МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

кафедра Компьютерных технологий

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

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Разработка защиты периметра корпоративной сети на основе оборудования Cisco ASA

Специальность _____

Выполнил (а) Уденов Рахтик Ридтауддинович
(Фамилия и инициалы) группа

Научный руководитель Тайжанова А.Н., ст. препод.
(Фамилия и инициалы, ученая степень, звание)

Консультанты:

по экономической части:
Ерешева З.Д., ст. преподаватель
(Фамилия и инициалы, ученая степень, звание)
Ерешева (подпись) «20» 05 2014 г.

по безопасности жизнедеятельности:
Ахметова И.Г. д.х.н., профессор
(Фамилия и инициалы, ученая степень, звание)
(подпись) «26» 05 2014 г.

по применению вычислительной техники:
Тайжанова А.Н. ст. препод.
(Фамилия и инициалы, ученая степень, звание)
(подпись) «26» мая 2014 г.

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

Нормоконтролер: Тусупов Д.М.
(Фамилия и инициалы, ученая степень, звание)
(подпись) «22» мая 2014 г.

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

Алматы 2014 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество

АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

Факультет Информационных технологий

Специальность Вычислительная техника и программное обеспечение

Кафедра Компьютерные технологии

ЗАДАНИЕ

на выполнение дипломного проекта

Студент Ердесов Ранатбек Риджаддинович

(фамилия, имя, отчество)

Тема проекта Разработка защиты периметра корпоративной сети на основе оборудования Cisco ASA

утверждена приказом ректора № 115 от «24» сентября 2013 г.

Срок сдачи законченной работы «___» июнь 2014 г.

Исходные данные к проекту требуемые параметры результатов проектирования (исследования) и исходные данные объекта материал в критовом формате по проектированию сетей

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

Анализ предметной области

Теоретические аспекты защиты корпоративной сети

Применение настроек конфигурации сети

Перечень графического материала (с точным указанием обязательных чертежей)

Структура взаимодействия с серверами

Рекомендуемая основная литература

Олифер В.Г., Олифер Н.А. Компьютерные сети

Консультанты по проекту с указанием относящихся к ним разделов

Раздел	Консультант	Сроки	Подпись
БЖД	Дюкарева Н.Г.	11.04 - 26.05.14	
Экономика	Брежнева З.Д.	15.04-20.05.14	Брежнева
Нормоконтроль	Гусупов Д.М.	22.05.14г.	
Спец. часть	Вихорькова А.Н.	11.04 - 26.05.14	

Г Р А Ф И К
подготовки дипломного проекта

№ п/п	Наименование разделов, перечень разрабатываемых вопросов	Сроки представления руководителю	Примечание
	Анализ предметной области	28.04	
	Проектирование и разработка	05.05	
	периметра сети		
	Тестирование	10.05	

Дата выдачи задания «3» март 20 14 г.

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

Руководитель Жосер Бостожекова О.Н.
(подпись) (Фамилия и инициалы)

Задание принял к исполнению
студент _____ Чуренов Р.Р.
(подпись) (Фамилия и инициалы)

Аңдатпа

Бітіру жобасы ішкі желіні сырты әсерлерден қорғау, кіруші және шығушы рұқсатты бақылау, ұйымның бас офисымен бөлімдер арасында қауіпсіз әрекеттесу және сонымен қатар аутентификациялау, авторландыру және желілік тексеру жүйесің жетілдіру мақсатымен Cisco ASA Series құрылғысының негізінде «S2RE» компаниясының корпоративтік желісінің периметрің корғауын ұйымдастыруна арналған.

Желілер кауіпсіздігінің жалпы проблемалары қозғалған және Cisco ASA Series құрылғысының таңдалуы негіздеделген.

Жобада экономикалық сипаттағы сұрақтары, яғни осы жобаны енгізудің тиімділігі және оны іске асырудың құны қарастырылған. Еңбекті қорғау және өмір тіршілік қауіпсіздігінің сұрақтары келтірілген.

Аннотация

Выпускной проект посвящен организации защиты периметра корпоративной сети компании «S2RE» на основе устройства адаптивной защиты Cisco ASA Series с целью защиты внутренней сети от внешних воздействий, контроля входящего и исходящего доступа, безопасного взаимодействия между головным офисом организации и филиалами, а также усовершенствования системы аутентификации, авторизации, и практики сетевого аудита.

Воздвигаются общие проблемы безопасности сетей и обоснование выбора устройства Cisco ASA Series.

В проекте рассмотрены вопросы экономического характера: выгодность внедрения данного проекта и стоимость его реализации. Затрагиваются вопросы охраны труда и безопасности жизнедеятельности.

Annotation

Graduation project is dedicated to organizing the protection of the corporate network perimeter «S2RE» based on the Adaptive Security Device Cisco ASA Series in order to protect the internal network from external influences, control inbound and outbound access , secure communication between the head office and branches , as well as improvement of system authentication authorization , and network auditing practices .

Erected shared security networks and rationale for selecting the device Cisco ASA Series.

The project addressed issues of economic nature : the profitability of the project implementation and the cost of its implementation. Addresses the issues of occupational health and safety.

СОДЕРЖАНИЕ

Введение

В настоящее время замечено резкое увеличение количества новых локальных сетей, числа пользователей этих сетей, а существующие сети, при этом, расширяются. Растут также и требования, предъявляемые к передаваемому трафику, пропускной способности, протяженности (масштабности), защите информации (передачи данных) и стоимости разработки и развертывания сети, причем, безопасность информации и стоимость локальной сети, становится критически важным стратегическим фактором построения и развития любой компании.

Сейчас все чаще в информационных источниках встречается понятие системного подхода при построении системы защиты информации. Данное понятие системности рассматривается не просто как создание соответствующих механизмов защиты, а представляет собой регулярный, живой процесс, осуществляемый на всех этапах жизненного цикла информационной системы.

Помимо задачи повышения защиты информации и увеличения пропускной способности магистральной составляющей сети, актуальной является задача информационного доступа к сети, основными требованиями к которой являются:

- широкая (разветвленная) инфраструктура;
- масштабность (протяженность);
- невысокая стоимость.

В дипломной работе разработана система защиты периметра сети на основе современного оборудования Cisco ASA Series позволяющая защитить информационную систему компаний. Основной задачей проекта является обеспечение безопасности информации и информационных источников от внешних угроз путем оценки экономической эффективности и создания налаженного механизма защиты информационной структуры. В дипломном проекте рассматриваются основные вопросы по конфигурации оборудования Cisco ASA Series.

1 Угрозы безопасности сети

1.1 Необходимость защиты сети

Распространение Интернет быстро меняет наши представления о том, как следует вести дела, учиться, жить и отдыхать. Особое влияние это оказывает на способы ведения бизнеса и управления на глобальном уровне. Лидеры мирового бизнеса бесспорно признают стратегическую роль Интернета в деле сохранения жизнеспособности и конкурентоспособности их компаний в XXI столетии. Потребители и конечные пользователи желают иметь надежно защищенные средства коммуникаций и ведения электронной торговли. К сожалению, из-за того, что Интернет изначально был основан на открытых стандартах, обеспечивающих простоту связи, были упущены некоторые ключевые компоненты защиты, к которым, например, можно отнести контроль удаленного доступа, тайну коммуникаций и защиту от помех в предоставлении сервиса. Необходимость защиты коммуникаций в Интернете вызвала бурное развитие технологий защиты сетей вообще.

Перед деловыми кругами встала пугающая проблема: как реализовать и совершенствовать средства и методы защиты, чтобы уменьшить уязвимость бизнеса в условиях постоянного роста угрозы нарушения защиты, вызванного развитием хакерских методов. Подходящее для всех решение проблемы сетевой безопасности предложить трудно, поскольку для локальной сети учебного заведения эффективными могут оказаться одни решения, а для глобальной сети - совсем другие. Некоторые решения защиты хороши для малых предприятий, но оказываются неприемлемыми для крупных организаций по причине трудоемкости, слишком высокой стоимости или чрезмерных затрат времени, требуемых на реализацию таких решений в больших сетях. Выход в Интернет создает дополнительную угрозу безопасности в связи с тем, что сетевой злоумышленник получает потенциальную возможность доступа к инфраструктуре данных компании.

Проблема защиты, стоящая перед современным бизнесом, сводится к задаче рассмотрения всего спектра имеющихся решений и выбора правильной их комбинации. Сегодня предлагается немало технологий и соответствующих средств защиты. Трудность реализации защиты сети заключается не в отсутствии подходящей технологии защиты, а в выборе из множества решений такого, которое лучше всего подойдет для конкретной сети и требований вашего бизнеса и при котором затраты на поддержку и сопровождение средств защиты, предлагаемых соответствующим поставщиком, окажутся минимальными.

После того как сетевой инженер выберет подходящий набор средств защиты для сетевой среды, потребуются также и средства, интегрирующие все это в рамках соответствующего предприятия и обеспечивающие осуществление

целостной и согласованной политики защиты, что в сегодняшних условиях является совсем непростым делом.

1.2 Причины возникновения проблем защиты

Доступ к внутренней сети, удаленный доступ и доступ в Интернет сегодня используются довольно широко. Но это порождает определенный риск и ставит целый ряд вопросов безопасности. В мире есть люди, имеющие желание, достаточную квалификацию, а подчас и материальную заинтересованность для того, чтобы использовать известные недостатки защиты, постоянно открывать и эксплуатировать новые. Существует, по крайней мере, три основные причины возникновения угроз защиты сети:

- Технологические недостатки**.** Каждая сеть и каждая компьютерная технология имеют свои проблемы защиты.
- Недостатки конфигурации**.** Даже самая надежная технология защиты может быть неправильно реализована или использована, результатом чего может оказаться появление проблем защиты.
- Недостатки политики защиты**.** Неподходящая или неправильно реализуемая политика защиты может сделать уязвимой даже самую лучшую технологию сетевой защиты.

1.2.1 Технологические недостатки

Компьютерные и сетевые технологии имеют свои внутренние проблемы защиты. Рассмотрим недостатки, присущие TCP/IP, операционным системам и сетевому оборудованию (рисунок 1.1).

Рисунок 1.1 - Технологические недостатки защиты сетевых и компьютерных компонентов

Недостатки TCP/IP. Протокол TCP/IP разрабатывался как открытый стандарт, чтобы упростить связь в сети. Службы, средства и утилиты, построенные на его основе, тоже разрабатывались с целью поддержки открытых коммуникаций. Рассмотрим некоторые особенности TCP/IP и соответствующих сервисов, характеризующие их внутреннюю уязвимость.

- Заголовки пакетов IP, TCP и UDP и их содержимое могут быть прочитаны, изменены и посланы повторно так, чтобы это не было обнаружено.
- Сетевая файловая система (NFS) позволяет получить незащищенный доверительный доступ к хостам. NFS не обеспечивает аутентификацию пользователей и использует случайные номера портов UDP для сеансов связи, что практически не дает возможности ограничить протокольный и пользовательский доступ.
- Telnet является мощным средством, предоставляющим пользователю возможность доступа ко многим утилитам и службам Internet, которые иначе оказываются недоступными. Используя Telnet и указывая номер порта вместе с именем хоста или IP-адресом, хакеры могут начать интерактивный диалог с сервисами, которые считаются недостаточно защищенными.
- В системе UNIX демон sendmail может позволить доступ к корневому уровню UNIX, в результате чего возможен нежелательный доступ ко всей системе. Сервис sendmail представляет собой программу, используемую для обмена электронной почтой в UNIX. Эта сложная программа имеет длинную историю проблем защиты.

Вот некоторые из них:

- sendmail можно использовать для получения доступа к корневому уровню UNIX путем внедрения соответствующих команд в фальсифицированные сообщения электронной почты;
- sendmail позволяет выяснить тип операционной системы, в которой выполняется эта программа (по номеру версии, возвращаемой фальсифицированными сообщениями); эта информация может использоваться для того, чтобы начать атаку точек уязвимости конкретной операционной системы;
- sendmail можно использовать для того, чтобы выяснить, какие узлы принадлежат домену с данным именем;
- sendmail можно использовать для того, чтобы направить почту по несанкционированным адресам.

Недостатки операционных систем**.** Каждая операционная система тоже имеет свои проблемы защиты. Linux, UNIX, Microsoft Windows 2000, Windows NT, Windows 98, Windows 95 и IBM OS/2 - все они имеют недостатки, которые были обнаружены и зафиксированы документально.

Недостатки сетевого оборудования**.** Сетевое оборудование любого производителя имеет свои недостатки защиты, которые тоже должны быть выяснены и в отношении которых должны быть приняты соответствующие меры. Примерами таких недостатков являются ненадежная защита пароля, отсутствие средств аутентификации, незащищенность протоколов

маршрутизации и бреши брандмауэров. Выявленные недостатки защиты сетевого оборудования большинство производителей исправляют достаточно быстро. Обычно такие недостатки исправляются с помощью программной "заплаты" или путем обновления операционной системы оборудования.

Бреши позволяют неуполномоченным пользователям получить несанкционированный доступ или повышенные привилегии доступа к системе. Причиной может оказаться дефект аппаратных средств или программного обеспечения.

1.2.2 Недостатки конфигурации

Недостатки конфигурации, показанные на рисунке 1.2, близки к технологическим. Они возникают вследствие неправильной конфигурации сетевого оборудования, используемого для решения выявленных или потенциальных проблем защиты. Следует заметить, что если недостатки конфигурации известны, их обычно можно легко исправить с минимальными затратами.

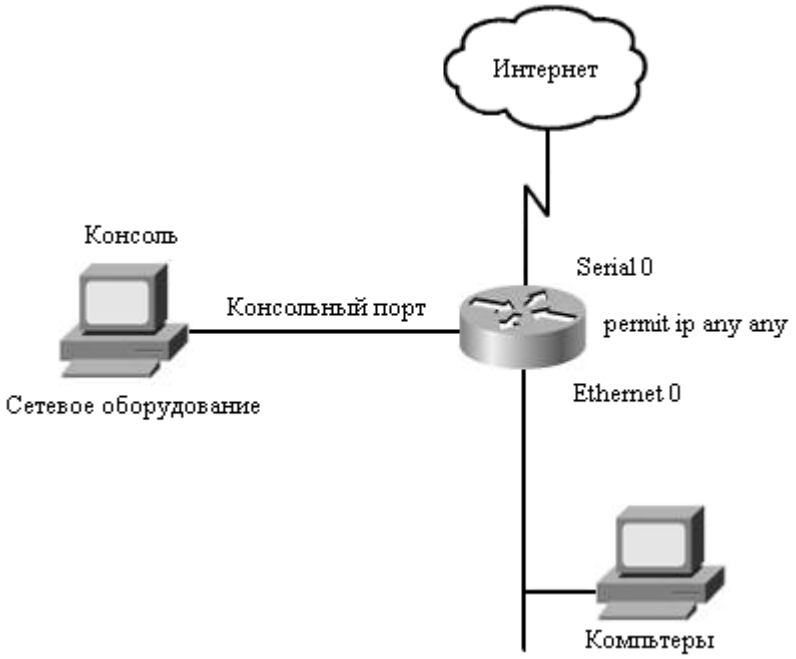

Рисунок 1.2 - Проблемы защиты, возникающие по причине неправильной конфигурации или неправильного использования оборудования

Вот несколько примеров недостатков конфигурации:

- Недостаточная защита, обеспечиваемая установками по умолчанию. Установки по умолчанию многих продуктов оставляют открытыми бреши в системе защиты. Пользователи должны проконсультироваться с фирмой-производителем или сообществом пользователей о том, какие установки по умолчанию порождают слабость защиты и как их следует изменить.

- Неправильная конфигурация сетевого оборудования**.** Неправильная конфигурация оборудования может вызывать серьезные проблемы защиты. Например, неправильная структура списков доступа, протоколов маршрутизации или групповых строк SNMP может открывать широкие бреши в системе защиты.
- Незащищенные учетные записи пользователей**.** Если информация об учетных записях пользователей передается по сети открыто, это дает возможность использовать имена пользователей и пароли злоумышленникам.
- Учетные записи пользователей, использующих слишком простые пароли. Эта широко распространенная проблема возникает в результате выбора пользователями легко угадываемых паролей из ограниченного множества вариантов. Например, системы NetWare, UNIX и Windows NT могут содержать учетные записи с именем пользователя guest и паролем guest.
- Неправильная настройка служб Internet**.** Общей проблемой является применение Java и JavaScript в обозревателях Web, что открывает возможности для атак внедрения вредоносных аплстов Java. Сетевое оборудование или операционная система компьютера могут допускать использование незащищенных служб TCP/IP, позволяющих удаленный доступ к сети.

1.2.3 Недостатки политики защиты сети

Документированная и объявленная персоналу политика защиты является существенным компонентом защиты сети. Но некоторые проблемы защиты могут быть вызваны недостатками самой политики защиты, и к таким проблемам можно отнести следующие.

- Отсутствие документированной политики защиты**.** Не представленную в виде набора документов политику невозможно применять последовательно и принудительно.
- Внутренние политические противоречия**.** Политические баталии, закулисные войны и скрытые конфликты будут препятствовать проведению согласованной и обязательной политики защиты.
- Отсутствие преемственности**.** Частая замена персонала, отвечающего за реализацию политики защиты, ведет к непостоянству в политике защиты.
- Отсутствие логичного контроля доступа к сетевому оборудованию. Недостаточно строго контролируемые процедуры выбора пароля пользователями открывают несанкционированный доступ к сети.
- Небрежность администрирования, мониторинга и контроля**.** Неадекватный мониторинг, аудит и несвоевременное устранение проблем позволяют атаковать систему защиты и незаконно использовать сетевые ресурсы в течение длительного времени, что означает расточительное использование средств компании и может привести к ответственности перед законом.

- Неосведомленность о возможности атаки. Организация может даже не знать о нарушениях, если в организации не проводится регулярный мониторинг сети или нет системы обнаружения сетевых вторжений вообще.
- Несоответствие программного обеспечения и аппаратных средств принятой политике защиты**.** Несанкционированные изменения топологии сети или установка непроверенных приложений создают бреши в системе защиты.
- Отсутствие процедур обработки инцидентов защиты и плана восстановления системы**.** Отсутствие четкого плана обработки инцидентов защиты и восстановления работоспособности сети предприятия в случае сетевой атаки приведет к хаосу, панике и ошибочным действиям.

Архивы CERT (Computer Emergency Response Team - группа компьютерной "скорой помощи") на странице www.cert.org документируют многочисленные технологические недостатки защиты самых разных протоколов, операционных систем и сетевого оборудования. Экспертные рекомендации CERT касаются проблем защиты Интернет-технологий. Они объясняют суть проблемы, помогают выяснить, имеет ли проблема отношение к вашей конкретной сети, предлагают возможные пути ее решения, а также предоставляют информацию о поставщике соответствующего оборудования.

1.3 Типы угроз безопасности сети

Диапазон угроз безопасности настолько широк, что невозможно подвергнуть их полной классификации и разработать совершенную систему защиты от них. Рассмотрим наиболее часто встречающиеся типы угроз безопасности сети.

- Разведка.
- Несанкционированный доступ.
- Блокирование сервиса.
- Подтасовка данных.

Эти категории угроз свидетельствуют об уязвимости сети и характеризуются атрибутами компьютера, позволяющими кому-либо начать враждебные действия против соответствующих сетевых объектов. В данном случае враждебное действие означает метод извлечения выгоды из уязвимости с помощью некоторой процедуры, сценария или программы. Целью такого действия является сбор имеющейся информации (разведка), блокирование системы обслуживания легальных пользователей, получение несанкционированного доступа к объектам и данным или подтасовка данных.

1.3.1 Разведка

Разведка представляет собой несанкционированное выявление структуры сети, построение ее карты и мониторинг систем, служб и точек уязвимости сети. К ней также относят мониторинг сетевого трафика. Разведка может быть активной или пассивной. Информация, полученная в результате атак разведки,

может затем использоваться для проведения атак другого типа в той же сети или для того, чтобы осуществить хищение важных данных. Атаки разведки могут иметь форму выявления целей, перехвата сообщений и кражи информации. На рисунке 1.3 показано, в каких именно точках сети предприятия могут предприниматься попытки провести разведывательные атаки

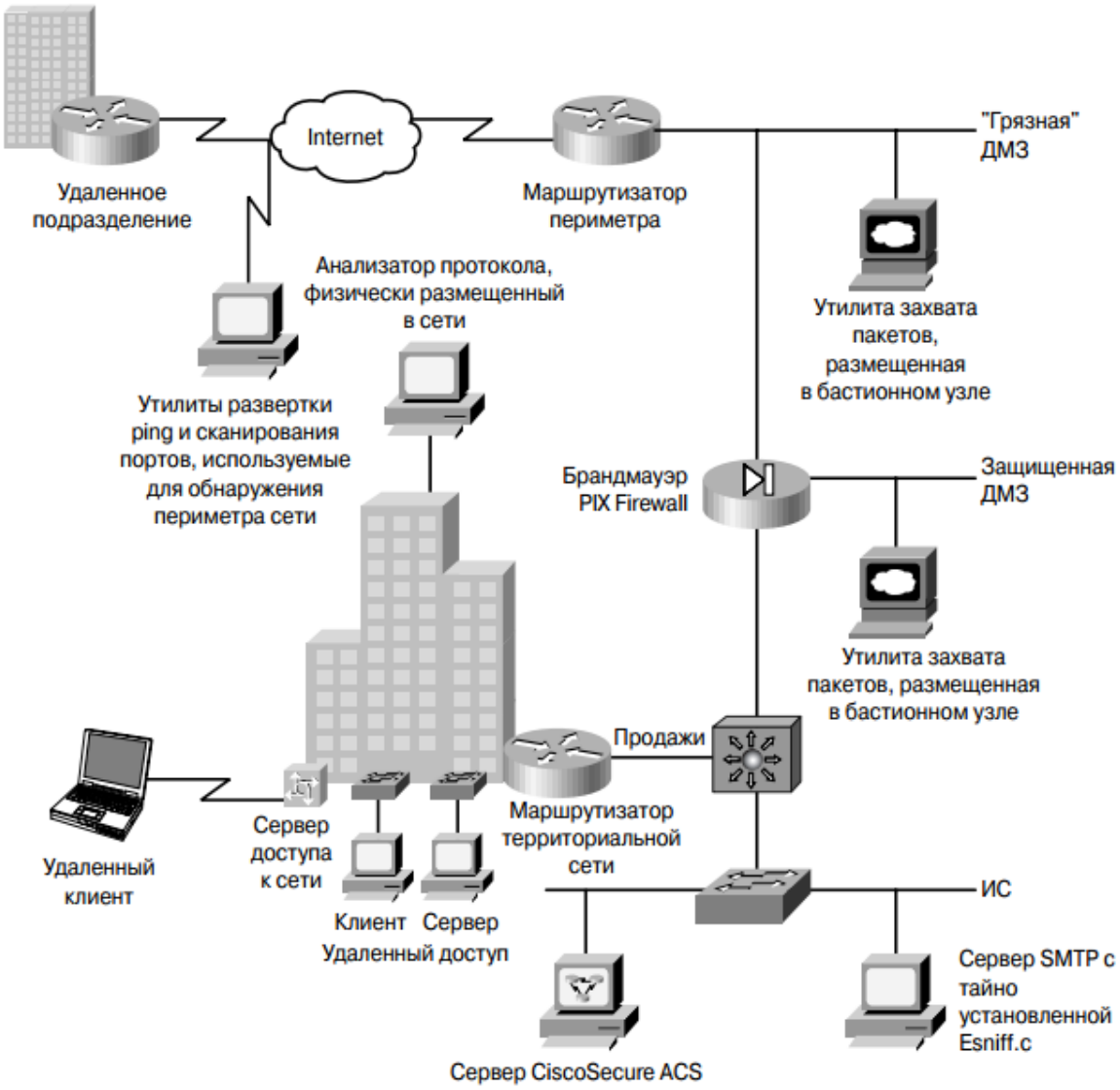

Рисунок 1.3 - Точки проведения разведывательных атак

Выявление целей. В данном случае выявление целей означает определение имен доменов и соответствующих IP-адресов, выяснение диапазона IP-адресов организации или IP-адресов конкретных узлов. Для конкретного узла можно выяснить список доступных сервисов или какую-то иную информацию об этом узле. Например, хакер может попытаться узнать IP-адрес интерфейса маршрутизатора периметра сети, обеспечивающего связь с поставщиком Интернет-услуг, чтобы получить возможность атаковать этот

маршрутизатор. Выявление целей может быть проведено с помощью общих команд опроса сети, развертки ping и сканирования портов.

Перехват сообщений. Перехват сообщений (сбор информации) является методом пассивного наблюдения за сетевым трафиком с помощью некоторого устройства или утилиты. Цель перехвата - выявление структуры потока данных, а также сбор данных для последующего анализа и кражи информации. Синонимами понятия "перехват" являются сетевое слежение и анализ пакетов. Информация, собранная посредством перехвата, может использоваться для подготовки других типов сетевых атак или кражи информации. Типичным способом перехвата сообщений в области коммуникаций является захват пакетов TCP/IP и декодирование их содержимого с помощью анализатора протокола или иной подобной утилиты. Захваченные пакеты с данными процедуры входа в сеть нарушитель может воспроизвести вновь, чтобы попытаться получить доступ к сети.

С помощью перехвата сетевые нарушители могут выяснить имена и пароли пользователей (чтобы получить право доступа к узлам сети), извлечь из пакета такие данные, как номер кредитной карточки, или другую частную информацию.

Кража информации**.** Перехват сообщений мало отличается от кражи информации. Кража может происходить во время передачи данных по внутренней или внешней сети. Нарушитель может украсть данные и с компьютера сети, получив к нему несанкционированный доступ.

1.3.2 Несанкционированный доступ

Нарушитель может пытаться получить несанкционированный удаленный доступ к компьютерам сети или сетевым устройствам самыми разными способами. Общей целью нарушителей является получение прав корневого пользователя (UNIX) или администратора (Windows) на том компьютере, где он имеет больше возможностей для управления интересующей его системой или для доступа к другим компьютерам сети. На рисунке 1.4 показаны основные точки сети, в которых нарушитель может пытаться получить несанкционированный доступ.

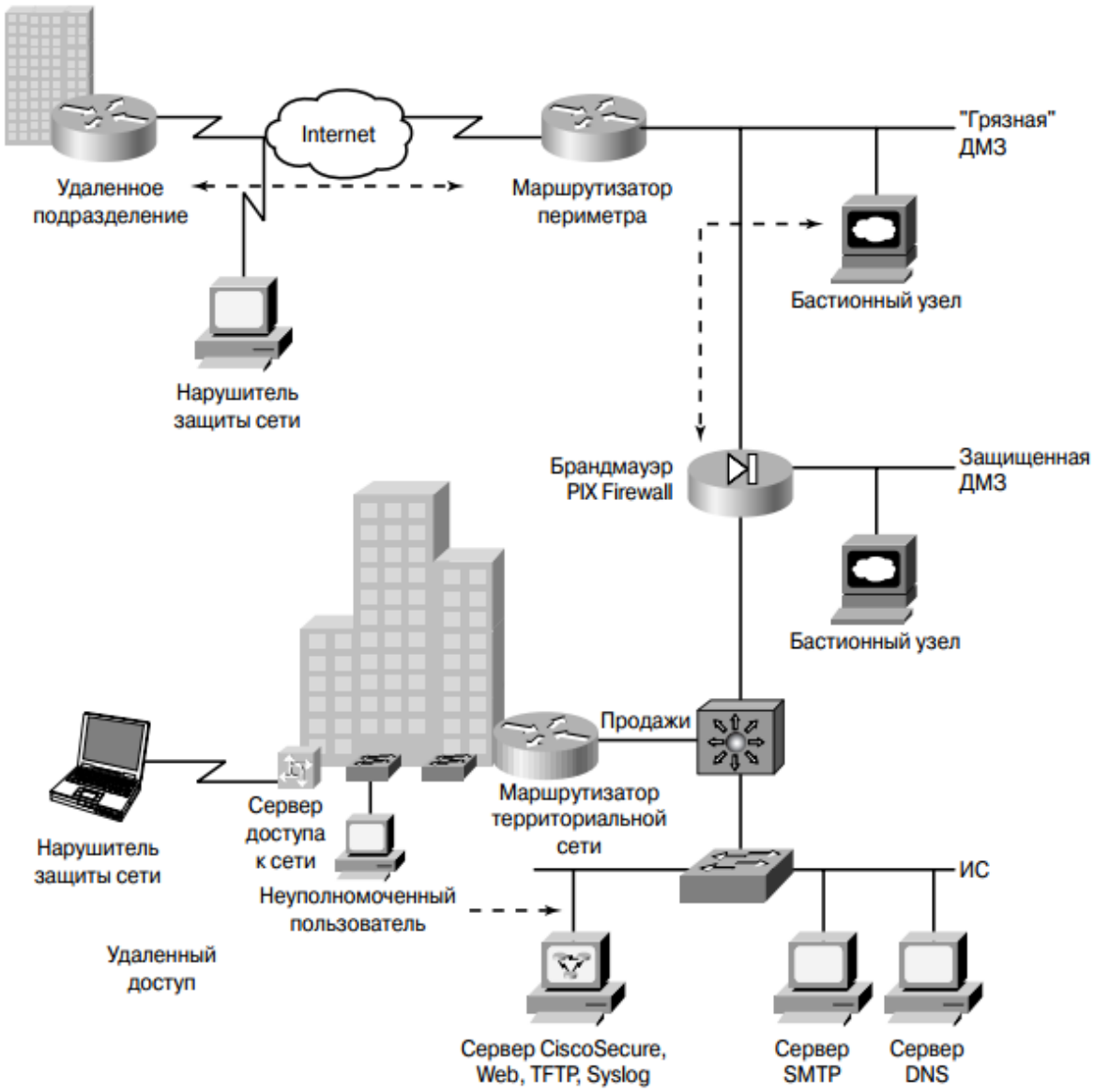

Рисунок 1.4 - Точки проведения атак несанкционированного доступа к сети

1.3.3 Блокирование сервиса

Блокирование сервиса означает попытку нарушить или прекратить работу сети, всей системы или отдельных сервисов, в результате чего отказ на запрос соответствующих сетевых услуг получат и легальные пользователи. Нарушители сетевой защиты порой демонстрируют бессмысленное создание помех (ради удовольствия) в использовании общедоступных сервисов, что очень напоминает акт вандализма. Кроме того, атаки блокирования сервиса используются и для проверки уязвимости системы, и как прелюдия к дальнейшим атакам, и как средство сокрытия следов несанкционированного доступа, и просто в отместку. Протокол IP весьма уязвим в отношении атак блокирования сервиса, поэтому существует множество типов таких атак, тем более что они реализуются так же просто, как сравнительно просто

реализуются акты вандализма. Атаки блокирования сервиса могут быть направлены против маршрутизатора периметра, бастионного узла или брандмауэра, как показано на рисунке 1.5.

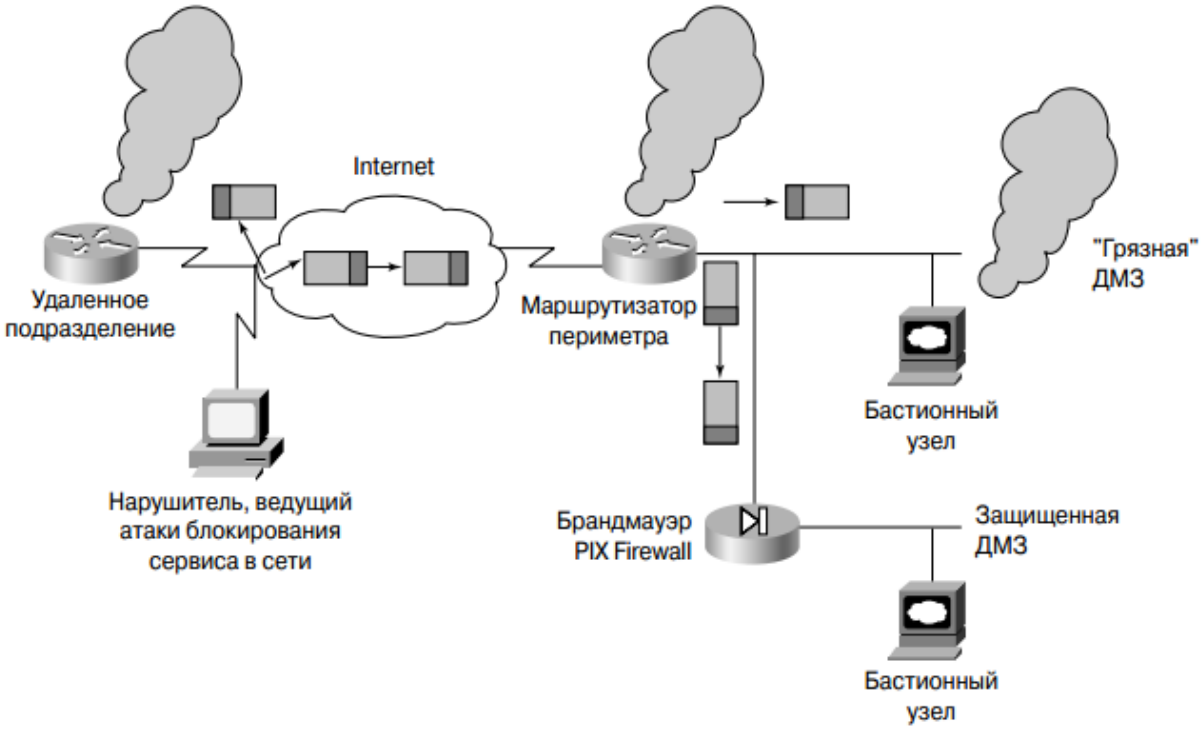

Рисунок 1.5 - Точки проведения атак блокирования сервиса

1.3.4 Подтасовка данных

Нарушитель может захватить пересылаемые по коммуникационному каналу данные, изменить их и воспроизвести повторно. Подтасовка данных именуется также имитацией, что подразумевает фальсификацию IP-адреса, повторное воспроизведение сообщений с целью захвата сеанса связи, изменение параметров маршрутизации и содержимого передаваемых сообщений. К подтасовке данных относят и граффити - своего рода вандализм в отношении Web-узла, заключающийся в изменении содержимого Web-страниц. Атаки подтасовки данных оказываются возможными вследствие уязвимости протокола IP, соответствующих сервисов и приложений. Атаки подтасовки данных называют также атаками посредника, поскольку обычно они предполагают внедрение в линию связи между двумя узлами, использующее уязвимость сеанса TCP/IP.

2 Обзор устройства защиты Cisco ASA Series

2.1 Возможности Cisco ASA Series

Устройства адаптивной защиты Cisco ASA Series представляют собой простые в развертывании решения, интегрующие сервисы межсетевого экрана, системы предотвращения вторжений (IPS), VPN с поддержкой SSL и IPSec, безопасности унифицированных коммуникаций (передача голосовых и видеоданных) и безопасности контента в гибкое семейство модульных продуктов. Разработанные в качестве основного компонента самозащищающейся сети Cisco, устройства Cisco ASA Series предоставляют интеллектуальную защиту от угроз и услуги безопасных коммуникаций, которые останавливают распространение атак прежде, чем они смогут оказать негативное влияние на целостность бизнеса. Устройства Cisco ASA Series предназначены для защиты сетей всех масштабов и позволяют организациям сократить общие расходы на развертывание и эксплуатацию, одновременно обеспечивая комплексную многоуровневую безопасность.

Рисунок 2.1 - Устройство защиты Cisco ASA Series

В техническом плане система ASA Series опирается на мощные средства безопасности, присутствующие в таких семействах продуктов Cisco, как PIX 500 Firewall, IDS 4200 Sensor и VPN 3000 Concentrator.

Cisco ASA Series предоставляет развитые механизмы адаптивной защиты от угроз, известные под общим названием Adaptive Threat Defense. Сюда входят средства защиты от неизвестных угроз (Anti-X), методы защиты бизнес-приложений (Application Security) и технологии контроля и защиты сети (Network Containment and Control), которые гарантируют унифицированную и полную защиту всех важных ресурсов предприятия от широкого спектра несанкционированных действий. В одном устройстве, которое включает в себя встроенную подсистему корреляции событий безопасности, заказчики получают средства защиты сети от многих неизвестных угроз (для борьбы с компьютерными червями и вирусами) и от шпионского и рекламного ПО, инструменты анализа трафика, выявления активности хакеров и предотвращения вторжений, а также средства предупреждения атак типа "отказ в обслуживании" (DoS).

2.1.1 Межсетевые средства защиты

Cisco ASA Series предоставляет расширенные поддерживаемые приложениями сервисы межсетевых экранов с контролем доступа на основе идентификации, защиту от атак типа «отказ в обслуживании» и целый ряд дополнительных сервисов, созданных на основе апробированной рынком технологии устройства защиты Cisco PIX.

Устройство защиты ASA - обеспечивает надежную защиту корпоративных сетей посредством контроля состояния соединений, и демонстрирует высокую производительность. Он предлагает широкие возможности защиты, полностью скрывая архитектуру внутренней сети от внешнего наблюдателя, и действует как “пограничник” между корпоративной сетью и Интернет, выполняя функции контроля.

Охрана корпоративной сети от вторжений должна осуществляться непрерывно. “Хранители” корпоративной сети должны использовать средства, гарантирующие безопасность сетевых соединений с сетью Интернет. Это вполне по силам устройству адаптивной защиты ASA. Некоторые сетевые инженеры вместо специализированных устройств защиты применяют в своих сетях решения, основанные на использовании соответствующих функциональных возможностей маршрутизаторов. После обновления программного обеспечения (а иногда и аппаратных элементов) маршрутизаторы действительно могут выполнять функции межсетевого экрана. Такое решение оправдывают тем, что специализированные межсетевые экраны слишком дороги и их сложно устанавливать. Но маршрутизаторы предназначены для обработки информации о маршрутах пакетов, а не для выполнения функций межсетевого экрана, контролирующего соединения. Поэтому возможностей маршрутизатора для построения системы обнаружения вторжений, работающий в реальном масштабе времени, часто оказывается недостаточно.

Достаточно сложные маршрутизаторы могут выполнять некоторые функции межсетевого экрана с помощью списков доступа, фильтров и "хитроумных" настроек конфигурации. На первых порах это может оказаться достаточно эффективным, но такое решение требует больших усилий с точки зрения управления и имеет ограниченные возможности масштабирования.

Компании, применяющие средства защиты на основе маршрутизаторов, отмечают их эффективность против "случайных хакеров", но по мере развития технологий хакеры стали более искушенными, начали читать техническую литературу и быстро распространять новую информацию через электронную почту, Web-узлы и "комнаты общения" (chat room). Для многих экспертов сетевой защиты стало правилом регулярно посещать Web-узлы известных групп хакеров, чтобы быть в курсе самых последних событий в области развития средств сетевых вторжений.

Устройства защиты ASA имеет следующие особенности:

- Встроенная операционная система**.** Cisco ASA работает под управлением встроенной защищенной операционной системы реального времени, не зависящей от проблем защиты UNIX или Windows. Операционная система ASA специально была усилена с точки зрения защиты от сетевых атак. Она и разрабатывалась с целью защиты.
- Алгоритм ASA (Adaptive Security Algorithm)**.** Алгоритм ASA записывает характеристики соединений, сохраняя эту информацию в таблице и используя ее для проверки исходящих и входящих пакетов, чтобы убедиться, что "состояние сеанса" остается точно таким же, как и при открытии соединения. Пока изменений не обнаруживается, трафик пропускается без задержки. При обнаружении какого-то несоответствия пересылка данных прекращается.

После запроса соединения алгоритм ASA записывает IP-адреса источника и адресата, порты источника и порядковые номера TCP, связанные с интерфейсом, по которому приходит запрос. На основе этих данных создается шифрованная подпись, которая используется устройством защиты ASA для того, чтобы распознать соответствующий хост в дальнейшем. Подпись действительна только в течение времени существования данного соединения. После закрытия соединения подпись становится недействительной. При каждом новом запросе соединения для хоста создается новая подпись.

Нарушителям, чтобы пройти через устройство защиты ASA и получить доступ к узлу внутренней сети, необходимо имитировать работу алгоритма ASA и в реальном масштабе времени генерировать полноценные пакеты (со "случайными" порядковыми номерами TCP, подходящими IP-адресами и номерами портов) в соответствии с записями базы данных соединений алгоритма ASA. Это должно оказаться непосильной задачей, чтобы хакер сразу же отказался от дальнейших попыток проникнуть в сеть и предпочел поискать другие, более доступные цели.

Преимущества алгоритма ASA:

- Ни один из пакетов, в которых информация о соединении и состоянии не соответствует данным таблицы алгоритма ASA, не сможет пройти через устройство защиты ASA.
- Разрешаются все исходящие соединения и состояния, кроме тех, которые специально запрещены выходными списками доступа. Исходящим называется соединение или состояние, в котором инициатор или клиент имеет интерфейс с более высоким уровнем безопасности, чем адресат или сервер. Внутренний интерфейс всегда имеет наивысший уровень безопасности, а внешний - самый низкий. Для дополнительных интерфейсов (типа ДМЗ) могут определяться уровни безопасности между уровнями внутреннего и внешнего интерфейсов.
- Входящие соединения и состояния запрещаются, если только они специально не разрешены каналами. Входящим называется соединение или состояние, в котором инициатор или клиент имеет интерфейс с более низким уровнем безопасности, чем адресат или сервер. Каждая трансляция адресов

допускает множество исключений, что позволяет разрешить доступ с любой машины, из любой сети или с любого хоста в Интернете к хосту, заданному трансляцией.

- Все попытки обойти указанные правила отвергаются, и серверу syslog посылается соответствующее сообщение.
- Отвергаются все пакеты ICMP, кроме тех, которые специально разрешены командой conduit permit icmp или access-list.

Сквозная опосредованная аутентификация (cut-through proxy). Система сквозной опосредованной аутентификации устройства защиты Cisco ASA выполняет начальную проверку пользователя на уровне приложения (подобно стандартному proxy-серверу), но как только пользователь идентифицирован с помощью сервера базы данных защиты типа TACACS+ или RADIUS, устройство защиты Cisco ASA авторизует пользователя в соответствии с политикой безопасности и открывает запрашиваемое соединение. Последующий же трафик для этого соединения больше не аутентифицируется на уровне приложений, а только инспектируется алгоритмом ASA на все время сопровождения состояния сеанса TCP/IP (эта система действует на существенно более быстром сетевом уровне), что значительно улучшает производительность.

Использование стандартной аутентификации с помощью proxy-сервера может замедлять обработку транзакций из-за работы на прикладном уровне. Скорость работы на прикладном уровне полностью зависит от скорости компьютера хоста и ограничивается скоростью процессора.

Инспектирование протоколов и приложений (Applications Inspection). Некоторые протоколы и приложения, которые используют организации в сетевых коммуникациях, могут блокироваться брандмауэром. Особенно протоколы, которые, динамически договариваются о портах (HTTP, ESMTP, FTP и H.323). Поэтому хороший межсетевой экран должен инспектировать пакеты выше сетевого уровня модели OSI и выполнять следующие требования протоколов либо приложений:

- безопасно открывает и закрывает динамически выделяемые порты или IP адреса для разрешенных клиент-серверных соединений;
- использует сетевую трансляцию адреса (NAT) внутри IP пакета;
- использует трансляцию портов (PAT) внутри пакета;
- инспектирует пакеты на предмет неправильного (злонамеренного) использования приложений.

Cisco ASA как раз удовлетворяет этим требованиям, и позволяют открывать защищенные коммуникации для ряда протоколов и приложений.

Виртуальный межсетевой экран (Security Contexts). С седьмой версии операционной системы Cisco ASA поддерживает технологию виртуальных межсетевых экранов (Security Contexts) (Рисунок 2.2).

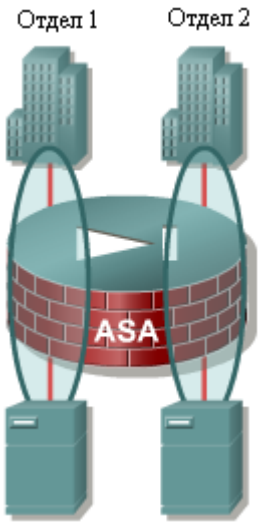

Рисунок 2.2 - Виртуальный межсетевой экран

Она позволяет в одном физическом устройстве определить несколько отдельных межсетевых экранов, каждый из которых может работать независимо - со своей конфигурацией, логическими интерфейсами, политикой безопасности, таблицей маршрутизации и администрированием. Однако данная функциональность лицензируется и доступна не на всех моделях устройств защиты.

Поддержка отказоустойчивости (Failover). Cisco ASA поддерживает конфигурацию отказоустойчивости (Failover), когда два одинаковых устройства защиты конфигурируются в паре, одно работает активным, а второе резервным. Только активное устройство выполняет свою функциональность, а резервное лишь ведет мониторинг и готово заменить активный межсетевой экран, если он даст сбой. С седьмой версии программного обеспечения поддерживается конфигурация активный/активный, когда оба устройства могут обрабатывать трафик. Данная конфигурация требует поддержки виртуальных межсетевых экранов (security contexts). На каждом устройстве конфигурируется два виртуальных межсетевых экрана. При нормальных условиях, в каждом из физических устройств один виртуальный межсетевой экран - активный, а другой - резервный. При выходе одного устройства из строя, второе задействует резервный виртуальный межсетевой экран и обрабатывает весь трафик. Также может быть сконфигурирована динамическая отказоустойчивость (stateful failover). Это значит, что при выходе активного устройства из строя, существующие соединения не теряются.

Прозрачный межсетевой экран (Transparent Firewalls). Начиная с седьмой версии, Cisco ASA могут функционировать в режиме прозрачного межсетевого экрана (режим моста), то есть в режиме устройства второго канального уровня модели OSI, обеспечивая при этом защиту сети до седьмого уровня. Это позволяет внедрять устройство защиты в существующую сеть без необходимости изменения адресации в сети.

ASDM (Adaptive Security Device Manager) - это графическая оболочка, разработанная для того, чтобы помочь в настройке и управлении устройством, без знания командной оболочки устройства (CLI).

2.1.2 Модуль AIP-SSM

Защитите свои важные сетевые активы от атак с помощью расширенных полнофункциональных услуг системы предотвращения вторжений (IPS). Cisco ASA Series обеспечивает эффективную, высокопроизводительную, современную защиту от угроз, включая уязвимости приложений и операционной системы, направленные атаки, червей, вирусов и другие формы вредоносных программ.

Рисунок 2.2 - Модуль AIP-SSM

2.1.3 VPN с поддержкой SSL и IPSec

Расширьте свою сеть с помощью защищенного, гибкого удаленного доступа без промежуточных обращений. Передовое VPN-решение Cisco ASA Series предлагает уникальную функциональную возможность портала, не требующую использования клиентского программного обеспечения (clientless), и межплатформенный полнофункциональный туннельный клиент для 5 000 одновременных соединений по протоколу SSL или IPsec в одном устройстве, защищенные сервисами межсетевого экрана мирового класса и многое другое.

Система ASA Series предлагает набор механизмов, обеспечивающих конфиденциальность трафика. Они основаны на использовании как протокола IPSec, так и SSL, и интегрированы с адаптивными технологиями защиты от угроз. Объединение IPSec и SSL VPN в устройствах Cisco ASA Series позволяет им легко приспособиться к любому сценарию применения VPN, включая конфигурации "точка-точка", удаленный доступ к корпоративной сети и доступ к сети партнера или сети экстранет. Посредством единственного устройства и управляемой инфраструктуры можно обеспечить высокозащищенный дистанционный доступ к сети для любого пользователя, где бы тот ни находился. Устройства Cisco ASA Series могут интегрироваться и с существующими кластерами Cisco VPN3000 Concentrator, что позволяет заказчикам использовать имеющиеся у них структуры VPN, внедряя самые современные службы VPN и безопасности.

Cisco ASA Series включает также богатый набор функций безопасности, которые получили название Threat-protected VPN (виртуальные частные сети с защитой от угроз). Сюда входит защита оконечных сетевых устройств, средства борьбы с угрозами, МСЭ для приложений и услуги управления доступом, которые защищают соединения VPN и пользовательские данные от сетевых червей, вирусов, шпионских программ и хакерских атак. Новые функции аварийного подхвата SSL VPN с учетом состояний поддерживают непрерывность бизнеса и повышают общую производительность труда.

С помощью ПО Cisco ASA Series версии 7.1 каждое устройство ASA Series поддерживает до 5000 одновременных сессий SSL VPN. Таким образом, организации любого размера могут предоставлять своим мобильным и удаленным сотрудникам простой и безопасный доступ к приложениям и сетевым ресурсам практически из любой точки земного шара. Встроенные функции балансировки нагрузки VPN и полномасштабная функциональность IPSec VPN позволяют сократить количество аппаратных устройств, необходимых для защиты виртуальных частных сетей и поддержки десятков тысяч пользователей одновременно. Кроме того, сокращается количество платформ VPN, которые требуются для поддержки функций VPN разных типов, включая IPSec, клиентские и неклиентские режимы SSL, удаленный доступ, связь между сайтами и экстранет.

В ПО ASA Series 7.1 усовершенствован механизм доставки контента в сетях SSL VPN. Появились мощные функции трансформации Web-контента для Web-страниц, включающих компоненты Java, ActiveX и сложные конструкты HTML и JavaScript. Оптимизация производительности приложений, поддержка разнообразных браузеров и настраиваемый пользовательский портал дополнительно расширяют для организаций возможности предоставления удаленным и мобильным сотрудникам удобного доступа к корпоративным ресурсам.

Немаловажно, что маршрутизаторы Cisco для интегрированных услуг (серии 800, 1800, 2800 и 3800) и маршрутизаторы Cisco 7200 и Cisco 7301 также поддерживают SSL VPN, что позволяет заказчикам на базе этой платформы строить безопасную систему маршрутизации. Услуги SSL VPN, реализованные в маршрутизаторах Cisco, поддерживают до 150 одновременных неклиентских и клиентских сессий SSL VPN, что отвечает потребностям малых и средних предприятий. Неклиентский доступ представляет собой надежно защищенный способ доступа к часто используемым сетевым приложениям, таким, как Citrix и Outlook, а также к внутрикорпоративным Web-страницам в сетях интранет. Клиентские же услуги SSL VPN предоставляют защищенные каналы доступа практически для любого бизнес-приложения. Они дополняют технологию IPSec VPN и современные услуги безопасности Cisco IOS (МСЭ, IPS и т. д.), отличаясь простотой внедрения и доступностью. Появление новых услуг SSL VPN в интегрированных сервисных маршрутизаторах Cisco значительно сокращает сроки окупаемости сетевой инфраструктуры и эксплуатационные расходы заказчика.

Во всех платформах Cisco SSL VPN реализована функция Cisco Secure Desktop, которая автоматически проверяет состояние системы безопасности каждого устройства, пытающегося подключиться к сети, и защищает данные в ходе сессии. Для этого создается "безопасная виртуальная машина", защищающая конфиденциальные данные и "чистящая" компьютер по завершении сеанса связи (в процессе "очистки" стираются все следы сессии, в ходе которой использовались данные конфиденциального характера).

2.1.4 Модуль CSC-SSM

Cisco ASA Series предоставляет модуль обеспечения безопасности контента и управления услугами безопасности - CSC-SSM (Content Security and Control Security Services Module). Он поддерживает полный набор услуг Anti-X, включая борьбу с вирусами и шпионскими программами, борьбу со спамом и фишинг-атаками, блокировку и фильтрацию адресов URL, а также фильтрацию контента, предотвращая доступ к потенциально опасным или не имеющим отношения к работе материалам. Модуль работает как Интернет-шлюз и защищает внутренние сетевые ресурсы от вредоносных программ и хакерских атак, распространяющихся через Интернет, что может помочь сократить эксплуатационные расходы, снизить количество неисправностей и повысить производительность сотрудников.

2.2 Модели Cisco ASA Series

Компания Cisco разработала линию устройств защиты ASA с учетом возможностей масштабирования и модернизации, чтобы обеспечить долговечность любой выбранной конфигурации. На сегодняшний день предлагает три модели ASA.

Модель Cisco ASA 5510**.** Является превосходным выбором для малых и средних предприятий, которым требуется надежная защита коммуникаций в рамках бюджетных ограничений и требований производительности территориальной сети начального масштаба.

Модель Cisco ASA 5520**.** Если для защиты вашей сети требуется более надежная платформа, чем может обеспечить ASA 5510 (т.е. необходимы дополнительные интерфейсы, поддержка Gigabit Ethernet или большего числа одновременно существующих соединений), подходящим может оказаться ASA модели 5520. Данная модель легко справляется с нагрузкой в сетях компаний, которым необходима защита на уровне всего предприятия (Рисунок 2.3).

Модель Cisco ASA 5540. Обеспечивает службы безопасности для крупных предприятий.

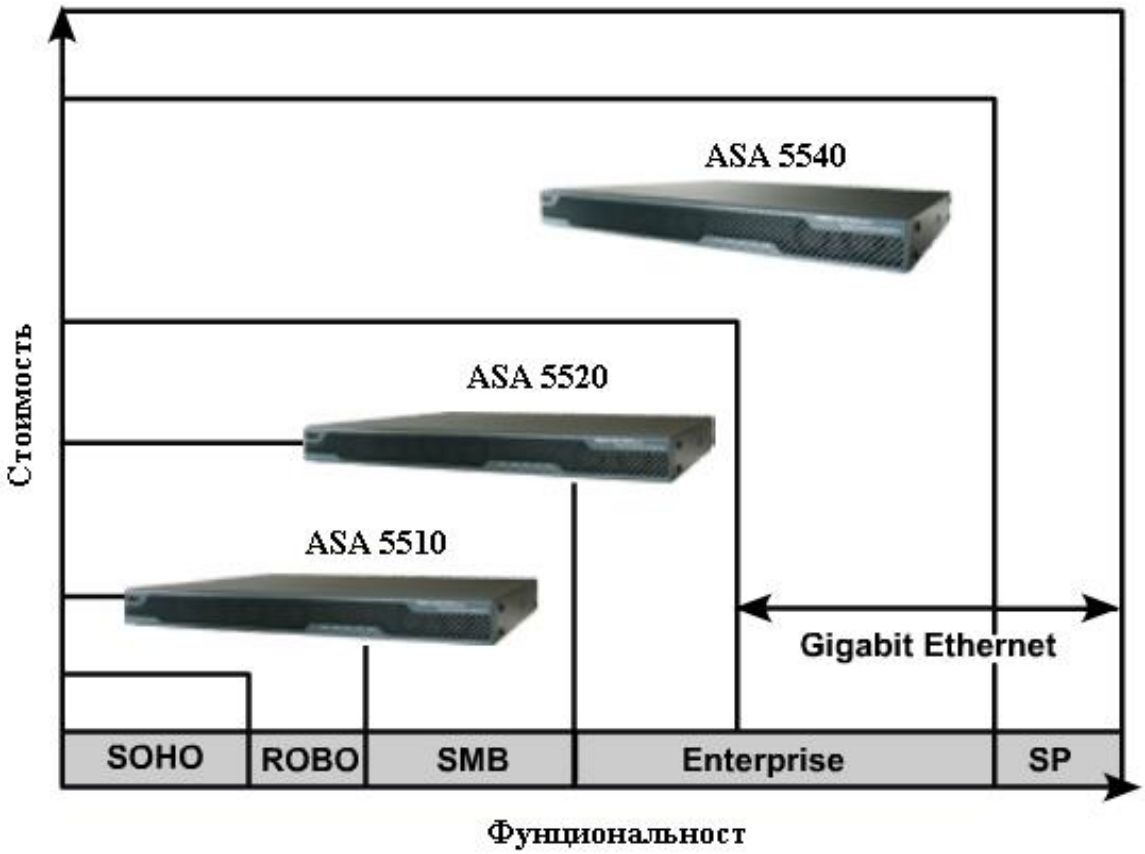

Рисунок 2.3 - Зависимость функциональности от стоимости продукции ASA

Во всех моделях предусмотрена возможность добавления других служб защиты, таких, как модули адаптивной проверки (Рисунок 2.4) и предотвращения атак (AIP-SSM) и обеспечения безопасности контента (CSC-SSM).

Рисунок 2.4 - SSM слот

За счет такой гибкой архитектуры устройства семейства Cisco ASA Series способны легко адаптироваться к новым вторжениям, предоставляя защиту в среде быстро развивающихся угроз.

В таблице 2.1 приведены характеристики устройств защиты ASA.

Т а б л и ц а 2.1 - Характеристики моделей Cisco ASA Series

	ASA 5510	ASA 5520	ASA 5540
Производительность МСЭ, Мбит/с	До 300	До 450	До 650
Производительность отражения атак, Мбит/с	150 с AIP SSM-10 300 с AIP SSM-20	225 с AIP-SSM-10 375 с AIP-SSM-20 450 с AIP-SSM-40	500 с AIP-SSM-20 650 с AIP-SSM-40
Производительность VPN, Мбит/с	До 170	До 225	До 325
Число одновременно поддерживаемых сессий	32 000/64 000*	130 000	280 000
Число туннелей IPSec VPN	50/150*	300/750*	500/2000*/5000***
Число туннелей SSL VPN	50/150*	300/750*	500/1250*/2500***
Виртуальные МСЭ	0	2/10**	2/50***
Отказоустойчивость	Active/Standby*	Active/Active и Active/Standby	Active/Active и Active/Standby
Кластеризация и балансировка VPN	Нет	Да	Да
Поддерживаемые физические интерфейсы	3 Fast Ethernet + 1 порт управления/5 Fast Ethernet*	4 Gigabit Ethernet + 1 Fast Ethernet	4 Gigabit Ethernet + 1 Fast Ethernet
Поддерживаемые логические интерфейсы VLAN 802.1q	0/10*	25	100
*С лицензиями 5510 Security Plus, 5520 VPN Plus и 5540 VPN Plus соответственно; ** с дополнительной лицензией (в базовой комплектации - 2); *** с лицензией 5540 VPN Premium.			

На передней панели (Рисунок 2.5 и 2.6) ASA имеются следующие светодиодные индикаторы:

1 **Power** - чистый зеленый указывает, что прибор включен.

2 Status - Мигание зеленого указывает, что система загружается, и выполняются проверка включения питания. чистый зеленый указывает, что системные испытания прошли, и система работает. Чистый янтарный указывает, что системные испытания неудавшиеся.

3 Active - Мигание зеленого указывает, что сеть активна.

4 VPN - Сплошной зеленый указывает, что один или более VPN туннели активен.

5 Flash - Сплошной зеленый указывает, что к Flash карточке с памятью обращаются.

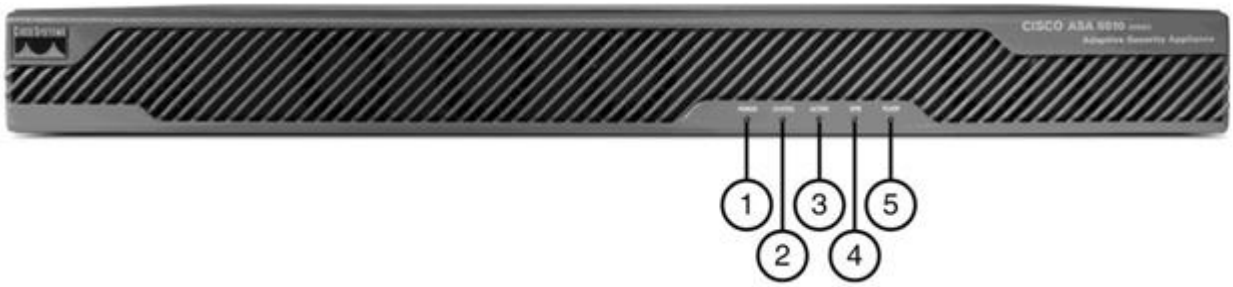

Рисунок 2.5 - Передняя панель модели Cisco ASA 5510

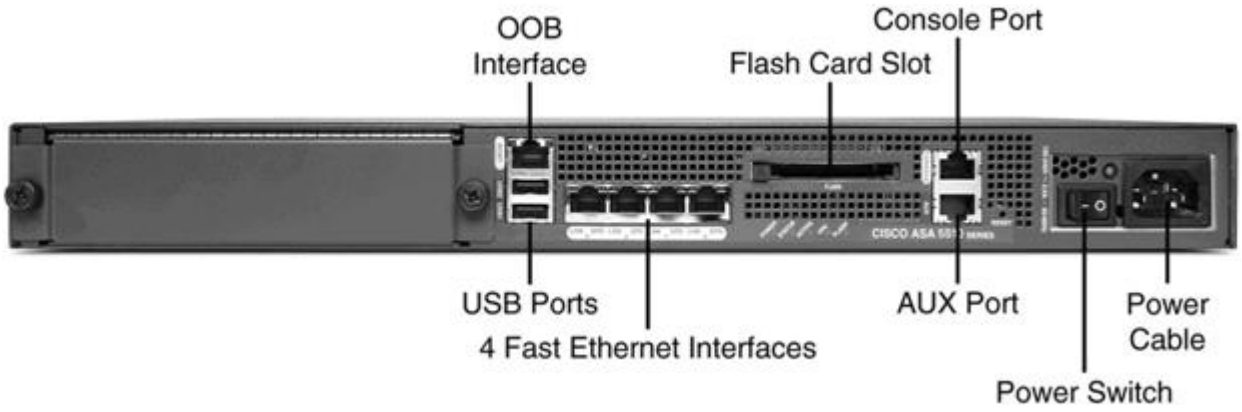

Рисунок 2.6 - Задняя панель модели Cisco ASA 5510

Все модели предлагают конструкцию one-rack unit (1RU). Внешние размещения одинаковы за исключением интерфейсов.

3 Защита периметра корпоративной сети «S2 RE»

3.1 Общая характеристика компании «S2RE»

Компания «S2RE» является одной из растущих компаний Республики Казахстан. Исторически сложилось так, что сетевая среда компании была полностью открытой: она допускала полный доступ ко всем сетевым ресурсам. Недавно, как было обнаружено отделом информационных систем (ИС), компания стала жертвой многочисленных сетевых вторжений.

Теперь компания осознает, что ее сеть уязвима, поэтому она готова потратить часть своих средств на то, чтобы с помощью средств сетевой защиты, предлагаемых компанией Cisco, обеспечить себе безопасную работу в сети. Компания «S2RE» уже является достаточно активным потребителем продукции Cisco, а сеть компании построена на использовании стека TCP/IP. В защите нуждаются три структурных сегмента сети - территориальная сеть, удаленный доступ и доступ к Интернету.

Компания «S2RE» хотела бы ограничить доступ внутренних и внешних пользователей к важным данным на серверах, контролировать исходящий трафик, усовершенствовать систему авторизации, аутентификации и практику сетевого аудита. Управление компании информировано о возможностях IPSec, SSL и сетях VPN (Virtual Private Network - виртуальная частная сеть).

Отдел информационных систем отвечает за работу сети всей компании. Приложения территориальной сети и файловые серверы размещаются на серверах Windows NT, которые доступны всем подразделениям компании (включая подразделения разработки и сбыта) и связаны с сетями партнеров. Отдел информационных систем использует систему сетевого управления на базе сервера Windows NT и соответствующее программное обеспечение сетевого управления. В рамках территориальной сети используются маршрутизаторы Cisco и коммутаторы Ethernet.

Компания «S2RE» намеревается ограничить доступ внутренних и внешних пользователей к важным данным, размещенным на серверах подсетей “разработки” и “сбыта”, поскольку руководство обеспокоено тем, что к данным этих серверов могут получить несанкционированный доступ посторонние лица. В Приложении А на Рисунке А.1 показана схема сети компании до применения технологий защиты Cisco. Как видно из схемы, не были задействованы даже настройки маршрутизатора, обеспечивающие защиту внутренней сети.

3.2 Технологии существующей сети

На сегодняшний день корпоративная сеть компании «S2RE» обхватывает два города: Астана и Алматы. Основные сервера находятся в главном офисе - в Алматы.

Рассмотрим технологии существующей сети.

Топология. Сеть построена на основе технологии Ethernet. Локальная сеть имеет пропускную способность 100 Мбит, магистраль от 100 Мбит до 1000Мбит. Каждый сотрудник подключаются отдельным независимым кабелем, который монтируется от ближайшего коммутатора до компьютера.

Оборудование. Используются высокопроизводительные коммутаторы Ethernet типа Catalyst фирмы Cisco. Сервера находятся под управлением надежных и защищенных операционных систем UNIX и Windows NT. Блоки бесперебойного и стабилизированного питания используются для защиты активного сетевого оборудования от скачков и отключения электричества. Осуществляется резервное копирование на специально-установленный сервер.

Кабель. Используется кабель «Витая пара» категории 5 и 5е, оптический кабель типа «одномод», что позволяет связывать офисы в рамках района на любых расстояниях и на скорости от 100Мбит.

Безопасность сети. Для обеспечения безопасности внутренней сети компания задействовала только настройки маршрутизатора периметра,

В компании «S2RE» в целях безопасности используются следующие методы и системы:

- устройство адаптивной защиты Cisco ASA 5510, которое включает себя:
    - межсетевой экран;
    - система предотвращения атак;
    - VPN концентратор.
- автоматическое резервное копирование данных и баз данных;
- источники бесперебойного питания;
- политика безопасности для пользователей, разграничение прав.

Структура существующей сети представлена в Приложении А.

3.1.1 Удаленный доступ

Компания «S2RE» имеет небольшую группу мобильных пользователей (это представители подразделения сбыта и системные инженеры), использующих портативные компьютеры с установленными системами Windows NT. Этим пользователям требуется доступ к серверам соответствующих подразделений. Некоторым служащим регулярно необходим дистанционный доступ к сети компании со своих компьютеров с установленными на них системами Windows NT. Кроме того, компания имеет несколько удаленных филиалов, в которых установлены маршрутизаторы Cisco 1720, использующие маршрутизацию по запросу для связи с территориальной сетью головного офиса. Компания планирует разрешить подключение к территориальной сети и поставщикам, разрешив им удаленный доступ к сети подразделения разработки. Для управления удаленным доступом компания «S2RE» использует серверы сетевого доступа Cisco 3640, связанные с коммутаторами Ethernet серии Catalyst и маршрутизаторами Cisco 4700 территориальной сети.

3.1.2 Доступ к Интернету

Компания «S2RE» имеет скоростное соединение с сетью поставщика услуг Интернет (ISP). Линия ISP соединена с маршрутизатором периметра Cisco 1720 территориальной сети. Внешними пользователями Интернет являются клиенты компании и служащие, получающие доступ к корпоративному бастионному узлу, на котором имеется сервер Web (с информацией о продуктах компании) и сервер FTP (содержащий демонстрационное программное обеспечение и документацию соответствующих продуктов). Цель компании - ограничить внешний доступ из Интернета к бастионному узлу. Внутренними пользователями Интернета являются служащие, которым доступ к Интернету необходим для исследований. Компания намеревается разрешить своим служащим неограниченный доступ к Интернету. Внутренние и внешние пользователи имеют возможность обмениваться сообщениями электронной почты, однако ввиду того, что присоединенные к сообщениям файлы и непроверенные приложения могут являться источником проблем, компания хотела бы иметь более совершенные средства управления трафиком SMTP.

Специалисты компании «S2RE» подозревают, хотя и не имеют пока неоспоримых доказательств, что недоброжелательно настроенные лица получали доступ к сети компании через Интернет. Web-узел компании был варварски разрушен. Настройки маршрутизатора связи с Интернет в результате атаки были изменены так, что легальные пользователи не могли получить доступ к Интернету вообще.

3.2 Подразделения компании

В использовании и защите сети заинтересованы три подразделения компании, а именно: подразделения информационных систем, разработки и сбыта.

3.2.1 Подразделение информационных систем

Данное подразделение имеет один сервер Windows NT, который является центром сетевого управления. Это подразделение отвечает за административный контроль и общее функционирование сети, серверов и рабочих станций, имея доступ ко всем сетевым устройствам через Telnet.

3.2.2 Подразделение сбыта

Структура подсети сбыта имеет следующие характеристики.

- Рабочие станции подсети функционируют под управлением Windows NT/XP.

- Мобильные торговые представители и инженеры подразделения сбыта используют портативные компьютеры с установленными системами Windows XP.
- Удаленные филиалы для доступа к территориальной сети головного офиса применяют маршрутизаторы Cisco 1720 и маршрутизацию по запросу.
- Приложения поддержки продаж, базы данных сбыта и файловый сервер размещены на сервере Windows NT.
- Удаленные пользователи получают доступ к серверу сетевого доступа Cisco 3640 с помощью модемов и аналоговых линий удаленного доступа.
- Подразделение сбыта связано с остальной частью территориальной сети через коммутатор Ethernet типа Catalyst и порт Ethernet маршрутизатора Cisco 4700.
- Служащим этого подразделения необходимо иметь доступ только к своим серверам Windows NT.

3.2.3 Подразделение разработки

Структура подсети отдела разработок имеет следующие характеристики.

- Рабочие станции подсети функционируют под управлением UNIX или Windows NT.
- Инженеры, которым требуется дистанционный доступ к сети компании, имеют как обычные персональные, так и мобильные компьютеры с установленными на них системами Windows NT.
- Удаленные пользователи получают доступ к серверу сетевого доступа Cisco 3640 с помощью модемов и аналоговых линий удаленного доступа.
- Подразделение разработки имеет свои серверы Windows NT с информацией о разрабатываемых продуктах, доступ к которой для других пользователей должен быть закрыт.
- Подразделение разработки связано с остальной частью территориальной сети через коммутатор Ethernet типа Catalyst и порт Ethernet маршрутизатора Cisco 4700.

3.2.4 Цели сетевой защиты компании «S2RE»

На основе применения устройства адаптивной защиты Cisco ASA Series компания «S2RE» в конечном счете, хотела бы обезопасить свою сетевую среду. Она надеется получить в свое распоряжение защищенную сеть, подобную показанной на рисунке А.2 в приложении А.

Топология этой защищенной сети показана на рисунке А.3 в приложении А.

Основные задачи проекта:

- Защита внутренней сети от внешних воздействий.
- Контроль входящего и исходящего доступа.
- Усовершенствование системы ААА.

- Надежное и безопасное взаимодействие между головным офисом организации и филиалами.

3.2.5 Системы защиты периметра сети

Защита периметра сети представляет собой сложный комплекс технологических решений по защите границы сети от вторжений. Задачей защиты периметра обычно является безопасность связи корпоративной сети с Интернет, но те, же методы и технологические решения могут использоваться и для того, чтобы обеспечить защиту соединений между частями одной и той же сети.

Подобно каменной стене и глубокому рву вокруг средневековой крепости, которые были предназначены для защиты от вторжений извне, защита периметра сети должна играть роль стены вокруг сети и обеспечивать защиту от вторжения сетевых нарушителей. Отсутствие или слабость защиты периметра открывает бреши в защите, которые могут быть использованы нарушителями.

Устройства адаптивной защиты Cisco ASA Series предлагает огромные возможности защиты, что делает его одним из лучших средств сетевой защиты, доступных на рынке сегодня. При использовании с маршрутизатором периметра, устройство защиты ASA создает практически неприступный барьер между частной сетью и внешним миром. Рекомендуемая конфигурация предполагает использование маршрутизатора Cisco в качестве первой линии защиты, за которой располагается устройства защиты ASA. Прохождение первой линии защиты означает, что нарушителю удалось обмануть списки доступа и правила аутентификации маршрутов, определенные сетевым администратором. И если нарушитель окажется достаточно опытным, для того чтобы обойти эти средства защиты, ему придется еще состязаться с ASA. Наличие нескольких интерфейсов позволяет сегментировать сеть на внутреннюю и демилитаризованную сеть, при этом механизм “прозрачного” межсетевого экрана (transparent firewall) позволяет даже не менять топологию сети. ASA в этом случае будет невидима для злоумышленников, но доступ через нее при обеспечении высокого уровня защиты будет прозрачным для пользователей.

Важной задачей системы защиты периметра является разделение сети на внутреннюю и внешнюю области. На рисунке 3.1 внутренней областью сети оказывается часть корпоративной сети, размещенная ниже устройства защиты ASA, а внешней - сеть Интернет. Внешней может быть и линия связи с деловым партнером или поставщиком.

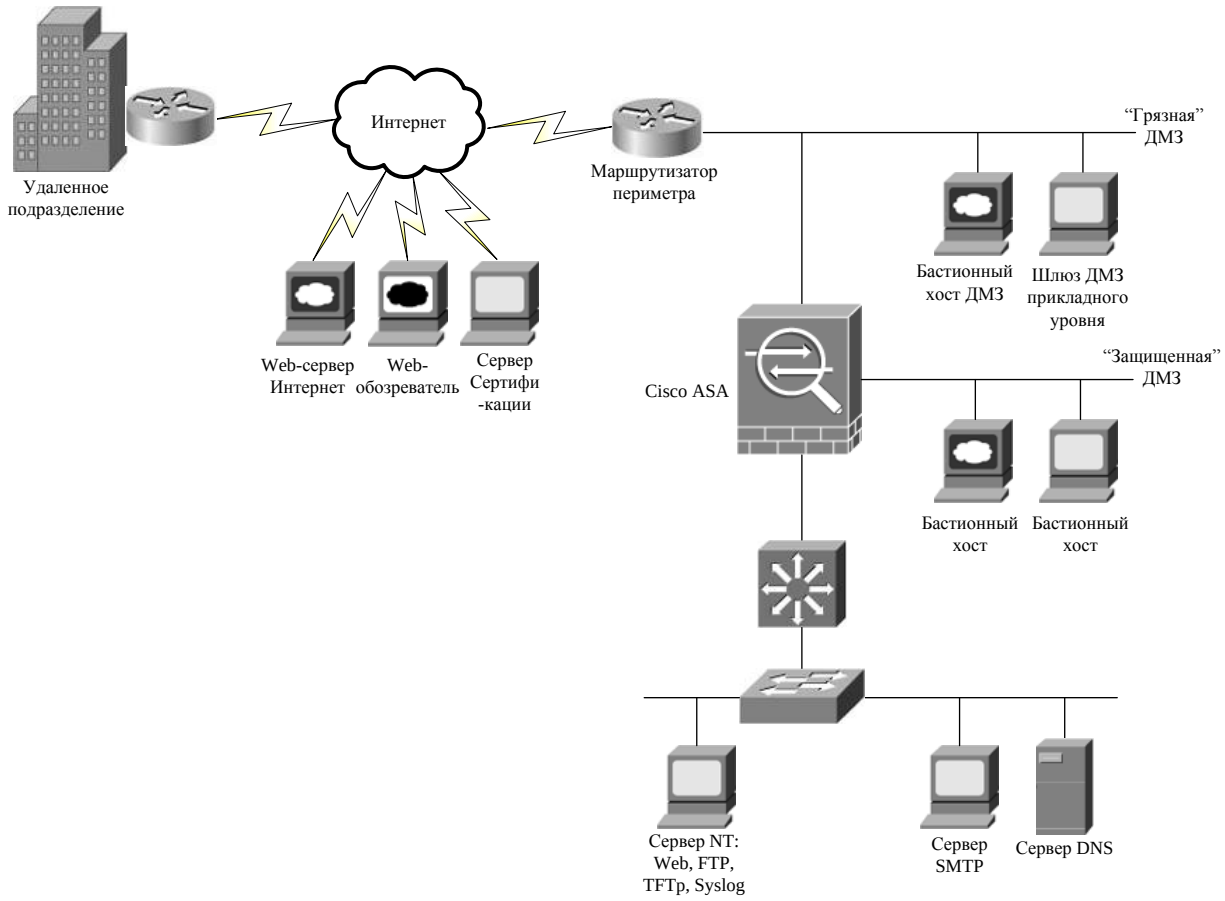

Рисунок 3.1 - Система защиты периметра компании «S2RE»

Устройства защиты периметра используются для реализации политики сетевой защиты в той ее части, которая касается взаимодействия внутренней и внешней частей сети.

Защиту периметра можно реализовать самыми разными способами, в зависимости от особенностей политики защиты, от того, что именно должно быть защищено, от уровня требуемой безопасности, бюджета и множества других факторов.

В данном проекте рассматривается вариант построения системы защиты периметра сети, обычно называемый архитектурой экранированной подсети, когда первая линия защиты создается с помощью маршрутизатора периметра (экранирующий маршрутизатор), а вторая строится на основе межсетевого экрана. Рассмотрим функции каждого из устройств, используемых в системе защиты периметра.

3.2.6 Маршрутизаторы периметра Cisco

Маршрутизатор периметра может использоваться для создания границы между незащищенной Интернет и частично защищенной “демилитаризованной зоной” (ДМЗ), представленной как "грязная" ДМЗ.

В качестве маршрутизатора периметра чаще всего используют обычный маршрутизатор типа Cisco 1720, обеспечивающий последовательное соединение с Интернет и Ethernet-соединение с ДМЗ. Маршрутизаторы Cisco имеют гибкие средства защиты периметра, позволяющие защитить связь с Интернет. Маршрутизатор Cisco предлагает следующие возможности.

- Создание первой линии защиты, которая определяет ДМЗ (или "грязную" ДМЗ, как показано на), обеспечивает защиту бастионных узлов ДМЗ и устройство защиты ASA от направленных атак и выполняет роль системы оповещения при выявлении попыток взломать маршрутизатор периметра или бастионный хост.
- Гибкий набор настраиваемых возможностей, которые можно адаптировать к постоянно возникающим новым угрозам защиты и новым Интернет - приложениям.
- Использование встроенных возможностей программного обеспечения Cisco IOS, включая специальные возможности МСЭ и средства защиты периметра.

Чтобы ограничить доступ к службам и приложениям TCP/IP, маршрутизатор периметра использует в основном правила фильтрации пакетов. Для реализации таких правил, вытекающих из требований политики сетевой защиты, применяются списки доступа. Маршрутизатор периметра создает "грязную" ДМЗ или экранированную подсеть. С помощью Cisco ASA можно создать "защищенную" ДМЗ, разместив бастионные узлы на третьем интерфейсе устройства защиты.

Инженеры Cisco предусмотрели ряд возможностей защиты периметра в рамках ядра программного обеспечения Cisco IOS, что позволяет клиентам Cisco использовать маршрутизаторы в качестве первичного средства контроля сетевого доступа к внутренним сетям. Возможности защиты включают аутентификацию пользователей, авторизацию доступа, ограничение связи с узлами, имеющими неизвестные или нежелательные адреса, маскировку внутренних IP-адресов для внешних наблюдателей, контроль потока данных, проходящих через маршрутизатор, а также применение специальных средств администрирования, позволяющих реализовать требования политики защиты в системе периметра сети.

Вариант настройки маршрутизатора периметра Cisco для корпоративной сети компании «S2RE» в соответствии с ее политикой защиты представлен в приложении Б.

3.2.7 Демилитаризованные зоны (ДМЗ)

ДМЗ, или изолированная локальная сеть, является буфером между корпоративной сетью и внешним миром. ДМЗ имеет уникальный сетевой номер, который отличается от номера корпоративной сети. Вообще говоря, сеть ДМЗ - это единственная часть сети корпорации, видимая извне.

ДМЗ создается устройствами защиты периметра, формирующими систему межсетевого экрана, которая состоит из маршрутизатора периметра, бастионного хоста и самого межсетевого экрана.

Маршрутизатор периметра создает "грязную" ДМЗ, которая представляет собой частично защищенное окружение бастионного хоста, обеспечивающего обслуживание внешних и внутренних пользователей, например, корпоративного Web-узла или шлюза прикладного уровня, предоставляющего сервис TCP/IP типа ретрансляции сообщений электронной почты.

3.2.8 Бастионный хост

Бастионный хост является защищенным сервером (обычно на базе Windows, UNIX или Linux), который размещается в ДМЗ. Он обеспечивает внешним пользователям следующие важные услуги:

- Сервис анонимного сервера FTP.
- Сервис сервера World Wide Web.
- Сервис DNS (Domain Name Service - служба имен доменов).
- Сервис SMTP для входящих сообщений электронной почты, обеспечивающий доставку электронной почты внутренним пользователям.
- Сервис посредника (proxy) при доступе в Интернет для внутренних хостов.

Бастионный хост должен быть защищен исключительно надежно: он уязвим, поскольку открыт для сети Интернет и обычно является главной точкой контакта с корпоративной сетью из Интернета. Бастионный хост может также быть доступен для внутренних пользователей.

Иногда бастионный хост обеспечивает сервис посредника, используя для этого специальное приложение или серверные программы. Сервис посредника предполагает прием запросов пользователей на предоставление Интернет-услуг (типа отправки электронной почты, FTP или Telnet) и последующую передачу запросов предоставляющим эти услуги сервисам на основе используемой политики сетевой защиты.

Если бастионный хост обеспечивает сервис посредника, он должен быть осведомлен о приложениях, в отношении которых осуществляется такое посредничество. Поэтому бастионный хост выполняет мониторинг портов TCP и UDP в целях обнаружения сервисов, для которых требуется посредник: это Telnet, FTP (File Transfer Protocol - протокол передачи файлов), HTTP (Hypertext Transfer Protocol - протокол передачи гипертекстовых файлов), gopher, WAIS (Wide Area Information Server - глобальный информационный сервер), NTP (Network Time Protocol - синхронизирующий сетевой протокол), NNTP (Network News Transfer Protocol - сетевой протокол передачи новостей) и SMTP (Simple Mail Transfer Protocol - простой протокол электронной почты).

Бастионный хост также может быть сконфигурирован как двухканальный хост, т.е. имеющий два сетевых интерфейса: один - для внутренней сети, а другой - для внешней. В такой конфигурации бастионный хост может

обеспечивать услуги МСЭ. Необходимо осуществлять тщательный мониторинг состояния бастионного хоста, чтобы попытки его скомпрометировать вовремя пресекались, так как в конфигурации двухканального хоста сеть оказывается исключительно уязвимой. В сравнении с двухканальным хостом, существенно более надежную защиту обеспечивает ASA, поэтому использование последнего является предпочтительным при построении системы межсетевого экрана.

3.2.9 Межсетевой экран (МСЭ)

МСЭ - это специализированное сетевое устройство, предназначенное для защиты внутренней сети от внешних воздействий. Имеет следующие особенности:

- трафик имеет узкое место - весь поток данных изнутри сети наружу и снаружи во внутреннюю часть сети должен пройти через межсетевой экран;
- пропускается только трафик, прошедший авторизацию в соответствии с локальной политикой защиты;
- межсетевой экран настраивается так, чтобы его защиту нельзя было преодолеть;
- межсетевой экран делает внутреннюю сеть невидимой снаружи.

Межсетевые экраны могут быть реализованы несколькими способами:

- Пакетный фильтр**.** Проверяет каждый пакет на наличие заданных пользователем параметров (адресов IP или портов TCP и UDP), но не осуществляет контроль сеансов.
- Шлюз прикладного уровня**.** Проверяет данные прикладного уровня во всех пакетах, проходящих через него до установки соединения. Через межсетевой экран позволяется движение только разрешенных данных. Например, шлюз FTP прикладного уровня проверяет FTP-пакеты на прикладном уровне и открывает только разрешенный FTP-доступ.
- Шлюз канального уровня**.** Проверяет легальность сеансов TCP и UDP перед открытием соединения (канала), проходящего через межсетевой экран. Такой шлюз рассматривает данные сеансов TCP и UDP, чтобы гарантировать прохождение через брандмауэр только разрешенных пакетов. В начале сеанса межсетевой экран создает таблицу допустимых соединений данного сеанса и разрешает прохождение данных только при условии соответствия параметров сеанса некоторой записи этой таблицы. По завершении сеанса соответствующая запись таблицы уничтожается, а канал закрывается.
- Прокси-сервер (сервер-посредник**).** Защищает внутреннюю (защищенную) сеть посредством замены IP-адреса хоста внутренней сети собственным IP-адресом для всего потока проходящих данных через межсетевой экран. Большинство предлагаемых сегодня шлюзов прикладного и канального уровней имеют встроенные возможности прокси-сервера, чтобы обеспечить дополнительную защиту. Производители межсетевых экранов

часто называют такие продукты прокси-серверами прикладного уровня или прокси-серверами канального уровня

Устройство защиты ASA (Рисунок 3.2) включает механизмы защиты периметра с помощью межсетевого экрана, отражения атак с помощью системы предотвращения вторжений, построения VPN для защиты удаленного доступа и межофисного взаимодействия, а также борьбы с вредоносными программами с помощью антивируса, антиспама, antispyware, антифишинга и контроля доступа к Интернет-сайтам.

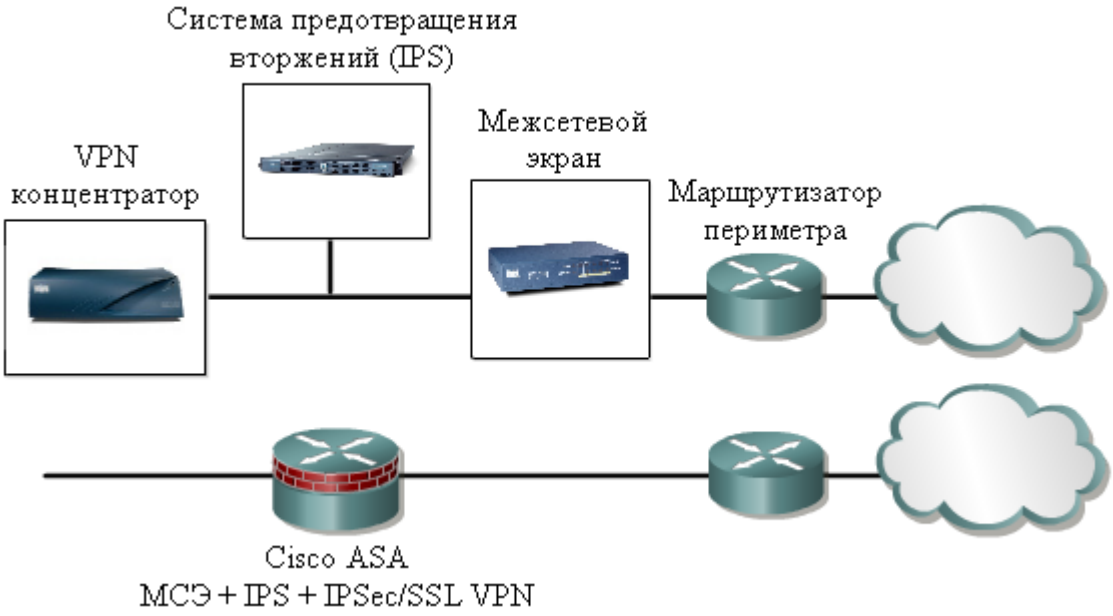

Рисунок 3.2 - Устройство защиты Cisco ASA

Компания «S2RE» приобрела устройство защиты Cisco ASA Series для работы с уже имеющимися в наличии маршрутизатором периметра и бастионными хостами в целях защиты внутренней сети от нарушителей. Необходимо так настроить устройство защиты, чтобы ограничить нежелательный доступ и в то же время оставить возможность для сотрудников аналитического отдела выполнять свою работу.

3.3 Контроль входящего и исходящего доступа

Прежде чем начать настройку параметров входящего и исходящего доступа, важно решить, сколько свободы следует предоставить пользователям при доступе к сети. В этом разделе обсуждаются две модели доступа (модели политики) - закрытая и открытая.

Открытая модель предоставляет пользователям максимальную (в разумных пределах) свободу сетевого доступа. Вообще говоря, такая модель предоставляет пользователям свободу Web- и FTP-доступа, а также доступа к сервисам POP3 и SMTP электронной почты. Открытая модель доступа обычно

предлагается “квалифицированным пользователям”, которым могут потребоваться специальные возможности доступа и которые имеют достаточный опыт для того, чтобы самостоятельно выбирать меры защиты (например, использовать собственный МСЭ или систему разрешения доступа к файлам). Большинство "квалифицированных пользователей" рассматривают такую дополнительную ответственность как неотъемлемую составляющую сетевой свободы. По умолчанию устройство защиты ASA использует открытую модель для всего исходящего трафика.

Закрытая модель соответствует наиболее агрессивной политике защиты компании. По существу, такая модель является реализацией подхода "запрещено все, что не разрешено явно". В таком окружении доступ Web и FTP осуществляется через прокси-сервер, поддерживающий специальный список управления доступом. Чаще всего в этом случае используется и фильтр управления доступом к содержимому Web. По умолчанию устройство защиты ASA применяет закрытую модель для всего входящего трафика.

Эти примеры типичны по своей природе, но они не дают исчерпывающей характеристики методов управления доступом. При использовании любого ограничения доступа пользователи могут сетовать на то, что их свобода слишком ограничена. В такой ситуации лучшим решением является сначала наложить максимум ограничений, а затем постепенно их ослаблять (по мере поступления запросов пользователей разрешить те или иные возможности).

Чтобы выяснить, будет ли подходящим то или иное решение, необходимо четко понимать лежащие в его основе технологии и сравнить возможности, доступные в рамках выбранного решения, с теми запросами, которые выдвигаются пользователями. Устройство защиты ASA уникален тем, что он может удовлетворить очень широкий диапазон запросов.

3.3.1 Настройка управления исходящим доступом

Ограничение доступа к защищенной сети является лишь одной из целей системы защиты. Многие эксперты защиты скажут, что для безопасности любой сетевой среды - как обычного офиса, так и большой корпорации и даже военной базы - контроль исходящего потока данных не менее важен, чем контроль входящего.

Устройство защиты ASA предлагает возможности, позволяющие относительно легко настраивать и модифицировать (а если требуется, то и отключать) средства управления исходящим доступом. Это средства NAT (Network Address Translation -трансляция сетевых адресов) и PAT (Port Address Translation - трансляция адресов портов).

Средства NAT устройства защиты ASA

Средства NAT устройства защиты ASA позволяют частным сетям, соединенным с Интернет, использовать IP-классы, которые обычно таким сетям недоступны (Рисунок 3.3). С помощью этих средств обеспечивается доступ к

Интернету незарегистрированным клиентам без перестройки всей схемы IP-адресации корпоративной сети. Эти средства позволяют также существенно расширить пространство адресов, доступных для использования во внутренней сети организации.

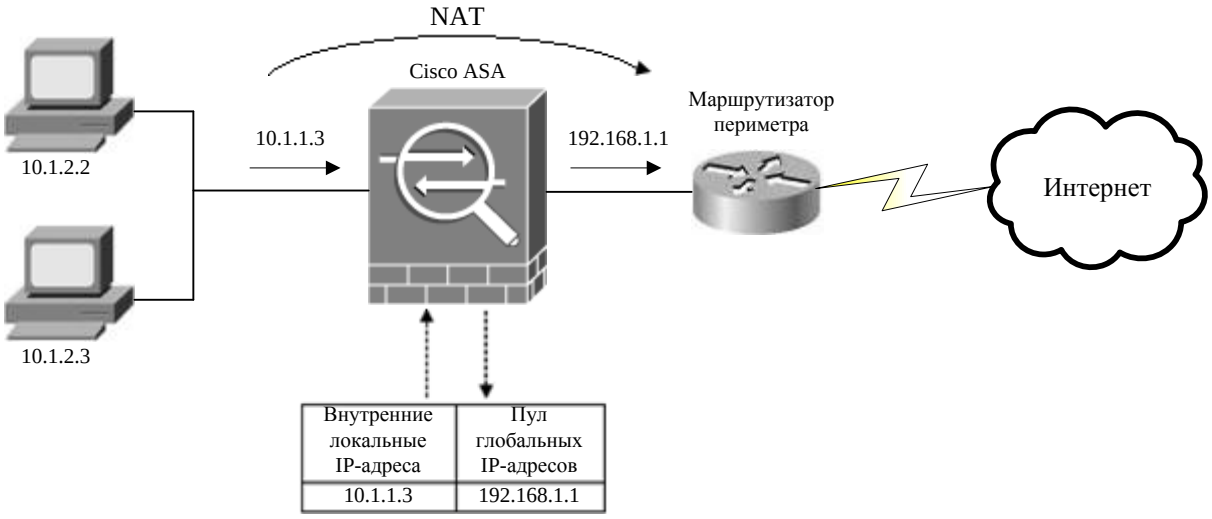

Рисунок 3.**3** - Пример использования NAT

Когда внутренний хост инициирует создание исходящего соединения, средства NAT транслируют IP-адреса внутренней сети в адреса, указанные командами global и static. Трансляция адресов позволяет защищенной сети иметь любую схему IP-адресации. Устройство ASA защищает внутренние адреса, не позволяя видеть их внешним сетям.

Существует три типа средств NAT, и все они имеют весьма гибкие возможности настройки.

Статические средства NAT**.** Эти средства используются тогда, когда адрес каждого хоста внутренней сети статически (т.е. однозначно) отображается во внешний сетевой адрес. Поскольку процесс отображения в данном случае не является динамическим, администрирование такого процесса требует немалых усилий.

Динамические средства NAT**.** Рассматриваемые средства перехватывают трафик, идущий от хоста внутренней сети, и транслируют его во внешний зарегистрированный IP-адрес из пула адресов, поддерживаемого устройством защиты ASA. Информация о трансляциях сохраняется в таблице, чтобы имелась возможность разрешить обратный трафик к внутреннему хосту.

PAT**.** Средства PAT (Port Address Translation - трансляция адресов портов) можно рассматривать как вариант NAT для портов. Трафик идентифицируется и направляется по одному и тому же IP-адресу, присвоенному внешнему интерфейсу устройства. Средства PAT отображают адреса источника соединений внутреннего хоста в один и тот же IP-адрес внешнего интерфейса. Устройство защиты ASA выбирает и присваивает пакетам (TCP или UDP) новые номера портов источника. Данные процесса отображения номеров

портов сохраняются устройством защиты ASA, чтобы обеспечить прохождение обратного трафика.

Настройка NAT для контроля исходящего доступа.

В этом разделе рассматривается применение средств NAT к трафику, направленному в сторону внешних сетей. Чтобы устройство защиты ASA выполнял трансляцию внутренних адресов источника во внешние зарегистрированные адреса, назначенные ASA, применяются команды global (outside) и nat(inside).

Команда global.

Определяет пул глобальных адресов. Этот пул обеспечивает IP-адрес каждому исходящему соединению и всем входящим, возникающим вследствие исходящих.

Команда global имеет следующий синтаксис:

```
global 1{иия_интерфейса)} global_id глобальн_ip[-
глобальн ip] [netmask глобальн_маска]
```

Команда nat.

Активизирует средства NAT. Эта команда связывает сеть с пулом IP-адресов, описанных командами global и static. Команда nat позволяет активизировать или отключить трансляцию адресов для каждого внутреннего адреса в отдельности.

С помощью команды nat можно более точно задать правила трансляции сетевых адресов, что позволяет (Таблица 3.1) работать как с отдельными адресами, так и с диапазонами адресов.

Команда nat имеет следующий синтаксис:

```
nat [(имя_иитерфейса)] nat_id локальн ip [маска
[max_conns [em_limit]]] [norandomseq]
```

Т а б л и ц а 3.1 - Параметры команды global

Параметр	Описание
имя_интерфейса	Имя внешнего сетевого интерфейса, где должны применяться глобальные адреса
global_id	Положительное числовое значение, соответствующее значению, указанному в команде nat, с которой связывается данная команда global.
глобальн_ip	Задает глобальные IP-адреса, которые ASA использует для соединений. Если внешняя сеть связана с Internet, то каждый глобальный IP-адрес должен быть зарегистрирован в сетевом информационном центре (NIC).

Окончание таблицы 3.1

Параметр	Описание
	Можно описать диапазон IP-адресов, разделив их дефисом (-). Можно создать оператор для PAT, указав один IP-адрес. Допускается только один такой оператор на интерфейс, но при этом может поддерживаться до 65535 объектов трансляции
netmask	Предшествует аргументу глобальная_маска
глобальн_маска	Определяет сетевую маску для адресов глобалън_1р. Если имеются подсети, используйте для них маску типа 255.255.255.128. При соответствующем выборе диапазона адресов и маски подсетей команда global не будет использовать широковещательные и сетевые адреса пула глобальных адресов. Например, если использовать значение 255.255.255.224 и диапазон адресов от 209.165.201.1 до 209.165.201.30, то широковещательный адрес 209.165.201.31 и сетевой адрес 209.165.201.0 не будут включены в пул глобальных адресов

Т а б л и ц а 3.2 - Параметры команды nat

Параметр	Описание
имя_интерфейса	Указывает имя внутреннего сетевого интерфейса. Если интерфейс должен ассоциироваться со списком доступа, то имя_интерфейса должно быть интерфейсом с более высоким уровнем защиты
nat_id	Все команды nat с одинаковыми значениями nat_id относятся к одной группе nat.
локалъи_ip	Задает подлежащий трансляции IP-адрес внутренней сети. Можно использовать 0.0.0.0, чтобы позволить устанавливать исходящие соединения всем хостам. Значение 0.0.0.0 можно сократить до О
маска	Указывает сетевую маску для локальн_ip. Можно использовать 0.0.0.0, чтобы разрешить трансляцию всех исходящих соединений с помощью пула глобальных IP-адресов
max_conns	Определяет максимальное число TCP-соединений с указанного интерфейса
em_limit	Определяет предельное число зарождающихся соединений. По умолчанию используется значение 0, означающее отсутствие ограничений.
norandomseq	Запрещает рандомизацию порядковых номеров TCP-пакетов. Используйте этот параметр только в тех случаях, когда рандомизация выполняется другим брандмауэром и

Окончание таблицы 3.2

Параметр	Описание
	в результате комбинации соответствующих функций искажаются данные. Применение этого параметра открывает брешь в системе защиты устройства ASA

Первым шагом на пути использования средств NAT является применение команды global, указывающей адреса, которые будут включены в пул внешних глобальных адресов, поддерживаемый устройством защиты ASA для трансляции.

```
ciscoasa (config)# global (outside) 1 192.168.1.128-
192.168.1.254
```

Число 1, указанное после команды outside, является идентификатором (global id), зависящим от того, сколько внутренних сетей будет использовать пул глобальных адресов. В данном случае трансляция должна выполняться только для одной внутренней сети, поэтому можно указать значение 1. Если трансляция требуется для большего числа сетей, можно выбрать значение от 2 до 2147483647. Это значение определяет связь команд global и nat.

Вторым шагом является непосредственное применение команды nat:

```
ciscoasa(config)# nat (inside)  1 10.1.0.0 255.255.0.0
```

Здесь все адреса внутренней сети 10.1.0.0 транслируются в глобальные адреса, указанные командой global со значением параметра global_id, равным 1. Если необходимо транслировать дополнительные адреса, важно знать номер global_id, отвечающий пулу глобальных адресов, используемому соответствующей командой nat. Сетевая маска 255.255.0.0 говорит устройству ASA о том, что запросы на трансляцию следует выполнять только тогда, когда они исходят от сети 10.10.x.x

Во время начальной настройки параметров устройства ASA можно разрешить всем внутренним узлам устанавливать соединения с любыми внешними узлами, воспользовавшись командой nat 1 0.0.0.0 0.0.0.0. Команда nat 1 0.0.0.0 0.0.0.0 включает трансляцию адресов и позволяет всем внутренним узлам (что определяется параметром 0.0.0.0) производить соединения, которые предусмотрены соответствующей командой global. С помощью команды nat можно более точно задать правила трансляции сетевых адресов, что позволяет работать как с отдельными адресами, так и с диапазонами адресов. Следует отметить, что синтаксис команды позволяет использовать символ 0 вместо строки 0.0.0.0. В следующей команде показан пример использования этого символа:

```
ciscoasa(config)# nat (inside) 1 0 0
```

Команда nat 0

Позволяет отключить трансляцию адресов, чтобы некоторые внутренние IP-адреса оставались видны извне. Эта возможность оказывается полезной тогда, когда в защищенной сети есть зарегистрированные IP-адреса, которые должны быть доступны пользователям из Интернета.

Необходимость использования команды nat 0 возникает, например, в случае, когда в сети имеется Web- или почтовый сервер, которые должны быть доступны из Интернет. Команду nat 0 можно также использовать со списком доступа в маршрутизаторе периметра, чтобы разрешить доступ к защищенной сети только определенным типам трафика портов (например, для обмена данными между центром сертификации и виртуальной частной сетью, использующей защищенные сертификаты для аутентификации).

При использовании в устройстве ASA более двух интерфейсов важно помнить о том, что команда nat 0 отменяет трансляцию адреса источника, независимо от того, по какому из интерфейсов уходит пакет.

С помощью команды nat 0 можно вообще отказаться от трансляции внутренних адресов. Первый 0 в команде nat 0 позволяет отключить трансляцию для соответствующих внутренних IP-адресов, чтобы они были видны извне. Если для параметров локального IP-адреса и маски сети указаны значения 0, то они интерпретируются как 0.0.0.0. Воспринимаем 0, как сокращение значения 0.0.0.0, означающего учет всех вариантов.

```
ciscoasa(config)# nat (inside)  0 0 0
```

Если необходимо сделать видимым только один адрес, то в командную строку следует ввести этот адрес и соответствующую маску:

```
ciscoasa(config)# nat (inside)  0 172.16.1.5 255.255.255.255
```

Команда nat-control

Указывает на то, что у всего трафика, идущего через ASA, должна быть определенная запись преобразования (инструкция nat с инструкцией проверки соответствия *global* или *static*); в таком случае он сможет пройти через ASA. По умолчанию в конфигурации ASA с программным обеспечением версии 7.0 используется команда *no nat-control*. Данное поведение можно изменить посредством ввода команды *nat-control*.

При отключении *nat-control* ASA пересылает пакеты с более защищенного интерфейса на менее защищенный интерфейс без наличия специальной записи преобразования в конфигурации. Для того, чтобы трафик проходил с менее защищенного интерфейса на более защищенный, необходимо использовать списки доступа. В результате ASA будет пересылать трафик.

Трансляция адресов портов

Средства PAT, часто называемые трансляцией типа “множество-один”, отображают весь трафик внутренней сети в один внешний IP-адрес.

Когда хост защищенной сети запрашивает ресурс, доступный через Интернет, в таблицу NAT устройтсва защиты ASA добавляется соответствующая запись, которая содержит следующую информацию о запросе:

- параметры трансляции локального адреса хоста в доступный глобальный адрес, выбранный устройством защиты ASA;
- параметры трансляции номера порта, выбранного хостом, в случайный номер порта, выбранный устройством защиты ASA.

Устройство защиты ASA, сохраняет и использует данные трансляции для проверки того, что запрос исходит изнутри защищенной сети. По завершении сеанса соответствующая информация уничтожается. Ниже этот процесс будет рассмотрен подробнее.

Средства PAT устройства защиты ASA позволяют расширить пул адресов компании на основе использования следующих возможностей:

- Один внешний IP-адрес может использоваться для (приблизительно) 4000 внутренних хостов. (Теоретически предел превышает 64000, но на практике предельным оказывается значение 4000).
- Реальные номера портов TCP отображаются в предписанные IP-адрес и номер порта, если специальной командой static не указано иное действие.
- Внутренние адреса источника маскируются с помощью одного IP-адреса из пула глобальных адресов, поддерживаемого устройством защиты ASA.

Средства PAT могут использоваться совместно со средствами NAT, и при этом адрес PAT является виртуальным адресом, отличным от адреса порта на внешнем интерфейсе.

Не следует применять средства PAT при доступе через устройство защиты ASA к приложениям мультимедиа. Такие приложения обращаются к конкретным портам и могут вступать в конфликт со средствами отображения портов, используемыми в рамках PAT. В тех случаях, когда трафик порта должен сохранять свою конфигурацию, можно использовать команду nat 0.

На рисунке 3.**4** показана схема сети, в которой средства PAT могут быть реализованы в минимальной конфигурации. Компания XYZ имеет три зарегистрированных IP-адреса. Маршрутизатору периметра, устройству защиты ASA и бастионному хосту присваивается по одному из этих адресов (при этом бастионный хост обычно является единственным хостом, доступным через Internet, и представляет собой Web-сервер или сервер электронной почты).

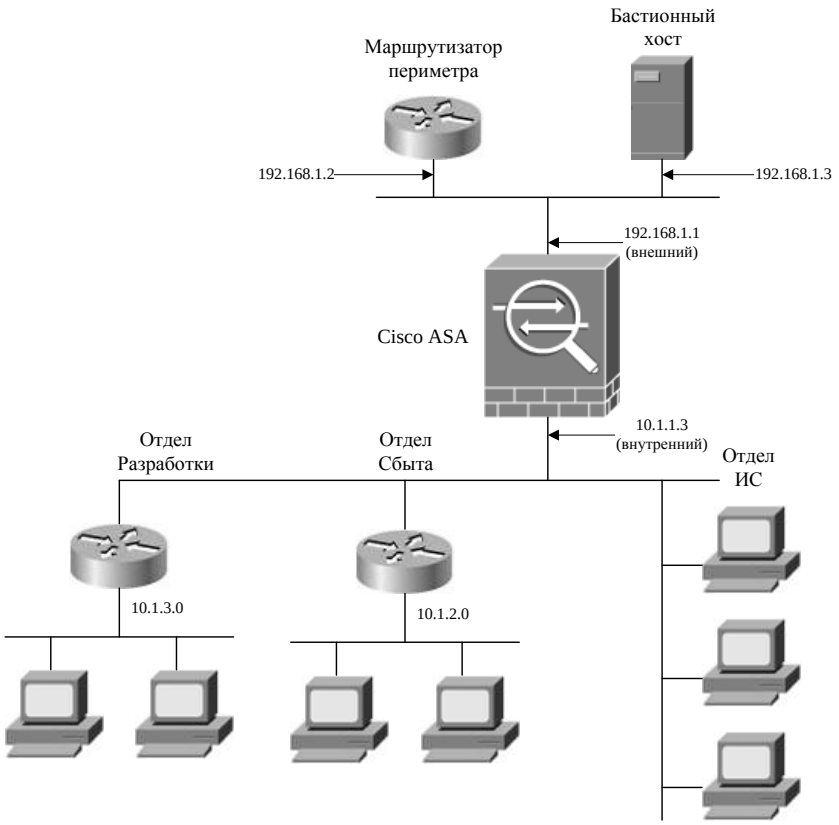

Рисунок 3.**4** - Использования PAT для внутренней сети 10.1.0.0

```
ciscoasa(config)! ip address  (inside) 10.1.1.3 255.255.252.0
ciscoasa(config)!   ip   address      (outside)      192.168.1.1
255.255.252.0
ciscoasa(config)! route (outside) 0 0 192.168.1.2 1
ciscoasa(config)! nat (inside) 2 10.1.0.0 255.255.0.0
ciscoasa(config)!   global   (outside)   2   192.168.1.4   netmask
255.255.252.0
```

Первая строка приписывает IP-адрес 10.1.1.3 интерфейсу устройства ASA, имеющему название "внутренний" (inside); это интерфейс, связанный с защищенной сетью. Вторая строка присваивает IP-адрес 192.168.1.1 интерфейсу устройства ASA, имеющему название "внешний" (outside); это интерфейс, который находится вне защищенной сети и открыт для Интернета. Третья строка сообщает ASA о том, какой трафик разрешается направлять через интерфейс 192.168.1.2 маршрутизатора периметра. При этом трафик, покидающий "внешний" интерфейс (IP-адрес 192.168.1.1), будет проверяться на соответствие значениям, указанным в команде для IP-адреса и маски сети. В данном случае приемлемым оказывается весь трафик, поскольку как для IP-адреса, так и для маски сети указаны значения 0. (0 является сокращением 0.0.0.0.) Четвертая строка присваивает NAT-идентификатор 2 внутренним хостам сети 10.1.0.0. Последняя строка помещает адрес 192.168.1.4 в пул глобальных адресов и сообщает брандмауэру о том, что IP-адрес 192.168.1.4 должен использоваться сервисом

3.3.2 Управление доступом к внутренним хостам

Важной задачей разработки стратегии сетевой безопасности является выбор процедур, позволяющих внешним объектам получить доступ к частной сети. В реальности это не порождает больших проблем, как может показаться на первый взгляд, поскольку каждый, кто хотя бы раз размещал Web-сервер или сервер электронной почты в ДМЗ ("демилитаризованной" зоне), решал именно эту задачу. Использование ДМЗ сегодня является типичным методом доступа к ресурсам, защищенным МСЭ. Устройство защиты ASA предлагает усовершенствованные возможности, которые еще больше усиливают защиту, присущую конфигурации МСЭ - ДМЗ.

Для предоставления доступа через устройство защиты ASA от менее доверенного устройства (передающего данные в брандмауэр PIX через интерфейс с меньшим уровнем безопасности) к более доверенному устройству (получающему данные от брандмауэра PIX через интерфейс с большим уровнем безопасности) существует два метода.

Ответ на корректный запрос (response to valid request). При установлении пользователем из внутренней сети соединения с устройством, находящемся во внешней сети, брандмауэр по умолчанию разрешает передачу ответа на запрос. Все информация об исходящих соединениях хранится в таблице трансляции (translation table) устройства защиты ASA. При запросе внешним устройством ответа на запрос брандмауэр PIX проверяет таблицу трансляции на наличие слота трансляции (translation slot) для этого запроса. Если такой слот существует, устройство защиты ASA разрешает дальнейшую передачу ответа на запрос. После завершения сеанса связи для этого слота трансляции запускается специальный таймер бездействия (idle timer).

Настройка канала передачи данных (configure a access-list). Использование передачи данных от внешнего интерфейса к внутреннему. Вначале необходимо настроить параметры статической трансляции (команда static) или динамической трансляции с помощью команд global и nat. (Несмотря на то что команды nat/global позволяют работать с соединениями, отправиетелм которых является внутренний интерфейс, если пользователю необходимо получить эхо-ответ от какого-либо устройства через устройство защиты ASA, необходимо настроить каналы передачи данных с помощью команды condiut.) Для настройки каналов передачи данных необходимо указать IP-адреса или группы IP-адресов, порт и (или) диапазон портов отправителя, которым разрешено передавать поток данных через устройство защиты ASA.

Новые версии операционной системы Cisco OS предоставляют пользователям два дополнительных метода для получения доступа из менее безопасных сетей в более безопасные. Один из них заключается в использовании команды access-list, другой - использовании шифрования и применения устройства защиты ASA в качестве получателя или отправителя в

сеансе шифрования. Оба этих метода не требуют создания канала передачи данных.

Статическая трансляция. Если политика защиты требует, чтобы внешние пользователи могли иметь доступ к серверам внутри защищенной сети, используйте команду static для указания IP-адресов, доступных извне, и команду conduit для разрешения (или запрета) доступа к ресурсам на основе номеров портов, протоколов и/или IP-адресов. При совместном использовании эти две команды создают туннель доступа, движение по которому разрешается только трафику, удовлетворяющему условиям, указанным командой conduit.

Команда static создает статическое отображение локального IP-адреса в глобальный IP-адрес (называемое сегментом статической трансляции или объектом xlate). Благодаря самой природе этого типа трансляции, устройству защиты ASA нет необходимости поддерживать базу данных состояний соединений или специальных метрик сеансов, что означает меньшую нагрузку на МСЭ.

Команда static. Статический адрес представляет собой постоянное взаимно однозначное отображение зарегистрированного IP-адреса в локальный IP-адрес внутри защищенной сети. Статические адреса рекомендуется использовать для хостов защищенной сети, которым требуется иметь конкретные IP-адреса. Команда static может создавать отдельную функцию трансляции (регулярную статику) или обеспечивать трансляцию диапазона адресов (сетевую статику). Данная команда аналогична статическому маршруту в таблице маршрутизации в том смысле, что она настраивается вручную и однозначно. Синтаксис команды:

static [(имя_ввутр_инт, иш_внешн_инт)] глобальн_ip локальн_ip
[netmask маска] [max_conns [em_limit]] [norandomseq]

Команда conduit. Открывает определенный порт ASA и разрешает потоку данных извне пройти к указанной подсети или хосту внутренней сети (обычно такой хост размещается в ДМЗ). Может оказаться удобным разместить в ДМЗ Web-сервер или сервер электронной почты, если по некоторым причинам к ним требуется доступ пользователей из Интернет. Синтаксис команды:

conduit {permit | deny} протокол глобальн_лр глобальн_маска
[оператор порт [порт]] внешн_ip внешн_маска
[оператор порт [порт]] оператор
conduit permit | deny icmp глобалън_ip глобальн_маска внешн ip
внешн_маска icmp_тип

Команда access-list Разрешает или запрещает устанавливать соединения из внешней сети по протоколам TCP, UDP и другим протоколам, поддерживаемых узлами внутренней сети. Кроме того, данная команда может

использоваться как для глобальных правил, так и для установки каких-то конкретных параметров. Например, команда access-list позволяет разрешить HTTP-доступ к определенному узлу.

Команды access-list и static необходимо использовать для обеспечения сеанса связи, направленного от интерфейса с более низким уровнем безопасности к интерфейсу с более высоким уровнем безопасности через устройство ASA, а также для передачи потока данных между этими двумя интерфейсами. Например, для разрешения входящего сеанса связи из внешней зоны в демилитаризованную или из внешней зоны - во внутреннюю.

Синтаксис команды: access-list {permit | deny} [оператор порт [порт]] внешн_ip внешн_маска протокол глобальн_лр глобальн_маска

Application Inspection. Позволяет проконтролировать, изменить, активизировать или отключить анализ протокола прикладного уровня в устройстве защиты ASA. Это очень мощное средство ASA, поскольку оно позволяет изменить содержимое пакета, чтобы последний удовлетворял требованиям конфигурации. Некоторые возможности защиты ASA опираются на средства контроля и изменения (или “исправления”) информации в пакетах, пересылаемых по сети. Различные сетевые протоколы (например, SMTP для передачи электронной почты) включают в пакеты специальную, зависящую от протокола информацию. Средства "исправления" протокола для пакетов SMTP предполагают изменение адресов, включенных в полезный груз пакета, проверку поддерживаемых команд и замену неподходящих символов.

По умолчанию устройство защиты ASA настроен на "исправление" протоколов FTP, SMTP, HTTP, RSH, SQL*NET и H.323.

Команда xlate. Очищает содержимое сегментов трансляции и возвращает к использованию для трансляции всего пула глобальных IP-адресов. Команду clear xlate следует использовать при удалении, изменении или добавлении псевдонимов, операторов conduit, global, nat и route. Это необходимо для того, чтобы старые преобразования не влияли на вновь настроенные и не нарушали их работу. Сегменты трансляции могут существовать в течение неопределенного времени, после того как в конфигурацию были внесены ключевые изменения. Если сегменты трансляции не очищаются с помощью команды clear xlate, следует сохранить конфигурацию и перезапустить устройство защиты ASA. Не забудьте включить в команду IP-адрес или имя интерфейса, который необходимо очистить, поскольку выполнение команды без указания соответствующего имени может привести *к нежелательным последствиям, не исключая повреждения таблицы соединений.*

Команда show xlate отображает подробный список параметров трансляции и соответствующих соединений.

Синтаксис команд:

clear xlate [глобальн_1р [локальн_1р]]
show xlate [глобальн_1р [локальн_1р]]

Команда ping (разрешение доступа). Ввиду того, что устройство защиты ASA по умолчанию запрещает весь трафик, вы не сможете использовать команду ping для проверки связи с защищенной сетью извне. Однако можно воспользоваться командой *conduit*, чтобы открыть канал, по которому ответы ICMP смогут вернуться назад через ASA.

При возможности направлять входящие запросы ping к внутренним хостам можно обеспечить более высокий уровень контроля, разрешив трафик echo-reply порта, но при этом возникает риск нарушения защиты.

Команда *conduit*, для проверки связи с защищенной сетью извне, должна использоваться только в целях отладки. Ее необходимо удалить сразу же по завершении проверки системы. Данная команда открывает брешь в ASA, наличием которой могут воспользоваться хакеры.

```
ciscoasa(config)# conduit permit icmp any any echo-reply
```

Ключевое слово *conduit* заставляет ASA подготовить коммуникационный конвейер, используя параметры, следующие за этим ключевым словом. Ключевое слово permit говорит ASA о том, что трафику, описанному следующим ключевым словом, следует разрешить любое движение через статику. Ключевое слово icmp информирует ASA о том, что протоколу ICMP (сообщениям ping) со всех глобальных IP-адресов будет открыт свободный проход. Ключевое слово any указывает, что через трафик ICMP извне могут быть доступны все глобальные IP-адреса. Ключевое слово any echo-reply сообщает ASA о том, что все внешние IP-адреса, к которым направляются запросы ping, должны иметь возможность отправить свои ответы echo-reply ICMP назад через ASA.

3.4 Аутентификация, авторизация и аудит

Зачастую, кроме определения каналов и статических отображений адресов, для реализации политики защиты в сети требуется иметь более надежные средства аутентификации и авторизации.

Чтобы централизованно управлять доступом пользователей и их правами, созданы приложения, позволяющие управление глобальной конфигурацией множества устройств. Это избавляет администратора от необходимости внесения изменений в конфигурацию каждого устройства в отдельности.

Несанкционированный доступ, а также возможность фальсификации и обмана в сетевой среде дают нарушителям потенциальную возможность получения доступа к сетевому оборудованию и сетевым службам. Архитектура AAA позволяет сильно ограничить возможности нарушителей, оставляя законным пользователям сети право иметь доступ к сетевым ресурсам.

Защита сетевого доступа - независимо от того, рассматривается она в применении к территориальной сети предприятия, удаленному доступу или

Интернет - имеет модульную архитектуру, состоящую из следующих трех компонентов.

Аутентификация. Требует от пользователей доказательства того, что они действительно являются теми, за кого себя выдают, например, посредством ввода имени пользователя и пароля, использования системы запросов/подтверждений, идентификационных карт или какого-то другого метода.

Пример: “Я - пользователь student, и мой пароль validateme доказывает это”.

Авторизация. После аутентификации пользователя сервис авторизации решает, - к каким ресурсам разрешается доступ данному пользователю и какие действия разрешается ему выполнять.

Пример: “Пользователь student может иметь доступ к узлу NT_Server посредством Telnet”

Аудит. Запись того, что пользователь действительно делал, к чему имел доступ и в течение какого времени, осуществляется с целью учета, контроля и выяснения стоимости. С помощью аудита можно проследить за тем, как используются сетевые ресурсы. Аудит может быть применен для анализа практики сетевого доступа и обнаружения сетевых вторжений.

Пример: “Пользователь student получал доступ к узлу NT посредством Telnet 15 раз”

Когда средства аудита AAA активизированы, устройство защиты ASA сообщает о действиях пользователя серверу TACACS+ или RADIUS в виде контрольных записей базы данных аудита.

Сервер TACACS+ или RADIUS может анализировать эти данные и компилировать новые с целью осуществления сетевого управления, контроля или взимания платы.

Настройка средств аутентификации и авторизации в устройстве ASA также называется настройкой режима прозрачного прокси-сервера (cut-through proxy). При использовании данной технологии прозрачной (т.е. невидимой пользователю) проверки идентификации пользователей резко повышается производительность брандмауэра. В результате этой проверки принимается решение о разрешении или блокировании доступа определенным TCP- и UDP-приложениям. Данный метод лишен недостатков, проявляющихся при сходной конфигурации в других МСЭ, реализованных на основе UNIX и других операционных систем. Кроме того, данный метод позволяет использовать службы аутентификации и авторизации на серверах CiscoSecure ACS. При работе в режиме прозрачного прокси-сервера устройство защиты ASA определяет необходимость основывающейся на пользователе аутентификации сеанса связи, предоставляет соответствующий механизм запроса пользовательского имени и пароля, а также аутентифицирует пользователей с помощью стандартных баз данных систем TACACS+ и RADIUS. После успешного прохождения пользователем аутентификации устройство защиты

ASA прекращает работу с этим потоком данных и дальнейший обмен информацией осуществляется непосредственно между клиентом и сервером. Брандмауэр же лишь следит за информацией о состоянии сеанса.

Типичным применением данной технологии является проверка пользователей, которые осуществляют доступ к ДМЗ из Интернета. На рисунке 3**.5** показан пример входа пользователя на определенный URL-адрес для доступа к Web-серверу. Для этого пользователю необходимо пройти аутентификацию и авторизацию, в ходе которых требуется ввести пользовательский идентификатор и пароль. Пользователь вводит данную информацию, затем она передается брандмауэру в незашифрованном виде, брандмауэр передает ее на AAA-сервер, на котором выполняется CiscoSecure ACS. В случае успешного прохождения аутентификации пользователь получает разрешение на взаимодействие с запрашиваемым сервером. Если для соединения требуется пароль для входа на Web-сервер, то пользователю необходимо также ввести и эти данные:

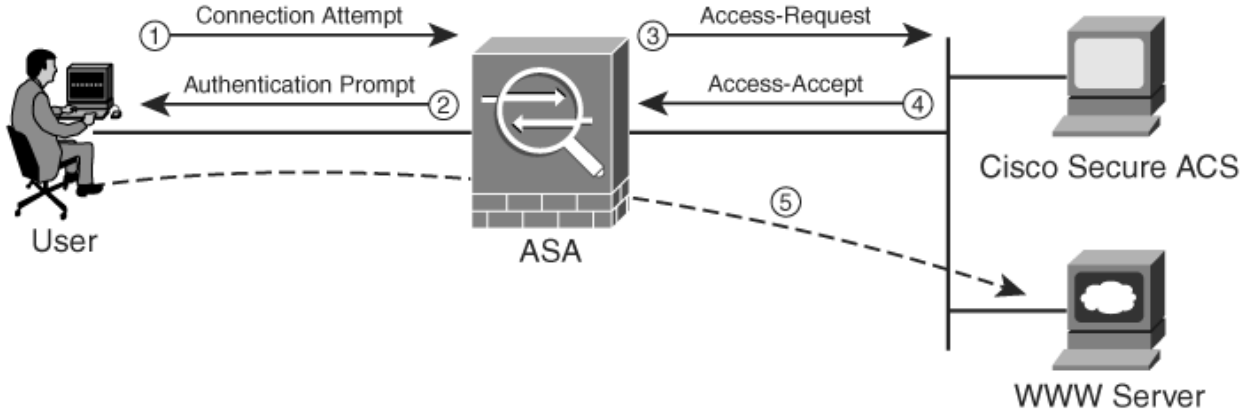

Рисунок 3.5 - Режим прозрачного прокси-сервера (Cut-Through Proxy Feature)

1) пользователь делает запрос на доступ к Web-серверу;

2) Cisco ASA запрашивает пользователя аутентификацию;

3) Cisco ASA передает ее на сервер CiscoSecure ACS для проверки введенных данных;

4) сервер подтверждает подлинность пользователя и посылает сообщение ASA;

5) Cisco ASA позволяет пользователю обращаться к серверу сети.

Настройка средств AAA

Первым шагом является информирование устройство защиты ASA о том, как получить доступ к серверу AAA и как обращаться к нему.

Следующая команда предназначена для инициализации настройки сервера AAA.

```
aaa-server тег_группы [имя_интерфейса) host гр_сервера ключ
timeout секунды
```

```
aaa-server тег_группы protocol протокол_аут
```

Т а б л и ц а 3.3 - Параметры команды AAA.

Параметр команды	Описание
тег_группы	Указывает имя, представляющее группу партнеров аутентификации
имя_иитерфейса	Имя интерфейса ASA (определяемое командой nameif), с которого разрешен доступ к серверу AAA
host ip_сервера	IP-адрес сервера AAA
ключ	Пароль, используемый совместно с сервером AAA
timeout секунды	Предельное время ожидания ответа сервера AAA устройства защиты ASA до обращения к следующему серверу AAA из соответствующего списка
protocol протокол_аут	Указывает протокол защиты, например radius или tacacs+

Параметр тег_группы оказывается важным в тех случаях, когда имеется необходимость аутентифицировать различные сервисы и адреса источников с разными типами услуг (RADIUS, TACACS+ и т.д.). Можно определить до 16 значений тег_группы, характеризующих состояния 16 серверов AAA. Это в совокупности дает 256 пригодных к использованию серверов AAA, что существенно превышает любые реально необходимые требования.

Чтобы начать процесс настройки конфигурации сервисов AAA, необходимо иметь следующую информацию:

- IP-адрес сервера AAA (например, 10.1.1.4).
- Название используемого протокола AAA. В данном проекте используется сервер CiscoSecure ACS, поэтому соответствующим протоколом является TACACS+.
- Общий ключ (пароль) для обмена данными с сервером AAA (в нашем случае паролем будет cieco).

```
ciscoasa(config)#aaa-server main protocol tacacs+
ciscoasa(config)#aaa-server main (inside) host 10.1.1.4 cisco
timeout 20
```

Теперь, когда устройство защиты ASA осведомлен о существовании сервера AAA в сети, можно приступить к реализации конкретных требований политики защиты в рамках возможностей AAA. Рассмотрим команды, используемые для настройки сервисов AAA.

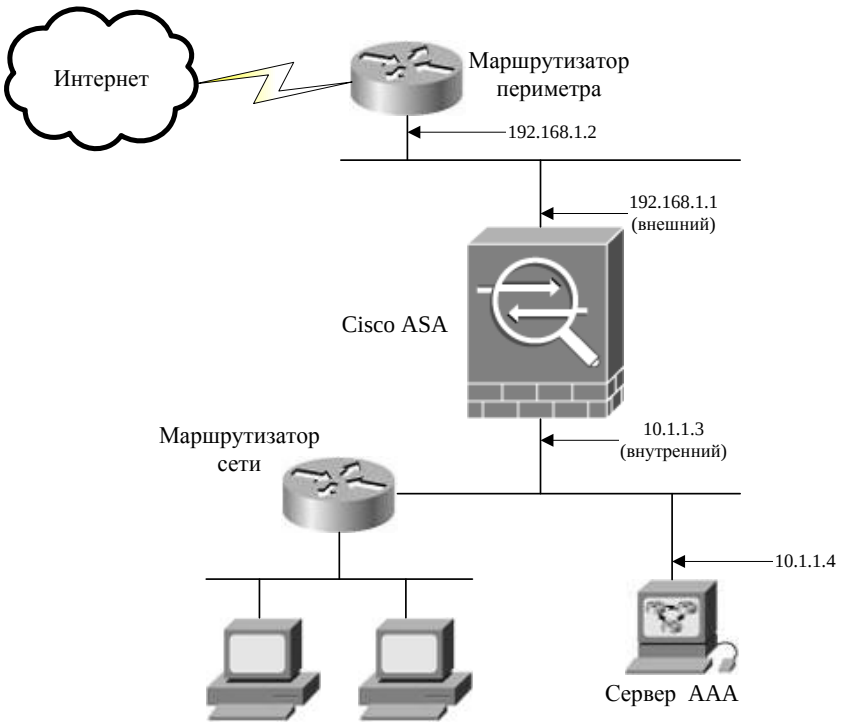

Рисунок 3.6 - Устройство защиты ASA в сети, предлагающей сервис защиты AAA

```
aaa authentication {include | exclude} сервяс_аут
{inbound | outbound | имя_интерфейса) локальн_ip локэльн_ыаска
внешн_ip  внешн_маска  тег_группы  aaa  authorization  {include  |
exclude} сервис_авт
{inbound | outbound | имя_интерфейса} покапьн_ip локалън_маска
вяешя_ip внешн_маска aaa accounting {include | exclude} сервис_ауд
{inbound | outbound | имя_интерфейса) локальн_ip локапьн_маска
внеши_ip внешн_маска тег_группы
```

Т а б л и ц а 3.4 - Параметры команд

Параметр	Описание
include	Создает новое правило, включающее указанный сервис
exclude	Создает исключение для ранее определенного правила с помощью отказа от необходимости аутентификации указанного сервиса для данного хоста. Позволяет указать порт для конкретного хоста (или хостов)
сервис_аут	Сервисы, требующие аутентификации для движения через брандмауэр. Можно использовать any, ftp, http или telnet. Значение any означает аутентификацию для всех сервисов TCP
сервис_авт	Сервисы, требующие авторизации. Можно использовать any, ftp, http или telnet. Для неуказанных сервисов выполняется неявная авторизация. Сервисы, указанные в команде aaa authentication, не влияют на авторизацию

Окончание таблицы 3.4

Параметр	Описание
сервнс_ауд	Сервис аудита. Контроль можно распространить как на все сервисы, так и на один или несколько типов сервиса. Допустимыми значениями являются any, ftp, http и telnet. Используйте any, чтобы обеспечить аудит для всех сервисов TCP. Чтобы обеспечить аудит для сервисов UDP, используйте форму "протокол/порт" команды
inbound	Аутентификация входящих соединений. "Входящие" означает, что соединения исходят от интерфейса с низшим уровнем защиты в направлении интерфейса с высшим уровнем защиты
outbound	Аутентификация исходящих соединений. "Исходящие" означает, что соединения исходят от интерфейса с высшим уровнем защиты в направлении интерфейса с низшим уровнем защиты
имя_интерфейса	Имя интерфейса, при обращении с которого требуется аутентификация пользователя. Используйте имя интерфейса в комбинации с адресами локальн_ip и внешн_ip, чтобы выяснить, откуда исходит попытка доступа. Адрес локальн_1p всегда размещается на интерфейсе с высшим уровнем защиты, а внешн_ip - на интерфейсе с низшим уровнем защиты
локальн_ip	IP-адрес хоста или сети, которые следует аутентифицировать. Можно установить этот адрес равным 0, чтобы обозначить все хосты и позволить серверу аутентификации самому решить, какие хосты следует аутентифицировать
локальн_маска	Сетевая маска для локальи ip. Всегда указывайте конкретное значение маски. Используйте 0, если для IP-адреса указано 0. Для хоста используйте 255.255.255.255
внешн_ip	IP-адрес хостов, которым разрешается доступ к адресу локальи ip. Используйте О, чтобы обозначить все хосты
внешн_маска	Сетевая маска для виеши ip. Всегда указывайте конкретное значение маски. Используйте 0, если для IP-адреса указано 0. Для хоста используйте 255.255.255.255
тег_группы	Тег группы, назначенный командой aaa-server

Как в большинстве других команд устройства защиты ASA, в IP-адресах и сетевых масках 0 является сокращением 0.0.0.0. Некоторые примеры команд аутентификации AAA устройства защиты ASA предлагаются ниже.

Пример авторизации для любого исходящего сеанса Telnet от сервера AAA с именем main:

```
ciscoasa(config)#aaa authorization telnet outbound 0 0 0 0 main
```

Пример авторизации всех сеансов, исходящих от сервера AAA с именем main.

```
ciscoasa(config)#aaa authorization any outbound 0 0 0 0 main
```

В следующем примере указано получение информации сервера AAA с именем main, необходимой для аутентификации доступа к консольному порту устройства ASA.

```
ciscoasa(config)iaaa authentication any serial console main
```

Команды всех трех примеров могут использоваться для контроля исходящего доступа к Интернету со стороны пользователей и внутренних сетевых устройств. Те же команды можно применить и для контроля действий пользователей, а также для того, чтобы разрешить или запретить им использовать определенные сервисы.

Сервисы AAA позволяют, даже в очень большой сети, реализовать политику защиты, имеющую высокую степень детализации. Соответствующие возможности огромны и поэтому должны использоваться аккуратно. Излишние требования авторизации и аутентификации означают лишнюю нагрузку на устройство защиты ASA, сервер AAA, сеть и пользователей. Как и всегда, в этом деле необходим баланс.

3.5 Безопасное взаимодействие между головным офисом и филиалами

Благодаря виртуальным частным сетям (VPN) с поддержкой протоколов SSL и IPsec, предприятия могут обеспечить защищенное соединение удаленных офисов и удаленных пользователей, используя вместо дорогостоящих выделенных каналов WAN или каналов связи удаленного доступа экономичный доступ в Интернет от сторонних поставщиков.

Предприятия могут сократить затраты на расширение пропускной способности WAN, увеличив скорость соединения за счет высокоскоростного подключения к Интернету (например, DSL, Ethernet и кабельное подключение) и защиты с помощью зашифрованных туннелей VPN IPsec или SSL.

Виртуальные частные сети обеспечивают наивысший уровень безопасности посредством технологий шифрования и аутентификации, предназначенных для защиты передающихся по VPN данных от несанкционированного доступа. Предприятия могут воспользоваться преимуществами простой в предоставлении Интернет-инфраструктуры для быстрого добавления новых подразделений или пользователей, а также

значительно увеличить размеры сетей без существенного расширения инфраструктуры.

VPN с поддержкой SSL и IPsec стали основным решением для соединения удаленных офисов, удаленных пользователей и деловых партнеров, поскольку они:

- обеспечивают защищенные взаимодействия с помощью прав доступа, настроенных для отдельных пользователей, например для сотрудников, подрядчиков или партнеров;
- повышают производительность за счет расширения корпоративной сети и распространения приложений;
- сокращают расходы на передачу данных и повышают гибкость.

Существует два типа зашифрованных VPN:

- **VPN с поддержкой IPsec и типом соединения «узел-узел»:** Этот альтернативный вариант Frame Relay или сетей WAN с арендованными каналами позволяет предприятиям предоставить сетевые ресурсы офисам филиалов, домашним офисам и компаниям деловых партнеров.
- **VPN удаленного доступа:** Эта сеть предоставляет почти все приложения по обработке данных, голоса или видео для удаленного компьютера, имитируя ПК основного офиса. В зависимости от требований к развертыванию VPN удаленного доступа можно развернуть с использованием SSL VPN, IPsec или обоих вариантов.

Управление компании информировано о возможностях IPSec и сетях VPN (Virtual Private Network - виртуальная частная сеть). Им требуется квалифицированная консультация по поводу того, как идентифицировать угрозы нарушения защиты сети и выбрать соответствующую политику защиты, а также необходима экспертиза конфигурации сети с точки зрения возможности применения решений защиты, предлагаемых компанией Cisco.

Продукты Cisco для поддержки VPN используют набор протоколов IPSec, являющийся на сегодня промышленным стандартом обеспечения широких возможностей VPN. IPSec предлагает механизм защищенной передачи данных в IP-сетях, обеспечивая конфиденциальность, целостность и достоверность данных, передаваемых через незащищенные сети типа Internet. IPSec обеспечивает следующие возможности VPN в сетях Cisco.

- **Конфиденциальность данных.** Отправитель данных IPSec имеет возможность шифровать пакеты перед тем, как передавать их по сети.
- **Целостность данных.** Получатель данных IPSec имеет возможность аутентифи-цировать сообщающиеся с ним стороны (устройства или программное обеспечение, в которых начинаются и заканчиваются туннели IPSec) и пакеты IPSec, посылаемые этими сторонами, чтобы быть уверенным в том, что данные не были изменены в пути.

- **Аутентификация источника данных.** Получатель данных IPSec имеет возможность аутентифицировать источник получаемых пакетов IPSec. Этот сервис зависит от сервиса целостности данных.
- **Защита от воспроизведения.** Получатель данных IPSec может обнаруживать и отвергать воспроизведенные пакеты, не допуская их фальсификации и проведения атак внедрения посредника.

IPSec представляет собой основанный на стандартах набор протоколов и алгоритмов защиты. Технология IPSec и связанные с ней протоколы защиты соответствуют открытым стандартам, которые поддерживаются группой IETF (Internet Engineering Task Force - проблемная группа проектирования Интернет) и описаны в спецификациях RFC и проектах IETF. IPSec действует на сетевом уровне, обеспечивая защиту и аутентификацию пакетов IP, пересылаемых между устройствами (сторонами) IPSec - такими как маршрутизаторы Cisco, устройства защиты ASA/PIX, клиенты и концентраторы Cisco VPN, а также многие другие продукты, поддерживающие IPSec. Средства поддержки IPSec допускают масштабирование от самых малых до очень больших сетей.

Ассоциации защиты. IPSec предлагает стандартный способ аутентификации и шифрования соединений между сообщающимися сторонами IPSec. Чтобы обеспечить защиту связей, средства IPSec используют стандартные алгоритмы (т.е. математические формулы) шифрования и аутентификации, называемые преобразованиями. В IPSec используются открытые стандарты согласования ключей шифрования и управления соединениями, что обеспечивает возможность взаимодействия между сторонами. Технология IPSec предлагает методы, позволяющие сторонам IPSec "договориться" о согласованном использовании сервисов. Чтобы указать согласуемые параметры, в IPSec используются ассоциации защиты.

Ассоциация защиты (Security Association - SA) представляет собой согласованную политику или способ обработки данных, обмен которыми предполагается между двумя устройствами сообщающихся сторон. Одной из составляющих такой политики может быть алгоритм, используемый для шифрования данных. Обе стороны могут использовать один и тот же алгоритм как для шифрования, так и для дешифрования. Действующие параметры SA сохраняются в базе данных ассоциаций защиты (Security Association Database - SAD) обеих сторон.

Протокол IKE (Internet Key Exchange - обмен Internet-ключами) является гибридным протоколом, обеспечивающим специальный сервис для IPSec, а именно аутентификацию сторон IPSec, согласование параметров ассоциаций защиты IKE и IPSec, а также выбор ключей для алгоритмов шифрования, используемых в рамках IPSec. Протокол IKE опирается на протоколы ISAKMP (Internet Security Association and Key Management Protocol - протокол управления ассоциациями и ключами защиты в сети Internet) и Oakley, которые применяются для управления процессом создания и обработки ключей шифрования, используемых в преобразованиях IPSec. Протокол IKE применяется также для формирования ассоциаций защиты между

потенциальными сторонами IPSec. В данной книге, как в маршрутизаторах Cisco и устройствах защиты ASA/PIX, IKE является синонимом ISAKMP, т.е. аббревиатура IKE используется для обозначения любого из этих протоколов.

Как IKE, так и IPSec используют ассоциации зашиты, чтобы указать параметры связи. Компоненты IPSec, ассоциаций защиты и IKE будут рассмотрены в данной главе немного позже.

Как работает IPSec

IPSec опирается на ряд технологических решений и методов шифрования, но действие IPSec в общем можно представить в виде следующих главных шагов.

Шаг 1. Начало процесса IPSec. Трафик, которому требуется шифрование в соответствии с политикой защиты IPSec, согласованной сторонами IPSec, начинает IKE-процесс.

Шаг 2. Первая фаза IKE. IKE-процесс выполняет аутентификацию сторон IPSec и ведет переговоры о параметрах ассоциаций защиты IKE, в результате чего создается защищенный канал для ведения переговоров о параметрах ассоциаций защиты IPSec в ходе второй фазы IKE.

Шаг 3. Вторая фаза IKE. IKE-процесс ведет переговоры о параметрах ассоциации защиты IPSec и устанавливает соответствующие ассоциации защиты IPSec для устройств сообщающихся сторон.

Шаг 4. Передача данных. Происходит обмен данными между сообщающимися сторонами IPSec, который основывается на параметрах IPSec и ключах, хранимых в базе данных ассоциаций защиты.

Шаг 5. Завершение работы туннеля IPSec. Ассоциации защиты IPSec завершают свою работу либо в результате их удаления, либо по причине превышения предельного времени их существования.

Технологии, используемые в рамках IPSec

В IPSec используются следующие технологии:

- протокол AH;
- протокол ESP;
- стандарт шифрования DES;
- стандарт шифрования 3DES;
- протокол IKE;
- метод согласования ключей по схеме Диффи-Хеллмана;
- хэшированные коды аутентичности сообщений (HMAC);
- защита RSA;
- центры сертификации.

4 Настройка устройства защиты Cisco ASA Series

Устройства защиты ASA может быть сконфигурировано с помощью интерфейса командной строки (CLI) и графического интерфейса ASDM. В данном проекте варианты конфигурации предоставлены с помощью интерфейса командной строки (CLI).

4.1 Настройка базовой конфигурации

Устройство защиты ASA можно настроить на выполнение функций защиты сети с помощью всего нескольких основных команд (*interface, nameif, security-level, ip address, speed, duplex, nat, global, nat-control* и *route*). Дополнительные возможности могут быть добавлены позже, в соответствии с политикой защиты.

Команда interface. Данная команда предназначена для идентификации типа используемых аппаратных средств, устанавливает параметры производительности и инициализирует интерфейсы.

Синтаксис команды: *interface идентификатор*

Команда nameif. Предназначена для задания имени каждому интерфейсу ASA. Синтаксис команды: *nameif идентификатор имя*

Команда security-level. определения уровня безопасности этого интерфейса (кроме имен которые заданы по умолчанию). В настройках по умолчанию внешнему интерфейсу присвоено имя Ethernet0 и уровень безопасности 0, а внутреннему интерфейсу присвоено имя Ethernet1 и уровень безопасности 100.

Синтаксис команды: *security-level уровень*

Команда ip address. Каждый из интерфейсов брандмауэра PIX настроен для работы с каким-либо определенным IP-адресом. После настройки IP-адреса системы и маски подсети можно с помощью команды show ip просмотреть список IP-адресов, связанных с сетевыми интерфейсами. В случае ошибки необходимо ввести повторно данную команду с корректными параметрами.

Синтаксис команды: *ip address имя IP_адрес [маска]*

Команда speed и duplex. Применяется для указания скорости и параметра дуплексной связи.

Синтаксис команды: *speed скорость [shutdown]*

Команда route. Устанавливает статический маршрут для интерфейса. Использование этой команды подразумевает задание определенного маршрута. Если же маршрут не указан, используется маршрут, заданный по умолчанию. Синтаксис данной команды выглядит следующим образом:

Синтаксис команды: *route имя IP_адрес маска шлюз [метрика]*

Команда global, позволяет создать пулы IP-адресов, с помощью которых команда nat сможет присваивать новые IP-адреса исходящим пакетам, чтобы

скрыть истинные адреса источника. Иными словами из более безопасных сетей (с более высоким уровнем безопасности интерфейса) к менее безопасным сетям (с менее высоким уровнем безопасности интерфейса).

Сетевая диаграмма, показанная на рисунке 4.1, представляет две пользовательские сети и призвана проиллюстрировать, как внутренние сети маскируются командами nat, применяемыми в этом случае.

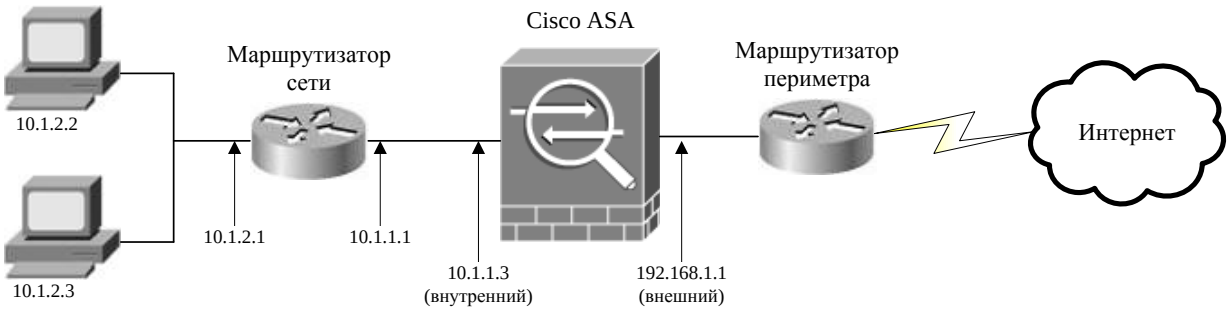

Рисунок 4.1 - Базовый пример конфигурации устройства защиты ASA

В листинге 4.1 показаны команды, которые следует ввести в режиме конфигурации, чтобы создать базовую конфигурацию устройства защиты ASA.

Листинг 4.1 Настройка базовой конфигурации ASA

```
! определим имена интерфейсов Ethernet 0 (внешний) и Ethernet 1 (внутренний), а также
! зададим их уровни безопасности и укажем скорость и параметры дуплексной связи
interface ethernet0
nameif outside
security-level 0
speed auto
!
interface ethernet1
nameif inside
security-level 100
spedd auto
! присваиваем IP-адреса внутренним и внешним сетевым интерфейсным платам
ip address inside 10.1.1.3 255.255.255.0
ip address outside 192.168.1.1 255.255.255.0
! определяем пул зарегистрированных IP-адресов, которые должны использоваться
! для исходящих соединений
global (outside) 1 192.168.1.128-192.168.1.254 netmask 255.255.255.0
! разрешаем трансляцию адресов источника пакета, входящих в ASA через внутренний
! интерфейс, в адреса из пула, обозначенного меткой 1
nat (inside) 1 0.0.0.0 0.0.0.0
! зададим маршруты по умолчанию для внутреннего и внешнего
```

```
интерфейсов.
! Поле метрика задает число транзитов от устройства ASA до
маршрутизатора;
! обычно оно равно 1
route outside 0.0.0.0 0.0.0.0 192.168.1.2 1
route inside 0.0.0.0 0.0.0.0 10.1.1.1 1
```

4.2 Настройка трансляции сетевых адресов в ASA

Для максимального повышения безопасности при реализации устройства защиты Cisco ASA важно знать, как пакеты передаются между интерфейсами с высоким уровнем безопасности и интерфейсами с низким уровнем безопасности, используя команды *nat, global, static* и *conduit* или *access-list* и *access-group* в программном обеспечении ASA версий 5.0 и более поздних.

Рассмотрим часть сети XYZ, которая показана на рисунке 4.2. Главным объектом внимания здесь является реализация политики защиты, обеспечивающей безопасность сети посредством трансляции сетевых адресов и размещения общедоступных серверов во внутреннем сегменте сети (с помощью команд static и conduit).

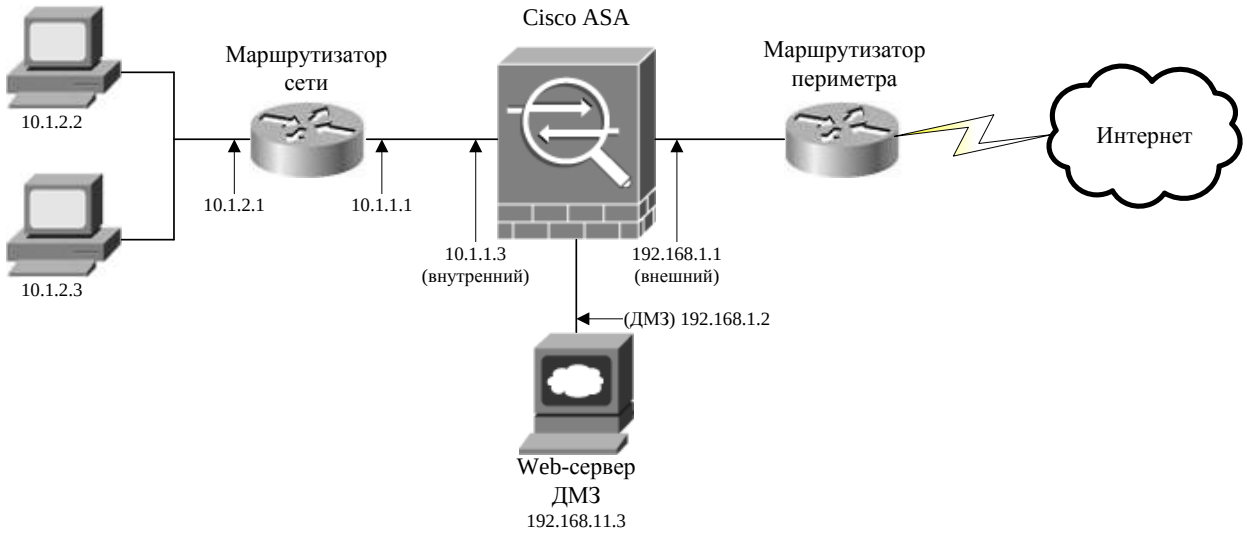

Рисунок 4.2 - Настройка трансляции сетевых адресов в ASA

Политика сетевой защиты, которую собирается реализовать компания XYZ, включает следующее:

- Использование средств трансляции сетевых адресов для перевода внутренних IP-адресов в зарегистрированные внешние IP-адреса.
- Размещение серверов, предлагающих общедоступные сервисы Интернет, в физически изолированном сегменте сети (ДМЗ) с целью максимальной защиты.
- Разрешение внутренним пользователям иметь доступ к серверам Интернет, размещенным в ДМЗ.

Команды конфигурации, представленные в листинге 4.2, позволяют настроить устройство защиты Cisco ASA в соответствии с целями компании XYZ.

Листинг 4.2. Вариант конфигурации трансляции сетевых адресов

```
interface ethernet0
nameif outside
security-level 0
speed auto
interface ethernet1
nameif inside
security-level 100
speed auto
interface ethernet0
nameif dmz
security-level 50
speed auto
enable password 6RD5.96v/eXN3kta encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname ASA1
ip address inside 10.1.1.3 255.255.255.0
ip address dmz 192.168.11.1 255.255.255.0
conduit permit icmp any any
conduit permit tcp host 192.168.1.10 eq www any
static    (dmz,outside)    192.168.1.10    192.168.11.3    netmask
255.255.255.255
nat(inside) 10 0
global (dmz) 1 192.168.11.10-192.168.11.20 netmask 255.255.255.0
global    (outside)    1    192.168.1.10    192.168.1.254    netmask
255.255.255.0
route outside 0.0.0.0 0.0.0.0 192.168.1.2 1
route inside 10.1.2.0 255.255.255.0 10.1.1.1
```

4.3 Настройка доступа через устройства защиты ASA

Компания XYZ приобрела устройство защиты Cisco ASA для работы с уже имеющимися в наличии маршрутизатором периметра и бастионными хостами в целях защиты внутренней сети от нарушителей. Необходимо так настроить брандмауэр, чтобы ограничить нежелательный доступ и в то же время оставить возможность для сотрудников аналитического отдела выполнять свою работу.

Рассмотрим часть сети XYZ, которая показана на рисунке 4.3. В фокусе внимания здесь оказывается создание системы защиты внутренних сетевых ресурсов, предполагающей минимум ограничений доступа для служащих при выполнении ими производственных функций.

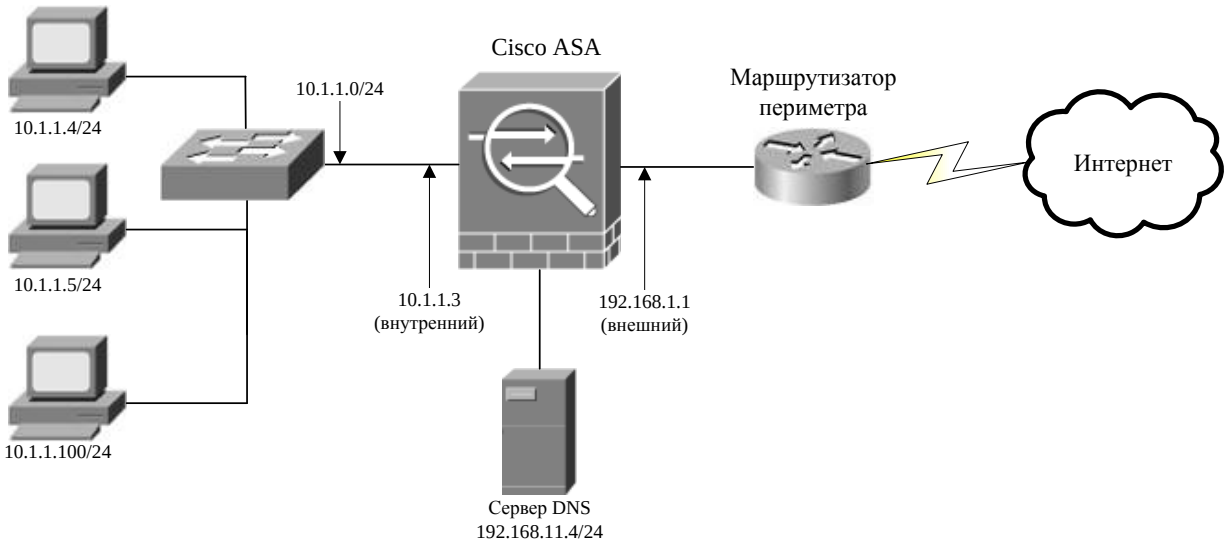

Рисунок 4.3 - Контроль доступа в Интернет компании XYZ

Политика сетевой защиты, которую намерена реализовать компания XYZ, предполагает следующее.

- Использование устройства защиты ASA для выполнения задач NAT в сети компании.
- Настройка статик для исходящего трафика с хоста DNS.
- Настройка статик и каналов для входящего трафика.
- Настройка устройство защиты ASA для доступа telnet.
- Настройка устройство защиты ASA для доступа ping.

После проверки конфигурации удалим команду conduit permit icmp any any echo-reply путем ввода команды no conduit permit icmp any any echo-reply.

Листинг 4.3. Вариант конфигурации доступа через ASA

```
interface ethernet0
nameif outside
security-level 0
speed auto
interface ethernet1
nameif inside
security-level 100
speed auto
interface ethernet0
nameif dmz
security-level 50
speed auto
enable password 6RD5.96v/eXN3kta encrypted
passwd 2KFQnbNIdI.2KY0U encrypted
hostname ASA1
pager lines 24
no logging timestamp
```

```
no logging standby
no logging console
no logging monitor
no logging buffered
no logging trap
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernetl auto
interface ethernet2 auto
mtu outside 1500
mtu inside 1500
mtu DMZ 1500
ip address outside 192.168.1.1 255.255.255.0
ip address inside 10.1.1.3 255.255.255.0
ip address DMZ 192.168 11.1 255.255.255.0
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address DMZ 0.0.0.0
arp timeout 14400
global    (outside)    1    192.168.1.10-192.168.1.254    netmask
255.255.255.0
nat (inside) 1 10.1.0.0 255.255.0.0 0 0
static    (inside,outside)    192.168.1.11    10.1.1.4    netmask
255.255.255.255 0 0
static    (inside,outside)    192.168.1.12    10.1.1.5    netmask
255.255.255.255 0 0
static   (inside,outside)   192.168.1.13   192.168.11.4   netmask
255.255.255.255 0 0
static    (inside,outside)    192.168.1.14    10.1.1.100    netmask
255.255.255.255 0 0
conduit permit icmp any any echo-reply
conduit permit tcp host 192.168.1.12 eq telnet host 192.168.1.2
conduit permit tcp host 192.168.1.11 eq www any
conduit permit udp host 192.168.1.11 eq syslog host 192.168.1.2
conduit permit tcp host 192.168.1.14 eq smtp any
no rip outside passive
no rip outside default
rip inside passive
rip inside default
no rip DMZ passive
no rip DMZ default
route outside 0.0.0.0 0.0.0.0 192.168.1.2 1
timeout  xlate  3:00:00  conn  1:00:00  half-closed  0:10:00  udp
0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
```

```
no snmp-server contact
snmp-server community public
no snmp-server enable traps
telnet timeout 5
terminal width 80
! Команда inspect esmtp (включенная в карту) позволяет серверу
! SMTP/ESMTP проверять приложение.
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
!
Cryptochecksum:377f6e0f8d9ac2f00141ef827bb4f9e6
: end
[OK]
```

Примечание: При использовании шифрования TLS для получения и передачи электронной почты, функция проверки ESMTP (подключаемая по умолчанию) в ASA теряет пакеты. Чтобы разрешить передачу электронных сообщения при включенном TLS, отключяем функцию проверки ESMTP, как показано ниже.

```
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#no inspect esmtp
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit
```

4.4 Настройка множества интерфейсов и средств AAA

Компании XYZ требуется установить устройство защиты ASA в главном здании, размещенном на территории предприятия. Часть этого здания компания XYZ сдает в субаренду партнерам (сеть которых является для компании внешней), обеспечивая им в качестве бонуса связь с Интернет. Для надежности компания XYZ имеет двух поставщиков услуг Интернет. Компания XYZ

намерена использовать устройство защиты ASA со множеством интерфейсов, чтобы обеспечить защиту сетевых соединений с каждым сегментом сети и с Интернет.

Структура сети и политика сетевой защиты должны быть реализованы с учетом следующих требований компании XYZ.

- IP-адреса:
  - административная сеть (локальная): 10.1.1.0/24;
  - сеть клиента 1 (локальная): 10.2.1.0/24;
  - сеть клиента 2 (локальная): 10.3.1.0/24;
  - ДМЗ (локальная): 192.168.11.0/24;
  - поставщик 1 (глобальная): 192.168.1.0/24;
  - поставщик 2 (глобальная): 192.168.2.0/24.

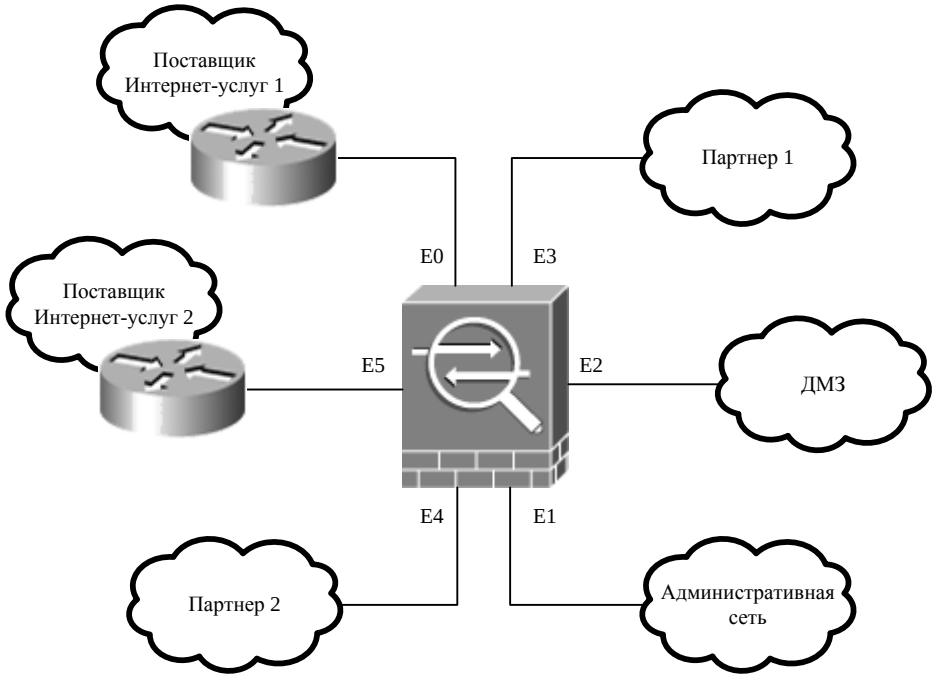

Рисунок 4.4 - Структура сети головного офиса компании XYZ

- Трансляция сетевых адресов:
  - управление класса C использует трансляцию PAT с адресом 192.168.1.127;
  - управление класса C использует диапазон глобальных IP-адресов от 192.168.1.10 до 192.168.1.126 (включительно);
  - клиент 1 использует глобальные адреса в диапазоне от 192.168.1.128 до 192.168.1.254 (включительно);
  - клиент 2 использует глобальные адреса в диапазоне от 192.168.2.128 до 192.168.2.254 (включительно);
  - все остальное (или дополнительное) управление и внутренние IP-адреса клиентов должны использовать для пула трансляции остальные глобальные адреса;

    - внутренние клиенты связываются с помощью полнодуплексных Ethernet-соединений типа 100BaseTX;
    - поставщики услуг Интернет связываются с помощью полудуплексных Ethernet-соединений типа l00BaseT.
- Некоторые адреса в ДМЗ будут отображаться статически.
- Доступ ICMP извне ограничивается, но разрешаются ответы на трафик, порожденный изнутри.
- Активизируется сервис syslog со следующими параметрами:
    - маршрутизатору периметра дается возможность посылать сообщения syslog в адрес 10.1.1.5 локальной сети администрирования;
    - сервис syslog связывается с адресом 10.1.1.5;
    - сообщения syslog должны включать информацию об отказах установки сеансов;
    - размер буфера syslog должен быть равным 1 Кбайт информации.
- Серверу AAA назначается адрес 10.1.1.4 локальной сети администрирования.
- Для доступа к частному Web-узлу активизируется аутентификация и аудит AAA.

Здесь показана лишь одна из возможных конфигураций, реализующих данную политику. Можно сконфигурировать устройство защиты ASA иначе, обеспечив выполнение тех же требований.

Листинг 4.4. Конфигурация множества интерфейсов и средств AAA

```
ciscoasal#write terminal
Building configuration... : Saved
ASA Version 7.2(1)
!
interface ethernet0
nameif providerl
security-level 0
interface ethernetl
nameif admin
security-level l00
interface ethernet2
nameif dmz
security-level 60
interface ethernet3
nameif clientl
security50
interface ethernet4
nameif client2
security-level 50
interface ethernet5
nameif provider2
security-level l0
enable password AOywFtG5fs31jpjx encrypted
```

```
passwd FSbblTfmfXKC.viH encrypted
hostname ciscoasal
pager lines 24
! Активизирует отправку контрольной информации серверу syslog.
logging timestamp
no logging standby
no logging console
no logging monitor
logging buffered errors
logging trap informational
logging facility 20
logging queue 1024
logging host admin 10.1.1.5
! Дополнительная информация для конфигурации интерфейсов Ethernet.
interface ethernet0 l0baset
interface ethernetl l00full
interface ethernet2 l00full
interface ethernet3 l00full
interface ethernet4 l00full
interface ethernet5 l0baset
mtu providerl 1500
mtu admin 1500
mtu clientl 1500
mtu client2 1500
mtu dmz 1500
mtu provider2 1500
! Дополнительная информация для конфигурации интерфейсов Ethernet.
ip address admin 10.1.1.1 255.255.254.0
ip address clientl 10.2.1.1 255.255.0.0
ip address client2 10.3.1.1 255.255.0.0
ip address dmz 192.168.11.1 255.255.255.0
ip address providerl 192.168.1.1 255.255.255.252
ip address provided 192.168.2.1 255.255.255.252
! Замечание. Адреса провайдера обычно задаются провайдером и не обязательно
! принадлежат диапазону IP-адресов, используемых глобально.
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
! Информация для пула NAT клиента.
nat (admin) 1 10.1.1.0255.255.255.0
nat (admin) 2 10.1.4.0 255.255.255.0
nat (clientl) 3 10.2.1.0 255.255.255.0
nat (client2) 4 10.3.1.0 255.255.255.0
nat (admin) 5 0.0.0.0 0.0.0.0
nat (clienti) 5 0 0        ! (это то же самое, что и 0.0.0.0)
nat (client2) 5 0 0
global (providerl) 1 192.168.1.10-192.168.1.126
```

```
global (providerl) 2 192.168.1.127
global (providerl) 3 192.168.1.128-192.168.1.253
global (provided) 4 192.168.2.128-192.168.2.254
global (providerl) 5 192.168.1.254
! Конфигурация статик и каналов NAT.
static    (dmz,provider1)    192.168.1.10    10.1.1.4    netmask
255.255.255.255 0 0
static    (dmz,provider1)    192.168.1.13    10.1.1.5    netmask
255.255.255.255 0 0
static   (dmz,providerl)   192.168.1.11   192.168.11.3   netmask
255.255.255.255 0 0
static   (dmz,provider1)   192.168.1.12   192.168.11.4   netmask
255.255.255.255 0 0
conduit permit tcp host 192.168.1.12 eq smtp any 0 0
conduit permit tcp host 192.168.1.11 eq www any 0 0
conduit permit tcp host 192.168.1.11 eq ftp any 0 0
conduit permit tcp host 192.168.2.11 eq ftp any 0 0
conduit permit tcp host 192.168.1.13 eq syslog any 0 0
! Разрешения для фильтрация ICMP.
conduit permit icmp any any echo-reply
conduit permit icmp any any unreachable
conduit permit icmp any any redirect
conduit permit icmp any any time-exceeded
conduit deny icmp any any
rip providerl passive
no rip providerl default
no rip admin passive
no rip admin default
no rip clientl passive
no rip clientl default
no rip client2 passive
no rip client2 default
no rip dmz passive
no rip dmz default
no rip provider2 passive
no rip provider2 default
timeout  xlate  24:00:00  conn  12:00:00  half-closed  0:10:00  udp
0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:05:00 absolute
! Настройка аутентификации клиента.
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server admin protocol tacacs+
aaa-server admin (admin) host 10.1.1.4 AdminKey timeout 30
aaa authentication http inbound host 0 0 0
aaa accounting http inbound 0 0 0 0 admin
snmp-server location Lexington, KY
snmp-server contact Scott Morris
snmp-server community emanon
snmp-server enable traps
telnet 10.1.1.4 255.255.255.0 admin
```

```
telnet timeout 5
terminal width 80
! Команда inspect esmtp (включенная в карту) позволяет серверу
! SMTP/ESMTP проверять приложение.
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
!
Cryptochecksum:dc2a867907ccf77cb25dl42d34fb3449
: end
```

4.5 Настройка дополнительных возможностей ASA

Компания XYZ намерена добавить некоторые новые возможности в сеть своего офиса и внести некоторые изменения в политику сетевой защиты. Напомню о том (см. пункт 4.1.4), что компания XYZ подключена к сетям двух поставщиков услуг Internet и обеспечивает сервис двум партнерам в рамках экстрасети.

Структура сети головного офиса компании XYZ на рисунке 4.4.

Изменения, которые компания XYZ намерена внести в структуру своей сети и политику защиты, являются следующими.

- Ограничивается доступ сетей внутренних клиентов к серверу Lotus Notes (адрес 192.168.11.44 в сети ДМЗ).
- Добавляется сервер WebSENSE (адрес 10.1.1.77 в локальной сети администрирования/управления), ограничивающий HTTP-доступ пользователей к локальной сети администрирования/управления.
- Добавляется локальная сеть для клиента 2, адреса которой не транслируются. Компания XYZ получила сеть 208.155.233.0/24.
- Вводится использование SNMP на базовом уровне, информация прерываний направляется системе CiscoWorks по адресу 10.1.1.99 в локальной сети администрирования/управления.

Здесь показана лишь одна из возможных конфигураций, реализующих данную политику. Можно сконфигурировать брандмауэр ASA иначе, обеспечив выполнение тех же требований.

Листинг 4.5. Конфигурация дополнительных возможностей ASA

```
ciscoasal#write terminal
Building configuration... : Saved
ASA Version 7.2(1)
!
interface ethernet0
nameif providerl
security-level 0
interface ethernetl
nameif admin
security-level l00
interface ethernet2
nameif dmz
security-level 60
interface ethernet3
nameif clientl
security50
interface ethernet4
nameif client2
security-level 50
interface ethernet5
nameif provider2
security-level l0
enable password AOywFtG5fs31jpjx encrypted
passwd FSbblTfmfXKC.viH encrypted
hostname ciscoasal
pager lines 24
! Активизирует отправку контрольной информации серверу syslog.
logging timestamp
no logging standby
no logging console
no logging monitor
logging buffered errors
logging trap informational
logging facility 20
logging queue 1024
logging host admin 10.1.1.5
! Дополнительная информация для конфигурации интерфейсов
Ethernet.
interface ethernet0 l0baset
interface ethernetl l00full
interface ethernet2 l00full
interface ethernet3 l00full
interface ethernet4 l00full
interface ethernet5 l0baset
mtu provider1 1500
mtu admin 1500
```

```
mtu clientl 1500
mtu client2 1500
mtu dmz 1500
mtu provider2 1500
! Дополнительная информация для конфигурации иитерфейсов Ethernet.
ip address admin 10.1.1.1 255.255.254.0
ip address clientl 10.2.1.1 255.255.0.0
ip address client2 10.3.1.1 255.255.0.0
ip address dmz 192.168.11.1 255.255.255.0
ip address providerl 192.168.1.1 255.255.255.252
ip address provided 192.168.2.1 255.255.255.252
! Замечание. Адреса провайдера обычно задаются провайдером и не обязательно
! принадлежат диапазону IP-адресов, используемых глобально.
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
! Иифopмация для пула NAT клиента.
nat (admin) 0 208.155.233.0 255.255.255.0
nat (admin) 1 10.1.1.0 255.255.255.0
nat (admin) 2 10.1.4.0 255.255.255.0
nat (clientl) 3 10.2.1.0 255.255.255.0
nat (client2) 4 10.3.1.0 255.255.255.0
nat (admin) 5 0.0.0.0 0.0.0.0
nat (clienti) 5 0 0        ! (это то же самое, что и 0.0.0.0)
nat (client2) 5 0 0
global (providerl) 1 192.168.1.10-192.168.1.126
! Команда inspect esmtp (включенная в карту) позволяет серверу
! SMTP/ESMTP проверять приложение.
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
```

4.6 Настройка средств IPSec VPN для работы с общими ключами

IPSec (IP Security - набор открытых стандартов обеспечения конфиденциальности, целостности и аутентификации данных между равноправными участниками обмена данными) является базой применения открытых стандартов защиты частных коммуникаций в сетях IP. IPSec гарантирует конфиденциальность, целостность и достоверность данных при пересылке их через открытые сети IP. IPSec предоставляет необходимые компоненты для реализации гибкой политики защиты, основанной на использовании стандартов. IPSec может использоваться для защиты трафика между устройствами защиты периметра, а также для создания виртуальных частных сетей (VPN) между центральным подразделением корпоративной сети и удаленными ее частями, удаленными филиалами или сетями внешних партнеров. При этом можно шифровать весь поток данных между устройствами защиты или только поток данных между отдельными узлами или частями сети, расположенными за устройствами защиты. Корпоративные потребители получают все преимущества, доступные для частных сетей, включая защиту, качество обслуживания (QoS), управляемость и надежность.

В процессе настройки средств шифрования IPSec устройства защиты ASA, использующих согласованные общие ключи, необходимо решить следующие четыре задачи.

Задача 1. Подготовка к использованию IPSec. Данная задача включает определение деталей политики шифрования, идентификацию хостов и сетей, которые необходимо защитить, выяснение характеристик сторон IPSec, возможностей IPSec, которые будут необходимы, а также проверку того, что существующие списки доступа, применяемые для фильтрования пакетов, позволяют использовать IPSec.

Для успешной реализации сети IPSec требуется тщательно спланировать процесс настройки взаимодействующих устройств защиты ASA и других объектов IPSec. Настройка параметров шифрования IPSec может оказаться достаточно сложным делом. Планирование для IPSec предполагает выполнение следующих действий.

Шаг 1. Определение политики IKE (первая фаза IKE, основной режим) для связи между сторонами IPSec в зависимости от числа и размещения сторон.

Шаг 2. Определение политики IPSec (вторая фаза IKE, быстрый режим), в частности такие параметры сторон IPSec, как IP-адреса, а также наборы преобразований и режимы IPSec.

Шаг 3. Проверка текущей конфигурации с помощью команд write terminal, show isakmp, show isakmp policy, show crypto map и других команд show.

Шаг 4. Проверка того, что сеть работает без шифрования, чтобы избежать основных проблем маршрутизации (для этого используется команда ping и тестовый трафик до включения средств шифрования).

Шаг 5. Проверка того, что существующие списки доступа в маршрутизаторе периметра и устройстве ASA позволяют трафик IPSec; в противном случае соответствующий трафик будет отфильтрован.

Задача 2. Настройка IKE для работы с заранее согласованными ключами. Предполагает активизацию средств IKE, создание политики IKE и проверку правильности выбранной конфигурации. Настройка параметров IKE предполагает выполнение следующих шагов.

Шаг 1. Активизация или отключение IKE с помощью команды isakmp enable.

Шаг 2. Создание политик IKE с помощью команд isakmp policy.

Шаг 3. Выбор общих ключей с помощью команды isakmp key и связанных с ней команд.

Шаг 4. Проверка конфигурации IKE с помощью команды show isakmp [policy].

Задача 3. Настройка IPSec. Определение множеств преобразований, создание списков шифрованного доступа и криптографических карт, а также применение криптографических карт к соответствующим интерфейсам. В этом разделе описываются действия, выполняемые в процессе настройки IPSec.

Шаг 1. Настройка списков шифрованного доступа с помощью команды access-list.

Шаг 2. Настройка наборов преобразований с помощью команды crypto ipsec transform-eet.

Шаг 3. (Необязательный.) Установка глобальных пределов существования ассоциаций защиты IPSec посредством команды crypto ipsec security-association lifetime.

Шаг 4. Настройка криптографических карт с помощью команды crypto map.

Шаг 5. Применение криптографических карт к интерфейсам посредством команды crypto map имя-карты interface интерфейс.

Шаг 6. Проверка конфигурации IPSec с помощью множества предназначенных для этого команд show.

Задача 4. Тестирование и контроль IPSec. Завершающей задачей настройки IPSec для работы с общими ключами является проверка того, что параметры IKE и IPSec были указаны правильно и вся система работает должным образом. Устройства ASA предлагает ряд команд show, clear и debug, которые оказываются полезными для проверки и контроля IKE и IPSec.

Компания XYZ хотела бы использовать устройство защиты Cisco ASA для создания защищенной сети VPN между узлами, связанными через Интернет. Нашей задачей является настройка шлюза защиты VPN, использующего связь IPSec между двумя брандмауэрами ASA с применением согласованных общих ключей и позволяющего доступ к Web-серверу.

Политика сетевой защиты, которую намерена реализовать компания XYZ, заключается в следующем:

• Необходимо использовать Интернет, чтобы связать сеть удаленного подразделения с корпоративной сетью и обеспечить возможность передачи данных.

• Необходимо аутентифицировать трафик между корпоративной сетью и филиалами, чтобы никто не мог модифицировать или фальсифицировать пакеты во время их передачи.

• Для аутентификации необходимо использовать заранее согласованные общие ключи IKE и алгоритм MD5.

• Целостность потока данных между корпоративной сетью и филиалами через Интернет должно обеспечивать шифрование DES с 56-битовым ключом.

• Трафик Web между внутренними серверами NT всех узлов должен шифроваться.

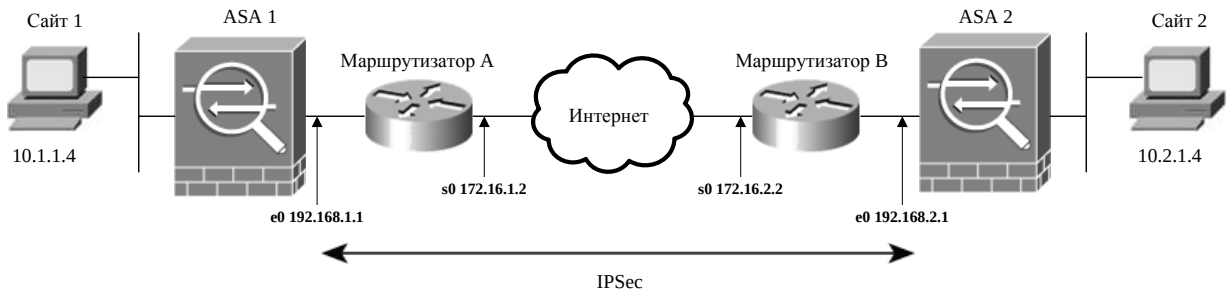

Рисунок 4.5 - Топология сети для использования IPSec в ASA

Рассмотрим вариант конфигурации брандмауэра ASA 1 и ASA 2 в сети компании XYZ, показанный в листингах 4.X и 4.X. В этом примере реализуются описанные выше требования политики защиты для IPSec. Здесь показана одна из возможных конфигураций, реализующих данную политику. Можно настроить брандмауэр иначе, обеспечив выполнение тех же требований. Обратите внимание на комментарии, объясняющие связь команд конфигурации с конкретными требованиями политики защиты. В данном примере показана конфигурация для брандмауэров Cisco ASA 5510.

Листинг x.x. Конфигурация для ASA 1

```
! Настройка IP-адресов для всех интерфейсов устройства ASA.
ip address outside 192.168.1.1 255.255.255.0
ip address inside 10.1.1.3 255.255.255.0
ip address dmz 192.168.11.1 255.255.255.0
global    (outside)    1    192.168.1.10-192.168.1.254    netmask
255.255.255.0
! Создание глобального пула на внешнем интерфейсе, активизация
NAT.
nat (inside) 1 10.0.0.0 255.0.0.0 0 0
!Создание статической трансляции между глобальным и внутренним
адресами
```

```
! сервера Windows NT.
static (inside,outside) 192.168.1.10 10.1.1.4 netmask
255.255.255.255 0 0
!Список шифрованного доступа указывает, что трафик между
внутренними серверами
! Windows NT за устройствами ASA должен шифроваться.
! IP-адреса источника и получателя являются глобальными IP-
адресами статик.
! Списки доступа устройств защиты демонстрируют зеркальное
соответствие.
access-list 101 permit ip host 192.168.1.10 host 192.168.2.10
!Каналы позволяют доступ ICMP и Web с целью тестирования.
conduit permit imp any any
conduit permit top host 192.168.1.10 eq www any
route outside 0.0.0.0 0.0.0.0 192.168.1.2 1
! Разрешение IPSec обойти список доступа и другие ограничения.
sysopt connection permit-ipsec
! Определяет использование esp-des в наборе преобразований
криптографической карты.
crypto ipsec transform-set asa2 esp-des
crypto nap peer2 10 ipsec-isakmp
!Определяет криптографическую карту.
crypto map peer2 10 match address 101
! Определяет удаленную сторону в криптографической карте путем
указания IP-адреса
! внешнего интерфейса удаленного устройства ASA.
crypto map peer2 10 set peer 192.168.2.1
! Определяет использование данного набора преобразований в
криптографической карте.
crypto map peer2 10 set transform-set asa2
! Связывает криптографическую карту с внешним интерфейсом
брандмауэра ASA.
! Как только криптографическая карта связывается с интерфейсом,
! политики IKE и IPSec становятся активными.
crypto map peer2 interface outside
! Активизирует IKE на внешнем интерфейсе.
isakmp enable outside
!Определяет общий ключ IKE.
isakmp key ciscol23 address 192.168.2.1 netmask 255.255.255.255
! Определяет политику IKE, использующую общие ключи для
аутентификации.
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash sha
! Определяет использование группы 1 Диффи-Хеллмана. Можно было
бы использовать
! группу 2, обеспечивающую более сильную защиту вместе с
преобразованием esp-3des,
! но для этого потребуется больше процессорного времени.
isakmp policy 10 group 1
! Определяет параметры длительности существования IKE.
isakmp policy 10 lifetime 86400
```

Листинг x.x. Конфигурация для ASA 2

```
! Настройка IP-адресов для всех интерфейсов устройства ASA.
ip address outside 192.168.2,1 255.255.255.0
ip address inside 10.2.1.3 255.255.255.0
ip address dmz 192.168.12.1 255.255.255.0
global (outside) 1 192.168.2.10-192.168.2.254 netmask
255.255.255.0
! Создание глобального пула на внешнем интерфейсе, активизация
NAT.
nat (inside) 1 10.0.0.0 255.0.0.0 0 0
! Создание статической трансляции между глобальным и внутренним
адресами
! сервера Windows NT.
static (inside,outside) 192.168.2.10 10.2.1.4 netmask
255.255.255.255 0 0
! Список шифрованного доступа указывает, что трафик между
внутренними серверами
! Windows NT за устройствами ASA должен шифроваться. IP-адреса
источника
! и получателя являются глобальными IP-адресами статик. Списки
доступа
! устройств ASA 1 и ASA 2 являются зеркальными отражениями друг
друга.
access-list 101 permit ip host 192.168.2.10 host 192.168.1.10
! Каналы позволяют доступ ICMP н Web с целью тестирования.
conduit permit icmp any any
conduit permit top host 192.168.2.10 eq www any
route outside 0.0.0.0 0.0.0.0 192.168.2.2 1
! Разрешение IPSec обойти список доступа и другие ограничения.
sysopt connection permit-ipsec
! Определяет использование esp-des в наборе преобразований
криптографической карты.
crypto ipsec transform-set asal esp-des
crypto map peerl 10 ipsec-isakmp
! Определяет криптографическую карту.
crypto map peerl 10 match address 101
! Определяет удаленную сторону в криптографической карте путем
указания IP-адреса
! внешнего интерфейса удаленного брандмауэра ASA.
crypto map peerl 10 set peer 192.168.1.1
! Определяет использование данного набора преобразований в
криптографической карте.
crypto map peerl 10 set transform-set asal
! Связывает криптографическую карту с внешним интерфейсом
устройства ASA.
! Как только криптографическая карта связывается с интерфейсом,
! политики IKE и IPSec становятся активными.
crypto map peerl interface outside
! Активизирует IKE на внешнем интерфейсе.
isakmp enable outside
! Определяет общий ключ IKE.
```

```
isakmp key ciscol23 address 192.168.2.2 netmask 255.255.255.255
! Определяет политику IKE, использующую общие ключи для аутентификации.
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash sha
! Определяет использование группы 1 Диффи-Хеллмаиа. Можно было бы использовать
! группу 2, обеспечивающую более сильную защиту вместе с преобразованием espSdes,
! но для этого потребуется больше процессорного времени.
isakmp policy 10 group 1
! Определяет параметры длительности существования IKE.
isakmp policy 10 lifetime 86400
```

5 Безопасность жизнедеятельности

5.1 Анализ условий труда

Согласно теме выпускной работы реализуется защита периметра корпоративной сети на основе применения устройства защиты Cisco ASA Series.

Основное оборудование располагается в серверной комнате, которая так же является центральным узлом управления сетью на сетях передачи данных. Включая необходимые сервера, в этом помещении установлены источники бесперебойного питания (UPS) на случай отключения основного электропитания, климато-техническая установка для поддержания нужных температурных условий, специальный серверный коммутационный шкаф и рабочие места для системного администратора и помощника.

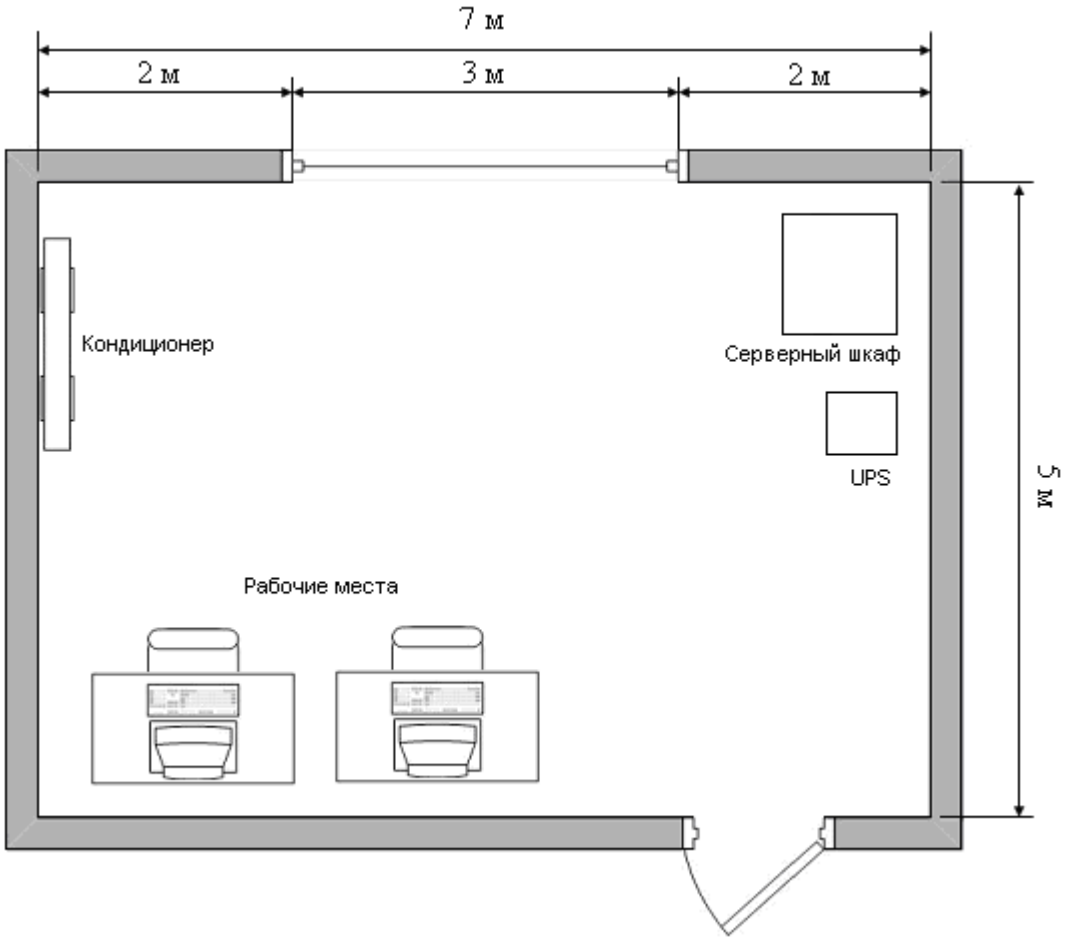

Рисунок 5.1 - Серверная комната

Для обслуживания оборудования и наблюдением за предоставляемыми услугами в помещении работает системный администратор и его помощник.

Согласно СНиП 2.2.2.542-96 общим требованиям к организации и оборудованию рабочих мест с ПЭВМ для сотрудников необходимо создать

условия труда, обеспечивающее оптимальную динамику работоспособности, хорошее самочувствие и сохранение их здоровья. Важным моментом организации рабочего места является определение занимаемой работником площади. Каждое рабочее место обеспечивается площадью 7 $м^2$ и кубатурой 21 $м^3$ на человека, при минимальных нормах 6 $м^2$ и кубатуре не менее 20 $м^3$. Эта площадь позволяет удобно и с наименьшей затратой энергии безопасно и производительно вести трудовой процесс.

Серверная комната, представленная на рисунке 5.1, имеет следующие размеры: длина - 7 м, ширина - 5 м и высота - 3 м.

5.1.1 Оценка освещенности

Рабочее помещение имеет достаточное естественное освещение, в виде 1 окна размером 1000 х 3000 мм. Естественное освещение не обеспечивает в течение всего рабочего времени необходимого освещения, поэтому в серверной комнате принята система искусственного общего освещения четырьмя светильниками по две люминесцентные лампы II группы ЛД, мощностью 40 Вт и световым потоком $Ф_л = 3120$ лм.

Для обеспечения искусственного освещения по СНиП РК 2.04-05-2002, необходимо чтобы выполнялось неравенство: $E_г \geq E_н$; где $E_н$ зависит от разряда зрительной работы. Установим разряд зрительной работы IV - средней точности, при этом $E_н = 150$ лк [18].

Работа системных администраторов в основном заключается в управлении и наблюдении за аппаратурой и при необходимости устранении мелких неполадок в работе оборудования. Таким образом, выполняемая работа системных администраторов относим к работе со средней точностью, т.е. к IV разряду зрительной работы.

Т а б л и ц а 5.1 - Разряд зрительной работы [18]

Размер минимального различаемого объекта	Расстояние от объекта до глаз работника	Разряд зрительной работы
1-10 мм	500 мм	IV

Вычислим $E_г$ и сравним с $E_н = 150$ лк. Расчет искусственного освещения проводим двумя методами: точечным и методом коэффициента использования светового потока.

5.1.2 Оценка микроклимата

Для вентиляции рабочего помещения используются каналы естественной вентиляции, прокладываемые при строительстве здания и открытые окна летом. Однако такая вентиляция не позволяет поддерживать климатические параметры рабочего помещения в пределах нормы (таблица 5.2) в условиях климата города Алматы (в особенности - летом).

Т а б л и ц а 5.2 - Допустимые нормы температуры, относительной влажности и скорости движения воздуха в обслуживаемой зоне жилых, общественных и административно-бытовых помещений для легкой (Iб) категории работ [19].

Период года	Температура воздуха, ^{0}C	Относительная влажность воздуха, %	Скорость движения воздуха, м/с, не более
Теплый	28 - 31	75	0,3
Холодный	20 - 24	75	0,2

Согласно ГОСТ 12.1.005-88 “ССБТ. Воздух рабочей зоны, общие санитарно-гигиенические требования”, работа людей в серверной комнате относится к категории Iб лёгкой физической. Категории работ по энергозатратам приведены в таблице 5.3.

Т а б л и ц а 5.3 - Категории работ по энергозатратам организма

Работа	Категория	Энергозатраты организма, Дж/с	Характеристика работы
Легкая	I б	138 - 172	Производится сидя, стоя или связана с ходьбой и сопровождается некоторым физическим напряжением

В серверной комнате, расположенного в городе Алматы, в период летнего времени температура +30°С и более, температура зимнего периода от +16 до +18°С. Сравнивая существующие параметры микроклимата комнаты и оптимальные микроклиматические условия для легкой категории работ видно что, в летнее время существует избыток тепла, а в зимний - недостаток. Таким образом, для поддержания условий микроклимата в помещении, целесообразно оборудовать системой кондиционирования. В связи с этим, произведем расчет системы кондиционирования.

5.2 Техническое решение вопросов охраны труда

5.2.1 Расчет искусственного освещения

Точечный метод

Исходные данные:

Разряд зрительной работы - IV;

Размеры помещения: 7х5х3;

Коэффициент отражения по IV разряду зрительных работ:

- потолка $\rho_{пот}$ = 70%;
- стен $\rho_{ст}$ = 50%;;
- пола $\rho_{пол}$ = 30%;

Нормируемая освещенность $E_н$ = 150 лк;

Коэффициент запаса $K_З$ =1,5;

Высота рабочей поверхности $h_p = 0,8$ м.

Т а б л и ц а 5.4 - Светораспределение светильников [17]

Сила света I_a, кд направлении угла α										
0	5	15	25	35	45	55	65	75	85	90
256	256	246	229	206	174	135	92	50	12	0

Высота светильника над освещаемой поверхностью

$$h = H - h_p = 3 - 0,8 = 2,2 \text{ м}$$

В серверной комнате принята система общего освещения люминесцентными лампами ЛБ (белого цвета), мощностью 40 Вт.

$$Z/h = К_З \qquad (5.1)$$

Отсюда $Z = 1,5 \cdot h = 1,5 \cdot 2,2 = 3,3$ м;

Ширина помещения равна 5 м, длина - 7 м, светильники лучше расположить в 2 ряда. Примем расстояние между светильниками в одном ряду - 3,3 м, расстояние между рядами - 3 м, расстояние от крайнего светильника до стены по длине - 1,85 м, по ширине - 1 м. Схема расположения светильников показана на рисунке 5.2.

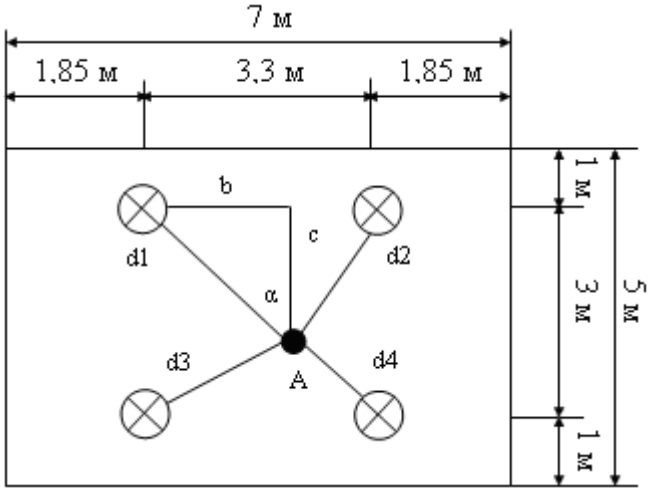

Рисунок 5.2 - Расположение светильников в рабочем помещении

Рассчитаем освещенность в точке А.

Расстояние от светильника до исследуемой точки d рассчитывается по формуле

$$d = \sqrt{b^2 + c^2} \qquad (5.2)$$

Расстояние от светильника до исследуемых точек d_1, d_2, d_3, и d_4:

- $b_{13} = 2{,}65$ м;
- $b_{24} = 0{,}65$ м;
- $c_{12} = 2$ м.;
- $c_{34} = 1$ м
- $d_1 = \sqrt{2{,}65^2 + 2^2} = 3{,}32$ м;
- $d_2 = \sqrt{0{,}65^2 + 2^2} = 2{,}1$ м;
- $d_3 = \sqrt{2{,}65^2 + 1^2} = 2{,}65$ м;
- $d_4 = \sqrt{0{,}65^2 + 1^2} = 0{,}65$ м.

Определим углы α

$$tg\alpha = d/h \qquad (5.3)$$

1 $tg\alpha = 3{,}32/2{,}2 = 1{,}51$; $\alpha = 56{,}5$; $\cos^3 56{,}5 = 0{,}168$;

I_α - по исходным данным при 56,5 равен 129 кд (по таблице 5.4)

2 $tg\alpha = 2{,}1/2{,}2 = 0{,}96$; $\alpha = 43{,}8$; $\cos^3 43{,}8 = 0{,}375$;

I_α - по исходным данным при 43,8 равен 177,84 кд (по таблице 5.4)

3 $tg\alpha = 2{,}65/2{,}2 = 1{,}21$; $\alpha = 50{,}4$; $\cos^3 50{,}4 = 0{,}259$;

I_α - по исходным данным при 50,4 равен 152,94 кд (по таблице 5.4)

4 $tg\alpha = 0{,}65/2{,}2 = 0{,}3$; $\alpha = 16{,}7$; $\cos^3 16{,}7 = 0{,}879$;

I_α - по исходным данным при 16,7 равен 243,11 кд (по таблице 5.4)

Суммарная освещенность рассчитывается по формуле

$$\Sigma e_г = I_\alpha \cdot Cos^3\alpha / h^2 \qquad (5.4)$$

Подставим полученные данные в формулу (5.4):

1 $e_г = 129 \cdot 0{,}168/2{,}2^2 = 4{,}48$;
2 $e_г = 177{,}84 \cdot 0{,}375/2{,}2^2 = 13{,}78$;
3 $e_г = 152{,}94 \cdot 0{,}259/2{,}2^2 = 8{,}18$;
4 $e_г = 243{,}11 \cdot 0{,}879/2{,}2^2 = 44{,}15$.

$\sum e_г = 4{,}48 + 13{,}78 + 8{,}18 + 44{,}15 = 70{,}59$

Световой поток определяется по формуле:

$$Ф = 1000 \cdot К_з \cdot Е_н / \mu \cdot \sum e_г \qquad (5.5)$$

где $Е_н$ - нормируемая освещенность;

μ - коэффициент, учитывающий дополнительную освещенность за счет отражения μ= 1,1;

$\sum e_г$ - суммарная освещенность создаваемая всеми источниками;

$К_з$ - коэффициент запаса.

$Ф = 1000 \cdot 1,5 \cdot 150 / 1,1 \cdot 70,59 = 2897,66$ лм.

Рассчитываем $Е_т$:

$$E_T = \frac{\varphi_л \mu}{1000 K_з} \cdot \sum e_T = \frac{3120 \cdot 1,1}{1000 \cdot 1,5} \cdot 70,59 = 161,51 \text{ лк};$$

Теперь сравним освещенность, полученную из расчета исходных данных с нормированной освещенностью, соответствующей заданному разряду зрительной работы (IV).

$Е_г = 160,51$ лк; $Е_н = 150$ лк; $Е_г > Е_н$;

Исходя из полученного результата видно, что действующая система освещения, обеспечивает помещение освещенностью соответствующей нормированной. Произведем расчет вторым методом.

Метод коэффициента использования

В серверной комнате принята система общего освещения люминесцентными лампами ЛБ (белого цвета), мощностью 40 Вт и световым потоком $Ф_л$ = 3120 лм, диаметром 40 мм и длинной со штырьками 1213.6 мм Высота рабочей поверхности $h_р$ = 0,8 м. Схема рабочего помещения представлена на рисунке 5.3.

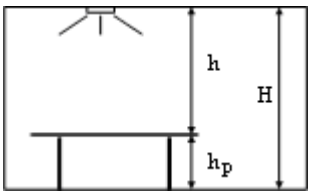

Рисунок 5.3 - Схема рабочего помещения

Определим необходимое расстояние между светильниками

$$L = \lambda \cdot h \qquad (5.6)$$

где $\lambda = 1{,}2 \div 1{,}4$.

Высота светильника над освещаемой поверхностью

$h = H - h_p = 3 - 0{,}8 = 2{,}2$ м.

Следовательно, находим, что необходимое расстояние между светильниками равно

$$L = 1{,}4 \cdot 2{,}2 = 3{,}08 \approx 3{,}1 \text{ м.}$$

Определим индекс помещения по формуле

$$I = \frac{A \cdot B}{h \cdot (A + B)} = \frac{5 \cdot 7}{2{,}2 \cdot (5 + 7)} = 1{,}33$$

Принимаем 2 ряда светильников с расстоянием от стен 1,25 метров, между рядами 4,5 метров.

Определим коэффициент использования η по таблице 2.6 [21]

$$\eta = 48\%$$

В качестве светильника возьмем ЛСП-02 рассчитанный на две лампы мощностью 40 Вт, диаметром 40 мм и длинной со штырьками 1213,6 мм.

Световой поток лампы ЛБ 40 Вт составляет 3120 лм, световой поток, излучаемый светильником равен:

$$\Phi_{св} = \Phi_л \cdot 2 = 3120 \cdot 2 = 6240 \text{ лм}$$

Определим число светильников по формуле

$$N = \frac{E \cdot K_з \cdot S \cdot z}{n \cdot \Phi_л \cdot \eta} \qquad (5.7)$$

где S - площадь помещения, S=35 м^2;

$К_з$ - коэффициент запаса, $К_з$ = 1,5;

E - заданная минимальная освещенность, E = 150 лк;

z - коэффициент неравномерности освещения, $z = 1{,}1 \div 1{,}2$;

n - количество ламп в светильнике, n = 2;

$Ф_л$ - световой поток выбранной лампы, $Ф_л$ = 3120 лм;

η - коэффициент использования, $\eta = 0{,}523$.

$$N = \frac{150 \cdot 1{,}5 \cdot 35 \cdot 1{,}2}{2 \cdot 3120 \cdot 0{,}48} = \frac{9450}{2995} \approx 4 \text{ светильника.}$$

Светильники размещаем в двух рядах по 2 в каждом (рисунок 5.4). Расстояние между светильниками в ряду 1 метр. Всего для создания нормируемой освещенности 150 лк необходимо 8 ламп ЛБ мощностью 40 Вт.

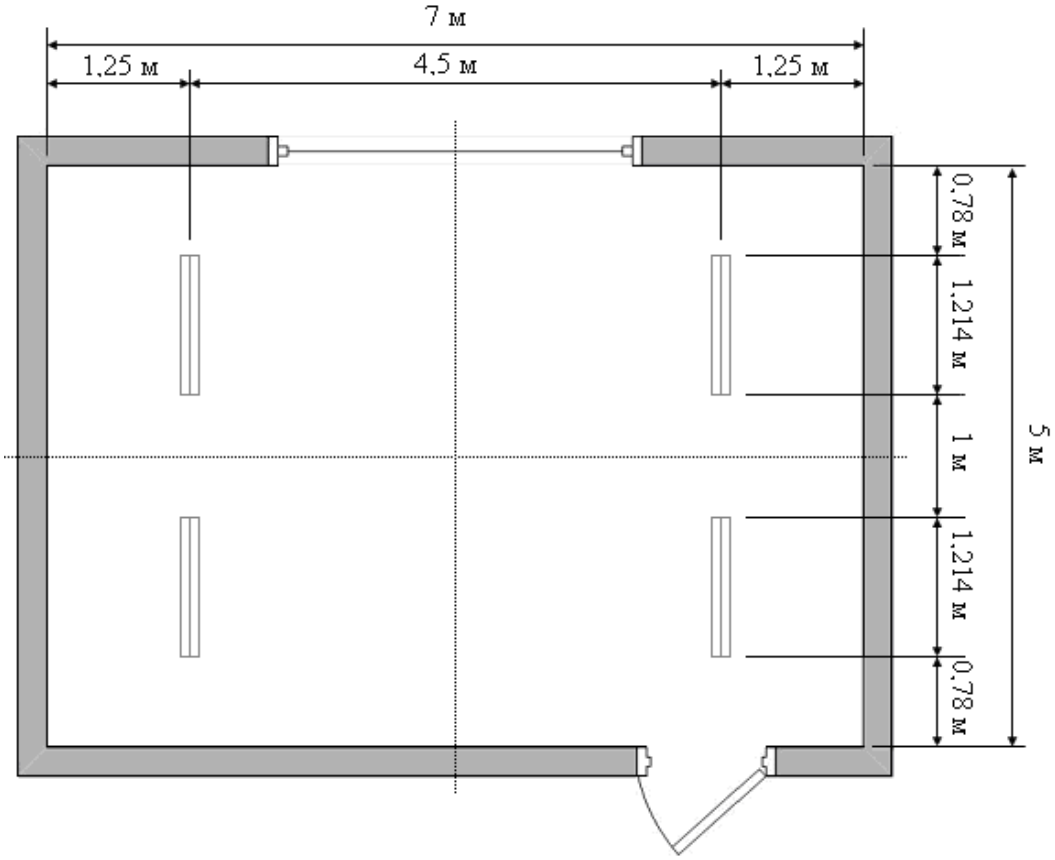

Рисунок 5.4 - Размещение светильников в серверной комнате

В результате проделанных расчетов просчитаны необходимые меры безопасности и условия труда инженера, которые соответствуют стандартам СНиП РК 2.04-05-2002.

Произведена необходимая освещенность рабочей поверхности. В качестве источника света выбран ЛСП-02, который обеспечивает оптимальную освещенность и по сравнению с другими светильниками относительно не дорогой и потребляет наименьшее количество энергии.

5.2.2 Расчет системы кондиционирования

Определим количество воздуха L $м^3$/ч, которое необходимо вывести за один час из помещения, чтобы вместе с ним удалить избыток тепла $Q_{изб}$ по следующей формуле

$$L = \frac{Q_{изб}}{C_в \cdot t \cdot y_в} \qquad (5.8)$$

где $C_в$ - теплоемкость сухого воздуха, ккал/кг ($C_в$ = 0,24 ккал/кг град);

$t = t_{УХ} - t_{ВХ}$ при расчетах возьмем t = 5°С;

$y_в$ - плотность уходящего воздуха, определяемая в зависимости от температуры, кг/м^3 (при расчетах принимается $y_в$ = 1,20 кг/м^3).

Определим избыточное тепло $Q_{изб}$ ккал/ч

$$Q_{изб} = Q_п - Q_{от} \qquad (5.9)$$

где $Q_п$ - количество тепла поступающего в воздух помещения, ккал/ч;

$Q_{от}$ - теплоотдача в окружающую среду через наружные ограждения (в теплое время года, при расчетах можно принять нулю).

Количество тепловыделений $Q_п$ зависит от мощности оборудования, числа работающих людей и тепла, которое вносится в помещение через оконные проемы [20]

$$Q_п = Q_{об} + Q_л + Q_р + Q_{оп} \qquad (5.10)$$

где $Q_{об}$ - тепло, выделяемое производственным оборудованием, ккал/ч;

$Q_л$ - тепло выделяемое людьми, ккал/ч;

$Q_{оп}$ - тепло выделяемое осветительными приборами;

$Q_р$ - тепло, вносимое солнечной радиацией, ккал/ч.

Тепло, выделяемое производственным оборудованием в рабочем помещение, определяется из соотношения:

$$Q_{об} = 860 \cdot P_{об} \cdot n \qquad (5.11)$$

где 860 тепловой эквивалент 1 кВт·ч, то есть тепло, эквивалентное 1 кВт·ч электрической энергии;

$P_{об}$ - мощность, потребляемая оборудованием $P_{об}$ = 0,8 кВт;

n - коэффициент перехода тепла в помещение, n=0,75.

$$Q_{об} = 860 \cdot 0{,}8 \cdot 0{,}75 = 516 \text{ ккал/ч.}$$

Тепло, вносимое солнечной, радиацией, определяется из соотношения

$$Q_р = m \cdot F \cdot g_{ост} \qquad (5.12)$$

где m - количество окон в помещение;

F - площадь одного окна F=3 м^2;

$g_{ост}$ - солнечная радиация через остекленную поверхность, то есть количество тепла, вносимое за 1ч через остекление площадью в 1 м^2.

Значение $g_{ост}$ в зависимости от географической ориентации поверхности и характеристики окон или фонарей принимается в пределах 70 - 210. Окно рабочего помещения направлено строго на восток, поэтому примем значение $g_{ост}$ равным 145 Вт/м^{2}С° [20].

$Q_р = 1 \cdot 3 \cdot 145 = 435$ ккал/ч.

Тепло выделяемое людьми определяется

$$Q_л = Q_ч \cdot n \qquad (5.12)$$

где $Q_ч$ - количество тепла выделяемое одним человеком;

n - количество человек.

$Q_л = 180 \cdot 2 = 360$ ккал/ч.

Тепло выделяемое осветительными приборами

$$Q_{оп} = N \cdot N_{оп} \qquad (5.13)$$

где N - коэффициент, учитывающий количество энергии, переходящей в тепло N = 0,8;

$N_{оп}$ - количество осветительных приборов.

$Q_{оп} = 0{,}8 \cdot 4 \cdot 40 = 256$ ккал/ч.

Тогда тепловыделение составит

$Q_{изб} = 516 + 435 + 360 + 256 = 1567$ ккал/ч.

Таким образом, необходимый воздухообмен будет равен:

$$L = \frac{1567}{0{,}24 \cdot 5 \cdot 1{,}20} = 1088{,}19 \text{ м}^3/\text{ч}.$$

Отношение количества воздуха, поступающего в помещение за один час, к объему помещения называется кратностью воздухообмена

$$K = \frac{L}{V_п} = \frac{1088{,}19}{105} = 10 \text{ ч}.$$

где $V_п$ - объем помещения $V_п = 105$ м^3.

Находим требуемую производительность кондиционера

$$W_k = k_з \cdot L \qquad (5.14)$$

где $k_з$ - коэффициент запаса, $k_з$ =1,3÷2,0;

$W_k = 1{,}7 \cdot 1088{,}19 = 1849{,}92$ м^3/ч.

Исходя из расчетов в помещение с оборудованием, для соблюдения требуемых параметров микроклимата следует установить один кондиционер с производительностью не менее 1849,92 м³/ч.

Данным параметрам удовлетворяет кондиционер LG-235EU63VW N54RT3 производства Южная Корея.

Паспортные характеристики кондиционера сведены в таблицу 5.4.

Т а б л и ц а 5.4 - Характеристики кондиционера

Технические характеристики	Значения
Электропитание	220-240 В; 50 Гц
Хладопроизводительность, кВт	3,60
Теплопроизводительность, кВт	4,65
Потребляемая мощность при охлаждении, кВт	1,29
Потребляемая мощность при обогреве, кВт	1,46
Максимальный потребляемый ток, А	7,0
Макс. длина соед. труб / перепад высот, м	15/5
Расход воздуха (Н/С/В) внутреннего блока, м3/час	372/450/540
Расход воздуха наружного блока, м3/час	3000
Кол-во выделяемой из воздуха влаги, л/час	2,5
Уровень шума (Н/С/В) внутреннего блока, дБ	35/39/44
Уровень шума наружного блока, дБ	51
Масса внутреннего блока без упаковки, кг	8
Масса наружного блока без упаковки, кг	38

Выбранный кондиционер, удовлетворяет всем потребностям и является относительно не дорогим по сравнению с другими.

6 Технико-экономическое обоснование

6.1 Обоснование выбора устройства защиты Cisco ASA Series

Согласно теме выпускной работы реализуется защита периметра корпоративной сети на основе устройства защиты Cisco ASA Series.

Основные задачи проекта:

- Защита внутренней сети от внешних воздействий
- Контроль исходящего и входящего доступа
- Безопасное взаимодействие между головным офисом организации и филиалами.

Правильно выбранное решение проблемы защиты уменьшит уязвимость сети и тем самым сэкономит средства компании. Правильное решение должно также минимизировать общие расходы компании на внедрение и эксплуатацию средств сетевой защиты.

Кроме того, правильное решение проблемы защиты может обеспечить возможность использования приложений электронной коммерции и межсетевых приложений, которые обеспечивали более тесные связи с поставщиками и партнерами, но ранее считались потенциально опасными из-за недостаточной надежности защиты.

Устройства Cisco ASA Series предназначены для защиты сетей всех масштабов от широкого спектра угроз. Прежде всего, стоит отметить, что семейство Cisco ASA Series призвано обеспечить масштабируемость интегрированных сервисов и унифицированное управление ими, гарантируя заказчику одновременную работу многих механизмов безопасности и их высокую производительность и эффективность, причем без усложнения процесса эксплуатации сетевой инфраструктуры.

Помимо функциональных, система Cisco ASA Series имеет ряд экономических и эксплуатационных преимуществ. В их числе возможность наращивания сервисов посредством ПО и аппаратных модулей, стандартизация платформы на разных объектах, упрощенный процесс эксплуатации с использованием общей службы управления и мониторинга для множества сервисов безопасности, а также упрощенный процесс поиска и устранения неисправностей. Профиль сервисов устройства позволяет оптимизировать их под определенную инфраструктуру и определенные функции, так что заказчики могут стандартизовать устройство защиты ASA Series для многих сфер применения в сети. Иначе для решения тех же самых задач потребовалось бы множество разнообразных платформ и систем управления. Такой адаптивный подход - "одно устройство, много назначений" - сокращает число платформ, которые приходится устанавливать и администрировать, и в то же время создает общую среду эксплуатации и управления для всех этих устройств. Это

упрощает конфигурирование, мониторинг, техническое обслуживание и обучение персонала службы безопасности.

Эффективное управление, позволяющее увеличить срок эксплуатации устройств, обеспечивает тем самым высокий уровень защиты инвестиций. Благодаря объединению эффективных, проверенных рынком механизмов защиты и построения VPN, а также встроенной поддержке соединений Gigabit Ethernet и бездисковой (а значит, более надежной) структуре с флэш-памятью устройства семейства Cisco ASA Series идеально подходят компаниям, которым необходимы лучшие среди аналогов решения, обеспечивающие высокую производительность, гибкость, надежность и защиту капиталовложений.

6.2 План организации защиты сети на основе Cisco ASA Series

Подготовка и внедрение устройства защиты Cisco ASA Series состоит из семи основных этапов:

- этап предпроектного исследования;
- этап технического задания, который заключает в себя постановку основных целей и задач, содержания проекта;
- этап подготовки устройства защиты Cisco ASA Series;
- этап внедрения устройства защиты Cisco ASA Series;
- этап тестирования;
- этап подготовки проекта к сдаче;
- этап сдачи проекта.

В данном проекте участвуют три разработчика: администратор, старший администратор и руководитель проекта.

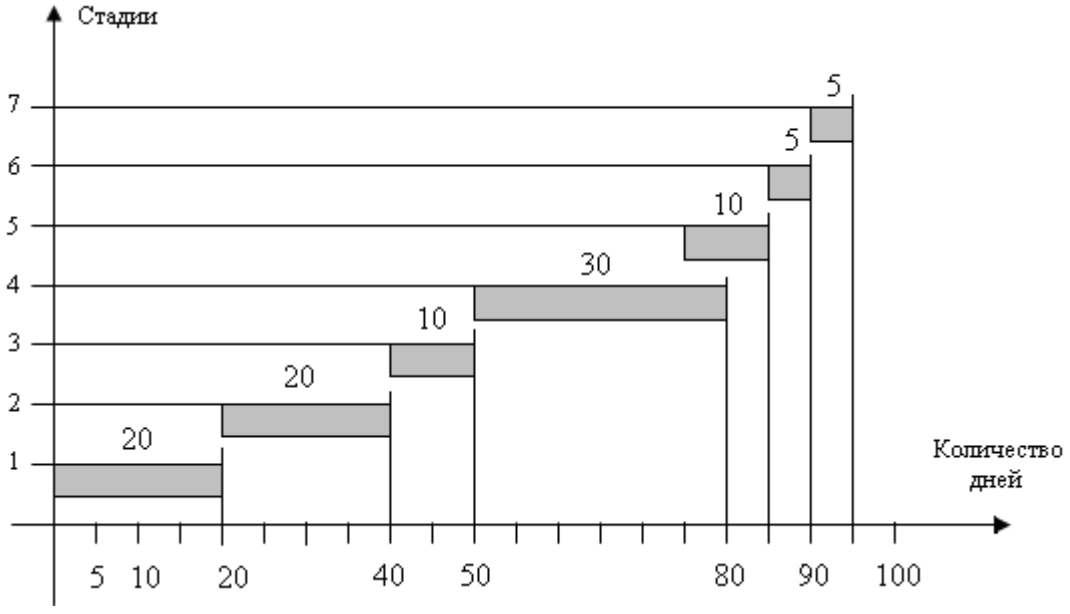

Рисунок 6.1 - Календарный график работы над проектом

6.3 Расчет стоимости внедрения Cisco ASA Series

Расчет осуществляется по калькуляционным статьям расходов.

Прежде всего, надо рассчитать себестоимость на протяжении всего жизненного цикла. Себестоимость - это все затраты на производство и реализацию проекта.

Себестоимость организации защиты сети на основе устройства Cisco ASA складывается из следующих статьей затрат:

- заработная плата основных разработчиков;
- дополнительная заработная плата;
- фонд оплаты труда;
- отчисления с фонда оплаты труда в социальный налог;
- амортизационные отчисления;
- расходные материалы;
- накладные расходы.

Таким образом, себестоимость разработки проекта определяется по следующей формуле [19]

$$С = ФОТ + О_С + Р_О + А + С_{Эл} + Н_Р + П_Р \quad (6.1)$$

где ФОТ - фонд оплаты труда (основная и дополнительная заработная плата);

$О_С$ - социальный налог;

$Р_О$ - расходы на оборудование;

А - амортизационные отчисления;

$С_{Эл}$ - расходы на электроэнергию;

$Н_Р$ - накладные расходы;

$П_Р$ - расходы на машинное время.

6.3.1 Расходы на заработную плату

Фонд оплаты труда состоит из основной и дополнительной заработной платы

$$ФОТ = З_{ОСН} + З_{ДОП} \quad (6.2)$$

Для расчета основной заработной платы необходимы данные по трудоемкости человеко-дней, человеко-месяцев, численности и размер установленного оклада за месяц.

Длительность цикла в днях по каждому виду работы укрупнено можно определить по формуле

$$t_n = \frac{T}{q_n \cdot 7 \cdot K}, \quad (6.3)$$

где Т - трудоёмкость этапа, нормо-час;

q_n - количество исполнителей по этапу;

7 - продолжительность рабочего дня, час;

К - коэффициент выполнения норм времени (К=1,1).

Сведем в таблице 6.1 данные о разработчиках, нормах, трудоёмкости и соответственно длительности поэтапного цикла.

Т а б л и ц а 6.1 - План внедрения устройства защиты Cisco ASA Series

Наименование этапов	Исполнители	Трудоёмкость		Количество исполнителей	Длительность цикла, дни
		Нормы Часы	% от общёй трудоёмкости		
Предпроектное исследование	Администратор	155	20 %	1	20
Техническое задание	Администратор Старший администратор Руководитель	460	20 %	3	20
Подготовка устройства	Администратор Старший администратор	150	10 %	2	10
Внедрение устройства	Администратор Старший администратор	460	35 %	2	30
Тестирование	Администратор Старший администратор	150	5 %	2	10
Подготовка к сдаче проека	Администратор	35	5 %	1	5
Сдача проекта	Администратор Руководитель	70	5 %	2	5

Затраты на заработную плату разработчиков рассчитываются по следующей формуле

$$Зр = Трi \cdot Зi, \qquad (6.4)$$

где Трi - трудоемкость работ i-го разработчика, чел.мес;

Зi - основная заработная плата i-го разработчика (оклад), тг/мес;

Учитывая, что в месяце 24 рабочих дня, то ежедневная трудоемкость составит 1/24 ежемесячной трудоемкости.

Оклад администратора составляет 60000 тенге в месяц. Оклады старшего администратора и руководителя проекта составляют 80000 тенге в месяц.

Исходя из вышеперечисленных данных поэтапно посчитаем затраты на заработную плату для каждого участника проекта.

1) Предпроектное исследование

Для администратора

$$Зр_А = \frac{20}{24} \cdot 60000 = 50000 \text{ тенге}$$

2) Техническое задание

Для администратора

$$Зр_А = \frac{20}{24} \cdot 60000 = 50000 \text{ тенге}$$

Для старшего администратора и руководителя проекта

$$Зр = \frac{20}{24} \cdot 80000 = 66666{,}67 \text{ тенге}$$

3) Подготовка устройства защиты Cisco ASA Series

Для администратора

$$Зр_А = \frac{10}{24} \cdot 60000 = 25000 \text{ тенге}$$

Для старшего администратора и руководителя проекта

$$Зр = \frac{10}{24} \cdot 80000 = 33333{,}33 \text{ тенге}$$

4) Внедрение устройства защиты Cisco ASA Series

Для администратора

$$Зр_{А} = \frac{30}{24} \cdot 60000 = 75000 \text{ тенге}$$

Для старшего администратора и руководителя проекта

$$Зр = \frac{30}{24} \cdot 80000 = 100000 \text{ тенге}$$

5) Тестирование
Для администратора

$$Зр_{А} = \frac{10}{24} \cdot 60000 = 25000 \text{ тенге;}$$

Для старшего администратора и руководителя проекта

$$Зр = \frac{10}{24} \cdot 80000 = 33333{,}33 \text{ тенге;}$$

6) Подготовка проекта к сдаче
Для администратора

$$Зр_{А} = \frac{5}{24} \cdot 60000 = 12500 \text{ тенге;}$$

Для старшего администратора и руководителя проекта:

$$Зр = \frac{5}{24} \cdot 80000 = 16666{,}67 \text{ тенге;}$$

Результаты расчета затрат по заработной плате с учетом трудоемкости и установленных окладов каждого участника проекта представлены в таблице 6.2.

Основная заработная плата рассчитывается как сумма оплаты труда всех работников, задействованных в разработке (таблица 6.2)

$З_{ОСН}$ = 537500 тенге

Т а б л и ц а 6.2 - Основная заработная плата разработчиков

№ п/п	Наименование этапа	Исполнители	Трудоёмкость		Оклад, тг./мес.	Затраты по з/п, тг
			чел. дн	чел. мес.		
1	Предпроектное исследование	Администратор	20	0,833	60000	50000,00
2	Техническое задание	Администратор	20	0,833	60000	50000,00
		Старший администратор			80000	66666,67
		Руководитель			80000	66666,67
3	Подготовка устройства	Администратор	10	0,417	60000	25000,00
		Старший администратор			80000	33333,33
4	Внедрение устройства	Администратор	30	1,250	60000	75000,00
		Старший администратор			80000	100000,00
5	Тестирование	Администратор	10	0,417	60000	25000,00
		Старший администратор			80000	33333,33
6	Подготовка проекта к сдаче	Администратор	5	0,208	60000	12500,00
7	Сдача проекта	Администратор				
		Руководитель				
					Итого:	537500,00

Дополнительная заработная плата (премии и т.д.) разработчиков составляет 20 % от основной заработной платы и рассчитывается по формуле

$$З_{доп} = З_{осн} \cdot \frac{20\%}{100\%} \qquad (6.5)$$

Согласно формуле (6.5) дополнительная заработная плата будет равна

$$З_{доп} = 537500 \cdot \frac{20}{100} = 107500$$

Тогда фонд оплаты труда в соответствии с формулой (6.2) составит

$$ФОТ = 537500 + 107500 = 645000 \text{ тенге}$$

Социальный налог согласно ст. 358 НК РК с 01.01.09 составляет 11% от дохода работника (ЗП + дополнительная оплата труда).

$$Ос = (ФОТ - ПО) \cdot 0{,}11 \qquad (6.6)$$

В соответствии со статьями налогового кодекса 144 и 145 о доходах, не подлежащих налогообложению, отчисления в пенсионный фонд в размере 10%

от фонда оплаты труда социальным налогом не облагаются. Пенсионные отчисления рассчитываются по формуле

$$ПО = ФОТ \cdot \frac{10\%}{100\%} \quad (6.7)$$

Согласно формуле (6.7) пенсионные отчисления будут равны

$$ПО = 645000 \cdot \frac{10\%}{100\%} = 64500 \text{ тенге}$$

Тогда отчисления по социальному налогу согласно формуле (6.6) составят

$$Ос = (645000 - 64500) \cdot 0{,}11 = 63855 \text{ тенге}$$

Прочие расходы (Пр) включают расходы на машинное время (порядка 3-х месяцев на подготовку, внедрение и тестирование устройство: 700 часов стоимостью 10 тг./час)

$$Пр = 700 \cdot 10 = 7000 \text{ тенге}$$

6.3.2 Расчет затрат на оборудование

Так как нашей задачей является организация защиты уже спроектированной сети, то нам необходимо закупить только устройства защиты Cisco ASA Series. Стоимость оборудования отражена в таблице 6.3.

Таблица 6.3. Расчёт используемого оборудования

Наименование оборудования	Количество, штук	Цена за единицу в тенге	Сумма в тенге
Cisco ASA 5510 [ASA-SSM-AIP-10-K9]	2	500000	1000000

Общая стоимость расходов на оборудование составляет 1000000 тенге.

6.3.3 Амортизационные отчисления

Расчет затрат на амортизацию производится по формуле[20]

$$A = \frac{H_A \cdot C_{ПЕР}}{100} \quad (6.8)$$

где А - ежегодная сумма амортизационных отчислений;

$С_{ПЕР}$ - первоначальная стоимость объекта;

$Н_А$ - норма амортизационных отчислений.

В соответствие со ст. 20 Налогового кодекса РК с 01.01.09, норма амортизационных отчислений ($Н_А$) на оборудование связи составляет 25%. Амортизация на устройства защиты Cisco ASA 5510 согласно формуле (6.8) будет равна

$$A = \frac{25 \cdot 1000000}{100} = 250000 \text{ тенге}$$

Тогда, согласно формуле (6.8) дневная сумма амортизации на устройства защиты Cisco ASA 5510 составит

$$A = \frac{250000}{12 \cdot 24} = 868{,}05 \text{ тенге}$$

Так как длительность непосредственного внедрения проекта и использования данного оборудования составляет 85 дней, то общие затраты на амортизацию будут равны

$$A = 868{,}05 \cdot 85 = 73784{,}72 \text{ тенге;}$$

6.3.4 Затраты на электроэнергии

Важной статьей затрат являются затраты на потребляемую электроэнергию.

Затраты на электроэнергию рассчитывается по следующей формуле

$$C_{Эл} = \mathrm{W} \cdot \mathrm{T} \cdot \mathrm{S} \qquad (6.9)$$

где W - потребляемая мощность, кВт;

T - количество часов работы;

S - стоимость киловатт-часа электроэнергии.

Виды используемого оборудования, а так же потребляемая ими мощность представлены в таблице 6.4. Исходя из этих данных рассчитывается стоимость расхода электроэнергии.

Согласно установленному тарифу по энергопотреблению стоимость 1 кВт составляет 8,84 тенге.

С учетом 24-часовой непрерывной работы оборудования и длительности разработки, внедрения проекта, количество часов работы составит

$$\mathrm{T} = 24 \cdot 85 = 2040 \text{ часов}$$

Т а б л и ц а 6.4 - Потребляемая мощность оборудования

Наименование оборудования	Количество, штук	Потребляемая мощность, кВт/час
Персональный компьютер	1	0,3
Cisco ASA 5510	2	0,06
Источник бесперебойного питания	1	0,7
Итого:		1,06

В соответствии с формулой (6.9) расходы на электроэнергию составят:

$$C_{эл} = 1{,}06 \cdot 2040 \cdot 8{,}84 = 19115{,}616 \text{ тенге}$$

6.3.5 Расчет затрат на накладные расходы

Накладные расходы на разработку проекта составляют 10% от общей суммы затрат и рассчитываются по формуле

$$Нр = (ФОТ + Ос + Ро + А + Сэл + Пр) \cdot 0{,}1; \qquad 6.10$$

Тогда, согласно формуле (6.10), накладные расходы будут равны

$$Нр = (645000 + 63855 + 1000000 + 73784{,}72 + 19115{,}616 + 7000) \cdot 0{,}1 = 180875{,}5336 \text{ тенге;}$$

6.3.6 Себестоимость проекта

В соответствии с произведенными расчетами по статьям затрат себестоимость проекта, согласно формуле (6.1), будет равна

$$С = 645000 + 63855 + 1000000 + 73784{,}72 + 19115{,}616 + 180875{,}5336 + 7000 = 1989630{,}87$$

Сводные результаты расчета стоимости проекта и их структура представлены в таблице 6.5. и на рисунке 6.2.

Т а б л и ц а 6.5 - Себестоимость

Статья расхода	Затраты в месяц, тенге	Структура, %
Фонд оплаты труда	645000	32,42
Социальный налог	63855	3,21
Расходы на оборудование	1000000	50,26
Амортизационные отчисления	73784,72	3,7

Затраты на электроэнергию	19115,616	0,96
Накладные расходы	180875,5336	9,09
Прочие расходы	7000	0,35
Итого:	1989630,87	

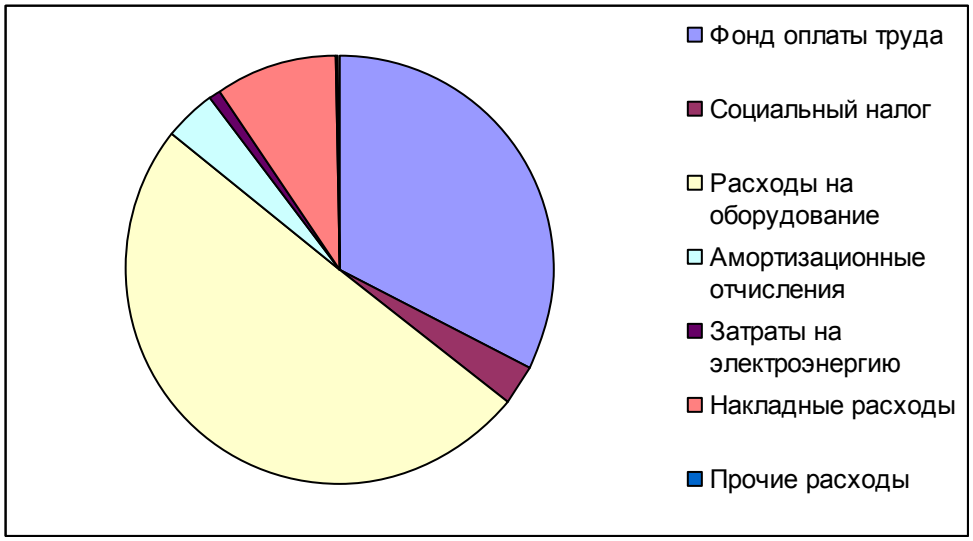

Рисунок 6.2 - Структура затрат

6.4 Стоимость поддержки устройства защиты ASA

Рассчитаем стоимость поддержки устройства защиты ASA за один год. Стоимость поддержки устройства защиты состоит из следующих составляющих:

1) Заработная плата администратора;

Поддерживать устройства защиты будет системный администратор, который участвовал в процессе внедрения. Вычислим его годовую зарплату

$$Зр_{А} = 12 \cdot 60000 = 720000 \text{ тенге}$$

2) Социальные отчисления:

Согласно формуле (6.7) пенсионные отчисления будут равны

$$ПО = 720000 \cdot \frac{10\%}{100\%} = 72000 \text{ тенге}$$

Согласно формуле (6.6) по социальному налогу составят

$$Ос = (720000 - 72000) \cdot 0{,}11 = 71280 \text{ тенге}$$

3) Затраты на электроэнергию

W - потребляемая мощность, составляет 1,06 кВт;

S - стоимость киловатт-часа электроэнергии составляет 8,84 тенге.

. С учетом 24-часовой непрерывной работы оборудования и количество часов работы за год составит

$$T = 24 \cdot 365 = 8760 \text{ часов}$$

В соответствии с формулой (6.9) расходы на электроэнергию составят

$$C_{Эл} = 1{,}06 \cdot 8760 \cdot 8{,}84 = 82084{,}704 \text{ тенге}$$

4) Годовая амортизация оборудования:

Годовая амортизация на устройства защиты Cisco ASA 5510 согласно формуле (6.8) будет равна

$$A = \frac{15 \cdot 1000000}{100} = 150000 \text{ тенге}$$

Таким образом, годовые затраты на поддержку устройства защиты Cisco ASA

$$З_{ГОД} = Зр_{А} + O_C + C_{ЭЛ} + A \qquad (6.11)$$

Рассчитаем по формуле (6.11)

$$З_{ГОД} = 720000 + 71280 + 82084{,}704 + 150000 = 1023364{,}704$$

6.5 Экономический эффект от работы устройства защиты ASA

Рассчитаем ущерб компании, понесенный в отсутствии устройства адаптивной защиты Cisco ASA Series.

В 2008 году на корпоративную сеть компании Manhattan было организовано 3 сетевых атак, первая из них причинила ущерб на сумму 10000 долларов (1500000 тенге), вторая - на сумму 14000 долларов (21000000 тенге), третья - на сумму 16000 долларов (2400000 тенге). Суммарный ущерб составил 40000 долларов (6000000 тенге).

Примем данную сумму в качестве условного годового дохода, полученного после внедрения устройства защиты ASA Series компании Cisco.

Условную прибыль найдем как разность годового дохода и эксплуатационных затрат на поддержку оборудования за первый год

$$П = Д - (З_{год} + С) \quad (6.12)$$

где П - годовая прибыль;

Д - условный годовой доход;

$З_{год}$ - стоимость поддержки устройства защиты ASA за один год;

С - себестоимость проекта.

Рассчитаем по формуле (6.12):

$$П = 6000000 - (1023364,704 + 1989630,87) = 2987004,426 \text{ тенге}$$

6.6 Срок окупаемости

Срок окупаемости рассчитаем по формуле (6.13)

$$Т_{ок} = \frac{С}{П} \quad (6.13)$$

где $Т_{ок}$ - срок окупаемости

$$Т_{ок} = \frac{1989630,87}{2987004,426} = 0,67 < 1 \text{ год;}$$

Проект окупается меньше чем за год, в последующие годы устройства защиты ASA Series принесет только прибыль.

Срок окупаемости является оптимальным с учетом инфляции и необходимыми затратами производимыми на выплату нормального функционирования всего проекта и отдельных его частей.

Внедрение устройства защиты Cisco ASA Series является оптимальным выбором для организации защиты корпоративной сети не только в техническом, но и в экономическом аспектах.

ЗАКЛЮЧЕНИЕ

Разработка защиты периметра корпоративной сети компании является очень актуальной на сегодняшний день, так как разрабатываемые работы основаны на оборудовании Cisco ASA Series, которое является негласным стандартом для построения сетей телекоммуникаций.

В разработке системы были рассмотрены основные вопросы по конфигурации оборудования Cisco ASA. Проделав данный курс работ по установке и настройке оборудования, компания «S2RE» увеличивает уровень безопасности внутрисетевой информации от внешних угроз и посягательства злоумышленников.

Сегодня оборудование Cisco ASA используют все наиболее крупные компании в различных сферах для реализации своих амбиций в полной мере, не беспокоясь о конфиденциальности информации как в Казахстане, так и во всем мире, что подтверждает востребованность не только оборудования, но и специалистов, настраивающих данную систему.

Актуальность данной работы для компаний трудно переоценить, так как финансовые затраты необходимые для выполнения такого рода работ окупаются менее чем за год, и, в то же время компании получают высокий уровень информационной безопасности, а наличие оборудования семейства Cisco ASA только подчеркнут статус и серьезность компании.

СПИСОК ЛИТЕРАТУРЫ

1. Джеймс Челлис, Чарльз Перкинс, Мэтью Стриб. Основы построения сетей. Учебное руководство для специалистов MCSE. Издательство «Лори»,1997. - 323 с.
2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. - СПб: Изд-во «Питер», 1999. - 672 с.
3. К. Андерсон, М.Минаси. Локальные сети. Полное руководство. - Корона, СПб. 1999. - 624 с.
4. Кульгин М. Технологии корпоративных сетей. Энциклопедия. - СПб: Изд-во «Питер», 1999. - 704 с.
5. Компьютерные сети. Книга 1: High-Performance Networking. Энциклопедия пользователя: Пер. с англ./Марк А. Спортак и др. - К.: Изд-во «ДиаСофт», 1999. - 432 с.
6. Персикова Т. Н. Межкультурная коммуникация и корпоративная культура. Издательство: Инфра-М, 2003 г. - 320 с.
7. Борисов Б. М. Самоучитель по работе с компьютерной сетью. Издательство: Альянс - пресс, 2003. - 495 с.
8. “Мультисервисная корпоративная сеть” //Электронная версия на сайте http://www.o-si.ru/file.html
9. “Оборудование для интеграции речи в каналах Frame Relay корпоративных сетей” //Электронная версия на сайте http://www.osp.ru/lan/1997/06.html
10. “Корпоративная сеть ОАО “Новгородэнерго”” //Электронная версия на сайте http://www.uni.ru/comp/
11. “Рынок частных сетей” //Электронная версия на сайте http://www.bytemag.ru/article.html
12. “Создание территориально распределенных сетей” //Электронная версия на сайте http://www.compulink.ru/global.html
13. “Интегрированные высокоскоростные сети передачи данных и голоса с использованием физических и радиоканалов” //Электронная версия на сайте http://www.inforad.ru.html
14. “Проект: Создание городской сети передачи данных Костромы” //Электронная версия на сайте http://www.pluscom.ru/
15. “Разработка проекта корпоративной сети масштаба предприятия на базе АТМ - технологии” //Электронная версия на сайте http://conf.mitme.ru/
16. “Проект корпоративной сети” //Электронная версия на сайте http://www.ronl.ru/
17. “Intranet: будущее Вашей локальной и корпоративной сети” //Электронная версия на сайте http://www.ci.ru/inform3_97/f1.html
18. “Корпоративные сети передачи данных” //Электронная версия на сайте http://www.vogss.ru/dtcn.html

19. “Информационно-Вычислительная Сеть МЭИ (ТУ)” //Электронная версия на сайте http://icc.mpei.ru/lang/rus/projects/icn.html

20. “Проект построения системы доступа к корпоративной сети Федерального центра проектного финансирования” //Электронная версия на сайте http://www.quarta.net/intra1.html

21. “Корпоративная интегрированная телекоммуникационная сеть” //Электронная версия на сайте http://www.tatenergo.ru/kits.shtml.html

22. “Корпоративная сеть ОАО ГМК «Норильский никель»” //Электронная версия на сайте http://www.pluscom.ru/off-line/solutions/examples/norilsk.html

23. Баклашов Н.И. Китаева Н.Ж. Охрана труда на предприятиях связи и охрана окружающей среды. - М.: Радио и связь, 1989, - 287 с

24. Аманжолова К.Б., Алибаева С.А. Экономика предприятий. Учебное пособие. - Алматы: АИЭС, 2003.

25. Ниеталин Ж.Н., Ниеталина Ж.Ж.. Дипломное проектирование. - Алматы: АИЭС, 2001.

26. Производственное освещение. Методические указания к выполнению раздела "Охрана труда" в дипломном проекте. - Алматы:АИЭС, 1989. - 40с.

27. СниШ 1 - 4 - 79. Естественное и искусственное освещение.

28. Расчет зануления. Методические указания к выполнению раздела "Охрана труда и окружающей среды" в дипломном проекте. - Алматы:АИЭС, 1991.-19с.

29. Сабиров Ю.Г., Сколотнев Н.И. Охрана труда в вычислительных центрах. - Машиностроение, 1985. - 78 с.

30. Голубицкая Е.А., Жигульская Г.М. Экономика связи. - М: Радио и связь, 1999.

31. Резникова Н.П. Маркетинг в телекоммуникациях. - М.: Эко-трендз, 1998.

ПРИЛОЖЕНИЕ А
ПРИЛОЖЕНИЕ Б
ПРИЛОЖЕНИЕ В