МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»
Институт Систем Управления и Информационных Технологии
Кафедра «Системы информационной безопасности»

«ДОПУЩЕН К ЗАЩИТЕ»
Зав.кафедрой _____
(ученая степень, звание, Ф.И.О.)
_____ «_____» _____20____г.
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Моделирование безопасной сети с помощью eve-ng на платформе Windows

Специальность: Системы Информационной безопасности

Выполнил(а) Лоскутов Максим Викторович_____ Группа СИБ-16-2___
(Ф.И.О.)

Научный руководитель к.т.н. профессор Тынымбаев С.Т._____
(ученая степень, звание, Ф.И.О.)

Консультанты:
по специальной части:
старший преподаватель Дмитриева Маргарита Валерьевна_____

_____ «_____» _____20____г.
(подпись)

по безопасности жизнедеятельности:
к.т.н. доцент Приходько Николай Георгиевич_____

_____ «_____» _____20____г.
(подпись)

Нормоконтролер:старший преподаватель Дмитриева Маргарита Валерьевна
(ученая степень, звание, Ф.И.О.)
_____ «_____» _____20____г.
(подпись)

Рецензент: к.т.н. доцент Сейлова Нургуль Абадуллаевна_____
(ученая степень, звание, Ф.И.О.)
_____ «_____» _____20____г
(подпись)

Алматы 2020

Задание на выполнение дипломного проекта

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

Институт Систем Управления и Информационных
Кафедра «Системы Информационной Безопасности
Специальность «Систем Информационной Безопасности»

ЗАДАНИЕ
на выполнение дипломного проекта

Студенту Лоскутову Максиму Викторовичу
(Ф.И.О.)

Тема проекта «Моделирование безопасной сети с помощью Eve-ng на платформе Windows»

Утверждена приказом по университету № _____ от «___» _____2020 г.

Срок сдачи законченного проекта «____» _____ 2020 г.

Исходные данные к проекту (требуемые параметры результатов исследования (проектирования) и исходные данные объекта): Исходные материалы для выполнения задания дипломного проекта – Схема незащищенного модуля сети, сервер Eve-ng,сервер Zentyal, сертификаты компонентов сети, Дополнительное ПО для работы с сервером Eve-ng, виртуальная среда Qemu.

Перечень вопросов, подлежащих разработке в дипломном проекте, или краткое содержание дипломного проекта: Цель работы – создание схемы безопасной сети. Моделирование будет производится в среде виртуальной лаборатории Eve-ng. Компоненты сети виртуализируются с учетом всех реальных особенностей. В схеме сети используются разноплановые механизмы защиты. _____

Перечень графического материала (с точным указанием обязательных чертежей): Топологическая схема сети для компаний малого и среднего бизнеса. __

Основная рекомендуемая литература: Олифер В.Г. Компьютерные сети.Приницпы,технологии,протоколы,официальная документация Designing Cisco Network Service Architectures, веб-сайт www.cisco.com, Хабракен Д. Маршрутизаторы Cisco, Андрончик А.Н. Сетевая защита на базе технологий фирмы Cisco Systems, Поляк-Брагинский А.В. Сеть своими руками.___

Консультации по проекту с указанием относящихся к ним разделов проекта

Раздел	Консультант	Сроки	Подпись
Анализ рисков информационной безопасности	старший преподаватель Дмитриева Маргарита Валерьевна	17.02.2020 – 09.05.2020	
Безопасность жизнедеятельности	к.т.н. доцент Приходько Николай Георгиевич	17.02.2020 – 09.05.2020	

График
подготовки дипломного проекта

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Развертывание виртуальной лаборатории	17.02.2020 – 21.02.2020	
Установка сертификатов компонентов сети	22.02.2020 – 24.02.2020	
Проектирование сетевой топологии	25.02.2020 – 12.03.2020	
Конфигурирование компонентов сети	13.03.2020 - 18.03.2020	
Настройка сетевого окружения	19.03.2020 – 22.03.2020	
Организация защитных мер сети	23.03.2020 - 04.04.2020	
Установка GRE-туннеля и IPsec шифрования	05.04.2020 - 16.04.2020	
Отладка работоспособности безопасной сети	17.04.2020 - 29.04.2020	
Анализ рисков ИБ. БЖД	30.04.2020 - 09.05.2020	

Аннотация

В данной дипломной работе рассматривается построения безопасной сети в виртуальной лаборатории от Eve-ng. Производится анализ лучших практик по построению сетей. Глубокий разбор аксиом и основ сетевых технологий. Рассматриваются компоненты сети используемые для полноценного функционирования сети. Функции и доступные технологии по осуществлению безопасности сетевой коммуникации. Проектирование сети осуществляется в виртуальной лаборатории от Eve-ng.Рассмотрены принципы архитектуры и жизненный цикл построения сети. Взят во внимание вопрос отказоустойчивости и живучести аппаратного комплекса, используемого в виртуальной среде. Создана тестовая схема сети для компании среднего размера. Схема может быть адаптирована и развернута для множества типичных средних компаний. Виртуальная лаборатория Eve-ng развертывается в среде операционной системы Windows.

Abstract

This thesis examines the construction of a secure network in a virtual laboratory from Eve-ng. The analysis of best practices for building networks is performed. Deep analysis of axioms and basics of network technologies. The components of the network used for the full functioning of the network are considered. Functions and available technologies for implementing network communication security. Network design is performed in a virtual laboratory from Eve-ng.The principles of architecture and the life cycle of building a network are considered. The issue of fault tolerance and survivability of the hardware complex used in the virtual environment is taken into account. A test network diagram was created for a medium-sized company. The scheme can be adapted and deployed for many typical medium-sized companies. The Eve-ng virtual lab is deployed in a Windows operating system environment.

Аңдатпа

Бұл дипломдық жұмыста Eve-ng виртуалды зертханасында Қауіпсіз желі құру қарастырылады. Желілерді құру бойынша үздік тәжірибелерге талдау жүргізіледі. Аксиом және желілік технологиялар негіздерін терең талдау. Желінің толық жұмыс істеуі үшін қолданылатын желі компоненттері қарастырылады. Желілік коммуникацияның қауіпсіздігін жүзеге асыру бойынша функциялар және қол жетімді технологиялар. Желіні жобалау Eve-ng виртуалды зертханасында жүзеге асырылады.Архитектураның принциптері және желі құрудың өмірлік циклі қарастырылған. Виртуалды ортада қолданылатын аппараттық кешеннің бас тарту тұрақтылығы мен өміршеңдігі мәселесі назарға алынды. Орташа өлшемді компания үшін желінің тестілік схемасы жасалды. Схема көптеген типтік орта компаниялар үшін бейімделуі және өрістеуі мүмкін. Eve-ng виртуалды зертханасы Windows операциялық жүйесінде орналасқан.

Содержание

Введение

В данный дипломный проект посвящен построению безопасной сети в виртуальной лаборатории Eve-ng. Акцент поставлен на раскрытие вопроса лучших практик построения сети. В наше время все больше желающих добиться успехов в своей области начинают всерьез относится к вопросу безопасности. Безопасность сама по себе является актуальным вопрос. Безопасность же сети используемой компанией для работы с данными будет являться одним из фундаментальных вопрос безопасности функционирования. Перед началом построения сети стоит начать с понимания фундаментальных принципов взаимодействия оборудования и протоколов. Также нужно обратить внимание на принципы построения архитектуры и установленные лучшими практиками аксиомы безопасности. Создаваться сеть будет в виртуальной лаборатории Eve-ng, развернутой на операционной системе Windows 10. Первостепенно нужно понимать, что все гениальное кроется в простом. Сеть будет обладать простой в понимании и надежностью предоставляемых возможностей.

Актуальностью обладает сам вопрос безопасности. Придумать революционно новое решение в вопросе безопасности сетевых технологий является очень сложным, поэтому мы будет использовать лишь известные нам технологии лучших практик. Актуальностью будет являться возможность построения безопасной сети в реальных компания по созданной в дипломной работе схеме.

В дипломной работе имеется две основные главы. Первая является теоретическим обзором по построению безопасной сети. В ней рассматривается архитектура и жизненный цикл проектируемой системы. Приводятся основные положения и аксиомы безопасности используемые в сетевых технология. Собранная информация опирается на лучшие практика в создании безопасных сетей. Вторая глава является практической частью. В ней происходит развертывание лаборатории и создание безопасной сети. Сет будет отличаться простотой и надежностью. Простота позволит ей быть актуальной в применении в реальных условиях. Но при всей простоте технологии используемые для защиты сети будут иметь интересную структуру. Надежность осуществляется за счет четко отлаженного взаимодействия всех компонентов сети.

1 Теоретический обзор к подходам построения безопасной сети

1.1 Постановка целей и задач дипломного проекта

Цель дипломной работы создания схемы безопасной сети, готовой к внедрению в компании с реальными условиями. Оградить от всех возможных угроз не имеет возможным быть. Угроза существует всегда и можно лишь большей или меньшей степени защититься от нее. Разработанная схема будет надежна и закроет большинство уязвимых зон. Для разработки будет использоваться виртуальная лаборатория Eve-ng развернутая на операционной системе Windows 10. Командлет используемый в настройке эмулируемого оборудования стандартный. Эмулироваться в большинстве будет оборудование, предоставляемое компанией Cisco. Функционал разработанной схемы будет доступен в понимании и иметь эшелонированную защиту. Задачи, решаемые созданной сетью:

а) Безопасное функционирование;
б) Своевременная реакция на несанкционированный доступ;
в) Надежность предоставляемого функционала;
г) Отказоустойчивость и живучесть;
д) Наличие современных практик;
е) Универсальность;
ж) Удовлетворение юридических требований.

Требования к проектируемой сети:

а) Разработка на операционной системе Windows 10. Продукт будет ориентирован для реализации в СНГ пространстве, в котором преобладает использование операционной системы Windows 10. Это облегчит процесс внедрения;
б) Разработка в виртуальной лаборатории Eve-ng. Eve-ng является мало кому известным продуктом. Разработчики этого продукта внедряют лучшие решения в области разработки сетей в виртуальном пространстве. Возможно, в будущем они смогут составить конкуренцию крупным компаниям;
в) Использования сертификатов реального оборудования для эмулирования. Это позволяет столкнуться с рядом проблем, встречающихся в реальных условиях, что позволяет приблизить проектируемую систему к реальным условиям;
г) Использования стандартного командлет для настройки оборудования. Позволяет адаптировать разработанную схему во многих компаниях.

1.2 Сеть и ее топология

В наше время сложно представить человека, который не слышал о интернете или им не пользовался. Интернет уверенной поступью зашел в

наши жизни и крепко закрепился в них. Одним из важных аспектов можно выделить Сеть.

Сеть – это некая среда служащая для передачи, хранения, распространения и прочей манипуляции с данными. Данные, находящиеся в сети, необходимо защитить от злоумышленников решивших воспользоваться слабостями системы [1].

Существует такое понятие, как компьютерные сети, под ним понимается некая компьютерная система, соединенная каналами передачи, в свою очередь основным параметров среды передачи является пропускная способность среды передачи. Более общее название компьютерной сети — это вычислительная сеть.

Классификация вычислительных сред по территориальной распространенности:

а) BAN(Body Area Network) – нательная компьютерная сеть) – сеть надеваемых, носимых компьютерных устройств;
б) PAN(Personal Area Network) – персональная сеть, используется для взаимодействия разнообразных устройств одного владельца;
в) LAN (Local Area Network) - локальные сети с замкнутой инфраструктурой, может обслужить от маленькой компании ,базирующейся в нескольких помещениях, до целых промышленных предприятий, суть данной сети это ее закрытость и допуск только ее сотрудников с выделенными им правами досутпа;
г) CAN (Campus Area Network) – Объединение нескольких близко расположенных локальных сетей;
д) MAN (Metropolitan Area Network) – Сети одного или нескольких городов состоящих из множества локальный сетей;
е) WAN (Wide Area Network) – Глобальная сеть, покрывающая большие географические объекты.

Сетевая топология – это структура нашей сети(графа), вершинами которого является вычислительные устройства и ребрами – информационные или физические связи между вершинами [2].

Классификация по сетевым топологиям:

а) Полносвязная – в такой топологии каждое вычислительное устройство напрямую связано со всеми другими;
б) Шина - в такой топологии все вычислительные устройства подключены к одной магистрали, а на концах находятся терминаторы. Вся передача данных осуществляется через магистраль;
в) Звезда – в данной сетевой топологии все вычислительные устройства подключены к одному концентратору, вся передача данных осуществляется через концентратор;
г) Кольцо - данная топология представляет из себя вычислительные устройства соединенные напрямую между собой в одном направлении. Данные в такой сети все время идут по одному направлению, а каждое

вычислительное устройство принимает лишь предназначенную для нее информацию. Реализовывается это все на основании маркера дающего в определенный момент время использовать сети лишь определнной вычислительному устройству, данная топология считается уязвимой, так как выход из строя одного вычислительного устройства приведет к нарушению функционирования всей сети;

д) Дерево – данная топология представляет из себя звездную иерархию, когда от одного вычислительного устройства отходит несколько других от которых в свою очередь отходят другие и таким образом получается четкая иерархия с под топологией звезда, напоминающее дерево;

е) Fat Tree (толстое дерево) - эффективная для создания высокопроизводительной сети, в которой происходит утолщение для получения более высокой пропускной способности.;

ж) Смешанная - такая топология включает с себя множество других топологий и используется при проектировании крупных сетей для достижения максимального эффекта при подборе разных типов топологий под конкретные задачи;

и) Децентрализация – данная сетевая топология предполагается несколько узлов, имеющих разные маршруты соединения на случай выхода их строя какого-либо компонента или участка вычислительной сети.

По типу среды передачи:

а) Проводные;

б) Беспроводные.

Также можно выделить классификацию по типам используемых операционных систем (Windows, Cisco, Unix), по скорости передачи данных, по необходимости постоянной поддержки соединения и т.д.

1.3 Компоненты сети

Далее ознакомимся с основными компонентами, которые могут входить в состав сети, часть других буде рассмотренная дальше[4] .

Маршрутизатор – появился он уже давно вместе с развитием интернета, под маршрутизатором понимается физическое сетевое устройство (компьютер, вычислительное устройство и т.д.) которое используется для передачи информации в локальной сети, между разными сетями и также интернетом, и сетью. Маршрутизатор также выполняет роль DHCP распределяя частные IP-адреса между устройствами сети. Таблица маршрутизации – это то, на что опирается маршрутизатор при построении маршрута передачи пакетов в сети. Таблица маршрутизации может быть обновлена динамически так и статически, когда человек сам прописывается маршруты и интерфейсы, при динамическом обновлении таблица маршрутизации заполняется самостоятельно на основе протокола, с которым он взаимодействует.

Коммутатор (Switch) — это физическое сетевое устройство позволяющее соединять разные участки сети для передачи пакетов между

ними, ранее роль коммутатор была на концентраторе. Концентратор или хаб – это сетевое устройство, к которому подключены вычислительные устройства, но которое не имеет технического оснащения для анализа данных и принятия решения. С коммутаторами все гораздо легче они иммеют возможность адресной отправки по MAC-адресам подключенных вычислительных устройств. Со временем таблица с адресами заполняется и коммутатор понимает куда отправлять пакет. На основании чего можно уверенно сказать, что сетевые коммутаторы используют канальный уровень модели OSI. У сетевых коммутаторов бывают свои режимы работы:

а) С промежуточным хранением и передачей. Коммутатор анализирует и проверяет пакет, тем самым берет его на краткосрочное хранение, а затем убедившись в его подлинности и отсутствии угрозы для системы отправляет получателю;
б) Сквозной режим – менее безопасный, но более быстрый режим, в котором коммутатор лишь пропускает через себя пакеты, не проверяя их содержимое и не проверяя контрольную сумму;
в) Безфрагментарный – в данном режиме считывается MAC – адрес и проверяются первые 64 байта данных, после чего пакет спокойно отправляется получателю, связано это с тем, что большинство ошибок содержится именно в этих первых байтах.

Коммутаторы также можно разделить по полосе пропускной способности на ассиметричные и симметричные, первые имеют на одном устройстве порты с разной пропускной способностью, вторые имеют лишь одинаковую пропускную способность.

Сервер-это компьютер способный на разнообразные манипуляции с данными: хранение, обработка, переправка и т.д. также имеется возможность оказания услуг, когда на сервере крутится определенное ПО. Сервера можно классифицировать по-разному, по объему обслуживаемой аудитории: рабочие группы, локальные предприятия, промышленные компании, города и т.д. Также можно классифицировать по типу решаемых задач: Web-серверы, Серверы баз данных, Серверы печати, Прокси-серверы, Файловые серверы, DHCP- серверы, серверы удаленного доступа, принт-серверы. В итоге мы получаем некий компьютер, способный решать множество разноплановых задач.

DMZ (демилитаризованная зона) – это сегмент сети функции которого направлены на обеспечение безопасности сети. DMZ можно установить на разные сегменты сети, но в большинстве случаев используется на коммутаторе, суть данной технологии заключается в создании барьера между внешней сетью и локальной. Достигается это с использованием межсетевых экранов, фильтрующих поступающий к ним трафик. Для достижения большего эффекта устанавливается два или более межсетевых экранов, дабы если один выйдет из строя другой мог обеспечить безопасную работоспособность сети. На разных межсетевых экранах могут

использоваться разные правила фильтрации, при установке DMZ на сервер можно настроить доступ лишь с определенного узла к определенному компоненту сервера.

IP- телефония – это технология использующая IP сеть для осуществления коммуникации абонентов. Если в сотовой сети используется обращения на станции провайдеров и для осуществления звонка не требуется выход в сеть, то для осуществления звонка по IP-телефону необходим прямой выход в сеть.

Voip-шлюзы – это физические устройства позволяющие телефонным аппаратами, офисным станциям и АТС иметь выход в IP-сеть.

Существует несколько видов IP-телефонии:

а) На каждом из компьютеров есть специальное ПО, которое имеет выход в сеть и связь осуществляется через него, также при таком способе можно иметь возможность вызова абонента из ТСОП(телефонная сеть общего пользования) в таком случае будет отправлен запрос на прокси-сервер, который в свою очередь с использованием интегрированных шлюзов найдет необходимого нам абонента и откроет с ним канал связи;

б) Клиент имеющий телефонный аппарат с использованием ТСОП отправляет запрос к провайдеру IP-телефонии, проходит аутентификацию на основе PIN-кода, затем провайдер находит прокси сервер абонента с которым мы хотим открыть канал связи , и с прокси сервера провайдера отправляется запрос на искомый сервер, а далее и использованием интегрированных шлюзов устанавливается контакт;

в) Используется на телефонных аппаратах с Voip-шлюзом. Абонент, желающий соединится с другим абонентом отправляет вызов, который обрабатывает провайдер, затем пересылает в ТСОП, который определят к кому прокси серверу относится запрашиваемый абонент, находя его создает канал при помощи интегрированного шлюза. При обратном соединении запрашиваемый абонент обрабатывает адрес(телефон) вызывающего, отправляет это запрос в ТСОП, который находит прикрепленный к номеру прокси сервер и при помощи интегрированных шлюзов открывает канал связи.

В итоге мы имеем множество плюсов IP- телефонии:

а) Низкая нагрузка на каналы передачи, данные передаются в цифровом формате и при передаче сжимаются;

б) Низкая цена – для осуществления звонка нам необходимо лишь иметь подключения в сети и нам открываются звонки в любые точки мира;

в) Функциональность – возможность реализовать то, что в телефонной сети либо не реализуемо, либо очень дорого;

г) Безопасность – все данные, передающиеся по каналам IP-телефонии, шифруются и идентифицируются потоком у получателя.

Cisco ASA – физическое сетевое устройство использующееся для достижения безопасности сети, имеющее функции межсетевого экрана и vpn, что позволяет создавать правила фильтрации, и защиту внутренних виртуальных сетей. Используется на множестве предприятий от малого до большого, создателем и дистрибьютером данного продукта является компания Cisco. Ходит много споров что лучше использовать Cisco ASA или Cisco маршрутизатор, на Cisco маршрутизаторе можно легко настроить межсетевой экран, а также VPN, в свою очередь Cisco ASA поддерживает технологию маршрутизации и способна динамически распределять адреса и вести адресную таблицу.

1.4 Основные положения при проектировании безопасной сети

Высокий темп развития технологий в сфере информационной безопасности представляет собой постоянную проблему для организаций. Быстрое распространение ботнетов, растущая изощренность сетевых атак, тревожный рост организованной преступности и шпионажа в Интернете, кража личных данных и данных, более инновационные инсайдерские атаки и появление новых форм угроз в мобильных системах являются примерами разнообразных и сложных реальных угроз, которые формируют современный образ безопасности.

В качестве ключевого фактора, дающего представления для клиентов о надежности продукта, сети должны разрабатываться и внедряться с учетом соображений безопасности для обеспечения конфиденциальности, целостности и доступности данных и системных ресурсов, поддерживающих ключевые бизнес-функции.

Достижение соответствующего уровня безопасности больше не является вопросом развертывания точечных продуктов, ограниченных сетевыми периметрами. Сегодня сложность и изощренность угроз требуют общесистемного подхода и взаимодействия со всеми участниками цепочки. С этой целью предприятия, работающие с данными, имеющими высокую степень риска, используют подход глубокой защиты, где несколько уровней защиты стратегически расположены по всей сети, но в рамках единой стратегии. Информация о событиях и положении дел совместно используется для большей наглядности, а ответные действия координируются в рамках общей стратегии контроля[5].

Множество компаний используют модульные конструкции, которые ускоряют развертывание и облегчают внедрение новых решений и технологий по мере развития потребностей бизнеса. Такая модульность продлевает срок полезного использования существующего оборудования, защищая денежные вложения. В то же время эти проекты включают в себя набор инструментов для облегчения повседневных операций, что сокращает общие оперативные расходы.

1.5 Cisco Security Control Framework (SCF)

В настоящее время наибольшей популярностью пользуются практики Cisco, они включают в себя:

а) Современные решения задач безопасности сети;
б) Серьезные практики по построению сети;
в) Надежные системы защиты;
г) Предоставление качественного оборудования;
д) Систему поддержки и ведению предоставляемого оборудования;
е) Целостную структуру системы;
ж)Документированную базу предоставляемого продукта;
и) Высокий функционал товара.

Cisco SCF-это система безопасности, направленная на обеспечение доступности сети и услуг, а также непрерывности бизнеса. Угрозы безопасности-это постоянно движущаяся цель, и SCF предназначен для решения текущих векторов угроз, а также отслеживания новых и развивающихся угроз с использованием лучших общих практик и комплексных решений. Cisco SAFE использует SCF для создания сетевых конструкций, которые обеспечивают доступность сети и сервиса, а также непрерывность бизнеса. Cisco SCF управляет выбором продуктов и возможностей безопасности и направляет их развертывание по всей сети, где они лучше всего улучшают видимость и контроль[3].

SCF предполагает наличие политики безопасности, разработанной в результате оценки угроз и рисков, а также в соответствии с бизнес-целями и задачами. Предполагается, что политики и руководящие принципы безопасности определяют приемлемое и безопасное использование каждой службы, устройства и системы в окружающей среде. Политика безопасности должна также определять процессы и процедуры, необходимые для достижения бизнес-целей и задач. Совокупность процессов и процедур определяет операции безопасности. Для успеха бизнеса крайне важно, чтобы политика безопасности, руководящие принципы и операции не препятствовали, а скорее расширяли возможности организации для достижения ее целей и задач.

Успех политики безопасности в конечном счете зависит от того, насколько она повышает видимость и контроль. Проще говоря, безопасность можно определить как функцию видимости и контроля. Без всякой видимости нет контроля, а без всякого контроля нет и безопасности. Поэтому основное внимание SCF уделяет повышению видимости и контроля. В контексте SAFE SCF управляет выбором и развертыванием платформ и возможностей для достижения желаемой степени видимости и контроля.

SCF определяет шесть действий безопасности, которые помогают обеспечить соблюдение политик безопасности и улучшить видимость и контроль. Видимость повышается за счет действий по идентификации,

мониторингу и корреляции. Контроль улучшается за счет действий по упрочнению, изоляции и принудительному применению.

Cisco Security Control Framework Model					
Total Visibility			Complete Control		
Identify, Monitor, Collect, Detect and Classify Users, Traffic, Applications and Protocols			Harden, Strengthen Resiliency, Limit Access, and Isolate Devices, Users, Traffic, Applications and Protocols		
Identify	Monitor	Correlate	Harden	Isolate	Enforce
• Identify, Classify and Assign Trust-Levels to Subscribers, Services and Traffic	• Monitor, Performance, Behaviours, Events and Compliance, with Policies • Identify Anomalous Traffic	• Collect, Correlate and Analyze System-Wide Events • Identify, Notify and Report on Significant Related	• Harden Devices, Transport, Services and Applications • Strengthen Infrastructure Resiliency, Redundancy and Fault	• Isolate Subscribers, Systems and Services • Contain and Protect	• Enforce Security Policies • Migrate Security Events • Dynamically Respond to Anomalous

Рисунок 1.1 – Модель контроля

На предприятии существуют различные места в сети, такие как центр обработки данных, кампус и филиал. Безопасные участки получены из применения SCF к каждой точки сети. Результатом является выявление технологий и наилучших общих практик, которые наилучшим образом удовлетворяют каждому из шести ключевых действий по обеспечению видимости и контроля. Таким образом, безопасные реализации включают в себя различные технологии и возможности по всей сети, чтобы получить видимость сетевой активности, обеспечить соблюдение сетевой политики и устранить аномальный трафик. В результате элементы сетевой инфраструктуры, такие как маршрутизаторы и коммутаторы, используются в качестве всепроникающих, принципиальных точек мониторинга политики и обеспечения ее соблюдения.

1.6 Жизненный цикл проектируемой архитектуры

Поскольку потребности бизнеса и безопасности постоянно меняются, современные практики проектирования безопасных сетей выступают за постоянный обзор и корректировку внедрения в соответствии с меняющимися требованиями. Для этого можно использовать цикл архитектуры[10].

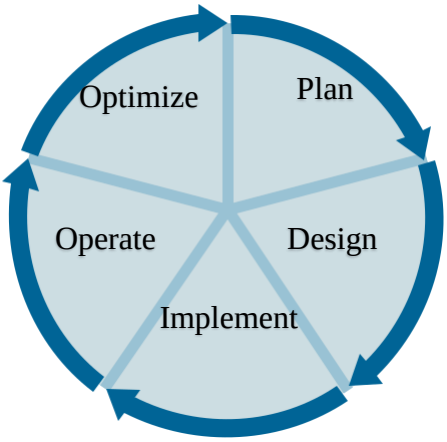

Рисунок 1.2 – Цикл архитектуры

Цикл начинается с планирования, которое должно включать оценку угроз и рисков, направленную на выявление активов и текущего состояния безопасности. Планирование должно также включать анализ пробелов для выявления сильных и слабых сторон существующей архитектуры.

После первоначального планирования цикл продолжается разработкой и отбором сред, возможностей и передовой практики, необходимых для

устранения разрыва и удовлетворения будущих потребностей. Это приводит к детальному проектированию с учетом технический и бизнес требований.

Реализация следует за проектом. Это включает в себя развертывание и подготовку сред и возможностей. Развертывание обычно выполняется в отдельные фазы, что требует последовательности выполнения плана.

Как только новая реализация будет внедрена, ее необходимо будет поддерживать и эксплуатировать. Это включает в себя управление и мониторинг инфраструктуры, а также разведку безопасности для смягчения угроз.

Наконец, поскольку требования к бизнесу и безопасности постоянно меняются, необходимо проводить регулярные оценки для выявления и устранения возможных пробелов. Для этих целей может быть использована информация, полученная в ходе повседневных операций и оценок.

Этот процесс является итерационным, и каждая итерация приводит к реализации, более подходящей для удовлетворения меняющихся потребностей бизнеса и политики безопасности.

1.7 Принципы архитектуры построения безопасных сетей

Процесс построения безопасной сети достаточно серьезный процесс, требующий всеобъемлющего подхода в своей реализации, а также использования лучших практик для достижения цели. На данный момент одними из лучших практик обладает Cisco. Далее рассмотрим принципы на , которые должны опираться люди при построении безопасной сети[10].

Защиты-в-глубину

В современных практиках безопасность встроена во всю сеть, следуя глубокому подходу защиты и обеспечивая конфиденциальность, целостность и доступность данных, приложений, конечных точек и самой сети. Для улучшения видимости и контроля богатый набор технологий и возможностей обеспечения безопасности развертывается на нескольких уровнях, но в рамках общей стратегии.

Модульность и гибкость

Чертежи следуют модульному проектированию, где все компоненты описываются функциональными ролями, а не точечными платформами. Общая сетевая инфраструктура разделена на функциональные модули, каждый из которых представляет собой особый PIN-код, такой как кампус и центр обработки данных. Функциональные модули затем подразделяются на более управляемые и детализированные функциональные слои, и блоки (например, уровень доступа, блок пограничного распределения), каждый из которых выполняет определенную роль в сети.

Модульные конструкции обеспечивают дополнительную гибкость при развертывании, позволяя поэтапно внедрять модули в соответствии с бизнес-потребностями организации. Тот факт, что компоненты описываются функциональными ролями, а не точечными платформами, облегчает выбор наилучших платформ для данных ролей и их возможную замену по мере

развития технологий и потребностей бизнеса. Наконец, модульность конструкции также ускоряет внедрение новых услуг и ролей, продлевая срок полезного использования существующего оборудования и защищая предыдущие капиталовложения.

Доступность и отказоустойчивость услуг

Схемы проектирования включают в себя несколько уровней избыточности для устранения отдельных точек сбоя и максимизации доступности сетевой инфраструктуры. Это включает в себя использование избыточных интерфейсов, резервных модулей, резервных устройств и топологически избыточных путей. Кроме того, в конструкции также используется широкий набор функций, предназначенных для повышения устойчивости сети к атакам и сбоям в работе сети.

Нормативные требования

При проектировании сети вкладывается такое понятие, как базовый уровень безопасности, встроенный как неотъемлемая часть сетевой инфраструктуры. Базовый уровень безопасности включает в себя богатый набор методов и функций обеспечения безопасности, обычно требуемых нормативными актами и стандартами, что облегчает достижение соответствия нормативным требованиям.

Проверка Реализации

Современные практики включают в себя набор инструментов для анализа и проверки функционирования и обеспечения соблюдения гарантий по всей сети, обеспечивая текущее представление о состоянии безопасности сети и помогая оценить соответствие политикам безопасности, стандартам и правилам.

Глобальный обмен информацией и сотрудничество

Многие зарекомендовавшие себя компании активно используют возможности обмена информацией и совместной работы, доступные на продуктах и платформах разных организаций. Информация о регистрации и событиях, генерируемая устройствами в сети, централизованно собирается, отслеживается и коррелируется для обеспечения максимальной видимости. Ответные меры и меры по смягчению последствий координируются централизованно для усиления контроля.

1.8 Аксиомы безопасности

Сетевые среды создаются из множества устройств, служб и информации, конфиденциальность, целостность и доступность которых могут быть нарушены. Правильная защита сети и ее сервисов требует понимания этих сетевых активов и их потенциальных угроз. Каждый сегмент сети можно считать, как цель для компрометации данных пользователя, поэтому рассмотрим сетевые компоненты как цели. Далее мы узнаем разные сегменты сети, ознакомимся с их назначением, узнаем из роли и применение в функционировании безопасной сети, а также разберем их слабые стороны[10].

Цели компонентов сетевой инфраструктуры

Сетевая инфраструктура состоит не только из маршрутизаторов и коммутаторов, но и из большого количества встроенных устройств, включая, но не ограничиваясь ими, брандмауэры, системы предотвращения вторжений, балансировщики нагрузки и устройства ускорения приложений. Все эти инфраструктурные устройства могут подвергаться атакам, направленным непосредственно на них или косвенно влияющим на доступность сети. Возможные атаки включают несанкционированный доступ, повышение привилегий, распределенный отказ в обслуживании (DDoS), переполнение буфера, атаки потока трафика и многое другое.

Как правило, устройства сетевой инфраструктуры предоставляют несколько механизмов доступа, включая консольный и удаленный доступ на основе таких протоколов, как Telnet, rlogin, HTTP, HTTPS и SSH. Упрочнение этих устройств имеет решающее значение для предотвращения несанкционированного доступа и компрометации. Передовая практика включает использование защищенных протоколов, отключение неиспользуемых служб, ограничение доступа к необходимым портам и протоколам, а также принудительную проверку подлинности, авторизацию и учет.

Однако инфраструктурные устройства не все одинаковы. Очень важно понять их уникальные характеристики и природу, чтобы правильно закрепить их. Основная цель маршрутизаторов и коммутаторов-обеспечить возможность подключения, поэтому конфигурации по умолчанию обычно разрешают проход трафика без ограничений.

Кроме того, на устройствах могут быть включены некоторые службы по умолчанию, которые могут не потребоваться для данной среды. Это дает возможность для эксплуатации, и следует предпринять надлежащие шаги, чтобы отключить ненужную услугу.

В частности, в обязанности маршрутизаторов входит изучение и распространение информации о маршруте и, в конечном счете, пересылка пакетов по наиболее подходящим путям. Успешные атаки на маршрутизаторы-это те, которые способны повлиять или нарушить одну, или несколько из этих основных функций путем компрометации самого маршрутизатора, его сеансов работы или информации о маршрутизации. Из-за их природы маршрутизаторы третьего уровня могут быть нацелены на удаленные сети. Рекомендации по обеспечению безопасности маршрутизаторов включают в себя упрочнение устройств, фильтрацию пакетов, ограничение членства в протоколе маршрутизации и контроль распространения и изучения информации о маршрутизации.

В отличие от маршрутизаторов, задача коммутаторов заключается в обеспечении подключения к локальной сети, поэтому они более уязвимы для атак второго уровня, которые чаще всего происходят внутри организации. Распространенные атаки на коммутируемые среды включают широковещательные штормы, наводнения MAC и атаки, предназначенные для

использования ограничений на поддерживающие протоколы, такие как протокол разрешения адресов ARP, протокол динамической конфигурации хоста DHCP и протокол связующего дерева STP. Рекомендации по обеспечению безопасности коммутаторов включают в себя упрочнение устройств, ограничение широковещательных доменов, безопасность SPT, проверку ARP, защиту от спуфинга, отключение неиспользуемых портов и следование рекомендациям VLAN.

Брандмауэры, балансировщики нагрузки и встроенные устройства в целом также подвержены несанкционированному доступу и компрометации, следовательно, их упрочнение имеет решающее значение. Как и любые другие устройства инфраструктуры, встроенные устройства имеют ограниченные ресурсы и возможности, и в результате они также потенциально уязвимы к атакам на истощение ресурсов. Такого рода атаки предназначены для истощения вычислительной мощности или памяти устройства. Это может быть достигнуто путем превышения пропускной способности устройства с точки зрения количества подключений в секунду, максимального количества подключений или количества пакетов в секунду. Атаки также могут быть нацелены на анализ протоколов и пакетов с использованием искаженных пакетов или манипуляций с протоколами. Рекомендации по обеспечению безопасности варьируются в зависимости от характера встроенного устройства.

Сетевые сервисы

Сетевые коммуникации зависят от ряда служб, включая, но не ограничиваясь ими, систему доменных имен (DNS), протокол сетевого времени (NTP) и DHCP. Нарушение работы таких служб может привести к частичной или полной потере связи, а их манипуляции могут служить платформой для кражи данных, отказа в обслуживании (DoS), злоупотребления услугами и другой вредоносной деятельности. В результате все большее число и разнообразие атак постоянно нацеливаются на инфраструктурные сервисы.

DNS обеспечивает взаимодействие между удобными для пользователя доменными именами и логическими IP-адресами. Поскольку доступ к большинству служб в интернете и интрасетях осуществляется по их доменным именам, а не по IP-адресам, нарушение работы DNS, скорее всего, приведет к потере подключения. DNS-атаки могут быть нацелены как на серверы имен, так и на клиенты, также известные как распознаватели. Некоторые распространенные атаки включают атаки усиления DNS, отравление кэша DNS и захват доменных имен. Атаки усиления DNS обычно состоят из наводнения серверов имен не запрошенными ответами, часто в ответ на рекурсивные запросы. Отравление кэша DNS состоит в злонамеренном изменении или введении записей DNS в кэш сервера, часто используемых для фишинга и атак типа "человек в середине". Угон доменного

имени относится к незаконному акту, когда кто-то крадет контроль над доменным именем у его законного владельца.

Рекомендации по снижению уровня риска включают исправления и анализ DNS-серверы, брандмауэры, используя для управления DNS-запросов и трафика в зоне реализации ИПС, чтобы выявлять и блокировать по DNS-атак и т. д.

NTP, который используется для синхронизации времени между компьютерными системами по IP-сети, используется для целого ряда приложений, основанных на времени, таких как аутентификация пользователей, ведение журнала событий, планирование процессов и т. д. Служба NTP может подвергаться различным атакам, начиная от недоброкачественными серверами NTP, вставки недопустимой информации NTP, до DoS на серверах NTP. Наилучшие методы обеспечения безопасности NTP включают использование одноранговой аутентификации NTP, использование списков контроля доступа, а также упрочнение устройств и т. д.

DHCP — это наиболее широко развернутый протокол для динамической настройки систем по IP-сети. Две из наиболее распространенных атак DHCP-это установка мошеннических DHCP-серверов и подмена адресов DHCP. Мошеннические DHCP-серверы используются для предоставления действительным пользователям неверных сведений о конфигурации, чтобы предотвратить их доступ к сети. Кроме того, мошеннические DHCP-серверы используются для атак man-in-the-middle (MITM), где действительным клиентам предоставляется IP-адрес скомпрометированной системы в качестве шлюза по умолчанию.[11] Подмена адресов DHCP — это еще один распространенный тип атаки. Он состоит из исчерпания пула IP-адресов, доступных DHCP-серверу в течение определенного периода времени, и достигается это путем трансляции поддельных DHCP-запросов одной или несколькими скомпрометированными системами в локальной сети. Рекомендации по защите от DHCP-сервера включает в себя закаливание и использование функций безопасности DHCP для коммутаторов, таких как DHCP snooping и безопасности портов и т. д.

Конечные точки – это цели

Конечная точка сети - это любая система, которая подключается к сети и взаимодействует с другими объектами через инфраструктуру. Серверы, настольные компьютеры, ноутбуки, сетевые системы хранения данных, IP-телефоны, мобильные устройства с поддержкой сети и IP-видеосистемы - все это примеры конечных точек. Из-за огромного разнообразия аппаратных платформ, операционных систем и приложений конечные точки представляют одну из самых сложных проблем с точки зрения безопасности. Обновления, исправления и исправления различных компонентов конечных точек обычно доступны из разных источников и в разное время, что затрудняет поддержание систем в актуальном состоянии. В дополнение к разнообразию

платформ и программного обеспечения портативные системы, такие как ноутбуки и мобильные устройства, часто используются в горячих точках Wi-Fi, гостиницах, домах сотрудников и других средах вне корпоративного контроля. Отчасти из-за проблем безопасности, упомянутых выше, конечные точки являются наиболее уязвимыми и наиболее успешно скомпрометированными устройствами.

Список угроз конечных точек столь же обширен и разнообразен, как и огромное разнообразие доступных платформ и программного обеспечения. Примерами распространенных угроз для конечных точек являются вредоносные программы, черви, ботнеты и спам по электронной почте. Вредоносное программное обеспечение-это вредоносное программное обеспечение, предназначенное для предоставления несанкционированного доступа и/или кражи данных у жертвы. Вредоносные программы, как правило, приобретаются с помощью сообщений электронной почты, содержащих троянскую программу, или при просмотре скомпрометированного веб-сайта. Регистраторы ключей и шпионские программы являются примерами вредоносных программ, предназначенных для записи поведения пользователей и кражи личной информации, такой как номера кредитных карт и социального страхования. Черви — это еще одна форма вредоносного программного обеспечения, которая имеет возможность автоматически распространяться по сети. Ботнеты — это одна из самых быстрорастущих форм вредоносного программного обеспечения, которая способна компрометировать очень большое количество систем для спама электронной почты, DoS на веб-серверах и другой вредоносной деятельности. Ботнеты обычно экономически мотивированы и управляются организованной киберпреступностью. Спам по электронной почте состоит из нежелательной электронной почты, часто содержащей вредоносные программы или являющейся частью фишинг-аферы.

Обеспечение безопасности конечных точек требует уделения пристального внимания каждому из компонентов системы и, что не менее важно, обеспечения осведомленности конечных пользователей. Лучшие практики включают в себя поддержание конечных точек в актуальном состоянии с последними обновлениями, исправлениями и исправлениями; укрепление операционной системы и приложений; внедрение программного обеспечения endpoint security; обеспечение безопасности веб-трафика и трафика электронной почты; а также постоянное информирование конечных пользователей о текущих угрозах и мерах безопасности.

Сетевая инфраструктура – цель для атаки

Целые сегменты Сети также могут быть объектом таких атак, как кража сервиса, злоупотребление сервисом, DoS, MITM и потеря данных. Кража сервиса относится к несанкционированному доступу и использованию сетевых ресурсов; хорошим примером является использование открытых беспроводных точек доступа неавторизованными пользователями.

Злоупотребление сетевыми услугами обходится организациям в миллионы долларов в год и заключается в использовании сетевых ресурсов не по назначению; например, личное использование сотрудниками корпоративных ресурсов. Сети также могут подвергаться DoS-атакам, предназначенным для нарушения работы сетевых служб, и атакам MITM, используемым для кражи личных данных.

Сетевые атаки относятся к числу наиболее трудных для борьбы, поскольку они обычно используют преимущества внутренней характеристики в том, как работает сеть. Сетевые атаки могут работать на уровне 2 или более.

Атаки уровня 2 часто используют преимущества доверительной структуры определенных протоколов уровня 2, таких как STP, ARP и CDP. Некоторые другие атаки уровня 2 могут быть нацелены на определенные характеристики транспортного носителя, такие как беспроводной доступ. Некоторые атаки уровня 2 могут быть смягчены с помощью лучших практик на коммутаторах, маршрутизаторах и беспроводных точках доступа.

Атаки на основе уровня 3 используют IP-транспорт и могут включать манипулирование протоколами маршрутизации. Примерами такого рода атак являются распределенные DoS (DDoS), бреши защиты, диверсия трафика. DDoS работает, заставляя десятки или сотни машин одновременно отправлять ложные данные на целевой IP-адрес. Цель такой атаки заключается не только в том, чтобы отключить определенный хост, но и в том, чтобы сделать всю сеть невосприимчивой. Другие частые атаки уровня 3 заключаются в введении неверных сведений о маршруте в процесс маршрутизации, чтобы намеренно перенаправить трафик, ограниченный целевой сетью. Трафик может быть перенаправлен в черную дыру, делая целевую сеть недостижимой, или в систему, настроенную для работы в качестве MITM. Наилучшие методы защиты от сетевых атак уровня 3 включают в себя защиту устройств, фильтрацию от спуфинга, защиту протокола маршрутизации, сетевую телеметрию, брандмауэры и системы предотвращения вторжений[12].

Приложения – цели для атак

Приложения кодируются людьми и поэтому подвержены многочисленным ошибкам. Необходимо позаботиться о том, чтобы коммерческие и общедоступные приложения были в курсе последних исправлений безопасности. Приложения общественного достояния, а также специально разработанные приложения также требуют проверки кода, чтобы убедиться, что эти приложения не представляют каких-либо рисков для безопасности, вызванных плохим программированием. Это может включать в себя такие сценарии, как способ очистки пользовательского ввода, как приложение выполняет вызовы другим приложениям или самой операционной системе, уровень привилегий, на котором выполняется приложение, степень доверия, которое приложение имеет к окружающим системам, и метод, используемый приложением для передачи данных по сети.

Плохое программирование может привести к переполнению буфера, эскалации привилегий, угадыванию учетных данных сеанса, инъекции SQL, атакам межсайтовых сценариев и т. д. Атаки переполнения буфера предназначены для запуска условия исключения в приложении, которое перезаписывает определенные части памяти, вызывая DoS или позволяя выполнить несанкционированную команду. Эскалация привилегий обычно происходит из-за отсутствия средств контроля принудительной авторизации. Использование предсказуемых учетных данных Пользователя или идентификационных данных сеанса облегчает захват сеанса и атаки на олицетворение пользователя. Инъекция SQL-это распространенная атака в веб-средах, использующих backend SQL и где пользовательский ввод не является должным образом очищенным. Проще говоря, атака заключается в манипулировании вводом данных для запуска выполнения созданного оператора SQL. Межсайтовые сценарии - это еще одна распространенная форма атаки, которая заключается в внедрении вредоносного кода на веб-страницы и в том, что он выполняется после просмотра другими пользователями. Межсайтовые сценарии возможны на веб-сайтах, где пользователи могут размещать контент и которые не могут должным образом проверить вводимые пользователем данные.

Среды приложений могут быть защищены с помощью программного обеспечения endpoint security и упрочнения операционной системы, в которой размещается приложение. Брандмауэры, системы предотвращения вторжений и XML-шлюзы также могут использоваться для смягчения атак на основе приложений.

1.9 Проектирование безопасной сети

Eve-ng в своих проектах использует самые современные и продвинутые практики по работе с сетевым оборудованием, законодателями моды являются Cisco. Проекты Eve-ng были созданы в соответствии с принципами архитектуры и в соответствии с аксиомами безопасности. При все более изощренных атаках точечные решения безопасности уже не являются эффективными. Сегодняшняя среда требует более высокой степени распространения, которая может быть достигнута только с помощью инфраструктурной разведки безопасности и совместной работы. С этой целью схемы проектирования Eve-ng используют различные формы сетевой телеметрии, присутствующие на сетевом оборудовании, устройствах безопасности и конечных точках, чтобы получить последовательное и точное представление о сетевой активности. В рамках мониторинга, анализа и корреляции событий собираются, анализируются и коррелируются данные регистрации и сведения о событиях, генерируемые маршрутизаторами, коммутаторами, брандмауэрами, системами предотвращения вторжений и программным обеспечением для защиты конечных точек. Архитектура также использует совместимость между платформами безопасности, такими как

системы предотвращения вторжений, брандмауэры и программное обеспечение для защиты конечных точек[14].

Сетевое оборудование определяет семь действий безопасности, которые помогают обеспечить соблюдение политик безопасности и улучшить видимость и контроль. Видимость повышается за счет действий по идентификации, мониторингу и корреляции. Предоставляя информацию о безопасности и совместной работе на уровне всей инфраструктуры, проектируемые безопасные сети могут эффективно предлагать следующее:

а) Улучшенная архитектура построения - на уровне всей инфраструктуры обеспечивает цельное видение топологий сети, путей атаки и степени повреждения;
б) Идентификация угроз - сбор и отслеживание тенденций, корреляция и протоколирование информации о событиях помогают определить наличие угроз безопасности, приход к компромиссам и выявление утечек данных;
в) Подтверждение действий - имея возможность отслеживать атаку, когда она проходит через сеть, и имея видимость на конечных точках, архитектура может подтвердить успех или неудачу атаки;
г) Уменьшение количества ложных срабатываний - конечная точка и доступность(целостность) системы помогают определить, действительно ли цель уязвима для данной атаки;
д) Уменьшение объема информации о событии - корреляция событий резко сокращает количество событий, экономя драгоценное время оператора безопасности и позволяя ему сосредоточиться на самом важном;
е) Определение степени серьезности инцидента-улучшенная видимость конечной точки и сети позволяет архитектуре динамически увеличивать или уменьшать степень серьезности инцидента в зависимости от степени уязвимости цели и контекста атаки;
ж) Сокращение времени отклика - наличие видимости по всей сети позволяет определить пути атаки и определить наилучшие места для применения мер по смягчению последствий.

Eve-ng использует общие для всей инфраструктуры возможности разведки и совместной работы, для контроля и смягчения хорошо известных атак и атак нулевого дня. В соответствии с проектами, использующимися в наилучших практиках построение безопасной сети, системы защиты от вторжений, брандмауэры, контроль доступа к сети, программное обеспечение для защиты конечных точек, а также системы мониторинга и анализа работают вместе для идентификации и динамического реагирования на атаки. Как часть контроля и сдерживания угроз, эти проекты имеют возможность идентифицировать источник угрозы, визуализировать ее путь атаки, а также предлагать и даже динамически применять ответные действия. Возможные

ответные действия включают изоляцию скомпрометированных систем, ограничение скорости, фильтрацию пакетов и многое другое.

Контроль улучшается за счет действий "задержать", "изолировать" и "принудить". Приведём некоторые из целей проектов eve-ng:

а) Адаптивная реакция на угрозы в реальном времени-исходные угрозы динамически идентифицируются и могут быть заблокированы в режиме реального времени;
б) Последовательный охват применения политики-меры по смягчению последствий и сдерживанию могут быть применены в различных местах сети для углубленной защиты;
в) Минимизация последствий атаки-ответные действия могут быть динамически инициированы сразу же после обнаружения атаки, минимизируя ущерб;
г) Единая политика и управление безопасностью-единая платформа управления политикой и безопасностью упрощает контроль и администрирование, а также снижает операционные расходы.

Корпоративные сети создаются с помощью маршрутизаторов, коммутаторов и других сетевых устройств, которые поддерживают работу приложений и служб. Поэтому правильная защита этих сетевых устройств имеет решающее значение для продолжения бизнес-операций. Сетевая инфраструктура не только часто используется в качестве платформы для атак, но и все чаще становится непосредственной целью вредоносной деятельности. По этой причине необходимо принять необходимые меры для обеспечения безопасности, надежности и доступности сетевой инфраструктуры. Eve-ng предполагает возможность использования ее виртуальной лаборатории и предоставляет рекомендуемые конструкции для повышения безопасности и лучшие практики для защиты областей управления и управления инфраструктурой. Эта архитектура закладывает прочный фундамент, на котором впоследствии могут быть построены более совершенные методы и приемы.

Лучшие практики и рекомендации по проектированию представлены в следующих областях[16]:

а) Доступ к инфраструктурным устройствам;
б) Устойчивость и живучесть устройства;
в) Инфраструктура маршрутизации;
г) Коммутационная инфраструктур;
д) Применение сетевой политики;
е) Сетевая телеметрия;
ж) Сетевое управление.

Проектная схема соответствует модульной схеме, в которой вся сетевая инфраструктура разделена на функциональные модули, каждый из которых представляет собой свою область действия. Функциональные модули затем

подразделяются на более управляемые и детализированные функциональные слои, и блоки, каждый из которых выполняет определенную роль в сети.

1.10 Защита сетевой инфраструктуры

Рассмотрим лучшие методы обеспечения безопасности самой сетевой инфраструктуры. Это включает в себя установление базовой линии безопасности для защиты области управления и контроля, а также создание прочной основы, на которой впоследствии могут быть построены более совершенные методы и приемы.

Ниже перечислены ключевые области базовой безопасности:

а) Доступ к инфраструктурным устройствам;
б) Инфраструктура маршрутизации;
в) Устойчивость и живучесть устройства;
г) Сетевая телеметрия;
д) Применение сетевой политики;
е) Коммутационная инфраструктура.

Приведём распространённые виды атак на сетевую инфраструктуру:

а) Отказ в обслуживании (DoS);
б) Распределенные DoS (DDoS);
в) Несанкционированный доступ;
г) Перехват сеанса;
д) Атака "человек-в-середине" (MITM) ;
е) Повышение привилегий;
ж) Вторжения;
и) Боты;
к) Атаки по протоколу маршрутизации;
л) Атаки на связующее дерево.

Доступ к устройствам инфраструктуры

Защита сетевой инфраструктуры требует обеспечения доступа управления к этим устройствам инфраструктуры. Если доступ к инфраструктурному устройству нарушен, то может быть нарушена безопасность и управление всей сетью. Следовательно, крайне важно установить соответствующие меры контроля для предотвращения несанкционированного доступа к инфраструктурным устройствам.

Устройства сетевой инфраструктуры часто предоставляют целый ряд различных механизмов доступа, включая консольные и асинхронные соединения, а также удаленный доступ на основе таких протоколов, как Telnet, rlogin, HTTP и SSH[16]. Некоторые механизмы обычно включены по умолчанию с минимальной безопасностью, связанной с ними. По этой причине каждое устройство инфраструктуры должно быть тщательно проверено и настроено таким образом, чтобы обеспечить включение только поддерживаемых механизмов доступа и их надлежащую защиту.

Основные меры по обеспечению как интерактивного, так и управленческого доступа к инфраструктурному устройству заключаются в следующем:

а) Ограничение доступности устройств-ограничить доступные порты и ограничить разрешенные коммуникаторы и разрешенные методы доступа;
б) Юридическое обоснование -отображение юридического обоснования, разработанного совместно с юридическим консультантом компании для интерактивных сессий;
в) Аутентификация доступа-убедитесь, что доступ предоставляется только аутентифицированным пользователям, группам и службам;
г) Авторизация действий-ограничение действий и представлений, разрешенных любым конкретным пользователем, группой или сервисом;
д) Обеспечение конфиденциальности данных-защита локально хранимых конфиденциальных данных от просмотра и копирования;
е) Журнал и учетная запись для всего доступа-запись того, кто обращался к устройству, что произошло и когда для произведения аудита.

Защита Локальных Паролей

Пароли, как правило, должны поддерживаться и контролироваться централизованным AAA-сервером. Тем не менее, во многих устройствах инфраструктуры, информацию можно хранить на локальном уровне. Некоторые локальные пароли и секретная информация могут потребоваться, например, для локального резервного копирования в случае отсутствия серверов AAA, специальных имен пользователей, секретных ключей и другой информации о паролях.

Глобальное шифрование пароля, локальное шифрование пароля пользователя и enable secret-это функции, доступные в Cisco IOS для защиты локально хранящейся конфиденциальной информации:

Включите автоматическое шифрование паролей с помощью глобальной команды service password-encryption. После настройки все пароли шифруются автоматически, включая пароли локально определенных пользователей.

Определите локальный пароль включения с помощью команды enable secret global. Включение должно быть доступно обработано с помощью протокола AAA, такого как TACACS+. Локально настроенный пароль включения будет использоваться в качестве резервного механизма после настройки AAA.

Определите строку с паролем с помощью команды password line для каждой строки, которую вы планируете использовать для администрирования системы. Обратите внимание, что такие пароли используются для начальной настройки и не действуют после настройки AAA. Также обратите внимание, что некоторые устройства могут иметь более 5 VTYs.

Обратите внимание, что алгоритм шифрования, используемый командой service password-encryption, является шифром Vigenere, который можно легко изменить. Следовательно, эта команда в первую очередь полезна для удержания несанкционированных лиц от просмотра паролей в конфигурационном файле.

Внедрение баннеров уведомлений

Рекомендуется, чтобы во всех интерактивных сеансах был представлен баннер с юридическим уведомлением, чтобы пользователи были уведомлены о применяемой политике безопасности и о том, что они подчиняются ей. В некоторых юрисдикциях гражданское или уголовное преследование злоумышленника, который врывается в систему, проще или даже требуется, если представлен законный баннер с уведомлением, информирующий несанкционированных пользователей о том, что их деятельность фактически не законна. В некоторых юрисдикциях также может быть запрещено контролировать деятельность неавторизованного пользователя, если он не был об этом уведомлён ил не дал согласие[17].

Требования к юридическому уведомлению являются сложными и различаются в каждой юрисдикции и ситуации. Даже в пределах юрисдикции юридические мнения различаются, и этот вопрос следует обсудить с вашим собственным юрисконсультом, чтобы убедиться, что он соответствует требованиям компании, местным и международным правовым требованиям. Это часто имеет решающее значение для обеспечения надлежащих действий в случае нарушения безопасности.

В сотрудничестве с юридическим консультантом компании заявления, которые могут быть включены в баннер юридического уведомления, включают следующее:

а) Уведомление о том, что доступ к системе и ее использование разрешены только специально уполномоченным персоналом, и уведомление о том, кто может предоставить это разрешение;
б) Уведомление о том, что несанкционированный доступ и использование системы являются незаконными и могут подлежать гражданскому или уголовному наказанию;
в) Уведомление о том, что доступ и использование системы могут регистрироваться или контролироваться без дополнительного уведомления, а полученные журналы могут использоваться в качестве доказательств в суде;
г) Дополнительные конкретные уведомления, требуемые местными законами.

С точки зрения информационной безопасности, а не юридической, баннер юридического уведомления не должен содержать никакой конкретной информации об устройстве, такой как его имя, модель, программное обеспечение, местоположение, оператор или владелец, поскольку этот вид информации может быть полезен злоумышленнику[18].

Безопасный Административный Доступ

Следуйте этим рекомендациям для обеспечения безопасного административного доступа:

а) Включить доступ по SSH при наличии небезопасного телнет соединения. Использовать с минимальным размером модуля 768 бит;

б) Избегайте доступа по протоколу HTTP. Если есть возможность использовать HTTPS;

в) Отключите ненужные линии доступа. Отключены те порты, которые не будут использоваться с командой no exec;

г) В каждой используемой строке явно определите протоколы, разрешенные для входящих и исходящих сеансов. Ограничение исходящих сеансов предотвращает использование системы в качестве промежуточного узла для других атак. Однако следует отметить, что исходящее Telnet соединение может потребоваться для управления интегрированными модулями, такими как сетевой модуль Cisco IPS для маршрутизаторов Cisco ISR;

д) Используйте базовые ACL для управления источниками, из которых будут разрешены сеансы. Источником обычно является подсеть, в которой находятся администраторы. Также стоит использовать ACL с расширенными списками, для настройки типа протокола, используемого между узлами;

е) Зарезервируйте последний VTY. Настроить доступ-класса, использовать только на безопасном оборудовании;

ж) Установить ожидания и времени ожидания сеанса—установить ожидания и времени ожидания сеанса в каждую линию. Включите TCP keepalives для обнаружения и закрытия зависших сеансов.

1.11 Лучшие практики использования маршрутизации

Маршрутизация является одной из наиболее важных частей инфраструктуры, которая поддерживает работу сети, и поэтому крайне важно принять необходимые меры для ее защиты. Существуют различные способы скомпрометировать маршрутизацию - от введения нелегитимных обновлений до DoS, специально разработанных для нарушения маршрутизации. Атаки могут быть нацелены на устройства маршрутизации, пиринговые сеансы или информацию о маршрутизации.

Лучшие практики по проектированию используют следующие меры для эффективной защиты плоскости маршрутизации:

а) Ограничить членство в протоколе маршрутизации— ограничить сеансы маршрутизации доверенными одноранговыми узлами, проверить происхождение и целостность обновлений маршрутизации;

б) Контроль распространения маршрута-применение фильтров маршрутов для обеспечения распространения только действительной информации о маршруте. Управление обменом информацией о маршрутизации между

одноранговыми узлами маршрутизации и между процессами перераспределения;

в) Контроль статуса сеансов - необходимо вести журнал логов, содержащий информацию о текущем сеансе и произведенных изменениях в его ходе.

Ограничение членства в протоколе маршрутизации

Многие протоколы динамической маршрутизации, в частности протоколы внутренних шлюзов, реализуют механизмы автоматического обнаружения одноранговых узлов, облегчающие развертывание и настройку маршрутизаторов. По умолчанию эти механизмы работают в предположении, что все одноранговые узлы должны быть доверенными, что позволяет устанавливать сеансы пиринга с фиктивных маршрутизаторов и вводить ложные данные маршрутизации. К счастью, Cisco IOS предоставляет ряд рекомендуемых функций, предназначенных для ограничения сеансов маршрутизации доверенными одноранговыми узлами и помогающих проверить происхождение и целостность обновлений маршрутизации:

а) Включите проверку подлинности соседей, чтобы обеспечить подлинность соседних маршрутов и целостность их обновлений маршрутизации. Доступно для BGP, IS-IS, OSPF, RIPv2 и EIGRP. Используйте аутентификацию по алгоритму дайджеста сообщений версии 5 (MD5), а не небезопасную аутентификацию по обычному тексту. Чтобы нормально функционировать, аутентификация соседей должна быть включена на обоих концах сеанса маршрутизации;

б) Используйте команду пассивного интерфейса по умолчанию при включении маршрутизации в диапазонах сети, соответствующих большому числу интерфейсов. Команда “passive-interface default” изменяет логику конфигурации на пассивную по умолчанию, предотвращая распространение обновлений маршрутизации на интерфейсе, если только интерфейс явно не настроен с помощью команды “no passive-interface”. Это позволяет выборочно включить распространение обновлений маршрутизации по интерфейсам, которые, как ожидается, будут частью процесса маршрутизации;

в) При использовании BGP включите проверку безопасности TTL, также известную как обобщенный механизм безопасности TTL (GTSM, RFC 3682). Проверка безопасности TTL предотвращает атаки DoS на основе маршрутизации, несанкционированный пиринг и сброс сеансов, запущенные из систем, не подключенных непосредственно к той же подсети, что и маршрутизаторы-жертвы. Для правильной работы проверка безопасности TTL должна быть настроена на обоих концах сеанса BGP.

Фильтрация Распространения Маршрутов

Фильтрация маршрутов-это еще один важный инструмент для обеспечения безопасности инфраструктуры маршрутизации. Большинство

протоколов маршрутизации допускают настройку фильтров маршрутов, которые предотвращают распространение приватных маршрутов по всей сети. С точки зрения безопасности эти фильтры полезны, поскольку они помогают гарантировать, что частные участки сети не отображаются в общедоступном пространстве сети.

Фильтрация маршрутов может быть разделена на две формы:

а) Фильтрация маршрутной информации, передаваемой между узлами маршрутизации;

б) Фильтрация маршрутной информации, передаваемой между процессами маршрутизации в одном маршрутизаторе в результате перераспределения.

Реализовать фильтрацию одноранговых префиксов по краям позволяет контролировать входящие фильтры по краям. Это позволит гарантировать, что в сеть будут введены только ожидаемые маршруты. Баланс между более высоким контролем и связанной с ним операционной нагрузкой.

Развертывайте фильтры на краях, откуда, скорее всего, может быть введена неверная информация о маршрутизации, например на краю глобальной сети. Управление входящими обновлениями маршрутизации на границе глобальной сети не только смягчает введение фиктивных маршрутов в филиалах, но и предотвращает превращение филиала с двойным доступом в транзитную сеть.

Если требуется перераспределение маршрутов, примените фильтры перераспределения, чтобы строго контролировать, какие маршруты объявляются. Реализация фильтров перераспределения маршрутов помогает сдерживать последствия потенциальной инъекции недопустимых маршрутов, предотвращает циклы и помогает поддерживать стабильность сети.

Также необходимо применение фильтров маршрутов на тупиковых маршрутизаторах и удаленных местах с тупиковыми сетями, данные фильтры позволят предотвратить распространения недопустимой информации о маршруте.

Ведение журнала изменений состояния

Частые изменения состояния соединения и сбросы являются общими симптомами проблем сетевого подключения и стабильности сети, которые должны быть исследованы. Эти симптомы могут также указывать на продолжающиеся атаки на инфраструктуру маршрутизации. Регистрация изменений состояния сеансов-это хорошая практика, которая помогает выявить такие проблемы и облегчает устранение неполадок. В большинстве протоколов маршрутизации ведение журнала сообщений об изменении состояния включено по умолчанию. Если этот параметр включен, то каждый раз, когда сеанс маршрутизатора изменяется или испытывает сброс, маршрутизатор генерирует сообщение журнала. Если включен системный журнал, то сообщение пересылается на сервер системного журнала. В противном случае оно хранится во внутреннем буфере маршрутизатора.

Ведение журнала сообщений об изменении состояния в BGP по умолчанию отключено; чтобы включить его, используйте команду маршрутизатора BGP “log-neighbor-changes”. По умолчанию состояние журнала EIGRP и OSPF изменяется. Если он отключен, его можно включить с помощью команды “EIGRP log-neighbor-changes router” для EIGRP и команды “log-adjacency-changes router” для OSPF.

1.12 Рекомендации по отказоустойчивости и живучести устройств

Маршрутизаторы и коммутаторы могут подвергаться атакам, направленным на то, чтобы косвенно повлиять на доступность сети. Возможные атаки включают DoS, основанные на несанкционированных и санкционированных протоколах, распределенные DoS, атаки переполнения, рекогносцировку, несанкционированный доступ и многое другое. Рассмотрим лучшие применяемые практики, предназначенные для сохранения устойчивости и живучести маршрутизаторов и коммутаторов, помогая сети поддерживать доступность даже во время выполнения атаки:

а) Отключение ненужных служб;
б) Использование ACL для защиты инфраструктуры;
в) Управление перегрузками маршрутизаторов (CoPP);
г) Безопасность портов;
д) Избыточность.

Отключение ненужных служб

Чтобы облегчить развертывание, маршрутизаторы и коммутаторы выходят из коробки со списком включенных служб, которые считаются подходящими для большинства сетевых сред. Однако, поскольку не все сети имеют одинаковые требования, некоторые из этих служб могут быть не нужны и поэтому могут быть отключены.

Отключение этих ненужных служб имеет два преимущества: это помогает сохранить системные ресурсы и устраняет потенциал эксплойтов безопасности на отключенных службах[18].

Рассмотри несколько общих рекомендаций:

а) Идентификация открытых портов - используйте команду “show control-plane host open-ports”, чтобы увидеть, какие порты UDP/TCP прослушивает маршрутизатор, и определить, какие службы необходимо отключить;
б) Глобальные службы отключены по умолчанию—если это не требуется явно, убедитесь, что finger, identification (identd), а также небольшие серверы TCP и UPD остаются отключенными на всех маршрутизаторах и коммутаторах;
в) Глобальные службы включены по умолчанию—если явно не требуется, BOOTP, IP- подобная маршрутизация и PAD-службы должны быть отключены глобально на всех маршрутизаторах;
г) IP-направленное вещание-убедитесь, что направленное вещание остается отключенным на всех интерфейсах;

д) Отключение CDP - отключите CDP на интерфейсах, где служба может представлять опасность. Например, на внешних интерфейсах, таких как те, что находятся на границе интернета, и только для данных портах в кампусе и филиале доступа;
е) Внешние порты и доступ-если не требуется, отключите MOP, IP-перенаправления и прокси-ARP на всех интерфейсах доступа и внешних интерфейсах. Это обычно включает в себя линии доступа в филиалах, а также внешние порты, такие как те, что находятся на границе Интернета.

Использование ACL для защиты инфраструктуры

Списки контроля доступа для защиты инфраструктуры (iacl) — это метод контроля доступа, который защищает сетевую инфраструктуру от внутренних и внешних атак. IACLs(Infrastructure access control list) -это метод, основанный на расширенных ACL, первоначально разработанных интернет-провайдерами (ISP) для защиты своих сетевых инфраструктур, но в последствии они получили широкое распространение во многих предприятиях желающих защитить свою инфрастрктуру.

В двух словах, iacl-это расширенные ACL, предназначенные для явного разрешения трафика управления, связанного с оборудованием инфраструктуры, таким как маршрутизаторы и коммутаторы, в то же время запрещая любой другой трафик, который не должен проходить через заданную инфраструктуру. Например, iACL, развернутый на пиринговом крае провайдера, настроен для явного разрешения сеансов BGP от известных одноранговых узлов, в то же время запрещая любой другой трафик, предназначенный к пиринговому маршрутизатору провайдера, а также к остальному адресному пространству инфраструктуры.

ACL наиболее полезны при развертывании на краях сети, где инфраструктура становится доступной для внутренних или внешних пользователей. Также на административных границах, где встречаются оборудование или ссылки под другим управлением. На предприятии ACL могут быть развернуты на многих краях сети:

а) WAN edge-защита базовой инфраструктуры от возможных угроз, исходящих из удаленных филиалов и мест расположения партнеров;
б) Доступ к кампусу/филиалу-защита инфраструктуры от возможных атак, исходящих из локальных сетей;
в) Пограничные фильтры интернета могут быть сконструированы таким образом, чтобы функционировать как iACL для защиты инфраструктуры от внешних угроз.

Хотя существует общая структура для построения iacl, фактические записи ACL будут сильно отличаться в зависимости от окружающей среды. IACL, построенный без должного понимания протоколов и задействованных устройств, может в конечном итоге оказаться неэффективным и даже привести к полной открытости для проведения хакерских атак на сеть. По

этой причине лучший подход к построению iACL-начать с ACL обнаружения, чтобы идентифицировать трафик и не контролировать доступ. IACL должен применяться только тогда, когда протоколы и порты, используемые инфраструктурой надежны и понятны.

2 Проектирование безопасной сети в виртуальной среде eve-ng

2.1 Развертывание и установка

В данной главе дипломной работы нам необходимо спроектировать безопасную сеть. Сеть будет проектировать в виртуальной лаборатории Eve-ng и будет иметь все необходимые параметры и функции для внедрения в офисах среднего и малого бизнеса. Для наглядности проектироваться сеть будет для компании “Marvel”, являющийся представителем среднего бизнеса. В состав компании будет входить центральный офис, берущий на себя основную часть нагрузки и два филиала, находящиеся в разных городах. Центральный офис располагается на первом этаже, состоит из 10 помещений и предоставляет 30 рабочих мест. Филиал будет выполнять задачи по оказанию услуг, предоставляемых компанией в области. Обладает менее расширенным спектром услуг, в отличии от центрального и предоставляет 10 рабочих мест.

Наша работа будет выполняться на платформе Windows 10. Перейдем к установке и отладке нашей виртуальной лаборатории. Для начала нам необходимо скачать платформу WMware Workstation в которой мы будет разворачивать виртуальный сервер eve-ng. Скачиваем образ бесплатной версии eve-ng. Также нам будет необходимо установить ряд дополнительного ПО:

а) Putty;
б) Plink;
в) Ultravnc_wrapper.bat;
г) Wireshark_wrapper.bat;
д) Wireshark;
е) UltraVnc (Viewer,Server);
ж) Qemu;
и) FileZilla.

Рисунок 2.1 – Информация о используемой системе

Рисунок 2.2 – Настройка виртуальной машины

После установки всех дополнительных компонентов необходимо развернуть саму виртуальную машину. После установки необходимо

правильно настроить виртуальную машину, после правильно проделанных всех действий мы увидим приветствующее окно eve-ng.

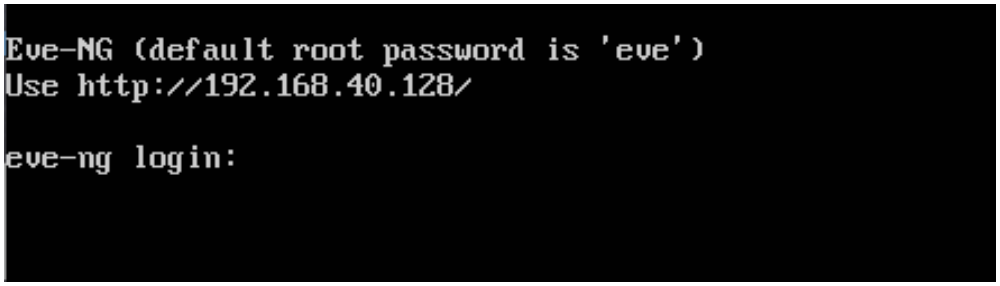

Рисунок 2.1 – Окно аутентификации в eve-ng

Адрес 192.168.40.128 будет использован для входа в виртуальную лабораторию eve-ng. Зайдем в виртуальную лабораторию.

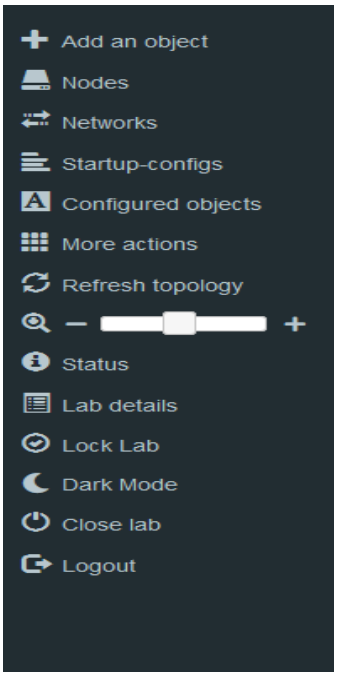

Рисунок 2.2 – Вкладка eve-ng

Поскольку мы будем виртуализировать компоненты сети, с учетом их всех реальных особенностей. Нам понадобиться установить сертификаты на все компоненты сети, которые мы будем использовать. Некоторые сертификаты можно найти в открытом доступе, но большинство необходимо приобретать за деньги. Использующиеся нами компоненты сети будут иметь все параметры реального оборудования.

После установки всех возможных сертификатов и отладки их работы, можно перейти к проектированию сети. Поскольку открытом доступе имеется мало сертификатов будем обходиться тем, что имеем, а точнее: cisco iol, cisco vios, ciscoasa, zentyal.

Проектируема система будет состоять из сетевого пространства главного офиса и филиала. Данные сетевые пространства будут иметь возможность полноценно взаимодействовать между собой, а также с ресурсами из вне. Основные методы, используемые для защиты сетевого пространства: разные виды паролей, ASA, vlan, acl, gre, ipsec.

2.2 Настройка маршрутизации между офисами

Проектирование системы начнем с создания роутера для филиала компании. Создаем и именуем его BranchRT. Команда “hostname BranchRT” позволяет нам это осуществить[19].

Рисунок 2.3 – Установка имени роутера

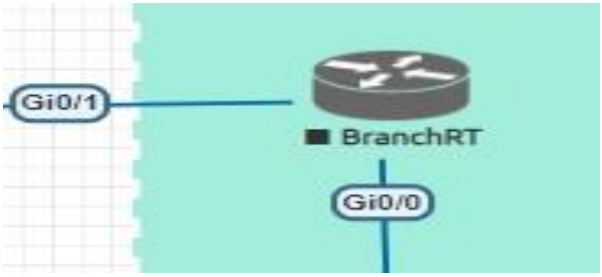

Рисунок 2.4 – Роутер филиала

Далее перейдем к самой настройки роутера BranchRT. Связь внутри филиала будет происходить через интерфейс Gi0/0, в адресном пространстве 10.10.10.200 с маской 255.255.255.0. Команда “int Gi0/0” позволяет нам зайти на необходимый интерфейс, а с помощью “ip address адресной пространство” установить необходимый адрес,также команда “no sh” позволяет включить нам выбранный интерфейс.

Рисунок 2.5 – Настройка роутера BranchRT

После настройки сети внутри филиала, необходимо настроить связь с главным офисом. Связь между главным офисом и филиалом будет осуществляться через ISP (Интернет-провайдер). Заходим на интерфейс Gi0/1 и устанавливаем адрес роутеру 172.168.112.2 с маской 255.255.255.252 для выхода в сеть (см Приложение А).

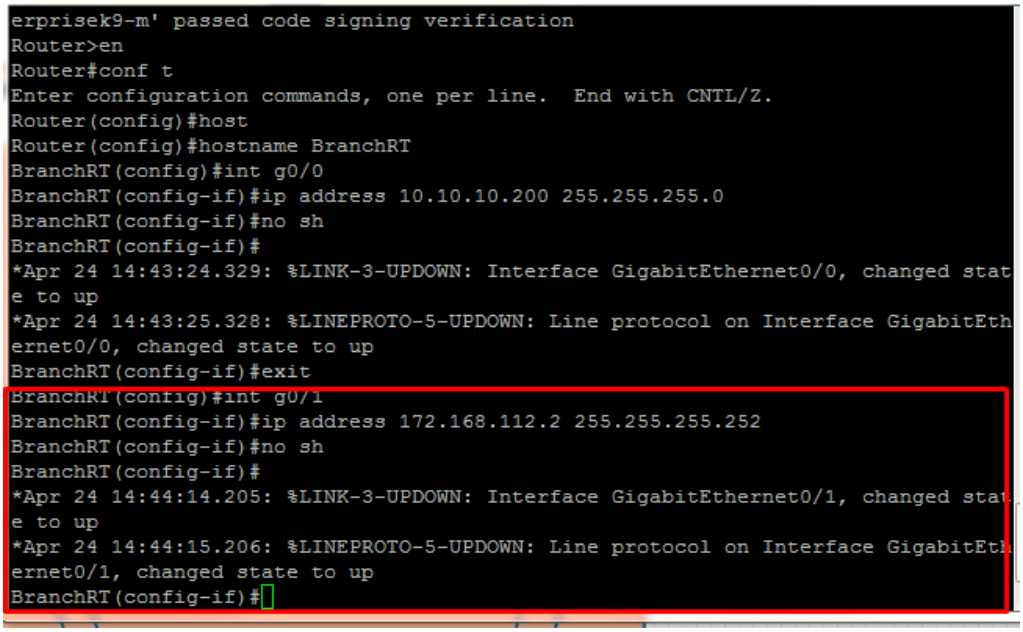

Рисунок 2.6 – Настройка роутера BranchRT

Установим адрес ISP для его взаимодействия с филиалом. Используя интерфейс Gi0/1 и адрес 172.168.112.1 с маской 255.255.255.252.

Рисунок 2.7 – Настройка ISP

Рисунок 2.8 – Схема соединения

Для взаимодействия между ISP и приграничным роутером главного офиса BorderRT будет использоваться адресное пространство 40.0.1.0 с маской 255.255.255.0. Заходим на интерфейс Gi0/0 и устанавливаем адрес 40.0.1.1 с маской 255.255.255.0, и поднимаем его.

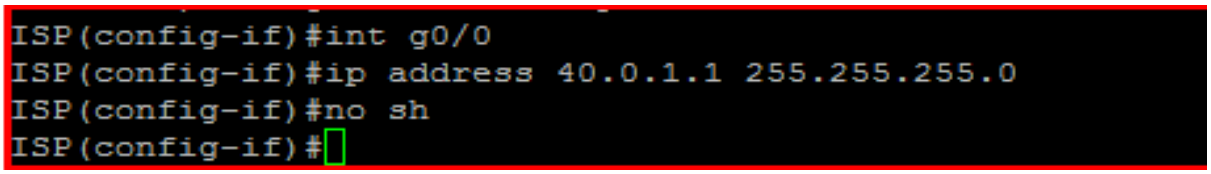

Рисунок 2.9 – Настройка ISP

Далее перейдем к настройке пограничного роутера главного офиса BorderRT.

BorderRT будет взаимодействовать с isp в адресном пространстве 40.0.1.0./24, а с внутренней сетью компании через 30.0.1.0/24. Для настройки выход в сеть зайдем на интерфейс Gi0/0 и установим адрес 40.0.1.2 с маской 255.255.255.0.

Для установки доступа во внутреннюю сеть зайдем на интерфейс Gi0/1 и установим адрес 30.0.1.1 с маской 255.255.255.0.

Рисунок 2.10 – Настройка роутера BorderRT

Настроим возможность прохода всего трафика через BorderRT в ISP используя адрес 40.0.1.1 установленный на ISP в интерфейсе Gi0/0. Команда “ip route 0.0.0.0 0.0.0.0 40.0.1.1” позволяет трафику из любого источника внутренней сети беспрепятственно проходить на ISP.

Рисунок 2.11 – Настройка маршрутизации роутера BorderRT

Теперь настроим маршрутизацию для ISP. Сначала настроим для взаимодействия с филиалом, в филиале используется адресное пространство 10.10.10.200, а для выхода на ISP 172.168.112.2. Используя команду “ ip route 10.10.10.0 255.255.255.0 172.168.112.2” установим маршрутизацию между ISP и BranchRT. По аналогии используя команду “30.0.1.0 255.255.255.0 40.0.1.2”, где 40.0.1.2 адрес BorderRT, а 30.0.1.0 адресное пространство выходящее на ASA, это позволит установить маршрутизацию трафика, исходящего из внутренней сети компании на BorderRT и далее в ISP.

Рисунок 2.12 – Настройка маршрутизации ISP

После настройки маршрутизации приграничного роутера BorderRT и ISP перейдем к настройки маршрутизации пакетов, проходящих через филиал. Команда “ip route0.0.0.0 0.0.0.0 172.168.112.1” мы устанавливаем проход пакетов и ISP с интерфейса Gi0/1. Командой “ip route 40.0.1.0 255.255.255.0 172.168.112” устанавливаем маршрутизацию пакетов от BranchRT через ISP на BorderRT. Командой “ip route 30.0.1.0 255.255.255.0 40.0.1.2” устанавливаем проход пакетов через роутер BorderRT во внутреннюю сеть главного отделения компании.

Рисунок 2.13 – Настройка маршрутизации BranchRT

Рисунок 2.14 – Схема взаимодействия офисов

2.3 Установка vlan в главном офисе

После построения взаимодействия филиала с сетью главного офиса перейдем к обустройству сетевого пространства внутренний сети офиса. Разберем структуру сети внутреннего офиса. Внутренняя сеть главного офиса будет состоять из: свитчей (BorderSw, Per_sw, Dmz_sw), CiscoASA (ASAvPrimary, ASAvSecondary) и DMZ.

В главном офисе для безопасности будет установлено две CiscoAsa, на случай если одна из них выйдет из строя, вторая сразу получит сигнал от первой и приступит к работе[21]. Рассмотрим основные возможности CiscoASA:

а) Статическая и динамическая маршрутизация;

б) Все виды NAT;

в) Динамическое межсетевое экранирование;

г) Modular Policy Framework (конструкция для сортировки пакетов по классам и применения к ним различных действий);

д) Анализ сложных протоколов (FTP, SIP, TFTP, IPSec);

е) IPSec Site-to-site, Easy VPN Server;

ж) SSLVPN;

и) Виртуальные межсетевые экраны;

к) Failover (Active/Standby и Active/Active);

л) Прозрачное экранирование (Transparent Firewall).

DMZ – используется в компании для повышения безопасности локальной сети, он создает разграничение между внешними сервисами, которые может использовать любой человек в сети от внутренних доступ к которым может иметь сотрудник компании.

Перейдем к самой настройки CiscoASA, настраивать будем ASAvPrimary. Настраивать в CiscoASA мы будет Vlan. Vlan(Virtual Local Area Network) – технология позволяющая создавать на одном физическом интерфейсе несколько виртуальных локальных сетей. Используется технология Vlan для разграничения или объединения групп устройств, к которым в дальнейшем можно будет применить политики безопасности.

Переходим к самой настройке, заходим на нужный нам интерфейс “int Gi0/0” , создаем на нем vlan 80, который будет смотреть на приграничный роутер BorderRT. Устанавливаем секьюрити левел(уровень доверия) 0, что значит отсутствие доверия проходящему трафику и даем адрес 30.0.1.10 с маской 255.255.255.0 для нашего vlan. Данный вилан будет служить для выхода на BorderSW.

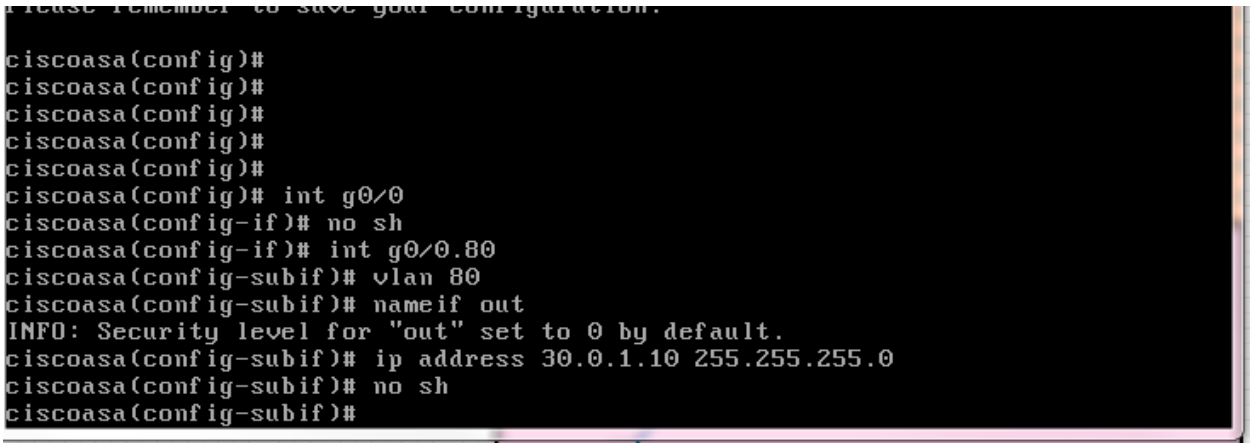

Рисунок 2.15 – Настройка ASAvPrimary

Поднимем еще один vlan на ASAvPrimary, смотрящий на DMZ. Заходим на интерфейс Gi0/1, привязываем к нему 40 vlan. Даем ему имя Dmz и адрес 192.168.40.1 с маской 255.255.255.0 (см. Приложение А). По стандарту всем создаваемым vlan присваивается 0 security-level (отсутствие доверия), изменяем security-level на 60, что значит средний уровень доверия к проходящему трафику через этот vlan.

Рисунок 2.16 – Настройка ASAvPrimary

Далее поднимем еще один vlan для взаимодействия с подключенными устройствами внутренней сети на Per_sw. Заходим на интерфейс Gi0/2 и создаем 50 vlan. Присваиваем ему 100 security-level(полное доверие к проходящему трафику) и даем адрес 192.168.50.1 с маской 255.255.255.0 .

Рисунок 2.17 – Настройка ASAvPrimary

Рисунок 2.18 – Схема соединения

Перейдем к настройке транк портов на свитче Dmz_sw. Trunk port — это коммутационный порт, при помощи которого может передаваться тегированный трафик от одного или нескольких vlan.

Заходим на интерфейс Gi0/0, создаем статический trunk командой “switchport mode trunk”, после его создания автоматически будут разрешены все vlan. Командой “switchport trunk allowed vlan 40,50” разрешим только 40 и 50 vlan. Поскольку мы используем несколько на одном порте несколько vlan нам необходимо настроить инкапсуляцию. Инкапсуляция это “заворачивание” одного фрейма в другой. На одном конце vlan инкапсулируются, а на другом “разинкапсулируются” обратно, мы будем использовать более укороченную

версию инкапсуляции dot1q. Выполним мы это командой “switchport encapsulation dot1q”.

Рисунок 2.19 – Настройка trunk port на dmz_sw

Производим аналогичные настройки на интерфейсе Gi0/1. Мы делаем транк для двух vlan, так как 40 vlan нужен для dmz, а 50 для устройств подключенных к per_sw.

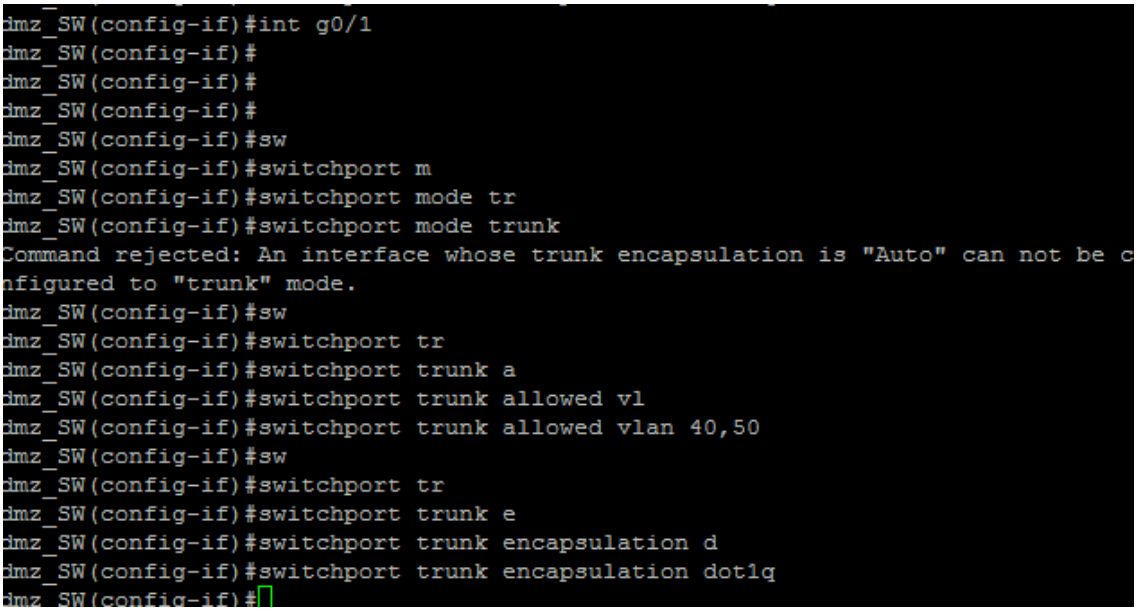

Рисунок 2.20 – Настройка trunk port на dmz_sw

Далее будем использовать access port, это порт, который принадлежит к одному vlan и может передавать нетегированный информационный трафик. Трафик проходящий через 40 vlan будет выходит через интерфейс Gi1/0 на dmz и через Gi1/2 на per_sw. Заходим на интерфейсы и командой “switchport mode access” переходим в access режим, а командой “switchport access vlan 40” разрешаем vlan 40 на данных интерфейсах.

Рисунок 2.21 – Настройка access port на dmz_sw

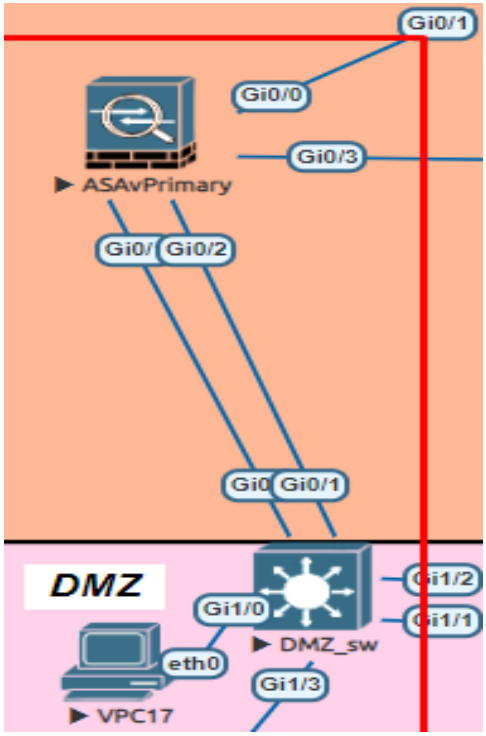

Рисунок 2.22 – Схема соединения

Настраиваем свитч per_SW. Данный свитч дает нам выход на подключенные устройства сотрудников компании. Заходим на интерфейсы, смотрящие на свитч dmz_sw и создаем trunk port для vlan 40,50, что разрешит их трафику спокойно проходить (см. Приложение А).

```
Switch(config)#hostname perSW
perSW(config)#
perSW(config)#
perSW(config)#int g0/0
perSW(config-if)#sw
perSW(config-if)#switchport tr
perSW(config-if)#switchport trunk a
perSW(config-if)#switchport trunk allowed vlan 40,50
perSW(config-if)#no sh
perSW(config-if)#exit
perSW(config)#
perSW(config)#int g0/1
perSW(config-if)#sw
perSW(config-if)#switchport tr
perSW(config-if)#switchport trunk a
perSW(config-if)#switchport trunk allowed vlan
perSW(config-if)#switchport trunk allowed vlan 40,50
perSW(config-if)#no sh
perSW(config-if)#exit
perSW(config)#
```

Рисунок 2.23 – Настройка trunk port на per_SW

Рисунок 2.24 – Схема соединения

2.4 Настройка отказоустойчивости и живучести CiscoASA

В главном офисе компании будет установлено две CiscoAsa. Одна будет основной и выполнять все функции, вторая будет в качестве резервной. В случаи если основная CiscoAsa выйдет из строя, будет передан сигнал на запасную. После получения сигнала, запасная CiscoAsa выгрузит необходимые данные и станет основной.

Настроим основную CiscoAsa именующуюся ASAvPrimary. Заходи на интерфейс Gi0/3 соединяющий ASAvPrimary и ASAvSecondary между собой и поднимаем интерфейс.

```
ciscoasa(config)#
ciscoasa(config)# int g0/3
ciscoasa(config-if)# no sh
ciscoasa(config-if)# exit
```

Рисунок 2.25 – Активация интерфейса

Далее нам необходимо показать свитчу BorderSw наши CiscoASA. Заходим на интерфейс Gi0/0 к которому прикреплен 80 vlan и смотрящий на BorderSW. Командой “ip address 30.0.1.100 255.255.255.0 standby 30.0.1.101” говорим, что адрес основной ASAvPrimary 30.0.1.100, а ASAvSecondary будет иметь логический адрес 30.0.1.101.

Рисунок 2.26 – Настройка ASAvPrimary

Настроим дополнительный адрес для dmz. В случаи отказа основной CiscoASA, дабы не скомпрометировать свою dmz. Заходим на интерфейс Gi0/1 с 40 vlan смотрящим на dmz. Командой “ip address 192.168.40.1 255.255.255.0 standby 192.168.40.101” устанавливаем дополнительный адрес 192.168.40.101 (см Приложение А).

Рисунок 2.27– Установка дополнительного адреса dmz

Установим канал связи между CiscoAsa, для этого заходим на ASAvPrimary, выбираем необходимый интерфейс. Используя команду “link failover g0/3” выбираем интерфейс для канала связи. Командой “ failover interface ip failover 20.0.1.1 255.255.255.252” указываем использующийся адрес. Выполняя команду “lan unit primary” говорим, что ASAvPrimary будет основной(первой).

Рисунок 2.28 – Настройка канала связи

Открываем запасную CiscoASA. Необходимо настроить, чтобы она была запасной(второй). Заходим на нужный интерфейс. Используем аналогичные команды, как при настройке основной. Разница лишь в команде “failover unit secondary”, которая делает ASAvSecondary запасной(второй).

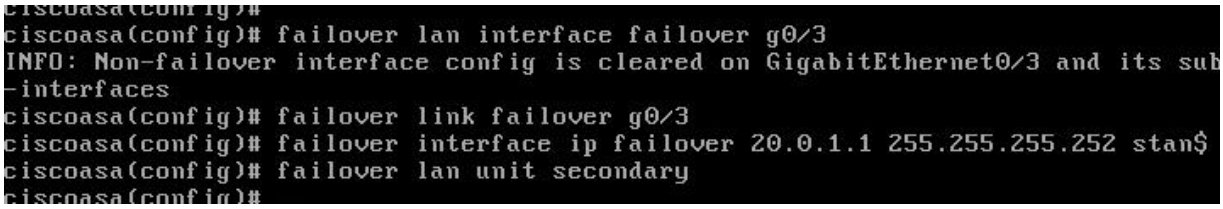

Рисунок 2.29 – Настройка

После настройки CiscoASA произведем тестирования работы. Для тестирование произведем отправку данных через канал передачи с ASAvPrimary на ASAvSecondary. Используя команду “failover” основная CiscoASA, начнет передавать данные, а запасная создавать и принимать CA сертификат. Данные сертификат будет использоваться для подписи передаваемых данных.

Рисунок 2.30 – Передача данных

Используя команду “show”, посмотрим на конфигурационные данные ASAvPrimary и ASAvSecondary. Выделенные строчки говорят нам о состоянии оборудования на данный момент времени. ASAvPrimary находится в состоянии “Active”, то есть сейчас с сетью компании работает она. ASAvSecondary находится в состоянии “Standby Ready”, все ее процессы стоят на месте, но она готова в любой момент включиться в работу.

Рисунок 2.31 – Проверка состояния CiscoASA

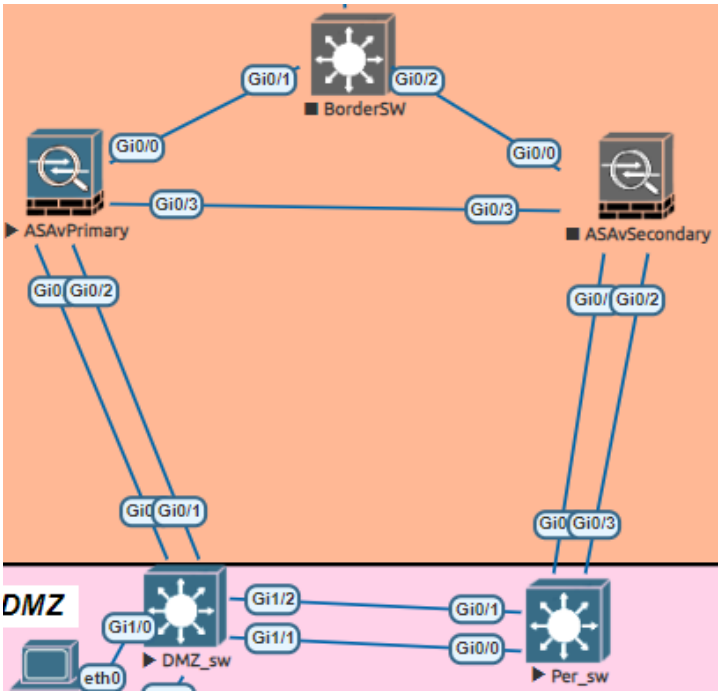

Рисунок 2.32 – Схема взаимодействия

2.5 Конфигурирование ACL листов

Далее займемся созданием ACL листов на ASAvPrimary.ACL листы — это текстовые команды несущие в себя условия [22]. ACl листы работают с трафиков проходящим через заданные места и способны фильтровать не только целые пакеты но и смотреть их содержимое. Часто их устанавливают на пограничных объектах, стоящих на рубеже внутренней и внешней сети для контроля трафика. Для начала зайдем на компьютер находящейся в dmz и зададим ему адресс. Команда “ ip 192.168.333.33” задает адрес.

Рисунок 2.33 – Установка адреса на компьютер

Будем создавать ACl листы для прохождения трафика из сети от устройства находящегося в dmz зоне во внутреннюю сеть компании. Мы будем создавать объекты, они позволяют обращаться через его имя, а не адрес. Командой “object network we_server” создаем объект. Далее командой “jost 192.168.33.33” указываем адрес хоста. После командой “nat (DMZ, out) static 10.10.10.33” указываем адрес нашего устройства, по которому к нему буду обращаться вне локальной сети. Создаем acl лист командой “access-list outside_dmz extended permit tcp any host 192.168.33.33”, который говорит нам разрешать взаимодействие хоста со всеми используя tcp протокол. После командой “access-group outside_dmz in interface out” мы добавляем наш список в группу и привязываем к интерфейсу.

Рисунок 2.34 – Создание ACl листа

Разрешим проход icmp запросов через ASAvPrimary. Делается это для возможности осуществления связи ASAvPrimary через icmp запросы с другими устройствами. Делается это командой “access-list internet-icmp permit icmp any any echo-reply”.

Рисунок 2.35 – Создание ACl листов

Далее привязываем созданный выше acl к интерфейсу. Выполняется это командой “access-group internet-icmp in interface out”. Устройство коммуницируют через установленный и настроенный на нем интерфейс, поэтому access-group нужно привязывать к конкретно выбранному интерфейсу, чтоб он мог контролировать именно его.

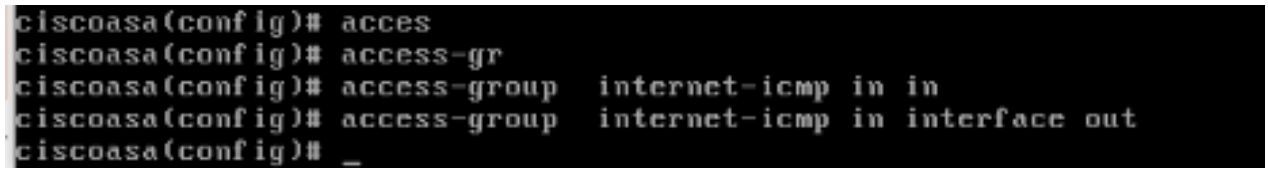

Рисунок 2.36 – Привязка к интерфейсу

Создаем Acl позволяющий отправлять http запросы используя tcp протокол. Разрешается только устройствам, имеющим порт больше 1024. Выполняется командой “access-list internet-http permit tcp any gt 1024 any eq www”.

Рисунок 2.37 – Создание Acl листа

Проверим существование наших acl листов на ASAvPrimary. Команда “sh access-list” выведет нам все acl листы (см. Приложение А).

Рисунок 2.38 – Информация о acl листах

2.6 Установка парольной защиты

Настроим парольную защиту роутеров. Создается она для уменьшения угрозы несанкционированного доступа. Парольная защита бывает разной и защищает разные точки. Сначала устанавливаем пароль на консоль. По умолчанию пароль на консоль отсутствует. Командой “conf t” заходим в режим глобальной конфигурации. Командой “line console 0 “ режим

консольной настройки. Значение 0 является порядковым номером консоли, по стандарту консольный порт один и имеет номер 0. Затем командой “login” разрешается вход с использованием заданного пароля.

Рисунок 2.39 – Установка консольного пароля на BranchRT

Заходим на BranchRT и проверяем наличие пароля.

```
% Password:  timeout expired!
Password:
**********************************************************************
* IOSv is strictly limited to use for evaluation, demonstration ar
* education. IOSv is provided as-is and is not supported by Cisco'
* Technical Advisory Center. Any use or disclosure, in whole or ir
* of the IOSv Software or Documentation to any third party for any
* purposes is expressly prohibited except as otherwise authorized
* Cisco in writing.
**********************************************************************
BranchRT>conf t
```

Рисунок 2.40 – Проверка пароля

Установим пароли для доступа по telnet и ssh. По стандарту эти пароли не установлены. Различие от других типов пароле, что пока пароля для этого соединения не будет установлен, по ssh и telnet не получится зайти на устройство. Будет сказано, что пока не установлен пароль, удаленный вход будет запрещен.

Командой “ line vty 0 4” заходим в режим настройки виртуальных терминалов, где 0 4 означает перейти в режим конфигурирования всех виртуальных терминалов с нулевого по четвертый.

```
BranchRT#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
BranchRT(config)#line vty 0 4
BranchRT(config-line)#password max
BranchRT(config-line)#login
BranchRT(config-line)#exit
BranchRT(config)#enable password max
BranchRT(config)#exit
BranchRT#
```

Рисунок 2.41 – Настройка паролей для telnet и ssh

Устанавливаем пароль на привилегированный режим. Подключаясь по консоли, мы изначально попадает в пользовательский режим, а командой “enable” мы переходим в привилегированный. Командой “ enable password max” мы устанавливаем пароль.

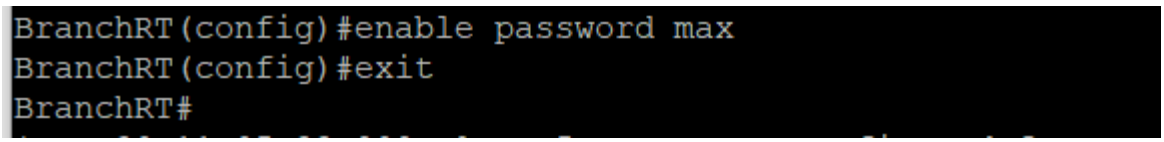

Рисунок 2.42 – Пароль на привилегированный режим

Зайдем в привилегированный режим. С нас сразу требует пароль.

Рисунок 2.43 – Проверка пароля

Все установленные пароли по стандарту хранятся в незашифрованном виде. Командой “service password-encryption” мы включаем сервис по шифрованию паролей.

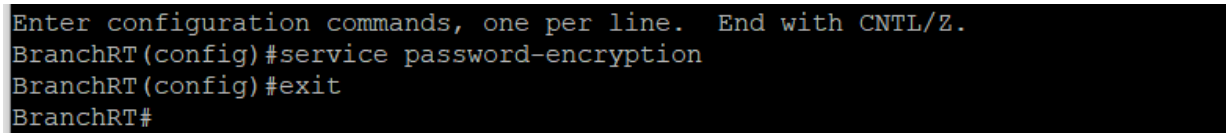

Рисунок 2.44 – Шифрование паролей

Зайдем в файл с конфигурациями и проверим установленные пароли и в каком виде они хранятся.

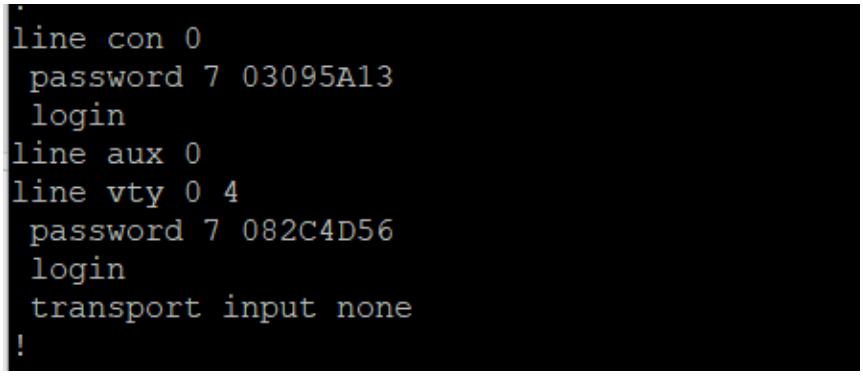

Рисунок 2.45 – Проверка паролей на BranchRT

Произведем аналогичные действия на роутере BorderRT (см. Приложение А).

Рисунок 2.46 – Установка паролей на BorderRT

Проверим наличие установленных пароле на BorderRT.

```
line con 0
 password 7 04560A1E
 login
line aux 0
line vty 0 4
 password 7 0009121E
 login
 transport input none
!
```

Рисунок 2.47 – Проверка паролей на BorderRT

2.7 Выход в сеть

Настроим выход в сеть на роутере. Во вкладке Network создадим объект Cloud и назначим ему параметр 5.

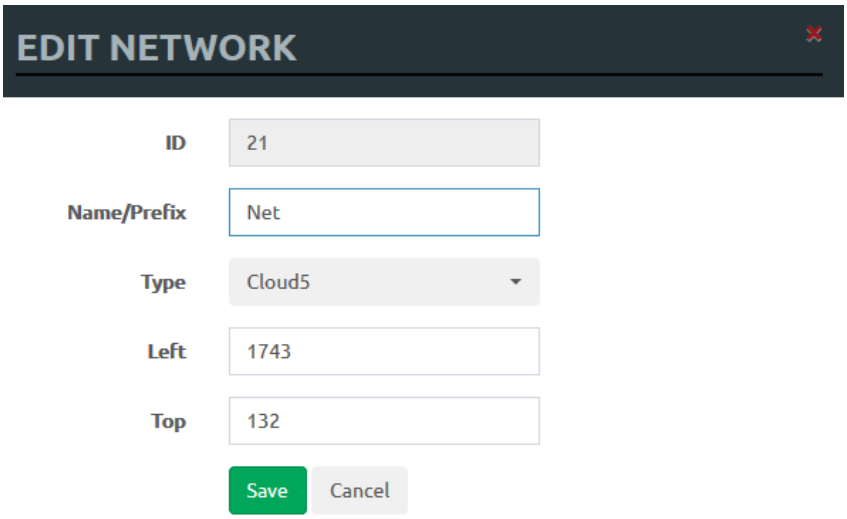

Рисунок 2.48 – Создание объекта Cloud

Создадим связь между Cloud5 и роутером. Пакеты будут поступать с роутера на Cloud5, который будет передавать их на сервер виртуальной машины eve-ng. Cloud5 будет привязан к pnet5 на сервер. Зайдем на сервер и командой “ip address add 172.16.0.10/24 dev pnet5” привяжем адрес к pnet5.

```
    link/ether ea:73:76:a9:40:c5 brd ff:ff:ff:ff:ff:ff
137: vunl0_16_5: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 9000 qdisc pfifo_fast state DOWN group def
ult qlen 1000
    link/ether 6e:51:7a:b4:bb:bd brd ff:ff:ff:ff:ff:ff
138: vunl0_16_6: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 9000 qdisc pfifo_fast state DOWN group def
ult qlen 1000
    link/ether f2:25:46:32:4a:df brd ff:ff:ff:ff:ff:ff
139: vunl0_16_7: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 9000 qdisc pfifo_fast state DOWN group def
ult qlen 1000
    link/ether e2:23:59:54:d4:66 brd ff:ff:ff:ff:ff:ff
141: vunl0_18_0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9000 qdisc pfifo_fast master vnet0_2 state U
 group default qlen 1000
    link/ether 7e:bb:5c:98:08:d0 brd ff:ff:ff:ff:ff:ff
root@eve-ng:~#
root@eve-ng:~#
root@eve-ng:~# ip address add 172.16.0.10/24
Not enough information: "dev" argument is required.
root@eve-ng:~# ip address add 172.16.0.10/24 dev pnet5
root@eve-ng:~# _
```

Рисунок 2.49 – Настройка адреса pnet5

Необходимо дать возможность проходить трафику через сервер eve-ng. По стандарту значения файла ip_forward 0, чтобы имелась возможность прохода трафика нам нужно изменить это значение на 1. Используя команду “nano” и путь к файлу изменим значение на 1.

Рисунок 2.50 – Настройка пропуска трафика

После предварительной настройки eve-ng, назначим адреса и маршрутизацию на роутере. Устанавливаем на выбранном интерфейсе адрес 172.16.0.100 с маской 255.255.255.0 и поднимаем его. Командой “do sh ip int br” выводим все установленные адреса и состояния интерфейсов. Пингуем адрес pnet5 172.16.0.10. Настроим маршрутизацию командой “ip route 0.0.0.0 0.0.0.0 172.16.0.10” что позволяет всем пакетам с роутера уходить на pnet5.

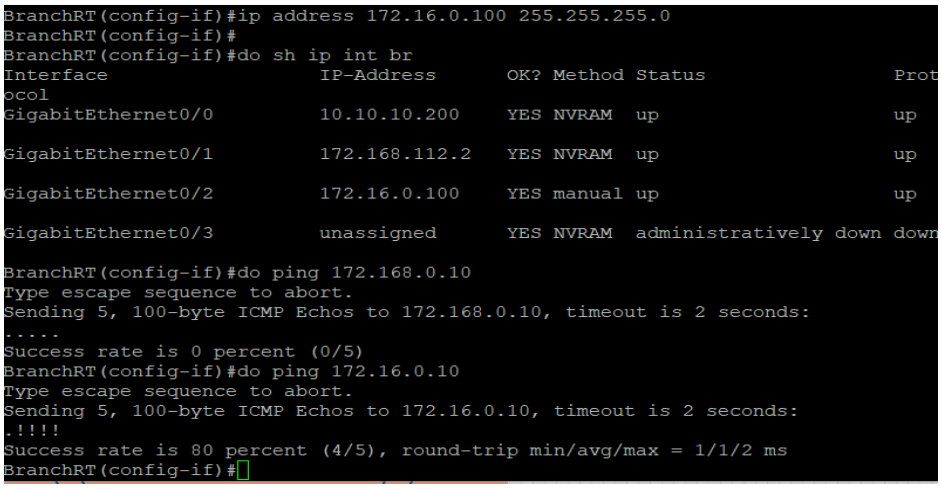

Рисунок 2.51 – Настройка роутера

Проделанные настройки не дают нам возможности выхода в интернет. У нас имеется лишь один адрес имеющий выход в сеть, и он привязан к pnet0. Заходим на сервер и вводим команду “iptables -t nat -A POSTROUTING -o pnet0 -s 172.16.0.0/24 -j MASQUERADE. Команда обращается к списку адресов и дает проход трафику из сети 172.16.0.0. через pnet0.

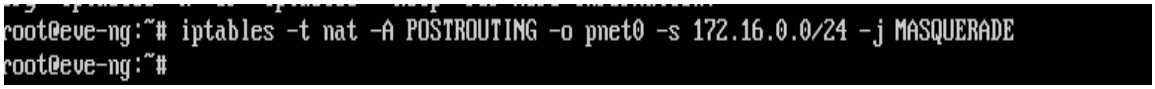

Рисунок 2.52 – Привязка адреса pnet5 к pnet0

Вернемся к роутеру и проверим выход в сеть командой “ping 8.8.8.8” обращение к серверам google.

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/3 ms
Router(config-if)#do ping 172.16.0.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.100, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 3/4/6 ms
Router(config-if)#exit
Router(config)#ip route 0.0.0.0 0.0.0.0 172.16.0.10
Router(config)#do ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 67/73/76 ms
Router(config)#
```

Рисунок 2.53 – Проверка выхода в сеть

Внесенные изменения должны остаться сохранёнными на сервере, для возможности работы с ними дальше. Если мы просто выйдем из сессии сервера eve-ng и перезагрузим его, то все слетит.

Перейдем в директорию /etc/network/if-pre-up.d/ и создадим там файл iptables-load. Откроем его и напишем небольшой скрипт. Второй строчкой мы создаем адрес с указанием маски и pnet к которому мы хотим его привязать. Третьей строчкой мы указываем откуда загружать настройки nat. Четвертой строчкой мы даем разрешение пропуска пакетов через виртуальную машину с указанием файла, значение которого надо изменить. Код пятой строчки будет давать возможность скрипту завершиться.

```
 GNU nano 2.5.3          File: /etc/network/if-pre-up.d/iptables-load

#!/bin/sh
ip address add 172.16.0.10/24 dev pnet5
iptables-restore < /etc/network/iptables.rules
echo "1" > /proc/sys/net/ipv4/ip_forward
exit 0

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos  ^Y Pr
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line ^V Ne
```

Рисунок 2.54 – Скрипт для сохранения настроек

После создания скрипта, проверим его наличие в директории. Нужно сделать этот файл исполняемым. Командой “chmod +x iptables-load” дадим права на исполнение файла. После этого можно спокойно перезагружать.

```
root@eve-ng:~# cd /etc/network/if.pre.up.d/
-bash: cd: /etc/network/if.pre.up.d/: No such file or directory
root@eve-ng:~# cd /etc/network/if-pre-up.d/
root@eve-ng:/etc/network/if-pre-up.d# ls -all
total 20
drwxr-xr-x 2 root root 4096 May  1 18:32 .
drwxr-xr-x 7 root root 4096 May  1 18:28 ..
lrwxrwxrwx 1 root root   29 Aug 20  2015 bridge -> /lib/bridge-utils/ifupdown.sh
-rwxr-xr-x 1 root root  344 Mar 14  2016 ethtool
-rw-r--r-- 1 root root  145 May  1 18:32 iptables-load
lrwxrwxrwx 1 root root   42 Oct  4  2018 openvswitch -> /usr/share/openvswitch/scripts/ifupdown.sh
-rwxr-xr-x 1 root root  241 Nov 17  2014 uml-utilities
root@eve-ng:/etc/network/if-pre-up.d# chmod +x iptables-load
root@eve-ng:/etc/network/if-pre-up.d# ls -all
total 20
drwxr-xr-x 2 root root 4096 May  1 18:32 .
drwxr-xr-x 7 root root 4096 May  1 18:28 ..
lrwxrwxrwx 1 root root   29 Aug 20  2015 bridge -> /lib/bridge-utils/ifupdown.sh
-rwxr-xr-x 1 root root  344 Mar 14  2016 ethtool
-rwxr-xr-x 1 root root  145 May  1 18:32 iptables-load
lrwxrwxrwx 1 root root   42 Oct  4  2018 openvswitch -> /usr/share/openvswitch/scripts/ifupdown.sh
-rwxr-xr-x 1 root root  241 Nov 17  2014 uml-utilities
root@eve-ng:/etc/network/if-pre-up.d# _
```

Рисунок 2.55 – Назначение прав файлу iptables-load

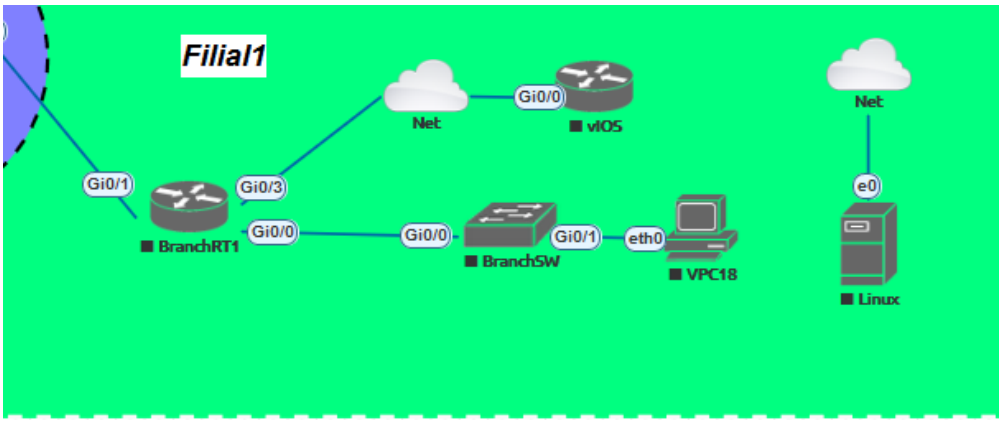

Рисунок 2.56 – Схема сети первого филиала

2.8 Настройка компонентов сети второго филиала

Перейдем к настройке сети второго филиала. Во втором филиале будет использоваться роутер BranchRT2, соединяющий филиал с основным офисом и со вторым филиалом. Будет использоваться CiscoASA, для безопасности и маршрутизации трафика. В филиале 2 настроим vlan 70 и 10 , для безопасной работы сотрудников. Зайдем на интерфейсы и зададим адреса 195.221.31.2/30 на выход в сеть и 31.0.1.1/24 на выход во внутреннюю сеть филиала.

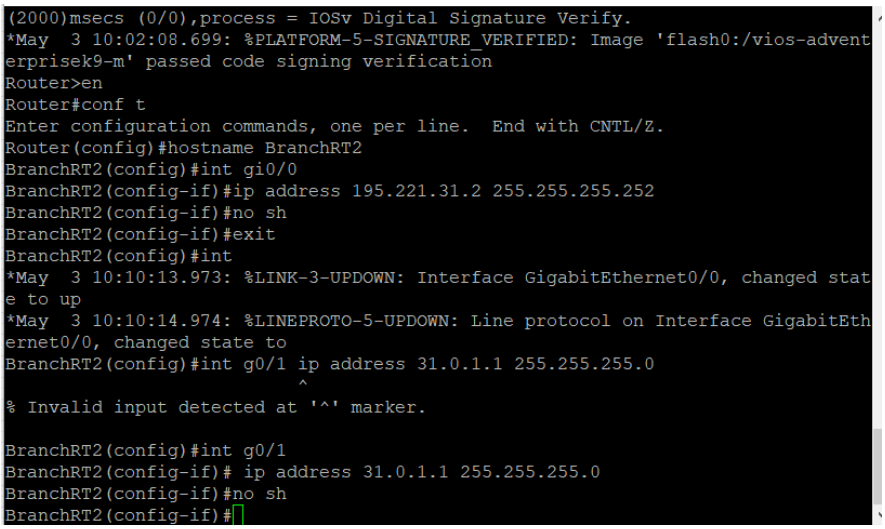

Рисунок 2.57 – Настройка роутера BranchRT2

Дале следует настройка CiscoASA. В CiscoASA создадим два vlan 72 и 10 для разграничения рабочего пространства сотрудников. Зайдем на интерфейс, смотрящий на BranchRT и зададим ему адрес.

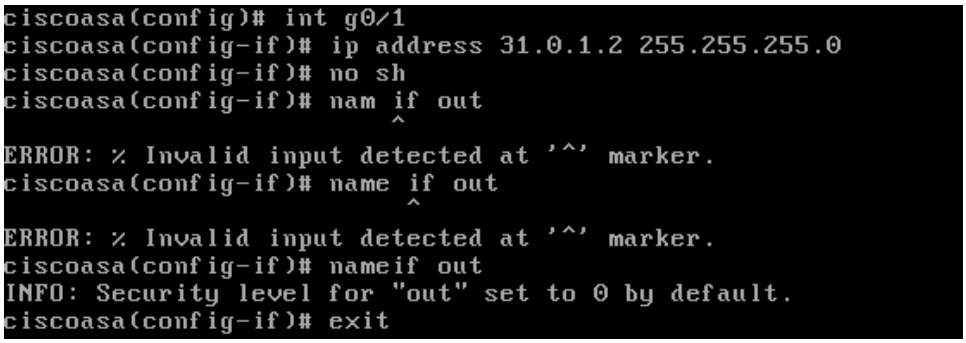

Рисунок 2.58 – Настройка CiscoASA

Создадим vlan, настроим их секьюрити лвл и назначим им адреса. На интерфейсе Gi0/0 смотрящего на внутреннюю сеть будут располагаться два vlan 72 и 10. Vlan 72 будет иметь название “ShareZone” и предназначен для устройств рядовых сотрудников. Vlan 10 будет иметь название “per” и предназначен для устройств доверенных сотрудников.

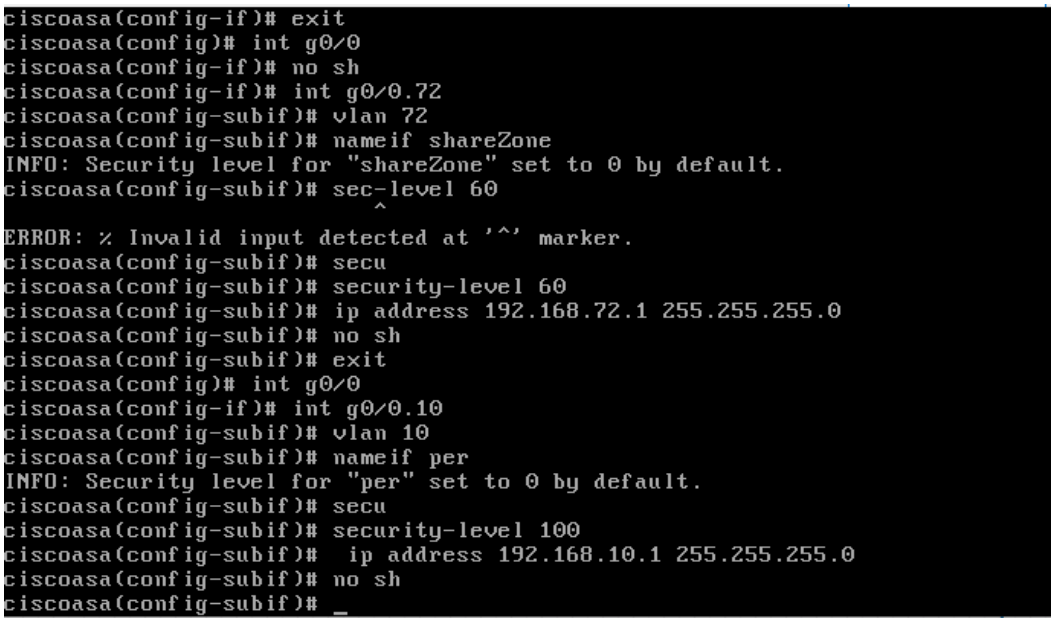

Рисунок 2.59 – Настройка vlan

После создания и настройки vlan, нам понадобиться настроить распределение vlan в switch на устройства сотрудников. Зайдем на интерфейс Gi0/0 смотрящий на CiscoASA. Командой “switchport trunk allowed vlan 72,10” разрешим прохождение трафика устройств входящих в эти vlan в CiscoASA.

Рисунок 2.60 – Настройка trunk

Теперь настроим на свитче распределение vlan. Через интерфейс g0/3 будет проходить трафик 72 vlan, а через g0/1 трафик 10 vlan.

Рисунок 2.61 – Распределение vlan

Зайдем в конфигурационный файл switch и проверим его содержимое. Из конфигурационного файл видно, что все vlan распределены и настроены верно, а значит сеть второго филиала стала более защищенной. Основной функцией vlan тут будет являться распределение областей сетей, в которых будут работать сотрудники.

Рисунок 2.62 – Конфигурационный файл switch

После всех проведенных настроек сеть второго филиала будет иметь среднюю степень защищенности.

Рисунок 2.63 – Схема сети второго филиала

2.9 Создание GRE туннеля

Generic Routing Encapsulation (GRE) – это один из возможных туннельных механизмов передачи пакетов. Созданный туннель позволят транспортировать в пакете одного протокола пакет другого протокола. Пакет, который транспортируется называется пакет “пассажир”. Пакет, который переносит “пассажира” называется транспортным протоколом. Туннель работает point to point, что значит пакет передается от отправителя точно к получателю. Настройка GRE требует создания логического интерфейса на конечных точках туннеля[22].

Будем создавать туннели между главным офисом и филиалами. Начнем настройки GRE туннеля между филиалами. Создаем логический интерфейс Tunnel1. Адрес 172.16.1.3 255.255.255.0 будет использоваться туннелем на стороне BranchRT2. GRE является инкапсулируемым протоколом(модульным), поэтому нам необходимо задать maximum transfer unit(mtu) и maximum segment size(mss). Командой “ip mtu 1400” утсановим mtu, а командой “ip tcp adjust-mss 1360” mss, заданных значений хватит, чтобы пакеты не фрагментировались. После нам нужно задать адрес хоста, используется адрес BranchRT2 и адрес получателя, которым является BranchRT. Далее используя команду “do s hip int br” выведем параметры всех интерфейсов устройства.

Рисунок 2.64 – Настройка GRE на BranchRT2

Перейдем на BranchRT1, являющийся роутером первого филиала и настроим GRE тут. Адрес туннеля на стороне BranchRT1 будет 172.16.1.4 с маской 255.255.255.0, адрес источник сам BranchRT1, а получатель роутер BranchRT2. После настройки произведем Icmp echos и убедимся в работе туннеля.

Рисунок 2.65– Настройка BranchRT1

Далее настроим GRE туннель между роутером главного офиса BorderRT и роутером первого филиала BranchRT1. Адрес туннеля на стороне BranchRT1 будет 40.16.1.1, адрес источника интерфейс BranchRT1 смотрящий на BorderRT, адрес получателя будет BorderRT.

Рисунок 2.66 – Настройка GRE на BranchRT

После настроим GRE на BorderRT. Адрес туннеля на стороне BorderRT будет 40.16.1.2. Источником будет адрес самого BorderRT, а получателем адрес BranchRT1.

Рисунок 2.67 – Настройка GRE на BorderRT

Проверим работоспособность GRE туннеля между BorderRT и BranchRT1, отправив Icmp echos на адреса входов в туннели.

Рисунок 2.68 – Проверка туннеля

Последним будем настраивать туннель между роутером главного офиса BorderRt и роутером второго офиса BranchRT2. Адрес туннеля на стороне BranchRT2 будет 172.50.1.9. Источником будет адрес самого BranchRT2, получателем будет BorderRT (см. Приложение А).

Рисунок 2.69 – Настройка GRE BranchRT2

Настроим GRE на стороне BorderRT. Адрес туннеля будет 172.50.1.10. Источником будет являться адрес самого роутера, получатель будет роутер BranchRT2. Значения mtu и mss останутся прежними.

Рисунок 2.70 – Настройка GRE на BranchRT2

Проверим работоспособность канала отправив Icmp echos на адрес туннеля.

Рисунок 2.71 – Проверка GRE туннеля

2.10 Настройка IPsec шифрования

Сам по себе GRE туннель не поддерживает шифрование и передает трафик в открытом виде от источника к получателю и без требования аутентификации. Можно установить поверх GRE туннеля Ipsec шифрование. Настройка Ipsec шифрования состоит из двух этапов. В первом определяем политику безопаности (ISAKAMP IKE) для создания туннеля. Во втором этапе настраиваем параметры туннеля (IPSec) для передачи данных [22].

Организуем IPSec шифрование между роутером главного офиса BorderRT и роутером второго филиала BranchRT2. Командой “crypto isakmp policy1” перейдем к настройке политик безопаности. Команда “encryption aes” определяет метод шифрования aes. Далее создаем метод аутентификации pre-share командой “authentication pre-share”. Group 2 является методом обмена секретными ключами, а именно методом Диффи-Хеллмана. Установим время жизни сессии 10000с. Определяем адрес конечной точки туннеля, а именно адрес BrnchRT2, а также их общий ключи pre-share для аутентификации. Командой “crypto ipsec transform-set GRE-IPSEC esp-3des esp-sha-hmac” настраиваем параметры туннеля IPSec.

Рисунок 2.72 - Настройка параметров туннеля IPSec

После установки всех параметров туннеля необходимо настроить профиль подключения. Командой “crypto ipsec GRE” устанавливаем название профиля GRE. Далее устанавливаем время жизни сессии. В конце нам необходимо привязать наш профиль к туннельному интерфейсу Tunnel3, для этого используем команду “tunne; protection ipsec profile GRE”.

Рисунок 2.73 – Настройка профиля IPSec

Произведем аналогичные настройки на роутере второго филиала BranchRT2. Разница будет адресе конечной точки туннеля, а именно адрес BorderRT (см. Приложение А).

Рисунок 2.74 – Настройка параметров туннеля IPSec на BranchRT2

Рисунок 2.75 – Настройка профиля безопасности IPSec на BranchRT

В итоге после настройки IPSec шифрования туннеля отобразим статус сесси шифрования туннеля. Используем команду “sh crypto session”. В отобразившимся конфиге мы видим, что отображены конечные и начальные точки входа трфика для шифрования, для поднятия сессии остается отправить Icmp echos.

Рисунок 2.76 - Конфигурационный файл шифрования

3 Безопасность жизнедеятельности

В дипломной работе производится разработка безопасной сети на основе eve-ng. Разработанный продукт будет внедрен в офисе компании “Marvel”. Безопасная сеть, разработанная в виртуальной лаборатории eve-ng основа на лучших практиках построения и ведения продуктов, предоставляющих безопасную инфраструктуру сети.

3.1 Анализ условий труда сотрудников офиса

Наш офис состоит находится на первом этаже состоит из 10 помещений в состав которых входит:

а) Серверная;
б) Уборная;
в) Отдел разработки;
г) Переговорная;
д) Отдел бухгалтерии
е) Кабинет начальника;
ж) Отдел тестирования;
и) Кабинет системного администратор;
к) Место хранения оборудования;
л) Отдел безопасности.

График работы будние дни с 9-00 до 18-00, без учетов праздников и вынужденного выхода на работу по разным обстоятельствам. В офисе одновременно может находится примерно 40 человек и для создания условий для безопасной, и продуктивной работы необходимо учитывать следующие факторы:

а) Микроклимат;
б) Шум;
в) Вибрации;
г) Электрические, магнитные, электромагнитные поля;
д) Качество используемого оборудования;
е) Освещение на рабочих местах;
ж) Вентиляция
и) Пожаробезопасность;
к) Эргономика.

На все эти факторы предусмотренные нормативы утвержденные СанПин 2.2.4.3359-16, СанПиН 2.2.4.548-12 и т.д. [24]

СанПин устанавливает оптимальные температурные значения на месте работы для создания благоприятного микроклимата. К показателям микроклимата относится (п. 2.2.1 СанПиН 2.2.4.3359-16):

а) Температура воздуха;
б) Температура поверхностей;

в) Относительная влажность воздуха;

г) Скорость движения воздуха;

д) Интенсивность теплового облучения.

Категории работ разграничиваются на основе интенсивности общих энергозатрат организма в ккал/ч(Вт). К категории Iа относятся работы с интенсивностью энергозатрат до 120 ккал/ч к коем можно отнести работу в офисе. [26]

Оптимальные значения параметров микроклимата на рабочих местах производственных и офисных помещений: [25]

Таблица 3.1 – Параметры микроклимата

Период года	Категория работ по уровню энергозатрат, Вт*	Температура воздуха, °С	Температура поверхностей, °С	Относительная влажность воздуха, %	Скорость движения воздуха, м/с
Холодный	Iа	22–24	21–25	60–40	0,1
	Iб	21–23	20–24	60–40	0,1
	IIа	19–21	18–22	60–40	0,2
	IIб	17–19	16–20	60–40	0,2
	III	16–18	15–19	60–40	0,3
Теплый	Iа	23–25	22–26	60–40	0,1
	Iб	22–24	21–25	60–40	0,1
	IIа	20–22	19–23	60–40	0,2
	IIб	19–21	18–22	60–40	0,2
	III	18–20	17–21	60–40	0,3

Для продуктивной работы сотрудников необходимо четко соблюдать значение норм микроклимата в компания офисного типа.

Важнейшей характеристикой воздушной среды является барометрическое давление, поскольку разница барометрического давления и давления воздуха в альвеолах легких определяет величину газообмена. Барометрическое давление считается и называется нормальным на уровне моря (одна атмосфера) и экспоненциально убывает с высотой.

Допустимые значения параметров микроклимата на рабочих местах производственных и офисных помещений [25]

Таблица 3.2 – Параметры микроклимата офисных помещений

Период года	Категория работ по уровню энергозатрат, Вт	Температура воздуха, °С		Температура поверхности, °С	Относительная влажность воздуха, %	Скорость движения воздуха, м/с	
		диапазон ниже оптимальных величин	диапазон выше оптимальных величин			для диапазона температуры воздуха ниже оптимальных величин, не более	для диапазона температуры воздуха выше оптимальных величин, не более
Холодный	Iа	20,0–21,9	24,1–25,0	19,0–26,0	15–75	0,1	0,1
	Iб	19,0–20,9	23,1–24,0	18,0–25,0	15–75	0,1	0,2
	IIа	17,0–18,9	21,1–23,0	16,0–24,0	15–75	0,1	0,4
	IIб	15,0–16,9	19,1–22,0	14,0–23,0	15–75	0,2	0,3
	III	13,0–15,9	18,1–21,0	12,0–22,0	15–75	0,2	0,4
Теплый	Iа	21,0–22,9	25,1–28,0	20,0–29,0	15–75	0,1	0,2
	Iб	20,0–21,9	24,1–28,0	19,0–28,0	15–75	0,1	0,3
	IIа	18,0–19,9	22,1–27,0	17,0–28,0	15–75	0,1	0,4
	IIб	16,0–17,9	21,1–27,0	15,0–28,0	15–75	0,2	0,5
	III	15,0–16,9	20,1–26,0	14,0–27,0	15–75	0,2	0,5

Для создания продуктивных условий работы также стоит обратить на уровень шума, создаваемый в офисе, уровень шума, не выходящий за нормы установленные в СН 2.2.4(2.1.8.562.96 Шум на рабочих местах в помещениях

жилых общественных зданий и на территории жилой застройки) создает благотворные условия для рабочей деятельности [26]

Постоянный шум, уровень звука которого за 8-часовой рабочий день или за время измерения в помещениях жилых и общественных зданий, на территории жилой застройки изменяется во времени не более чем на 5 дБА при измерениях на временной характеристике шумомера.

Непостоянный шум, уровень звука которого за 8-часовой рабочий день, за рабочую смену или во время измерения в помещениях жилых и общественных зданий, на территории жилой застройки изменяется во времени более чем на 5 дБА при измерениях на временной характеристике шумомера "медленно".

Таблица 3.3 – Шумовые показатели

N п / п	Вид трудовой деятельности, рабочее место	Уровни звукового давления, дБ, в октавных полосах со среднегеометрическими частотами, Гц									Уровни звука и эквивалентные уровни звука в (дБА
		31,5	63	125	250	500	1000	2000	4000	8000	
1	2	3	4	5	6	7	8	9	10	11	12

1	Рабочие места в помещениях, дирекции, проектно-конструкторских бюро, расчетчиков, программистов вычислительны машин, в лабораториях для теоретических работ и об-работки данных, приема больных в здравпунктах, творческая и руководящая деятельность, составление логистических запросов, ведения и разработка виртуальных продуктов.	86	71	61	54	49	45	42	40	38	50

3.2 Расчет эвакуации людей из офиса

В любом офисе может произойти ситуация, требующая экстренной эвакуации людей из зоны поражения, здоровье людей напрямую зависит от качественной и надежной работы по созданию плана эвакуации. Эвакуационные выходы были еще предусмотрены нормами безопасности при проектировании здания согласно СП 1.13130.2009 [24]

Выходные пути из офиса можно считать эвакуационными, если использование их обеспечивает безопасность людей от угрозы воздействия огня, газов, задымления, выброса и т.д.

Основными параметрами, обеспечивающими безопасную эвакуацию, являются:

а) Количество выходов, которые могут привести эвакуируемого в безопасную для жизни область;
б) Правильно выбранный маршрут эвакуации;
в) Соответствие путей эвакуации стандартам безопасности предусмотренными конструкторами здания;
г) Отсутствие вызываемых помех от предметов, окружающих путь эвакуации;
д) Отстраненность путей эвакуации от мест, потенциально имеющих высокий шанс возгорания;
е) Проведение периодических тренировок с персоналом предприятия;
ж) Высокая степень осведомленность персонала о серьезности и важности сохранения спокойствия в критических ситуациях;
и) Качественном построенный план эвакуации.

В каждом офисе помимо плана эвакуации должна иметься надежная система оповещения о возникновении угроз персоналу, также должна иметься система раннего реагирования и система контрмер по обеспечению безопасности персонала. В систему раннего реагирования входит:

а) Потолочные водяные разбрызгиватели, установленные в каждом помещении в соответствии с нормами безопасности;
б) Основная и экстренная система вентиляции офиса. Устанавливается на случай выхода из строя основной и снабжении необходимым кислородом персонал не имеющий возможности эвакуироваться согласно плану эвакуации;
в) Система очистки воздуха. Данная система полноценно устанавливается лишь в некоторых офисах. Данная система предназначена для очистки воздуха от элементов, затрудняющих дыхание без использования комплекса респираторных приспособлений;
г) Система изоляции. Данная система, как и система очистки воздуха в полной степени устанавливается лишь в некоторых офисах и необходима для предотвращения распространения элементов, угрожающих безопасности человека.

Число выходов с помещений и этажей не должно быть менее двух. У эвакуационного выхода есть свои четкие параметры высота не менее 1,9 м, а ширина при количестве людей более 60 человек – 1,2м. Двери использующиеся при эвакуации должны открываться наружу, а также не иметь запоров. Также стоит отдельно уделить внимание инвалидам, при их наличии необходимо предусмотреть пандусы для колясочников, если они работают на втором или выше этаже нужно предусмотреть лифт с размерами не менее: ширина-1,3 м, глубина - 2,2 м, ширина дверного проема – 0,95м. [25]

Произведем расчеты времени эвакуации офиса

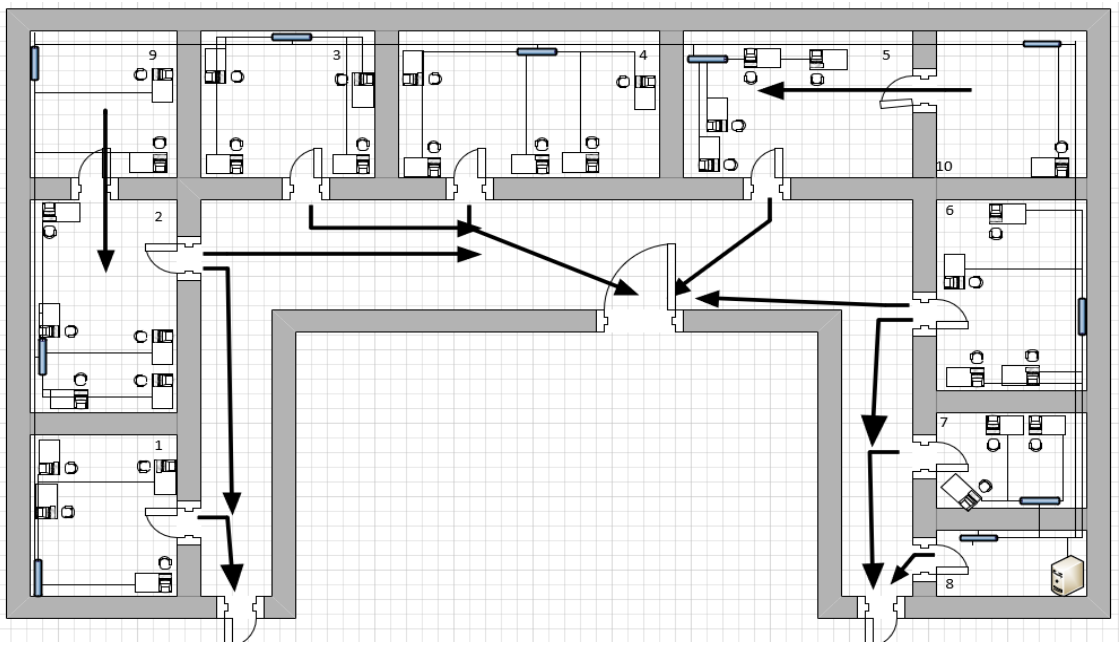

Рисунок 3.1 - План эвакуации

Время преодоления предельного расстояния до выхода из помещения по формуле [27]:

$$\tau_1 = L_1/V_0 \quad (3.1)$$

Где L_1 – расстояние от наиболее удаленного места; L_1= 12 м
V_0 – средняя скорость движения потока людей, м/мин; V_0 = 20 м/мин
τ_1 = 12/20=0,6 мин.

Производим расчет времени преодоления дверей для всех отделов. Расчет необходимо будет произвести десять раз. Также присутствуют помещения выход из которых требует преодоления двух дверей

Время преодоления дверей по формуле [27]:

$$\tau_2 = N/(f*n_0) \quad (3.2)$$

Где N – число работающих в отделе, чел; N=4 человек.
f – ширина двери, м; f= 0,8м.
n_0 – пропускная способность двери, чел/м; n_0=60 чел/м* мин.

τ_2 = 4/(0,8*60) = 0,08 мин.

Второе помещение:
Где N – число работающих в компании, чел; N=5 человек
f – ширина двери, м; f= 0,8м.
n_0 – пропускная способность двери, чел/м; n_0=60 чел/м* мин.
τ_3 = 5/(0,8*60) = 0,1 мин.

Третье помещение:
Где N – число работающих в компании, чел; N=4 человек
f – ширина двери, м; f= 0,8м.
n_0 – пропускная способность двери, чел/м; n_0=60 чел/м* мин.
τ_4 = 4/(0,8*60) = 0,08 мин.

Четвертое помещение:
Где N – число работающих в компании, чел; N=5 человек
f – ширина двери, м; f= 0,8м.
n_0 – пропускная способность двери, чел/м; n_0=60 чел/м* мин.
τ_5 = 5/(0,8*60) = 0,1 мин.

Пятое помещение:
Где N – число работающих в компании, чел; N=4 человек
f – ширина двери, м; f= 0,8м.
n_0 – пропускная способность двери, чел/м; n_0=60 чел/м* мин.
τ_6 = 4/(0,8*60) = 0,08 мин.

Шестое помещение:

Где N – число работающих в компании, чел; N=4 человек
f – ширина двери, м; f= 0,8м.
n_0 – пропускная способность двери, чел/м; n_0=60 чел/м* мин.

$\boldsymbol{\tau}_7 = 4/(0,8*60) = 0,08$ мин.

Седьмое помещение:
Где N – число работающих в компании, чел; N=3 человек
f – ширина двери, м; f= 0,8м.
n_0 – пропускная способность двери, чел/м; n_0=60 чел/м* мин.

$\boldsymbol{\tau}_8 = 3/ (0,8*60) = 0,06$ мин.

Восьмое помещение:
Где N – число работающих в компании, чел; N=1 человек
f – ширина двери, м; f= 0,8м.
n_0 – пропускная способность двери, чел/м; n_0=60 чел/м* мин.

$\boldsymbol{\tau}_9 = 1/(0,8*60) = 0,03$ мин.

Далее произведем расчет для помещений выход из которых требует преодоление двух дверей.

Девятое помещенье граничит со вторым помещением. Мы произведем расчет необходимого времени для выхода из девятого помещения. Далее необходимо будет рассчитать сколько людей к этому времени покинули второе помещение. После этого мы будет иметь время затраченное, чтобы покинуть девятое помещение и второе помещение, останется прибавить одно к другому с разницей времени, потраченному на ожидание.

Девятое помещение:
Где N – число работающих в компании, чел; N=2 человек.
f – ширина двери, м; f= 0,8м.
n_0 – пропускная способность двери, чел/м; n_0=60 чел/м* мин.

$\boldsymbol{\tau}_{10} = 2/(0,8*60) = 0,04$ мин.

Мы знаем, что время необходимое чтобы покинуть второе помещение τ_3=0,1.

Следовательно, персоналу, покинувшему девятое помещение, придется ждать примерно 0,06 минуты. В итоге персонал девятого помещения потратит $\tau_{10=}$ 0,1 мин, чтобы пройти все двери.

Далее по аналогии рассчитаем время прохождение дверей для персонала из 10 помещения, которое граничит с пятым.

Десятое помещение:
Где N – число работающих в компании, чел; N=1 человек
f – ширина двери, м; f= 0,8м.
n_0 – пропускная способность двери, чел/м; n_0=60 чел/м* мин.

$\boldsymbol{\tau}_{11}= 1/(0,8*60) = 0,03$ мин.

Персонал пятого помещения потратит τ_6= 0,8 мин, чтобы преодолеть двери. Следовательно, персоналу десятого помещения придется ждать 0,05

минуты. В итоге персоналу десятого помещения понадобится $\tau_{11=}$0,08 мин, чтобы пройти все двери.

В офисе имеется три аварийных выхода, люди покидающие свои кабинеты образуют потоки, которыми они следуют к местам эвакуации. В нашем случаи получается восемь потоков.

Время преодоления расстояния от двери до выхода

Первое помещение:

V_0 – средняя скорость движения потока людей, м/мин; V_0 = 20 м/мин.

L_2 – расстояние от дверей первого помещения до экстренного выхода, м; L_2=2м.

$\tau_{12=}2/20 = 0,1$ мин.

Второе помещение:

V_0 – средняя скорость движения потока людей, м/мин; V_0 = 20 м/мин.

L_2 – расстояние от дверей первого помещения до экстренного выхода, м; L_2=10м.

$\tau_{13=}10/20 = 0,5$ мин.

Третье помещение:

V_0 – средняя скорость движения потока людей, м/мин; V_0 = 20 м/мин.

L_2 – расстояние от дверей первого помещения до экстренного выхода, м; L_2=10м.

$\tau_{14=}10/20 = 0,5$ мин.

Четвертое помещение:

V_0 – средняя скорость движения потока людей, м/мин; V_0 = 20 м/мин.

L_2 – расстояние от дверей первого помещения до экстренного выхода, м; L_2=6м.

$\tau_{15=}6/20 = 0,3$ мин.

Пятое помещение:

V_0 – средняя скорость движения потока людей, м/мин; V_0 = 20 м/мин.

L_2 – расстояние от дверей первого помещения до экстренного выхода, м; L_2=4.

$\tau_{16=}10/20 = 0,2$ мин.

Шестое помещение:

V_0 – средняя скорость движения потока людей, м/мин; V_0 = 20 м/мин.

L_2 – расстояние от дверей первого помещения до экстренного выхода, м; L_2=8.

$\tau_{17=}8/20 = 0,4$ мин.

Седьмое помещение:

V_0 – средняя скорость движения потока людей, м/мин; V_0 = 20 м/мин.

L_2 – расстояние от дверей первого помещения до экстренного выхода, м; L_2=4.

$\tau_{18=}4/20 = 0,2$ мин.

Восьмое помещение:

V_0 – средняя скорость движения потока людей, м/мин; V_0 = 20 м/мин.

L_2 – расстояние от дверей первого помещения до экстренного выхода, м; L_2=1,5.

$\tau_{19=}$1,5/20 = 0,1 мин.

Далее нам необходимо рассчитать время, потраченное персоналом на выход из дверей, у нас имеется 3 экстренных выхода и на каждом разное количество нагрузки людей. Поэтому нам нужно будет произвести 3 расчета.

Время, потраченное на выход из дверей по формуле [27]:

$$\boldsymbol{\tau}_{20}= N_1/(\gamma*n) \quad (3.3)$$

Где N_1 – число сотрудников, проходящих через дверь, чел; N_1=N/2

N_1 = 14/2=7чел.

γ □□□Ширина входной двери, м; γ=1,6

$\boldsymbol{\tau}_{20}$= 7/(1,6*60)=0,07 мин.

Левый выход:

Где N_1 – число сотрудников, проходящих через дверь, чел; N_1=N/2

N_1 = 8/2=4чел.

γ □□□Ширина входной двери, м; γ=1,2

$\boldsymbol{\tau}_{21}$= 4/(1,2*60)=0,05 мин.

Правый выход:

Где N_1 – число сотрудников, проходящих через дверь, чел; N_1=N/2

N_1 = 8/2=4чел.

γ □□□Ширина входной двери, м; γ=1,2

$\boldsymbol{\tau}_{22}$= 4/(1,2*60)=0,05 мин.

В конечном расчете нам нужно рассчитать полное время эвакуации персонала по формуле [27]:

$$\tau_{пол}= \tau_1 + \tau_2 + \tau_3 + \tau_4 + \tau_5 + \tau_{6+} \tau_7 + \tau_8 + \tau_9 + \tau_{10} + \tau_{11} + \tau_{12+} \tau_{13} + \tau_{14} + \tau_{15} + \tau_{16} + \tau_{17} + \tau_{18+} \tau_{19} + \tau_{20} + \tau_{21+} \tau_{22} \quad (3.4)$$

$\tau_{пол}$=0,6+0,08+0,1+0,08+0,1+0,08+0,08+0,06+0,03+0,1+0,08+0,1+0,5+0,5+ 0,3+0,2+0,4+0,2+0,1+0,07+0,05+0,05=3,86 мин

$\tau_{пол} < \tau_{доп}$, где $\tau_{доп}$ допускаемо время при эвакуации, мин; $\tau_{пол}$ = 8 мин.

В итоге можно сделать вывод, что в случае возникновения ситуации угрожающей жизни персоналу, он сможет быстро эвакуироваться и минимизировать вред своему организму.

3.3 Расчет обеспечения безопасности от поражения электрическим током в офисе

Произведём расчеты на основе, что мы имеем офис, находящийся на первом этаже жилого комплекса. Офис используется it- компанией “Marvel”, которая активно использует техническое оборудование потребляющие много электроэнергии.

В офисе используется техника, подключенная в сеть электропитания. Следовательно, должны соблюдаться меры предосторожности по

использованию техники. Персонал должен быть хорошо осведомлен о технических характеристиках техники и правилах ее использования.

Защитное заземление должно обеспечить безопасность людей от поражения электрическим током при взаимодействии с проводниками электрического тока.

Защитное заземление или зануление электроустановок следует выполнять:

а) При номинальном напряжении 380 В и выше переменного тока 440 В, и выше постоянного тока - во всех случаях;
б) При номинальном напряжении от 42 В до 380 В переменного тока и от 110 В до 440 В постоянного тока ;
в) При работах в условиях с повышенной опасностью и особо опасных по ГОСТ 12.1.013-78.

Материал, конструкция заземляющих защитных проводников должны обеспечить устойчивость к механическим, химическим и термическим воздействиям

Для питания аппаратуры на предприятиях используется трехфазный ток напряжением 380-220В. В таком случае потенциал не должен превышать 125В. [27]

Сопротивление высчитывается по формуле [28]:

$$R_з = 125/I_з \quad (3.5)$$

Сопротивление не более 4 Ом.

Где $R_з$- сопротивление заземлителя

$I_з$ – ток замыкания на землю

По этой норме в эффективно заземленных сетях электробезопасность считается обеспеченной, если $\varphi \leq$ 10 кВ и напряжение прикосновения и шага в любое время года не превышает допустимых значений ГОСТ 12.1.019 – 2017.

Оборудование использует напряжение 380/220В, следовательно, $R_з \leq 4$Ом. ГОСТ 12.1.038 – 83. [28]

Значения сопротивления растекания заземлителя определяется путем инструментальных замеров примем $R_е$ = 19 Ом.

Значение растекания искусственного заземлителя высчитывается по формуле: [29]

$$R_и=(R_е*R_з)/(R_е-R) \quad (3.6)$$

$R_з$ = 4 Ом;

$R_е$ = 19 Ом;

$R_и=(19*4)/(19–4)=5,1$Ом

Далее определим удельное сопротивление почвы согласно ГОСТ 12.1.030-81 для вертикальных заземлителей по формуле [29]:

$$\rho_{расч} = \rho_{изм} * \psi \quad (3.7)$$

где ψ – коэффициент сезонности равный 1,3

ρизм – сопротивление грунта (смешанный грунт) равен 100 Ом*м, используя данные значения произведем расчет удельного сопротивления грунта:

$\rho_{расч}$ = 100 * 1,3= 130 Ом*м.

Произведя расчет для вертикальных заземлителей по аналогии рассчитаем сопротивление горизонтальных заземлителей, из таблицы берем ψ = 2,3:

$\rho_{расч}$ = 100 * 2,3= 230 Ом*м

Далее мы определяемся с типом заземлителя. В данном расчете будем использовать стержневой электрод длиной l=2,1 м, диаметром d=0,1 м и глубиной заложения t= 0,7 метра. Верхние концы соединены с помощью горизонтального электрода – стальной полосы сечением 4х65 мм.

Далее определяем сопротивление одиночного вертикального заземлителя. Произведем расчет растекания сопротивления электродов для стержневого заземлителя круглого сечения в земле по формуле [30]:

$$R_в = (p/2\pi l)(\ln 21/d+(\ln(4t+l)/(4t-l))/2 \quad (3.8)$$

ρ - удельное сопротивление грунта при вертикальном заземлителе ρ=130 Ом

$R_в$ = (130/2х3,14*2,1)(ln2*2,1/0,1+(ln(4*0,7+2,1)/(4*0,7-2,1))/2) ~81,7 Ом

Далее произведем расчеты сопротивления растеканию электродов для стержневого заземлителя в земле по формуле [30]:

$$R_г = (\rho/2\pi L)(\ln L2 /bt) \quad (3.9)$$

L – длина стальной ленты (которая укладывается на расстоянии 1,4м), L=45,5м

Rг = (230 / 2 * 3,14 * 45,5)(ln 45,5*2 / 0,1 * 0,7) = 88 Ом.

При размещении электродов по периметру на расстоянии 1,4 м от каркаса здания, количество вертикальных электродов составляет n = 32 шт. на расстоянии 3 м друг от друга. Коэффициенты использования электродов составляют – для вертикального ηв = 0,73 для горизонтального - $\eta_г$ = 0,62.

Сопротивление растекания группового заземлителя по формуле [30]:

$$R = R_в R_г/(R_в\eta_г+R_г\eta_в n) \quad (3.10)$$

R = 81,7 * 88/ (81,7 * 0,62+88 * 0,73 * 32) = 3,4 Ом.

В конце проверяем соблюдение необходимого условия $R_з \geq R$, следовательно, 4≥3,4, что дает нам возможность утверждать, что необходимое условие электробезопасности выполняется.

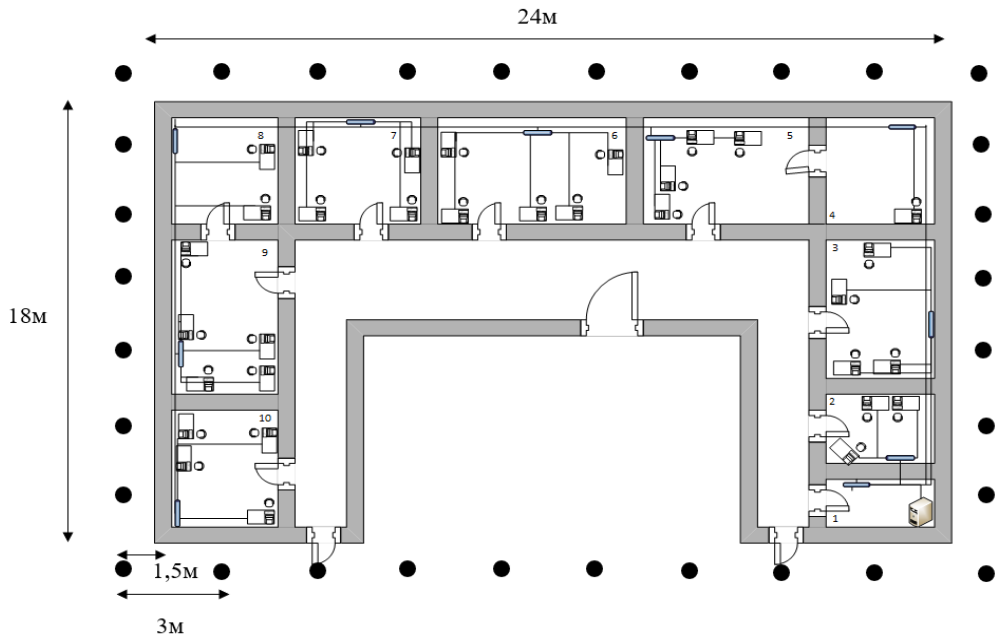

Рисунок 3.2 - Схема заземления офиса

3.4 Вывод по разделу БЖД

В первом случаи мы произвели расчеты времени эвакуации людей из офиса. Согласно произведенным расчетам мы удовлетворили требования, получив время эвакуации 3.86 минуты, когда допустимое время 8 минут. Стоит заметить, что важную роль играет не только время эвакуации, но и способы оповещения и реагирования. Качественные способы оповещения позволяют быстро оповестить людей о угрозе из жизни. Средства быстрого реагирования позволяют минимизировать области воздействия опасных для жизни факторов.

Во втором случаи мы произвели расчет безопасности от поражения электрическим током в офисе. В выполненных расчетах удовлетворяется условие, сопротивление растекания группового заземлителя R=3,4Ом не превышает сопротивление заземлителя $R_з$= 4 Ом. Важно определиться с типом используемого заземлителя и его размерами. Также стоит учесть количество используемых заземлителей по периметру здания. В итоге нужно отметить важность и точность произведения расчетов, так как от них напрямую зависит жизнь человека.

4 Анализ и оценка рисков

Целью любой организации является достижение определенных показателей, характеризующих результаты ее деятельности. Например, для коммерческих компаний это извлечение прибыли, рост капитализации, доли рынка или оборота, а для правительственных организаций – предоставление государственных услуг населению и решение задач управления. В любом случае, независимо от цели деятельности организации, достижению этой цели может помешать реализация рисков информационной безопасности. При этом каждая организация по-своему оценивает риски и возможность инвестирования в их снижение. Таким образом, целью управления рисками информационной безопасности является поддерживание их на приемлемом для организации уровне. Для решения данной задачи организации создают комплексные системы информационной безопасности (СИБ).

Все риски, в том числе риски информационной безопасности, характеризуется двумя параметрами: потенциальным ущербом для организации и вероятностью реализации. Использование для анализа рисков совокупности этих двух характеристик позволяет сравнивать риски с различными уровнями ущерба и вероятности, приводя их к общему выражению, понятному для лиц, принимающих решение относительно минимизации рисков в организации

При оценке рисков необходимо понимание оценки информационных структур. Необходимо понимать, что ущерб нанесенных информационным структурам повлияет на целостность, конфиденциальность и доступность.

Принятое по каждому риску решение должно быть зафиксировано в плане реагирования на риски. Принятие решения по рискам и разработка плана реагирования на риски. Для определения совокупности мер реагирования на риски необходимо провести анализ идентифицированных и оцененных рисков. Идентификация, анализ и оценка рисков. Для принятия решения относительно рисков они должны быть однозначно идентифицированы и оценены с точки зрения ущерба от реализации риска и вероятности его реализации. При оценке ущерба определяется степень влияния риска на ИТ-активы организации и поддерживаемые ими бизнес-процессы. При оценке вероятности производится анализ вероятности реализации риска. Оценка данных параметров может базироваться на выявлении и анализе уязвимостей, присущим ИТ-активам, на которые может влиять риск, и угрозам, реализация которых возможная посредством эксплуатации данных уязвимостей. Также в зависимости от используемой методики оценки рисков, в качестве исходных данных для их оценки может быть использована модель злоумышленника, информация о бизнес-процессах организации и других сопутствующих реализации риска факторах, таких как политическая, экономическая, рыночная или социальная ситуация в среде деятельности организации

4.1 Идентификация активов и мер защиты

Один из этапов анализа рисков состоит в идентификации всех объектов, нуждающихся в защите. Некоторые активы (например аппаратура) идентифицируются очевидным образом. Про другие (например, про людей, использующих информационные системы) нередко забывают. Необходимо принять во внимание все, что может пострадать от нарушений режима безопасности.

Может быть использована следующая классификация активов:

а) Аппаратура: процессоры, модули, клавиатуры, терминалы, рабочие станции, персональные компьютеры, принтеры, дисководы, коммуникационные линии, терминальные серверы, мосты, маршрутизаторы;
б) Программное обеспечение: исходные тексты, объектные модули, утилиты, диагностические программы, операционные системы, коммуникационные программы;
в) Данные: обрабатываемые,непосредственнодоступные, архивированные, сохраненные в видерезервной копии, регистрационные журналы, базы данных, данные, передаваемые по коммуникационным линиям;
г) Люди: пользователи, обслуживающий персонал;
д) Документация: по программам, по аппаратуре, системная, по административным процедурам, по безопасности;
е) Расходные материалы: бумага, формы, бланки, красящая лента, магнитные носители.

После того как выявлены активы, нуждающиеся в защите, необходимо идентифицировать угрозы этим активам и размеры возможного ущерба. Эта работа должна быть направлена на то, чтобы понять, каких угроз следует опасаться больше всего.

Несанкционированный доступ к компьютерным ресурсам - угроза, типичная для большинства организаций. Несанкционированный доступ может принимать различные формы. Иногда это нелегальное использование счета другого пользователя для получения доступа к системе. В других случаях ресурсами пользуются без предварительно полученного разрешения.

Степень важности проблемы несанкционированного доступа для разных организаций разная. Порой передача прав доступа неавторизованному пользователю может привести к разрушению магнитных носителей. Чаще несанкционированный доступ облегчает исполнение других угроз. Разнится и реальность нападения: некоторые организации (известные университеты, правительственные и военные учреждения) как бы притягивают к себе злоумышленников. Следовательно, риск несанкционированного доступа меняется от предприятия к предприятию.

Нелегальное ознакомление с информацией - другая распространенная угроза. Определите степень конфиденциальности информации, хранящейся в ваших компьютерах.

Компьютеры и сети предоставляют своим пользователям множество ценных услуг, от которых зависит эффективная работа многих людей. Когда услуги вдруг становятся недоступными, возникают потери -прямые и косвенные.

Отказ в обслуживании возникает по разным причинам и проявляется по-разному. Сеть может прийти в неработоспособное состояние от поддельного пакета, перегрузки или по причине отказа компонента. Вирус способен замедлить или парализовать работу компьютерной системы. Каждая организация должна определить для себя набор необходимых сервисов и для каждого из них проанализировать последствия его недоступности.

Активы, рассмотренные в данной работе:

а) Dmz (почтовый, веб-сервер);
б) Сервер(dhcp,dns,ad,мэ);
в) Маршрутизатор;
г) Коммутатор;
д) CiscoASA;
е) PC.

Таблица 4.1 – Активы

№	Код актива	Наименование	Кол-во	Ответственный	Ценность	Приоритет	Стоимость
1	DM	Dmz(почтовый,веб-сервер)	1	Сетевой администратор	6	3	1500000 тг.
2	SR	Сервер(dhcp,dns,мэ,ad)	1	Инженер ИБ	5	4	2000000 тг.
3	RO	Маршрутизатор	4	Сетевой администратор	3	4	170000 тг.
4	SW	Коммутатор	5	Сетевой администратор	3	5	250000 тг.
5	AS	CiscoASA	2	Инженер ИБ	5	2	3900000 тг.
6	PC	PC(персональный компьютер)	20	Сетевой адинистартор	3	2	4000000 тг.

Рассмотрим меры защиты, используемые для создания безопасной сети:

а) Межсетевые экраны нового поколения Cisco ASA серии 5500-X помогают заказчикам найти баланс между эффективностью обеспечения безопасности и производительностью. Это решение, представляющее собой сочетание самого популярного в отрасли межсетевого экрана с контролем состояния соединений и полного ассортимента сервисов сетевой безопасности нового поколения;

б) ACL (access control list) — это строго говоря, механизм для выбора из всего потока трафика какой-то части, по заданным критериям. ACL-и бывают двух видов: стандартные и расширенные. Стандартные позволяют отфильтровывать трафик только по одному критерию: адрес отправителя, в CCNA рассматривается конкретно только ip адрес отправителя. Расширенный ACL позволяет фильтровать трафик по большому количеству параметров: адрес отправителя, адрес получателя, TCP/UDP порт отправителя, TCP/UDP порт получателя, протоколу, завёрнутому в ip (отфильтровать только tcp, только udp, только icmp, только gre и т.п.),типу трафика для данного протокола (например, для icmp отфильтровать только icmp-reply);

в) VLAN (Virtual Local Area Network, виртуальная локальная сеть) — это функция в роутерах и коммутаторах, позволяющая на одном физическом сетевом интерфейсе (Ethernet, Wi-Fi интерфейсе) создать несколько виртуальных локальных сетей. VLAN используют для создания логической топологии сети, которая никак не зависит от физической топологии;

г) Туннелирование предоставляет механизм транспортировки пакета одного протокола внутри другого. Протокол, который транспортируется называется протоколом пассажиром. Протокол, который "несет" протокол пассажир называется транспортным протоколом. Generic Routing Encapsulation (GRE) — это один из возможных туннельних механизмов, который использует IP как транспортный протокол и может быть использован для переноса многих других протоколов пассажиров. Туннели являются point-to-point соединениями, определяющимися tunnel source и tunnel destination адресами на обоих концах;

д) IPsec (сокращение от IP Security) — набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP. Позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и/или шифрование IP-пакетов. IPsec также включает в себя протоколы для защищённого обмена ключами в сети Интернет. В основном, применяется для организации VPN-соединений;

е) Для защиты устройств cisco от несанкционированного доступа используется несколько видов паролей. В курсе CCNA рассматривается настройка паролей на консоль, паролей на подключение по telnet и ssh, а

также пароль для доступа в привилегированный режим работы устройства. Пароли настраиваются одинаковым образом для маршрутизаторов и коммутаторов.

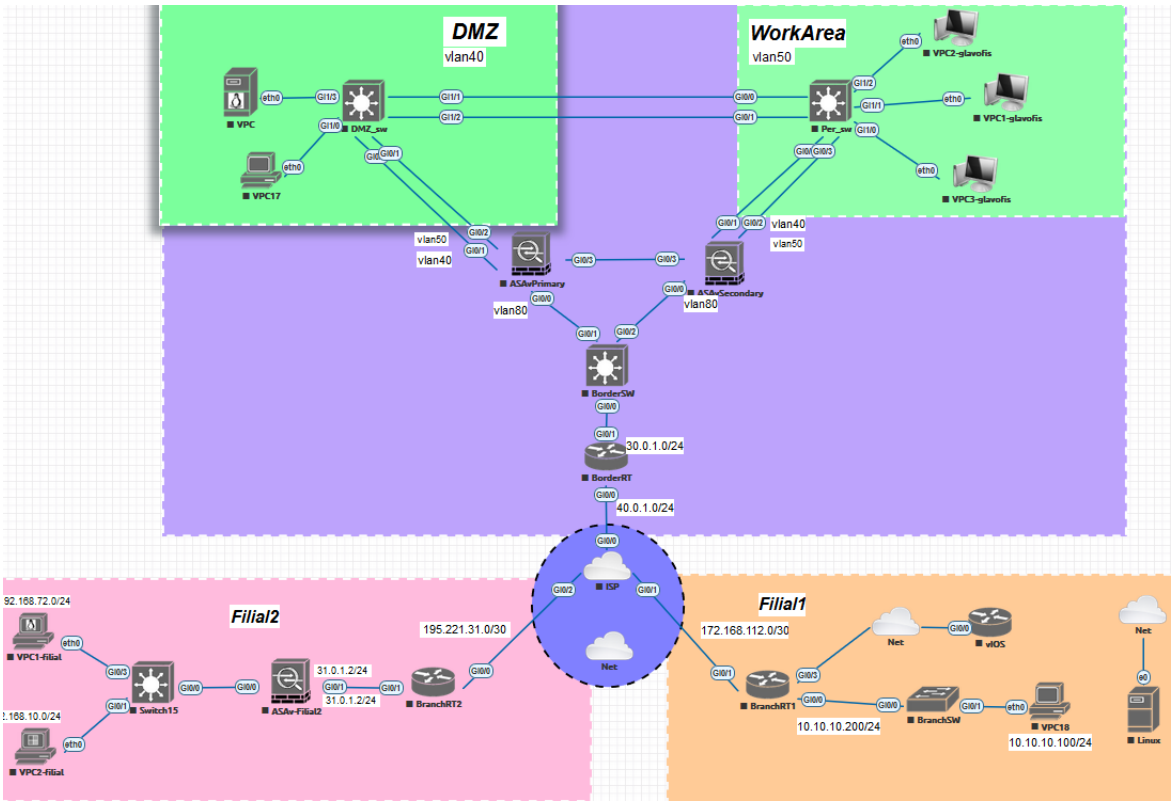

Рисунок 4.1 – Схема безопасной сети

4.2 Расчетная часть

При расчете рисков по двум параметрам таблица использована, чтобы связать факторы последствий (ценность активов) с вероятностью возникновения угрозы. Первый шаг состоит в оценивании последствий по заранее определенной шкале, от 1 до 5, для каждого находящегося под угрозой актива. Второй шаг состоит в оценивании вероятности возникновения угрозы по заранее определенной школе (от 1 до 4). Третий шаг состоит в вычислении меры риска путем умножения ценности актива на вероятности возникновения угроз

Таблица 4.2- Шкала вероятности возникновения риска

Шкала вероятности возникновения риска	
Значение	Описание
0 - очень низкий	раз в несколько лет
1 - низкий	один раз в 3 года
2 - средний	несколько раз в год
3 - высокий	один раз в месяц
4 - очень высокий	несколько раз в месяц

Таблица 4.3 - Оценка рисков по двум параметрам

№	Угроза	Уязвимость	Максимальный уровень риска	Меры по снижению риска	Остаточный уровень риска	Дата	Комментарий
1	Актив: DMZ						
DM.1	НСД	Доступ к серверу лиц, не имеющих на это прав	12	Двухфакторная аутентификация. Уникальная система аутентификации.	6	13.03.2020	Сетевой Администратор
DM.2	Сетевые атаки	Внедрение SQl инъекций. Переполнение буфера.	18	Фильтрация трафика. Межсетевые	12	13.03.2020	Сетевой Администратор

Продолжение таблицы 4.3

		Внедрение вредоносного кода. Модификация управляющих инструкций. Модификация алгоритмов передачи трафика с использование уязвимостей сетевых пакетов		экраны. Вспомогательное ПО для защиты периметра сети.			
DM.3	Сбои и отказ	Получение физического доступа. Воздействие вредоносного ПО из внешней сети. Ddos-атаки на веб-сервера.	12	Создание политики безопасности, с учетом всех особенностей компании. Системы физической защиты. Межсетевые экраны нового поколения. Настройка аварийного режима работы. Настройка отказоустойчивости и живучести	6	13.03.2020	Сетевой Администратор

2	Актив: Маршрутизатор						
RO.1	Перехват трафика	Прослушивание канала передачи данных. Внедрение в канал передачи и модификация точек обращения.	9	Использование IPsec шифрования. Установка поверх GRE туннеля шифрование трафика	6	13.03.2020	Сетевой Администратор

Продолжение таблицы 4.3

RO.2	Перехват управления	Внедрение исполняемых команд в сетевые протоколы. Уязвимость алгоритмов анализа сетевых протоколов.	9	Создание GRE туннеля между роутерами филиалов, что позволит создать устойчивый канал. Установка точек приема трафика	6	13.03.2020	Сетевой Администратор

RO.3	Заражение устройства	Внедрение вредоносного кода в устройство. Использование гибридного вируса, распространяющегося на все устройства за роутером.	12	Фильтрация поступающего трафика. Создание правил прохождения трафика. Система анализа и применения контрмер по борьбе с вредоносным ПО.	9	13.03.2020	Сетевой Администратор
3	Актив: Сервер						
SR.1	Изменение данных, порча	Внедрение вредоносного кода, модификация передаваемого трафика.	10	Резервное восстановление БД. Алгоритмы копирования данных	5	13.03.2020	Инженер ИБ

Продолжение таблицы 4.3

SR.2	Физический доступ	Доступ к серверу лиц, не имеющих на это право. Изменение фундаментальных основ работы сервера. Кража конфиденциальных данных.	10	Охранная система. Контрольно-пропускные меры.	5	13.03.2020	Инженер ИБ
SR.3	DDOS атака	Вывод из строя сервера. Нарушение доступности к данным.	15	Установка и настройка межсетевого экрана, с строго настроенными правилами. Система мониторинга сетевой активности.	10	13.03.2020	Инженер ИБ
4	Актив: Коммутатор						
SW.1	Вторжение в канал передачи	Доступ со стороны одного скомпрометированного устройства на другое более важное.	6	Получение настроек vlan от ciscoasa, правильность сконфигурированных trunk port и access port.	3	13.03.2020	Сетевой Администратор

SW.2	Перехват управления	Получение трафика и его модификация, что приводит к получению доступа к терминалу управления устройством.	12	Создание и настройка acl- листов для контроля точек соединения и прохождения трафика.	9	13.03.2020	Сетевой Администратор

Продолжение таблицы 4.3

SW.3	Переполнение буфера	Нарушаются границы выделенной оперативной памяти, что приводит к аварийному завершению работы устройства и выполнению двоичных команд.	12	Настройка неисполнимости буфера. Установка ограничения выполняемых инструкций.	8	13.03.2020	Сетевой Администратор
5	Актив: CiscoASA						
AS.1	Вывод из строя	Изменение процессов и режимов работы. Внедрение исполняемого кода. Доступ к управляющей консоли.	10	Наличие запасной CiscoAsa. Настройка failover между ними, что позволит передать все данные на резервеную	5	13.03.2020	Инженер ИБ

				CiscoAsa			
AS.2	Модификация трафика	Внедрение вредоносного кода	15	Система мониторинга прохождения трафика. Настроенные vlan и acl	10	13.03.2020	Инженер ИБ

Продолжение таблицы 4.3

AS.3	НСД	Доступ к компьютеру лиц, не имеющих на это право	15	Двухфакторная аутентификация, доступ к серверу через систему мониторинга Pors. Отключение портов доступа.	10	13.03.2020	Инженер ИБ

6	Актив: Персональный компьютер						
РС.1	Физический доступ	Доступ к персональному компьютеру людей, не имеющих на это право.	9	Система аутентификации. Охранная система компании.	6	13.03.2020	Сетевой инженер
РС.2	Понижение СЗИ на рабочей станции	Вывод из строя компонентов защиты пк. Отсутствие системы мониторинга внесения изменений в функционирования пк.	12	Использование программно-аппаратного комплекса мониторинга изменений в устройстве.	8	13.03.2020	Сетевой инженер
РС.3	Изменение процессов защиты и режимов работы ПО	Доступ к реестру пк. Возможность внесения изменений от администратора. Внедрения вредоносного кода	6	Изоляция доступа к возможностям администратора. Установка защитного ПО.	3	13.03.2020	Сетевой инженер

4.3 Анализ рисков с использованием CORAS

Для построения схем и диаграмм будет использована среда CORAS. Произведем построение схемы активов находящихся в зоне рисков. В разрабатываемой в дипломной работе сетевой схеме основными активами будут являться: коммутатор, маршрутизатор, dmz(сервер), сервер(web,dhcp,dns), CiscoASA, pc(персональный компьютер).

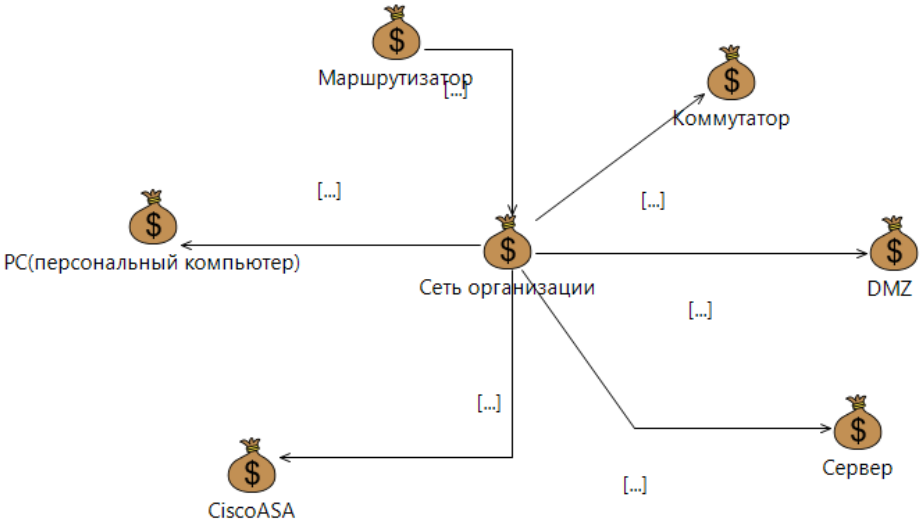

Рисунок 4.4- Активы

Источниками рисковых ситуаций будут являться: нарушитель, администратор сети, система (представляет цельный программно-аппаратный комплекс ведения, обслуживания, развертывания нашей структуры), пользователь (сотрудник компании, клиент). Каждый из источников угроз имеет возможность эксплуатировать уязвимость системы. Эксплуатация этих уязвимостей может привести к возникновению рисковых ситуаций, за этим последует нанесения

ущерба компании. Создадим схему пары угроз и уязвимость, чтобы наглядно увидеть потенциальные места возникновения рисковых ситуаций.

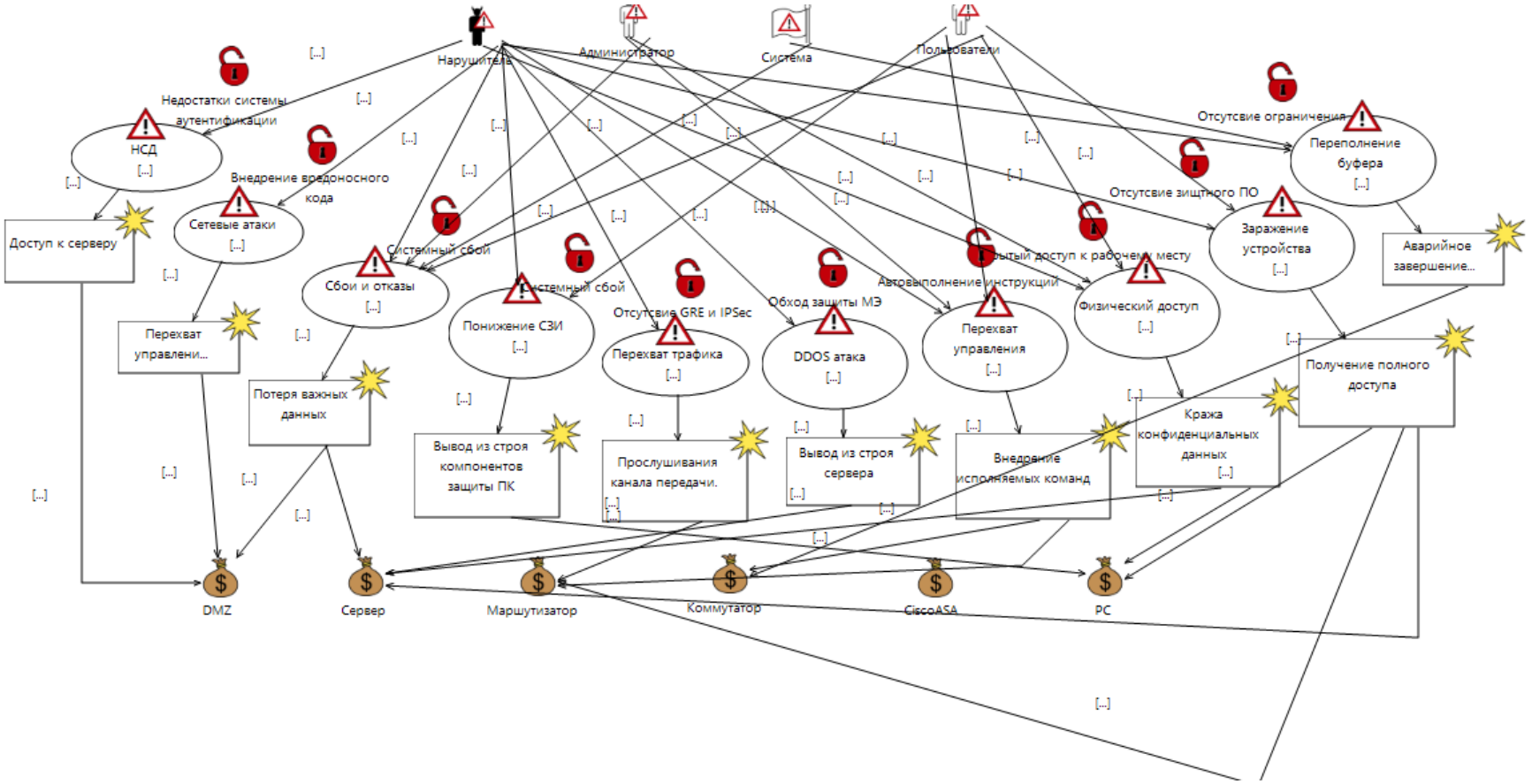

Рисунок 4.5 – Описание пары угроза+узвимость

Далее создадим диаграмму рисков. Она покажет, что является источником возниконовения рисков и на какие активы это повлияет.

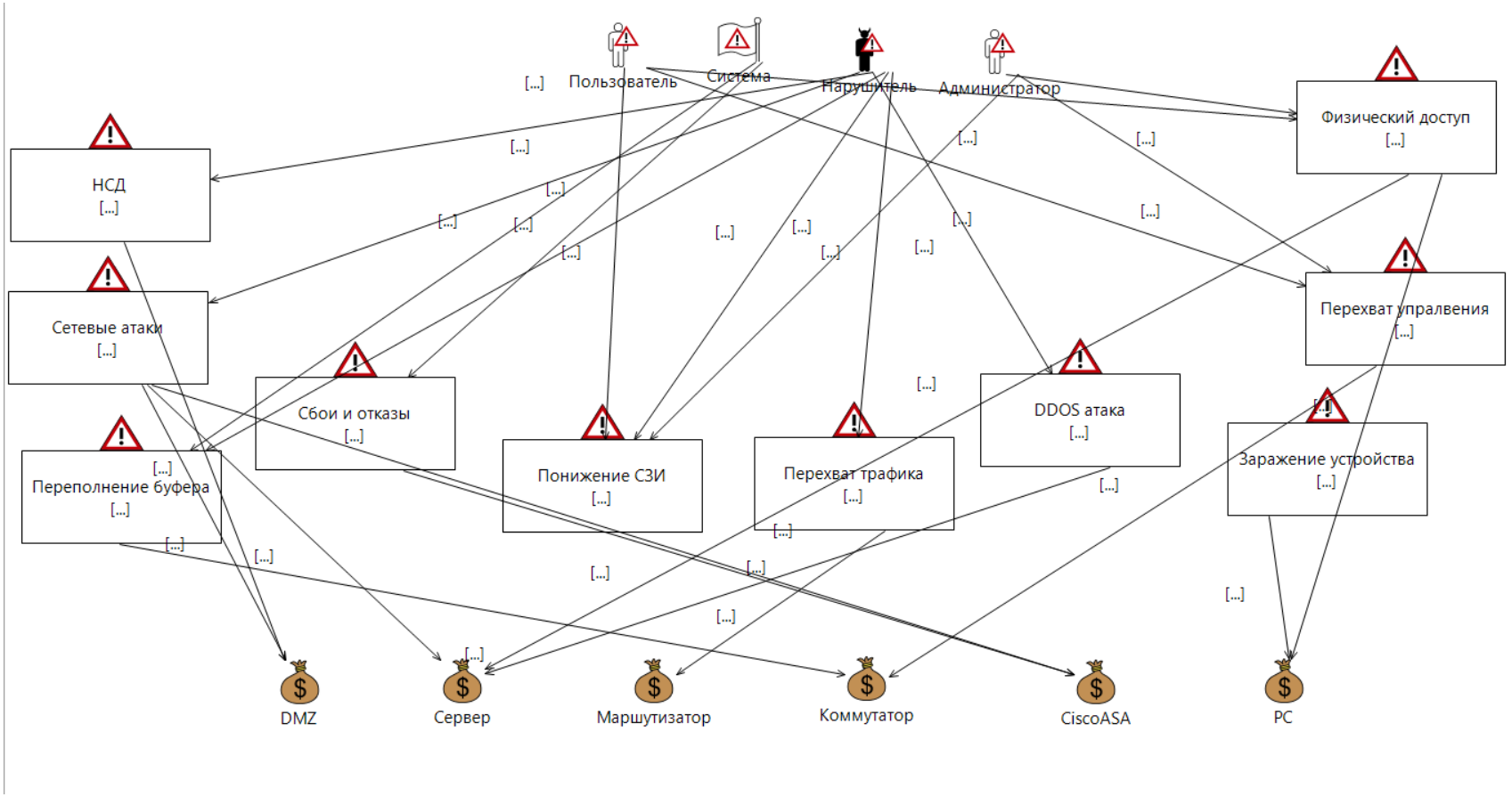

Рисунок 4.6 – Диаграмма рисков

Определим является ли создаваемая угрозой рисковая ситуация приемлемой или нет. В случае если риск приемлемый, то меры по защите актива не требуются, если же риск не приемлемый, то актив подлежит защите.

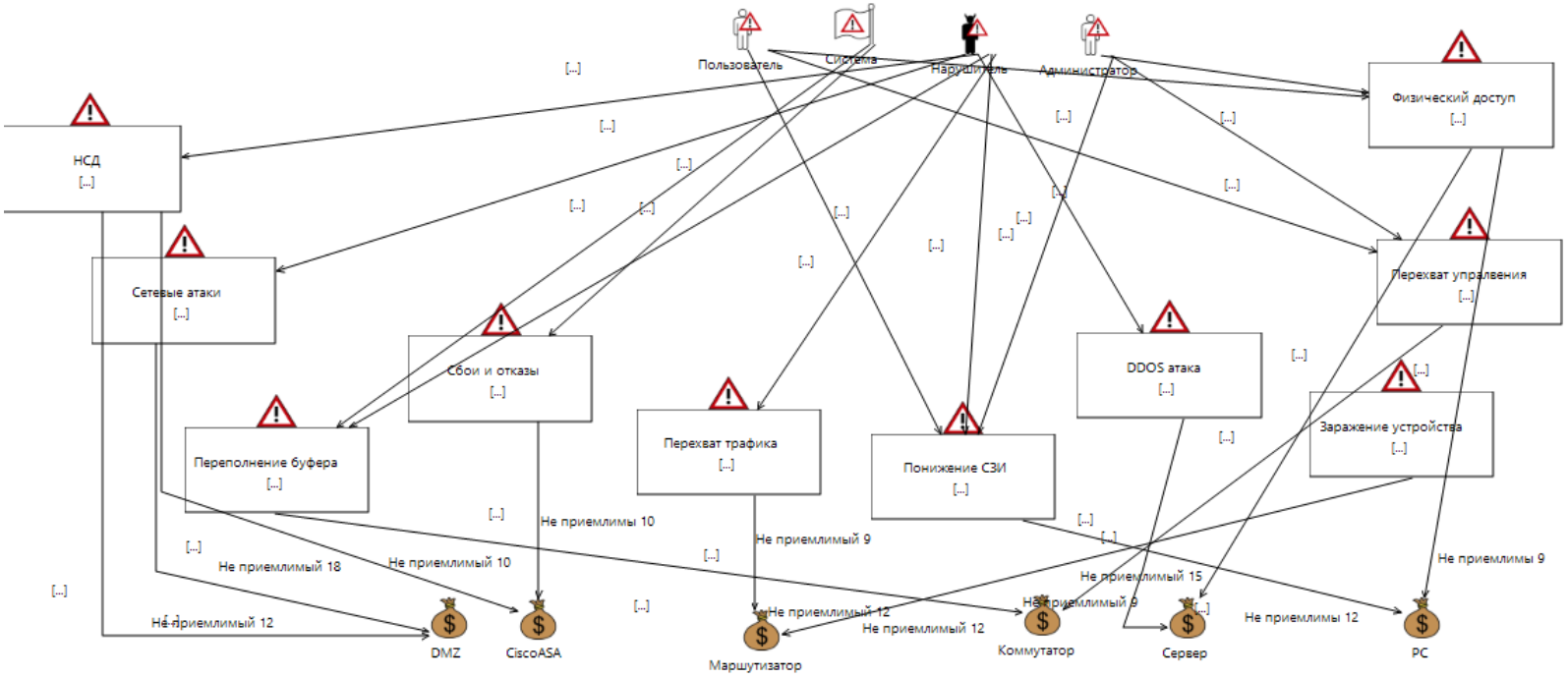

Рисунок 4.7 – Диаграмма рисков с оценкой

Вводим меры по защите активов от угроз. Каждая угроза риск, который является не приемлемый подлежит внедрения сзи.

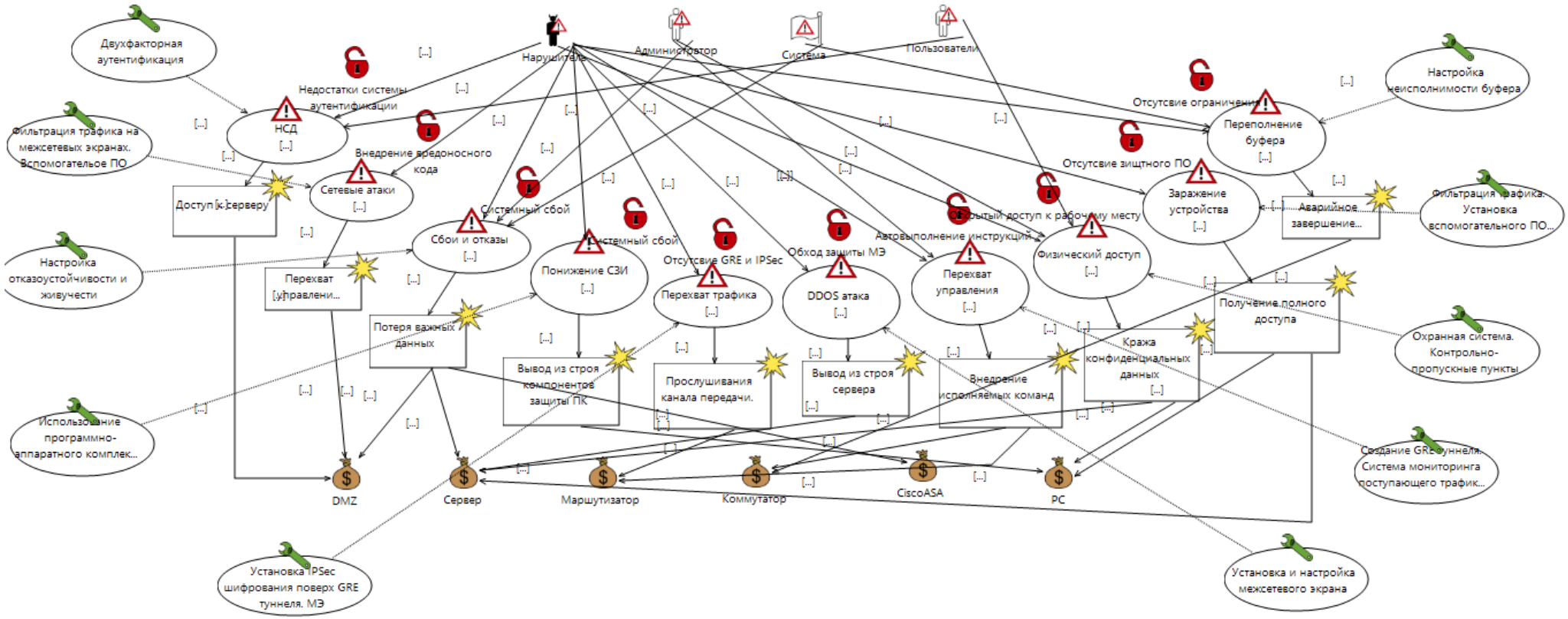

Рисунок 4.8 – Включение СЗИ в диаграмму угроза и уязвимость

После внедрения защитных мер мы получим новое значение для рисковой ситуации, если риск будет приемлемый, то меры по защите оправдывают себя и актив можно считать потенциально защищенным.

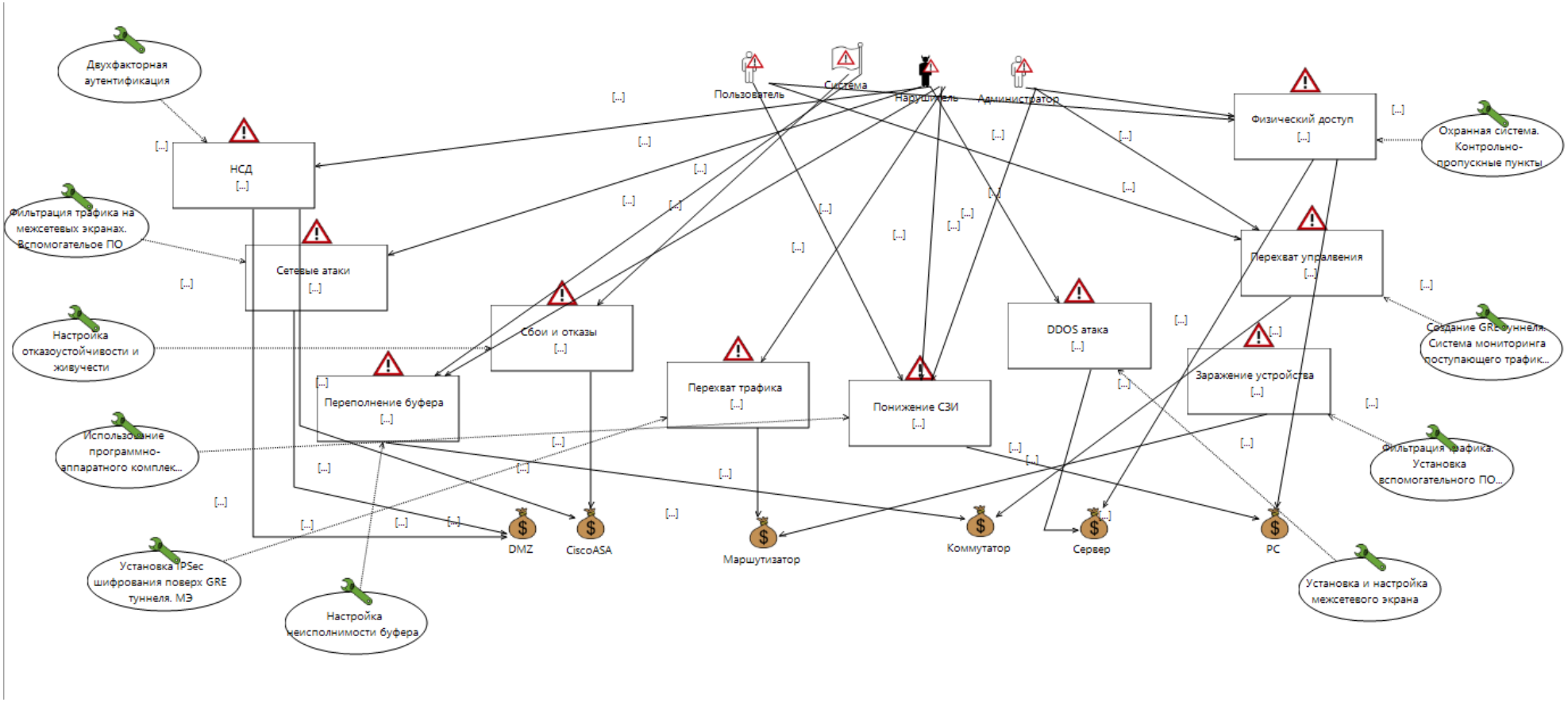

Рисунок 4.9 - Диаграмма рисков с мерами по их исключению

4.4 Вывод по разделу анализ и оценка рисков

В данной главе дипломной работы был произведен расчет рисков проектируемой сетевой схемы. Расчет производился по двум параметрам. Сначала были выявлены активы, находящиеся в зоне рисков иб, им были присвоены ценность и приоритет. После был произведен расчет максимального значения риска, что позволило выявить приемлемость риска для угрозы, воздействующей на актив. Были введены меры защитные меры в состав которых входили: фильтрация трафика, двухфакторная аутентификация, физическая безопасность, установка парольной защиты, gre туннель с ipsec шифрованием, vlan, acl-листы и т.д. Далее произведены повторные вычисления, после которых риски стали приемлемыми. Значение остаточного риска в среднем стало меньше на 5 и риски стали приемлемыми, что позволяет утверждать, что внедренные защитные меры оправдывают свое использование.

Заключение

В данной дипломной работе производилось проектирование безопасной сети с помощью eve-ng на платформе Windows 10. В первой части производился теоретический обзор к подходу построения безопасной сети. В ходе обзора были рассмотрены темы: топологии сети, основные положения в проектировании сети, жизненный цикл системы, аксиомы безопасности, защита сетевой инфраструктуры. При проектировании сети мы будем опираться на лучшие практики, описанные в первом разделе. Во второй части переходим развертыванию виртуальной лаборатории eve-ng на Windows 10. В ходе разработки основными компонентами были маршрутизаторы, коммутаторы, ciscoasa. В качестве защитных меры использовались: vlan, acl-листы, парольная защита, gre-туннель, ipsec шифрование. Для повышения отказоустойчивости сетевого модуля на ciscoasa был настроен failover. Для возможности в случаи возникновения чрезвычайной ситуации отправки данных на резервную ciscoasa готовую к работе. Третья часть работы было посвящена безопасности жизнедеятельности. Сначала был произведен анализ условий труда сотрудников офиса. В который входили нормы по созданию микроклимата офисных помещений и допустимого уровня шума. Расчетная часть состоит из расчета времени эвакуации и обеспечении безопасности от поражения электрическим током сотрудников офиса. Финальные значение полученные в расчетах полностью удовлетворяют установленные нормы безопасности. В четвертой части происходит анализ и оценка рисков. Оценка рисков происходит по двум параметрам. Активами являются: маршрутизатор, коммутатор, dmz,server,pc,ciscoasa. Сначала мы выяснили, что возможные риски для этих активов неприемлемы. После мы ввели защитные меры и произвели расчеты повторно. Введение защитных мер позволило снизить риски и перевести риски в категории приемлемых. В завершении дипломной работы мы имеем разработанный модуль безопасной сети, рассчитанный на внедрение в компании среднего и малого бизнеса.

Список литературы

1. Поляк-Брагинский А.В. Сеть под Microsoft Windows. -М.:Литрес, 2003. – 650с.
2. Куроуз Д. Компьютерные сети.Нисходящий подход. М.: Изд-во Эксмо, 2013. – 912с.
3. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам. -М.: Изд-во Диалектика-Вильямс, 2012. – 706с
4. Таненбаум Э., Уэзеролл Д. Компьютерные сети. -СПб.: Питер,2012.-960с.
5. Олифер В.Г., Олифер Н.А. Компьютерные сети.Принципы, технологии, протоколы. -СПб.: Изд-во Питер,2010.-944с.
6. Блам Э. Сеть. Как устроен и как работает Интернет. -М.: Изд-во AST Publishers, 2014.-136с.
7. Дибров М. Компьютерные сети и телекоммуникации. Маршрутизация в ip-сетях в 2 ч. Часть 1. -М.: Изд-во Юрайт,2017.-334с.
8. Дибров М. Компьютерные сети и телекоммуникации. Маршрутизация в ip-сетях в 2 ч. Часть 2. -М.: Изд-во Юрайт,2017.-352с.
9. Ибе О. Компьютерные сети и службы удаленного доступа. -М.: Изд-во ДМК Пресс,2018.-337с.
10. Проскуряков А. Компьютерные сети.Основы построения компьютерных сетей и телекоммуникаций. -М.: Изд-во Факел,2018.-203с.
11. Пайпер Б. Администрирование сетей Cisco. -М.: Изд. ДМК Пресс, 2017. – 318с.
12. Хабракен Д. Маршрутизаторы Cisco: Практическое применение. -М.: Изд-во ДМК Пресс,2016.- 318с.
13. Оглтри В. Firewalls: Практическое применение межсетевых экранов. -М.: Изд-во ДМК Пресс, 2016.-405с.
14. Букатов А.А., Гуда С.А. Компьютерные сети: расширенный начальный курс. – СПб.: Изд-во Питер, 2019.-497с.
15. Джером Ф. Маршрутизаторы Cisco: Пособие для самостоятельного изучения. -М.: Изд-во Символ-Плюс, 2003. – 508с.
16. Андрончик А.Н., Коллеров А.С. Сетевая защита на базе технологий фирмы Cisco Systems: Учебное пособие. -Новосибирск: Изд-во Флинта,2018.-179с.
17. Меньшуткин А. Справочник по настройке сетевого оборудования Cisco. -М.: ЛитРес, 2020.-330с.
18. Палмер М. Проектирование и внедрение компьютерных сетей: Учебный курс. -М.: Изд-во “BHV”, 2004.-752с.
19. Сергеев А.Н. Основы локальных компьютерных сетей. -М.: Изд-во Лань,2016.-184с.

20. Робачевский А. Интернет изнутри. -М.: Изд-во Альпина Паблишер, 2017.-224с.
21. Поляк-Брагинский А.В. Сеть своими руками. -М.: ЛитРес, 2008.-275с.
22. Ващенко Б. Проектирование сети кампуса. -М.:ЛитРес, 2006.-327с.
23. Ефремова О.С. Документация по охране труда в организации: Практическое пособие. -5-е изд. перераб. и доп. -М.: Изд-во Альфа-Пресс,2015 г. – 152 с.
24. Ефремов О.С. Охрана труда в организации в схемах и таблицах. [Текст] / О.С. Ефремова 7-е изд. перераб. и доп. -М.: Изд-во Альфа-Пресс,2018 г. – 124 с.
25. СанПин 2.2.4.548-2001.Санитарные правила и нормы. Гигиенические требования к микроклимату производственных помещений. Санитарные правила и нормы. – М.: Информационно-издательский центр Минздрава Казахстана. 2001. -20 с.
26. СН 2.2.4/2.1.8.562-96. Санитарные нормы. Шум на рабочих местах, в жилых помещениях, общественных зданиях и на территории жилой застройки. Санитарные нормы. -М.: Издательский центр Минздрава РФ. 1996. – 25 с.
27. СП 1.13130.2009. Системы противопожарной защиты. Эвакуационные пути и выходы. Системы противопожарной защиты. -М.: Центр информатизации РФ. 2009. 47с
28. ГОСТ Р 505713-2009(МЭК 60363-4-41:2005. Электроустановки низковольтные. Требования для обеспечения безопасности. Защита от поражения электрическим током. -М.: Издательский центр Стандартинформ, 2009.-70 с.
29. ГОСТ IEC 61140-2012. Защита от поражения электрическим током. Общие положения безопасности установок и оборудования. - М.: Стандартинформ, 2012 – 30с.
30. ГОСТ 12.1.038-82. Система стандартов безопасности труда. Электробезопасность. Предельно допустимые значения напряжений и токов. - М.: ИПК издательство стандартов, 2001-15с.

Приложение А.
Код настройки компонентов сети.

```
branchRT>en
branchRT#conf t
branchRT(config)#interface Gi0/0
branchRT(config-if)#ip address 10.10.10.200 255.255.255.0
branchRT(config-if)#no shutdown
branchRT(config-if)#exit
branchRT(config)#interface Gi0/1
branchRT(config-if)#ip address 172.168.112.2 255.255.255.252
branchRT(config-if)#no shutdown
branchRT(config-if)#exit
branchRT(config)#ip route 40.0.1.0 255.255.255.0 172.168.112.1
branchRT(config)#ip route 30.0.1.0 255.255.255.0 40.0.1.2
branchRT(config)#exit
branchRT# wr mem
VPC# ip 10.10.10.100/24 10.10.10.200
VPC# save config
ISP#conf t
ISP(config)#interface Gi0/1
ISP(config-if)#ip address 172.168.112.1 255.255.255.252
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#interface Gi0/0
ISP(config-if)#ip address 40.0.1.1 255.255.255.0
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#ip route 10.10.10.0 255.255.255.0 172.168.112.2
ISP(config)#ip route 30.0.1.0 255.255.255.0 40.0.1.2
ISP(config)#exit
ISP# wr mem
ISP(config)reboot
BorderRT(config)#int g0/0
BorderRT(config-if)#ip add
BorderRT(config-if)#ip address 40.0.1.2 255.255.255.0
BorderRT(config-if)#no sh
BorderRT(config)#int g0/1
BorderRT(config-if)#ip add
BorderRT(config-if)#ip address 30.0.1.1 255.255.255.0
BorderRT(config-if)#no sh
asaPrimary
ciscoasa(config)#int Gi0/0
no sh
```

Продолжение приложения А

```
int Gi0/0.30
vlan 30
nameif outside
sec-level 0
ip address 30.0.1.100 255.255.255.0
no sh
exit
int g0/1
no sh
int g0/1.40(dmz)
vlan 40
nameif DMZ
sec-level 60
ip add 192.168.40.1 255.255.255.0
no sh
int g0/2.50(Perimeter)
vlan 50
nameif Perimeter
sec-level 100
ip add 192.168.50.1 255.255.255.0
no sh
static nat
object network DMZ_server
host 192.168.40.10
object network staticNAT_DMZ_server
host 172.16.11.10
exit
nat (DMZ,outside) source static DMZ_server staticNAT_DMZ_server
access-list nat_dmz extended permit icmp 192.168.172.0 255.255.255.0
10.10.10.0 255.255.255.0
access-group nat_dmz in interface outside
standby
interface g0/0
ip address 30.0.1.30 255.255.255.0 standby 30.0.1.101
interface g0/1.40
ip address 192.168.40.1 255.255.255.0 standby 192.168.40.101
interface g0/2.50
ip address 192.168.50.1 255.255.255.0 standby 192.168.50.101
interface g0/3
no sh
failover lan interface failover(это имя интерфейса) g0/3
failover link failover g0/3
failover interface ip failover 20.0.1.1 255.255.255.252 standby 20.0.1.2
```

Продолжение приложения А

```
failover lan unit primary
failover
asaSecond
failover lan interface failover(это имя интерфейса) g0/3
failover link failover g0/3
failover interface ip failover 20.0.1.1 255.255.255.252 standby 20.0.1.2
failover lan unit secondary
failover
dmz switch
interface GigabitEthernet0/0
switchport trunk allowed vlan 40,50
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface GigabitEthernet0/1
 switchport trunk allowed vlan 40,50
switchport trunk encapsulation dot1q
switchport mode trunk
interface GigabitEthernet0/2
switchport trunk allowed vlan 40,50
switchport trunk encapsulation dot1q
switchport mode trunk
interface GigabitEthernet0/3
switchport trunk allowed vlan 40,50
switchport trunk encapsulation dot1q
switchport mode trunk
interface GigabitEthernet0/0
 switchport trunk allowed vlan 40,50
 media-type rj45
 negotiation auto
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
 spanning-tree portfast edge
!
interface GigabitEthernet0/2
 media-type rj45
 negotiation auto
!
interface GigabitEthernet0/3
 media-type rj45
```

```
 negotiation auto
!
interface GigabitEthernet1/0
 switchport access vlan 172
 switchport mode access
 media-type rj45
 negotiation auto
!
interface GigabitEthernet1/0
 switchport access vlan 50
 switchport mode access
 media-type rj45
 negotiation auto
!
interface GigabitEthernet1/2
 media-type rj45
 negotiation auto
!
interface GigabitEthernet1/3
 media-type rj45
 negotiation auto
!
interface Vlan100
 no ip address
 shutdown
!
interface Vlan172
 no ip address
 shutdown
 ip route 10.112.0.0 255.255.255.0 212.192.88.151
per switch
Switch#conf t
Switch(config)#int Gi0/0
Command rejected: An interface whose trunk encapsulation is "Auto" can
not be configured to "trunk" mode.
Switch(config-if)#switchport trunk allowed vlan 100,172
Switch(config-if)#exit
Switch(config)#int Gi0/1
Switch(config-if)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can
not be configured to "trunk" mode.
Switch(config-if)#switchport trunk allowed vlan 100,172
Switch(config-if)#end
```

Продолжение приложения А

```
2nd branchRT
hostname branchRT
int g0/0
ip address 195.221.31.2 255.255.255.252
no sh
int g0/1
ip address 31.0.1.1 255.255.255.0
no sh
asa branch
int g0/1
ip address 31.0.1.2 255.255.255.0
no sh
nameif out
exit
int g0/0
no sh
int g0/0.72
vlan 72
nameif shareZONE
sec-level 60
ip address 192.168.72.1 255.255.255.0
no sh
int g0/0.10
vlan 10
nameif Per
sec-level 100
ip address 192.168.10.1 255.255.255.0
no sh
ciscoasa(config-network-object)host 192.168.33.33
(config-network-object) nat(DMZ,out) static 10.10.10.33
(config-network-object) exit
Ciscoasa(config) access-list outside_dmz extended permit tcp any host
192.168.33.33
Ciscoasa(config) access-group outside_dmz in interface out
Ciscoasa(config) exit
Ciscoasa(config) access-list internet-icmp permit icmp any any echo-reply
Ciscoasa(config) access-group internet-icmp in interface out
Ciscoasa(config) access-list internet-http permit tcp any gt 1024 any eq
www
BranchRT(config)#line console 0
BranchRT(config-line) #password max
BranchRT(config-line)# login
BranchRT(config-line) exit
```

Продолжение приложения А

```
BranchRT(config)# line vty 0 4
BranchRT(config-line) # password max
BranchRT(config-line) # login
BranchRT(config-line) # exit
BranchRT(config)#enable password max
BranchRT(config)# exit
BranchRT(config)#enable password max
BranchRT(config)# exit
BranchRT(config)# service password-encryption
BranchRT(config)#exit
BorderRT(config)#line console 0
BorderRT(config-line) #password max
BorderRT(config-line)# login
BorderRT(config-line) exit
BorderRT(config)# exit
BorderRT(config)# line vty 0 4
BorderRT(config-line) # password max
BorderRT(config-line) # login
BorderRT(config-line) # exit
BorderRT(config)#enable password max
BorderRT(config)# exit
BorderRT(config)#enable password max
BorderRT(config)# exit
BorderRT(config)# service password-encryption
BorderRT(config)#exit
root@eve-ng:# ip address add 172.16.0.10/24 dev pnet5
root@eve-ng:# cat /proc/sys/net/ipv4/ip_forward
root@eve-ng:# cd /etc/network/if-pre-up.d/
root@eve-ng:# /etc/network/if-pre-up.d# ls-all
root@eve-ng:# iptables -t nat -A POSTROUTING -o pnet0 -s 172.16.0.0/24
-j MASQUERADE
Router (config) #int g0/0
Router (config-if)# no sh
Router (config-if) # exit
Router (config) int Tunnel1
Router (config-if) interface Tunnel1
Router (config-if) ip address 172.168.1.3 255.255.255.0
Router (config-if) ip mtu 1400
Router (config-if) ip tcp adjust-mss 1360
Router (config-if) tunnel source 195.221.31.2
Router (config-if) tunnel destination 172.168.112.2
Router (config-if) do s hip int br
Router (config-if) do ping 172.16.1.3
```

Продолжение приложения А

```
BranchRT (config-if) interface Tunnel1
BranchRT (config-if) ip address 172.16.1.4 255.255.255.0
BranchRT (config-if) ip mtu 1400
BranchRT (config-if) ip tcp adjust-mss 1360
BranchRT  (config-if) tunnel source 172.168.112.2
BranchRT (config-if) tunnel destination 195.221.31.2
BranchRT (config-if) do s hip int br
BranchRT  (config) interfave Tunnel2
BorderRT (config-if) ip address 40.16.1.1 255.255.255.0
BorderRT (config-if) ip mtu 1400
BorderRT (config-if) ip tcp adj
BorderRT (config-if) ip tcp adjust-mss 1360
BorderRT (config-if) tunnel source 172.168.112.2
BorderRT (config-if) tunnel destionition 40.0.1.2
BorderRT(config)# crypto isakmp policy 1
BorderRT (config-isakmp)# encryption aes
BorderRT (config-isakmp)# authentication pre-share
BorderRT (config-isakmp)# group 2
BorderRT (config-isakmp)# lifetime 10000
BorderRT (config-isakmp)# exit
BorderRT (config)# crypto isakmp key 6 PASSWORD address 172.50.1.9
BorderRT (config)#crypto ipsec transform-set GRE-IPSEC esp-3des esp-
sha-hmac
BorderRT (config)# crypto ipsec profile GRE
BorderRT (ipsec-profile)# set security-association lifetime seconds 10000
BorderRT (ipsec-profile)# set transform-set GRE-IPSEC
BorderRT (ipsec-profile)# exit
BorderRT (config-if)# tunnel protection ipsec profile GRE
Router(config-isakmp) # encryption aes
Router(config-isakmp) # authentication pre-share
Router(config-isakmp) # group
Router(config-isakmp) # lifetime 10000
Router(config) # crypto isakmp key 6 PASSWORD address 172.50.1.10
Router(config) crypto ipsec transform-set GRE-IPSEC esp-3des esp-sha-
hmac
Router(config) crypto ipsec profile GRE
Router(ipsec-profile) # set security-association lifetime seconds 10000
Router(ipsec-profile) set transform-set GRE-IPSEC
Router(config-if) tunnel protection ipsec profile GRE
```