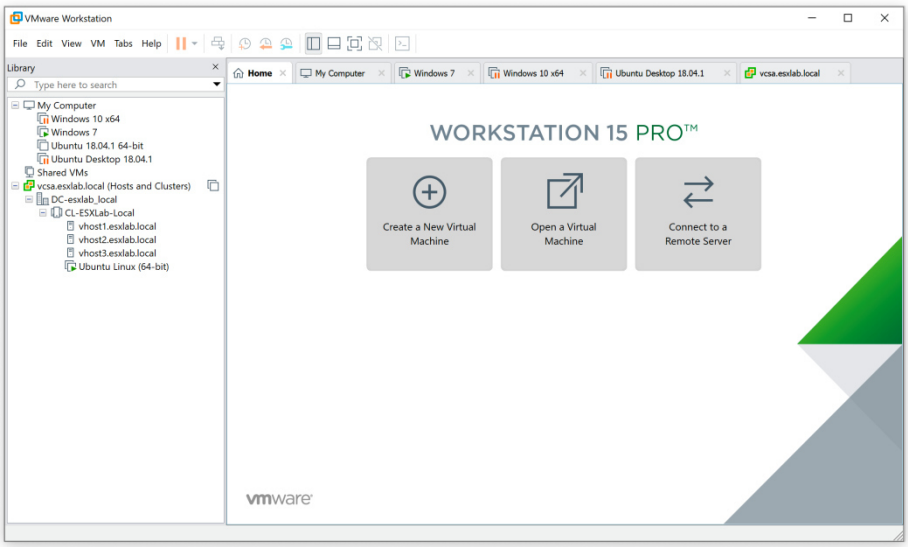


Рисунок 2.1 – Интерфейс VMware Workstation PRO 15

VMware ESXI – программное обеспечение для виртуализации уровня предприятия, разработанное все той же компанией Vmware (рисунок 2.2). ESXI является встроенным гипервизором и устанавливается непосредственно

на «голое железо», то есть при установке не требует наличия на машине установленной ОС.

ESXi позволяет распределить ресурсы физической машины на логические разделы, именуемые виртуальными машинами. Объединяет в себе средства управления виртуальными машинами и ресурсами. Обозначает определённый набор требований к аппаратному обеспечению – например, является обязательным наличие поддержки виртуализации со стороны материнской платы и процессора. ESXI требует не менее 4 ГБ ОЗУ.

Гипервизор VMware ESXI, по своей сути, является огромным виртуальным пространством, ограниченным лишь производительностью «железа», на которое он будет устанавливаться. Данное пространство можно заполнять множеством виртуальных машин и объедеить их в одну сеть. В ESXI предусмотрен виртуальный коммутатор для объединения машин через портгруппы. Также виртуально можно добавлять новые сетевые интерфейсы, по мере необходимости, что является очень полезным при построении корпоративных сетей. Установив на гипервизор межсетевой экран, серверные и клиентские машины, разбив их на отдельные сегменты можно добиться создания правдоподобной модели корпоративной сети.

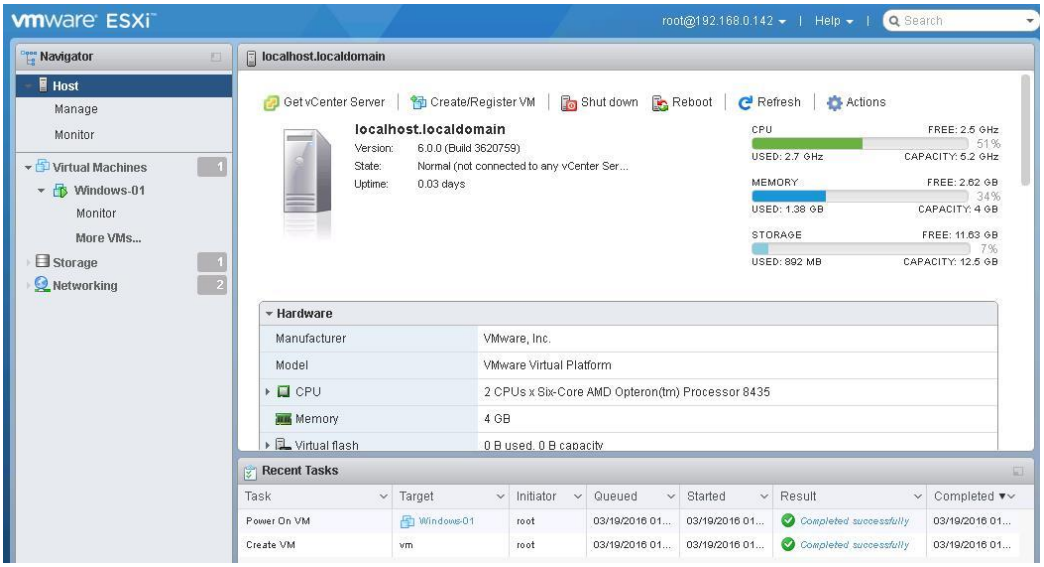


Рисунок 2.2 – Интерфейс VMware ESXI 6.7

2.2 Операционные системы

Windows 7 – пользовательская ОС семейства Windows NT компании Microsoft (рисунок 2.3). Поступила в продажу в 2009 году, на момент 2019 года всё еще сохраняет популярность – составляет почти 20% среди используемых операционных систем во всём мире. Имеет довольно тесную интеграцию с производителями драйверов. Большинство драйверов определяются в автоматическом порядке. Имеет очень удобный интерфейс, высокую степень безопасности системы, а также оказывает относительно

небольшую нагрузку на аппаратную составляющую компьютера. Отличный вариант для клиентской машины в рамках модели корпоративной сети.

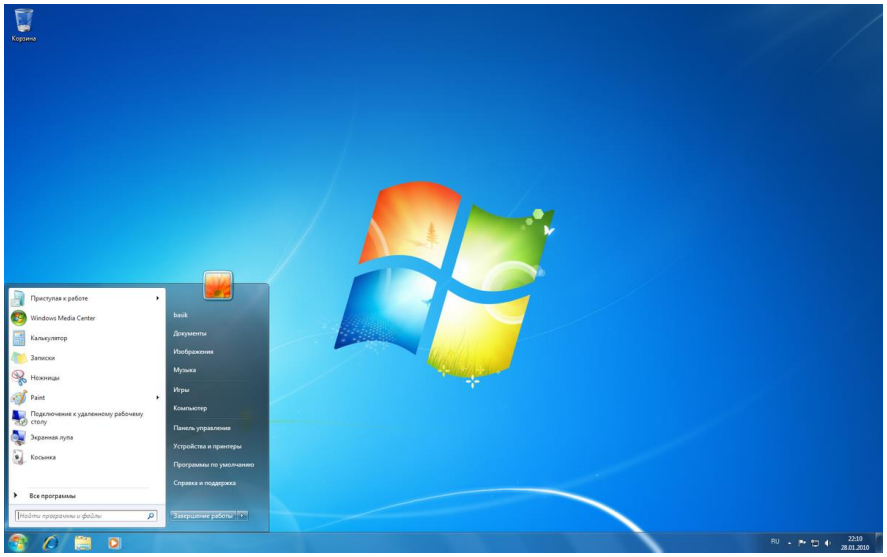


Рисунок 2.3 – Windows 7

Windows Server – серверная операционная система, используемая во многих центрах обработки данных, предоставляющая широкий набор возможностей предприятиям любого размера по всему миру (рисунок 2.4). В Windows Server 2012 реализованы весомые инновации в области виртуализации, сетевых технологий, систем хранения данных и удобства работы.

Данная ОС обеспечивает реализацию комплексного подхода к решению задач современного бизнеса в сфере информационных технологий. Дает возможность эффективно использовать современные бизнес-приложения независимо от их размещения. Windows Server 2012 содержит в себе весь необходимый набор новейших технологий для создания простой и эффективной серверной платформы, обеспечивает необходимую гибкость выбора стратегии использования и развития ИТ-инфраструктуры. С ней организация может увеличивать эффективность уже имеющихся средств, расширить их функционал за счет новых технологий.

Использование Windows Server 2012 позволяет создать высокодоступную мультисерверную платформу с высокой степенью автоматизации и простым управлением без ощутимых финансовых вложений. Windows Server 2012 – крайне универсальная, масштабируемая и эластичная платформа для приложений и web.

Данная операционная система – универсальный и незаменимый инструмент системного администратора. В её рамках может быть реализовано огромное количество серверов – DNS, DHCP, FTP, LDAP, RADIUS и другие. Важнейший плюс – удобство в администрировании всех вышеперечисленных серверов и возможность значительно сократить человеческие ресурсы на одной позиции.

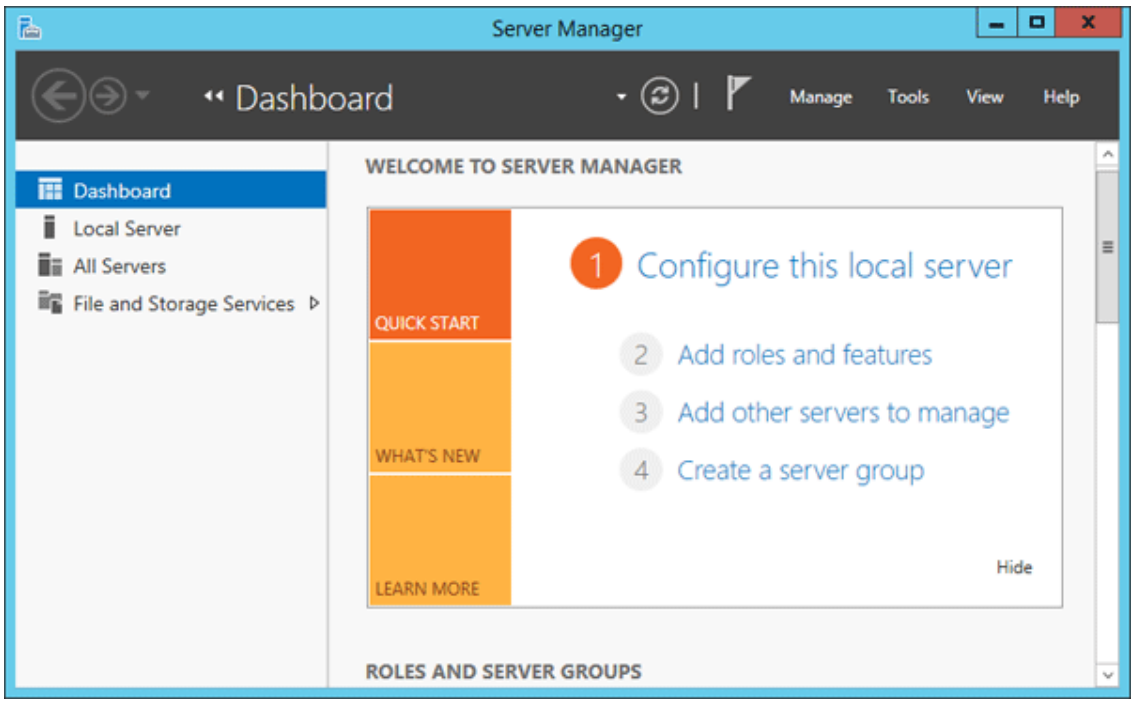


Рисунок 2.4 – Server Manager в Windows Server 2012

2.3 Межсетевой экран pfSense

pfSense – дистрибутив для создания межсетевого экрана или маршрутизатора, основанный на FreeBSD (рисунок 2.5). pfSense предназначен для установки на персональный компьютер, является самым популярным open source решением за счет своего функционала, почти не уступающего дорогим коммерческим межсетевым экранам. pfSense основан на ядре FreeBSD, но не требует каких-либо знаний и умений, специфичных для данной ОС. Практически весь обширный функционал реализован через веб-интерфейс. Поддерживаются следующие возможности:

- стандартная фильтрация на основе адресов и портов источника/назначения;
- фильтрация на основе фингерпринтинга ОС, с которой устанавливается соединение;
- прозрачный брандмауэр второго уровня;
- нормализация пакетов – отбрасывание пакетов с неправильно сформированными полями, которые могут, в принципе, быть и специфическим путем атаки;
- поддержка состояния соединений;
- гибкая поддержка NAT;
- VPN – поддерживаются IPSec, PPTP и OpenVPN;
- мониторинг и статистика. Рисование графиков с помощью RRD и в реальном времени;
- множество DDNS-сервисов.

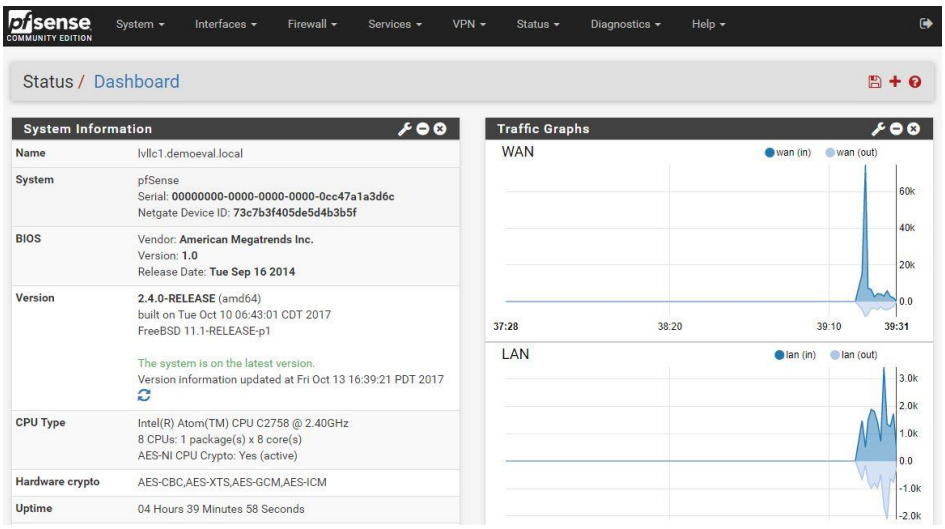


Рисунок 2.5 – Интерфейс pfSense

В меню System находятся такие вещи, как обновление, общие настройки систем, управление сертификатами и пользователями. Также в меню System есть возможность установки дополнительных пакетов.

В меню Interfaces можно управлять сетевыми интерфейсами – задавать им алиасы, управлять типом выделения адреса.

В меню брандмауэра (Firewall) находятся настройки NAT, алиасов для адресов и портов, шейпинга трафика, включения правил по расписанию и сами правила. Правила обрабатываются до первого соответствия, то есть, например, если первым поставить правило, запрещающее всё, все остальные правила не отработают. В pfSense реализовано создание правил на основе состояния соединений, и фильтрация на основе TCP-флагов.

Меню Services предоставляет доступ к настройкам различных сервисов – например DHCP, Dynamic DNS, NTP. VPN – настройка всевозможных видов VPN - IPSec, PPTP, L2TP и OpenVPN. В меню Status отображается состояние и статистика различных подсистем, графики RRD и логи. В Diagnostics можно проводить не только диагностические действия, но и, например, останавливать/перезагружать систему, редактировать файлы. Здесь имеется даже возможность выполнять команды оболочки.

2.4 Squid и Snort

Squid – программное обеспечение, реализующее функцию кэширующего прокси-сервера. Является open source программой. Используется в UNIX-подобных системах и в ОС Windows. Имеет возможность синхронизации с Active Directory Windows Server путём аутентификации через LDAP, что позволяет использовать разграничения доступа к интернет ресурсам у пользователей сети.

Входит в пакет расширений к фаерволлу pfSense. В рамках корпоративной сети необходим для экономии трафика, засчет кэширования веб-страниц, то есть, если один из пользователей сети загрузил веб-страницу, то при обращении к ней со стороны других пользователей им будет

возвращаться сохраненная страница из кэша (рисунок 2.6). Дает возможность мониторинга ресурсов, которые посещают сотрудники, ограничения доступа к страницам и мониторинг длительности сессии для каждого из пользователей по его IP-адресу.

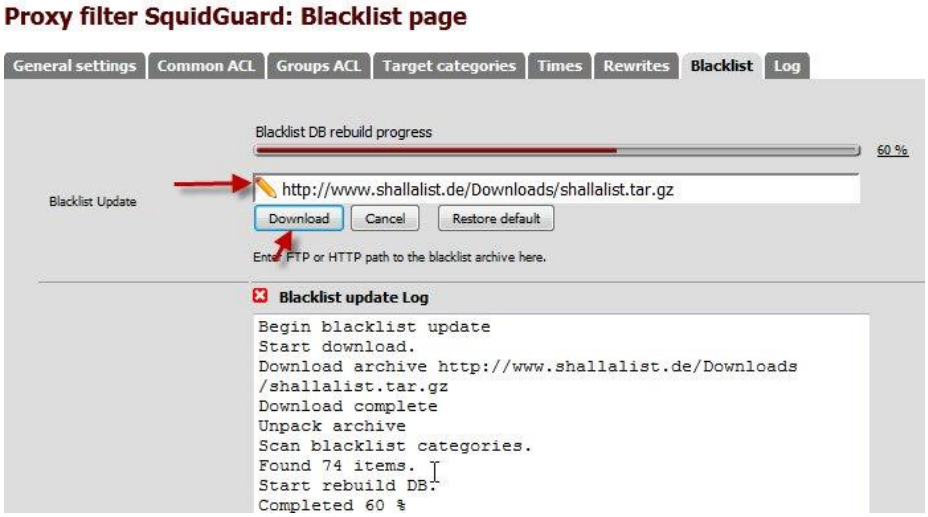


Рисунок 2.6 – Фильтрация в squid в рамках pfSense

Snort – это open source система обнаружения вторжений, IDS (рисунок 2.7). Она может работать в режиме сниффера или логгера, но самое главное, в режиме IDS. В таком режиме Snort проверяет все принимаемые пакеты на признаки известных видов сетевых атак (DDoS, сканирование портов, брутфорс и так далее).

Приведем пример: владельцы магазинов устанавливают камеры, как охранные меры, чтобы обезопасить себя от кражи. Однако они не могут помешать вскрыть замки, но фиксируют действия злоумышленников и помогут в их поимке. Примерно так же работают системы обнаружения вторжений. Они не могут предотвратить нападение, но оповещают об атаке и помогают в расследовании инцидентов.

Одни из главных преимуществ Snort:

- простота в написании своих правил;
- хорошая поддержка с информативной почтовой рассылкой;
- частые обновления.

Еще один огромный плюс данной IDS в том, что на данный момент продукт принадлежит компании Cisco. Данный факт говорит о том, что Snort действительно можно доверять.

В нашей модели корпоративной сети Snort – незаменимый компонент, поскольку обеспечивает высокую вероятность обнаружения атак и входит в набор пакетов pfSense. Он содержит в себе огромное количество готовых правил против разных видов сетевых атак, что существенно облегчает задачу администратора, поскольку вручную ничего прописывать не надо.

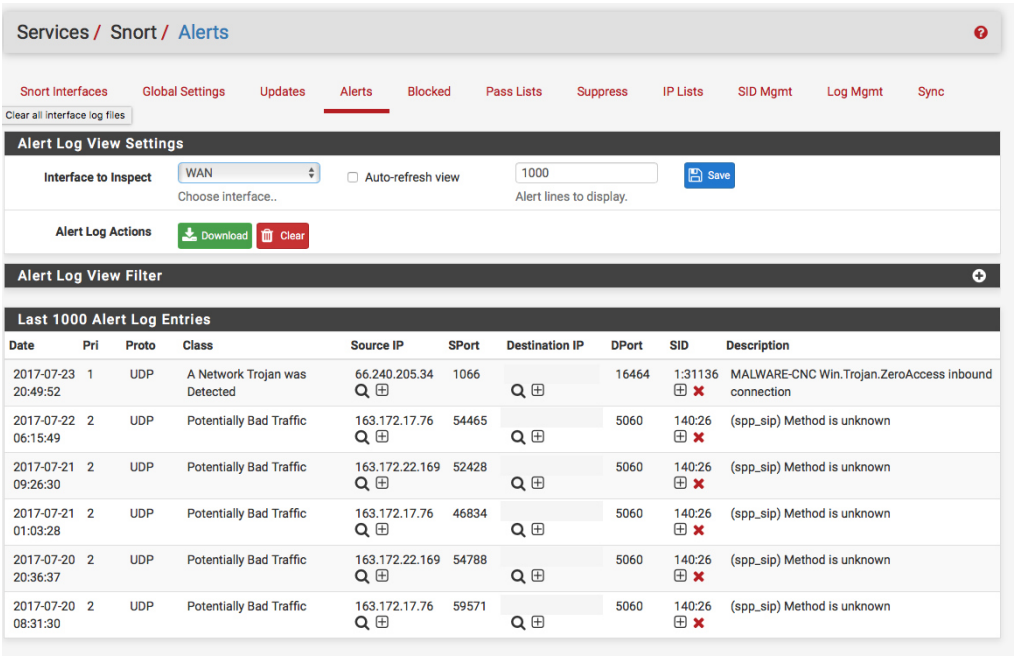


Рисунок 2.7 – Snort в pfSense

Вывод

В данной главе я рассмотрел средства и программные продукты, используемые мной в своем дипломном проекте и обосновал свой выбор. Поскольку для выполнения проекта намного целесообразнее пользоваться виртуальными машинами, гипервизор будет установлен на VMware Workstation. Гипервизоре VMware ESXI среди своих аналогов является наиболее релевантным выбором, поскольку он достаточно понятен в использовании, а его распространенность, в случае затруднительных моментов позволяет найти необходимое решение проблемы в сети Интернет. В качестве клиентской машины Windows 7 обеспечит удобство в интерфейсе и минимальные затраты на производительность, что имеет огромную степень важности для аппаратной составляющей. Когда речь заходит о корпоративной сети для предприятия, в штате которого множество сотрудников, необходимым является доменная структура Active Directory, DHCP-сервер и другое. Для этих целей нужна машина с ОС Windows Server 2012, потому что она включает в себя все эти необходимые компоненты, а также понятна и удобна в использовании.

В корпоративной сети необходимо обеспечить маршрутизацию и контролировать весь внутренний и внешний трафик. Для этой задачи необходимо лишь грамотно составить набор правил в межсетевом экране. pfSense является наиболее популярным open source решением благодаря широкому функционалу, едва ли не уступающему платным корпоративным фаерволлам. В него входят необходимые средства безопасности – прокси Squid и IDS Snort.

3 Практическая часть

Первым шагом при проектировании является создание виртуальной машины под гипервизор ESXI 6.7. Приоритетным параметром для данной машины является объём оперативной памяти. В моем случае – 8 Гб (рисунок 3.1).

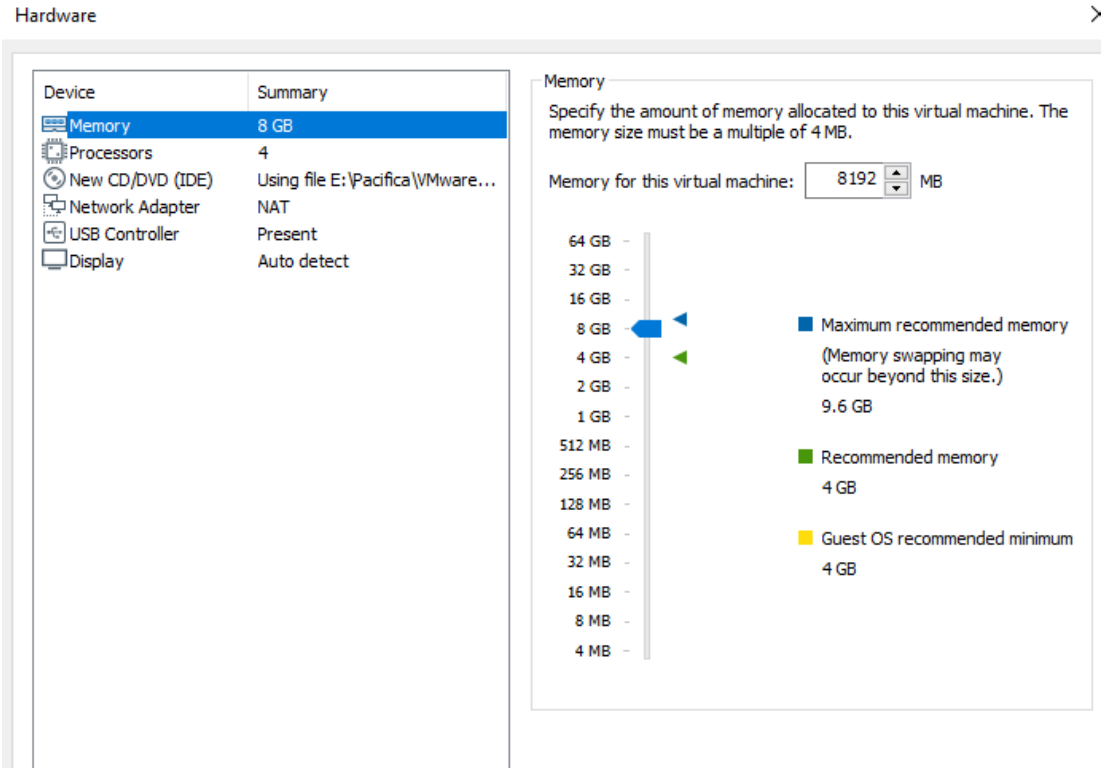


Рисунок 3.1 – Создание виртуальной машины

Далее происходит установка самого гипервизора (рисунок 3.2).

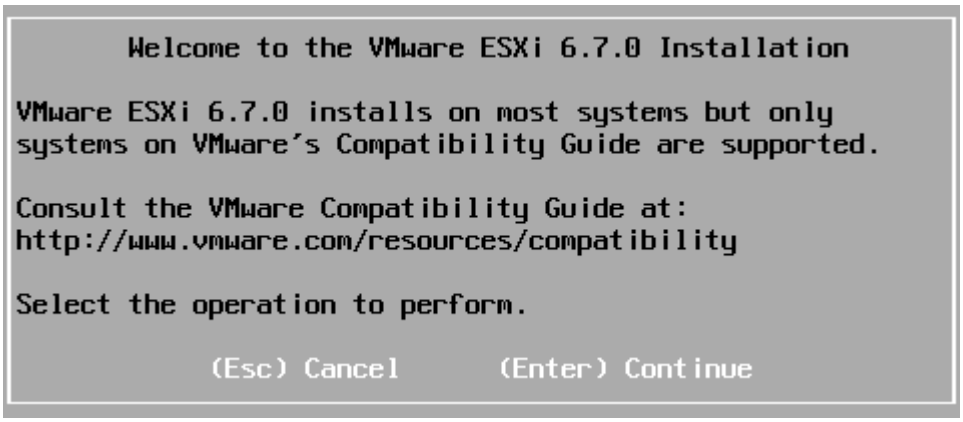


Рисунок 3.2 – Установка ESXI 6.7

После процесса установки и создания пароля администратора, попадаем в главное меню ESXI (рисунок 3.3).

Рисунок 3.3 – Главное меню ESXI 6.7

По указанном IP-адресу – 192.168.1.15, через браузер попадаем в веб-интерфейс гипервизора (рисунок 3.5). Логин администратора – root (рисунок 3.4).

Рисунок 3.4 – Аутентификация в веб-интерфейс

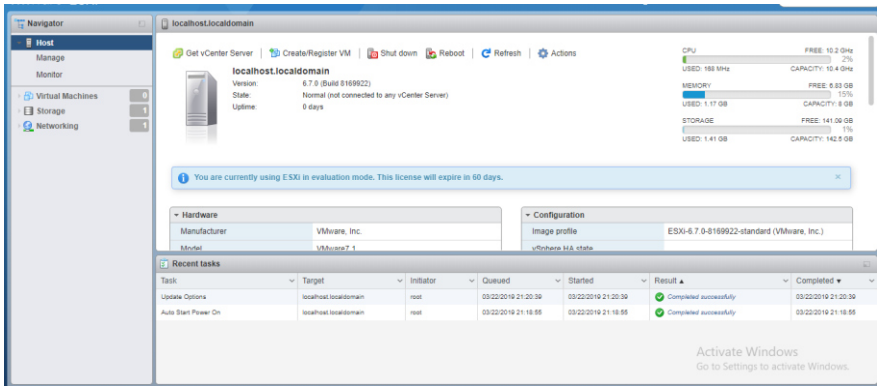


Рисунок 3.5 – Веб-интерфейс

Отправляемся в сетевые настройки и в параметрах сетевого интерфейса добавляем порт группу, указываем VLAN ID = 4095, для того, чтобы трафик был нетэгированным (рисунок 3.6).

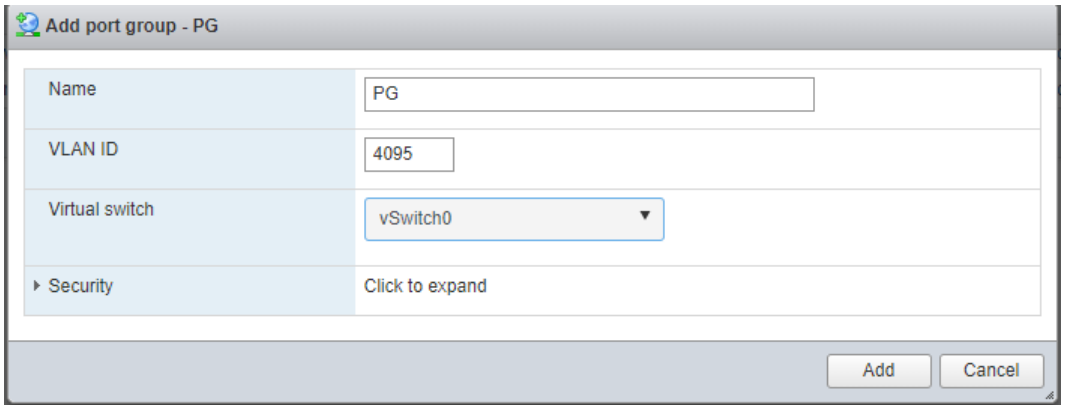


Рисунок 3.6 – Добавление портгруппы

Первой виртуальной машиной на нашем гипервизоре станет дистрибутив межсетевого экрана pfSense. Загружаем его в пространство ESXI через Datastore Browser (рисунок 3.7).

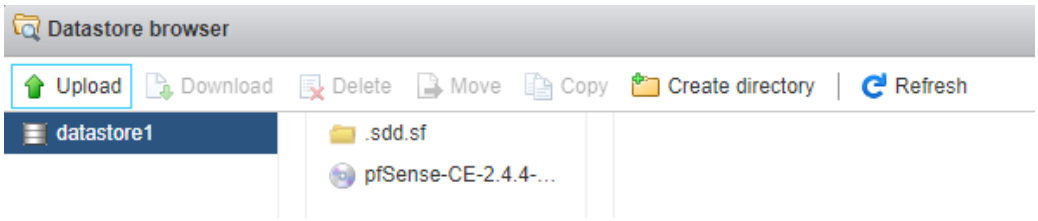


Рисунок 3.7 – Datastore browser

Выставляем технические параметры – самое главное указываем сетевой интерфейс, созданный нами ранее – PG (рисунок 3.8).

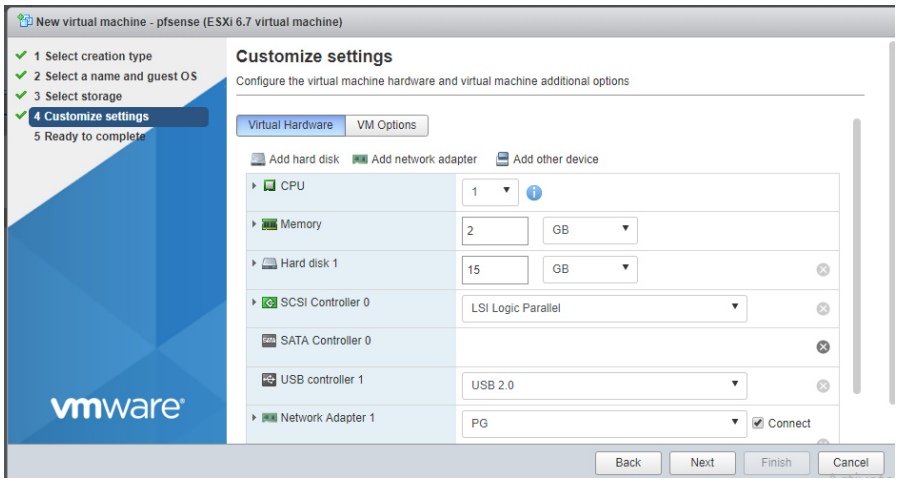


Рисунок 3.8 – Параметры виртуальной машины

Производим установку самого брандмауэра (рисунок 3.9).

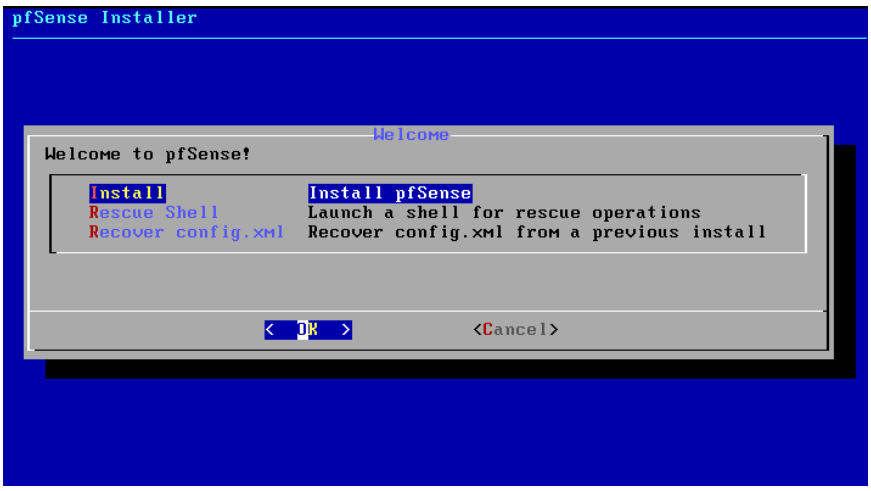


Рисунок 3.9 – Установка pfSense

Попадаем в командную строку межсетевого экрана и наглядно наблюдаем UNIX-подобную принадлежность продукта. Первым делом система спрашивает у пользователя о настройках VLAN (рисунок 3.10).

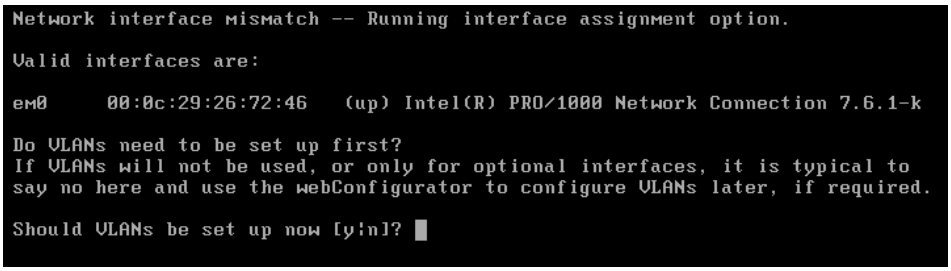


Рисунок 3.10 – Меню брандмауэра

Далее нам нужно разбить сеть на VLAN`ы и создать необходимые сетевые интерфейсы. Вся работа будет основываться на следующей схеме (рисунок 3.11).

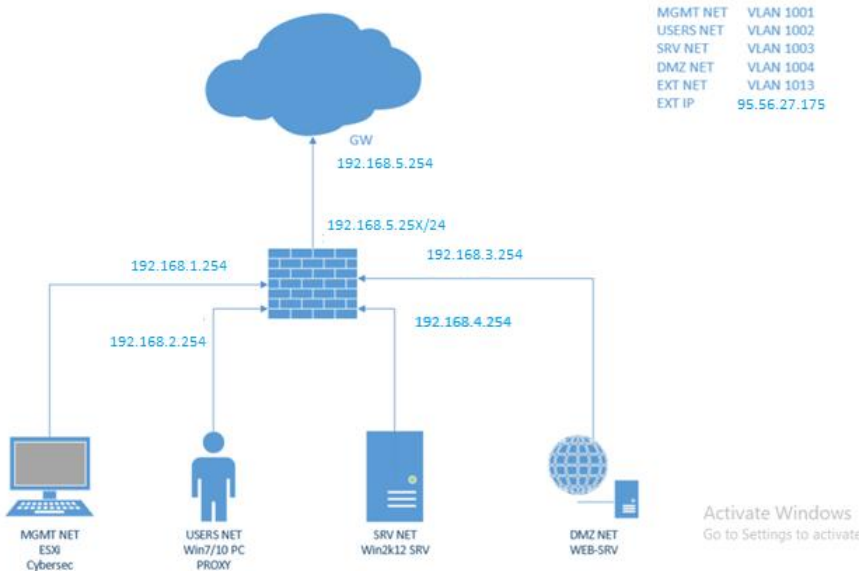


Рисунок 3.11 – Структурная схема сети

Создаем 5 сетевых интерфейсов со своими VLAN ID, как указано на схеме.

MGMT NET – подсеть, предназначенная для управления, то есть предполагаемая только для пользователей с доступом уровня администратора. Только находясь в этой подсети возможно управлять гипервизором и межсетевым экраном. VLAN ID = 1001.

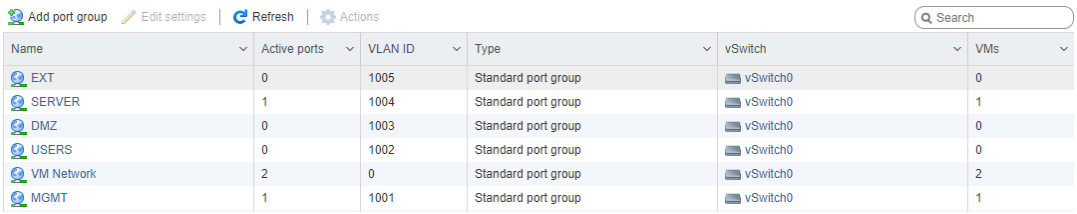
USERS NET – подсеть, предназначенная для рядовых сотрудников компании, не имеющих отношения к администрированию. Данные пользователи будут частью доменной структуры предприятия. VLAN ID = 1002.

DMZ NET – внутренняя подсеть, предназначенная для веб-сервера. VLAN ID = 1003.

SERVER NET – подсеть, в которой будут находиться DHCP, DNS сервера в рамках Windows Server 2012. VLAN ID = 1004.

EXT NET – подсеть, отвечающая за соединение с сетью Интернет, или же попросту WAN интерфейс. VLAN ID = 1005.

Далее на гипервизоре создаем новые портгруппы с соответствующими VLAN ID. Данные сетевые адаптеры предназначены для виртуальных машин из соответствующих подсетей (рисунок 3.12).



Name	Active ports	VLAN ID	Type	vSwitch	VMs
EXT	0	1005	Standard port group	vSwitch0	0
SERVER	1	1004	Standard port group	vSwitch0	1
DMZ	0	1003	Standard port group	vSwitch0	0
USERS	0	1002	Standard port group	vSwitch0	0
VM Network	2	0	Standard port group	vSwitch0	2
MGMT	1	1001	Standard port group	vSwitch0	1

Рисунок 3.12 – Создание портгрупп

Следующим шагом необходимо в фаерволле разбить сетевой адаптер на 5 самостоятельных с указанными выше VLAN ID (рисунок 3.13).

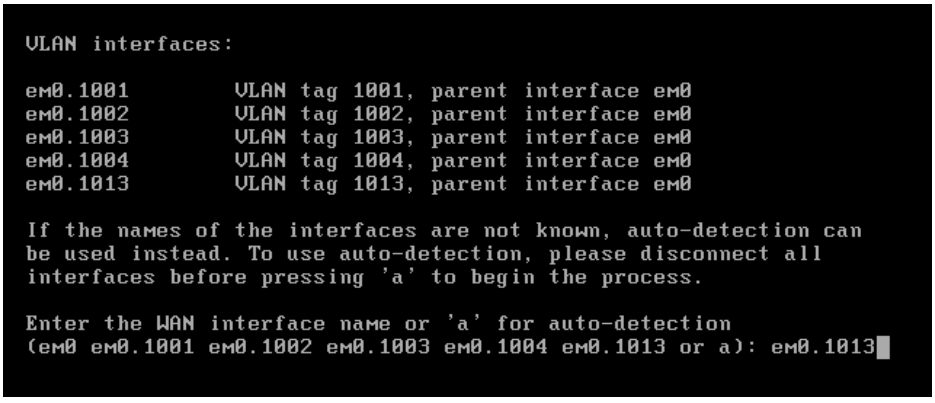


Рисунок 3.13 – Разделение на VLAN

После этого pfSense требует из имеющихся сетевых адаптеров определить их роли. WAN – внешний, LAN – внутренний (рисунок 3.14).

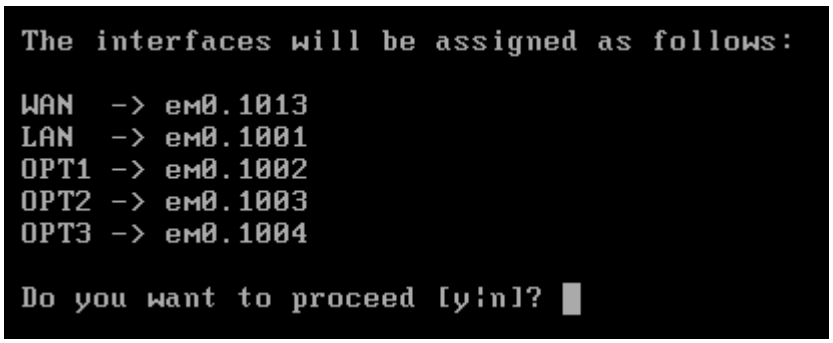


Рисунок 3.14 – Роли сетевых адаптеров

Теперь необходимо каждому сетевому интерфейсу присвоить IP адрес (рисунок 3.15).

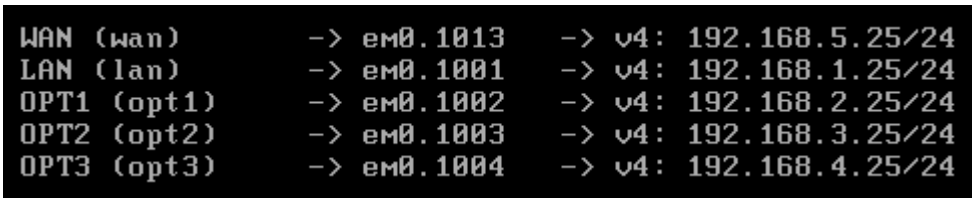


Рисунок 3.15 – IP адреса сетевых интерфейсов

Теперь мы можем попасть в веб-интерфейс межсетевого экрана по его LAN IP – 192.168.1.25. Для управления pfSense установим на гипервизоре виртуальную машину с операционной системой Windows 7 (рисунки 3.16, 3.17).

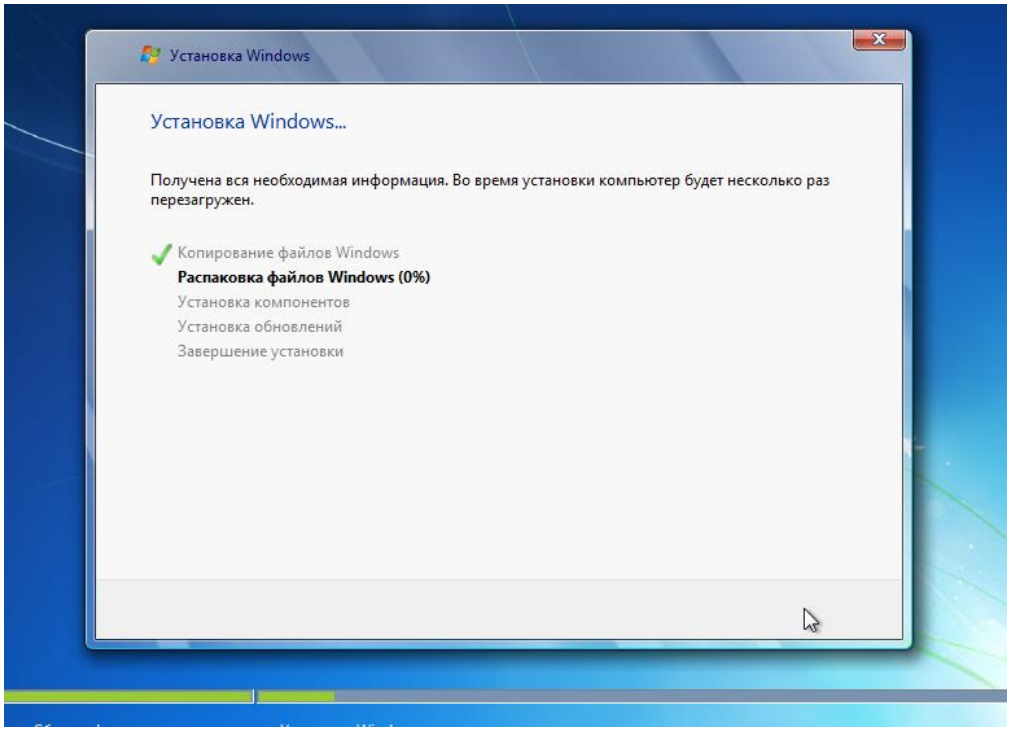


Рисунок 3.16 – Установка Windows 7

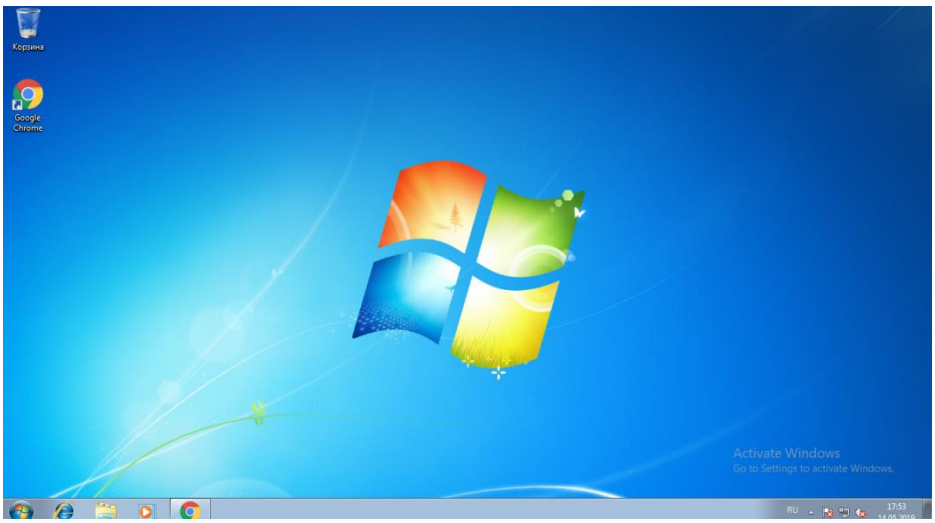


Рисунок 3.17 – Установленный Windows 7

Переходим в консоль управления pfSense через браузер Google Chrome (рисунок 3.18). Логин по умолчанию – pfsense, пароль – admin.

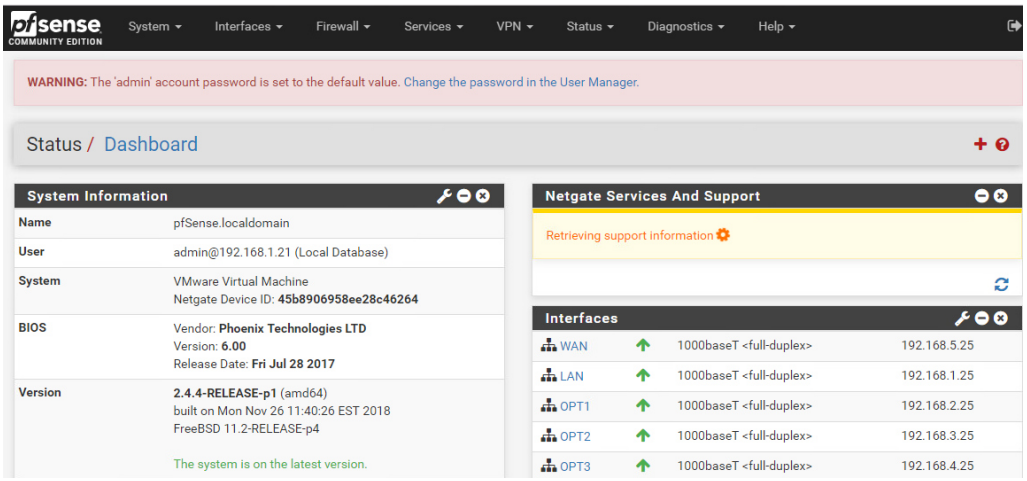


Рисунок 3.18 – Веб-интерфейс брандмауэра

Далее создаем новое правило в Firewall-Rules, которое открывает все порты и протоколы на LAN интерфейсе (рисунки 3.19, 3.20).

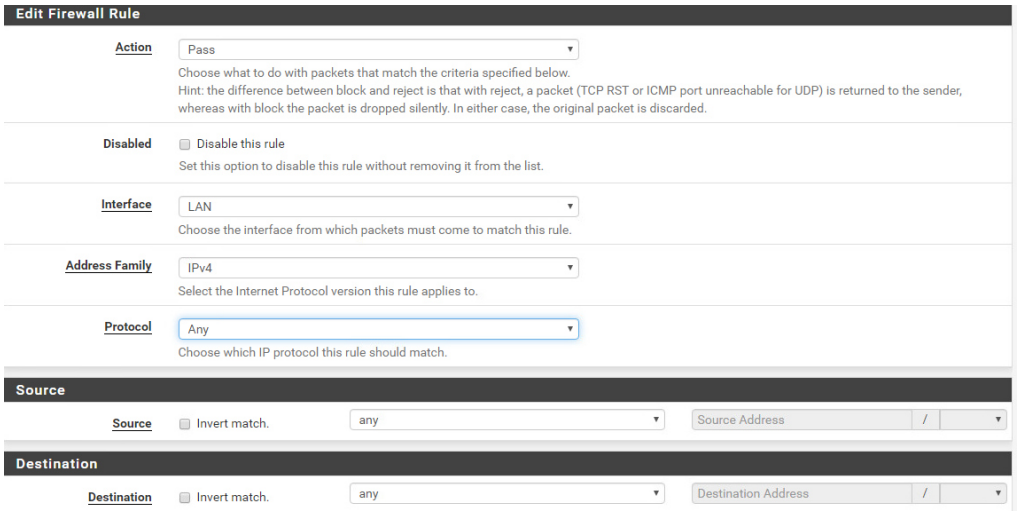


Рисунок 3.19 – Создание правил маршрутизации

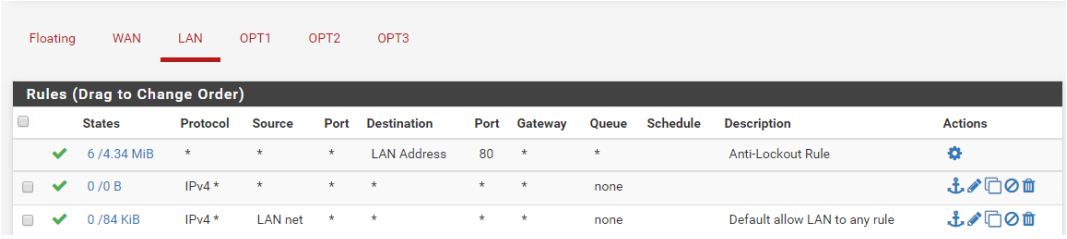


Рисунок 3.20 – Правила маршрутизации

Для того, чтобы обеспечить для всех наших подсетей выход в интернет, необходимо прописать NAT правила (рисунок 3.21). На данный момент единственная подсеть, которая имеет доступ к интернету – EXT NET, которая является WAN интерфейсом. Вся суть правил – разрешить остальным интерфейсам «ходить» в интернет под одним публичным IP адресом (рисунок 3.22).

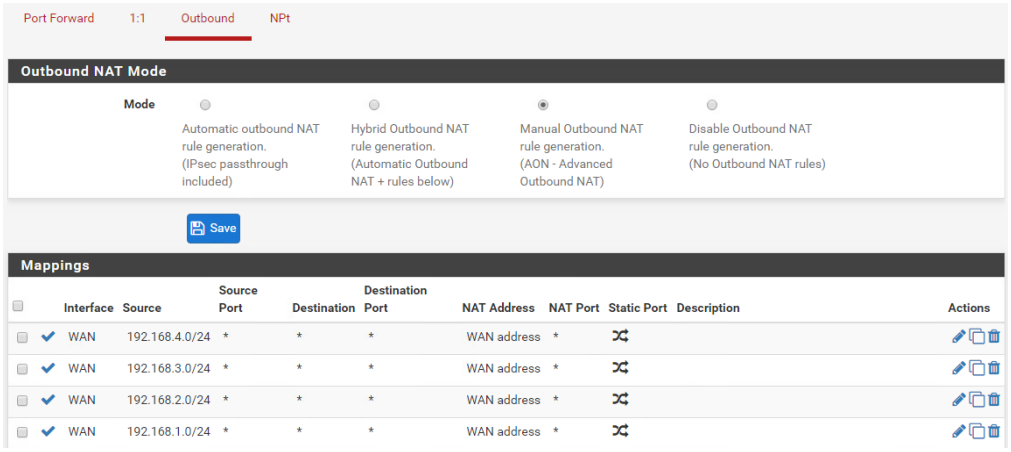


Рисунок 3.21 – Настройка NAT

Благодаря указанным правилам, мы получаем выход в глобальную сеть.

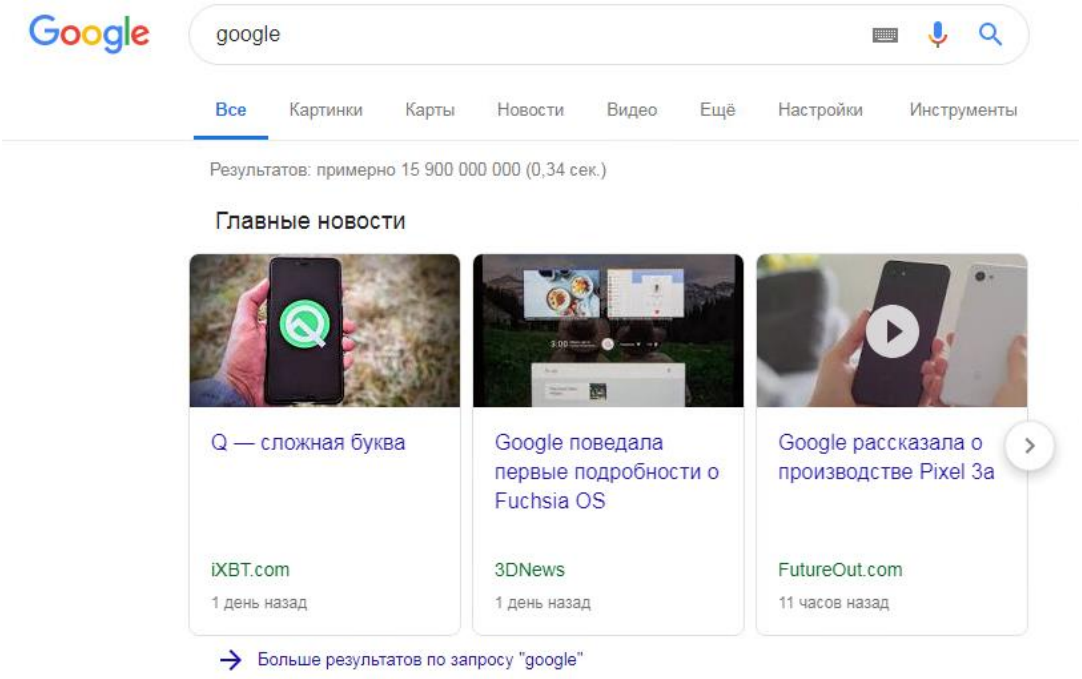


Рисунок 3.22 – Доступ в Интернет

Следующим шагом будет установка серверной машины с ОС Windows Server 2012, которая будет располагаться в SERVER NET (рисунки 3.23, 3.24).

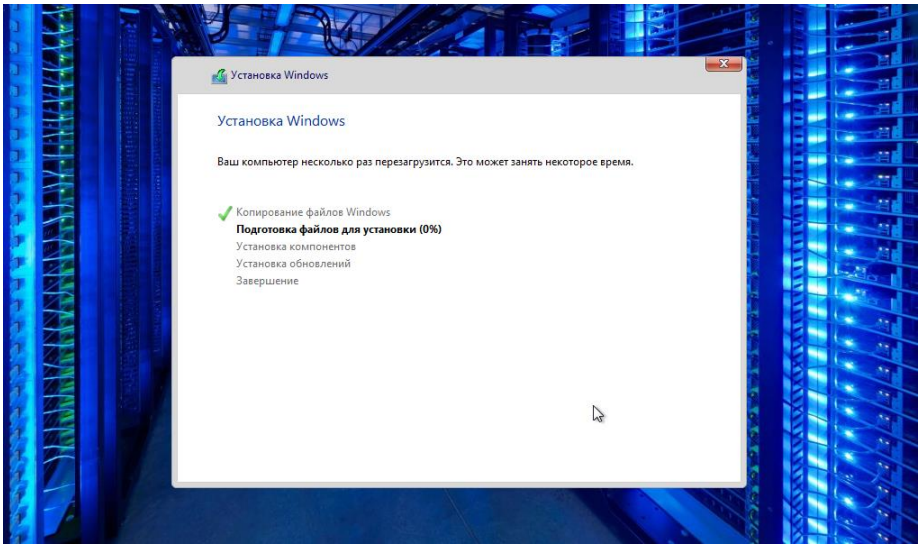


Рисунок 3.23 – Установка Windows Server 2012

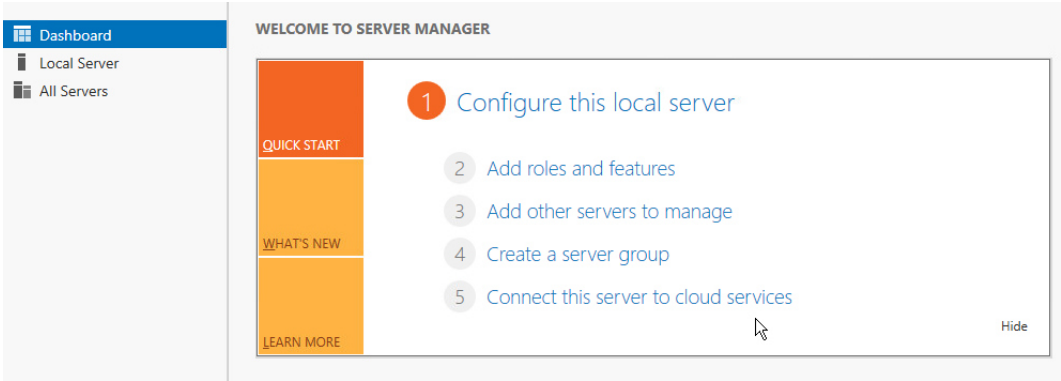


Рисунок 3.24 – Server Manager

Данная операционная система в нашей сети необходима для создания структуры Active Directory, DNS и DHCP ролей. Первым делом добавим роль доменных служб AD (рисунки 3.25, 3.26, 3.27).

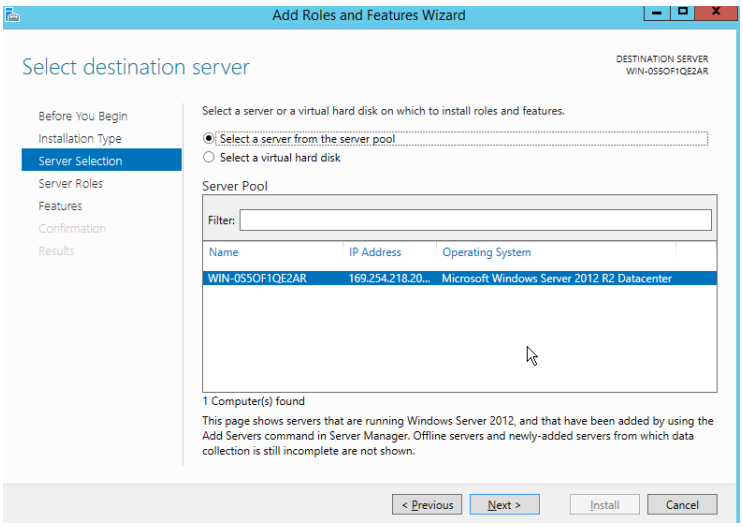


Рисунок 3.25 – Выбор сервера

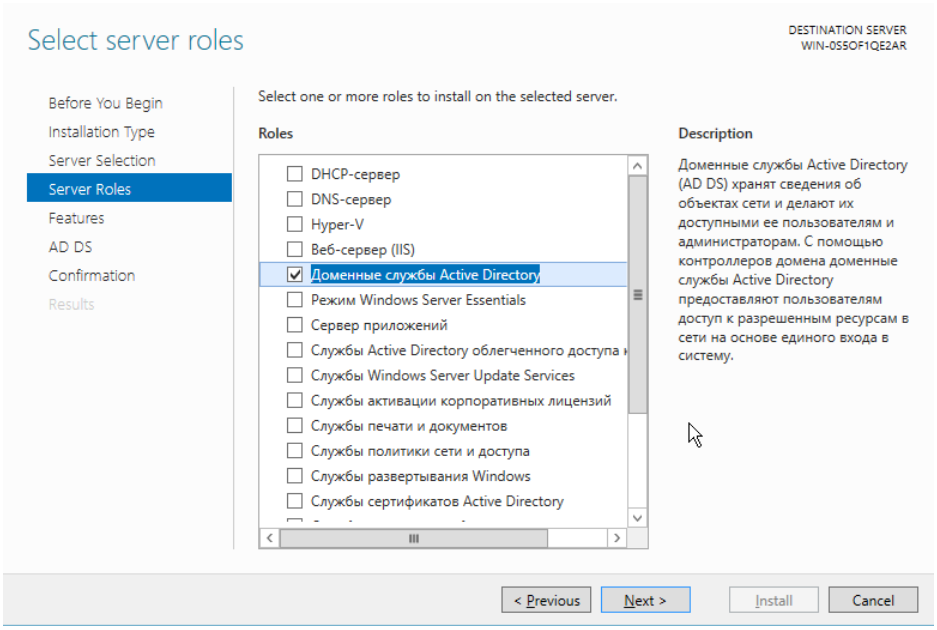


Рисунок 3.26 – Добавление роли AD

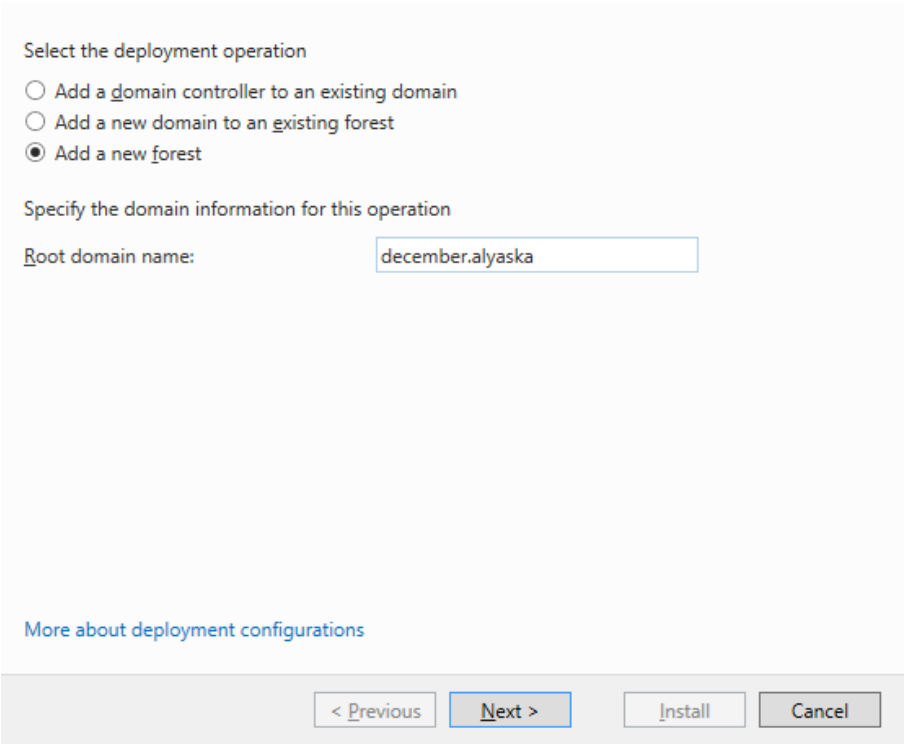


Рисунок 3.27 – Добавление нового леса

Теперь необходимо подождать, пока ОС применит все изменения по созданию нового домена – december.alyaska и возьмет на себя роль контроллера домена (рисунки 3.28, 3.29).

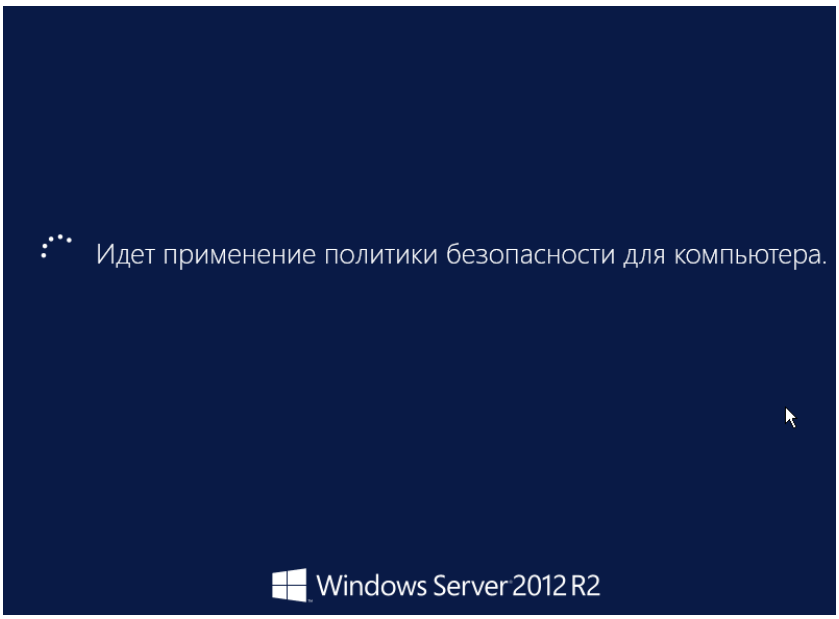


Рисунок 3.28 – Применение политик безопасности

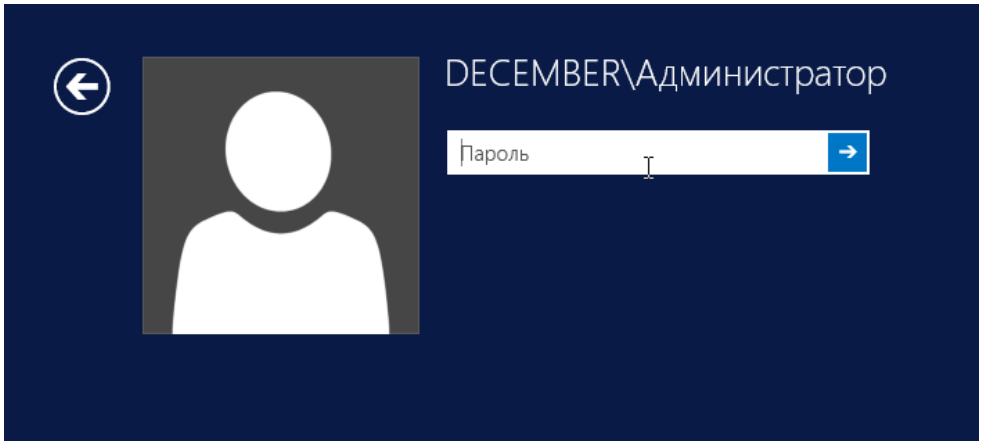


Рисунок 3.29 – Авторизация в контроллер домена

Следующим шагом будет установка DNS (рисунки 3.30, 3.31).

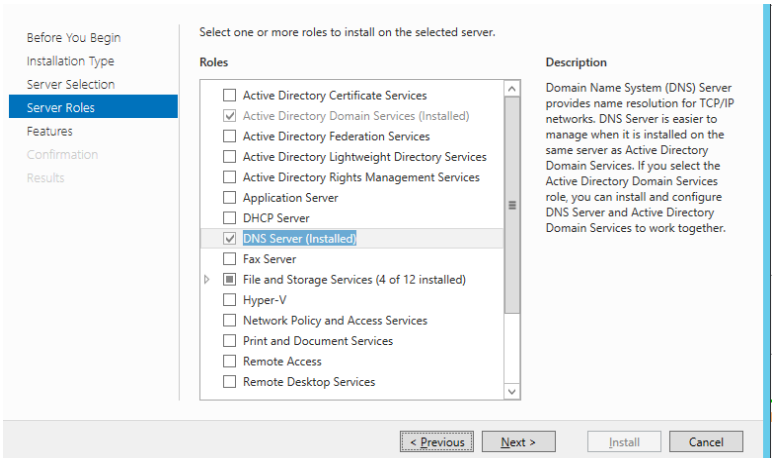


Рисунок 3.30 – Установка DNS

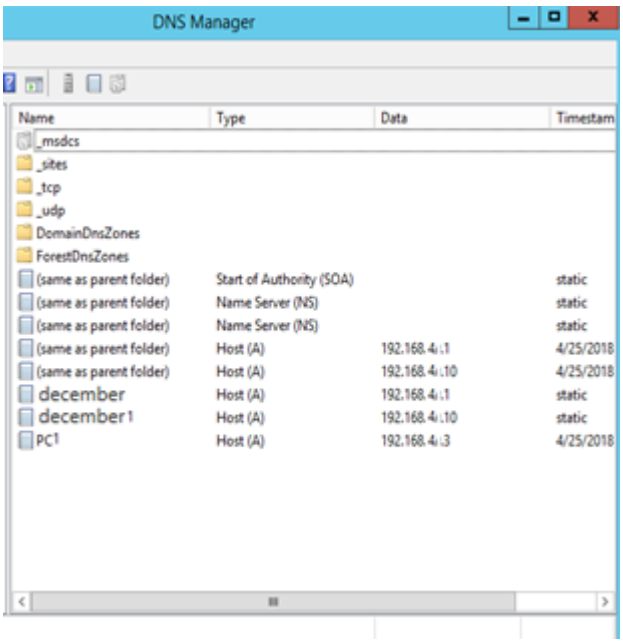


Рисунок 3.31 – DNS записи

Теперь когда на сервере есть домен контроллер и установлена роль Active Directory, необходимо создать группы пользователей по структуре предприятия (рисунок 3.32).

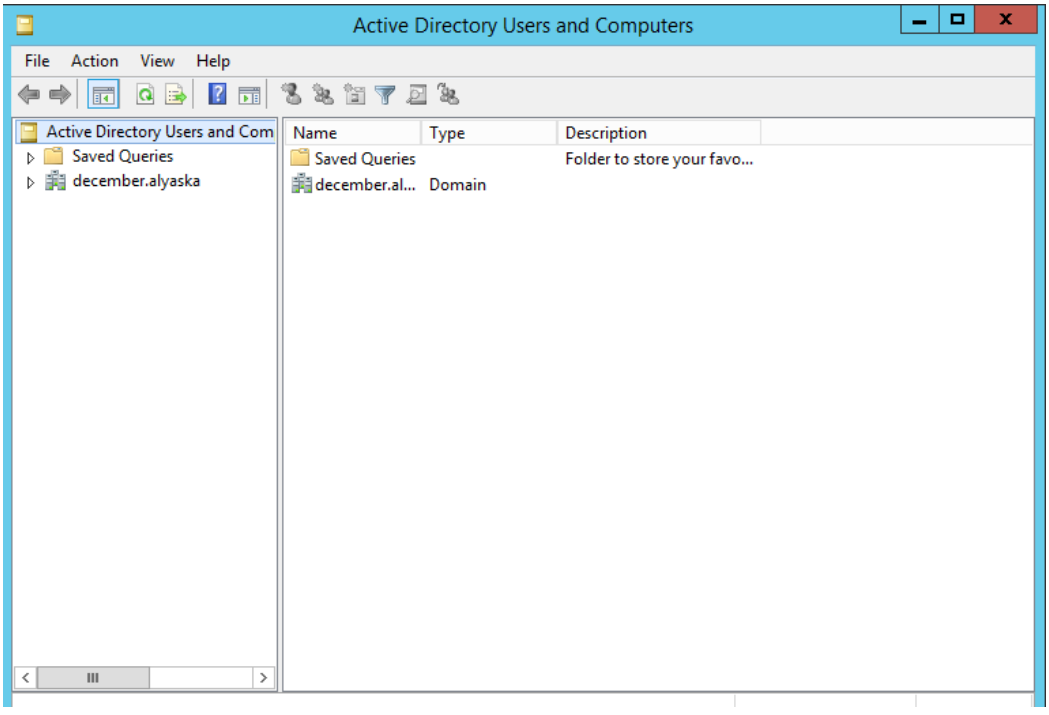


Рисунок 3.32 – Оснастка AD

Для начала создам одного пользователя и подключу его к домену, чтобы убедиться в правильности предыдущих настроек (рисунки 3.33, 3.34, 3.35).

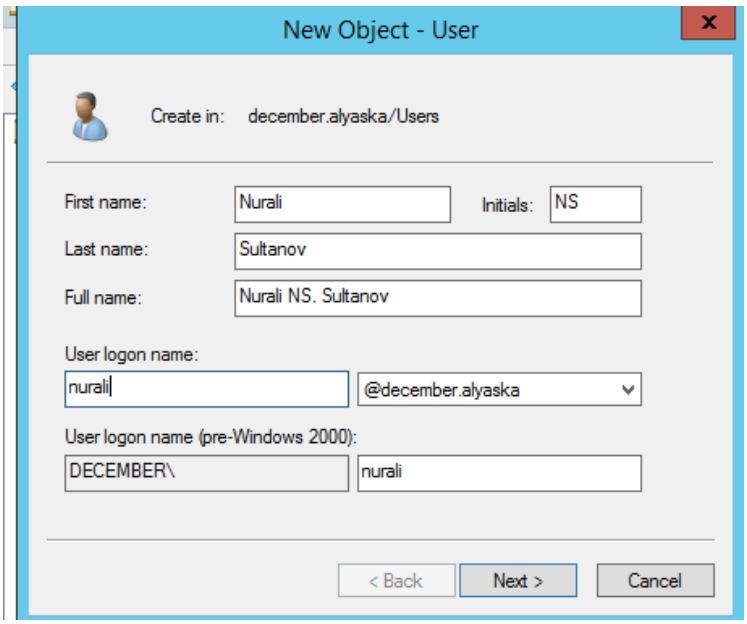


Рисунок 3.33 – Создание пользователя

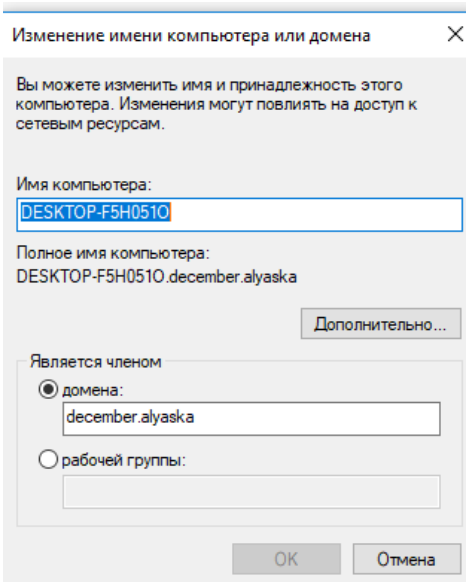


Рисунок 3.34 – Подключение к домену

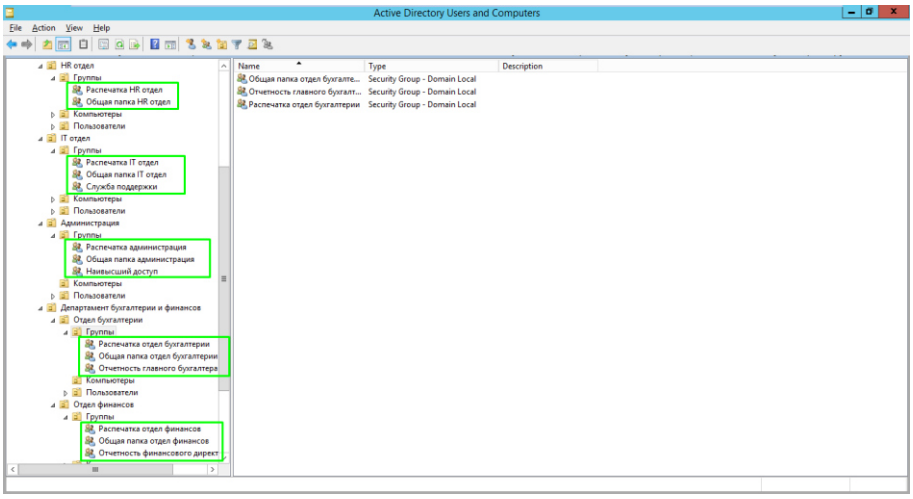


Рисунок 3.35 – Департаменты и группы

Следующий шаг – настроить DHCP сервер для автоматического присваивания IP-адресов пользователям из USERS NET (рисунки 3.36, 3.37). Адреса должны находиться в пользовательской подсети – 192.168.2.X.

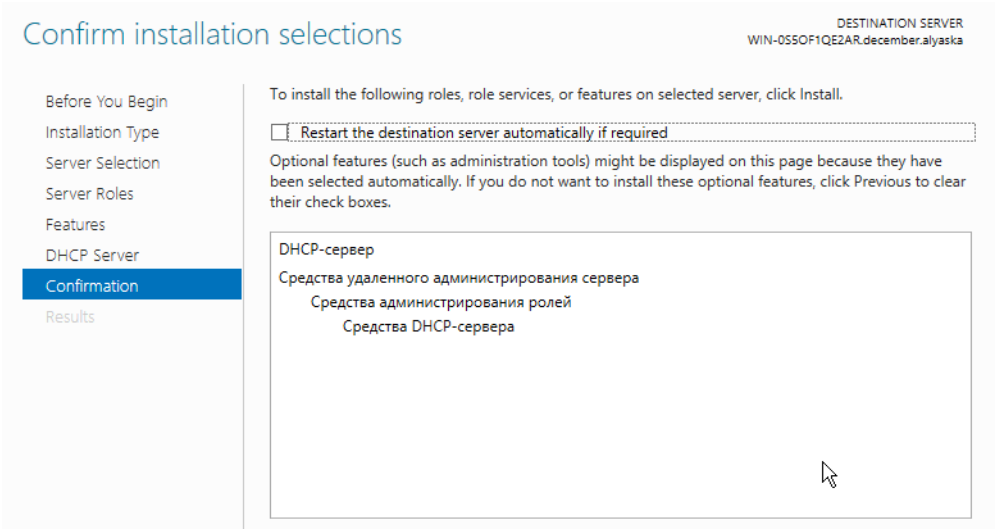


Рисунок 3.36 – Добавление роли DHCP

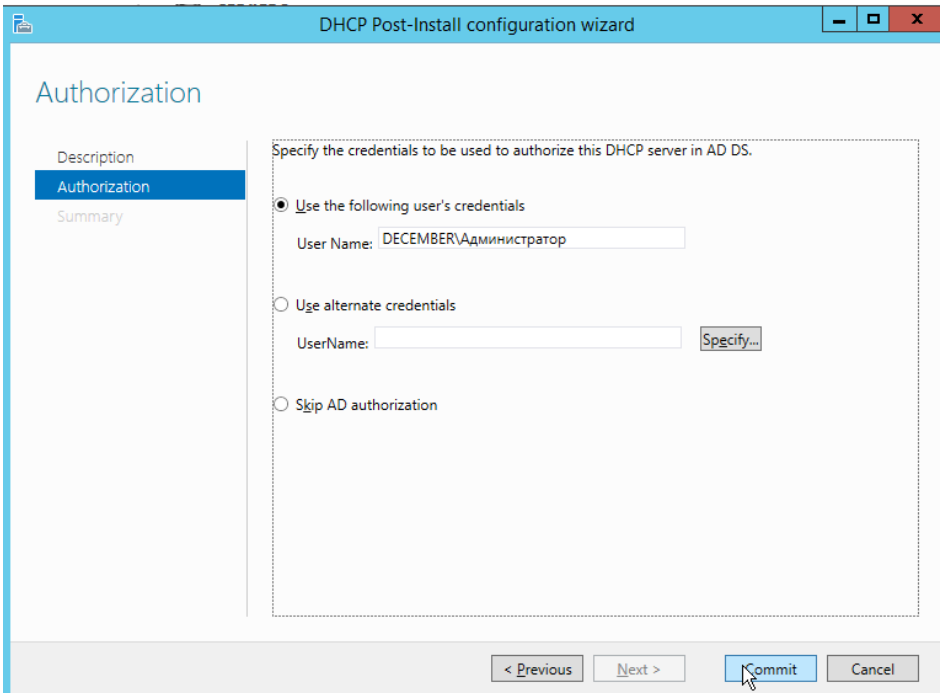


Рисунок 3.37 – Настройка DHCP

Необходимо указать диапазон раздаваемых сервером IP адресов (рисунки 3.38, 3.39).

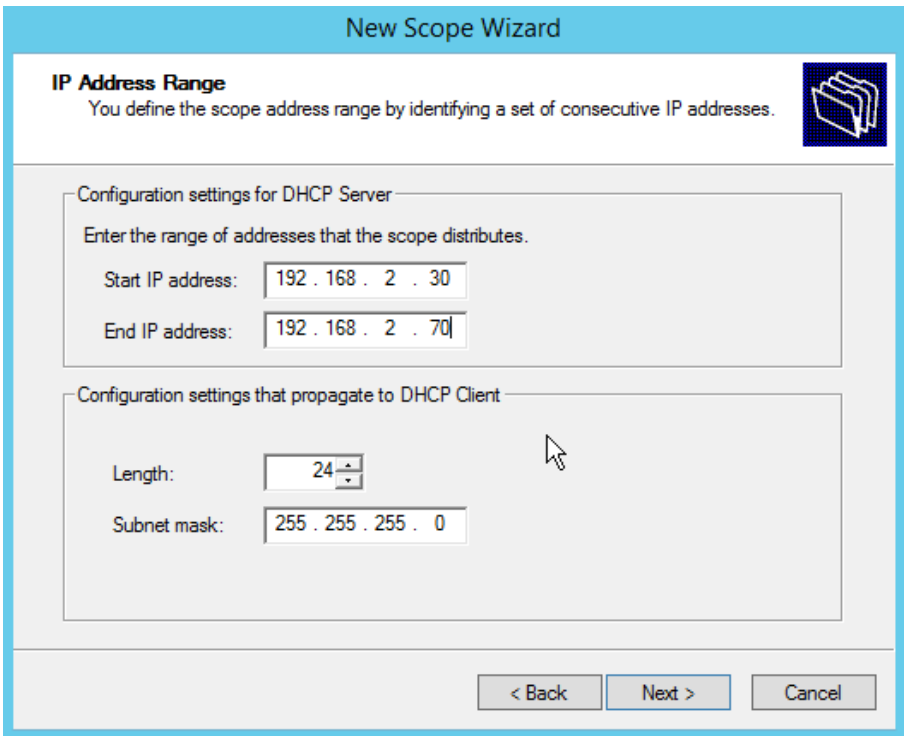


Рисунок 3.38 – Диапазон адресов

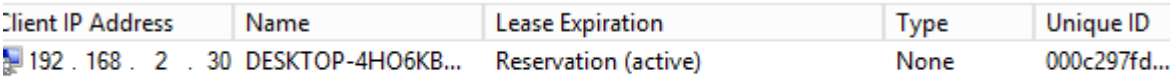


Рисунок 3.39 – Успешное подключение клиентской машины

Теперь, когда сотрудники могут подключиться к рабочей сети, необходимой мерой является настройка Proxy, для кэширования страниц, а также мониторинга за клиентами. Squid Proxy является одним из пакетов, доступных в pfSense. Необходимо установить его через Package Manager (рисунок 3.40).

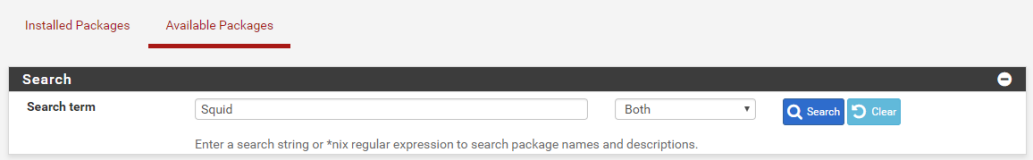


Рисунок 3.40 – Squid в Package Manager

После его установки, необходимо в файле конфигурации realname.cfg указать необходимых нам пользователей (рисунки 3.41, 3.42).

```
vi /usr/local/etc/lightsquid/realname.cfg
```

Рисунок 3.41 – Путь к файлу конфигурации

```
192.168.2.31 Nurali
192.168.2.32 Bayan
192.168.2.33 Erman
```

Рисунок 3.42 – Добавление пользователей

Для мониторинга необходимо аутентифицироваться как администратору прокси сервера, и перейти в интерфейс Lightsquid (рисунки 3.43, 3.44, 3.45, 3.46).

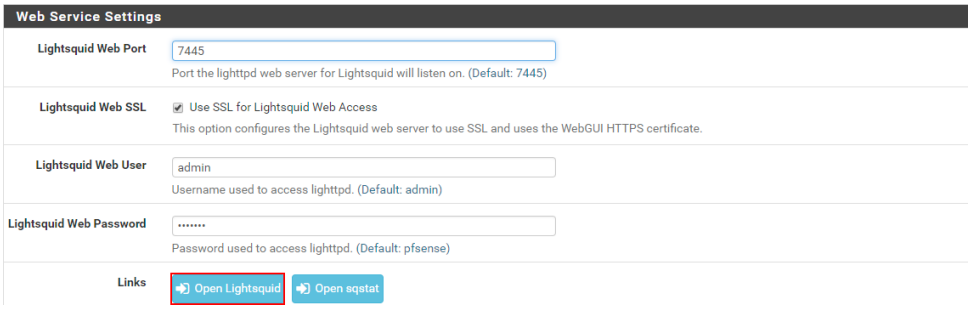


Рисунок 3.43 - Аутентификация

Отчёт по использованию интернета, прокси-сервер Squid.

Дата: 5 май 2019

Популярные сайты (отчёт)

Кто скачал БОЛЬШИЕ файлы (отчёт)

№	Время	Пользователь	Ф.И.О	Соединений	Байт	%	Группа
1		192.168.3.32	Bayan	123	1.0 M	97.5%	?
2		192.168.3.33	Erman	22	25 860	2.3%	?
3		127.0.0.1	?	1	750	0.0%	?

Рисунок 3.44 – Отчет Squid

Отчёт по использованию интернета, прокси-сервер Squid.

целиком МЕСЯЦ

№	Время	График	МЕСЯЦ	Пользователь	Ф.И.О	Соединений	Байт	%	Итого
1			[M]	192.168.3.32	Bayan	144	1.0 M	97.5%	1.0 M
2			[M]	192.168.3.33	Erman	22	25 860	2.3%	1.1 M
3			[M]	127.0.0.1	?	1	750	0.0%	1.1 M

Рисунок 3.45 – Отчет Squid

Всего			1.0 M		
№	Посещённые сайты	Соединений	Байт	Итого	%
1	jetem.podberi-kolyasku.ru	58	789 892	789 892	73.1%
2	podberi-sotik.ru	8	185 337	975 229	17.1%
3	ocsp.godaddy.com	6	14 144	989 373	1.3%
4	yandex.ocsp-responder.com	6	11 328	1 000 701	1.0%
5	ocsp2.globalsign.com	5	11 077	1 011 778	1.0%
6	clients1.google.com	10	8 900	1 020 678	0.8%
7	apps.identrust.com	5	6 585	1 027 263	0.6%
8	ocsp.digicert.com	5	4 603	1 031 866	0.4%
9	ocsp.globalsign.com	2	4 362	1 036 228	0.4%
10	subca.ocsp-certum.com	2	4 041	1 040 269	0.3%
11	g2.symcb.com	2	3 680	1 043 949	0.3%
12	podberi-kolyasku.ru	2	3 250	1 047 199	0.3%
13	ocsp.comodoca.com	3	3 171	1.0 M	0.2%
14	counter.yadro.ru	5	2 617	1.0 M	0.2%
15	repository.certum.pl	2	2 548	1.0 M	0.2%
16	s.symcd.com	1	2 226	1.0 M	0.2%
17	crt.comodoca.com	1	2 075	1.0 M	0.1%
18	isrg.trustid.ocsp.identrust.com	1	1 885	1.0 M	0.1%
19	gn.symcd.com	1	1 881	1.0 M	0.1%
20	gp.symcd.com	1	1 878	1.0 M	0.1%
21	g.symcd.com	1	1 853	1.0 M	0.1%

Рисунок 3.46 – Отчет Squid

Ключевым средством безопасности моей сети будет IDS Snort. Также как и прокси, она является одним из доступных пакетов в межсетевом экране (рисунок 3.47).

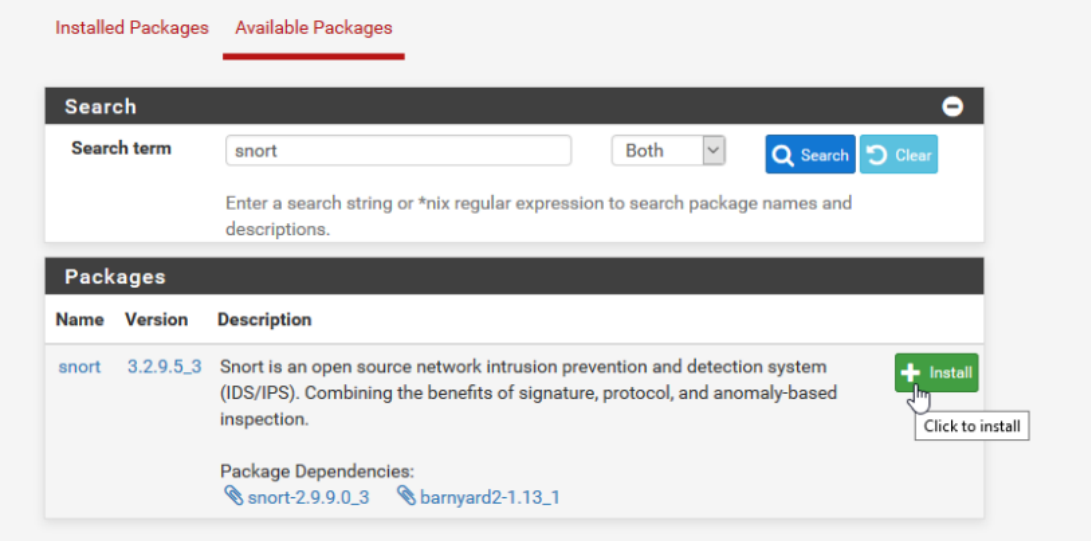


Рисунок 3.47 – Snort в pfSense

После установки IDS, необходимо обновить правила, для того, чтобы наша система распознавала все актуальные атаки (рисунок 3.48).

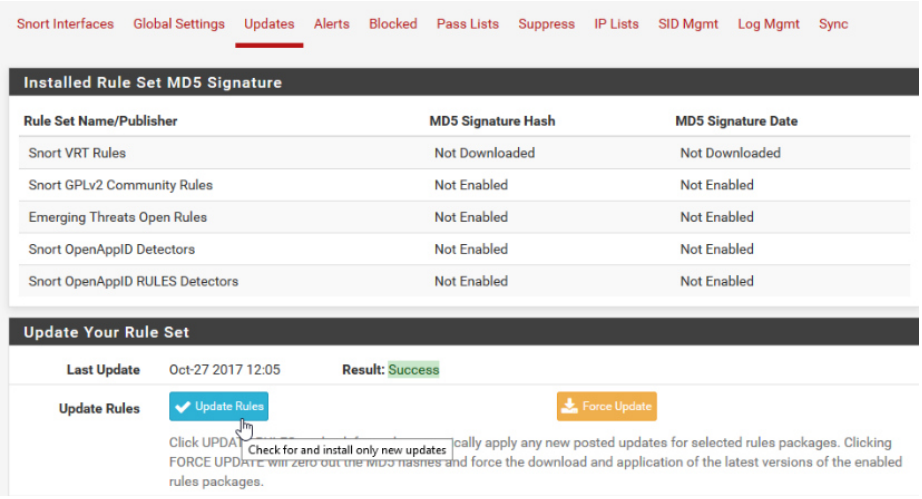


Рисунок 3.48 – Обновление правил

Задаем настройки Snort, среди которых подсеть, системные логи, включение опции блокировки по IP адресам (рисунок 3.49).

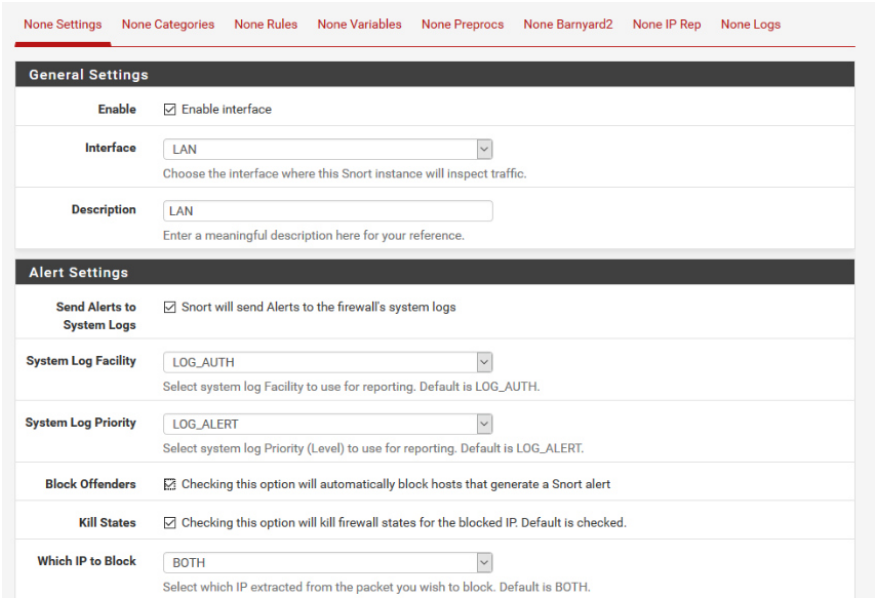


Рисунок 3.49 – Настройка Snort

Во вкладке Alerts указывая нужную нам подсеть, можно мониторить все инциденты (рисунок 3.50).

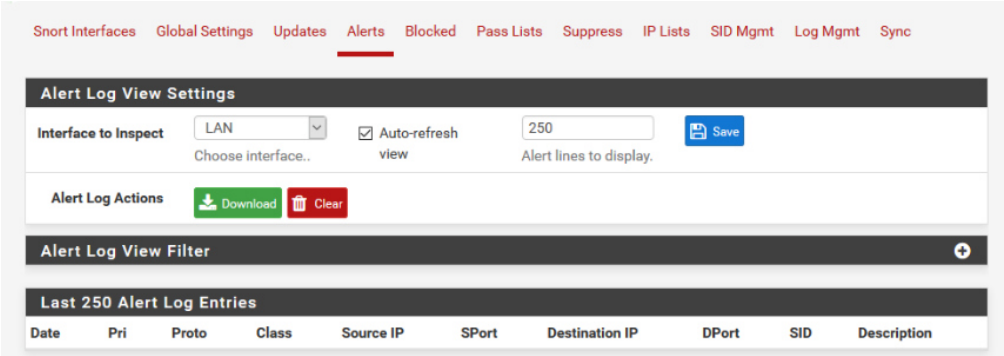


Рисунок 3.50 - Alerts

Прежде чем запускать систему обнаружения вторжений необходимо указать по каким правилам ей работать. Правила можно прописывать вручную, но в этом нет необходимости, поскольку Snort по умолчанию содержит в себе сигнатуры почти всех возможных атак с небольшим периодом обновлений (рисунок 3.51).

Enabled	Ruleset: ET Open Rules	Enabled	Ruleset: Snort Text Rules	Enabled	Ruleset: Snort SO Rules	Snort OPENAPPID rules are not enabled.
☐	emerging-activex.rules	☐	snort_app-detect.rules	☐	snort_browser-ie.so.rules	
☐	emerging-attack_response.rules	☐	snort_attack-responses.rules	☐	snort_browser-other.so.rules	
☐	emerging-botcc.portgrouped.rules	☐	snort_backdoor.rules	☐	snort_browser-plugins.so.rules	
☐	emerging-botcc.rules	☐	snort_bad-traffic.rules	☐	snort_exploit-kit.so.rules	
☑	emerging-chat.rules	☐	snort_blacklist.rules	☐	snort_file-executable.so.rules	
☐	emerging-ciarmy.rules	☐	snort_botnet-cnc.rules	☐	snort_file-flash.so.rules	
☐	emerging-compromised.rules	☐	snort_browser-chrome.rules	☐	snort_file-image.so.rules	
☐	emerging-current_events.rules	☐	snort_browser-firefox.rules	☐	snort_file-java.so.rules	
☐	emerging-deleted.rules	☐	snort_browser-ie.rules	☐	snort_file-multimedia.so.rules	
☑	emerging-dns.rules	☐	snort_browser-other.rules	☐	snort_file-office.so.rules	
☐	emerging-dos.rules	☐	snort_browser-plugins.rules	☐	snort_file-other.so.rules	
☐	emerging-drop.rules	☐	snort_browser-webkit.rules	☐	snort_file-pdf.so.rules	
☐	emerging-dshield.rules	☐	snort_chat.rules	☐	snort_indicator-shellcode.so.rules	
☐	emerging-exploit.rules	☐	snort_content-replace.rules	☐	snort_malware-cnc.so.rules	
☐	emerging-ftp.rules	☐	snort_ddos.rules	☐	snort_malware-other.so.rules	

Рисунок 3.51 – Правила Snort

После того как были включены необходимые правила системы обнаружения вторжений, необходимо проверить её реагирования на различные атаки и несанкционированные действия. Для начала я проверил IDS, посетив страницу, содержащую вредоносный код (рисунки 3.52, 3.53).

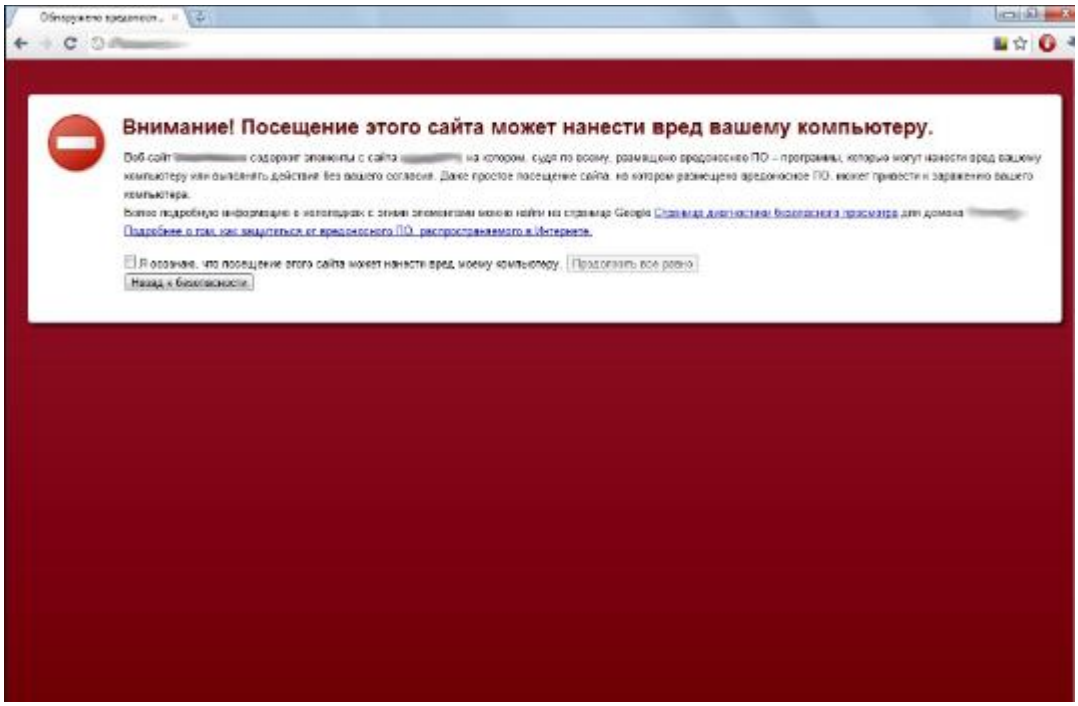


Рисунок 3.52 – Вредоносная страница

	GID	SID	Proto	Source	SPort	Destination	DPort	Message
✓	1	5808	tcp	$HOME_NET	any	$EXTERNAL_NET	$HTTP_PORTS	BLACKLIST User-Agent known malicious user agent - SAH Agent
✓	1	5900	tcp	$HOME_NET	any	$EXTERNAL_NET	$HTTP_PORTS	BLACKLIST User-Agent known malicious user agent - Async HTTP Agent

Рисунок 3.53 – Snort Alerts

Snort отреагировал на вредоносный код, определив источник, а также выдал сообщение о вредоносном коде – User-agent known malicious user agent.

Далее, я решил воспользоваться некоторыми инструментами Kali Linux, установленными на моей рабочей станции. Первый из них – Ettercap, позволяющий реализовать атаку Man In The Middle (рисунки 3.54, 3.55, 3.56).

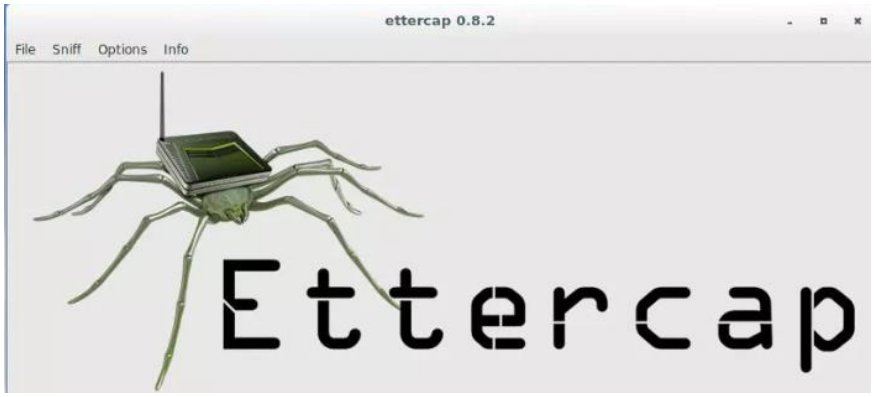


Рисунок 3.54 – Ettercap

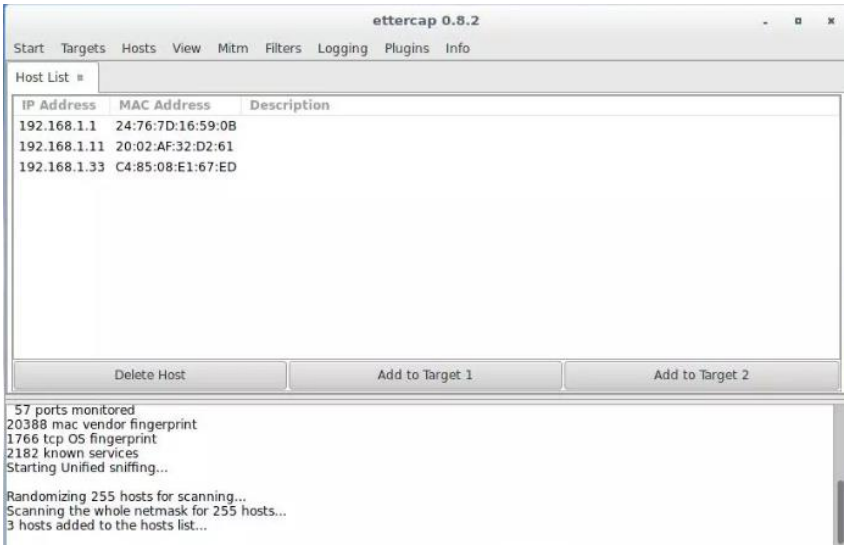


Рисунок 3.55 – Реализация атаки Mitm

UDP	Potentially Bad Traffic	163.172.22.169	52428	5060	140:26	(spp_sip) Method is unknown
UDP	Potentially Bad Traffic	163.172.17.76	46834	5060	140:26	(spp_sip) Method is unknown
UDP	Potentially Bad Traffic	163.172.22.169	54788	5060	140:26	(spp_sip) Method is unknown
UDP	Potentially Bad Traffic	163.172.17.76	59571	5060	140:26	(spp_sip) Method is unknown

Рисунок 3.56 – Snort Alerts

Далее была проведена попытка подобрать пароль на доступ к ftp соединению через bruteforce (рисунки 3.57, 3.58).

Рисунок 3.57 – Подборка пароля через Brutespray

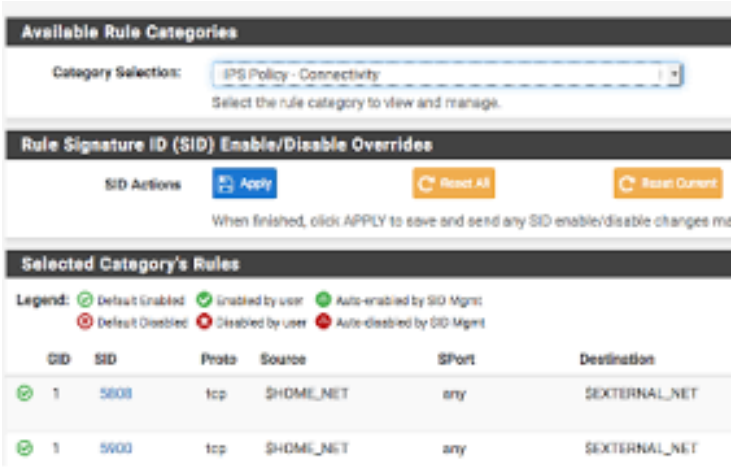


Рисунок 3.58 – Snort Alerts

И последняя попытка проведения атаки – dnslookup, посредством инструмента сканирования портов nmap (рисунки 3.59, 3.60).

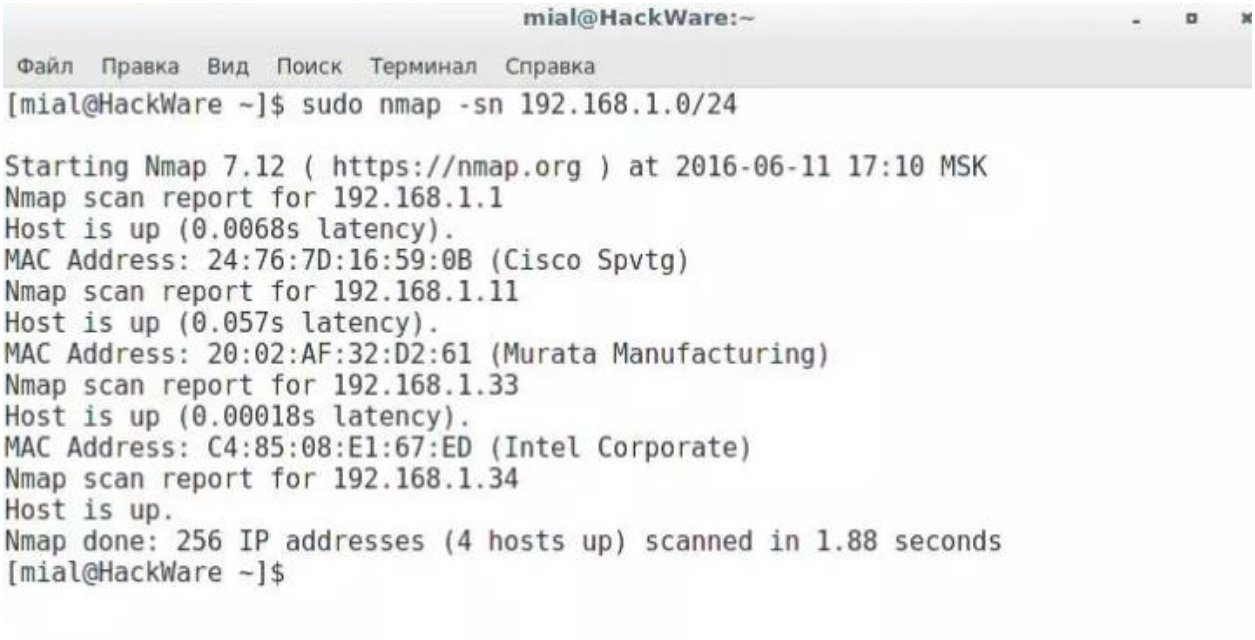


Рисунок 3.59 - Nmap

Рисунок 3.60 – Snort Alerts

Вывод

В данной главе было реализовано построение корпоративной сети на практике. Сначала, в виртуальном пространстве я установил гипервизор ESXI 6.7, на котором и был выполнен весь проект. В сетевых конфигурациях были созданы портгруппы на виртуальном коммутаторе с необходимыми VLAN ID. Далее на виртуальной машине в гипервизоре был установлен межсетевой экран pfSense, в котором были разделены все подсети по заранее составленной структурной схеме. Каждому сетевому интерфейсу была присвоена своя роль. Затем была установлена виртуальная машина с ОС Windows 7 для двух целей – управления межсетевым экраном, а также для проверки пользовательской составляющей. Затем я создал серверную машину для ролей AD, DNS, DHCP. Провел анализ работоспособности вышеуказанных ролей, а также создал структуру персонала в оснастке Active Directory. Установил прокси-сервер, а также систему обнаружения вторжений. Проанализировал безопасность сети, попытавшись реализовать некоторые типы компьютерных атак.

4 Технико-экономическое обоснование

Данный дипломный проект посвящен моделированию безопасной корпоративной сети в виртуальном пространстве, на базе гипервизора VMware ESXI 6.7.0

В разработке программного обеспечения предполагается участие следующих работников технический руководитель, программист-разработчик. В обязанности технического руководителя входит координация рабочего процесса, изучение предметной области и анализ требований к системе. В обязанности программиста-разработчика входит разработка технического обоснования, разработка, внедрение программного обеспечения, обеспечение его безопасности, тестирование и поддержка. Следовательно, основная работа ложится на плечи программиста-разработчика, в то время как технический руководитель занимается организационными вопросами.

4.1 Определение сложности разработки ПО

Для определения трудоемкости разработки модели приведен перечень всех основных этапов и видов работ, которые должны быть выполнены. Форма разделения работ по этапам с указанием трудоемкости их выполнения приведена в таблице 4.1

Таблица 4.1 – Этапы разработки ПО

Этапы разработки ПО	Вид работы	Трудоемкость, чел. час.
Этап 1	Знакомство с материалами проекта	10
Этап 2	Изучение особенностей виртуализации	15
Этап 3	Изучение особенностей коммутаторов (виртуальных)	15
Этап 4	Изучение особенностей VLAN	15
Этап 5	Установка и настройка гипервизора VMware ESXI 6.7.0 на базе VMware Workstation PRO 15 (vswitch, vlan, рабочие станции)	50
Этап 6	Установка и настройка фаерволла pfsense (lannet, NAT, VPN)	35
Этап 7	Развертывание и настройка веб-сервера nginx, с уязвимым mutillidae	20
Этап 8	Обеспечение безопасности сети (proxy, ids)	25
Этап 9	Анализ выполненных работ	25
Итого: трудоемкость выполнения проекта		210

4.2 Расчет затрат на разработку ПО

Определение затрат необходимых для разработки программного обеспечения производится на основе имеющейся сметы, которая включает следующие элементы:

- материальные затраты;
- затраты на оплату труда;
- социальный налог;
- амортизация основных фондов;
- прочие затраты.

Материальные затраты делятся на основные и вспомогательные затраты на материалы, энергию и другие затраты необходимые для разработки ПО. Расчет материальных затрат происходит по форме, предоставленной в таблице 4.2 [13].

Таблица 4.2 – Затраты на материальные ресурсы

Наименование материала	Марка	Ед. измерения	Количество	Цена за ед. в тенге	Сумма в тенге
Бумага для офиса	Mondi	Упаковка	3	1 000	3 000
Шариковые ручки	Pilot	Упаковка	2	600	1200
Степлер	Eagle	Штук	1	600	600
Файлы	Herlitz	Упаковка	1	700	700
Магнитно-маркерная доска	Kaz-Delta	Штук	1	6000	6000
Стикеры	Stick-In	Упаковка	3	600	1800
Маркеры	Profymark	Штук	3	150	450
Итого:					13 750

Для разработки программного обеспечения будет использоваться компьютер Intel® Pentium® Dual Core Inside

Общую сумму, необходимую на материальные средства ($З_м$) можно рассчитать по следующей формуле:

$$З_м = \sum P_i * Ц_i, \quad (4.1)$$

где P_i - расход i-го вида материального ресурса, натуральные единицы;

$Ц_i$ - цена за единицу i-го вида материального ресурса, тг;

i - вид материального ресурса;

n - количество видов материальных ресурсов.

Расчет затрат на необходимое оборудование и программное обеспечение производится по форме, приведенной в таблице 4.3.

Таблица 4.3 – Расчет затрат на оборудование и ПО, необходимое для проекта

Наименование материала	Марка	Ед. измерения	Количество	Цена за ед. в тенге	Сумма в тенге
Стационарный компьютер	Intel	Штук	1	140 000	140 000
Монитор	Acer	Штук	1	25 000	25 000
Мышь	A4tech	Штук	1	3000	3000
Клавиатура	A4tech	Штук	1	4000	4000
Принтер	Hp LaserJet P1102	Штук	1	25 000	25 000
Итого:					197 000

$$Зм = 13\ 750 + 197\ 000 = 210\ 750\ (тг)$$

Для реализации программного обеспечения необходимы материалы на сумму 210 750 тенге.

4.3 Расчет затрат на электроэнергию

При разработке программного обеспечения необходимо произвести расчет затрат на электроэнергию. Время работы оборудования для разработки ПО равно 210 часам, данное количество часов было рассчитано в таблице 4.1. Для принтера расчет будет проводиться для периода в 24 часа, так как нет необходимости постоянно использовать принтер.

$$Э = З_{эл.эн.обор.} + З_{доп.нужды.}, \quad (4.2)$$

где $З_{эл.эн.обор.}$ – затраты на электроэнергию оборудования;

$З_{доп.нужды.}$ – затраты электроэнергии на дополнительные нужды.

Расчет электроэнергии, которая необходима для оборудования определяется по следующей формуле:

$$З_{эл.эн.обор.} = \sum W * К_{исц} * S * T, \quad (4.3)$$

где W – потребляемая мощность, Вт;

$К_{исц}$ – коэффициент использования ($К_{исц}$ = 0,7..0,9);

T – время работы;

S – тариф (1кВт/ч = 17,81 тг).

Итоги по расчетам стоимости затрачиваемой электроэнергии представлены в таблице 4.4.

$$З_{эл.эн.обор.} = 8494\ (тенге)$$

Таблица 4.4 – Затраты на электроэнергию

Наименование приборов	Паспортная мощность, кВт	Коэффициент мощности	Время работы оборудования, ч	Цена ЭЭ тг/кВтч	Сумма, тг.
Системный блок	0,3	0,9	210	17,81	793,40
Монитор	0,05	0,9	210	17,81	132,20
Принтер	0,25	0,7	24	17,81	74,80
Кондиционер	2,6	0,9	210	17,81	6876,40
Освещение	0,3	0,7	210	17,81	617,10
Итого:					8494

На дополнительные потребности расходы подсчитываются на основе повышенного показателя в объеме 5% от расходов на электроэнергию:

$$З_{\text{доп.нужды}} = 5\% * З_{\text{эл.эн.обор.}}, \quad (4.4)$$

Определим затраты на дополнительные потребности согласно формуле (4.4):

$$З_{\text{доп.нужды}} = 0.05 * 8494 = 424{,}7 \text{ (тенге)}$$

Исходя из всех расчетов, полные расходы на электроэнергию составляют:

$$Э = 424{,}7 + 8494 = 8918{,}7 \text{ (тенге)}$$

4.4 Расчет затрат на оплату труда

Для разработки программного обеспечения, как указывалось ранее, необходимо два работника:

- технический руководитель – изучение предметной области, анализ требований к системе, координация;
- программист-разработчик – реализация ПП, тестирование продукта.

Сумму расходов на оплату труда можно рассчитать по следующей формуле:

$$З_{\text{тр}} = \sum ЧС_i * T_i \quad (4.5)$$

где $ЧС_i$ - часовая ставка i-го работника, тг;

T_i - трудоемкость разработки модели, чел.×ч; i - категория работника;

n - количество работников, занятых разработкой ПП.

Во время реализации проекта рабочее время участников не равномерно, поэтому имеет смысл установить часовую ставку каждого работника и общий объем заработной платы.

Часовую ставку сотрудника можно рассчитать по следующей формуле:

$$ЧС_i = \frac{ЗП_i}{ФРВ_i} \quad (4.6)$$

где $ЗП_i$ - месячная заработная плата i-го работника, тг;
$ФРВ_i$ - месячный фонд рабочего времени i-го работника, час.

Месячная заработная плата руководителя равняется 220 000 тенге и месячная заработная плата разработчика равняется 200 000 тенге. Рассчитаем часовую ставку каждого работника согласно формуле (4.6):

$$ЧС_{руководитель} = \frac{220\,000}{26 * 8} = 1\,057 \text{ тг/ч}$$
$$ЧС_{разработчик} = \frac{200\,000}{26 * 8} = 961 \text{ тг/ч}$$

Руководитель вовлечен не во все этапы разработки ПО. Этапы, в которых руководитель принимает непосредственное участие: 1, 2, 3, 4, 9.

Часовая ставка руководителя составляет 1 057 (тг/ч), трудоемкость разработки равняется 80 часам. Часовая ставка разработчика составляет 961 (тг/ч), трудоемкость разработки равняется 210 часам. Согласно формуле (4.5) можно рассчитать сумму расходов на заработную плату работников:

$$З_{тр} = 1\,057 * 80 + 961 * 210 = 84\,560 + 201\,810 = 286\,370$$

Расчеты затрат по оплате труда показаны в таблице (4.5).

Таблица 4.5. – Расчет заработной платы

Категория работника	Квалификация	Трудоемкость разработки ПП, час.	Часовая ставка, тг/ч	Сумма, тг.
Руководитель	Проектный руководитель	80	1 057	84560
Разработчик	Программист	210	961	201810
Итого:				286 370

4.5 Расчет затрат по социальному налогу

Согласно Налоговому кодексу Республики Казахстан социальный налог составляет 9,5% от фонта оплаты труда. Социальный налог можно рассчитать по следующей формуле:

$$С_н = (ФОТ - ПО) * 0{,}095 \quad (4.7)$$

где ПО - отчисления в пенсионный фонд, они составляют 10% от ФОТ.

$$ПО = 286\,370 * 0{,}1 = 28\,637 \text{ тенге}$$
$$С_н = (286\,370 - 28\,637) * 0{,}095 = 24\,484 \text{ тенге}$$

Результаты расчетов представлены в таблице (4,6):

Таблица 4.6 – Начисление социального налога

Категория работника	Количество человек	Заработная плата, тг	Пенсионные отчисления, тг	Социальный налог, тг
Технический руководитель	1	84 560	8456	7229,90
Программист-разработчик	1	201 810	20181	17254,10
Итого:				24 484

4.6 Амортизация основных фондов и прочие затраты

Нормы амортизации ОФ необходимо определить в соответствии с налоговым кодексом РК. Амортизацию ОФ можно определить по следующей формуле:

$$A_г = \frac{С_{об} * Н_а}{100} \quad (4.8)$$

где, $С_{об}$ – стоимость оборудования;

$Н_а$ – норма амортизации (норма амортизация = 25);

Формула (4.8) позволяет рассчитать нужную сумму для амортизационных отчислений за год для системного блока :

$$A_г = \frac{140\,000 * 25}{100} = 35\,000 \text{ тенге}$$

Теперь необходимо рассчитать норму амортизации за период разработки:

$$A_г = \frac{35\,000 * 26}{365} = 2\,493{,}2 \text{ тенге}$$

Подобным образом необходимо рассчитать норму амортизации для всего оборудования. Результаты расчетов приведены в таблице (4.7).

Таблица 4.7 – Амортизация ОФ

Наименование оборудования и ПО	Стоимость оборудования и ПО, тг	Годовая норма амортизации, %	Сумма амортизации за год, тг	Сумма амортизации за время разработки, тг
Системный блок	140 000	25	35 000	2 493,20
Монитор	25 000	25	6 250	582
Мышь	3000	25	750	69,90
Клавиатура	4000	25	1000	93,20
Принтер	25 000	25	6 250	582
Итого:			49 250	3 820,30

Смета расходов на разработку ПО.

На основе всех представленных расчетов необходимо оформить смету расходов на разработку ПО согласно форме, которая приведена в таблице (4.8). На рисунке 4.1 продемонстрирована диаграмма рабочих расходов.

Таблица 4.8 – Смета затрат на разработку ПО

Статьи затрат	Сумма, тг
Затраты на оборудование и материальные ресурсы	210 750
Затраты на оплату труда	286 370
Социальные налоги	24 484
Затраты на электроэнергию	8918,70
Амортизация основных фондов	3 820,30
Итого по смете:	534 343

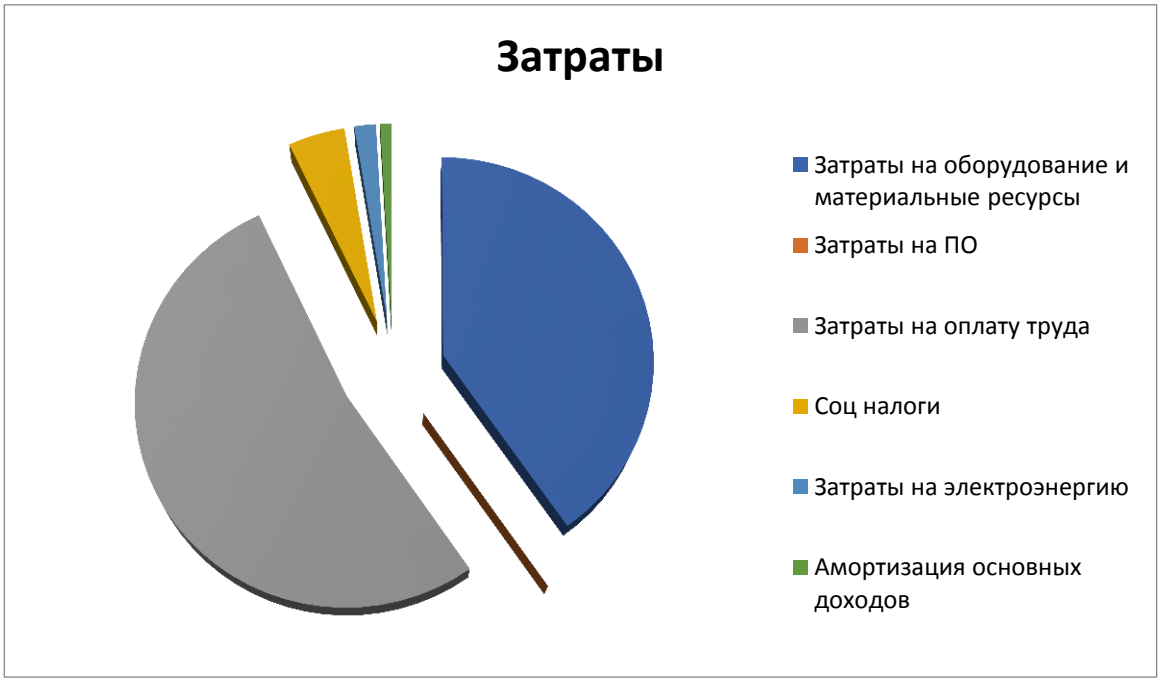


Рисунок 4.1 – Диаграмма затрат

4.7 Определение возможной (договорной) цены ПО

Стоимость программного обеспечения определяется на основе качества разработанного продукта, сроков его разработки и производительности продукта. Стоимость $Ц_Д$ для программного обеспечения можно рассчитать по следующей формуле:

$$Ц_Д = З_{нир}\left(1 + \frac{P}{100}\right), \quad (4.9)$$

где $З_{нир}$ – затраты на разработку программного обеспечения, тг;

Р – средний уровень рентабельности ПО, (%). Данный параметр принят равным 25%.

$$Ц_Д = 534\ 343\left(1 + \frac{25}{100}\right) = 667\ 928{,}8 \text{ тенге}$$

Далее необходимо определить стоимость реализации с учетом НДС, ставка НДС устанавливается законодательством РК. На 2019 года ставка НДС составляет 12%. Стоимость реализации учитывая НДС можно рассчитать по следующей формуле:

$$Ц_р = Ц_д + Ц_д * НДС, \qquad (4.10)$$

$$Ц_р = 667\ 928{,}8 + 667\ 928{,}8 * 0{,}12 = 748\ 080 \text{ тенге}$$

Таким образом, цена реализации составляет 748 080 тенге, себестоимость - 534 343 тенге, прибыль - 133 586 тенге.

Вывод

Данная глава дипломного проекта содержит экономические расчеты, которые позволяют определить затраты необходимые для разработки программного продукта. Расчеты включают в себя:

- расчет трудоемкости разработки программного продукта;
- расчет затрат на разработку программного продукта;
- расчет затрат на электроэнергию;
- расчет затрат на оплату труда;
- расчет затрат по социальному налогу;
- амортизация основных фондов и прочие затраты.

Договорная цена программного продукта равняется 748 080 тенге, данное значение является рациональным с точки зрения экономической эффективности.

5 Безопасность жизнедеятельности

5.1 Анализ условий труда

Организация безопасной корпоративной сети предполагает собой наличие различного компьютерного оборудования и программного обеспечения. Для организации рабочего процесса сотрудников «AGMACSOURCE» необходимо обеспечить их определенными удобствами: просторным рабочим пространством, обеспечивающим комфортное совершение определенных действий и перемещений в ходе рабочего процесса; комфортными креслами, снижающими нагрузку на позвоночник; аспирационными системами, обеспечивающими вентиляцию воздуха и поддерживающими оптимальную комнатную температуру [11].

Рабочее помещение расположено на 6 этаже бизнес центра. Планировка помещения представлена на рисунке.

Рабочее помещение рассчитано для работы 2-х сотрудников (мужчины – 2), имеющих служебные места, включая меня.

Характеристики кабинета: длина L = 5 метров, ширина W= 4 метров, высота H = 3 метра. В кабинете имеется лишь одно окно, что является недостаточной мерой обеспечения вентиляционного процесса. Также присутствует вторая дверь, примыкающая к помещению с серверами. Исходные данные указаны в таблице 5.1.

Используемое оборудование и его характеристики:

- два персональных компьютера;
- принтер.

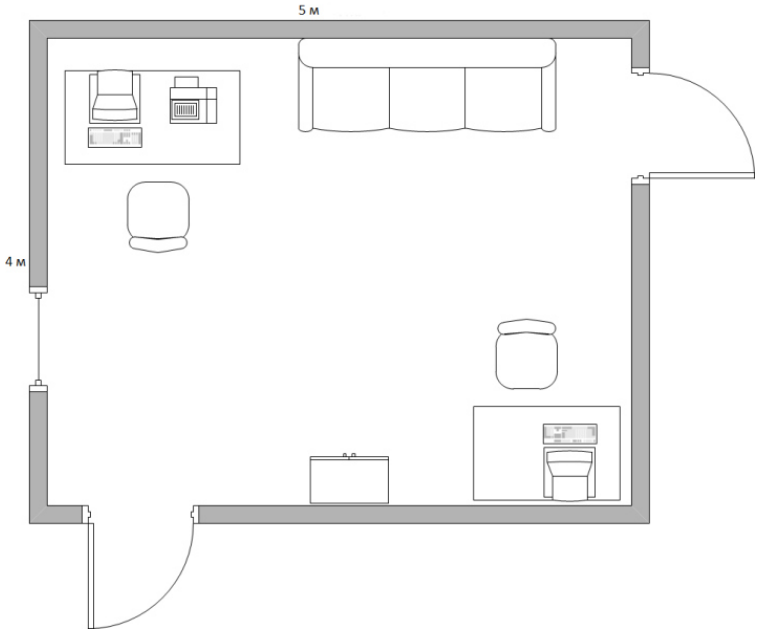


Рисунок 5.1 – Рабочее помещение

Таблица 5.1 – Исходные данные

Город		Алматы
Параметры помещения (L x W x H), м		5 x 4 x 3
Данные по оборудованию	кол-во, шт	2
	мощ. $P_{об}$, кВт/ч	0,65
	КПД, η	0,95
Данные по источникам света	мощ. N ос.уст., Вт/м^2	60
	вид ист. св.	лампы накаливания
Число сотрудников, из них	мужчины	2
	женщины	0
Окна	кол-во	1
	площадь 1 окна, м^2	1.5
	расположение	ЮЗ
	вид	жалюзи, метал. переплеты, одинарные, загрязнение незначительное
Расчетное время суток, ч.	14-15	
Температура в помещении, ^{0}C	летом	25
	зимой	19
Вид положения работы	Сидя	

5.2 Расчет тепловых нагрузок в помещении

В помещениях различного назначения действуют в основном тепловые нагрузки, возникающие снаружи помещения (наружные); а также тепловые нагрузки, возникающие внутри зданий (внутренние).

Наружные тепловые нагрузки характеризуются определенными составляющими:

– теплопоступления или теплопотери в результате разности температур снаружи и внутри здания через стены, потолки, полы, окна и двери.

– разность температур снаружи здания и внутри него летом является положительной, в результате чего имеет место приток тепла снаружи

вовнутрь помещения; и наоборот – зимой эта разность отрицательна и направление потока тепла меняется;

– теплопоступления от солнечного излучения через застекленные площади; данная нагрузка проявляется в форме ощущаемого тепла;

– теплопоступления от инфильтрации.

В зависимости от времени года и времени суток наружные тепловые нагрузки могут быть положительными. Теплопоступления и теплопотери в результате разности температур определяются по формуле 1.1:

$Q_{огр} = V_{пом} * X_о * (t_{Нрасч} – t_{Врасч})$, Вт (1.1), где

$V_{пом}$ – объем помещения, $м^3$;

$V_{пом} = 5*4*3=60$ $м^3$;

$X_о$ – удельная тепловая характеристика, $Вт/м^3*^0С$;

$X_о= 0,33$ $Вт/м^3*^0С$;

$t_{Нрасч}$ – наружная температура (параметр А). Для холодного периода – средняя температура самого холодного месяца в 13 часов, для теплого периода – средней температуре самого жаркого месяца в 13 часов.

$t_{Врасч}$ – внутренняя температура, выбирается с учетом комфортных условий или технологических требований, предъявляемых к производственным процессам.

Для теплого времени года:

$t_{Нрасч} = 29,4$ $^0С$

$t_{Врасч} = 25$ $^0С$

$Q_{огр}= 60*0,33*4,4=87,1$ Вт

Для холодного времени года

$t_{Нрасч} = -9$ 0С

$t_{Врасч} = 19$ 0С

$Q_{огр} = 60*0,33*(-28) = -554,4$ Вт

Избыточная теплота солнечного излучения в зависимости от типа стекла почти до 90% поглощается средой помещения, остальная часть отражается. Максимальная тепловая нагрузка достигается при максимальном уровне излучения, которое имеет прямую и рассеянную составляющие. Интенсивность излучения зависит от ширины местности, времени года и времени суток.

Теплопоступление от солнечного излучения через остекление определяется по формуле 1.2:

$Q_р = (q^I F^I_о + q^{II} F^{II}_о) * βс.з$ (1.2), где

q^I, q^{II} – тепловые потоки от прямой и рассеянной солнечной радиации, $Вт/м^2$;

F^I_0, F^{II}_0 – площади светового проема, облучаемые и необлучаемые прямой солнечной радиацией, $м^2$;

βс.з. – коэффициент теплопропускания. Для штор-жалюзи с металлическими пластинами:

βс.з. = 0,15

При отсутствии наружных затеняющих козырьков, ребер и т. д. для периода облучения остекления солнцем, когда его лучи проникают через окно в помещение $F^{I}_{0} = F^{II}_{0} = F_{0} = 0$, (1.3):

$$Q_р = q^{II} F_0 * \beta с.з = q_{вр} * K^{T}_{1} * K_2 * \beta с.з * n * S_{0;}$$

$q_{вп}$; $q_{вр}$ – тепловые потоки от рассеянной радиации, Вт/м^2. Для широты в 43^{0}СШ (Алматы) после полудня в 14-15 ч. при расположении ЮЗ:

$q_{вр} = 97$ Вт/м^2;

$F_о = nS_о = 1 \cdot 1{,}5 = 1{,}5$ м^2 – площадь светового проема (n – число окон; $S_о$ – площадь 1 окна);

K_1 – коэффициент затемнения остекления переплетами (K^{T}_{1} – для проемов в тени).

$K^{T}_{1} = 1{,}28$;

K_2 – коэффициент загрязнения остекления.

$K_2 = 0{,}95$.

Тогда:

$Q_р = 97*1{,}28*0{,}95*0{,}15*1{,}5 = 26{,}5$ Вт

Внутренние нагрузки в жилых, офисных или относящихся к сфере обслуживания помещениях слагаются в основном из тепла:

- выделяемого людьми;
- выделяемого лампами и осветительными, электробытовыми приборами;
- выделяемого компьютерами, печатающими устройствами фотокопировальными машинами пр.;

Теплопоступления от людей зависит от интенсивности выполняемой работы и параметров окружающего воздуха. Тепло, выделяемое человеком, складывается из ощутимого (явного), то есть передаваемого в воздух помещения путем конвекции и лучеиспусканий, и скрытого тепла, затрачиваемого на испарение влаги с поверхности кожи и из легких [12].

Летом при 24 ^{0}С один мужчина выделяет явного тепла 67 Вт, а общего – 102 Вт. Женщина выделяет 85% от нормы тепловыделений взрослого мужчины. Тогда выделение явного тепла в помещении составит:

$Q_л^{я} = 67*2 = 134$ Вт

А выделение общего тепла:

$Q_л^{о} = 102*2 = 204$ Вт

Зимой при 18 ^{0}С один мужчина выделяет явного тепла 89 Вт, а общего – 104 Вт. Тогда выделение явного тепла в помещении составит:

$Q_з^{я} = 89*2 = 188$ Вт

А выделение общего тепла:

$Q_з^{о} = 104*2 = 208$ Вт

Теплопоступление от осветительных приборов, оргтехники и оборудования рассчитывается следующим образом. Теплопоступление от ламп определяется по формуле (5) [1]:

$$Q_{осв} = \eta \cdot N_{осв} \cdot F_{пол}, \quad Вт \qquad (1.4)$$

где η – коэффициент перехода электрической энергии в тепловую (для лампы накаливания η=0,92-0,97);

$N_{осв}$ – установленная мощность ламп (N=60 Вт/м^2);

$F_{пол}$ – площадь пола:

$F_{пол}$ = 5*4=20 м^2

Тогда:

$Q_{осв}$ = 0,94*60*20 = 1128 Вт

Тепло, выделяемое производственным оборудованием, определяется по формуле (6) [1]:

$$Q_{об} = N_{уст} \cdot K \qquad (1.5)$$

$Q_{об}$ = 0,65 * 2 * 0,95 * 10^3 = 1,24 кВт.

Теплопритоки, возникающие за счёт находящейся оргтехники – это 30% мощности оборудования:

$Q_{орг}$ = 1 * 0,3 * 0,3 * 10^3 = 0,09 кВт

5.3 Расчет теплового баланса помещения

На основании выполненных расчетов составим баланс теплопоступлений в помещении:

$$Q_{изб} = Q_р + Q^я + Q_{осв} + Q_{об} + Q_{орг} + Q_{огр}$$

Лето: $Q_{изб}^{Л}$ = 26,5 + 134 + 1128 + 1240 + 90 + 87,1 = 2,705 кВт

Зима: $Q_{изб}^{З}$ = 26,5 + 188+ 1128 + 1240 + 90 – 554,4 = 2,118 кВт

Так как тепловой баланс для лета больше зимнего теплового баланса, то рассчитаем теплонапряженность воздуха по формуле:

$$Q_н = \frac{Q_{изб.лето} \times 860}{V_{пом}}$$

$$Q_н = \frac{2,705 \cdot 860}{60} = 38,7 \text{ ккал/м3} \ .$$

При $Q_н$ >20ккал/м^3, Δt =8 °С,

при $Q_н$ <20ккал/м^3, Δt =6 °С.

Определение количества воздуха, необходимое для поступления в помещение:

$$L = \frac{Q_{изб} \times 860}{C \times \Delta t \times \gamma}$$

$$L = \frac{2,705 \cdot 860}{0,24 \cdot 8 \cdot 1,206} = 1004,6 \text{ м3/час}$$

где С=0,24 ккал/(кг · °С) – теплоемкость воздуха,

γ=1,206 кг/м^3 – удельная масса приточного воздуха.

Определение кратности воздухообмена:

N = L/$V_{пом}$ = 1004,6/60 = 16,7 час$^{-1}$

5.4 Выбор кондиционера. Схема расположения

Исходя из полученных результатов, для удаления лишнего тепла и очистки воздуха нужно использовать вентиляционную систему, которая способна обеспечить требуемую подачу воздуха L=1004,6 (м3/ч). В данном случае подойдет Кондиционер Daikin FAQ100B/RR100BV Nord-40T. Данный кондиционер способен обеспечить подачу воздуха до 1380 м3 /ч.

Технические характеристики:

- мощность (охлаждение): 3.56 кВт;
- мощность (обогрев): 3.56 кВт;
- потребляемая мощность при охлаждении: 2600 Вт;
- потребляемая мощность при обогреве: 2800 Вт;
- обслуживаемая площадь: 80 м2;
- уровень шума внутреннего блока: 45 дБ;
- уровень шума внешнего блока: 53 дБ;
- цвет: белый.

Характеристики подключения:

- вентиляция: 1380 м3/час;
- класс энергоэффективности при охлаждении/обогреве: A++/A++;
- электропитание, В/Гц/Ф:220 Вт;
- энергопотребление в режиме ожидания не более 1 Вт.

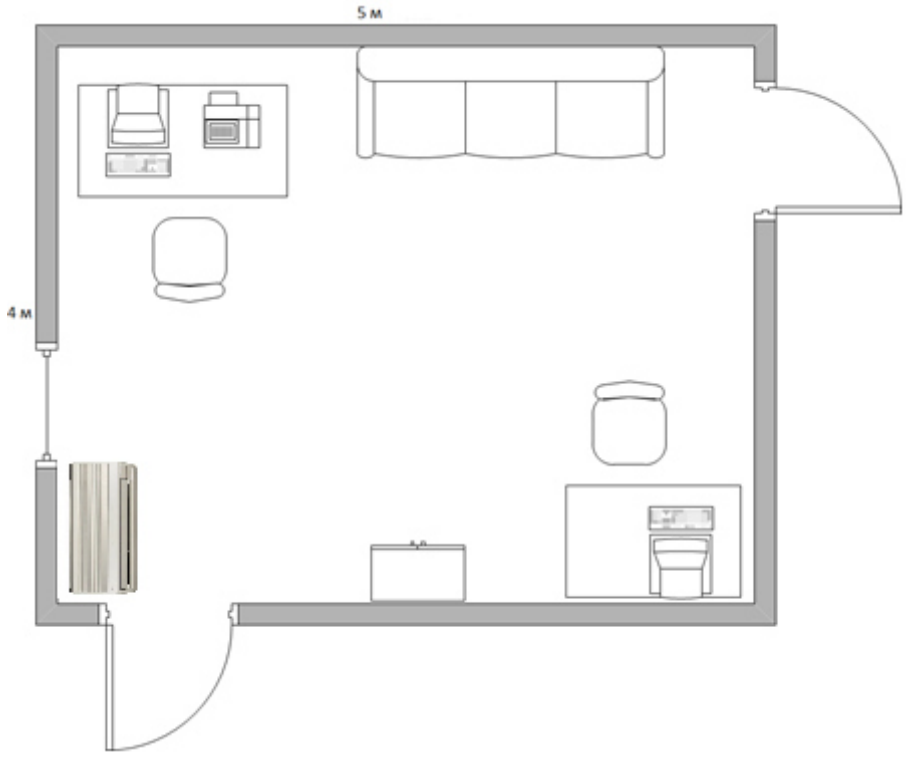


Рисунок 5.2 – Расположение кондиционера

Вывод

В данном разделе дипломного проекта были рассмотрены и рассчитаны воздушные показатели для благоприятных условий труда, а именно, тепловые нагрузки в помещении, наружные и внутренние. Исходя из расчетов, была выбрана модель кондиционера с соответствующими характеристиками. По расчетам можно наблюдать, что избыток тепла летом составляет 2,705 кВт, что делает необходимым установку достаточно мощной системы кондиционирования. Для создания хороших условий труда необходим один кондиционер с подачей воздуха не менее 1004 м3 /ч, в текущем случае был выбран кондиционер Daikin FAQ100B/RR100BV Nord-40T с подачей воздуха до 1380 м3 /ч.

Заключение

Анализ внутренних сетей предприятий показывает, что большинство мелких и средних компаний пренебрегают безопасностью локальной (корпоративной) сети, ссылаясь на разные причины. Одни считают данную меру безопасности дорогостоящей, другие попросту думают, что у них «нечего красть», однако в цифровую эпоху 21-го века любая информация имеет свою ценность в денежном эквиваленте. В своем дипломном проекте я спроектировал безопасную корпоративную сеть для предприятия, пользуюясь open source решениями, что влечёт за собой минимальные затраты. Назревает вопрос о том, почему во многих предприятиях данные меры отсутствуют, если реализация материально незначительна. Ответ кроется в том, что на данный момент в нашем городе дефицит гражданских специалистов в сфере информационной безопасности. Модель, созданная мной, служит образцом корпоративной сети, пригодным как для учебных целей, так и для небольших предприятий.

Пространством для создания моей корпоративной сети послужил гипервизор, в котором комфортно можно создавать виртуальные машины, сопряженные между собой. Для этих целей мной были проведены настройки сетевой среды гипервизора, а конкретно его виртуального коммутатора. Были добавлены портгруппы, соответствующие структурной схеме сети. Во время данного процесса я сделал вывод, что разделение внутри сети посредством VLAN – наибоее практично. Был установлен межсетевой экран pfSense, в котором и было реализовано разделение одной большой структуры на подсети. Данное решение при выполнении проекта являлось фундаментальным, поскольку включает в себя и настройку маршрутизации, NAT, а также средства безопасности.

Корпоративная сеть должна включать в себя определенное количество пользователей, объединенных в группы и департаменты. Для этих целей мною была установлена ОС Windows Server 2012, включающая в себя роли домен-контроллера, DNS, DHCP и Active Directory. Таким образом каждый член пользовательской подсети был объединен и структурирован, а также автоматически получал свой IP адрес.

Перед корпоративной сетью стоит множество задач, в их числе – экономия интернет ресурсов, а также мониторинг деятельности сотрудников. Для этих целей был установлен прокси сервер, являющийся пакетом брандмауэра. С его помощью было организовано кэширование веб-страниц, а также отслеживание ресурсов, посещаемых конечным пользователем. Также нельзя забывать, что сеть – это объект атак злоумышленников. Предотвращением вмешательств в нормальную работу сети выступила система обнаружения вторжений Snort. Её работа была протестирована с положительным результатом.

Список литературы

1 Одом У. Компьютерные сети. Первый шаг. – СПб.: Вильямс, 2006.

2 Таненбаум Э, Уэзеролл Д. Компьютерные сети. – СПб.: Питер, 2012.

3 Корпоративная сеть предприятия – что это такое. URL: https://www.stekspb.ru/autsorsing-it-infrastruktury/it-glossary/corporate-network/ (дата обращения: 17.04.2019)

4 Рындин А.А., Хаустович А.В. Проектирование корпоративных информационных систем. – Воронеж: Юга, 2010.

5 Википедия. Свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/Корпоративная_сеть. (дата обращения: 18.04.2019).

6 Макаллистер Н. Виртуализация серверов. – Ньюкасл: Netswill, 2007.

7 Черняк Л.Я. Виртуализация серверов стандартной архитектуры. – М.: Омега, 2008.

8 Что такое виртуализация и как работает виртуальный сервер. URL: https://habr.com/ru/company/vps_house/blog/344048. (дата обращения: 20.04.2019).

9 Таненбаум Э. Виртуальные локальные сети. – М.: Искра, 2010.

10 Лапонина О. Р. Межсетевое экранирование. – М.: Бином: 2014.

11 Абдимуратов Ж.С., Мананбаева С.Е. Безопасность жизнедеятельности. Методические указания к выполнению раздела «Расчет производственного освещения» в выпускных работах для всех специальностей. – Алматы: АУЭС, 2009.

12 Хакимжанов Т.Е. Расчет аспирационных систем. Дипломное проектирование. Для студентов всех форм обучения всех специальностей. – Алматы: АУЭС, 2014.

13 Бекишева А.И. Методические указания к выполнению экономической части дипломной работы для бакалавров специальности 5В0703 – Информационные системы – Алматы: АУЭС, 2013.

Перечень сокращений

LAN – Local Area Network
RIP – Routing Information Protocol
OSI - Open Systems Interconnection
IP – Internet Protocol
ИТ – Информационные технологии
ПО – Программное обеспечение
ВМ – Виртуальная машина
ОС – Операционная система
ПК – Персональный компьютер
IDS – Intrusion Detection System
NAT – Network Adress Translation
DNS – Domain Name System
AD – Active Directory