МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

кафедра „Компьютерные технологии"

«Допущен к защите»
Заведующий кафедрой _____
(Ф.И.О., ученая степень, звание)
_____ «_____»_____ **20__ г.**
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: "Разработка проекта "Сеть без границ" для банковской системы"

Специальность 5В070400- Вычислительная техника и программное обеспечение

Выполнил (а) Лебедев О. Г. (Фамилия и инициалы) ВТ-10-04 группа

Научный руководитель Майгожинова А. Ж., ст. препод. (Фамилия и инициалы, ученая степень, звание)

Консультанты:

по экономической части:
Ержанова З.Ж., сен. преподаватель
(Фамилия и инициалы, ученая степень, звание)
Ержанова «14» мая 2014 г.
(подпись)

по безопасности жизнедеятельности:
Джиенбаев К.Г., д.х.н., профессор
(Фамилия и инициалы, ученая степень, звание)
_____ «16» 05 2014 г.
(подпись)

по применению вычислительной техники:
Майгожинова А.Ж., ст. препод.
(Фамилия и инициалы, ученая степень, звание)
_____ «6» мая 2014 г.
(подпись)

_____
(Фамилия и инициалы, ученая степень, звание)
_____ «_____»_____ 20__ г.
(подпись)

Нормоконтролер: Тусупов Ф.М
(Фамилия и инициалы, ученая степень, звание)
_____ «20» мая 2014 г.
(подпись)

Рецензент: _____
(Фамилия и инициалы, ученая степень, звание)
_____ «_____»_____ 20__ г.
(подпись)

Алматы 2014 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

Факультет "Информационные технологии"
Специальность "Вычислительная техника и программное обеспечение"
Кафедра "Компьютерные технологии"

ЗАДАНИЕ
на выполнение дипломного проекта

Студент Лебедев Олег Геннадьевич
(фамилия, имя, отчество)
Тема проекта "Разработка проекта "Сети без границ" для банковской системы"

утверждена приказом ректора № 115 от «24» сентября 2013 г.
Срок сдачи законченной работы «7» июня 2014 г.
Исходные данные к проекту требуемые параметры результатов проектирования (исследования) и исходные данные объекта
Документации Cisco, книги по проектированию и безопасности корпоративных локальных сетей

Перечень подлежащих разработке дипломного проекта вопросов или краткое содержание дипломного проекта:
1. Классическая архитектура корпоративной сети.
2. Cisco TrustSec в рамках архитектура "Сети без границ"
3. Cisco EnergyWise в рамках архитектура "Сети без границ"
4. Безопасность жизнедеятельности.
5. Бизнес-план

Перечень графического материала (с точным указанием обязательных чертежей)

Топология корпоративной сети предприятия
Архитектура проекта "сеть без границ"

Рекомендуемая основная литература

1. Бакучев Т. А. "Безопасность корпоративных сетей".
2. Баличкий А., Рябко С.Р. "Защита информации в сети. Анализ технологий и систем решений".
3. Документация Cisco.
4. З.Д. Еркешева "Методические указания к выполнению самостоятельной работы для студентов специальности 5В070400".
5. СНиП РК 2.04-05-2002 Естественное и искусственное освещение. Строительные нормы и правила.

Консультанты по проекту с указанием относящихся к ним разделов

Раздел	Консультант	Сроки	Подпись
Технология	Еркешева З.Д.	15.04-14.05.14	Еркешева
БЖД	Джаббарова Н.Г.	16.04-16.05.14	
Основная часть	Байгожинова А.Н.	11.04-20.05.14	

Г Р А Ф И К
подготовки дипломного проекта

№ п/п	Наименование разделов, перечень разрабатываемых вопросов	Сроки представления руководителю	Примечание
1.	Обзор классической архитектуры сети предприятия. Анализ архитектура. Разработка сети предприятия в Packet Tracer	1.04.2014	
2.	Настройка архитектур сети, конфигурация оборудования в Packet Tracer.	10.04.2014.	
3.	Написание основной части, анализ политик безопасности, анализ сервиса TrustSec арх-ра "Сети без границ".	25-04.2014	
4.	Анализ и написание основной части, анализ сервиса Cisco Energy Wise.		
5.	Сбор готовой схема в Cisco Packet Tracer.	28.04.2014.	
6.	Безопасность жизнедеятельности	1.05.2014	
7.	Бизнес-план проекта	8.05.2014	

Дата выдачи задания «3» марта 2014 г.

Заведующий кафедрой _____ _____
(подпись) (Фамилия и инициалы)

Руководитель _____ Тайгонкинова А.Ш.
(подпись) (Фамилия и инициалы)

Задание принял к исполнению
студент _____ Лебедев О.Г.
(подпись) (Фамилия и инициалы)

АҢДАТПА

Бұл диплом жұмысында Cisco компаниясы инновациялық архитектураны қолдана отырып әзірлеген «Шексіз желілер» корпоративтік желілерді құрудың негізгі концепциясы қаралған. Корпоративтік желілерді құрудың дәстүрлі схемалары талданылды, атап айтқанда, ҚР Ұлттық Банкінің корпоративтік желісінің архитектурасы қаралды, сондай-ақ кіруге рұқсат беруді бақылау және желіні қорғау әдістері зерттелді. Желі құрылымы егжей-тегжейлі зерттелгеннен кейін, банктің корпоративтік желісі «Шексіз желі» архитектурасы шеңберінде белгілі қызметтерін енгізу арқылы жаңартылды, бұл банк жүйесіннің кейбір процестерін автоматтандырды және біршама жеңілдетті.

Бұдан басқа тіршілік қауіпсіздігі мәселелері қаралды, сондай-ақ жобаның бизнес-жоспары ұсынылды.

АННОТАЦИЯ

В данной выпускной работе рассмотрены основные концепции построения корпоративной сети с применением инновационной архитектуры «Сети без границ», разработанной компанией Cisco. Были проанализированы традиционные схемы построения корпоративных сетей, в частности, была рассмотрена архитектура корпоративной сети подразделения Национального Банка РК, а так же изучены методы защиты сети и контроля доступа. После детального изучения структуры сети, корпоративная сеть банка была подвергнута модернизации посредством внедрения в нее определенных сервисов в рамках архитектуры «Сети без границ», что значительно облегчило и автоматизировало некоторые процессы в банковской системе.

Помимо этого были рассмотрены вопросы безопасности жизнедеятельности, а также представлен бизнес-план проекта.

ANNOTATION

In this graduation work the basic concepts of building a corporate network with applying an innovative «Borderless Network» architecture were considered, which was developed by Cisco Company. As well, the traditional schemes of building a corporate network were analyzed, in particular, the network architecture of branch of the National Bank of Kazakhstan were considered, also, the main methods of access control and protection the corporate network was investigated. After a detailed studying of the structure of the network, a corporate network of the bank was upgraded by using some of «Borderless Network» architecture services, which greatly simplify and automate some processes in the bank system.

In addition, the main issues of life safety and business-plan were considered.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

На сегодняшний день новые технологии становятся неотъемлемой частью нашей жизни, и как следствие, происходят следующие изменения. На рынок трудовых ресурсов приходит новое поколение заказчиков и сотрудников. Представители нового поколения являются фанатами мультимедиа и постоянными пользователями социальных сетей. Они приносят на свои рабочие места мобильные и портативные видеоустройства и рассчитывают, что видео станет частью взаимодействия с сотрудниками, заказчиками и партнерами. Таким образом, сотрудники ИТ - подразделения сталкиваются не только с необходимостью поддерживать новые устройства и модели их использования, но и с изменением принципов работы, что создает новые колоссальные требования к внутренней инфраструктуре предприятия.

Для современной рабочей среды все более характерным становится расположение основных бизнес - ресурсов, включая центры обработки данных (далее ЦОД), приложения, сотрудников и заказчиков, вне привычных границ предприятия. Расширение границ бизнеса для охвата всего персонала и ресурсов возлагает большую ответственность на ИТ - подразделение. Но масштабирование ИТ - решений становится невозможным в условиях, когда каждый проект является исключением из традиционных принципов построения ИТ - архитектуры и ИТ- управления. ИТ - подразделению требуется более эффективный способ масштабирования и управления пользователями и заказчиками, которые могут находиться где угодно, и обеспечить пользователям системы возможность использования практически любых устройств для доступа к любым приложениям, расположенным в любой точке мира. В связи с этим меняется и стандартное представление о рабочем месте. Теперь оно не ограничивается офисом и даже страной, в которой мы работаем, т.е. размывается такое понятие, как «границы предприятия».

По оценкам некоторых исследовательских фирм, в ближайшем будущем предприятия будут претерпевать следующие изменения, а именно:

- к 2015 году 90% предприятий будет использовать личные устройства на рабочих местах;
- около 60% работников будут осуществлять свою деятельность вне офиса;
- к 2015 году на рынке беспроводной связи ведущую позицию займет технология Wi-Fi 802.11n и 802.11ac;
- Wi-Fi может стать основной технологией для работы с данными на смартфонах.

Таким образом, технологии беспроводного доступа получили практически повсеместное распространение. Тем не менее, множество предприятий до сих пор используют проводные беспроводные сети как отдельные объекты.

В связи с этим компания Cisco разработала абсолютно новую, инновационную архитектуру - «Сети без границ». Данная архитектура представляет платформу для объединения средств проводного и беспроводного доступа. Кроме того, она включает функции обеспечения безопасности, контроля доступа и управления производительностью устройств различных типов.

Таким образом, актуальной проблемой для большинства предприятий и различных структур Казахстана на сегодняшний день является проблема выхода за рамки традиционного понятия «границы предприятия», то есть, необходимость кардинального пересмотра традиционной схемы построения инфраструктуры сети. Поэтому компания Ciscoпредлагает абсолютно новую концепцию унифицированного доступа на основе политик, при этом отказавшись от традиционного понятия корпоративной сети.

Дипломный проект направлен на пересмотр традиционной архитектуры сети банковской системы и внедрение некоторых инновационных решений архитектуры «Сети без границ», таких как архитектура Cisco TrustSec, которая позволяет обеспечить безопасный доступ к корпоративными сервисам приложений на основе системы идентификации пользователей, а так же архитектура Cisco EnergyWise - новая архитектура управления энергопотреблением, которая позволяет средствами и ресурсами ИТ выполнять измерения и тонкую настройку использования электроэнергии, чтобы значительно сократить расходы. Технология Cisco EnergyWise позволяет снизить энергопотребление на всех устройствах, подключенных к сети Cisco - от устройств PoE (например, IP-телефонов) и точек беспроводного доступа до контроллеров зданий и системы освещения. Эта технология основана на архитектуре интеллектуальной сети и позволяет ИТ-подразделениям и коммунальным службам осознавать, оптимизировать, и эффективно управлять энергопотреблением в масштабе всей корпоративной инфраструктуры, контролируя практически каждое устройство, подключенное к сети.

1 Классическая архитектура корпоративной сети

Прежде чем начинать строить сеть с применением новой архитектуры Cisco «Сети без границ», необходимо рассмотреть основные принципы и аспекты построения традиционной архитектуры корпоративной сети, а так же методы обеспечения безопасности и политик доступа к тем или иным приложениям, находящимся как внутри локальной сети предприятия (сервера, ЦОД), так и за её пределами (доступ к Интернет и др.). Рассмотрим классическую схему построения корпоративной сети (Рисунок 1.1).

Рисунок 1.1 - Традиционная архитектура корпоративной сети

Как видно из рисунка 1.1, корпоративная сеть предприятия (в нашем случае, банка), состоит из главного офиса (HQ), удаленных филиалов и удаленных сотрудников (сотрудники, работающие из дома и подключающиеся к внутренним ресурсам сети через виртуальную защищённую сеть (VPN-туннель)). К внутренним ресурсам банка относятся сервера, которые выполняют все операции и занимаются обработкой данных, иными словами - центры обработки данных (ЦОДы). Это могут быть сервера баз данных (Database Servers), Интернет сервера (Web - Servers), файловые сервера (FTP Servers), почтовые сервера (Mail Servers), сервера приложений (Application Servers) и многие другие. Так как все эти сервера являются главным вычислительным ядром всей корпоративной сети, то они обычно располагаются отдельно в серверной комнате в отдельно выделенном сегменте сети (или даже сегментах) в так называемой DMZ - зоне. Между входом в

DMZ- зону и локальной сетью предприятия находится Межсетевой Экран (так же его ещё называют Firewall), который выполняет некую роль посредника между источником и приемником, при этом фильтруя и анализируя входящий и исходящий трафик. Межсетевой экран так же располагается между внутренней локальной сетью предприятия и глобальной сетью. Таким образом, внутренняя локальная сеть главного офиса находится в своеобразной защищенной области, а роль «защитника» этой области обеспечивает Межсетевой экран. С удаленным филиалом (филиалами) центральный офис обменивается информацией через защищенную приватную сеть (Virtual Private Network) , иными словами, своеобразный «туннель». Таким же образом, и сотрудник, работающий дома, подключается к корпоративной сети предприятия через защищенный VPN - туннель.

Таким образом, исходя из рисунка 1.1, границы нашей корпоративной сети четко определены из соображений безопасности, предприятие может лишь контролировать входящий и исходящий трафики, то есть, нет такой возможности сделать весть трафик «прозрачным», а именно знать, кто и что подключается к вашей корпоративной сети, откуда происходит подключение и как происходит подключение. С внедрением одного из решений архитектуры «Сети без границ», а именно, нового решения по обеспечению комплексной безопасности Cisco TrustSec, все это станет возможным и такое понятие как «границы предприятия» размоются, и новая корпоративная сеть будет выглядеть, как показано на рисунке 1.2.

Рисунок 1.2 - Архитектура «Сети без границ»

Таким образом, Cisco предлагает новую концепцию построения корпоративной сети предприятия, в которой будут интегрированы такие понятия как «проводная сеть», «беспроводная сеть» и сеть «VPN», при этом будет реализована единая политика управления для данного нового решения (Рисунок 1.3).

Рисунок 1.3 - Решение «Унифицированного доступа»

Прежде чем рассматривать решение Cisco TrustSec, нужно более детально рассмотреть основные методы защиты и политики в рамках данной корпоративной сети, а так же устройства (коммутаторы, маршрутизаторы, межсетевые экраны), на которых эта защита реализуется.

1.1 Средства, реализующие защиту компьютерной сети в банковской системе

Наиболее популярным в наше время средством защиты корпоративной информации от внешних и внутренних угроз является межсетевой экран. Межсетевой экран - это система межсетевой защиты, позволяющая разделить каждую сеть на две и более части и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую. Как правило, эта граница проводится между корпоративной (локальной) сетью предприятия и глобальной сетью Интернет (Рисунок 1.4), хотя ее можно провести и внутри корпоративной сети предприятия [1].

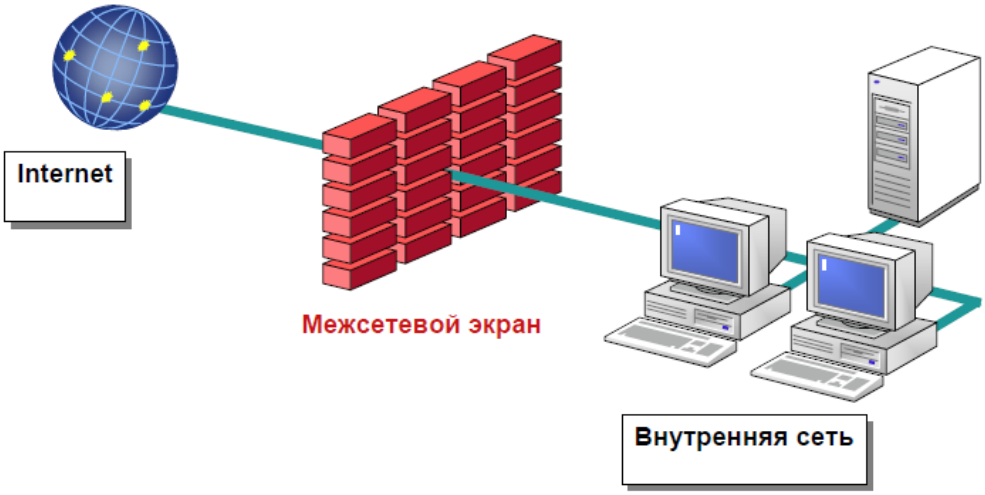

Рисунок 1.4 - Традиционное размещение МЭ в корпоративной сети

1.2 Функции межсетевых экранов

Основными функциями межсетевых экранов, как контрольных пунктов, на сегодняшний день является контроль трафика, входящего во внутреннюю корпоративную сеть, и трафика, исходящего из внутренней корпоративной сети.

Контроль информационных потоков, проходящих через межсетевой экран, состоит в их фильтрации и преобразовании в соответствии с набором определенных заданных правил. Поскольку в современных МЭ фильтрация может осуществляться на разных уровнях эталонной модели взаимодействия открытых систем (ЭМВОС, OSI), МЭ удобно представить в виде системы фильтров. Каждый фильтр на основе анализа проходящих через него данных, принимает решение - пропустить дальше, перебросить за экран, блокировать или преобразовать данные (Рисунок 1.5) [1].

Рисунок 1.5 - Схема фильтрации в межсетевом экране

Неотъемлемой функцией МЭ является протоколирование информационного обмена. Ведение журналов регистрации позволяет администратору выявить подозрительные действия, ошибки в конфигурации МЭ и принять решение об изменении правил МЭ.

1.2.1 Фильтрация трафика

Так как основное предназначение межсетевого экрана заключается в фильтрации трафика, то его можно представить как ряд фильтров. Каждый из фильтров предназначен для интерпретации отдельных правил фильтрации путем:

1) анализа информации по заданным в интерпретируемых правилах критериям, например по адресам получателя и отправителя или по типу приложения, для которого эта информация предназначена;

2) принятия на основе интерпретируемых правил одного из следующих решений:

- не пропустить данные;
- обработать данные от имени получателя и возвратить результат отправителю;
- передать данные на следующий фильтр для продолжения анализа;
- пропустить данные, игнорируя следующие фильтры.

Правила фильтрации могут задавать и дополнительные действия, которые относятся к функциям посредничества, например преобразование данных, регистрация событий и др. Соответственно правила фильтрации определяют перечень условий, по которым осуществляется:

- разрешение или запрещение дальнейшей передачи данных;
- выполнение дополнительных защитных функций.

В качестве критериев анализа информационного потока могут использоваться следующие параметры:

- служебные поля пакетов сообщений, содержащие сетевые адреса, идентификаторы, адреса интерфейсов, номера портов и другие значимые данные;
- непосредственное содержимое пакетов сообщений, проверяемое, например, на наличие компьютерных вирусов;
- внешние характеристики потока информации, например, временные, частотные характеристики, объем данных и т. д.

Используемые критерии анализа зависят от уровней модели OSI, на которых осуществляется фильтрация. В общем случае, чем выше уровень модели OSI, на котором МЭ фильтрует пакеты, тем выше и обеспечиваемый им уровень защиты [1].

1.2.2 Выполнение функции посредничества

Функции посредничества МЭ выполняет с помощью специальных программ, называемых экранирующими агентами или программами-посредниками. Эти программы являются резидентными и запрещают непосредственную передачу пакетов сообщений между внешней и внутренней сетью.

При необходимости доступа из внутренней сети во внешнюю сеть или наоборот вначале должно быть установлено логическое соединение с программой-посредником, функционирующей на компьютере МЭ. Программа-посредник проверяет допустимость запрошенного межсетевого взаимодействия и при его разрешении сама устанавливает отдельное соединение с требуемым компьютером. Далее обмен информацией между компьютерами внутренней и внешней сети осуществляется через программного посредника, который может выполнять фильтрацию потока сообщений, а также осуществлять другие защитные функции.

Следует иметь в виду, что МЭ может выполнять функции фильтрации без применения программ-посредников, обеспечивая прозрачное взаимодействие между внутренней и внешней сетью. Вместе с тем программные посредники могут и не осуществлять фильтрацию потока сообщений.

В общем случае программы-посредники, блокируя прозрачную передачу потока сообщений, могут выполнять следующие функции:

- проверку подлинности передаваемых данных;
- фильтрацию и преобразование потока сообщений, например, динамический поиск вирусов и прозрачное шифрование информации;
- разграничение доступа к ресурсам внутренней сети;
- разграничение доступа к ресурсам внешней сети;
- кэширование данных, запрашиваемых из внешней сети;
- идентификацию и аутентификацию пользователей;
- трансляцию внутренних сетевых адресов для исходящих пакетов сообщений;
- регистрацию событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерацию отчетов.

Программы-посредники могут осуществлять проверку подлинности получаемых и передаваемых данных. Это актуально не только для аутентификации электронных сообщений, но и мигрирующих программ (Java, ActiveX Controls), по отношению к которым может быть выполнен подлог. Проверка подлинности сообщений и программ заключается в контроле их цифровых подписей [2].

Программы-посредники могут выполнять разграничение доступа к ресурсам внутренней или внешней сети, используя результаты идентификации и аутентификации пользователей при их обращении к МЭ.

Способы разграничения доступа к ресурсам внутренней сети практически не отличаются от способов разграничения, поддерживаемых на уровне операционной системы.

При разграничении доступа к ресурсам внешней сети чаще всего используется один из следующих подходов:

- разрешение доступа только по заданным адресам во внешней сети;
- фильтрация запросов на основе обновляемых списков недопустимых адресов и блокировка поиска информационных ресурсов по нежелательным ключевым словам;
- накопление и обновление администратором санкционированных информационных ресурсов внешней сети в дисковой памяти МЭ и полный запрет доступа во внешнюю сеть.

С помощью специальных посредников поддерживается также кэширование данных, запрашиваемых из внешней сети. При доступе пользователей внутренней сети к информационным ресурсам внешней сети вся информация накапливается на пространстве жесткого диска МЭ, называемого в этом случае proxy-сервером. Поэтому если при очередном запросе нужная информация окажется на proxy-сервере, то посредник предоставляет ее без обращения к внешней сети, что существенно ускоряет доступ. Администратору следует позаботиться только о периодическом обновлении содержимого proxy-сервера.

Функция кэширования успешно может использоваться для ограничения доступа к информационным ресурсам внешней сети. В этом случае все санкционированные информационные ресурсы внешней сети накапливаются и обновляются администратором на proxy-сервере. Пользователям внутренней сети разрешается доступ только к информационным ресурсам proxy-сервера, а непосредственный доступ к ресурсам внешней сети запрещается.

Фильтрация и преобразование потока сообщений выполняется посредником на основе заданного набора правил. Здесь следует различать два вида программ-посредников:

- экранирующие агенты, ориентированные на анализ потока сообщений для определенных видов сервиса, например FTP, HTTP, Telnet;
- универсальные экранирующие агенты, обрабатывающие весь поток сообщений, например агенты, ориентированные на поиск и обезвреживание компьютерных вирусов, или прозрачное шифрование данных.

Программный посредник анализирует поступающие к нему пакеты данных и, если какой-либо объект не соответствует заданным критериям, то либо блокирует его дальнейшее продвижение, либо выполняет соответствующие преобразования, например, обезвреживает обнаруженные компьютерные вирусы. При анализе содержимого пакетов важно, чтобы экранирующий агент мог автоматически распаковывать проходящие файловые архивы [2].

МЭ с посредниками позволяют также организовывать защищенные виртуальные сети VPN (Virtual Private Network), например, безопасно

объединять несколько локальных сетей, подключенных к Интернет, в одну виртуальную сеть.

1.2.3 Идентификация и аутентификация пользователей

Кроме разрешения или запрещения допуска различных приложений в сеть, МЭ могут также выполнять аналогичные действия и для пользователей, которые желают получить доступ к внешним или внутренним ресурсам, разделяемым МЭ.

Прежде чем пользователю будет предоставлено право использования какого-либо сервиса, необходимо убедиться, что он действительно тот, за кого себя выдает. Идентификация и аутентификация пользователей являются важными компонентами концепции МЭ. Авторизация пользователя обычно рассматривается в контексте аутентификации - как только пользователь аутентифицирован, для него определяются разрешенные ему сервисы.

Идентификация и аутентификация пользователя иногда осуществляются при предъявлении обычного идентификатора (имени) и пароля. Однако эта схема уязвима с точки зрения безопасности - пароль может быть перехвачен и использован другим лицом. Многие инциденты в сети Интернет произошли отчасти из-за уязвимости традиционных многоразовых паролей. Злоумышленники могут наблюдать за каналами в сети Интернет и перехватывать передающиеся в них открытым текстом пароли, поэтому такая схема аутентификации считается неэффективной. Пароль следует передавать через общедоступные коммуникации в зашифрованном виде. Это позволяет предотвратить получение несанкционированного доступа путем перехвата сетевых пакетов (Рисунок 1.6) [2].

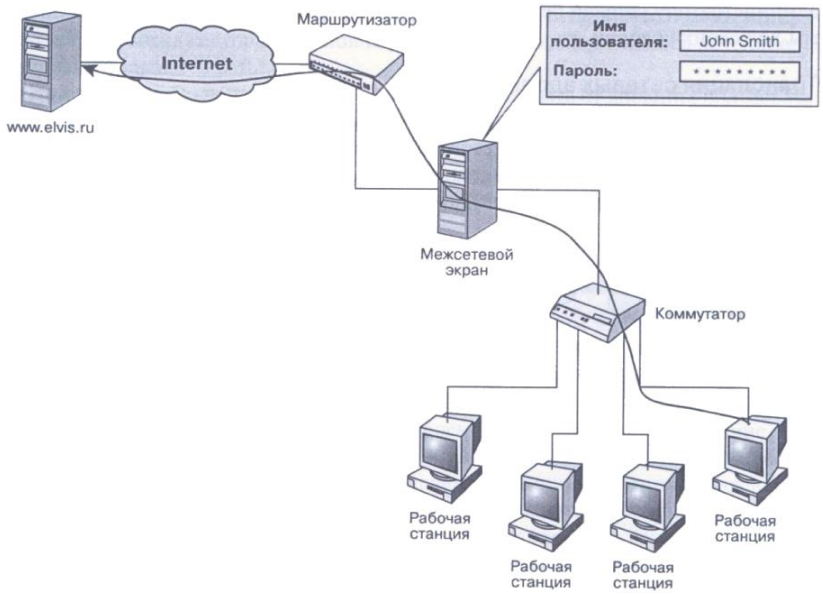

Рисунок 1.6 - Схема аутентификации пользователя по предъявляемому паролю

Более надежным методом аутентификации является использование одноразовых паролей. Широкое распространение получила технология аутентификации на основе одноразовых паролей SecurID.

Удобно и надежно также применение цифровых сертификатов, выдаваемых доверенными органами, например центром распределения ключей. Большинство программ-посредников разрабатываются таким образом, чтобы пользователь аутентифицировался только в начале сеанса работы с МЭ. После этого от него не требуется дополнительная аутентификация в течение времени, определяемого администратором.

Так как МЭ могут централизовать управление доступом в сети, они являются подходящим местом для установки программ или устройств усиленной аутентификации. Хотя средства усиленной аутентификации могут использоваться на каждом хосте, более практично их размещение на МЭ. При отсутствии МЭ, использующего меры усиленной аутентификации, неаутентифицированный трафик таких приложений, как Telnet или FTP, может напрямую проходить к внутренним системам в сети.

Ряд МЭ поддерживают Kerberos - один из распространенных методов аутентификации. Как правило, большинство коммерческих МЭ поддерживают несколько различных схем аутентификации, позволяя администратору сетевой безопасности сделать выбор наиболее приемлемой схемы для своих условий.

1.2.4 Трансляция сетевых адресов

Для реализации многих атак злоумышленнику необходимо знать адрес своей жертвы. Чтобы скрыть эти адреса, а также топологию всей сети, МЭ выполняют очень важную функцию - трансляцию внутренних сетевых адресов (Network Address Translation) или сокращенно - NAT (Рисунок 1.7).

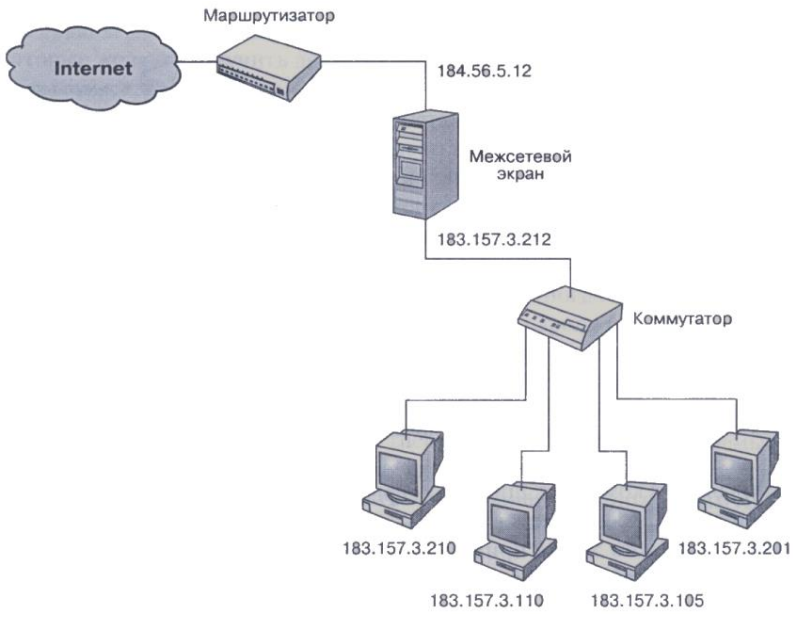

Рисунок 1.7 - Трансляция сетевых адресов

Данная функция реализуется по отношению ко всем пакетам, следующим из внутренней сети во внешнюю. Для этих пакетов выполняется автоматическое преобразование IP-адресов компьютеров-отправителей в один «надежный» IP-адрес.

Трансляция внутренних сетевых адресов может осуществляться двумя способами - динамически и статически. В первом случае адрес выделяется узлу в момент обращения к МЭ. После завершения соединения адрес освобождается и может быть использован любым другим узлом корпоративной сети. Во втором случае адрес узла всегда привязывается к одному адресу МЭ, из которого передаются все исходящие пакеты. IP-адрес МЭ становится единственным активным IP-адресом, который попадает во внешнюю сеть. В результате все исходящие из внутренней сети пакеты оказываются отправленными МЭ, что исключает прямой контакт между авторизованной внутренней сетью и являющейся потенциально опасной внешней сетью [2].

При таком подходе топология внутренней сети скрыта от внешних пользователей, что усложняет задачу несанкционированного доступа. Кроме повышения безопасности трансляция адресов позволяет иметь внутри сети собственную систему адресации, не согласованную с адресацией во внешней сети, например в сети Internet. Это эффективно решает проблему расширения адресного пространства внутренней сети и дефицита адресов внешней сети.

1.2.5 Администрирование, регистрация событий и генерация отчетов

Простота и удобство администрирования является одним из ключевых аспектов в создании эффективной и надежной системы защиты. Ошибки при определении правил доступа могут образовать дыру, через которую возможен взлом системы. Поэтому в большинстве МЭ реализованы сервисные утилиты, облегчающие ввод, удаление, просмотр набора правил. Наличие этих утилит позволяет также производить проверки на синтаксические или логические ошибки при вводе или редактирования правил. Как правило, утилиты позволяют просматривать информацию, сгруппированную по каким-либо критериям, например все, что относится к конкретному пользователю или сервису.

Важными функциями МЭ являются регистрация событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и составление отчетов. МЭ, являясь критическим элементом системы защиты корпоративной сети, имеет возможность регистрации всех действий, им фиксируемых. К таким действиям относятся не только пропуск или блокирование сетевых пакетов, но и изменение правил разграничения доступа администратором безопасности и другие действия. Такая регистрация позволяет обращаться к создаваемым журналам по мере необходимости (в случае возникновения инцидента безопасности или сбора доказательств для предоставления их в судебные инстанции или для внутреннего расследования).

При правильно настроенной системе фиксации сигналов о подозрительных событиях (alarm) МЭ может дать детальную информацию о том, были ли МЭ или сеть атакованы или зондированы. Собирать статистику использования сети и доказательства ее зондирования важно по нескольким причинам. Прежде всего, нужно знать наверняка, что МЭ устойчив к зондированию и атакам, и определить, адекватны ли меры защиты МЭ. Кроме того, статистика использования сети важна в качестве исходных данных при проведении исследований и анализе риска для формулирования требований к сетевому оборудованию и программам [2].

Многие МЭ содержат мощную систему регистрации, сбора и анализа статистики. Учет может вестись по адресам клиента и сервера, идентификаторам пользователей, времени сеансов, времени соединений, количеству переданных/принятых данных, действиям администратора и пользователей. Системы учета позволяют произвести анализ статистики и предоставляют администраторам подробные отчеты. За счет использования специальных протоколов МЭ могут выполнить удаленное оповещение об определенных событиях в режиме реального времени.

В качестве обязательной реакции на обнаружение попыток выполнения несанкционированных действий должно быть определено уведомление администратора, т. е. выдача предупредительных сигналов. Любой МЭ, который не способен посылать предупредительные сигналы при обнаружении нападения, нельзя считать эффективным средством межсетевой защиты.

1.3 Классификация МЭ

Выделяют следующую классификацию МЭ, в соответствие с функционированием на разных уровнях МВОС (OSI) [1]:

- Мостиковые экраны (2 уровень OSI).
- Фильтрующие маршрутизаторы (3 и 4 уровни OSI).
- Шлюзы сеансового уровня (5 уровень OSI).
- Шлюзы прикладного уровня (7 уровень OSI).
- Комплексные экраны (3-7 уровни OSI).

Рассмотрим более подробно каждую категорию и выявим достоинства и недостатки каждой категории.

1.3.1 Мостиковые МЭ

Данный класс МЭ, функционирующий на 2-м уровне модели OSI, известен также как прозрачный (stealth), скрытый, теневой МЭ. Мостиковые МЭ появились сравнительно недавно и представляют перспективное направление развития технологий межсетевого экранирования. Фильтрация трафика ими осуществляется на канальном уровне, т.е. МЭ работают с фреймами (frame, кадр).

К достоинствам подобных МЭ можно отнести:

- Нет необходимости в изменении настроек корпоративной сети, не требуется дополнительного конфигурирования сетевых интерфейсов МЭ.
- Высокая производительность. Поскольку это простые устройства, они не требуют больших затрат ресурсов. Ресурсы требуются либо для повышения возможностей машин, либо для более глубокого анализа данных.
- Прозрачность. Ключевым для этого устройства является его функционирование на 2 уровне модели OSI. Это означает, что сетевой интерфейс не имеет IP-адреса. Эта особенность более важна, чем легкость в настройке. Без IP-адреса это устройство не доступно в сети и является невидимым для окружающего мира. Если такой МЭ недоступен, то, как его атаковать? Атакующие даже не будут знать, что существует МЭ, проверяющий каждый их пакет [1].

1.3.2 Фильтрующие маршрутизаторы

Packet-filtering firewall (Межсетевой экран с фильтрацией пакетов) - межсетевой экран, который является маршрутизатором или компьютером, на котором работает программное обеспечение, сконфигурированное таким образом, чтобы отфильтровывать определенные виды входящих и исходящих пакетов. Фильтрация пакетов осуществляется на основе информации, содержащейся в TCP- и IP-заголовках пакетов (адреса отправителя и получателя, их номера портов и др.).

Особенности:

- Работают на 3 уровне.
- Также известны, как МЭ на основе порта.
- Каждый пакет сравнивается со списками правил (адрес источника/получателя, порт источника/получателя).
- Недорогой, быстрый (производительный в силу простоты), но наименее безопасный.
- Технология 20-летней давности [1].

Пример: список контроля доступа (ACL, Access Control Lists) маршрутизатора.

1.3.3 Шлюз сеансового уровня

Шлюз сеансового уровня (Circuit-level gateway) - межсетевой экран, который исключает прямое взаимодействие между авторизированным клиентом и внешним хостом. Сначала он принимает запрос доверенного клиента на определенные услуги и, после проверки допустимости запрошенного сеанса, устанавливает соединение с внешним хостом. На рисунке 1.8 показана схема функционирования шлюза сеансового уровня [1].

Рисунок 1.8 - Схема функционирования шлюза сеансового уровня

После этого шлюз просто копирует пакеты в обоих направлениях, не осуществляя их фильтрации. На этом уровне появляется возможность использования функции сетевой трансляции адресов (NAT, network address translation). Трансляция внутренних адресов выполняется по отношению ко всем пакетам, следующим из внутренней сети во внешнюю. Для этих пакетов IP-адреса компьютеров - отправителей внутренней сети автоматически преобразуются в один IP-адрес, ассоциируемый с экранирующим межсетевым экраном. В результате все пакеты, исходящие из внутренней сети, оказываются отправленными межсетевым экраном, что исключает прямой контакт между внутренней и внешней сетью. IP-адрес шлюза сеансового уровня становится единственным активным IP-адресом, который попадает во внешнюю сеть.

Особенности:

- Работает на 4 уровне.
- Передает TCP подключения, основываясь на порте.
- Недорогой, но более безопасный, чем фильтр пакетов.
- Обычно требует работы пользователя или программы конфигурации для полноценной работы.

1.3.4 Шлюз прикладного уровня

Шлюз прикладного уровня (Application-level gateways) - межсетевой экран, который исключает прямое взаимодействие между авторизированным клиентом и внешним хостом, фильтруя все входящие и исходящие пакеты на прикладном уровне модели OSI. На рисунке 1.9 показано функционирование шлюза прикладного уровня.

Связанные с приложением программы-посредники перенаправляют через шлюз информацию, генерируемую конкретными сервисами TCP/IP [1].

Возможности:

- идентификация и аутентификация пользователей при попытке установления соединения через межсетевой экран;

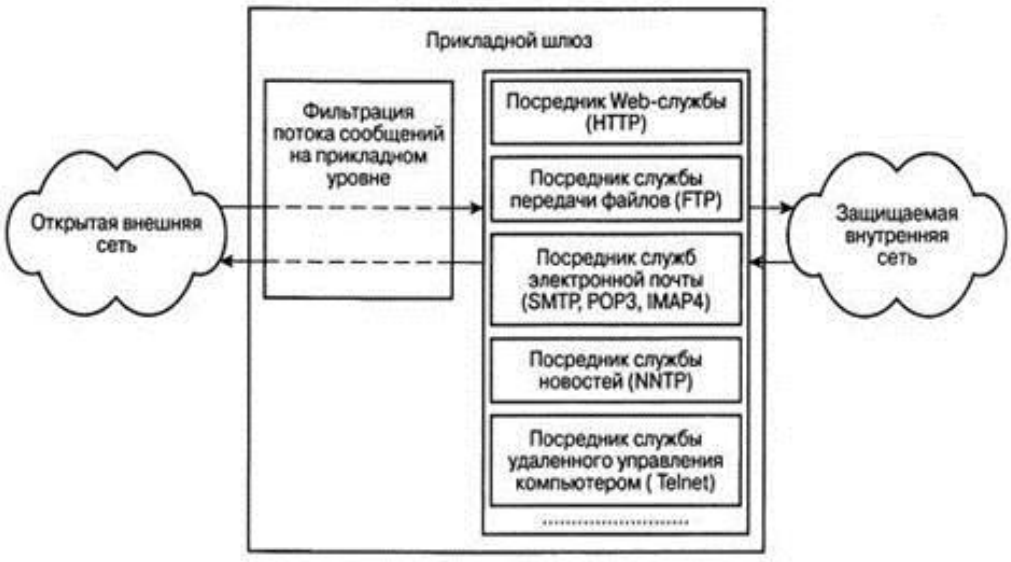

Рисунок 1.9 - Схема функционирования шлюза прикладного уровня

- фильтрация потока сообщений, например, динамический поиск вирусов и прозрачное шифрование информации;
- регистрация событий и реагирование на события;
- кэширование данных, запрашиваемых из внешней сети.

На этом уровне появляется возможность использования функций посредничества (Proxy).

Для каждого обсуживаемого протокола прикладного уровня можно вводить программных посредников - HTTP-посредник, FTP-посредник и т.д. Посредник каждой службы TCP/IP ориентирован на обработку сообщений и выполнение функций защиты, относящихся именно к этой службе. Также, как и шлюз сеансового уровня, прикладной шлюз перехватывает с помощью соответствующих экранирующих агентов входящие и сходящие пакеты, копирует и перенаправляет информацию через шлюз, и функционирует в качестве сервера-посредника, исключая прямые соединения между внутренней и внешней сетью. Однако, посредники, используемые прикладным шлюзом, имеют важные отличия от канальных посредников шлюзов сеансового уровня. Во-первых, посредники прикладного шлюза связаны с конкретными приложениями программными серверами), а во-вторых, они могут фильтровать поток сообщений на прикладном уровне модели МВОС [1].

Особенности:

- работает на 7 уровне;
- специфический для приложений;
- умеренно дорогой и медленный, но более безопасный и допускает регистрацию деятельности пользователей;
- требует работы пользователя или программы конфигурации для полноценной работы.

Пример: Web (http) proxy.

1.3.5 МЭ экспертного уровня

Stateful Inspection Firewall - межсетевой экран экспертного уровня, который проверяет содержимое принимаемых пакетов на трех уровнях модели OSI: сетевом, сеансовом и прикладном. При выполнении этой задачи используются специальные алгоритмы фильтрации пакетов, с помощью которых каждый пакет сравнивается с известным шаблоном авторизированных пакетов.

Особенности:

- фильтрация 3 уровня;
- проверка правильности на 4 уровне;
- осмотр 5 уровня;
- высокие уровни стоимости, защиты и сложности.

Пример: CheckPoint Firewall-1.

Некоторые современные МЭ используют комбинацию вышеперечисленных методов и обеспечивают дополнительные способы защиты, как сетей, так и систем.

1.4 Политика работы МЭ

МЭ функционируют по одному из двух принципов:

- запрещать все, что не разрешено в явной форме;
- разрешать все, что не запрещено в явной форме.

1.5 Схемы подключения МЭ

Схемы подключения МЭ:

- Схема единой защиты локальной сети.
- Схема защищаемой закрытой и не защищаемой открытой подсетями.
- Схема с раздельной защитой закрытой и открытой подсетей [1].

1.5.1 Схема единой защиты локальной сети

Наиболее простым является решение, при котором межсетевой экран просто экранирует локальную сеть от глобальной. При этом WWW-сервер, FTP-сервер, почтовый сервер и другие сервера, оказываются также защищены межсетевым экраном. При этом требуется уделить много внимания на предотвращение проникновения на защищаемые станции локальной сети при помощи средств легкодоступных WWW-серверов. Схема подключения представлена на рисунке 1.10 [1].

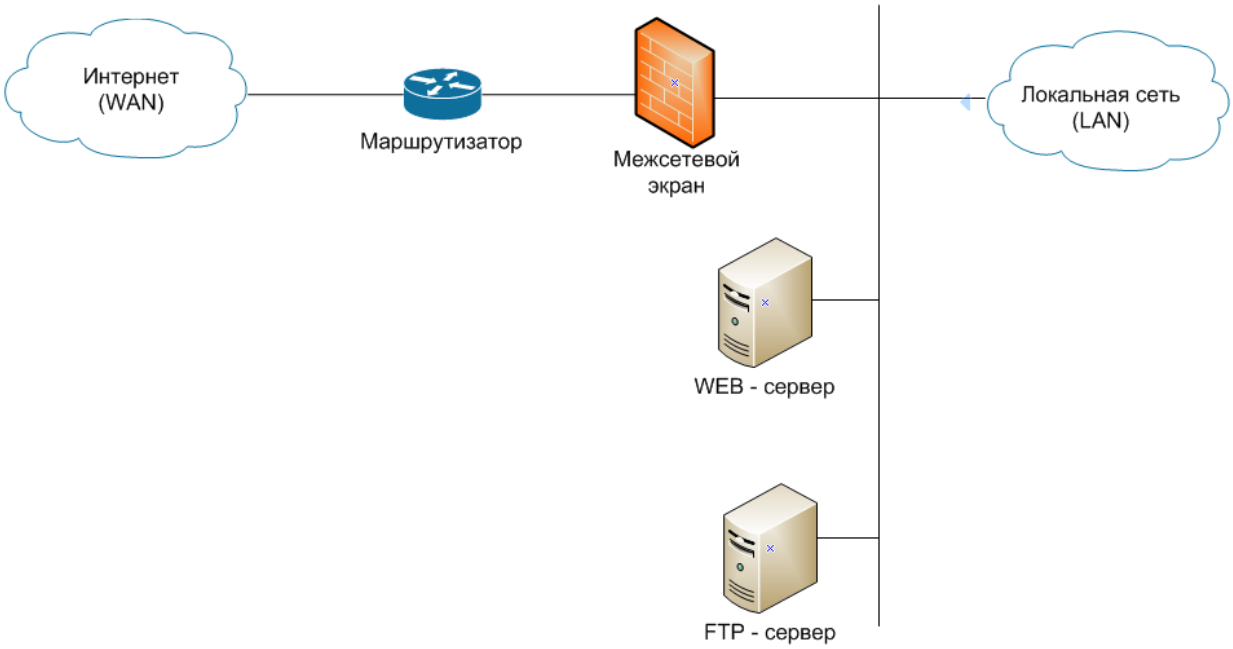

Рисунок 1.10 - Схема единой защиты локальной сети

Основной минус такой схемы состоит в том, что доступ из локальной сети предприятия остается неконтролируемым, так как межсетевой экран фильтрует только трафик, который приходит из глобальной сети (WAN).Поэтому данную схему подключения firewall можно использовать лишь при отсутствии в локальной сети открытых серверов или когда имеющиеся открытые серверы делаются доступными из внешней сети только для ограниченного числа пользователей, которым можно доверять.

1.5.2 Схема защищаемой закрытой и не защищаемой открытой подсетями

Для предотвращения доступа в локальную сеть, используя ресурсы WWW-сервера, рекомендуется общедоступные серверы подключать перед межсетевым экраном. Данный способ обладает более высокой защищенностью локальной сети, но низким уровнем защищенности WWW- и FTP-серверов (Рисунок 1.11).

Данный способ обладает более высокой защищенностью закрытой части локальной сети, но обеспечивает пониженную безопасность открытых серверов, расположенных до межсетевого экрана.

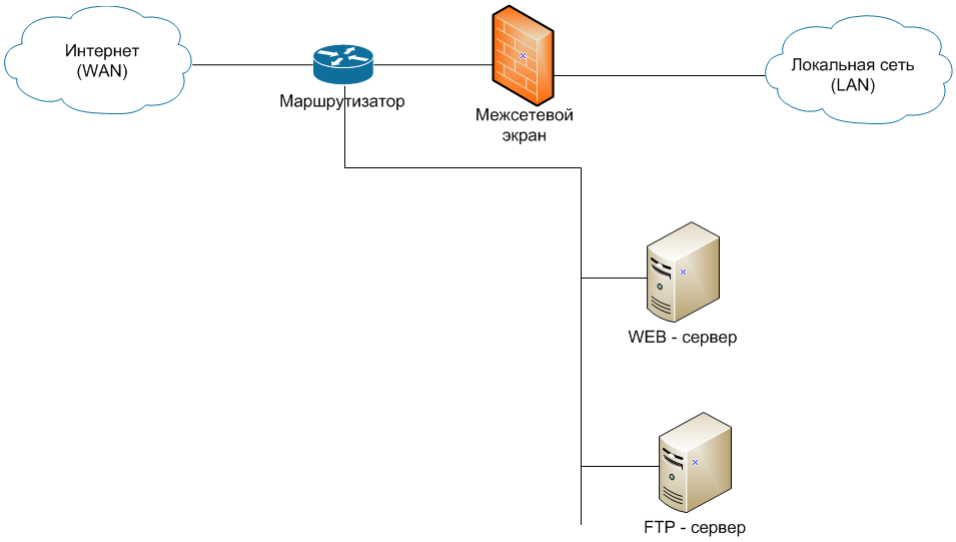

Рисунок 1.11 - Схема защищаемой закрытой и не защищаемой открытой подсетями

1.5.3 Схема с раздельной защитой закрытой и открытой подсетей

Данная схема подключения обладает наивысшей защищенностью по сравнению с рассмотренными выше. Схема основана на применении двух МЭ, защищающих отдельно закрытую и открытую подсети (Рисунок 1.12). Участок сети между МЭ также называется экранированной подсетью или демилитаризованной зоной (DMZ, demilitarized zone) [1].

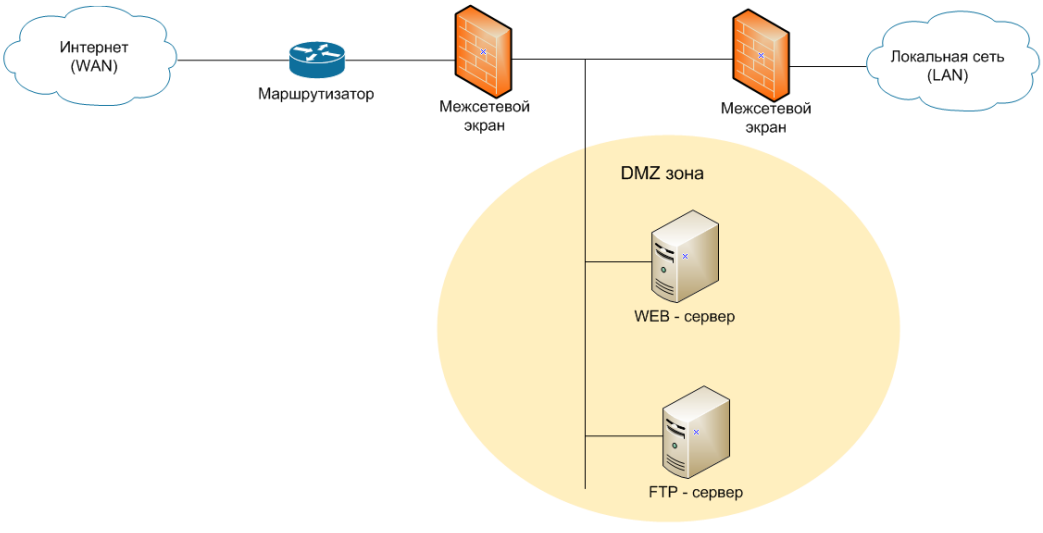

Рисунок 1.12 - Схема с раздельной защитой закрытой и открытой подсетей

Из этих двух схем большую степень безопасности межсетевых взаимодействий обеспечивает схема с двумя МЭ, каждый из которых образует

отдельный эшелон защиты закрытой подсети. Защищаемая открытая подсеть здесь выступает в качестве экранирующей подсети.

Обычно экранирующую подсеть конфигурируют таким образом, чтобы обеспечить доступ к компьютерам подсети как из потенциально враждебной внешней сети, так и из закрытой подсети локальной сети. Однако прямой обмен информационными пакетами между внешней сетью и закрытой подсетью невозможен. При атаке системы с экранирующей подсетью необходимо преодолеть, по крайней мере, две независимые линии защиты, что является весьма сложной задачей. Средства мониторинга состояния межсетевых экранов позволяют практически всегда обнаружить подобную попытку, и администратор системы может своевременно предпринять необходимые действия по предотвращению несанкционированного доступа.

1.6 Основные недостатки контроля доступа в традиционной архитектуре корпоративной сети

Как было рассмотрено выше, в большинстве случаев в корпоративной сети контроль доступа предоставляют межсетевые экраны. Конечно, межсетевые экраны и на сегодняшний день являются главным эшелоном защиты в любой корпоративной сети. Они работают по четко определенным правилам (ACL списки), которые фильтруют весь входящий и исходящий трафик, блокируя при этом весь трафик, который по определению не должен проникнуть за границу данного МЭ, иными словами, во внутреннюю корпоративную сеть. На сегодняшний день у МЭ нет возможности гибко управлять проводным, беспроводным и VPN доступом как единым целом, что позволило, например, используя беспроводную сеть, дать возможность своим сотрудникам приносить свои личные устройства (КПК, планшеты др.) и не быть привязанным к своему рабочему месту; так же дать возможность гостям и контрактникам компании подключаться к определенным ресурсам компании, при этом централизованно контролировать все подключения и видеть любое устройство, с которого происходит подключение, и кто с него подключается, используя соответствующие политики доступа.

Именно поэтому компания Cisco в рамках архитектуры «Сети без границ» разработала новое решение Cisco TrustSec, которое позволит все вышеперечисленные недоставки устранить, при этом значительно облегчить работу IT- отдела и значительно увеличить эффективность всей компании.

Так же, по прогнозам многих экспертов, сейчас межсетевые экраны перестают быть главным звеном защиты корпоративной сети, и на первое место перебираются управляемые коммутаторы, в особенности новейшие линейки коммутаторов Cisco Catalystсерии 3K,4K,5K,5K,7K (Cisco Nexus), которые вместе с мозгом данного решения - Cisco ISE, смогут выполнить все вышеперечисленные требования и обеспечить безопасность всего предприятия на высшем уровне.

2 Cisco TrustSec в рамках архитектуры «Сети без границ»

2.1 Что такое Cisco TrustSec?

Решение Cisco TrustSec является платформой на основе политик, которая обеспечивает интеграцию сервисов оценки состояния, профилирования и гостевых функций для принятия решений по управлению доступом с учетом контекста. Решение TrustSec уникально тем, что строится на основе имеющейся инфраструктуры с учетом идентификационных данных путем реализации этих политик с возможностью дальнейшего масштабирования. Данное решение позволяет выполнить следующее [4]:

- **Способствует повышению продуктивности бизнеса**. Оно дает растущему числу мобильных сотрудников и высококвалифицированных специалистов доступ к нужным ресурсам с гарантированной защитой.
- **Обеспечивает безопасность и устранение рисков, связанных с несоответствием нормативным требованиям**. Решение дает полное представление о том, кто и с помощью каких устройств подключается к сети, а также позволяет контролировать, к каким ресурсам пользователь имеет доступ и что он может делать.
- **Повышает эффективность работы ИТ-персонала**. Снижает нагрузку ИТ-служб за счет централизованных сервисов безопасности, интегрированного управления политиками и масштабируемых механизмов реализации политик

Полная прозрачность:

- **Организация сети с контролем идентификационных данных**. Cisco TrustSec поддерживает методы гибкой аутентификации (FlexAuth), в том числе IEEE 802.1X, web- аутентификацию (WebAuth) и обход аутентификации по MAC-адресам (MAB), используя сеть для идентификации пользователей и устройств.
- **Оптимизированное профилирование устройств**. Автоматически выполняется идентификация и классификация устройств путем сбора данных об оконечных устройствах с помощью сетевых сенсоров устройств в коммутационной инфраструктуре Cisco Catalyst. Результаты классификации дополнительно уточняются с использованием технологии направленного активного сканирования оконечных устройств на основе политик.
- **Гостевой доступ и управление жизненным циклом**. Приглашенные сотрудниками гости получают ограниченный доступ к определенным ресурсам (Интернет, принтеры и т. д.) через персонализированный web-портал. Доступ к внутренней сети блокируется, а действия пользователя отслеживаются и фиксируются для отчета.

Абсолютный контроль:

- Централизованная политика и ее реализация. Платформа централизованных политик поддерживает формирование скоординированных политик и единообразную реализацию политик на основе контекста в масштабе

всей корпоративной инфраструктуры, включая центральный офис, филиалы и удаленных пользователей. Устройства, не соответствующие требованиям, могут быть подвергнуты карантину или восстановлены до требуемого состояния, либо им может быть предоставлен ограниченный доступ.

- **Независимое от топологии управление доступом**. Новая революционная технология доступа для групп безопасности (Security Group Access, SGA), позволяет клиентам трансформировать свои бизнес-цели в решения по управлению доступом к сети. Технология SGA объединяет управление доступом на основе ролей с масштабируемыми, согласованными механизмами авторизации и реализации политик, которые не зависят от топологии сети.

Таким образом, Cisco TrustSec можно рассматривать как системный подход к контролю доступа, который объединяет в себе следующие компоненты:

- IEEE 802.1X (Dot1x);
- технологии профилирования;
- гостевые сервисы;
- метки безопасности (secure group tag);
- канальное шифрование macsec (802.1ae).

2.2 Задачи управления доступом Cisco TrustSec

Новое решение Cisco TrustSec позволяет решить следующие задачи управления доступом (Рисунок 2.1):

- кто подключился (сотрудник, контрактник, гость и т.д.);
- что за устройство подключилось (рабочая станция, ноутбук, планшет и т.д.);
- где произошло подключение (центральный офис, филиал, вне периметра корпоративной сети и т.д.);
- куда произошло подключение (hr, itи т.д.).

Рисунок 2.1- Задачи управления доступом

2.3 Архитектура Cisco TrustSec

Cisco TrustSec обеспечивает следующие сервисы для сетевого подключения (Рисунок 2.2):

- идентификация (ответ на вопрос «кто и что включается в сеть»);
- политики доступа или авторизация (ответ на вопрос «куда мы имеем доступ»);
- динамический контекст (ответ на вопрос «как устройство включается в сеть»).

Рисунок 2.2- Архитектура Cisco TrustSec

Третий подпункт «динамический контекст» как раз и отличает архитектуру Cisco TrustSec от политик доступа обычных компаний (когда имеется логин, пароль и сертификат и сотрудник получает доступ в сеть). Но насколько логин и пароль является атрибутом безопасности? Ведь при таком случае не видно, с какого устройства идет подключение к сети, так же невозможно оценить, насколько безопасно данное устройство (установлены ли необходимые компоненты защиты на данном устройстве), как подключилось данное устройство (проводное подключение, беспроводное подключение, VPN подключение) (Рисунок 2.3).

Рисунок 2.3 - Динамический контекст

Таким образом, исходя из вышесказанного, архитектура Cisco TrustSec базируется на трех ключевых компонентах:

- **Проверенная сетевая инфраструктура**. После того как первое устройство (которое еще называют корневым) проходит аутентификацию на сервере аутентификации (Cisco ACS или Cisco ISE), создается Cisco TrustSec домен. Каждое следующее добавляемое сетевое устройство в домен проходит аутентификацию с пирами, уже находящимися в домене. Такое новое добавляемое устройство идентифицируется сервером аутентификации и ему назначается номер группы безопасности в соответствии с политиками, настроенным на сервере.

- **Безопасный контроль доступа на основе групп (Security Group Access, SGA)**. Политики доступа внутри Cisco TrustSec домена не зависят от топологии сети, а базируются на так называемых ролях (о чем свидетельствует номер SG) устройства-источника и устройства-назначения. Все пакеты, проходящие между двумя устройствами в сети, тэгируются номером SG источника.

- **Защищенные соединения**. На устройствах с поддержкой аппаратного шифрования все пакеты на линках могут быть зашифрованы.

Ниже, на рисунке 2.4, представлен пример Cisco TrustSec домена. В этом примере некоторые сетевые устройства и конечные компьютеры находятся внутри домена, а некоторые нет.

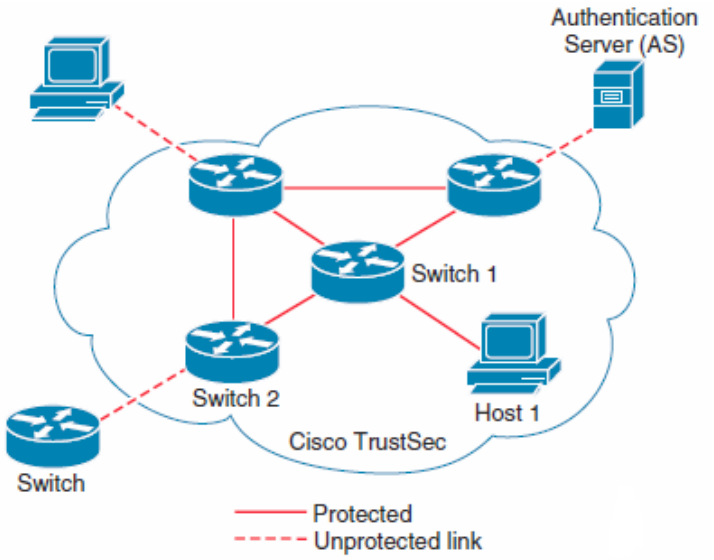

Рисунок 2.4 - Домен Cisco TrustSec

Каждый участник в процессе аутентификации CTS берет на себя одну из следующих ролей:

- **Саппликант (Supplicant, проситель)**. Это неаутентифицированное устройство, которое подсоединяется к легитимному устройству внутри безопасного домена, и пытается в стать членом этого домена (на рисунке 2.4 таковым является устройство, находящееся вне домена Cisco TrustSec).

- **Сервер аутентификации**. Это сервер, который проверяется валидность сапликанта и определяет те политики, которые будут применены к просителю.

- **Аутентификатор**. Это сетевое устройство, которое уже прошло процесс аутентификации на сервере и в данный момент времени является частью CTS домена и может провести аутентификацию нового пира, задействуя для этого сервер аутентификации (на рисунке 2.4 таковым является устройство, находящееся внутри домена Cisco TrustSec, например, Switch2 или Switch1).

Когда связь между сапликантом и аутентификатором переходит в состояние UP, обычно происходит следующий набор событий:

1. Аутентификация. Сапликант проходит проверку подлинности на сервере аутентификации. Возможно установление взаимной аутентификации.

2. Авторизация. Основываясь на информации от сапликанта, сервер аутентификации выдает политики авторизации - например, назначение группы безопасности (SGT) или ACL.

3. Установление ассоциаций безопасности протокола (Security Association Protocol, SAP). Если обе стороны линка поддерживают шифрование, то сапликант и аутентификатор договариваются о необходимых параметрах для установки ассоциаций безопасности (Security Associations, SA).

После того, как все три шага, описанных выше, выполнены, аутентификатор изменяет состояние своего линка с неавторизованного на авторизованное и сапликант становится частью домена CTS.

2.4 Компоненты Cisco TrustSec

В традиционном подходе реализация политик выглядит как показано на рисунке 2.5.

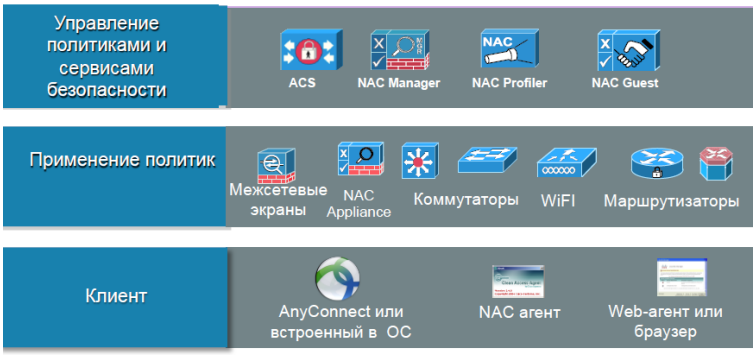

Рисунок 2.5 - Традиционный подход контроля доступа

Как видно из рисунка 2.5, для управления политиками требовалось многообразие сервисов, таких как ACS (Access Control Server) для централизованной аутентификации, авторизации и журналирования, NAC Guest

для работы с гостевым доступом, NAC Profiler, служащий для распознавания конечных устройств и т.д.

В банковской системе реализация политик доступа представляется следующим образом (Рисунок 2.6).

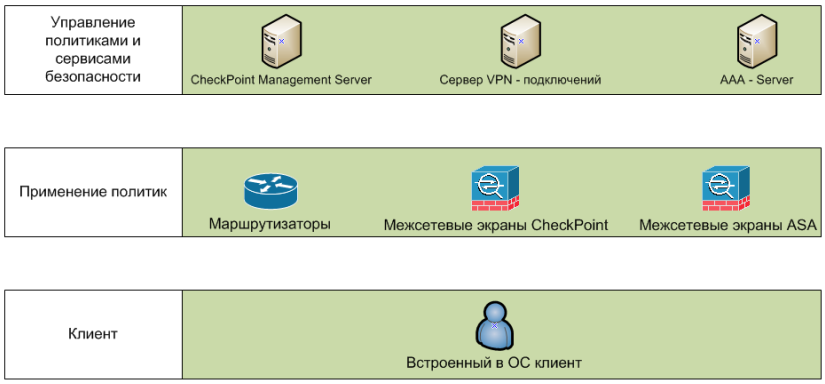

Рисунок 2.6 - Контроль доступа в банковской системе

Так же можно заметить, что приходится разворачивать немалое количество серверов безопасности, что бы стараться обезопасить свою корпоративную сеть, что тоже не очень удобно (это ещё без учета гостевого доступа, для которого необходимо развернуть дополнительный сервис по контролю гостевого доступа).

Cisco TrustSec предлагает более оптимально решение, которое значительно увеличит работу и эффективность IT- отдела.

Реализация политик Cisco TrustSec будет основываться на использовании следующих компонент, которые представляют собой 3 основных уровня (Рисунок 2.7).

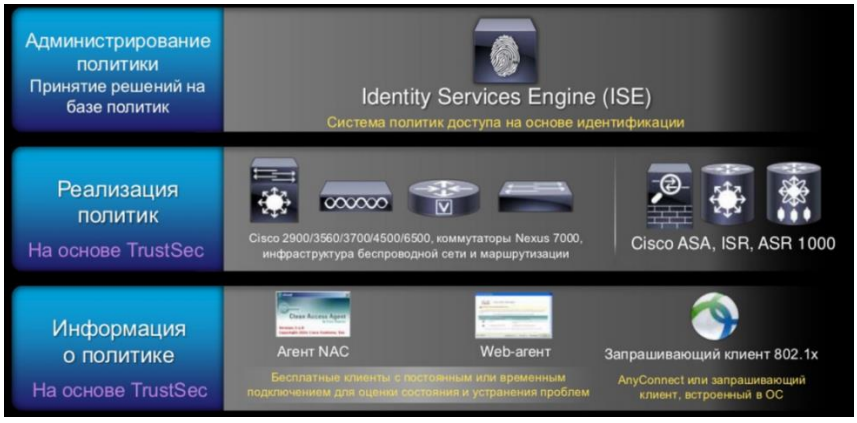

Рисунок 2.7 - Контроль доступа TrustSec

Как видно из рисунка 2.7, основным «мозгом» данной архитектуры является Cisco ISE (Identity Services Engine) - сервис, в котором и определяется все политик доступа и централизованно внедряются, т.е. данный сервис и дает

ответ на вопрос: кто включается в сеть, с какого устройства произошло подключение, как произошло подключение. Применение данных политик осуществляется на сетевых устройствах, таких как коммутаторы, контроллеры беспроводной сети, маршрутизаторы и межсетевые экраны. В роли клиента выступает любая станция, в которой есть хотя бы один из перечисленных на рисунке 2.7 сервисов.

Таким образом, в отличие от традиционного контроля доступа, в котором ядром управления и внедрения политик является множество сервисов, Cisco ISE образует платформу централизованных политик на основе идентификации для принятия решений по управлению доступом с учетом контекста в масштабе всей инфраструктуры проводной, беспроводной и VPN-сети (Рисунок 2.8). Cisco ISE объединяет функции аутентификации, авторизации и учета (AAA), оценки состояния, профилирования и управления гостевым доступом в рамках единого унифицированного устройства, обеспечивая единую точку управления политиками, мониторинга и диагностики (Рисунок 2.9).

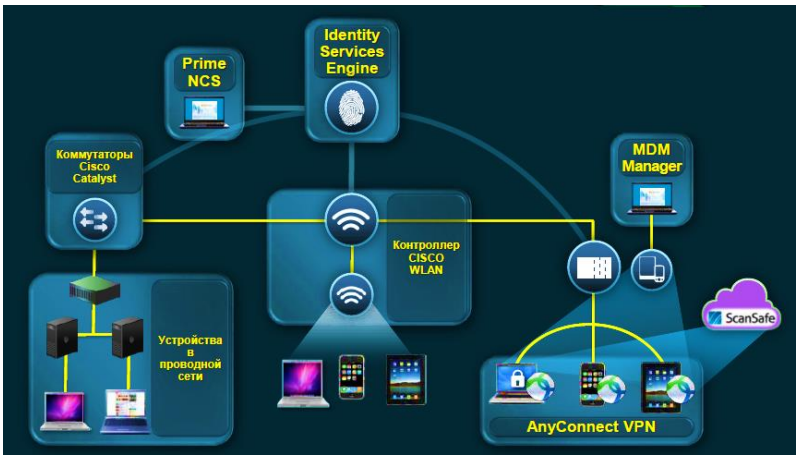

Рисунок 2.8 - Централизованная политика по управлению доступом

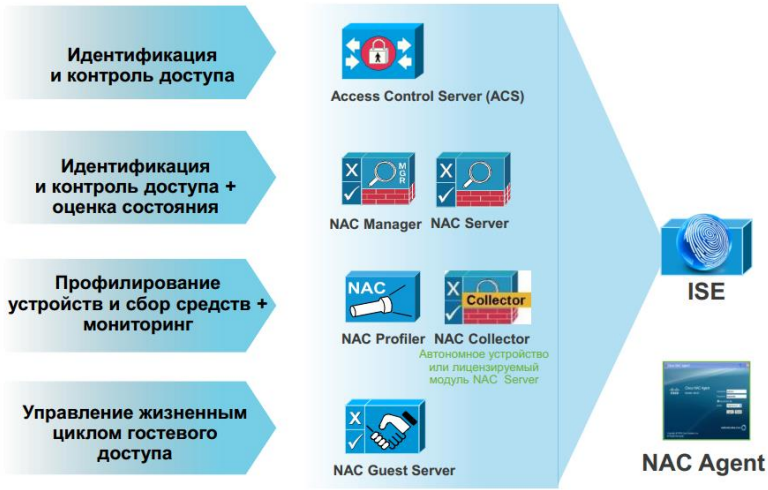

Рисунок 2.9 - Единая платформа для реализации политик

2.5 Инфраструктура Cisco TrustSec

Инфраструктура Cisco TrustSec в общем виде представлена на рисунке 2.10.

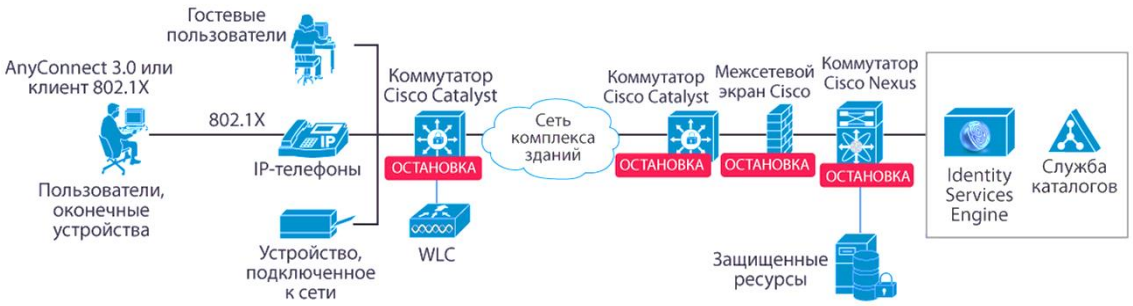

Рисунок 2.10 - Инфраструктура Cisco TrustSec

Как видно из рисунка 2.10, доступ во внутреннюю сеть предприятия будет реализовываться на коммутаторах Cisco Catalyst версии 3Кили 4K (так же доступ можно реализовать на маршрутизатор нового поколения Cisco ISR G2), так же на контроллерах беспроводной сети, доступ к внутренним защищаемым ресурсам обеспечивают коммутаторы ядра Cisco Nexuscерий 7Кили 5K. Центральным «ядром» является Cisco ISE, который, основываясь на встроенной базе данных (либо используя службу каталогов или Active Directory), будет выдавать соответствующую политику доступа на сетевое устройство.

2.6 Сетевая аутентификация и идентификация Cisco TrustSec

Аутентификация позволяет идентифицировать конечные устройства (или же пользователей), которые подключаются к сети. В процессе аутентификации система проверяет некоторые атрибуты устройства (например, логин и пароль или сертификат) и узнает, к какой группе относится тот или иной девайс. Cisco TrustSec предоставляет три метода аутентификации:

1 аутентификация IEEE802.1X для пользователей и устройств;

2 обход аутентификации по MAC-адресам (MAB), т.е. устройства, не поддерживающие (или без) 802.1X могут быть аутентифицированы по MAC (физическому адресу) устройства;

3 web-аутентификация (гости, сотрудники с чужого компьютера, а так же устройства, не поддерживающие 802.1X).

2.6.1 Настройка Flexible Authentication на порту коммутатора

Благодаря новой линейке коммутаторов Cisco, можно настраивать так называемый Flexible Authentication (гибкая аутентификация), т.е. на любом порту коммутатора можно выставлять вышеперечисленные методы

аутентификации, а так же устанавливать их порядок и приоритет, а так же действие в случае неудачи (Рисунок 2.11) [7].

Рисунок 2.11 - Работа Flexible Authentication

802.1X- протокол, который работает на канальном уровне и определяет контроль доступа к сети на основе принадлежности к порту, поэтому, согласно данному протоколу, доступ к сети получают только те пользователи, которые прошли аутентификацию, в противном случае, доступ с соответствующего порта будет запрещен. Пример работы протокола 802.1X показан на рисунке 2.12 [13].

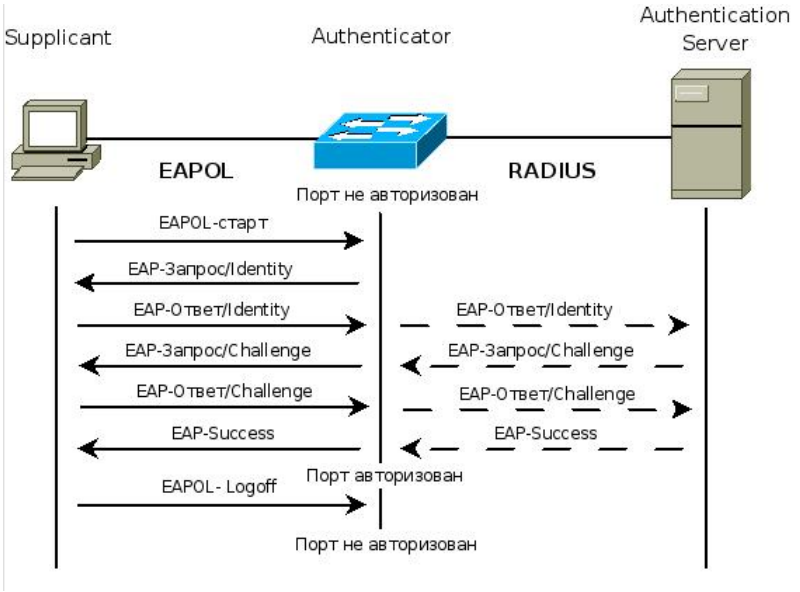

Рисунок 2.12 - Протокол 802.1X в действии

1 Клиент отправляет сообщение EAPOL-старт аутентификатору.

2 Аутентификатор отправляет клиенту EAP-Запрос и клиент отвечает EAP-ответом.

3 Аутентификатор инкапсулирует ответ в формат RADIUS и пересылает ответ серверу аутентификации.

4 Сервер аутентификации отправляет EAP-MD5 Challenge клиенту, а клиент присылает ответ (передает сообщения аутентификатор соответствующим образом инкапсулируя и деинкапсулируя фреймы).

5 Сервер аутентификации подтверждает подлинность клиента и сообщает аутентификатору о необходимости разрешить доступ клиента к сети.

6 Аутентификатор авторизует порт и клиент получает доступ к сети.

Теперь рассмотрим, как можно настроить все 3 метода аутентификации на порту коммутатора (или маршрутизатора), используя Flexible Authentication, как показано на рисунке 2.11:

Для того чтобы настроить 802.1X аутентификацию,MAB-аутентификацию и Web-аутентификацию, необходимо выполнить следующее:

1 Настроить параметры RADIUS - сервера (Рисунок 2.13).

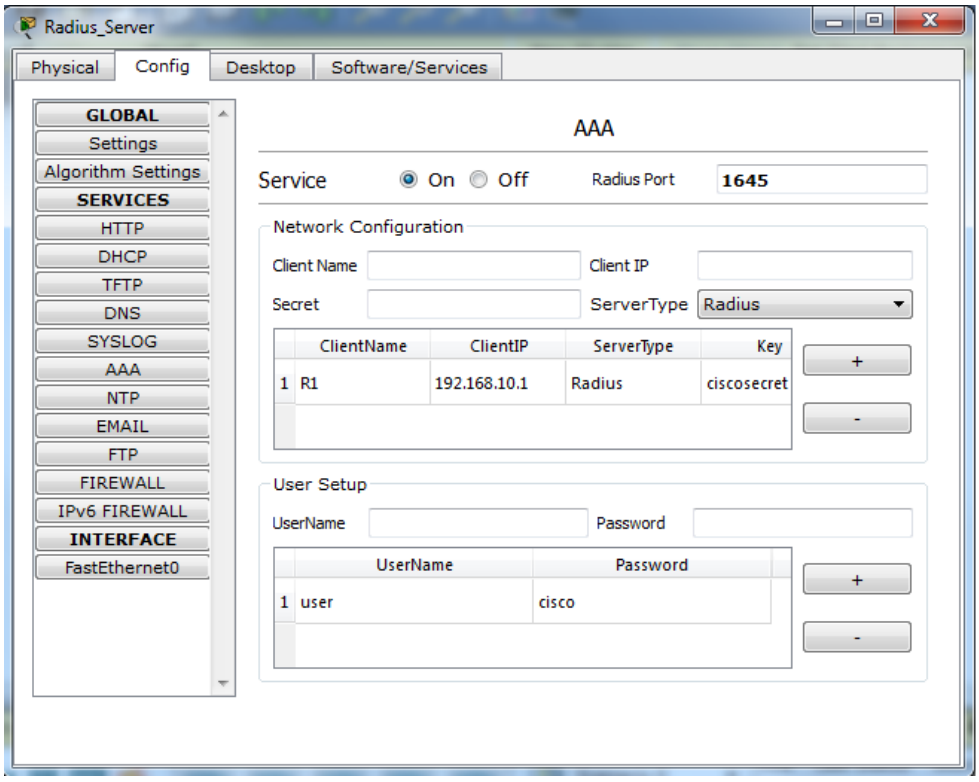

Рисунок 2.13 - Настройка RADIUS - сервера

Как видно из рисунка 2.13, в роли аутентификатора выступает маршрутизатор R1 с заданным ip-адресом и паролем. В роли аутентификатора так же может выступать коммутатор уровня 3, т.е. коммутатор, который умеет маршрутизировать трафик (работает на 3 - м уровне модели OSI):

2 Теперь нужно настроить Flexible Authenticationна маршрутизаторе или коммутаторе L3 (таблица 2.1):

Таблица 2.1 - Настройка 3 методов аутентификации на порту коммутатора (или маршрутизатора), или настройка Flexible Authentication.

Команда	Цель
Шаг 1: configure terminal **Пример:** switch# configure terminal switch(config)#	Вход в глобальный режим конфигурации
Шаг 2: ip radius source-interface *interface* **Пример:** ip radius source-interface Loopback0	Указание интерфейса коммутатора, адрес которого будет использоваться как адрес отправителя в сообщениях RADIUS-серверу:
Шаг3: **aaa new-model** **Пример:** switch(config)#aaa new-model	Включение AAA
Шаг4: **aaa authentication dot1x <default|listname> method1 [method2 ...]** **aaa authentication dot1x default group**group-name **aaa authorization cts default group** group-name **Пример:** switch(config)# aaa authentication dot1x default group Rad1 switch(config)# aaa authorization cts default group Rad1	Определяет группы RADIUS - сервера, используемого для аутентификации по технологии 802.1X (авторизации по технологии TrustSec)
Шаг 5: switch(config)#dot1x system-auth-control	Включение аутентификации 802.1X на коммутаторе
Шаг 6: **interface**[FastEthernet, GigabitEthernet, Loopback,…]<0-n> **Пример:** switch(config)#interface GigabitEthernet2/1 switch(config - if)#	Перейти в режим конфигурирования интерфейса
Шаг 7: authentication port-control auto **Пример:** switch(config-if)# authentication port-control auto	Включение 802.1X наинтерфейсе:
Шаг 8: show authentication interface gigabitEthernet 2/1 **Пример:** switch# show authentication interface gigabitEthernet 2/1 **Client list:** Interface MAC Address Domain Status Gi2/1 000c.293a.048e DATA Authz Success **Available methods list:** Handle Priority Name 3 0 **dot1x** **Runnable methods list:** Handle Priority Name	(Опционально). Просмотреть конфигурацию

Окончание таблицы 2.1

Команда	Цель
3 1 **dot1x**	
Шаг 9: switch(config)# interface GigabitEthernet2/1 switch(config-if)# authentication port-control auto switch(config-if)# mab	Настройка MABна том же порту (если клиент не поддерживает 802.1Xпротокол или для аутентификации таких устройств как принтеры, сканеры, IP-и т.д.)
Шаг 10: switch# show authentication interface gigabitEthernet 2/1 **Client list:** Interface MAC Address Domain Status Gi2/1 000c.293a.048e DATAAuthz Success **Available methods list:** Handle Priority Name 2 1 **mab** **Runnable methods list:** Handle Priority Name 2 0 **mab**	(Опционально). Просмотреть конфигурацию
Шаг 11: switch(config)# ip http server switch(config)# ip access-list extended POLICY switch(config-ext-nacl)# permit udp any anyeqbootps switch(config-ext-nacl)# permit udp any anyeq domain switch(config)# ip admission name HTTP proxy http switch(config)# fallback profile FALLBACK_PROFILE switch(config-fallback-profile)# ip access-group POLICY in switch(config-fallback-profile)# ip admission HTTP switch(config)# interface GigabitEthernet2/1 switch(config-if)# authentication port-control auto switch(config-if)# authentication fallback FALLBACK_PROFILE6500(config-if)#ip access-group POLICY in	Настройка Web-аутентификации для случая, когда по первым двум методам пользователь не был аутентифицирован, и он перенаправляется на гостевой портал (GuestPortal)
Шаг 12: switch# show authentication interface gigabitEthernet 2/1 **Client list:** Interface MAC Address Domain Status Gi2/1 000c.293a.048e DATA Authz Success **Available methods list:** Handle Priority Name 1 2 **webauth** Runnable methods list: Handle Priority Name 1 0 **webauth**	(Опционально). Просмотреть конфигурацию
Шаг 13: switch(config)# interface gigabitEthernet 2/1 switch(config-if)# authentication order mab dot1x webauth	Настройка порядка методов аутентификации на порту

Исходя из таблицы 2.1, благодаря гибкой аутентификации (Flexible Authentication), можно настроить все три метода аутентификации на любом порту коммутатора, при этом порядок аутентификации можно выбирать любой, а так же выставлять приоритеты каждого метода, что значительно упрощает контроль доступа.

2.7 Авторизация и применение политик в сети

После окончания процесса аутентификации, саппликант и аутентификатор получают политики доступа от сервера аутентификации, т.е. начинается процесс авторизации. Технология TrustSec поддерживает различные механизмы авторизации для обеспечения политики доступа в сеть. К трем основным механизмам относится:

1 Назначение или присвоениеVLAN - Ingress
2 Присвоение dACL (downloadable ACL) -Ingress
3 Использование Security Group ACL (SGACL) - Egress

Слова Ingress и Egressозначают, где будет применяться данная политика - на входе или на выходе (Рисунок 2.14).

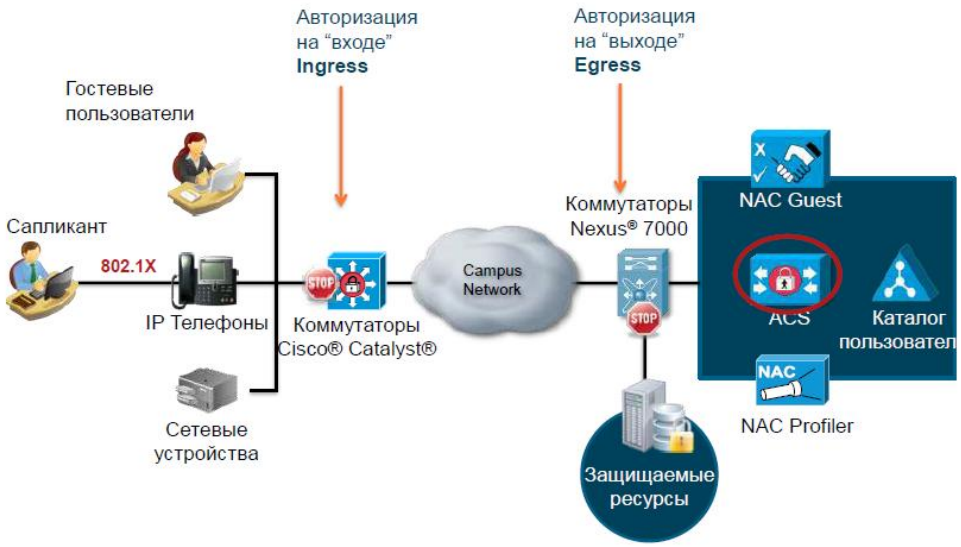

Рисунок 2.14 - CTS:Авторизация и точки применения политик в сети

2.7.1 Авторизация на основе VLAN и dACL

Технология CTS позволяет использовать новый метод авторизации на основе групп безопасности (Security Group). Давайте сравним данный метод авторизации с теми, которые были перечислены в пункте 1 и 2 (VLAN и dACL), и найдем основные недостатки традиционного метода контроля доступа (Рисунок 2.15).

Метод сегментации	Точка применения	Преимущества	Недостатки
VLANS	Вход	• Не требует управления ACL на порту коммутатора • Предпочтельный способ изоляция трафика на всем пути	• Обычно требует изменения IP-адресов • Требует распространения общих сетей VLAN по всей сети доступа. • VLANs требуют разворачивания дополнительных механизмов применения политик
dACLs	Вход	• Не требуется изменения IP • Не требуется распространения общих VLANs в сети доступа и их управление • Обеспечивает контроль доступа прямо на порту коммутатора, а не на отдельном устройстве	• Ограничение ресурсов коммутатора по количеству записей в ACL.
Secure Group Access	Выход	• Упрощает управление ACL • Уменьшает размер политики • Разделяет политику и IP-адресацию.	• Пока нет универсальной поддержки SGA на всех Cisco-платформах

Рисунок 2.15 - Методы сегментации сети: преимущества и недостатки

Как видно из рисунка 2.15, основным недостатком VLAN является дополнительный контроль, т.е. так же нужно будет ограничивать какой - либо трафик; при появлении новой подсети необходимо создавать новый VLAN, что значительно усложняет эксплуатацию всей корпоративной сети предприятия.

Вторым методом является списки контроля доступа. Как видно из рисунка 2.15, данный метод имеет меньше недостатков по сравнению с использование VLAN, т.к. ACL применяется прямо на порту коммутатора, а так же не требуется изменения IP-адреса. Т.е. здесь, наверное, главным недостатком является лимит ресурсов по количеству записей в ACL, а так же, при изменении адреса получателя необходимо отразить данное изменение во всех ACE, что так же приведет к переполнению лимита аппаратных ресурсов коммутатора, особенно, если на предприятии более 1000 рабочих станций.

В рассматриваемой нами банковской системе используется комбинированные методы авторизации (Рисунок 2.16), т.е. вся сеть поделена на сегменты (VLAN), так же для некоторых VLANна портах коммутатора применяются списки контроля доступа (ACL), поэтому данный метод защиты в данной системе является надежным, хотя, как уже говорилось выше, на данном предприятии около 1000 рабочих станций, и списки контроля доступа переваливают за 1000 строк, и как следствие, весь контроль доступа может потребовать детального редизайна всей сети, а это является очень трудоемким и затратным процессом.

Рисунок 2.16 - Контроль доступа на входе

2.7.2 Авторизация на основе Групп Безопасности

Технология TrsutSec предлагает абсолютно новый метод контроля доступа, основанный на использовании Групп Безопасности (Security Group). Группа Безопасности - это группа пользователей, конечных сетевых устройств, которые разделяют одинаковые политики доступа в сетевую инфраструктуру. Группы определяются администратором на сервере аутентификации. CTS назначает каждой группе уникальный (в пределах домена) 16-ти битный номер. После того, как устройство однажды было аутентифицировано, все пакеты от данного устройства помечаются с помощью SGT. Пакет переносит этот тэг через всю защищенную сеть внутри CTS заголовка. Формально, SGT - просто метка, которая определяет уровень доступа устройства-источника.

Поскольку SGT содержит в себе номер группы безопасности источника, то такой тэг часто называют SGT источника. Целевое устройство (устройство назначения пакета, destination device) также имеет свою метку, которую называют тэгом группы назначения (Destination Group Tag, DTG).Схема работы данного метода изображена на рисунке 2.17.

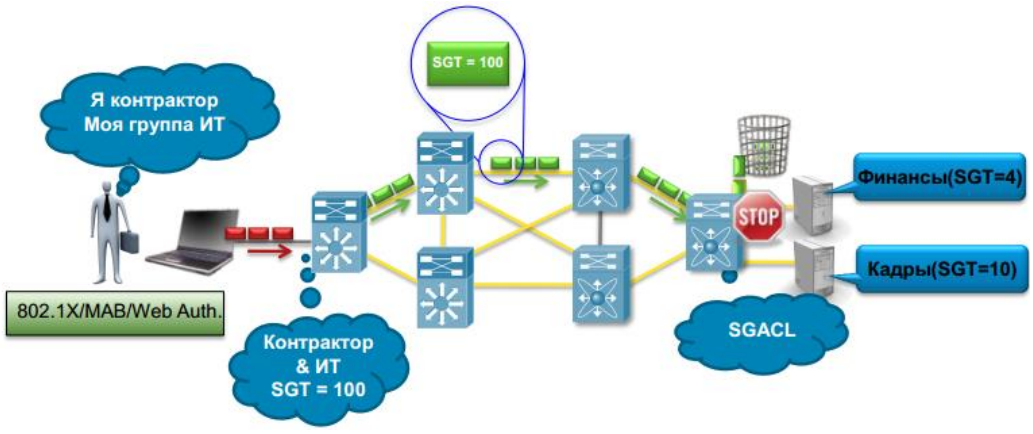

Рисунок 2.17 - Контроль доступа на основе Групп Безопасности

Как видно из рисунка 2.17, по сравнению с первыми двумя методами, где точка применения приходилась на вход, здесь точка применения политики приходится на выход. В отличие от VLAN и ACL которые привязываются к IP-адресу, в данном методе каждой роли присваивается уникальная 16 - битная метка.

Рассмотрим пример контроля доступа в нашей банковской системе (Рисунок 2.18).

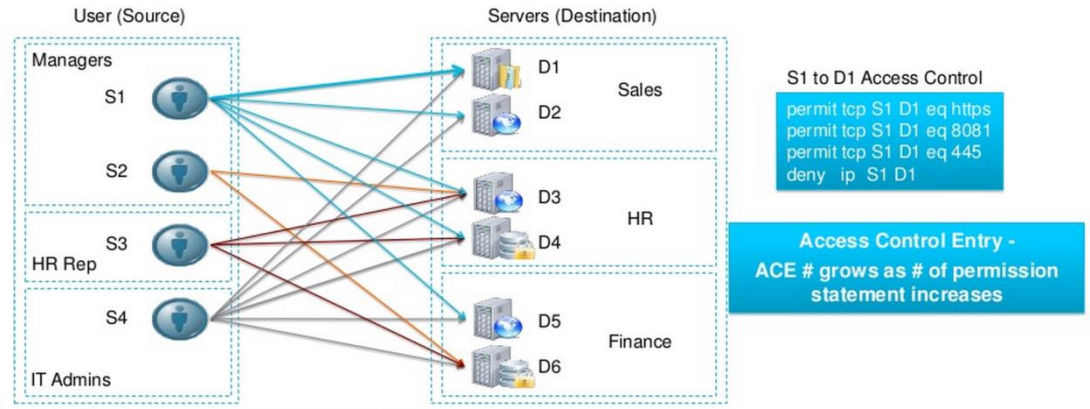

Рисунок 2.18 - Традиционный контроль доступа по ACL

Как видно из рисунка 2.18, чтобы контролировать трафик из департамента менеджеров, уже необходимо написать громоздкий список ACL, а если ещё и писать с фильтрацией по источнику (S1, S2, S3, S4), то данный список вырастет в десятки раз. Теперь рассмотрим, как данная схема будет выглядеть с использованием меток безопасности (Рисунок 2.19).

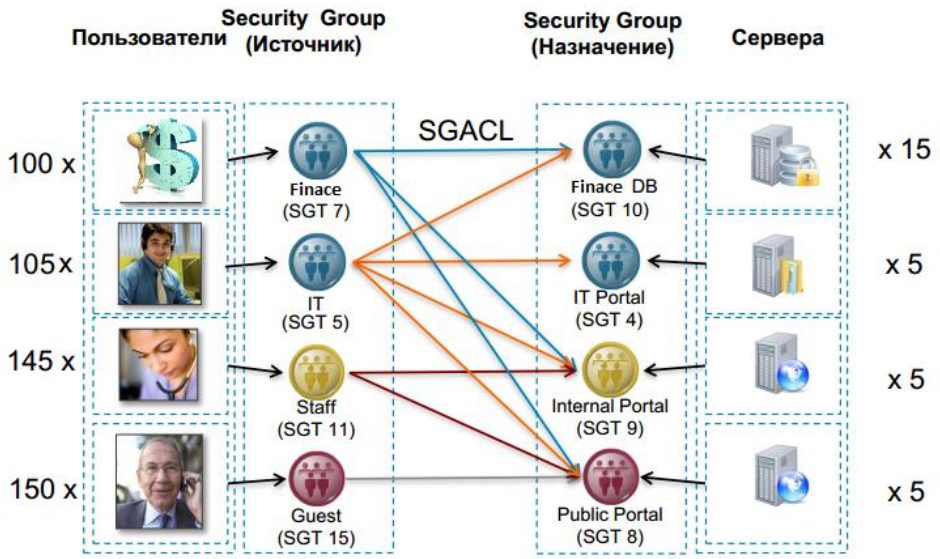

Рисунок 2.19 - Контроль доступа на основе меток безопасности

В применяемой технологии строится так называемая «матрица политик», которая более наглядно помогает представить контроль доступа (Рисунок 2.20).

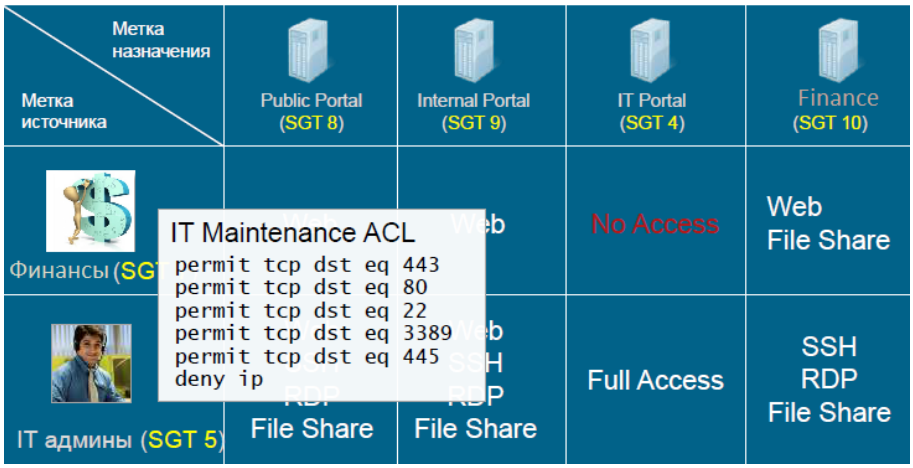

Рисунок 2.20 - Матрица политик SGACL

Элементарными математическими расчетами можно определить эффективность SGACL в реальных условиях. Рассчитаем эффективность SGACL для нашей банковской системы (Рисунок 2.21). Для примера будем считать, что 400 пользователей получают доступ к 30 сетевым ресурсам с 4 типами полномочий для каждого ресурса.

Рисунок 2.21 - Эффективность SGACL

Т.е. из рисунка 2.21 наглядно видно, как данный метод значительно сокращает количество ACE, что значительно экономит аппаратные и вычислительные ресурсы коммутатора или маршрутизатора. Так выглядит настройка матрицы разрешений в более развернутом виде (Рисунок 2.22).

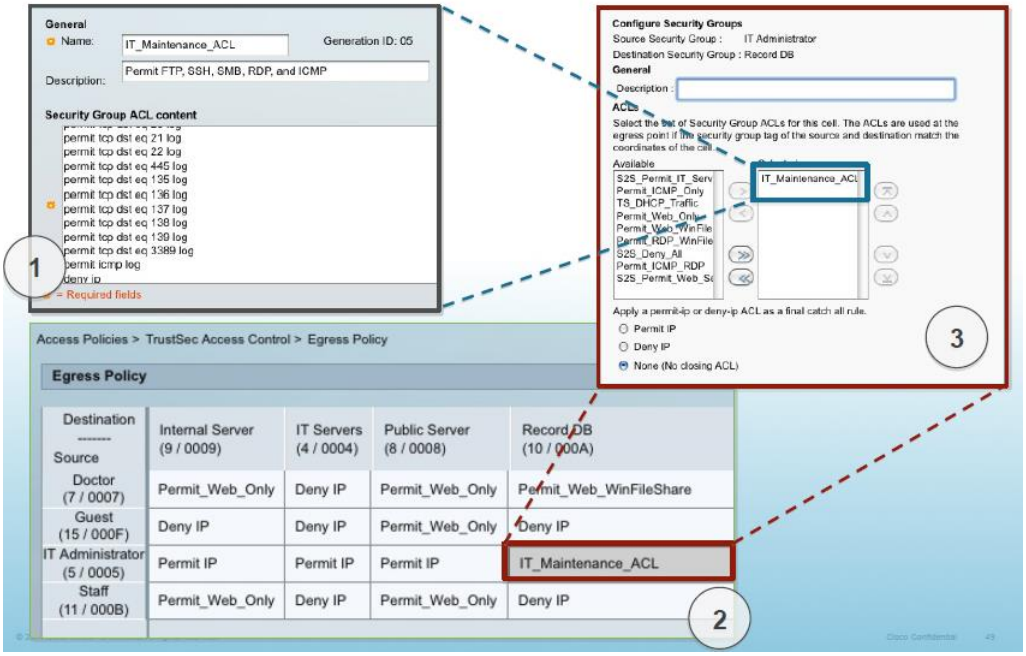

Рисунок 2.22 - Настройка матрицы SGACL

Как видно из рисунка 2.22, каждая ячейка такой матрицы содержит специфичный ACL, который определяет взаимодействие между устройством-источником и целевым устройством.

2.8 Профилирование и оценка состояния устройств

Профилирование так же является одной из инноваций технологии Cisco TrustSec, которое и отвечает на вопросы «что» включается в мою сеть и «как» включается в мою сеть. В базе данных Cisco ISEсодержатся предопределенные шаблоны устройств для различных оконечных девайсов, таких как IP-телефоны, принтеры, IP-камеры, смартфоны и планшеты. Администраторы могут создавать собственные шаблоны устройств. Их можно использовать для автоматического обнаружения, классификации и связывания определенных администраторами идентификационных данных при подключении оконечных устройств к сети. Кроме того, администраторы могут задавать политики авторизации на основе типа устройства.

Платформа Cisco Identity Services Engine собирает сведения об атрибутах оконечных устройств с использованием средств пассивной сетевой телеметрии, путем активного сканирования оконечных устройств, а также путем взаимодействия с сенсорами устройств, функционирующими на коммутаторах Cisco Catalyst.

Средства профилирования устройств, размещенные на коммутаторах Cisco Catalyst, являются одним из элементов технологии профилирования Cisco ISE. Они позволяют коммутаторам быстро собрать сведения об оконечных устройствах, подключенных к ним, и передать собранные сведения по

протоколу RADIUS платформе Cisco ISE для классификации устройств и назначения соответствующих политик. Технология профилирования с использованием сенсоров на коммутаторах позволяет осуществить эффективный сбор сведений об оконечных устройствах в рамках распределенной ИТ-инфраструктуры, а также обеспечивает масштабируемость платформы, упрощает развертывание и позволяет повысить эффективность классификации устройств.

Как работает профилирование? Любое устройство оставляет некий «след» в сети, например: MAC -адрес устройства, поддерживает ли устройство протокол CDP; если в устройстве есть браузер, то мы можем узнать атрибуты браузера, если устройство получает адрес по DHCP, то из параметров DHCPможно узнать различные параметры устройства и т.д., т.е., используя около десятка разных атрибутов и сигнатур, ISEопределяет, какое устройство и какого типа включается в сеть (Рисунок 2.23).

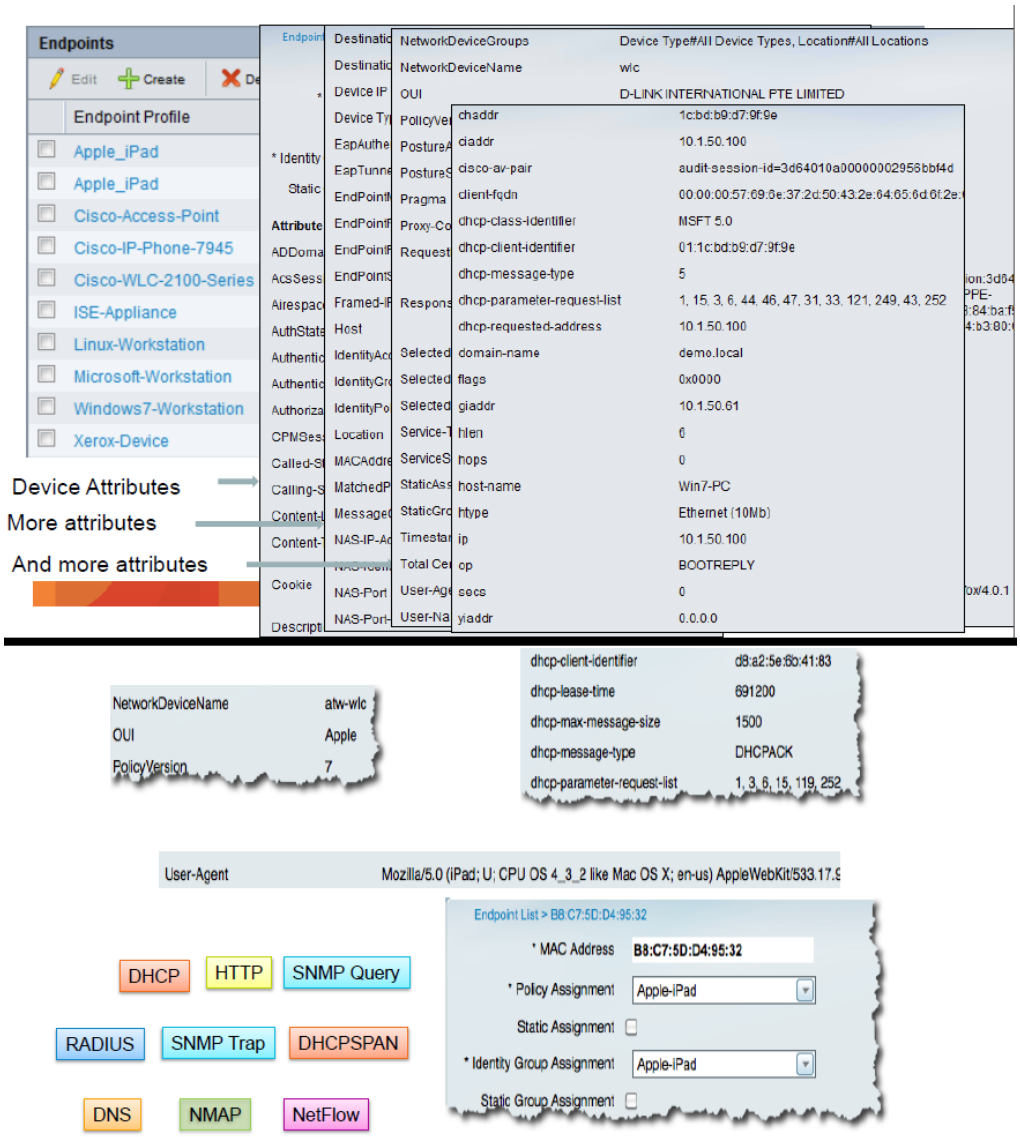

Рисунок 2.23 - Сбор атрибутов устройств

После сбора необходимых атрибутов, Cisco ISE использует условия для определения устройства и по принципу наилучшего совпадения задает политику для данного устройства (Рисунок 2.24).

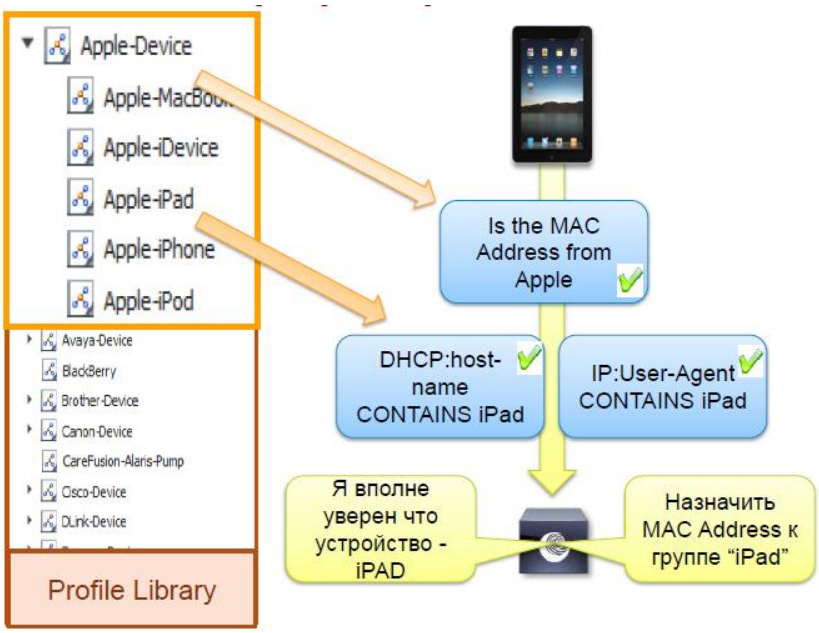

Рисунок 2.24 - Политики профилирования

Это был динамический метод профилирования устройства, т.е. определения типа устройства по различным атрибутам. Так же можно профилировать устройства статически, т.е. присвоить типы MAC-адресам устройств (Рисунок 2.25).

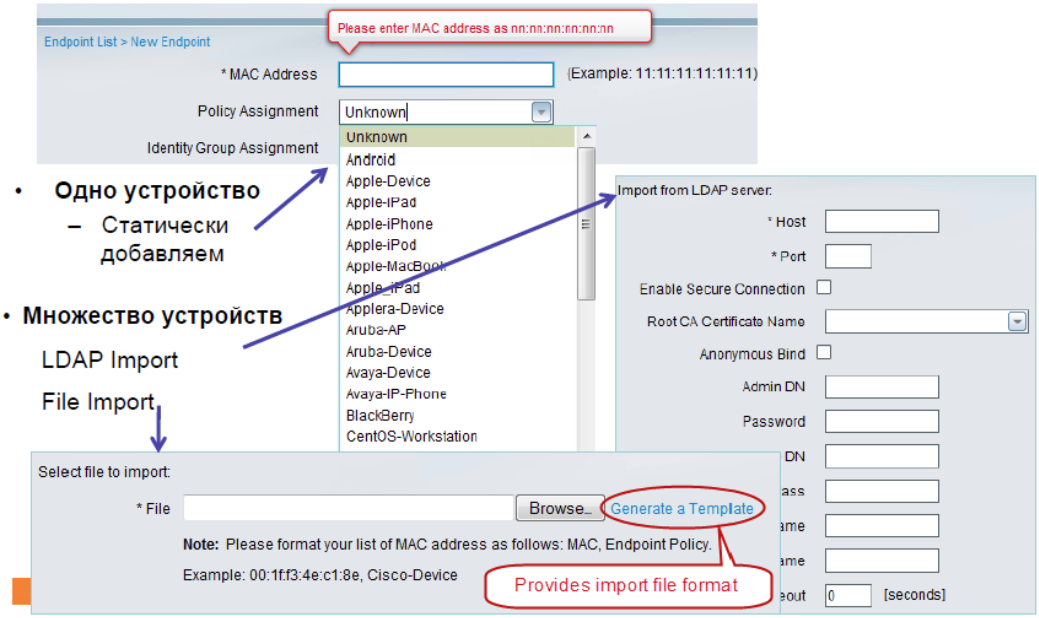

Рисунок 2.25 - Статическая классификация MAC-записей

Сервис ISEсодержит целую библиотеку готовых профайлов, в которой собраны наиболее популярные устройства на сегодняшний день (Рисунок 2.26).

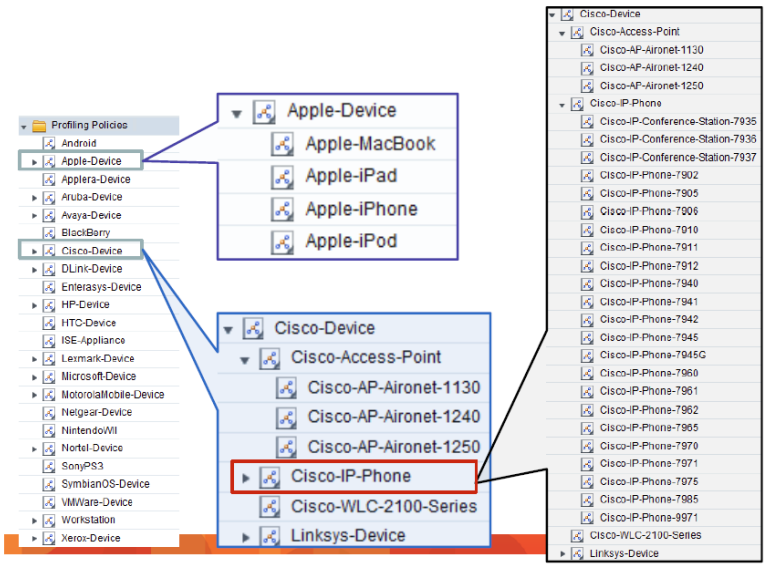

Рисунок 2.26 - Библиотека профайлов ISE

Еще одним немаловажным сервисом ISE является оценка состояния устройства, т.е. состояние соответствия устройства политике безопасности компании. В рассматриваемой нами банковской системе требуется, чтобы на устройствах (корпоративных и личных) был инсталлирован и обновлен антивирус, а так же установлены последние Windows-патчи. Cisco ISE проверяет устройство, подключающееся в сеть путем анализа реестра системы, файлов, процессов и приложений, файлов обновлений Windowsи др. (Рисунок 2.27).

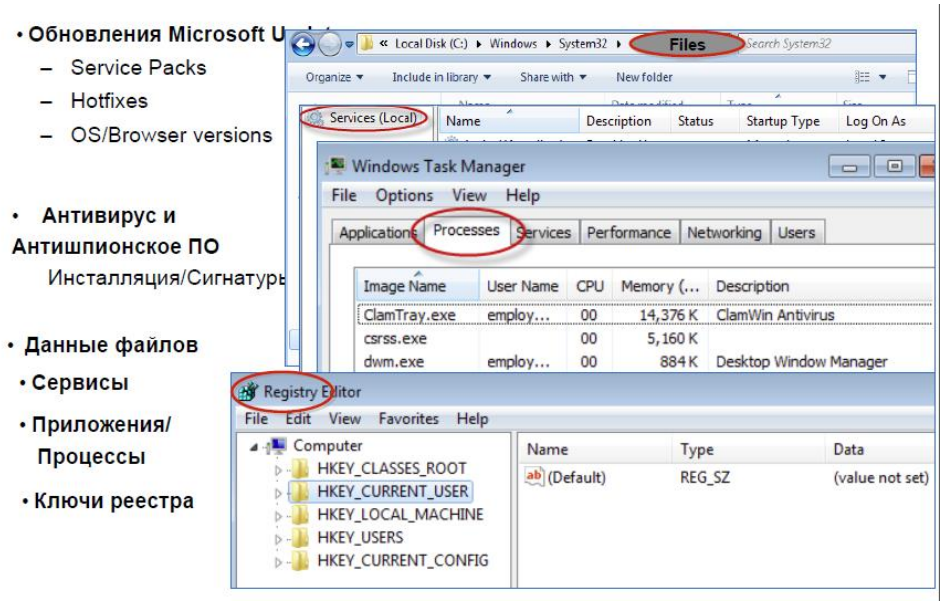

Рисунок 2.27 - Доступные проверки оценки состояния

Если ISE устанавливает несоответствие политике предприятия, то устройство помещается в карантин до тех пор, пока не будет инсталлировано все необходимое (Рисунок 2.28).

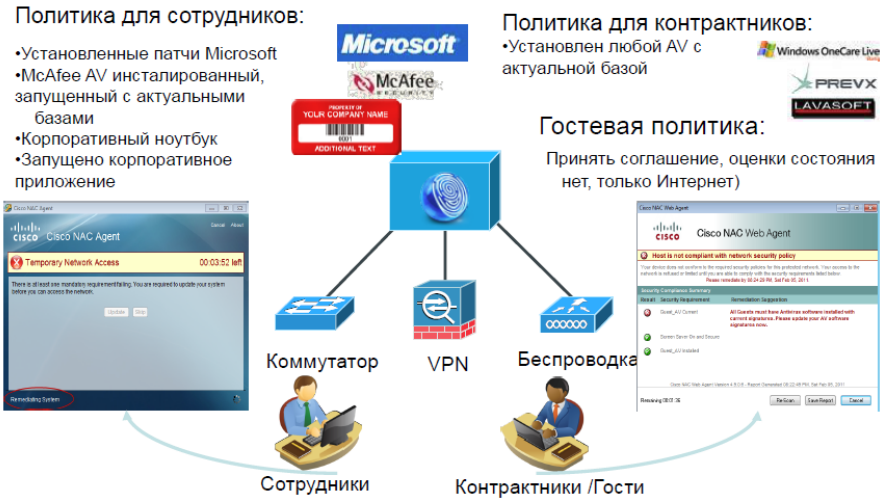

Рисунок 2.28 - Политики состояния ISE

2.9 Гостевой доступ

Cisco ISE поддерживает ещё один сервис, который называется гостевым сервисом. Благодаря данному сервису в банковской системе появится возможность автоматизировать процесс гостевого подключения, т.е. гости или партнеры банка смогут получить доступ к определенным внутренним ресурсам банка благодаря гостевому порталу Cisco ISE, например, гости могут использовать только выход в Интернет, а партнеры, помимо Интернета, могут иметь доступ и к определенным внутренним ресурсам банка (Рисунок 2.29).

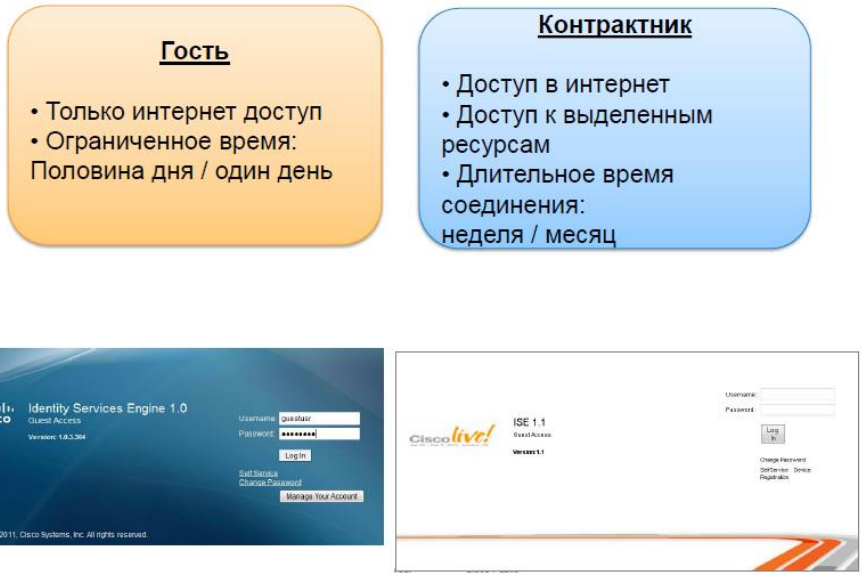

Рисунок 2.29 - Разные гостевые роли

Жизненный цикл гостевого доступа состоит из следующих компонентов (Рисунок 2.30):

- предоставление (гостевые аккаунты предоставляются посредством гостевого портала);
- уведомление (предоставленные аккаунты отсылаются через email, sms или печать);
- управление (управление гостевыми аккаунтами, настройки политик для гостей или партнеров);
- аутентификация/авторизация (через web - портал ise);
- отчетность (все аспекты гостевых учетных записей).

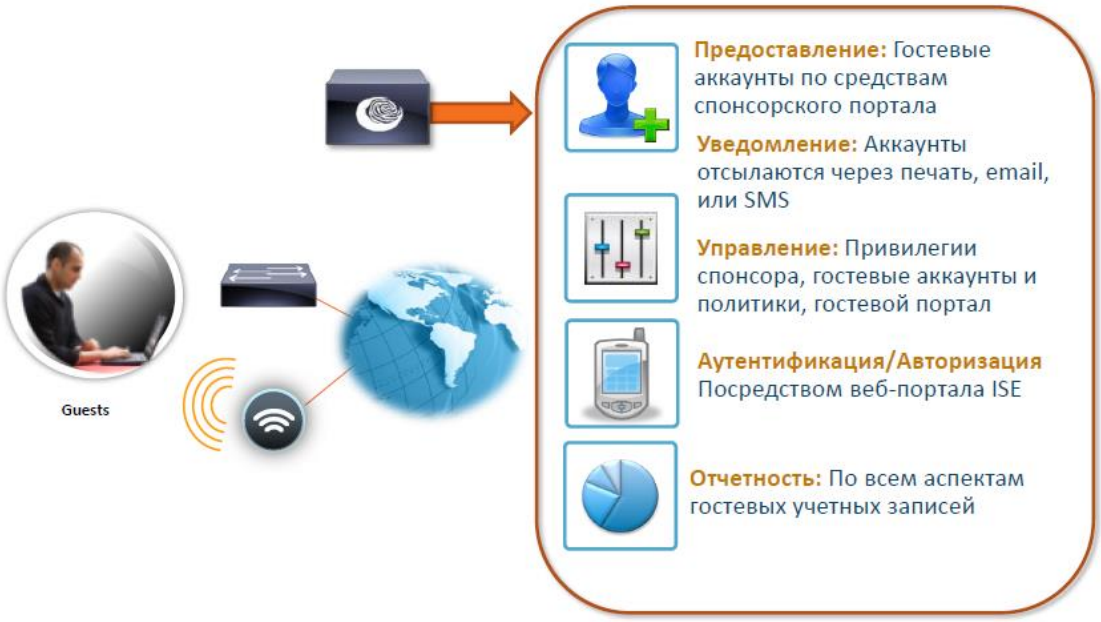

Рисунок 2.30 - Компоненты полного жизненного цикла гостя

Гостевой доступ можно реализовать двумя способами - это гостевой доступ по приглашению или самостоятельная регистрация гостей. Для того, чтобы реализовать гостевой доступ по первому способу, необходимо чтобы приглашающая сторона или «спонсор» создал на спонсорском портале гостевую учетную запись причем создавать данные учетные записи могут не только специалисты из IT-отдела, а тот человек, к которому данный гость или партнер пришел, например, секретарь (Рисунок 2.31).

Как видно из рисунка 2.31, чтобы создать гостевую учетную запись, необходимо лишь заполнить необходимые поля, выбрать из списка профилей профиль «Guest», т.е. гость, и выбрать время, в течение которого сессия будет находиться в активном состоянии. После этого на гостевом сервере ISEпоявляется данная учетная запись с паролем. Далее гость запускает браузер и перенаправляется на гостевой портал (Рисунок 2.32), где гость вводит предоставленный ему логин и пароль, который проверяется в ISE Guest User

Identity Store, и если проверка прошла успешно, то гостю предоставляется доступ к определенным ресурсам банка (в нашем случае, к Интернету).

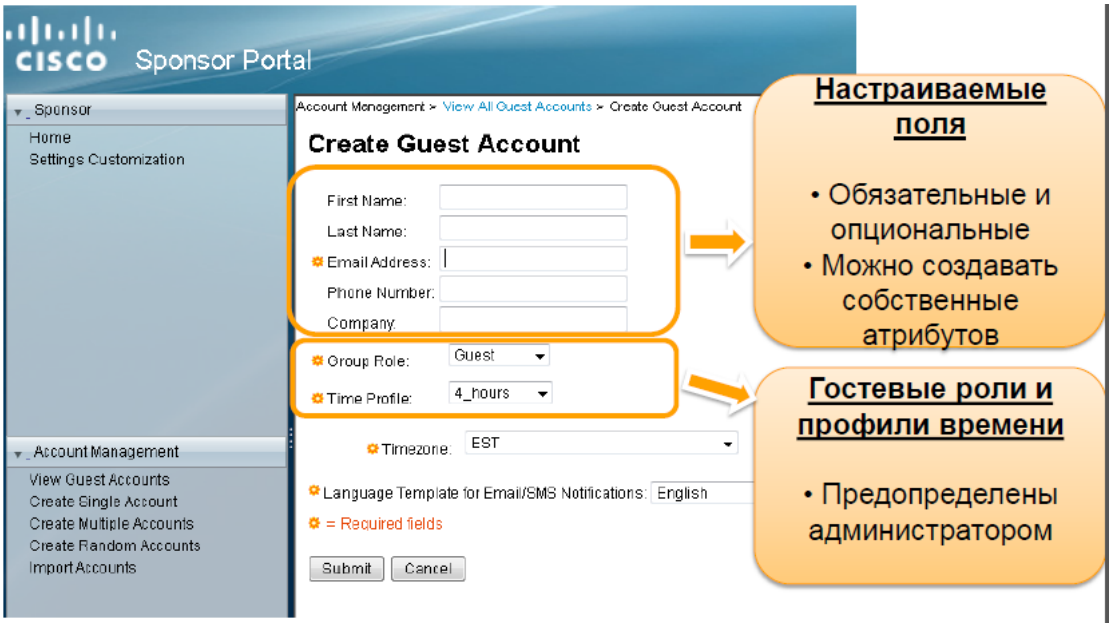

Рисунок 2.31 - Спонсорский портал ISE

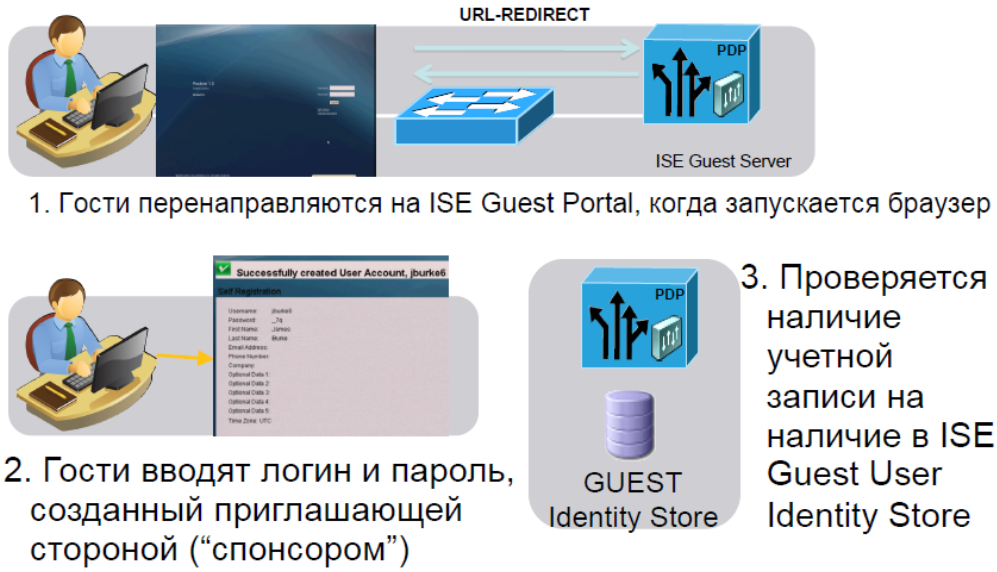

Рисунок 2.32 - Гостевой доступ по приглашению

Второй вариант - это самостоятельная регистрация гостей. Пользователи выбирают саморегистрацию на портале и после и после запуска браузера перенаправляются на гостевой портал, после чего гость заполняет обязательные поля для аутентификации. После того, как все обязательные поля были заполнены, в ISE Guest Identity Store создаются гостевые учетные данные (Рисунок 2.33).

Рисунок 2.33 - Создание гостевой записи в ISE Guest Identity Store

После того как учетные данные были созданы, гость повторно перенаправляется на главную страницу гостевого портала для ввода сгенерированных ранее логина и пароля. После этого к гостю применятся авторотационная политика для Интернет - доступа. Все это время учетная запись мониторится на соответствие временным ограничениям (Рисунок 2.34).

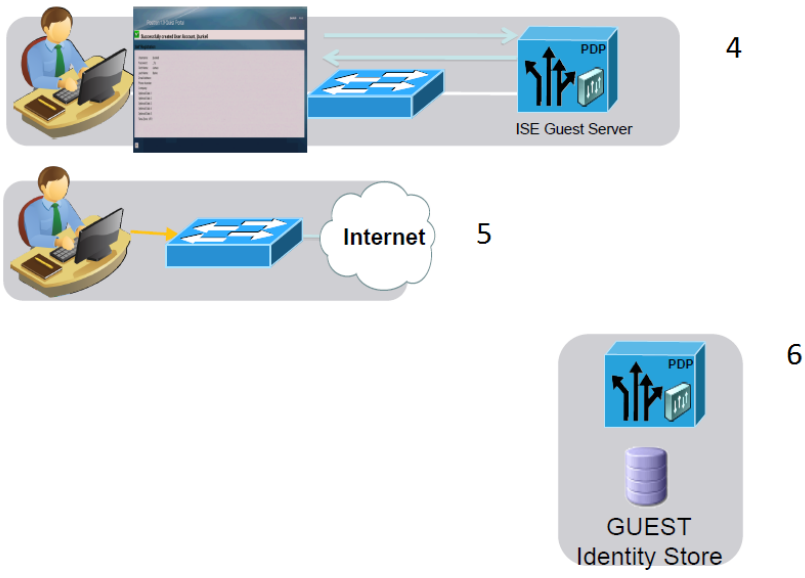

Рисунок 2.34 - Авторизация и мониторинг гостевой учетной записи

Cisco ISE позволяет проводить подробнейший аудит жизненного цикла каждого гостя, что значительно упрощает контроль и обслуживание IT-персоналу (Рисунок 2.35).

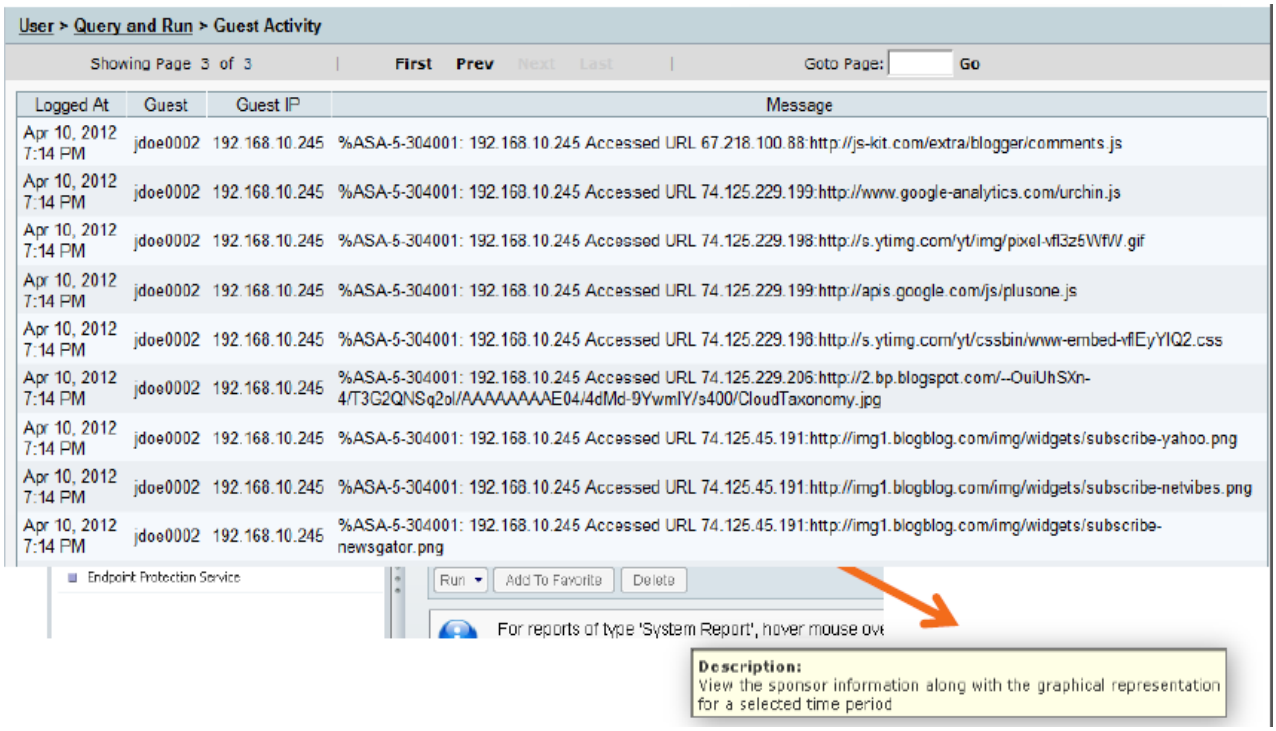

Рисунок 2.35 - Полный аудит гостевого жизненного цикла

На рисунке 2.36 представлен примерный сценарий подключения гостевого пользователя в нашем банке.

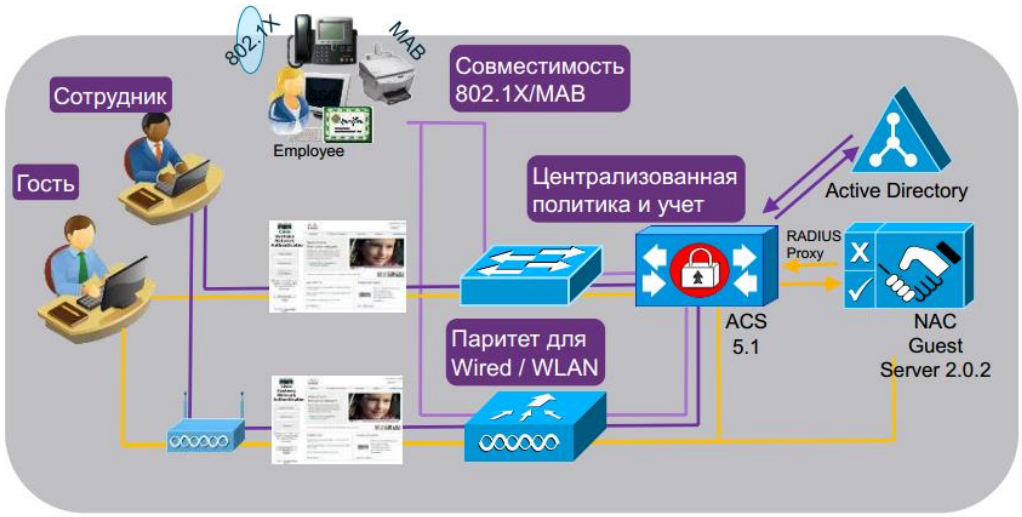

Рисунок 2.36 -Унифицированная веб-аутентификация для проводного и беспроводного доступов сотрудников и гостей

3 Cisco Energy Wise в рамках архитектуры «Сети без границ»

3.1 Что такое Cisco EnergyWise?

На сегодняшний день острой проблемой для любой уважающей для себя компании или предприятия является вопрос кардинального сокращений затрат на электроэнергию, чтобы получить от этого больше прибыли. Как следствие, появляется все больший спрос на рациональные решения для управление ИТ, т.к. бизнес во всем мире уделяет все больше внимания вопросам измерения потребления электропитания и контроля выделения энергии, поэтому основной задачей является уменьшение расходов на электроэнергию, повышение эффективности управления и консолидация управления энергопотреблением различных устройств и средств коммуникации [6].

Технология Cisco EnergyWise призвана решить данную проблему. Она позволяет организации измерять, управлять, а также получать отчеты об энергопотреблении всех устройств корпоративной сети, начиная с PoE устройств и заканчивая IP-контроллерами зданий, для последующей оптимизации использования энергии на основе пользовательских политик. Управляемое отключение компьютеров, освещения, кондиционеров на ночь, распределение энергопотребления для IP-телефонов и точек доступа, отключение питания неиспользуемых портов коммутатора и сетевых модулей - все это позволяет сэкономить предприятию значительную часть средств, расходуемых на оплату электричества. А ведь для крупных компаний это десятки и даже сотни тысяч долларов в год. Данная технология встраивается в коммутаторы и маршрутизаторы Cisco, помогая заказчикам измерять, отслеживать и сокращать потребление энергии во всей корпоративной инфраструктуре.

EnergyWise определяет несколько стандартных уровней потребления энергии, понятных всем сетевым устройствам. Затем это решение дает возможность сети автоматически распознать все управляемые устройства. После этого сеть начинает отслеживать энергопотребление и реагировать на команды и запросы. Она использует систему доменных имен и метки из ключевых слов для запросов и суммирования информации, получаемой от больших групп устройств. Сеть становится платформой для обобщения энергетических данных и распространения единого набора правил по всему "сетевому облаку", что значительно упрощает управление энергопотреблением и повышает его масштабируемость.

Передовая технология EnergyWise реализуема на новых платформах 2960-S, 3560-X и 3705-X с ПО Cisco IOS Base, LAN Base и LAN Lite, а также Cisco ISR G2 и Catalyst 6500. Технология обратно совместима с коммутаторами серий 3750 и 3750G с интегрированным контроллером беспроводного доступа и маршрутизаторами Cisco ISR. В коммутаторах серии 2960-S представлены источники питания с повышенным КПД по сравнению с коммутаторами 2960-

G. Благодаря повышению КПД источников питания эксплуатация новых коммутаторов обходится дешевле.

3.2 Архитектура Cisco EnergyWise

Стехнологией Cisco EnergyWise управление питанием осуществляется с помощью сетевой инфраструктуры компании, т.е. сама сеть в совокупности с устройствами и программным обеспечением может управлять потреблением энергии всех типов устройств, а так же в будущем планируется интеграции данной технологии с Системами Управления Зданием (BMS) (к ним относятся лифты, электромагнитные турникеты, системы пожарной безопасности, системы управления климатом, сигнализация, системы видеонаблюдения и др.). Таким образом, Cisco EnergyWise обеспечивает гибкое и единое управление электропитанием оконечных устройств различных вендоров. На рисунке 3.1 изображена архитектура Cisco EnergyWise.

Рисунок 3.1 - Архитектура Cisco EnergyWise

Как видно из рисунка 3.1, верхний ярус архитектуры состоит из приложений управления - как собственных платформ по управлению, разработанных Cisco, так и партнеров компании Cisco. Приложения управления используют или инструментарий управления Cisco EnergyWise Toolkit Management API (MAPI), или протокол SNMP для мониторинга и контроля питания членов домена EnergyWise. При использовании MAPI, приложения управления посылают запрос по протоколу Cisco EnergyWise другим членам домена, которые далее распространяют его по другим членам домена и т.д. После этого, результаты направляются обратно в приложения управления, которые собирают и отображают или архивирует результаты, которые будут

использоваться для последующей отчетности. Протокол Cisco EnergyWise был специально разработан, чтобы обеспечить более масштабируемый механизм для обращения к нескольким устройствам в домене, в то время как протокол SNMP устанавливает или получает команды индивидуально для каждого домена.

Второй ярус архитектуры Cisco EnergyWise состоит из компонентов сетевой инфраструктуры, таких как Cisco Catalyst коммутаторов и ISR G2 маршрутизаторов, которые также называют Cisco EnergyWise доменами или членами домена Cisco EnergyWise. Члены домена отправляют запросы, которые приходят от приложений управления или от других членов домена, используя Cisco EnergyWise протокол.

Третий ярус данной архитектуры составляют оконечные устройства. Устройства, которые поддерживают Cisco EnergyWise SDK, реагируют на запросы, пришедшие от приложения управления или других членов домена, поддерживающий протокол Cisco EnergyWise, а для устройств, которые не поддерживают данную технологию, например, некоторые модели IP-телефонов или точек доступа, то здесь на запрос реагирует порт коммутатора, к которому данное устройство присоединено.

3.3 Домен Cisco EnergyWise

Домен Cisco EnergyWise является административной группировкой устройств с целью контроля и управления электропитанием. Эти устройства могут состоять из сетевого оборудования Cisco, такого как коммутаторы Cisco Catalyst и маршрутизаторы ISR G2, оконечные устройства, питающиеся через PoE и подключённые к коммутаторам Catalyst, такие как IP-телефоны, беспроводные точки доступа и т.д. На рисунке 3.2 изображен пример домена EnergyWise.

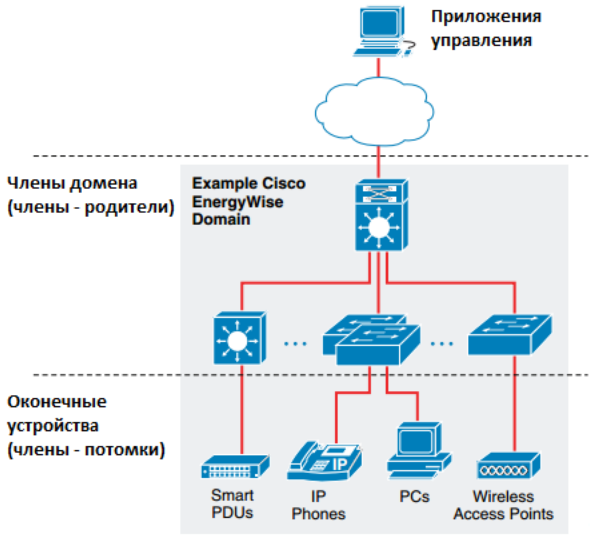

Рисунок 3.2 -Домен EnergyWise

Домен Cisco EnergyWise не имеет отношения к другим группам сетевой инфраструктуры, таким как протоколы маршрутизации или VTP доменам. Устройство может быть членом только одного домена в определенное время, т.е. оно не может быть членом сразу нескольких доменов.

В домене EnergyWise каждое устройство (сущность) имеет свою роль и название. Между данными сущностями имеются отношения: сосед - сосед и родитель - ребенок (Рисунок 3.3).

Рисунок 3.3 - Отношение сущностей

Как видно из рисунка 3.3, соседи образуют между собой равноправные отношения, и данные отношения формируются автоматически за счет обмена пакетными данными, используя протоколы CDP или UDP. Так же можно настроить отношения соседей статически (Рисунок 3.4). В домене Cisco EnergyWise образуется так же связь родитель - ребенок, где конечные точки (устройства) называют сущность - ребенок, т.е. те сущности, которые могут только отвечать на запросы EnergyWise, в то время как сущности - родители могут как генерировать, так и отвечать на запросы Cisco EnergyWise (на рисунке 3.3 в качестве родителей выступают коммутаторы, а в роли детей - оконечные устройства).

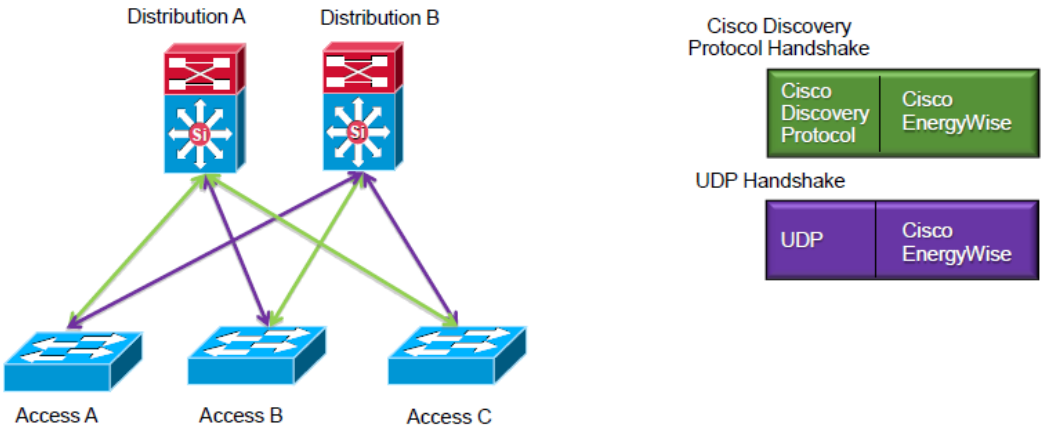

Рисунок 3.4 - Установление соседских отношений

3.4 Атрибуты Cisco EnergyWise

Технология Cisco EnergyWise позволяет использовать опциональные атрибуты, которые могут быть настроены как глобально, так и на любом порту коммутатора Catalyst или маршрутизатора ISR G2. К таким атрибутам относятся *важность, ключевые слова, имена и роли.* Данные атрибуты функционируют в качестве значений, устанавливая контекст, тем самым, сетевой администратор имеет возможность устанавливать общие критерии для конечных точек. Данные атрибуты настраиваются на уровне порта коммутатора или маршрутизатора, поддерживающие PoE. Рассмотрим каждый из этих атрибутов:

- **Важность (Importance)** - атрибут, позволяющий дифференцировать устройства в сети в зависимости от их относительной значимости, и имеет численное значение от 1 - 100 (где 100 - наивысшая значимость). Пример приведен на рисунке 3.5.

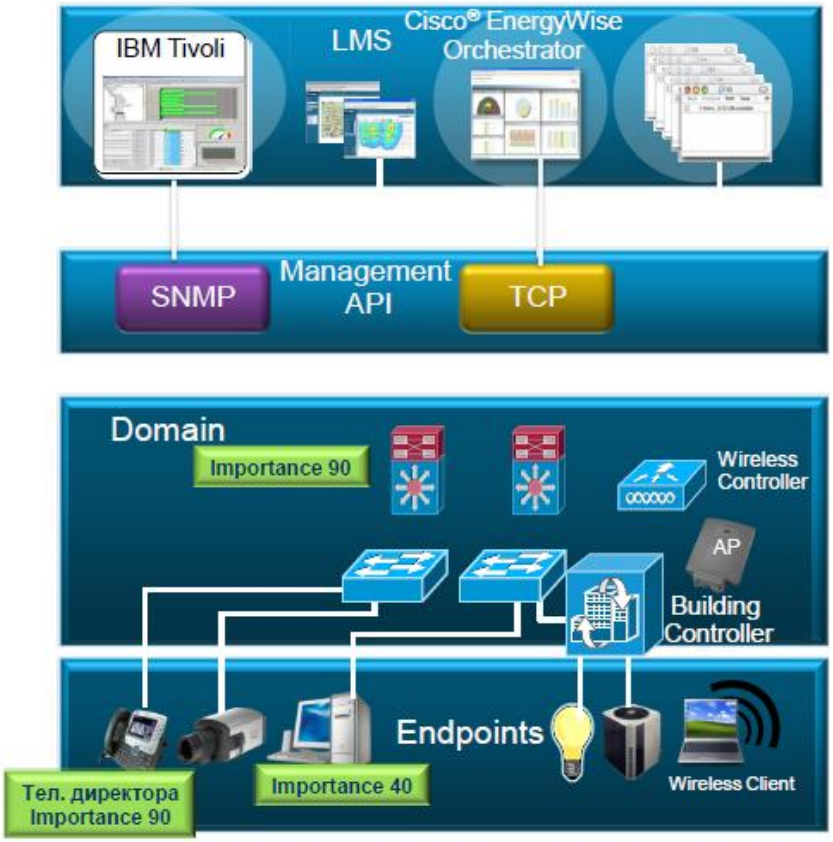

Рисунок 3.5 - Атрибут Importance (Важность)

Ниже приведена таблица атрибута *Importance* и соответствующие числовые значения:

Т а б л и ц а 3.1 - Значения атрибута Importance

Тип	Ранг атрибута
Устройства аварийного реагирования	90-100
Управляющие сотрудники	80-89
Регулярные сотрудники	70-79
Обслуживающий персонал	60-69
Публичные или гостевые устройства	40-59
Декоративные, такие как микроволновые печи	0-39

Как видно из рисунка 3.5, значения атрибута Importance для телефона директора имеет более высокий ранг по сравнению с рабочей станцией обычного сотрудника.

Для того чтобы настроить данный атрибут на порту коммутатора, необходимо выполнить следующие команды:

```
swicth(config)#interface FastEthernetX/X,..,GigabitEthernetX/X
swicth(config-if)# energywise importance importance[1-100]
```

- **Ключевые слова (Keywords), Имена (Name) и роли (Roles)**. Ключевое слово *keyword* позволяют создавать контекст устройств и могут иметь любые название, например: IT, floor2 и т.д. Атрибут *name* служит для задания имени устройства, например Phone5. Атрибут *role* служит для определения функции, выполняемой устройством на основе бизнес - контекста, например PC_Administrator. На рисунке 3.6 изображен пример использования данных атрибутов.

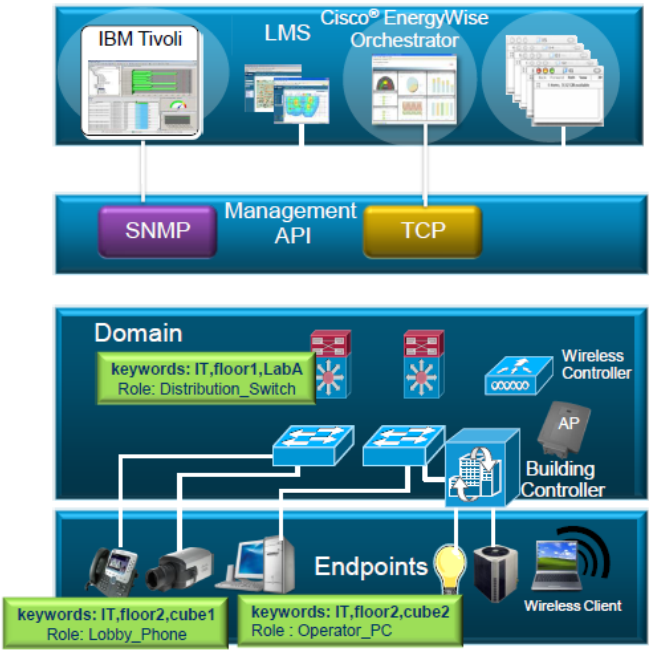

Рисунок 3.6 - Атрибуты keyword, name и role

Для того чтобы настроить данные атрибуты на порту коммутатора, необходимо выполнить следующие команды:

```
Switch(config)#intfa1/0/17
Switch(config-if)#energywise keywords lobby,sattelite
Switch(config-if)#energywise role role.lobbyaccess
Switch(config-if)#energywise importance 50
Switch#shrun intfa1/0/17
!
interface FastEthernet1/0/17
energywise level 0 recurrence priority 100 at 0 8 * * *
energywise level 10 recurrence priority 100 at 0 20 * * *
energywise level 7
energywise importance 50
energywise role role.lobbyaccess
energywise keywords lobby,sattelite
energywise name kiosk.17
end
```

3.5 Уровни EnergyWise

Технология Cisco EnergyWise использует набор определенных действующих уровней для контроля электропитания, так как устройства в сети Cisco EnergyWise могут быть от разных производителей. Уровни Cisco EnergyWise показаны в таблице 3.2.

Т а б л и ц а 3.2 - Уровни Cisco EnergyWise

Категория	Цвет	Код	Цвет	Уровень	Метка
Действующий		FF0000	Красный	10	Full
				9	High
		FFF00	Желтый	8	Reduced
				7	Medium
		00FF00	Зеленый	6	Frugal
				5	Low
Резервный		0000FF	Синий	4	Ready
				3	Standby
		A52A2A	Коричневый	2	Sleep
				1	Hibernate
Недействующий		000000	Черный	0	Shutdown

Таким образом, с помощью уровней (levels), сеть может скомандовать устройствам изменить свой текущий уровень энергопотребления, а так же сообщить сети свой текущий уровень энергопотребления.

Чтобы настроить соответствующий уровень потребления энергии на порту коммутатора, необходимо выполнить следующий команды:

```
Switch(config)#intfa1/0/17
Switch(config-if)#energywise level level[0-10]
```

Так же можно, согласно политике предприятия, устанавливать время, когда неиспользуемые устройства можно выключать (задавать уровень, равный 0), либо переводить режим энергопотребления на минимум. Вот небольшой пример настройки порта коммутатора согласно политике, приведенной ниже:

```
Switch(config)#interface FastEthernetX/X
Switch(config-if) #energywise level 10 recurrence importance 50 at [minute] [hour] [day of month] [month of year] [day of week]
Switch(config-if)#energywise level 10 recurrence importance 50 at 0 7 * * 1,2,3,4,5
Switch(config-if)#energywise level 0 recurrence importance 50 at 0 0 * * 0,1,2,3,4,5,6
Switch(config-if)#energywise level 0 recurrence importance 50 at 0 19 * * 1,2,3,4,5
Switch(config-if)#energywise level 10 recurrence importance 50 at 0 12 * * 0,6
Switch(config-if)#energywise level 0 recurrence importance 50 at 0 17 * * 0,6
Switch(config-if)#energywise importance 50
Switch(config-if)#energywise role end UserInterface
Switch(config-if)#energywise keywords phone,videophone
```

В приведенном выше примере, значения 0 7 * * 1,2,3,4,5 означают:

- 0 минут
- 7 часов (7 AM)
- *дней (все дни в месяце)
- *месяцы (все месяцы в году)
- 1,2,3,4,5 (с понедельника по пятницу)

До внедрения технологии EnergyWise в нашу банковскую систему все устройства работали круглосуточно. С технологией EnergyWise можно значительно сократить потребление энергии, используя определенную политику для некоторых устройств. Приведем пример: рабочие часы банка - с 9.00 до 18.00, поэтому можно разработать следующую политику для некоторых устройств - на ночь отключать определенные устройства или переводить их в режим минимального энергопотребления (Рисунок 3.7).

Рисунок 3.7 - Пример политики EnergyWise для банка

Как видно из рисунка 3.7, уже, отключая на ночь некоторые устройства (IP-телефоны, точки доступа, ноутбуки и т.д.), можно добиться значительной экономии, а если компания имеет около 10000 рабочих станций, точек доступа, а так же удаленные офисы, где так же можно переводить в режим минимального потребления большинство устройств, выключать устройства в переговорных комнатах и конференц-залах во внерабочее время, то, согласитесь, экономятся колоссальные объемы энергии, что существенно снижает затраты всего предприятия и экономия может составлять тысячи, а иногда и десятки тысяч долларов в год.

3.6 Запросы EnergyWise

Домен EnergyWise образует виртуальную распределенную базу данных, поэтому с помощью них можно производить мониторинг и контролировать потребление всей сети, например: какова потребляемая мощность устройств в домене? (Рисунок 3.8).

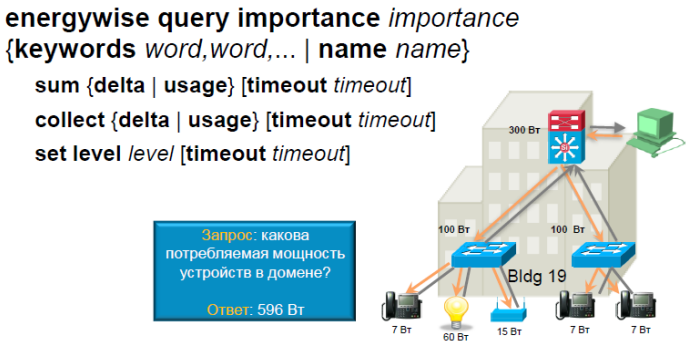

Рисунок 3.8 - Запросы EnergyWise

Общая структура запроса выглядит как показано на рисунке 3.8.

Приведем примеры некоторых запросов, с помощью которых можно проводить мониторинг и собирать данные по электропотреблению любого устройства в домене:

Пример запроса Collect (данный запрос выдает информацию об энергопотреблении отдельных устройств):

```
Switch# energywise query importance 80 keyword Admin collect usage
EnergyWise query, timeout is 3 seconds:
Host                Name              Usage          Level      Imp
--------------------
192.168.40.2        shipping.1        6.3 (W)        10         1
192.168.60.3        pc.1              200.0 (W)      8          75
Queried: 2 Responded: 2 Time: 0.11 seconds
```

Пример запроса Sum(Запрос выдает суммарную информацию об энергопотреблении):

```
Switch# energywise query importance 100 name * sum usage
EnergyWise query, timeout is 3 seconds:
Total Usage
----------
346.3 (W)
Queried: 147 Responded: 147 Time: 0.42 seconds
```

Пример запроса Set (Запрос меняет режимы энергопотребления устройств):

```
Switch# energywise query importance 50 name * set level 10
EnergyWise query, timeout is 3 seconds:
!!!!!!!!!!!!!!!!!!!!!!
Success rate is (47/47) setting entities
Queried: 47 Enacted: 47 Time: 0.16 seconds
```

3.7 Прототип системы доменов для банковской системы

Таким образом, домен EnergyWise представляет собой совокупность устройств (сущностей), взаимодействующих между собой по протоколу CDP или UDPи устанавливающие между собой определенные отношения, при этом предоставляя мощный инструмент для контроля и мониторинга потребления энергии любым устройством в домене. Поэтому любую корпоративную сеть предприятия можно представить как совокупность доменов EnergyWise. Для нашей сети банковской системы можно предложить следующий прототип системы доменов EnergyWise (Рисунок 3.9).

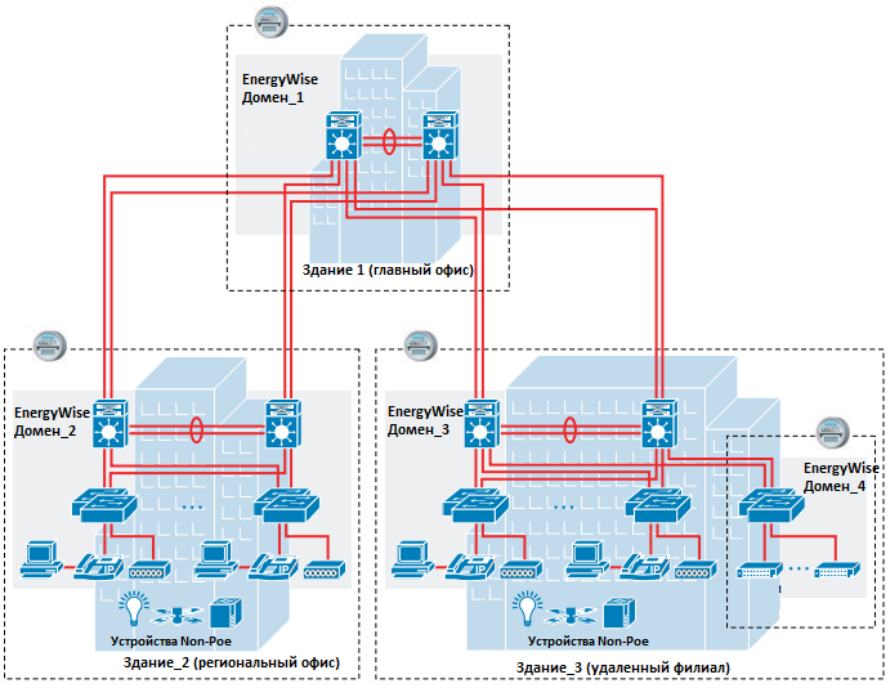

Рисунок 3.9 - Дизайн сети банка с использованием доменов EnergyWise

4 Безопасность жизнедеятельности

4.1 Анализ условий труда сотрудников

В данной выпускной работе разрабатывается модернизация сети с использованием инновационной технологии Cisco «Сети без границ» для главного офиса Национального Банка РК, поэтому основные работы будут проводиться администраторами за компьютером. Мы рассматриваем офисное помещение отдела Информационных Технологий. В рассматриваемом офисном помещении работают шесть администраторов, каждый из которых имеет свое рабочее место. Для сотрудников необходимо создать комфортные условия труда, такие как рабочее место и состояние внутренней среды комнаты, обеспечивающее оптимальную динамику работоспособности, хорошее самочувствие и сохранение их здоровья. Рабочее место обеспечивает возможность удобного выполнения работ в положении сидя. При выборе положения работающего необходимо учитывать физическую тяжесть работ; размеры рабочей зоны и необходимость передвижения в ней работающего в процессе выполнения работ; мероприятия направленные на снижение утомляемости.

Как уже было отмечено, важным моментом организации рабочего места является также определение занимаемой работником площади. Необходимо, чтобы эта площадь позволяла удобно и с наименьшей затратой энергии безопасно и производительно вести трудовой процесс.

Все электротехническое оборудование в данном помещении является потенциальным источником возникновения пожарной опасности. Оборудование малошумящее - вредность в качестве повышенного шума отсутствует. Рабочее помещение, распложенное в здании, не находится в непосредственной близости от железнодорожной магистрали или нагруженной автомагистрали, аэропорта и так далее, поэтому внешних источников шума, влияющих на процесс работы - нет. Так же отсутствует повышенный уровень электромагнитных излучений (в данном офисе применены мониторы типа LCD, а также беспроводное оборудование). При эксплуатации электрооборудования существует опасность поражения электрическим током. Поражение электрическим током может произойти при коротком замыкании, при не правильном обращении с компьютером, при случайном попадании воды на токоведущие части. В целях предотвращения поражения электрическим током в системе питания электрооборудования предусмотрено защитное зануление (все вилки и розетки имеют контакты зануления).

Выполняемая работа относится к категории легких работ (категория Iа), выполняемых в сидячем положении (ГОСТ 12.2.032-78) [17].

Высота рабочей поверхности: 725 мм, высота сиденья: 420 мм, данные ГОСТа указаны в таблице 6.1.

Т а б л и ц а 4.1 - Виды работ (ГОСТ 12.2.032-78)

Наименование работ	Класс работ	Пол работника	Высота рабочей поверхности при организации рабочего места	Высота сиденья
Легкие работы (конторская работа)	Класс Iа (работа, выполняемая в сидячем положении)	Мужской, женский	725 мм	420 мм

Размер различаемых в процессе работы объектов: 1 мм, расстояние от объекта до глаз работника: 500 мм - разряд зрительной работы: IV (СНиП РК 2.04-05-2002), данные СНиПа указаны в таблице 4.2 [18].

Т а б л и ц а 4.2 - Разряд зрительной работы (СНиП РК 2.04-05-2002)

Размер минимального различаемого объекта, мм	Расстояние от объекта до глаз работника, мм	Разряд зрительной работы
0,5-1	500	IV

4.2 Характеристики здания и помещения

Перечислим основные технические характеристики здание и офисного помещения:

- здание расположено в городе Алматы в черте города. Здание семиэтажное;
- рабочее помещение находится на пятом этаже здания, в кабинете отдела информационной и сетевой безопасности;
- размеры рабочего помещения: длина $l=9,5м$, ширина $s=6м$, высота $h=4м$;
- остекление помещения - двойное (два окна размером 3500х1800 мм) без стального переплетения;
- внутренняя отделка стен - светлая;
- искусственное освещение - светильники: люминесцентные лампы ЛБ40-4 (12 штук).

План помещения представлен на рисунке 4.1.

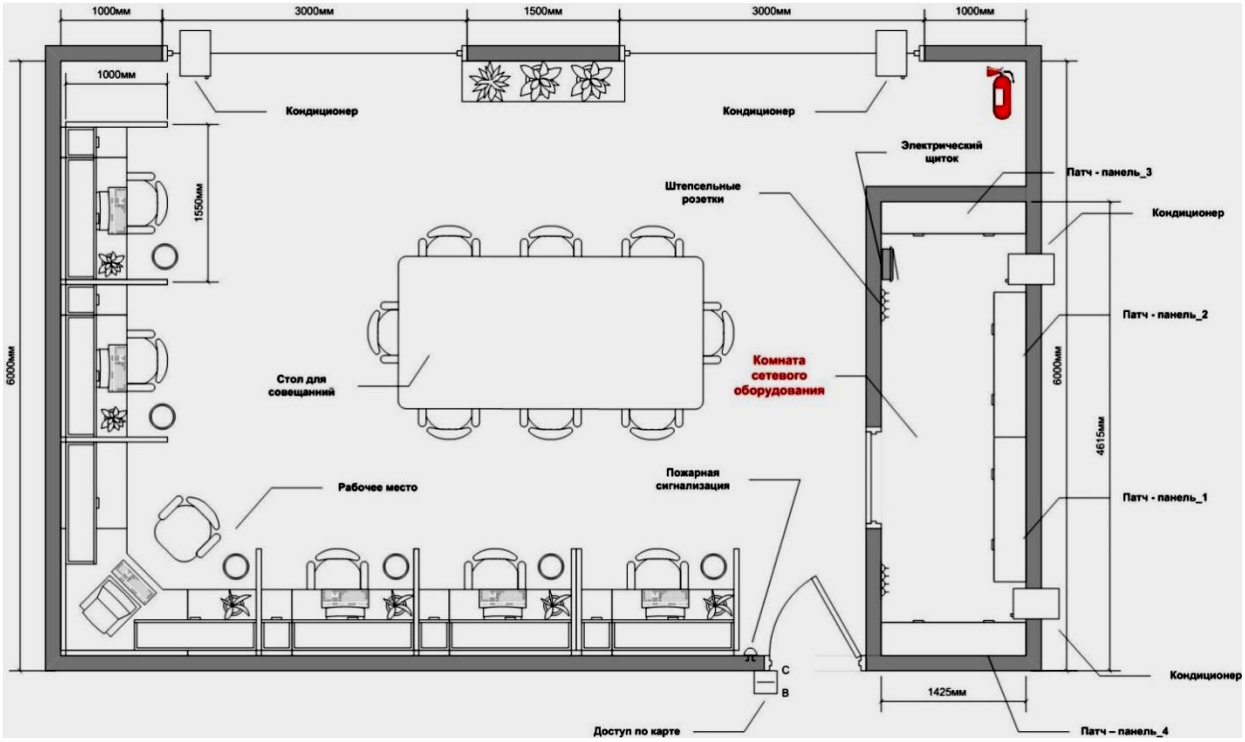

Рисунок 4.1 - План офисного помещения

Режим работы (продолжительность рабочего дня) - с 9:00 до 18:00.

Здание относится к I степени огнестойкости (СНиП РК 2.02-05-2002), данные СНиПа указаны в таблице 4.3 [19].

Т а б л и ц а 4.3 - Конструктивная характеристика зданий в зависимости от их степени огнестойкости (СНиП РК 2.02-05-2002)

Степень огнестойкости	Конструктивные характеристики
I	Здания с несущими и ограждающими конструкциями из естественных или искусственных материалов, бетона или железобетона с применением листовых и плитных негорючих материалов

Общая площадь помещения составляет 57 кв.м.

Для вентиляции рабочего помещения используются каналы естественной вентиляции, прокладываемые при строительстве здания, открытые окна (в теплый период), а также система кондиционирования. Такая вентиляция позволяет поддерживать климатические параметры рабочего помещения в пределах нормы (таблица 4.4) в условиях климата города Алматы (в том числе - и в теплый период года), СНиП 2.04.05-91 [20].

Таблица 4.4 - Оптимальные нормы температуры, относительной влажности и скорости движения воздуха в обслуживаемой зоне жилых, общественных и административно-бытовых помещений (СНиП 2.04.05-91)

Период года	Температура воздуха, ^{o}C	Относительная влажность воздуха, %	Скорость движения воздуха, м/с.
Теплый	20-22	60-30	0,2, не более
	23-25	60-30	0,3, не более
Холодный и переходные условия	20-22	45-30	0,2, не более

Рабочее помещение имеет естественное освещение в виде двух окон размером 3500х1800 мм. Также используется система общего освещения (искусственное освещение): люминесцентные лампы ЛБ40-4 (12 штук).

Существующая площадь окон соответствует нормативам естественного освещения.

Рабочее помещение по вопросам пожарной безопасности относится к классу «Д».

Рабочее помещение (кабинет технического отдела) оборудовано химическим огнетушителем ОП в количестве 1 шт.

Все работники каждый год сдают экзамен по технике безопасности, также принимаются дополнительные меры безопасности: плакаты с напоминанием о необходимости осторожного обращения с огнем, выделенные места для курения и т.д.

Для тушения пожаров и возгораний необходимо установить автоматическую систему пожаротушения на основе спринклерной установки. При возникновении пожара в производственных помещениях, помимо принятия мер по его ликвидации, необходимо также осуществить эвакуацию из опасной зоны работающего персонала. Эвакуация людей осуществляется по эвакуационным путям.

4.2 Технические характеристики оборудования

Технические характеристики рабочих станций (ПК):
- Intel Core(TM) i5-3230M (CPU 3.20 GHz);
- ОЗУ 4 GB;
- HDD 600 Gb;
- габариты: 1200х750х800(персональный компьютер + стол);
- электропитание: переменное напряжение 220-250 В, частотой 50 Гц.
- потребляемая мощность: 500 Вт;

Технические характеристики точек доступа:
- Беспроводная точка доступа Cisco 3500 series;
- Потребляемая мощность:12,95 Вт.

Технические характеристики коммутаторов Cisco Catalyst:
- Cisco 3750X-48PF-S.
- Потребляемая мощность:1100 Вт.

Технические характеристики коммутатора Cisco Nexus 7000:
- Cisco Nexus 7000 series.
- Потребляемая мощность: = 450 Вт.

Технические характеристики маршрутизаторов Cisco ISR G2 3900 series:
- Cisco ISR G2 3925.
- Потребляемая мощность: 105 Вт.

4.3 Расчет зануления

В электроустановках напряжением до 1 кВ с заземленной нейтралью для надежной защиты людей от поражения электрическим током применяется зануление, обеспечивающее автоматическое отключение участка сети, на котором произошел пробой на корпус. Занулением называется преднамеренное электрическое соединение с нулевым защитным проводником металлических не токоведущих частей, которые могут оказаться под напряжением. Защитный эффект от зануления заключается в уменьшении длительности замыкания на корпус, а следовательно, в сокращении времени воздействия электрического тока на человека.

В сетях однофазного тока электрооборудование включается между фазным и нулевым рабочим проводниками. В этом случае зануление осуществляется отдельным проводником, который одновременно не может служить проводником для рабочего тока, так как при обрыве рабочего нулевого проводника (перегорании предохранителя) все присоединённые к нему корпуса окажутся под фазным напряжением. Такое соединение превращает любое замыкание на корпус в короткое замыкание, при котором срабатывает максимальная токовая защита (плавкая вставка или автоматический выключатель), отключая поврежденную электроустановку от сети. На рисунках 4.2 и 4.3 изображены вертикальные и горизонтальные заземления.

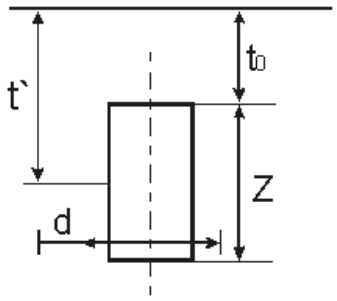

Рисунок 4.2 - Расположение вертикального заземлителя

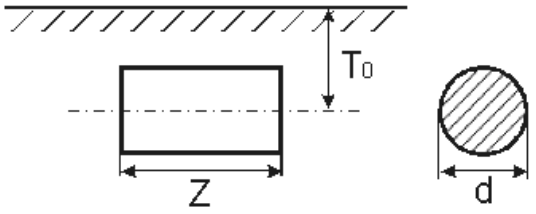

Рисунок 4.3 - Расположение горизонтального заземлителя

Расчет зануления сводиться к определению условий, при которых обеспечиваются быстрое срабатывание максимально-токовой защиты и отключение поврежденной установки от сети.

Для расчета зануления и выбора автоматического выключателя необходимо знать потребляемую мощность и ток каждым электротехническим оборудованием:

- потребляемая мощность компьютера - 450Вт. Переменное напряжение питания 220-250 В. Следовательно, потребляемый ток компьютером составит:

$I_{пк} = 450/220 = 2$ А

- потребляемая мощность точек доступа - 12,95 Вт. Переменное напряжение питания 220-250 В. Следовательно, потребляемый ток точками доступа составит:

$I_{т.д.} = 12,95/220 = 0,05$ А

- потребляемая мощность коммутаторов Cisco Catalyst - 1100 Вт. Переменное напряжение питания 220-250 В. Следовательно, потребляемый ток точками доступа составит:

$I_{к} = 1100/220 = 5$ А

- потребляемая мощность коммутаторов Cisco Nexus - 450 Вт. Переменное напряжение питания 220-250 В. Следовательно, потребляемый ток точками доступа составит:

$I_{кCN} = 450/220 = 2,04$ А

- потребляемая мощность маршрутизаторов Cisco ISRG2 - 105 Вт. Переменное напряжение питания 220-250 В. Следовательно, потребляемый ток точками доступа составит:

$I_{м} = 105/220 = 0,47$А

В помещении работают 6 компьютеров, 2 точки доступа, 10 коммутаторов и 2 маршрутизатора. Следовательно, общая потребляемая мощность составит:

Pn = 6*450 + 9*1100 + 1*450 + 2*12,95 + 2*105 = 2700 + 9900 + 450 +25,9 + 210 = 13285,9 Вт ≈ 13 кВт

Напряжение питания *U*= 220В

Расстояние от щитка до самого удаленного потребителя равно $L = 8$м.

Для электропитания оборудования применен кабель марки ВВГ 3×2,5 (с медными жилами). В кабеле электропитания предусмотрен провод зануления.

Основные технические параметры фазного и нулевого проводов:

- диаметр d=1,8мм;
- сечение S=2,5мм^2.

Расстояние между двумя проводниками (фазный и нулевой провод) соизмеримо с их размерами.

Для надежного отключения аварийного участка необходимо, чтобы ток в короткозамкнутой цепи ($I_{\text{КЗ Н}}$) значительно превосходил ток уставки ($I_{\text{Н}}$) автомата защиты, т.е. должно выполняться неравенство

$$I_{\text{КЗН}} \geq kI_{\text{Н}} \qquad (4.1)$$

где k - коэффициент, при защите автоматическими выключателями с номинальными токами до 100А, k=1,4.

Номинальный ток определяется по формуле:

$$I_{\text{Н}} = \frac{P_{\text{П}}}{\text{U}} \qquad (4.2)$$

Тогда:

$$I_{\text{Н}} = \frac{13 \cdot 10^3}{220} = 59{,}09A$$

Тогда ожидаемый ток короткого замыкания из выражения (4.1) равен:

$$I_{\text{КЗН}} \geq 1{,}4 \cdot 59{,}09 = 82{,}73A$$

Сопротивление фазного $R_ф$и нулевого $R_н$ проводов определяется по следующей формуле:

$$R = \rho \frac{L}{S} \qquad (4.3)$$

где ρ - удельное сопротивление, равное 0,018 Ом*м для меди;

L - длина провода, м;

S - сечение провода, мм^2.

Тогда сопротивление фазного провода равно:

$$R_{ф} = 0{,}018 \frac{8}{1{,}8} = 0{,}08\ Ом$$

Нулевой провод имеет аналогичное исполнение, поэтому его сопротивление совпадает с сопротивление фазного:

$$R_{Н} = R_{\Ф} = 0{,}08\ Ом$$

Внутренние индуктивные сопротивления фазного $X_ф$ и нулевого $X_н$ проводов из меди малы и ими можно пренебречь.

Полное сопротивление цепи «фаза-нуль» определяется следующим образом:

$$Z_{КЗ} = Z_{\Ф} + Z_{Н} + jX_{П} = (R_{\Ф} + R_{Н}) + j(X_{\Ф} + X_{Н} + X_{В}) \qquad (4.4)$$

где $X_п$ - полное индуктивное сопротивление цепи «фаза-нуль»;

$X_в$ - внешнее индуктивное сопротивление цепи «фаза-нуль».

Когда фазный и нулевой проводники расположены в непосредственной близости один от другого, сопротивление $X_в$ мало и им можно пренебречь.

Тогда полное сопротивление $Z_{кз}$ равно:

$$Z_{КЗ} = R_{\Ф} + R_{Н} = 0{,}08 + 0{,}08 = 0{,}16 Ом$$

Ток однофазного короткого замыкания фазы на зануленный корпус определяется как

$$I_{КЗ} = \frac{U_{\Ф}}{\frac{Z_{Т}}{3} + Z_{КЗ}} \qquad (4.5)$$

где $Z_Т$ - полное сопротивление обмоток трехфазных трансформаторов при обмотках низшего напряжения 400/230В.

Схема соединения обмоток трансформатора Δ/Y, мощность трансформатора равна 160 кВА, $Z_Т$ = 0,047 Ом (таблица 4.5).

Т а б л и ц а 4.5 - Приближенные значения полных сопротивлений обмоток масляных трансформаторов Z_T, Ом, при различных схемах соединения обмоток

Мощность трансформатора, кВА	$Z_т/3$, Ом	
	Схема соединения трансформатора	
	звезда/звезда	треугольник/звезда, звезда/зигзаг
25	1.036	0.302
40	0.649	0.187
63	0.412	0.12
100	0.259	0.0754
160	0.162	0.047
250	0.104	0.03
400	0.065	0.019
630	0.043	0.014
1000	0.027	0.009
1600	0.018	0.0056
2500	-	0.0036

Тогда ток короткого замыкания составит:

$$I_{кз} = \frac{220}{\frac{0,047}{3} + 0,16} = 1257,1\ A$$

Выражение (4.1) выполняется для тока короткого замыкания, который значительно превышает номинальный ток (1257,1≥82,73). Таким образом, автоматический выключатель гарантированно сработает и отключит аварийный участок.

Автоматический выключатель выбирается на номинальный ток, полученный из выражения (4.2):

$I_н$ = 59,09 A

Выбирается двухполюсный автоматический выключатель S192 компании ABB.

Технические характеристики:

- номинальный ток $I_н$ =25 А;
- отключающая способность 6 кА;
- номинальное напряжение 230/240В;
- характеристика срабатывания С (I_m=5...10$I_н$), В (I_m=3...5$I_н$).

4.4 Анализ пожарной безопасности

Согласно СНиП 2.02-15-2003 здание по степени опасности развития пожара, от функционального назначения и пожарной нагрузки горючих материалов, относится к 1-ой группе категории Д (помещения, в которых обращаются негорючие вещества и материалы в холодном состоянии.) [21].

Причинами возникновения пожара могут быть:

- Возгорание элементов аппаратуры;
- Возгорание отделочных материалов от неисправных выключателей, розеток.
- Несоблюдение режимов эксплуатации оборудования, неправильное действие персонала.

При возникновении пожара может пострадать не только помещение, но и дорогостоящая аппаратура. Поэтому необходимо чтобы были приняты меры по раннему выявлению и ликвидации пожаров. Источниками зажигания могут оказаться электронные схемы ЭВМ, приборы, применяемые для технического обслуживания, устройства электропитания, кондиционеры воздуха, где в результате различных нарушений образуются перегретые элементы и др.

В соответствии с требованиями правил пожарной безопасности помещение оборудовано углекислотными огнетушителями ОУ-5 с учетом - один огнетушитель на 100 м^2. Общая площадь помещения управления (Рисунок 4.1) составляет 57 м^2,поэтому устанавливаются 1 огнетушитель. В качестве огнетушащего вещества применяется комбинированный углекислотно-хладоновый состав. Расчетная масса комбинированного углекислотно-хладонового состава (кг) для объемного пожаротушения определяется по формуле:

$$m_d = k \cdot g_n \cdot V \qquad (4.6)$$

где k = 1,2- коэффициент компенсации не учитываемых потерь углекислотно-хладонового состава (таблица 4.6),

g_n- нормативная массовая огнетушащая концентрация углекислотно-хладонового состава, принимается 0,27 кг/м^3 при времени заполнения помещения, равном 30 с, и 0,4 кг/м^3 при времени заполнения помещения, равном 60 с;

V - объем помещения.

Таблица 4.6 - Коэффициент компенсации неучитываемых потерь комбинированного состава k

Помещение	Значение коэффициента k
С дверными и оконными проемами	1,13-1,25
Без оконных проемов	1,07-1,15

Объем помещения равен:

$$V = 9{,}5 \cdot 6 \cdot 4 = 228\ м^3$$

Рассчитаем m_d:

$$m_d = 1{,}2 \cdot 0{,}4 \cdot 228 = 10{,}94 \approx 109{,}44\ кг$$

Внутренний диаметр магистрального трубопровода d_i(мм) определяется по формуле:

$$d_i = 12 \cdot \sqrt{2} = 17 мм$$

Эквивалентная длина магистрального трубопроводаl_2(м)определяется по формуле:

$$l_1 = k_1 \cdot l_2 \qquad (4.7)$$

где k_1 = 1,2 - коэффициент увеличения длины трубопровода для компенсации не учитывающих местных потерь (таблица 4.7),

l = 17м - длина трубопровода по проекту, тогда

$$l_1 = 1{,}2 \cdot 17 = 20{,}4 м$$

Т а б л и ц а 4.7 - Коэффициент увеличения длины трубопроводаk_1

Диаметр прохода магистрального трубопровода d, мм	Значение коэффициентаk_1
До 35	1,2
35-50	1,1
Свыше 50	1,05

Расход углекислотно-хладонового состава Q (кг/с) в зависимости от эквивалентной длины и диаметра трубопровода вычислим по графику (Рисунок 4.4).

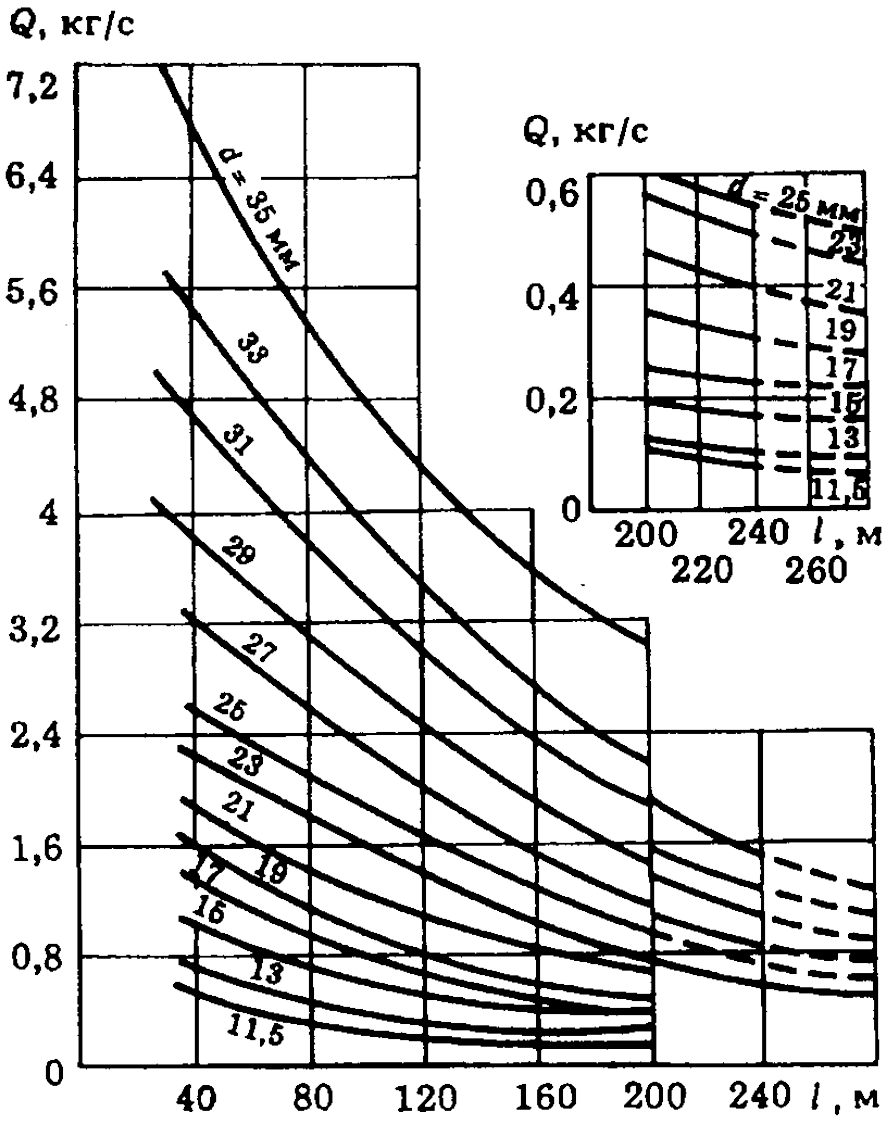

Рисунок 4.4 - График для определения расхода углекислотно-хладонового состава, кг/с

Расход углекислотно-хладонового состава Q по рисунку 4.4 равен 2,0 кг/с.

Расчетное время подачи углекислотно-хладонового состава *t*, мин, определяется по формуле:

$$t = \frac{m_d}{60Q} \tag{4.8}$$

Тогда:

$$t = \frac{109,44}{60 \cdot 2,0} = 0,912 мин \approx 55 сек$$

Масса основного запаса углекислотно-хладонового состава m (кг) определяется по формуле:

$$m = 1{,}1 \cdot m_d \cdot \left(1 + \frac{k_2}{k}\right) \quad (4.8)$$

где k_2- коэффициент, учитывающий остаток углекислотно-хладонового состава в баллонах и трубопроводах (таблица 4.8).

$$m = 1{,}1 \cdot 109{,}44 \cdot \left(1 + \frac{0{,}2}{1{,}2}\right) = 140{,}5\ кг$$

Таблица 4.8 - коэффициент, учитывающий остаток углекислотно-хладонового состава в баллонах и трубопроводах

Диаметр сифонной трубки, мм	Значение коэффициента k_2при длине трубопровода по проекту, м		
	До 100	От 101 до 200	Свыше 200
10	0,2	0,23	0,26
12	0,2	0,25	0,29

Расчетное число баллонов ξ определяется из расчета вместимости в 40-литровый баллон 25 кг углекислотно-хладонового состава. Поэтому для 140,5 кг углекислотно-хладонового состава понадобится:

$$\xi = \frac{140{,}5}{25} = 5{,}62 \approx 6$$

Таким образом, из полученных результатов можно сделать вывод, что для обеспечения нормального функционирования системы автоматического пожаротушения потребуется 6 баллонов углекислотно-хладонового состава вместимостью 40 литров, с массой смеси 140,5 кг. Автоматические установки газового пожаротушения имеют устройства для автоматического пуска в соответствии с ГОСТ 12.4.009-83 [22].

5 Бизнес план

5.1 Резюме

Главной целью данного проекта является модернизация корпоративной сети подразделения Национального Банка РК с использованием архитектуры «Сети без границ», разработанной компанией Cisco. Основой экономической эффективности данной технологии является автоматизация и упрощение некоторых процессов, происходящих в сети, а так же оптимизация и снижение энергопотребления.

5.2 Финансовый план

Этот раздел бизнес-плана является расчётным. Финансовый план включает: расчет величины, определение источника инвестиций, прогноз объема реализации, доходы от продажи товаров или услуг, издержки, прибыль.

5.2.1 Расчет капитальных вложений

Для того, чтобы построить (в нашем случае, модернизировать) сеть, необходимы существенные затраты как на оборудование, так и на монтажные работы по установке оборудования, а так же необходимы затраты на проектирование сети. Расчет капитальных затрат производится по формуле:

$$\Sigma К_{кап} = К_{об} + К_{м} + К_{пр} \quad (5.1)$$

где $К_{м}$ - капитальное вложение на монтаж;

$К_{пр}$ - капитальное вложение на проектирование сети;

$К_{об}$ - капитальное вложение на приобретение оборудования;

$К_{т}$ - капитальные вложения на транспортные расходы;

Транспортные расходы включены в стоимость оборудования [14].

На осуществление данного проекта необходимо задействовать следующие виды наименования оборудования и комплектующих, общей стоимостью 3 658 815 тенге:

Стоимость устанавливаемого оборудования и комплектующих сети отражены в таблице D1.

5.2.2 Расчет стоимости монтажа

Для подключения оборудования необходимо провести монтажные работы. Данные работы будет производить сторонняя организация. Общая стоимость монтажных работ составляет 265 000тенге. Виды проведенных работ и их стоимость отражены в таблице D2.

5.2.3 Расчет затрат на проектирование сети

В состав затрат на проектирование сети входят следующие статьи затрат:
- заработная плата разработчиков;
- социальный налог;
- электроэнергия;
- накладные расходы.

Расходы на проектирование рассчитываются по формуле:

$$К_{ПР} = ФОТ + О_С + Н + М \quad (5.2)$$

где ФОТ - фонд оплаты труда;

Ос - отчисления на социальные нужды;

Н - накладные расходы;

М - расходы на материалы

5.2.4 Расчет затрат на материалы для проектирования сети

К затратам на материалы относятся все затраты на магнитные носители данных, бумагу на печатающих устройствах и другие материалы, необходимые для разработки проекта. В ходе разработки проекта были использованы следующие материалы:

– бумага;
– картридж принтера;
– CD диски.

Общая стоимость материалов составляет 29600 тенге. Виды материалов и их стоимость отражены в таблице D3.

5.2.5 Расходы на оплату труда

Расходы на оплату труда включают в себя затраты на основную и дополнительную заработную плату и рассчитывается по формуле:

$$ФОТ = З_{ОСН} + З_{ДОП} \quad (5.3)$$

Основная заработная плата определяется как сумма оплаты труда всех исполнителей:

$$З_{ОСН} = \sum_{i=1}^{n} З_i \cdot Т_i \quad (5.4)$$

где $З_i$ - зарплата i-го работника в день, тенге;

$Т_i$ - затраты времени i-го работника, дней.

Дополнительная заработная плата составляет 10% от основной заработной платы и рассчитывается по формуле:

$$З_{ДОП} = 0,1*З_{ОСН} \quad (5.5)$$

Труд разработчиков оплачивается согласно штатному расписанию. Количество исполнителей и размер месячной заработной платы представлены таблице D4.

Стоимость человека-дня вычисляется по формуле:

$$Д = \frac{ЗПм}{Др} \quad (5.6)$$

где $ЗП_м$ - заработная плата за месяц, тенге;

$Д_р$ - среднемесячное количество рабочих дней.

Среднемесячное количество рабочих дней - 24.

Стоимость человека-дня для инженера:

$$Д = \frac{200000}{24} = 8333 \text{ тенге}$$

Стоимость человека-дня для главного инженера:

$$Д = \frac{260000}{24} = 10833 \text{ тенге}$$

Стоимость человека-дня для руководителя проекта:

$$Д = \frac{250000}{24} = 10416 \text{ тенге}$$

На основе данных стоимости одного человека-дня и продолжительности выполнения каждого этапа разработки рассчитываем затраты на оплату труда для каждой категории работников (таблица D5).

Основная заработная плата определяется как сумма оплаты труда всех разработчиков:

$$З_{ОСН} = \sum_{i=1}^{n} (Зi \cdot Ti) = 416650 + 416650 + 416650 + 541650 + 520800 = 2312400 тенге$$

Дополнительная заработная плата составляет 10 % от основной заработной платы:

$$З_{ДОП} = 0,1 \cdot З_{ОСН} = 0,1 \cdot 2312400 = 231240 тенге$$

Суммарный фонд оплаты труда (ФОТ) составит:

ФОТ = 2 312 400 + 231 240 = 2 543 640 тенге

5.2.6 Расчет социальных отчислений

В соответствии со статьей 385 Налогового кодекса РК социальный налог составляет 11% от начисленных доходов и рассчитывается по формуле:

$$Oc = 0{,}11 \cdot (ФОТ - ПО) \tag{5.7}$$

где ПО - отчисления в пенсионный фонд, тенге;
ФОТ - фонд оплаты труда, тенге;
0,11 - ставка на социальные нужды.

Отчисления в пенсионный фонд составляют 10% от ФОТ, социальным налогом не облагаются и рассчитываются по формуле:

$$ПО = 0{,}1 \cdot ФОТ \tag{5.8}$$

Поэтому:

$$ПО = 0{,}1 \cdot 2543640 = 253464 тенге$$

Тогда социальный налог будет равен:

$$Oc = 0{,}11 \cdot (2543640 - 253464) = 251920 тенге$$

5.2.7 Расчет накладных расходов

Накладные расходы составляют 25% от общей суммы понесенных расходов и рассчитываются по формуле

$$H = 0{,}25 \times (ФОТ + Oc + M) \tag{5.9}$$

Поэтому:

$$H = 0{,}25 \times (2543640 + 251920 + 45800) = 710340 тенге$$

Результаты расчетов затрат на проектирование сети представлены в таблице D6.

Суммарные затраты на проектирование сети и в соответствии с приведенной формулой (5.2) и расчетами составляют:

$$К_{ПР} = 2543640 + 251920 + 710340 + 45800 = 3551700 тенге$$

Общая сумма капитальных затрат в соответствии с формулой 5.1 составит:

$\Sigma К_{кап}$ = 3 658 815+ 265 000 + 3 551 700 = 7 475 515 тенге

5.3 Эксплуатационные издержки

Текущие затраты на эксплуатацию определяются по формуле:

$$Э_Р = ФОТ + О_С + А_О + Э + Н \quad (5.10)$$

где ФОТ - фонд оплаты труда;

$О_С$ - отчисления на соц. нужды;

$А_О$ - амортизационные отчисления;

Э - электроэнергия для производственных нужд;

Н - накладные затраты.

Стоимость поддержки устройства защиты состоит из следующих составляющих:

1) Заработная плата инженера;

Поддерживать устройства защиты будет инженер. С модернизацией сети упрощается эксплуатация оборудования и сети становится значительно проще сопровождать, поэтому штат сотрудников сокращается на 2 единицы (таблица 5.4).

Заработная плата инженера представлена в таблице D4, поэтому годовая заработная плата равна:

$Зр_и$ = 200 000*12 = 2 400 000 тенге

2) Социальные отчисления

Согласно формуле (5.8) пенсионные отчисления будут равны:

$$ПО = 2400000 \cdot \frac{10\%}{100\%} = 240000 \text{ тенге}$$

Согласно формуле (5.7), социальный налог составит:

$$Ос = 0{,}11 \cdot (2400000 - 240000) = 237600 \text{ тенге}$$

3) Затраты на электроэнергию рассчитываются по формуле:

$$З_{ЭЛ.ЭН.} = W \cdot T \cdot S \quad (5.11)$$

где *W*- потребляемая мощность, составляет 90 000 Вт;

S - стоимость киловатт-часа электроэнергии составляет 14,36 тенге.

T - время работы оборудования;

С учетом внедрения новой технологии, оборудование будет работать не круглосуточно, а в зависимости от положений корпоративной политики предприятия (в нашем случае, время работы оборудования составляет 10 часов, а так же учет выходных дней, когда неосновное оборудование не потребляет энергии). Время работы рассчитывается по формуле:

$$\mathrm{T} = T_1 * T_2 \tag{5.12}$$

где T_1 - время работы оборудования в день, часы;

T_2 - количество дней.

Поэтому, по формуле 5.12, время работы оборудования составит:

$$\mathrm{T} = 10 \cdot (365 - 90) = 2750 \text{ часов}$$

В соответствии с формулой (5.11) расходы на электроэнергию составят (расчетный период):

$$З_{эл.эн.} = 90000 \cdot 2750 \cdot 14{,}36 = 3554100 \text{ тенге}$$

До внедрения данной технологии время работы оборудования составляло:

$$\mathrm{T} = 24 * 365 = 8760 \text{ часов}$$

А затраты на потребление энергии составляли (базовый период):

$$З_{эл.эн.} = 90000 \cdot 8760 \cdot 14{,}36 = 11321424 \text{ тенге}$$

4) Амортизационные отчисления берутся исходя из того, что норма амортизации на оборудование связи составляет 10% и вычисляются по следующей формуле

$$A_0 = H_A \cdot \sum K \tag{5.13}$$

где H_A-норма амортизации;

∑К - стоимость оборудования.

Поэтому:

$$A_0 = H_A \cdot \sum K = 0{,}1 \cdot 7475515 = 747551 \text{ тенге}$$

5) Накладные расходы составляют 50% от ФОТ и рассчитываются по формуле:

$$H = 0{,}5 \cdot ФОТ \qquad (5.14)$$

Тогда накладные затраты составят:

$H = 0{,}5 \cdot 2400000 = 1200000$ тенге

Таким образам, эксплуатационные издержки составят:

Э = 2 400 000 + 240 000 + 747 551+ 3 554 100 + 1 200 000= 8 141 651 тенге

Ниже приведена таблица эксплуатационных издержек до модернизации сети и после модернизации сети:

Т а б л и ц а 5.1 - Годовые эксплуатационные издержки

До модернизации			После модернизации		
Наименование статей	Сумма, тенге	%	Наименование статей	Сумма, тенге	%
ФОТ	7 200 000	31,10	ФОТ	2 400 000	29,49
Отчисления на социальные нужды (Ос)	712 800	3,08	Отчисления на социальные нужды (Ос)	237 600	2,92
Амортизационные отчисления ($А_0$)	315 680	1,36	Амортизационные отчисления ($А_0$)	747 551	9,18
Затраты на электроэнергию (Э)	11 321 424	48,90	Затраты на электроэнергию (Э)	3 554 100	43,67
Накладные расходы (Н)	3 600 000	15,55	Накладные расходы (Н)	1 200 000	14,74
ИТОГО	23 149 904	100,00	ИТОГО	8 139 251	100,00

Ниже приведена сравнительная диаграмма годовых эксплуатационных расходов до модернизации и после модернизации сети:

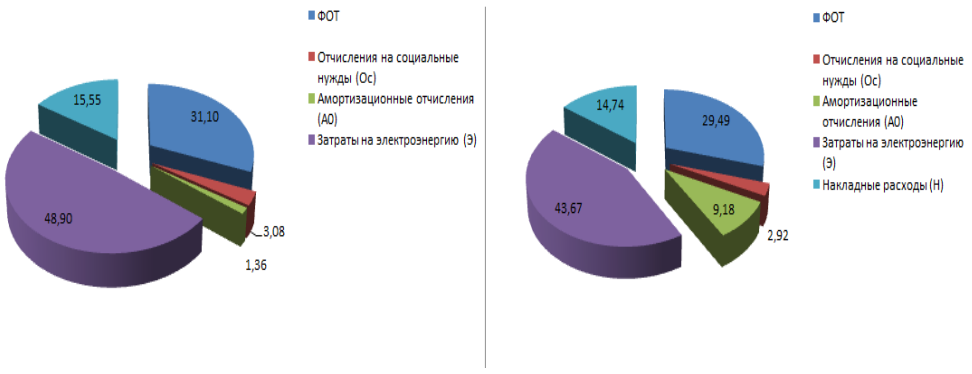

Рисунок 5.1 - Структура эксплуатационных расходов

5.4 Оценка эффективности реализации проекта

Оценка эффективности от реализации проекта производится на основе следующих показателей [15]:

1. Чистый доход;
2. Чистый приведенный доход;
3. Срок окупаемости без дисконтирования;
4. Срок окупаемости с учетом дисконтирования.

Рассчитаем условный доход, полученный от модернизации сети предприятия.

Условный доход получим путем сокращения обслуживающего технического персонала на две штатные единицы, а так же путем сокращения затрат по пункту «затраты на электроэнергию» в эксплуатационных издержках.

Заработная плата инженера в месяц 200 000 тенге (согласно таблице D4). Тогда условный доход за год получим [16]:

$Д_1$ = (200 000*2)*12 = 4 800 000 тенге

Условный доход за год за счет сокращения затрат на электроэнергию:

$Д_2$ = 11 321 424 - 3 554 100= 7 767 324 тенге

Суммарный условный годовой доход равен:

$$Д = Д_1 + Д_2 \quad (5.15)$$

Тогда:

Д = 4 800 000 + 7 767 324 = 12 567 324 тенге

Для расчета срока окупаемости необходимо определить чистый доход. Чистая прибыль от реализации услуг определяется по формуле:

$$ЧП = П - КПН \quad (5.16)$$

где П- прибыль;

КПН - корпоративный подоходный налог.

Сумма налога в бюджет составляет 20% от чистого дохода предприятия. Чистый доход предприятия после налогообложения рассчитывается по формуле:

$$КПН = 0{,}2 \cdot П \quad (5.17)$$

Прибыль от реализации услуг рассчитывается по формуле:

$$П = Д - \sum Э \qquad (5.18)$$

где Д - реальный доход от внедрения услуг в год,

∑Э - эксплуатационные расходы

Прибыль от реализации услуг в соответствии с формулой (5.18) составит:

$$П = 12567324 - 8139251 = 4\,428\,073 \text{ тенге}$$

КПН в соответствии с формулой (5.18) составит:

$$КПН = 0{,}2 \cdot (12567324 - 8139251) = 885\,614 \text{ тенге}$$

Тогда чистая прибыль после налогообложения в соответствии с формулой (5.17) составит:

$$ЧП = 4428073 - 885614 = 3\,542\,459 \text{ тенге}$$

Т а б л и ц а 5.2 - Показатели эффективности без учёта дисконтирования

Наименование показателя	Годы						
	1	2	3	4	5	6	7
Доходы, тенге	12 567 324	12 567 324	12 567 324	12 567 324	12 567 324	12 567 324	12 567 324
Эксплуатац. расходы, тенге	8 139 251	8 139 251	8 139 251	8 139 251	8 139 251	8 139 251	8 139 251
Прибыль, тенге	4 428 073	4 428 073	4 428 073	4 428 073	4 428 073	4 428 073	4 428 073
Чистая прибыль, тенге	3 542 459	3 542 459	3 542 459	3 542 459	3 542 459	3 542 459	3 542 459
Амортизация, тенге	747 551	747 551	747 551	747 551	747 551	747 551	747 551
Чистый денежный поток нарастающим итогом, тенге	4 290 010	12 870 030	25 740 060	42 900 100	64 350 150	90 090 210	120 120 280
Капитальные вложения, тенге	7 475 515	-	-	-	-	-	-
Чистые поступления, тенге	-3 185 505	5 394 515	18 264 545	35 424 585	56 874 635	82 614 695	112 644 765

По графику на рисунке 5.2 графически определим срок окупаемости средств, вложенных в проект. Без дисконтирования срок окупаемости проекта составит 2,2 года. График построен по данным таблицы 5.2

Для приведения разновременных затрат к единому моменту времени необходимо произвести оценку эффективности проекта на основе показателей чистого приведенного дохода и срока окупаемости с учетом дисконтирования.

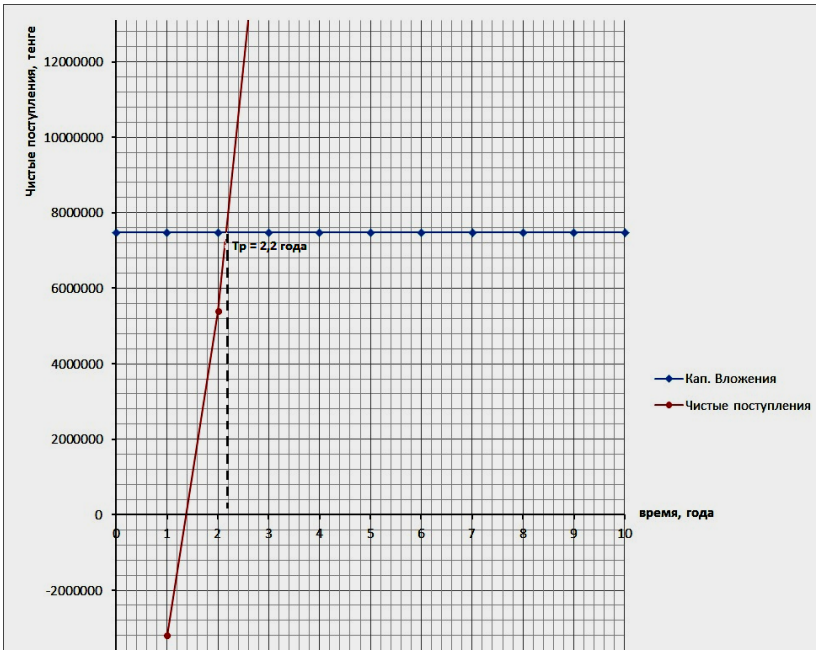

Рисунок 5.2 - График срока окупаемости проекта без учета дисконтирования

Приведенный чистый доход рассчитывается по формуле:

$$ПЧД = Кпр \cdot ЧД \qquad (5.19)$$

где ЧД - чистый доход от внедрения проекта.

$К_{ПР}$ - коэффициент дисконтирования, который рассчитывается по формуле:

$$Кпр = 1/(1+r)^t \qquad (5.20)$$

где *t*- год после внедрения проекта;

r - ставка дисконта принимаем равную 10% или 0,10

Коэффициент дисконтирования для 7 лет:

Для 1 года:

$$Кпр_1 = 1/(1+0.10)^1 = 0.9$$

Для 2 лет:

$$Кпр_2 = 1/(1+0.1)^2 = 0.82$$

Для 3 лет:

$$Кпр_3 = 1/(1+0.1)^3 = 0.75$$

Для 4 лет:

$$Knp_4 = 1/(1+0.1)^4 = 0.68$$

Для 5 лет:

$$Knp_5 = 1/(1+0.1)^5 = 0.62$$

Для 6 лет:

$$Knp_6 = 1/(1+0.1)^6 = 0.56$$

Для 7 лет:

$$Knp_7 = 1/(1+0.1)^7 = 0.51$$

Результаты расчета показателей дохода с дисконтированием представлены в таблице 5.3.

Т а б л и ц а 5.3 - Показатели эффективности с учетом дисконтирования

Наименование показателя	Годы						
	1	2	3	4	5	6	7
Доходы, тенге	12 567 324	12 567 324	12 567 324	12 567 324	12 567 324	12 567 324	12 567 324
Эксплуатац. расходы, тенге	8 139 251	8 139 251	8 139 251	8 139 251	8 139 251	8 139 251	8 139 251
Прибыль, тенге	4 428 073	4 428 073	4 428 073	4 428 073	4 428 073	4 428 073	4 428 073
Чистая прибыль, тенге	3 542 459	3 542 459	3 542 459	3 542 459	3 542 459	3 542 459	3 542 459
Амортизация, тенге	747 551	747 551	747 551	747 551	747 551	747 551	747 551
Чистый денежный поток, тенге	4 290 010	8 580 020	12 870 030	17 160 040	21 450 050	25 740 060	30 030 070
$К_{ПР}$	0,9	0,82	0,75	0,68	0,62	0,56	0,51
Приведенный ЧД с учетом дисконтирования, тенге	3 861 009	10 896 625 ,4	20 549 147, 9	32 217 975 ,1	45 517 006 ,1	59 931 439 ,7	75 246 775 ,4
Капитальные вложения, тенге	7 475 515	-	-	-	-	-	-
Чистые поступления, тенге	-3 614 506	3 421 110, 4	13 073 632, 9	24 742 460 ,1	38 041 491 ,1	52 455 924 ,7	67 771 260 ,4

По графику на рисунке 5.3 графически определяется срок окупаемости капиталовложений с учётом дисконтирования, который составил 2,4 года. График построен на основании данных таблицы 5.3.

Коэффициент экономической эффективности проекта рассчитывается по формуле:

$$Ер = \frac{(Д - Э)}{Кв} \quad (5.21)$$

Тогда:

$$Ер = \frac{12567324 - 8139251}{7475515} = 0.59$$

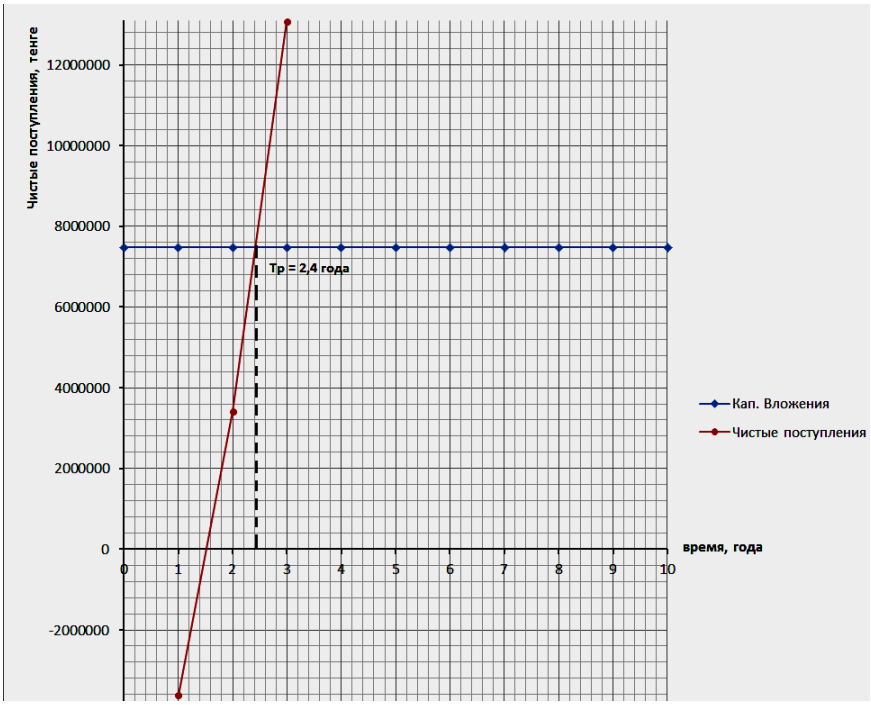

Рисунок 5.3 - График срока окупаемости проекта с учетом дисконтирования

Рассчитаем ЧДД по формуле:

$$ЧДД = \sum_{t=0}^{T} (P_t - З_t) * \frac{1}{(1+E)^t} - K \quad (5.22)$$

Тогда ЧДД равен:

$$ЧДД = \frac{12567324}{1,1} + \frac{12567324}{(1,1)^2} + \frac{12567324}{(1,1)^3} - 7475515 = 23777559,6 \text{ тенге}$$

Чтобы определить, сможет ли текущий доход от проекта покрыть капитальные вложения в него, необходимо рассчитать индекс доходности:

$$ИД = \frac{1}{K} \times \sum_{t=0}^{T} (P_t - З_t) * \frac{1}{(1+r)^t} \quad (5.23)$$

Рассчитаем ИД по формуле (5.23):

$$ИД = \frac{23777559,6}{7475515} = 3,18$$

Инвестиции считаются эффективными, если индекс доходности выше единицы, *ИД*>1, следовательно, инвестиции в данный проект эффективны.

Сводные результаты оценки экономической эффективности от внедрения модернизации корпоративной сети Национального Банка РК представлены в таблице 5.4.

Т а б л и ц а 5.4 - Показатели эффективности реализации проекта

Наименование	Значение
1 Капитальные вложения, тенге	7 475 515
2 Годовые эксплуатационные расходы, тенге	8 139 251
3 Условный годовой доход, тенге	12 567 324
4 Коэффициент экономической эффективности, $E_Р$	0,59
5Индекс доходности, ИД	3,18
6 Срок окупаемости без дисконтирования, лет	3,5
7 Срок окупаемости с дисконтированием, лет	6,6

5.5 Вывод

В данной части дипломного проекта был представлен бизнес - план, в котором рассматривался вопрос о разработке архитектуры «Сети без границ» для корпоративной сети банка.

Внедрение данной технологии дает следующие преимущества в работе сети:

- упрощение эксплуатации оборудования, что влечет за собой сокращение численности персонала, а вследствие, и сокращение затрат на заработную плату сотрудников;

- экономия электроэнергии, что так же влечет за собой сокращение расходов на её потребление.

Так же было произведен расчет годовых эксплуатационных издержек до модернизации сети и после модернизации сети, и, как видно из таблицы 5.1, после внедрения данного проекта издержки значительно сократились.

Был рассчитан срок окупаемости данного проекта, который составил $Т_Р$ = 2,2 года без учета дисконтирования и 2,4 года с учетом дисконтирования, кроме этого, был рассчитан индекс доходности, который составил ИД = 3,18 > 1, что свидетельствует о целесообразности внедрения данного проекта.

Заключение

В данной дипломной работе приводится описание и план разработки архитектуры «Сети баз границ» для банковской системы.

В работе были детально изучены схема и топология сети банка, основные её методы защиты и контроля доступа, а так же были рассмотрены устройства защиты, на которых данные политики реализуются. Были рассмотрены основные принципы работы классической архитектуры сети, а так же был рассмотрен новый концептуальный подход к проектированию сети, используя инновационную архитектуру «Сети без границ», разработанной компанией Cisco. Существующая сеть банка была модернизирована путем внедрения в неё сервисов, входящих в состав архитектуры «Сети без границ», таких как Cisco TrustSec и Cisco EnergyWise.

В технико - экономической части были произведены расчеты, такие как затраты на реализацию данного проекта, а так же экономическая эффективность данного проекта. Расчетным путем была доказана выгодность внедрения данного проекта путем сокращения годовых эксплуатационных затрат.

В работе также рассмотрены основные вопросы охраны труда и безопасности жизнедеятельности при работе с сетевым оборудованием. Представлены основные расчеты по работе с пожарной безопасностью, а так же был представлен расчет зануления во избежание перегрева проводников и порчи дорого сетевого оборудования.

Внедрение данных сервисов в банковскую сеть дает следующие преимущества в ее работе:

- контроль всей сети становится намного легче и прозрачнее, так как сервис Cisco TrustSec дает возможность контролировать все устройства в сети, при этом предоставляя подробнейшую информацию о том кто, когда, откуда и как подключился к данной сети - а это значительно упрощает эксплуатацию все корпоративной сети предприятия, требуется меньше трудовых ресурсов, для того чтобы контролировать всю сеть, отпадает возможность создавать сложные политики доступа, покупать огромное количество дорогостоящих файерволов, VPN - концентраторов и т.д. - за всем этим теперь может следить так называемый «мозг» Cisco ISE, который и применяет политик ко всем устройствам в сети и контролирует весь трафик в совокупности с новейшими маршрутизаторами и коммутаторами Cisco;

- сервис Cisco EnergyWise тщательно следит и регулирует энергопотребление во всей сети, а благодаря гибким политикам и новым коммутаторам и маршрутизаторам Cisco, становится возможным управлять всеми устройствами в сети и регулировать потребление энергии всех устройств в сети, что приводит к колоссальной экономии денежных средств на расходы по статье «затраты на электроэнергию».

Список использованной литературы

1 Биячуев Т.А. / под ред. Л.Г.Осовецкого Безопасность корпоративных сетей. - СПб: СПб ГУ ИТМО, 2004. - 161 с.

2 Галицкий А., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети. Анализ технологий и синтез решений. - М.: ДМК Пресс, 2004. - 615

3 Сайт http://gblogs.cisco.com/ru/a-power-of-secure-network-simplifies-adoption-of-new-mobile-devices/

4 Сайт www.cisco.com/go/ trustsec

5 Сайт http://www.cisco.com/assets/cdc_content_elements/flash/netsys/calc/demo.html

6 Сайт http://www.cisco.com/go/energywise

7 Сайт http://www.cisco.com/cisco/web/support/RU/112/1120/1120451_116497-configure-trustsec-00.html

8 Сайт www.cisco.com/go/enterprise

9 Биячуев Т.А. Безопасность корпоративных сетей / под ред. Л.Г.Осовецкого. - СПб: СПб ГУ ИТМО, 2004.- 161 с.

10 А. В. Соколов, В. Ф. Шаньгин. Защита информации в распределенных корпоративных сетях и системах. - М.: ДМК Пресс, 2002. - 656 с.

11 Гайкович В., Першин А. Безопасность банковских электронных систем. - М.:1993.

12 Осовецкий Л.Г., Немолочнов О.Ф., Твердый Л.В., Беляков Д.А.Основы корпоративной теории информации. -СПб: СПбГУ ИТМО, 2004.

13 Сайт http://xgu.ru/wiki/802.1X_%D0%B2_Cisco

14 З.Д. Еркешева, Г.Ш. Боканова. Методические указания к выполнению семестровых работ для студентов специальности 5В070400 - «Вычислительная техника и программное обеспечение». - Алматы: АУЭС, 2013.

15 Брусакова И.А., Чертовской В.Д. Информационные системы и технологии в экономике. - М.: Финансы и статистика, 2007. - 352 с.

16 Голубицкая Е.А. Экономика связи. -М.: Ирмас, 2006.

17 ГОСТ 12.2.032-78 ССБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования. - М.: Издательство стандартов, 1978.

18 СНиП РК 2.04-05-2002 Естественное и искусственное освещение строительные нормы и правила. - А.: Издательство стандартов, 2002.

19 СНиП РК 2.02-05-2002 Пожарная безопасность зданий и сооружений. - А.: Издательство стандартов, 2002.

20 СНиП РК 2.04.05-91 Отопление, вентиляция и кондиционирование. - А.: Издательство стандартов, 1991.

21 СНиП РК 2.02-15-2003 Пожарная автоматика зданий и сооружений. - А.: Издательство стандартов, 2003.

22 ГОСТ 12.4.009-83 Система стандартов безопасности труда. Пожарная техника для защиты объектов. Основные виды. Размещение и обслуживание. - М.: Издательство стандартов, 1983.

Список сокращений

AAA - Authentication, Authorization and Accounting
ACE - Access Control Entries
ACL - Access Control Lists
ACS -Access Control Server
BMS - Building Management System
CTS - Cisco TrustSec
dACL - downloadable Access Control Lists
DHCP - Dynamic Host Configuration Protocol
DMZ - Demilitarized Zone
DTG - Destination Group Tag
EAP - Extensible Authentication Protocol
EAPOL - Extensible Authentication Protocol over LAN
ISE - Identity Services Engine
ISP - Internet Service Provider
IT - Information Technologies
LAN - Local Area Network
MAB - MAC Authentication Bypass
OSI - Open Systems Interconnection
PoE - Power over Ethernet
RADIUS - Remote Authentication in Dial-In User Service
SAP - Security Association Protocol
SGACL - Security Group Access Control Lists
SGT - Security Group Tag
SNMP - Simple Network Management Protocol
UDP - User Datagram Protocol
VLAN - Virtual Local Area Network
VPN - Virtual Private Network
VTP - VLAN Trunking Protocol
WAN - Wide Area Network
ИТ - Информационные Технологии
МВОС - Модель Взаимодействия Открытых Систем
МЭ - Межсетевой Экран
ЦОД - Центр Обработки Данных

Приложение А

Топология сети банка и удаленного филиала (до внедрения Cisco TrustSec и Cisco EnergyWise):

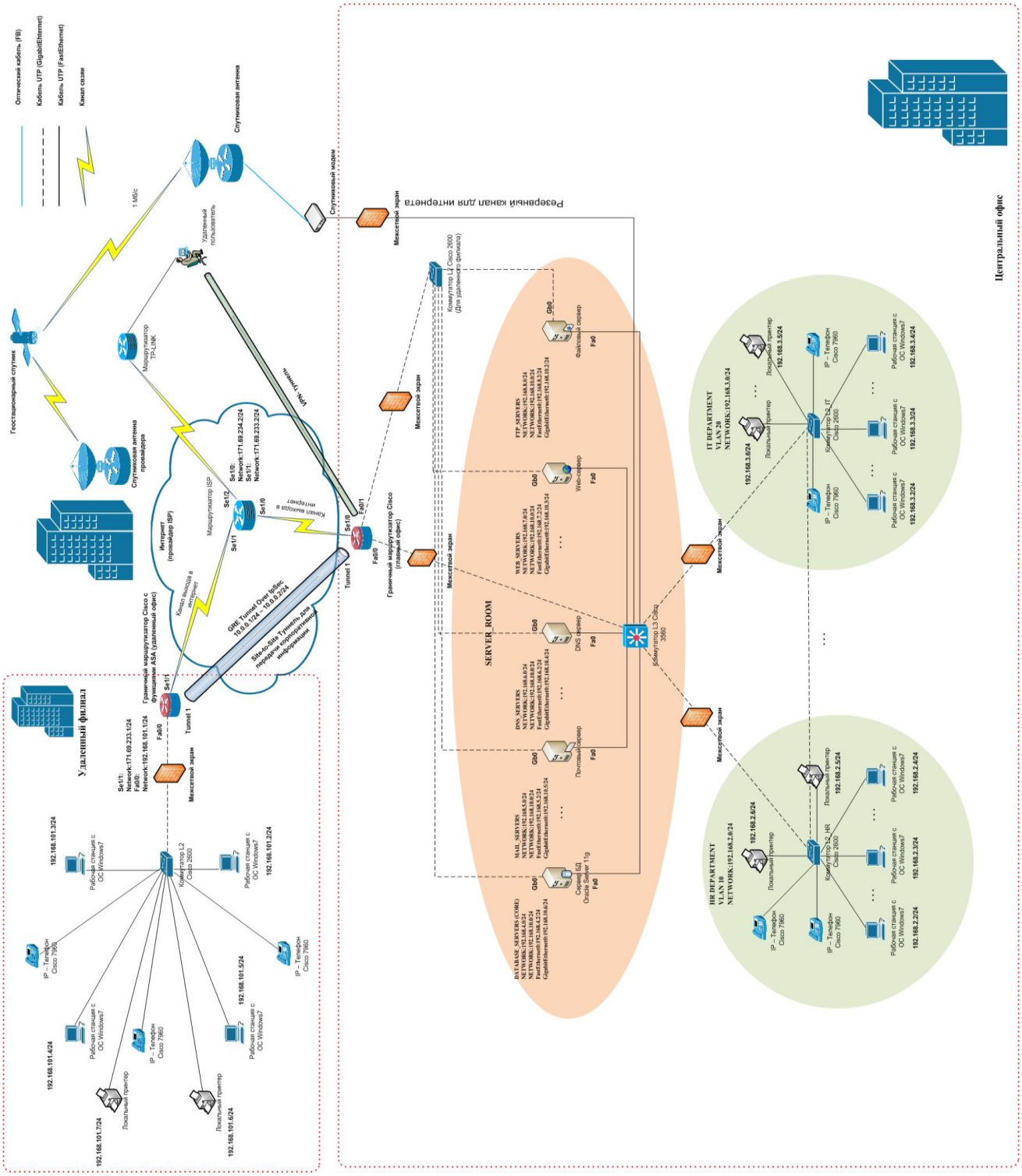

Рисунок А1 - Топология сети банка и удаленного филиала (MS Visio)

Топология сети банка и удаленного филиала, собранная в симуляторе PacketTracer:

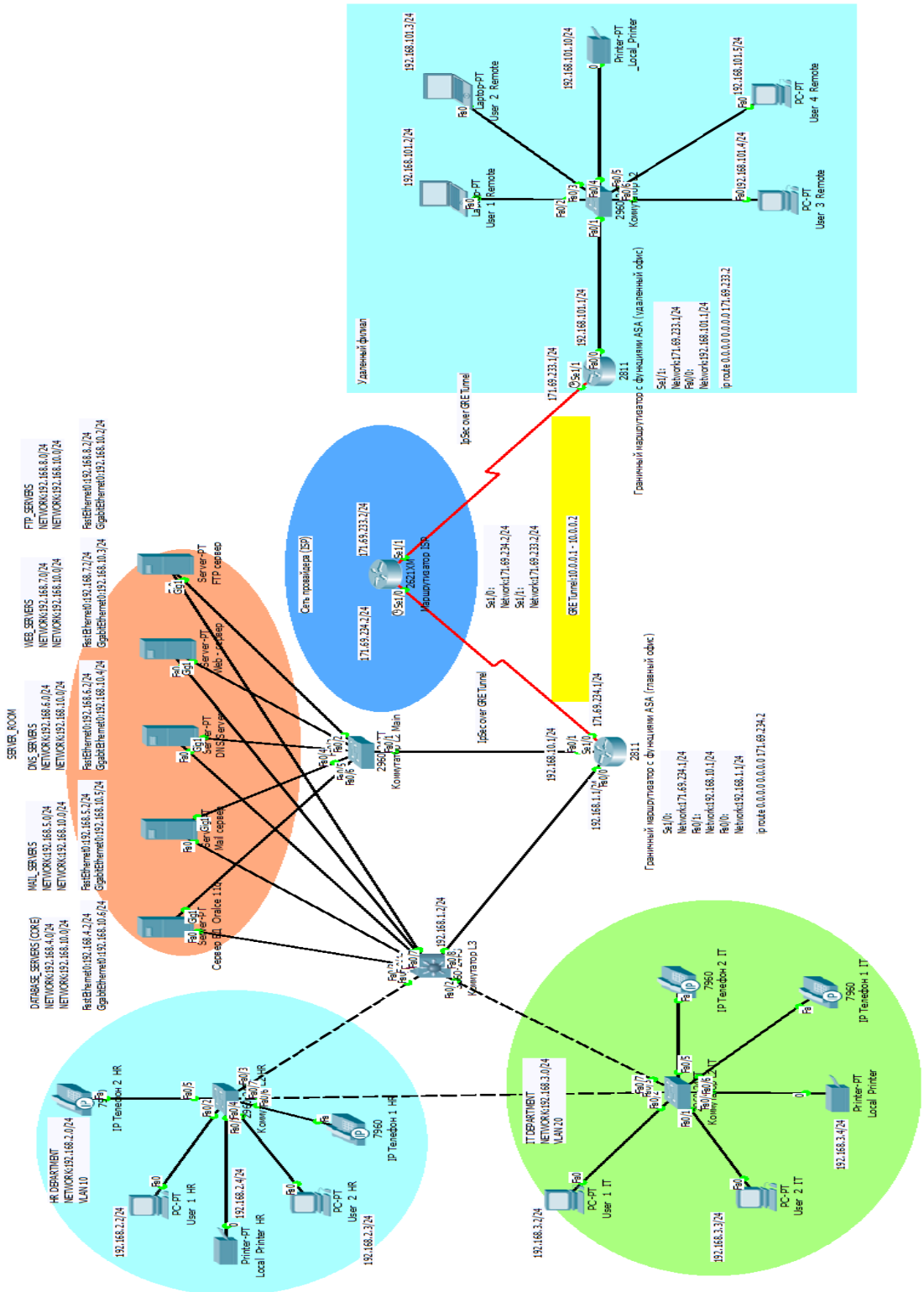

Рисунок А2 - Топология сети банка и удаленного филиала (Cisco PacketTracer)

Настройка и конфигурация сетевого оборудования, маршрутов и протоколов передачи данных:

Коммутатор L2 HR:

```
no service timestamps log datetimemsec
no service timestamps debug datetimemsec
no service password-encryption
!
hostname Switch
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
enable password cisco
!
spanning-tree mode pvst
!
interface FastEthernet0/1
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/2
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/3
switchport trunk allowed vlan 10,20
switchport mode trunk
!
interface FastEthernet0/4
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/5
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/6
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/7
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/8
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/9
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/10
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/11
```

```
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/12
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/13
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/14
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/15
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/16
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/17
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/18
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/19
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/20
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/21
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/22
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/23
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/24
switchport access vlan 10
switchport mode access
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
```

```
interface Vlan1
no ip address
shutdown
!
line con 0
password cisco
login
!
linevty 0 4
password cisco
login
linevty 5 15
password cisco
login
!
End
```

Коммутатор L2_IT:

```
no service timestamps log datetimemsec
no service timestamps debug datetimemsec
no service password-encryption
!
hostname Switch
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
enable password cisco
!
spanning-tree mode pvst
!
interface FastEthernet0/1
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/2
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/3
switchport trunk allowed vlan 10,20
switchport mode trunk
!
interface FastEthernet0/4
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/5
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/6
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/7
switchport access vlan 20
switchport mode access
!
```

```
interface FastEthernet0/8
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/9
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/10
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/11
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/12
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/13
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/14
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/15
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/16
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/17
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/18
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/19
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/20
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/21
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/22
switchport access vlan 20
switchport mode access
```

```
!
interface FastEthernet0/23
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/24
switchport access vlan 20
switchport mode access
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface Vlan1
no ip address
shutdown
!
line con 0
password cisco
login
!
linevty 0 4
password cisco
login
linevty 5 15
password cisco
login
!
End
```

Коммутатор L3:

```
no service timestamps log datetimemsec
no service timestamps debug datetimemsec
no service password-encryption
!
hostname MSW
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
enable password cisco
!
ip routing
!
spanning-tree mode pvst
!
interface FastEthernet0/1
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/2
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/3
noswitchport
ip address 192.168.4.1 255.255.255.0
```

```
duplex auto
speed auto
!
interface FastEthernet0/4
noswitchport
ip address 192.168.5.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/5
noswitchport
ip address 192.168.6.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/6
noswitchport
ip address 192.168.7.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/7
noswitchport
ip address 192.168.8.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/8
noswitchport
ip address 192.168.1.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/9
noswitchport
no ip address
duplex auto
speed auto
shutdown
!
interface FastEthernet0/10
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
```

```
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
ip address 192.168.2.1 255.255.255.0
ip access-group DENY_TELNET_HR in
!
interface Vlan20
ip address 192.168.3.1 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.1.1
ip route 0.0.0.0 0.0.0.0 192.168.10.1
ip route 192.168.1.0 255.255.255.0 192.168.1.1
ip route 192.168.1.0 255.255.255.0 171.69.234.2
!
ip access-list extended DENY_TELNET_HR
permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
permit ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
permit ip 192.168.3.0 0.0.0.255 192.168.3.0 0.0.0.255
permit ip 192.168.3.0 0.0.0.255 192.168.4.0 0.0.0.255
permit ip 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255
permit ip 192.168.3.0 0.0.0.255 192.168.6.0 0.0.0.255
permit ip 192.168.3.0 0.0.0.255 192.168.7.0 0.0.0.255
permit ip 192.168.3.0 0.0.0.255 192.168.8.0 0.0.0.255
permiticmp 192.168.2.0 0.0.0.255 192.168.4.0 0.0.0.255 echo
permiticmp 192.168.2.0 0.0.0.255 192.168.5.0 0.0.0.255 echo
permiticmp 192.168.2.0 0.0.0.255 192.168.6.0 0.0.0.255 echo
permiticmp 192.168.2.0 0.0.0.255 192.168.7.0 0.0.0.255 echo
permiticmp 192.168.2.0 0.0.0.255 192.168.8.0 0.0.0.255 echo
permittcp 192.168.2.0 0.0.0.255 192.168.8.0 0.0.0.255 eq ftp
permittcp 192.168.2.0 0.0.0.255 192.168.5.0 0.0.0.255 eqsmtp
permittcp 192.168.2.0 0.0.0.255 192.168.2.0 0.0.0.255 eqsmtp
permittcp 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255 eqsmtp
permittcp 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255 eq pop3
permittcp 192.168.2.0 0.0.0.255 192.168.2.0 0.0.0.255 eq pop3
permittcp 192.168.2.0 0.0.0.255 192.168.5.0 0.0.0.255 eq pop3
permittcp 192.168.2.0 0.0.0.255 192.168.7.0 0.0.0.255 eq www
permit ip 192.168.2.0 0.0.0.255 192.168.6.0 0.0.0.255
denytcp 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 eq telnet
denytcp 192.168.2.0 0.0.0.255 192.168.2.0 0.0.0.255 eq telnet
```

```
denytcp 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255 eq telnet
denytcp 192.168.2.0 0.0.0.255 192.168.4.0 0.0.0.255 eq telnet
denytcp 192.168.2.0 0.0.0.255 192.168.5.0 0.0.0.255 eq telnet
denytcp 192.168.2.0 0.0.0.255 192.168.6.0 0.0.0.255 eq telnet
denytcp 192.168.2.0 0.0.0.255 192.168.7.0 0.0.0.255 eq telnet
denytcp 192.168.2.0 0.0.0.255 192.168.8.0 0.0.0.255 eq telnet
!
line con 0
password cisco
login
!
line aux 0
!
linevty 0 4
password cisco
login
linevty 5 15
passwordcisco
login
!
End
```

Граничный маршрутизатор с функциями ASA (главный офис):

```
no service timestamps log datetimemsec
no service timestamps debug datetimemsec
no service password-encryption
!
hostname HQ
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
enable password cisco
!
cryptoisakmp policy 1
encr 3des
hash md5
authentication pre-share
group 5
lifetime 3600
!
cryptoisakmp key cisco address 171.69.233.1
!
cryptoipsec transform-set set1 ah-sha-hmac esp-3des
!
crypto map map1 1 ipsec-isakmp
set peer 171.69.233.1
set transform-set set1
match address 101
!
no ip domain-lookup
!
spanning-tree mode pvst
!
interface Tunnel1
ip address 10.0.0.1 255.255.255.0
tunnel source Serial1/0
tunnel destination 171.69.233.1
tunnel mode gre ip
!
```

```
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/0.10
encapsulation dot1Q 10
ip address 192.168.2.1 255.255.255.0
!
interface FastEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.3.1 255.255.255.0
!
interface FastEthernet0/1
ip address 192.168.10.1 255.255.255.0
duplex auto
speed auto
!
interface Serial1/0
ip address 171.69.234.1 255.255.255.0
crypto map map1
!
interface Serial1/1
no ip address
shutdown
!
interface Serial1/2
no ip address
shutdown
!
interface Serial1/3
no ip address
shutdown
!
interface Vlan1
no ip address
shutdown
!
routereigrp 1
network 192.168.10.0
network 10.0.0.0
no auto-summary
!
ip classless
ip route 192.168.101.0 255.255.255.0 10.0.0.2
ip route 0.0.0.0 0.0.0.0 171.69.234.2
!
!
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.101.0 0.0.0.255
!
telephony-service
max-ephones 20
max-dn 4
ip source-address 192.168.1.1 port 2000
auto assign 4 to 6
auto assign 1 to 5
!
ephone-dn 1
number 0001
```

```
!
ephone-dn 2
number 0002
!
ephone-dn 3
number 0003
!
ephone-dn 4
number 0004
!
line con 0
password cisco
login
!
line aux 0
!
linevty 0 4
password cisco
login
linevty 5 15
password cisco
login
!
End
```

Маршрутизатор ISP:

```
no service timestamps log datetimemsec
no service timestamps debug datetimemsec
no service password-encryption
!
hostname ISP
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
enable password cisco
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial1/0
ip address 171.69.234.2 255.255.255.0
!
interface Serial1/1
ip address 171.69.233.2 255.255.255.0
!
interface Serial1/2
no ip address
shutdown
!
```

```
interface Serial1/3
no ip address
shutdown
!
ip classless
!
line con 0
password cisco
login
!
line aux 0
!
linevty 0 4
password cisco
login
linevty 5 15
passwordcisco
login
!
End
```

Граничный маршрутизатор с функциями ASA (удаленный офис):

```
no service timestamps log datetimemsec
no service timestamps debug datetimemsec
no service password-encryption
!
hostnameRemote_Router
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
enable password class
!
cryptoisakmp policy 1
encr 3des
hash md5
authentication pre-share
group 5
lifetime 3600
!
cryptoisakmp key cisco address 171.69.234.1
!
cryptoipsec transform-set set2 ah-sha-hmac esp-3des
!
crypto map map2 1 ipsec-isakmp
set peer 171.69.234.1
set transform-set set2
match address 101
!
spanning-tree mode pvst
!
interface Tunnel1
ip address 10.0.0.2 255.255.255.0
tunnel source Serial1/1
tunnel destination 171.69.234.1
tunnel mode gre ip
!
```

```
interface FastEthernet0/0
ip address 192.168.101.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial1/0
no ip address
shutdown
!
interface Serial1/1
ip address 171.69.233.1 255.255.255.0
crypto map map2
!
interface Serial1/2
no ip address
shutdown
!
interface Serial1/3
no ip address
shutdown
!
interface Vlan1
no ip address
shutdown
!
routereigrp 1
network 10.0.0.0
network 192.168.101.0
no auto-summary
!
ip classless
ip route 192.168.10.0 255.255.255.0 10.0.0.1
ip route 0.0.0.0 0.0.0.0 171.69.233.2
!
access-list 101 permit ip 192.168.101.0 0.0.0.255 192.168.10.0 0.0.0.255
!
line con 0
password cisco
login
!
line aux 0
!
linevty 0 4
password cisco
login
linevty 5 15
password cisco
login
!
End
```

Коммутатор L2_Main:

```
no service timestamps log datetimemsec
no service timestamps debug datetimemsec
no service password-encryption
!
hostname Switch
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
enable password cisco
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
```

```
!
interface FastEthernet0/24
!

interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface Vlan1
no ip address
shutdown
!
!
line con 0
password cisco
login
!
linevty 0 4
password cisco
login
linevty 5 15
password cisco
login
!
!
End
```

Коммутатор L2 удаленный:

```
no service timestamps log datetimemsec
no service timestamps debug datetimemsec
no service password-encryption
!
hostname Switch
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
enable password class
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
```

```
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!

interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface Vlan1
no ip address
shutdown
!
line con 0
password cisco
login
!
linevty 0 4
password cisco
login
linevty 5 15
passwordcisco
login
!
End
```

Настройка почтового сервера (на рисунке А2 - Mail сервер):

Для каждого пользователя из HR департамента и из IT-департамента задаем имя пользователя и пароль (Рисунок А3).

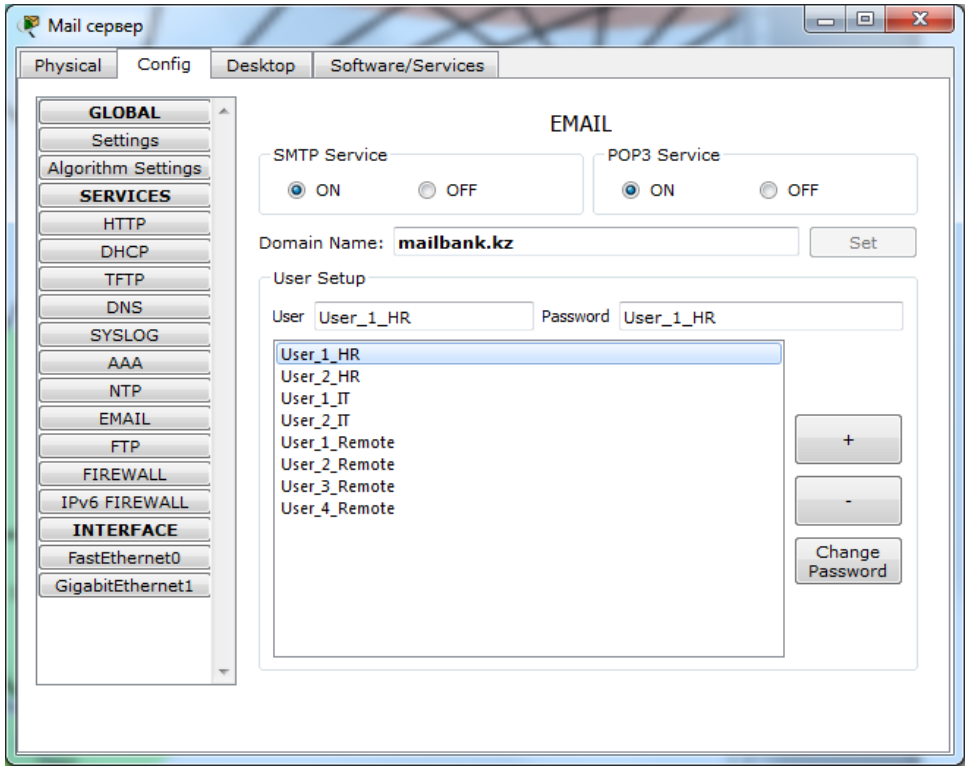

Рисунок А3 - Настройки Mail сервера

Настройка DNS - сервера (на рисунке А2 - DNS сервер).

Для каждого имени задаем адрес, чтобы обращаться к какому - либо серверу по имени, а не по ip-адресу (Рисунок А4).

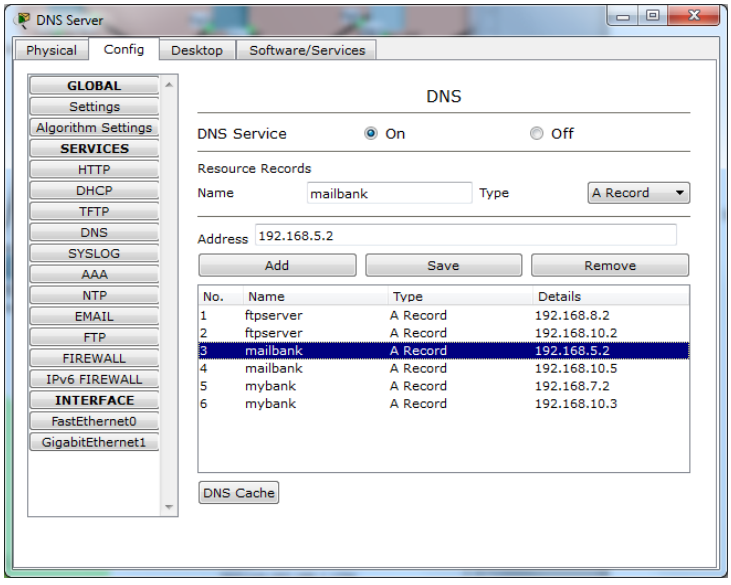

Рисунок А4 - Настройка DNS- сервера

Настройка FTP - сервера (на рисунке А2 - FTP сервер):

Для каждого пользователя назначаем права доступа к FTP-серверу (Рисунок А5).

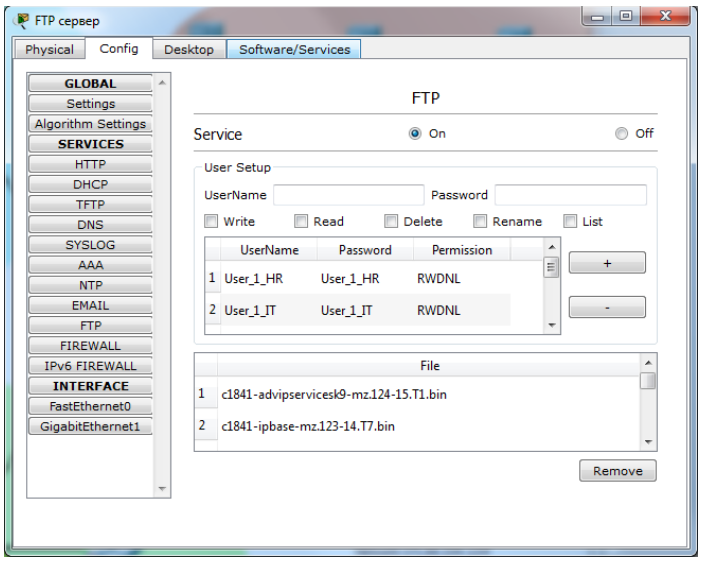

Рисунок А5 - Настройка FTP - сервера

Настройка почтового клиента на рабочей станции HRDEPARTMENTUser_1_HR (остальные настраиваются аналогичным образом) (Рисунок А6).

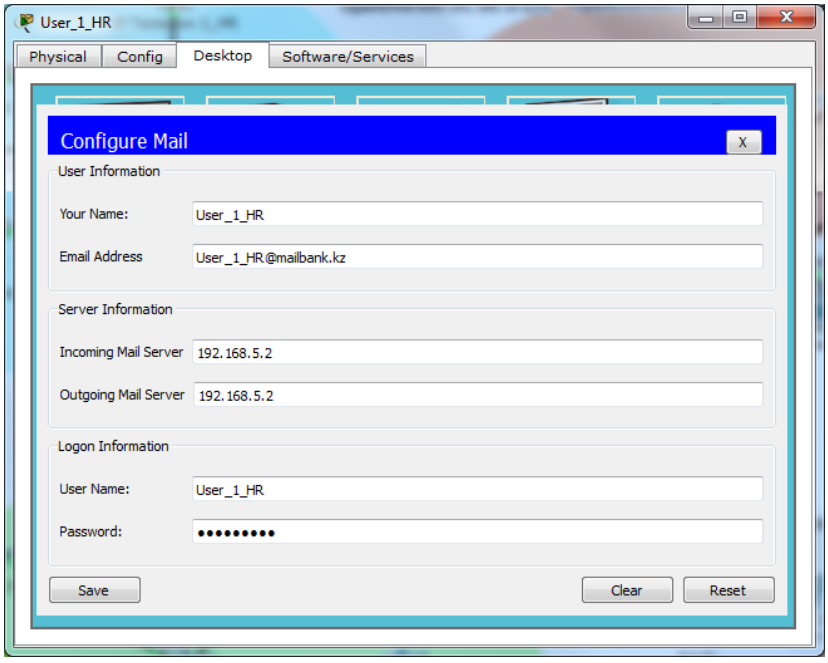

Рисунок А6 - Настройка почтового клиента

В поле Email Address указываем имя пользователя + домен, который мы настроили на сервере DNS.

В поле User Name и Password указываем соответственно имя пользователя и пароль, который мы создали на почтовом сервере (Mail сервер).

Приложение В

Топология сети банка и удаленного филиала (после внедрения Cisco TrustSec и Cisco EnergyWise) изображена на рисунке В1.

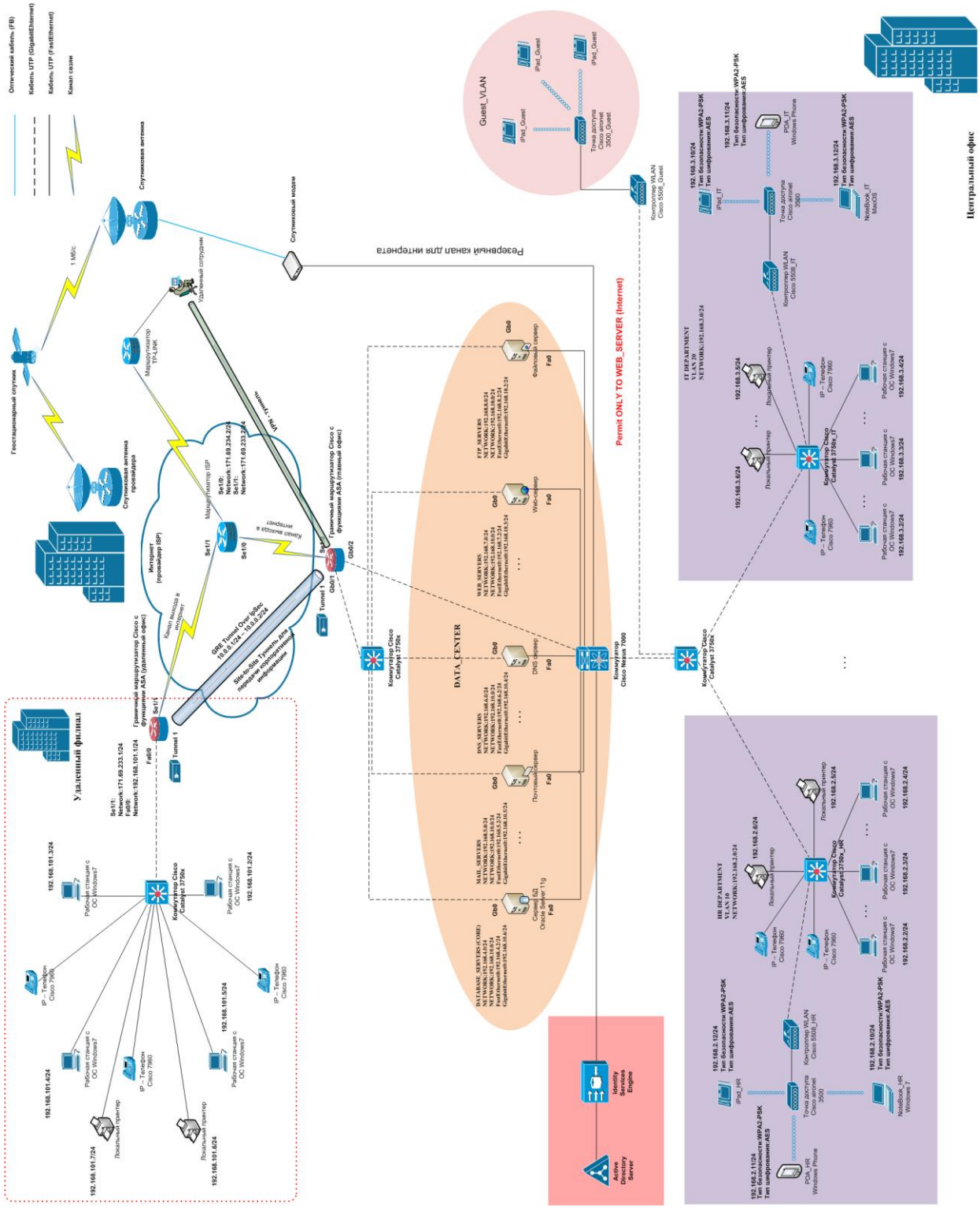

Рисунок В1 - Разработка архитектуры «сети без границ» для банка

Топология архитектуры «сети без границ» для банка, собранная в симуляторе PacketTracer, изображена на рисунке В2.

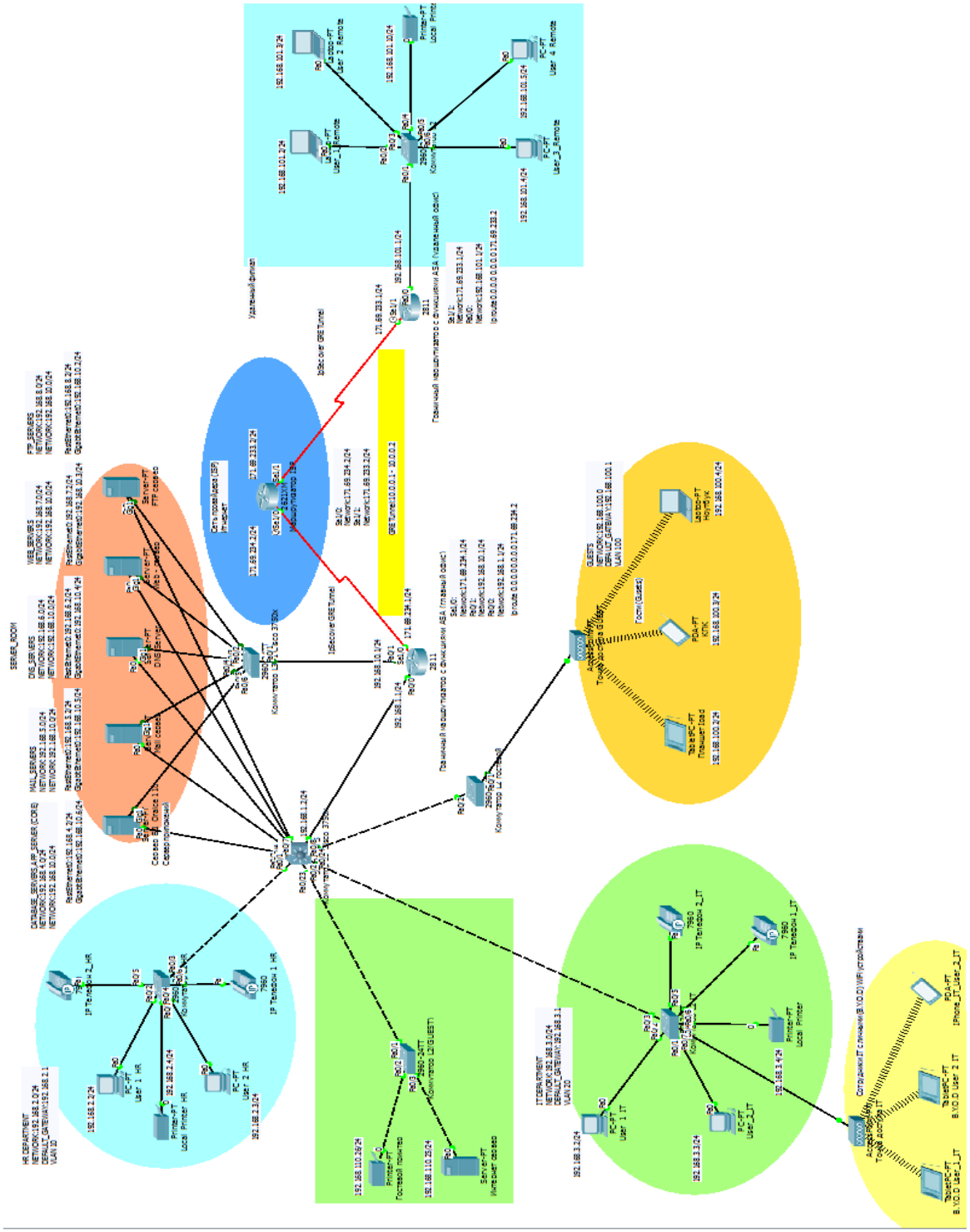

Рисунок В2 - Разработка архитектуры «сети без границ» для банка (Cisco PacketTracer)

Основные настройки остаются как в приложении А, за исключением настроек коммутаторов 3750X_HRи 3750X_IT (Рисунок В1).

Настройка Flexible Authenticationна портах коммутатора (в роли RADIUS-сервера выступает единая платформа ISE):

Коммутатор 3750X_HR:

```
switch# configure terminal
switch(config)# ip radius source-interface GigabitEthernet1/1
switch(config)#aaa new-model
switch(config)# aaa authentication dot1x default group Rad1
switch(config)# aaa authorization cts default group Rad1
switch(config)#dot1x system-auth-control
switch(config)#interface GigabitEthernet2/1
switch(config-if)# authentication port-control auto
switch(config)# interface GigabitEthernet2/1
switch(config-if)# authentication port-control auto
switch(config-if)# mab
switch(config)# ip http server
switch(config)# ip access-list extended POLICY
switch(config-ext-nacl)# permit udp any anyeqbootps
switch(config-ext-nacl)# permit udp any anyeq domain
switch(config)# ip admission name HTTP proxy http
switch(config)# fallback profile FALLBACK_PROFILE
switch(config-fallback-profile)# ip access-group POLICY in
switch(config-fallback-profile)# ip admission HTTP
switch(config)# interface GigabitEthernet2/1
switch(config-if)# authentication port-control auto
switch(config-if)#authentication fallback FALLBACK_PROFILE6500
switch(config-if)#ip access-group POLICY in
switch(config)# interface gigabitEthernet 2/1
switch(config-if)# authentication order mab dot1x webauth
switch(config)#copy running-config startup-config
switch(config)#exit
```

Коммутатор 3750X_IT:

```
switch# configure terminal
switch(config)# ip radius source-interface GigabitEthernet1/1
switch(config)# aaa new-model
switch(config)# aaa authentication dot1x default group Rad1
switch(config)# aaa authorization cts default group Rad1
switch(config)#dot1x system-auth-control
switch(config)#interface GigabitEthernet2/1
switch(config-if)# authentication port-control auto
switch(config)# interface GigabitEthernet2/1
switch(config-if)# authentication port-control auto
```

```
switch(config-if)# mab
switch(config)# ip http server
switch(config)# ip access-list extended POLICY
switch(config-ext-nacl)# permit udp any anyeqbootps
switch(config-ext-nacl)# permit udp any anyeq domain
switch(config)# ip admission name HTTP proxy http
switch(config)# fallback profile FALLBACK_PROFILE
switch(config-fallback-profile)# ip access-group POLICY in

switch(config-fallback-profile)# ip admission HTTP
switch(config)# interface GigabitEthernet2/1
switch(config-if)# authentication port-control auto
switch(config-if)#authentication fallback FALLBACK_PROFILE6500
switch(config-if)#ip access-group POLICY in
switch(config)# interface gigabitEthernet 2/1
switch(config-if)# authentication order mab dot1x webauth
switch(config)#copy running-config startup-config
switch(config)#exit
```

Приложение С

Топология сети банка и удаленного филиала (после внедрения технологии CiscoEnergyWise):

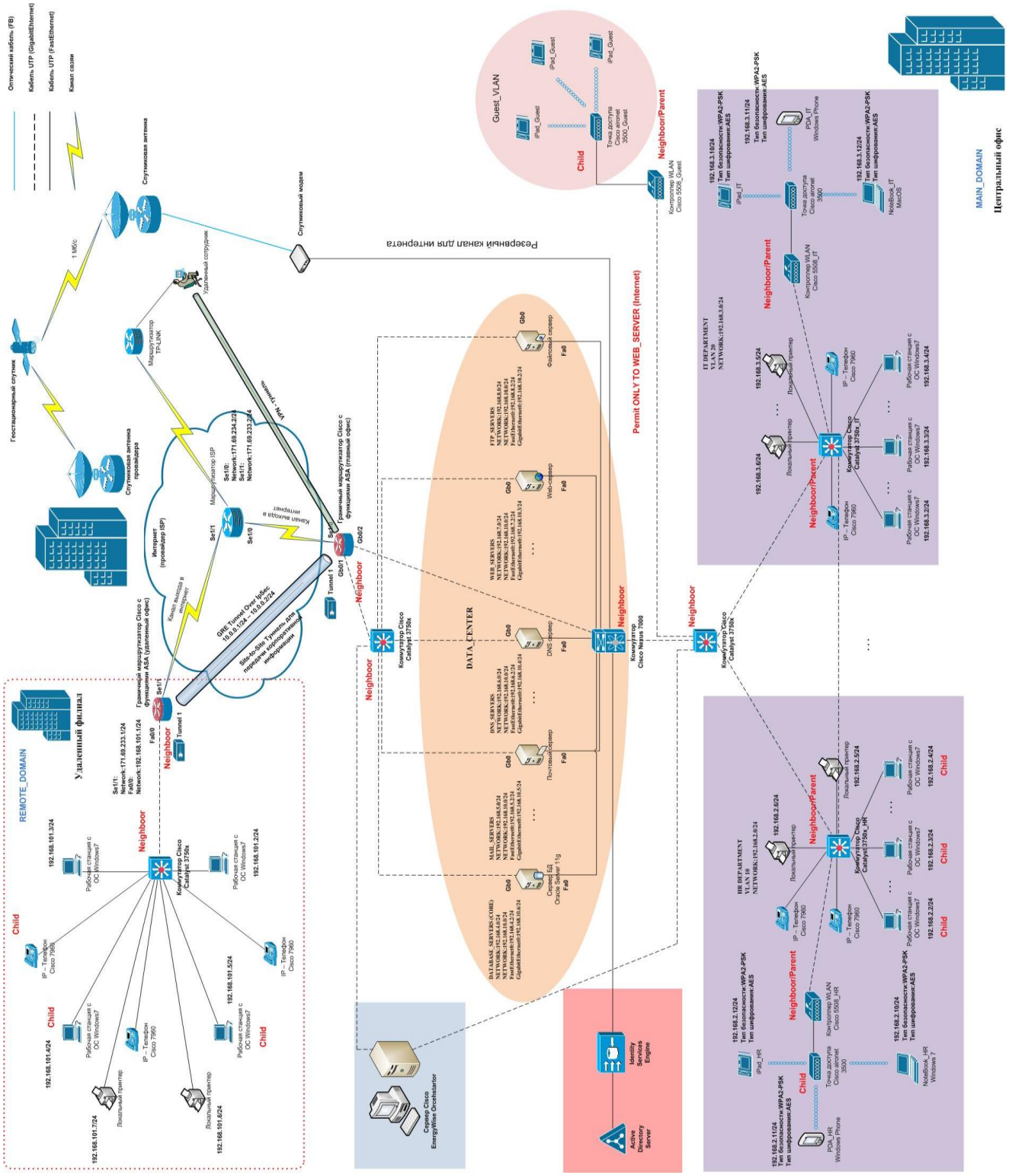

Рисунок С1 - Внедрение технологии EnergyWise в сеть банка

Настройка домена EnergyWise на коммутаторе Cisco Catalyst 3750X

```
Switch#configure terminal
Switch(config)#energywise domain Cisco security shared-secret 0 cisco protocol udp port 43440 ip
192.168.10.1
Switch(config)#energywise importance 80
Switch(config)#energywise keywords itdepartment
Switch(config)#service password-encryption
Switch(config)#energywise management security shared-secret 7 070C285F4D06 port 60500
Switch(config)#energywise name floor.itdep
Switch(config)#energywise neighbor 192.168.20.1 43440
Switch(config)#energywise role access4itdep
Switch(config)#energywise allow query save
Switch(config)#time-range onitdepfloor
Switch(config-time-range)#absolute start 00:00 01 January 2014 end 23:59 01 Jan 2014
Switch(config-time-range)#periodic weekdays 9:00 to 18:00
Switch(config-time-range)#periodic weekend 10:00 to 17:00
Switch(config)#time-range offlabfloor
Switch(config-time-range)#absolute start 00:00 01 January 2014 end 23:59 01 Jan 2014
Switch(config-time-range)#periodic weekdays 00:00 to 08:00
Switch(config-time-range)#periodic weekdays 20:00 to 23:59
Switch(config-time-range)#periodic weekend 00:00 to 10:00
Switch(config-time-range)#periodic weekend 17:00 to 23:59
Switch(config)#interface fastEthernet1/0
Switch(config-if)#energywise level 10 recurrence importance 80 time-range onlabfloor
Switch(config-if)#energywise level 0 recurrence importance 80 time-range offlabfloor
Switch(config-if)#energywise name IP_phone
Switch(config-if)#energywise role manager
Switch(config-if)#end
switch(config)#copy running-config startup-config
Switch(config)#exit
```

Приложение D

Т а б л и ц а D1 - Затраты на оборудование и комплектующие

Наименование оборудования и комплектующих	Количество	Стоимость, тенге	Сумма, тенге
1.КоммутаторCisco Catalyst WS-C3750X-48P-S	2	673 920	1 047 840
2.Коммутатор Cisco Nexus 5000	1	978 480	978 480
3.Маршрутизатор Cisco 3900	1	853 800	853 800
4.Беспроводные точки доступа CiscoAironet 3500	5	50 000	250 000
5.Система охлаждения Cisco N5K-C5010-FAN	1	71 640	71 640
6.Беспроводной контроллер Wireless LAN controllers 2500	1	108 680	108 680
7. Коммутационные шнуры RJ45-RJ45 0,5м cat 5	3	225	675
8. Выдвижнаяпатч-панель на 50 портов cat	3	15 900	47 700
Итого			3 658 815

Т а б л и ц а D2 - Данные по стоимости монтажа

Наименование оборудования и работ, ед. изм	Количество	Стоимость, тенге	Сумма, тенге
1 Монтаж волоконно-оптического кабеля, метр	500	250	125 000
2. Установка ПО, шт.	1	120 000	120 000
3.Монтаж кабельной системы передачи данных	10	2000	20 000
Итого			265 000

Т а б л и ц а D3 - Затраты на материалы

Наименование материала	Марка	Единица измерения	Кол-во.	Цена за единицу, тенге	Сумма, тенге
Бумага (Ватман)	А1	шт.	10	300	30 000
Бумага писчая	«Белоснежка» А4 95% 80 г/м	пачка	10	600	6000
CD диски	CD-RWVerbatim	шт.	30	60	1 800
Картридж принтера	Cartridgefor HP 1015	шт.	2	4000	8000
Итого					45 800

Т а б л и ц а D4 - Количество исполнителей и их заработная плата

Исполнитель	Кол-во человек	Зар.плата за месяц, тенге
Инженер	3	600 000
Главный инженер	1	260 000
Руководитель проекта	1	250 000

Т а б л и ц а D5 - Трудозатраты

Исполнитель	Дневная зарплата, тенге	Количество дней	Сумма, тенге
Инженер	8 333	50	416 650
Главный инженер	10 833	50	541 650
Руководитель проекта	10 416	50	520 800
Итого			2 312 400

Т а б л и ц а D6 - Затраты на проектирование сети

Показатель	Сумма, тенге
ФОТ, тенге	2 543 640
Отчисления на социальные нужды, тенге	251 920
Затраты на материалы, тенге	45 800
Накладные расходы, тенге	710 340
Итого	3 551 700

Т а б л и ц а D7 - Капитальные затраты на оборудование до модернизации сети

Капитальные затраты	Сумма, тенге.
приобретение нового оборудования	1 996 800
монтаж оборудования	160 000
проектирование	1 000 000
Итого	3 156 800