МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»

Политехнический институт

Факультет механико-технологический
Кафедра техники и технологии

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой, к.т.н.,
доцент
_____А.В. Прохоров
_____2018 г.

Реализация сетевой безопасности на базе аппаратно-программных решений компании Cisco

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 090301.2018.628. ПЗ ВКР

Руководитель работы,
профессор кафедры техники и
технологии ЮУрГУ, д.т.н.,
старший научный сотрудник
_____Е.Н. Симонов
_____2018 г.
Автор работы -
студент группы ДО-532
_____Е.Ю. Корчагин
_____2018 г.

Нормоконтролер, старший
преподаватель
_____Д.П. Химичева
_____2018 г.

Челябинск 2018

АННОТАЦИЯ

Корчагин, Е.Ю. Реализация сетевой безопасности на базе аппаратно-программных решений компании Cisco. – Челябинск: ЮУрГУ, ДО-532; 2018. – 57 с. 24 илл., библиогр. список – 41 наим., презентация на 12 слайдах.

В работе рассмотрены принципы построения локальной вычислительной сети и ее компоненты, описана базовая эталонная модель OSI, даны пояснения по каждому ее уровню. Рассмотрена теория информационной и сетевой безопасности, даны сведения о часто используемых методах шифрования. В работе приведены примеры распространенных сетевых атак и методов борьбы с ними.

Практическая часть представляет собой реализацию сетевой безопасности на предприятии. Внедрение важных компонентов безопасности, замена незащищенных протоколов и технологий на аналоги, удовлетворяющие требованиям сетевой безопасности, удовлетворение требований руководства на ограничение доступа к некоторым информационным системам и т. п.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ 4
1 КСПД И СЕТЕВАЯ БЕЗОПАСНОСТЬ
1.1 Локальная вычислительная сеть и КСПД 6
1.2 Модель OSI 7
1.3 Сетевое оборудование 14
1.4 Теория информационной и сетевой безопасности 19
1.5 Шифрование данных 23
1.6 Распространенные сетевые атаки 26
1.7 Распространенные методы защиты сети 29
2 СРАВНЕНИЕ ОТЕЧЕСТВЕННЫХ И ПЕРЕДОВЫХ ЗАРУБЕЖНЫХ ТЕХНОЛОГИЙ И РЕШЕНИЙ 35
3 РЕАЛИЗАЦИЯ СЕТЕВОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ
3.1 Аудит КСПД предприятия 39
3.2 Постановка задачи 41
3.3 Внедрение сетевой безопасности 42
ЗАКЛЮЧЕНИЕ 54
БИБЛИОГРАФИЧЕСКИЙ СПИСОК 55

ВВЕДЕНИЕ

Актуальность темы. В современном мире корпоративная сеть передачи данных (далее КСПД) является неотъемлемой частью любой организации. КСПД обеспечивает быстрый, централизованный, защищенный доступ к информации, также позволяет обмениваться данными между отделами и сотрудниками организации. В КСПД зачастую передается и хранится конфиденциальные информация, утечка этой информации может повлечь за собой огромные финансовые потери. Именно поэтому каждая КСПД нуждается в обеспечении информационной безопасности и ее систематическом улучшении, т. к. постоянно появляются новые вредоносные программы, методы взлома, находятся уязвимости в той или иной информационной системе.

Целью выпускной квалификационной работы является реализация сетевой безопасности на базе аппаратно-программных решений компании Cisco.

Задачи выпускной квалификационной работы:

– Изучить КСПД и основные устройства, обеспечивающие ее работоспособность, модель OSI.

– Изучить сетевую безопасность, а именно распространенные атаки на сеть, методы борьбы с ними, лучшие практики защиты и предотвращения атак.

– Сравнить отечественные и передовые зарубежные технологии и решения.

– Реализовать некоторые практики по защите КСПД в соответствии с задачами, учитывая исходные данные.

Объектом выпускной квалификационной работы является КСПД и обеспечение ее сетевой безопасности.

Предметом выпускной квалификационной работы является реализация (внедрение) различных методик защиты сетевых и конечных пользовательских устройств в КСПД.

Практическая значимость выпускной квалификационной работы состоит в снижении рисков нарушения безопасности, устранения уязвимостей в протоколах сетевых устройств.

Структура выпускной квалификационной работы состоит из введения, трех разделов, заключения и библиографического списка. Раздел 1 посвящен теоретическому обоснованию темы исследования, описываются сетевые технологии КСПД, модель OSI, рассматривается видение сетевой безопасности компанией Cisco, разбираются различные атаки на КСПД и методы борьбы с ними. В разделе 2 сравниваются отечественные и передовые зарубежные технологии. Раздел 3 – реализация сетевой безопасности на конкретном предприятии, с использованием сетевых устройств компании Cisco.

Объем выпускной квалификационной работы составляет 57 страниц машинописного текста и содержит 24 иллюстраций, 2 таблицы, библиографический список из 41 наименования.

1 КСПД И СЕТЕВАЯ БЕЗОПАСНОСТЬ

1.1 Локальная вычислительная сеть и КСПД

Локальные сети (Local Area Network, LAN) – это объединения сетевых устройств, компьютеров, сосредоточенных на небольшой территории, хотя в отдельных случаях локальная сеть может иметь и большие размеры. В общем случае локальная сеть представляет собой коммуникационную систему, принадлежащую одной организации [1]. В середине 80-х годов утвердились стандартные сетевые технологии объединения компьютеров в сеть – Ethernet, Token Ring, несколько позже – FDDI. Сетевые технологии – это согласованный набор программных и аппаратных средств (например, драйверов, сетевых адаптеров, кабелей и разъемов), а также механизмов передачи данных по линиям связи, достаточный для построения локальной вычислительной сети (ЛВС). ЛВС – это сети, предназначенные для обработки, хранения и передачи данных, и представляет из себя кабельную систему объекта (здания) или группы объектов (зданий).

Преимущества использования ЛВС:

– Распределение данных (Data Sharing). Данные в ЛВС хранятся на сервере и могут быть доступны для чтения и записи на рабочих станциях пользователей.

– Совместное использование элементов сети, доступ к локальным сетевым устройствам (принтеры, сканеры, факсы и другие внешние устройства).

– Возможность быстрого доступа к необходимой информации.

– Распределение программ (Software Sharing). Все пользователи ЛВС могут совместно иметь доступ к программам поддерживающим сетевой режим.

– Надежное хранение и резервирование данных.

– Защиту информации.

– Использование ресурсов современных технологий (доступ в Интернет, системы электронного документооборота и проч.).

КСПД – система, обеспечивающая передачу информации между различными приложениями, клиентами, серверами, используемыми в сети корпорации. На рисунке ниже представлен пример КСПД.

Рисунок 1 – Пример КСПД

КСПД рассчитаны не только на локальное использование, но способны объединять офисы, подразделения и другие структуры компании, находящиеся в других городах или странах. Принцип построения территориальных корпоративных сетей отличается от создания локальных сетей. Главным отличием является аренда линий связи. Когда у локальной сети основные затраты идут на оборудование, то у территориальных сетей на арендную плату каналов связи [3].

1.2 Модель OSI

Для единого представления данных в сетях с неоднородными устройствами и программным обеспечением международная организация по стандартам ISO (International Standardization Organization) разработала базовую модель связи открытых систем OSI (Open Systems Interconnection) [8]. Эта модель описывает правила и процедуры передачи данных в различных сетевых средах при организации сеанса связи. Основными элементами модели являются уровни,

прикладные процессы и физические средства соединения. На рисунке 2 представлена структура базовой модели.

Рисунок 2 – Уровни модели OSI

Каждый уровень модели OSI выполняет определенную задачу в процессе передачи данных по сети. Базовая модель является основой для разработки сетевых протоколов. OSI разделяет коммуникационные функции в сети на семь уровней, каждый из которых обслуживает различные части процесса области взаимодействия открытых систем. Модель OSI описывает только системные средства взаимодействия, не касаясь приложений конечных пользователей.

Приложения реализуют свои собственные протоколы взаимодействия, обращаясь к системным средствам [4].

Подробнее об уровнях модели OSI:

1) Физический (Physical). Физический уровень предназначен для сопряжения с физическими средствами соединения. Физические средства соединения – это совокупность физической среды, аппаратных и программных средств, обеспечивающая передачу сигналов между системами. Физическая среда – это материальная субстанция, через которую осуществляется передача сигналов. Физическая среда является основой, на которой строятся физические средства соединения. В качестве физической среды широко используются эфир, металлы, оптическое стекло и кварц. Физический уровень состоит из Подуровня стыковки со средой и Подуровня преобразования передачи. Первый из них обеспечивает сопряжение потока данных с используемым физическим каналом связи. Второй осуществляет преобразования, связанные с применяемыми протоколами. Физический уровень обеспечивает физический интерфейс с каналом передачи данных, а также описывает процедуры передачи сигналов в канал и получения их из канала. На этом уровне определяются электрические, механические, функциональные и процедурные параметры для физической связи в системах. Физический уровень получает пакеты данных от вышележащего канального уровня и преобразует их в оптические или электрические сигналы, соответствующие 0 и 1 бинарного потока. Эти сигналы посылаются через среду передачи на приемный узел Наиболее распространенная спецификаций физического уровня IEEE 802.3 – Ethernet.

2) Канальный (Data link). Единицей информации канального уровня являются кадры (frame). Кадры – это логически организованная структура, в которую можно помещать данные. Задача канального уровня – передавать кадры от сетевого уровня к физическому уровню. Канальный уровень обеспечивает корректность передачи каждого кадра, помещая специальную последовательность бит, в начало и конец каждого кадра, чтобы отметить его, а также вычисляет

контрольную сумму, суммируя все байты кадра определенным способом и добавляя контрольную сумму к кадру. Когда кадр приходит, получатель снова вычисляет контрольную сумму полученных данных и сравнивает результат с контрольной суммой из кадра. Если они совпадают, кадр считается правильным и принимается. Если же контрольные суммы не совпадают, то фиксируется ошибка. Задача канального уровня – брать пакеты, поступающие с сетевого уровня и готовить их к передаче, укладывая в кадр соответствующего размера. Этот уровень обязан определить, где начинается и где заканчивается блок, а также обнаруживать ошибки передачи. На этом же уровне определяются правила использования физического уровня узлами сети. Электрическое представление данных в ЛВС (биты данных, методы кодирования данных и маркеры) распознаются на этом и только на этом уровне. Здесь обнаруживаются и исправляются (путем требований повторной передачи данных) ошибки. Наиболее часто используемые на уровне 2 протоколы включают: IEEE 802.2 LLC (тип I и тип II) обеспечивают MAC для сред 802.x, Ethernet.

3) Сетевой (Network). Сетевой уровень обеспечивает прокладку каналов, соединяющих абонентские и административные системы через коммуникационную сеть, выбор маршрута наиболее быстрого и надежного пути. Сетевой уровень устанавливает связь в вычислительной сети между двумя системами и обеспечивает прокладку виртуальных каналов между ними. Виртуальный или логический канал – это такое функционирование компонентов сети, которое создает взаимодействующим компонентам иллюзию прокладки между ними нужного тракта. Кроме этого, сетевой уровень сообщает транспортному уровню о появляющихся ошибках. Сообщения сетевого уровня принято называть пакетами (packet). В них помещаются фрагменты данных. Сетевой уровень отвечает за их адресацию и доставку между сетями. Прокладка наилучшего пути для передачи данных называется маршрутизацией, и ее решение является главной задачей сетевого уровня. Эта проблема осложняется тем, что самый короткий путь не всегда самый лучший. Часто критерием при выборе

маршрута является время передачи данных по этому маршруту; оно зависит от пропускной способности каналов связи и интенсивности трафика, которая может изменяться с течением времени. Некоторые алгоритмы маршрутизации пытаются приспособиться к изменению нагрузки, в то время как другие принимают решения на основе средних показателей за длительное время. Выбор маршрута может осуществляться и по другим критериям, например, надежности передачи.
Сетевой уровень отвечает за деление пользователей на группы и маршрутизацию пакетов на основе преобразования MAC-адресов в сетевые адреса. Сетевой уровень обеспечивает также прозрачную передачу пакетов на транспортный уровень. Наиболее часто на сетевом уровне используются протоколы: IP, IPsec, GRE, ICMP.

4) Транспортный (Transport). Транспортный уровень предназначен для передачи пакетов через коммуникационную сеть. На транспортном уровне пакеты разбиваются на блоки (сегменты). На пути от отправителя к получателю пакеты могут быть искажены или утеряны. Хотя некоторые приложения имеют собственные средства обработки ошибок, существуют и такие, которые предпочитают сразу иметь дело с надежным соединением. Работа транспортного уровня заключается в том, чтобы обеспечить приложениям или верхним уровням модели (прикладному и сеансовому) передачу данных с той степенью надежности, которая им требуется. Модель OSI определяет пять классов сервиса, предоставляемых транспортным уровнем. Эти виды сервиса отличаются качеством предоставляемых услуг: срочностью, возможностью восстановления прерванной связи, наличием средств мультиплексирования нескольких соединений между различными прикладными протоколами через общий транспортный протокол, а главное способностью к обнаружению и исправлению ошибок передачи, таких как искажение, потеря и дублирование пакетов. Транспортный уровень определяет адресацию физических устройств (систем, их частей) в сети. Этот уровень гарантирует доставку блоков информации адресатам и управляет этой доставкой. Его главной задачей является обеспечение

эффективных, удобных и надежных форм передачи информации между системами. Когда в процессе обработки находится более одного пакета, транспортный уровень контролирует очередность прохождения пакетов. Если проходит дубликат принятого ранее сообщения, то данный уровень опознает это и игнорирует сообщение. Наиболее распространенные протоколы транспортного уровня включают: TCP, UDP.

5) Сеансовый (Session). Сеансовый уровень – это уровень, определяющий процедуру проведения сеансов между пользователями или прикладными процессами. Сеансовый уровень обеспечивает управление диалогом для того, чтобы фиксировать, какая из сторон является активной в настоящий момент, а также предоставляет средства синхронизации. Последние позволяют вставлять контрольные точки в длинные передачи, чтобы в случае отказа можно было вернуться назад к последней контрольной точке, вместо того чтобы начинать все сначала. На практике немногие приложения используют сеансовый уровень, и он редко реализуется. Сеансовый уровень управляет передачей информации между прикладными процессами, координирует прием, передачу и выдачу одного сеанса связи. Кроме того, сеансовый уровень содержит дополнительно функции управления паролями, управления диалогом, синхронизации и отмены связи в сеансе передачи после сбоя вследствие ошибок в нижерасположенных уровнях. Функции этого уровня состоят в координации связи между двумя прикладными программами, работающими на разных рабочих станциях. Это происходит в виде хорошо структурированного диалога. В число этих функций входит создание сеанса, управление передачей и приемом пакетов сообщений во время сеанса и завершение сеанса.

6) Представительский (Presentation). Функции данного уровня – представление данных, передаваемых между прикладными процессами, в нужной форме. Этот уровень обеспечивает то, что информация, передаваемая прикладным уровнем, будет понятна прикладному уровню в другой системе. В случаях необходимости уровень представления в момент передачи информации

выполняет преобразование форматов данных в некоторый общий формат представления, а в момент приема, соответственно, выполняет обратное преобразование. Таким образом, прикладные уровни могут преодолеть, например, синтаксические различия в представлении данных. Такая ситуация может возникнуть в ЛВС с неоднотипными компьютерами (IBM PC и Macintosh), которым необходимо обмениваться данными. Так, в полях баз данных информация должна быть представлена в виде букв и цифр, а зачастую и в виде графического изображения. Обрабатывать же эти данные нужно, например, как числа с плавающей запятой. В основу общего представления данных положена единая для всех уровней модели система ASN. Эта система служит для описания структуры файлов, а также позволяет решить проблему шифрования данных. На этом уровне может выполняться шифрование и дешифрование данных, благодаря которым секретность обмена данными обеспечивается сразу для всех прикладных сервисов. Примером такого протокола является протокол Secure Socket Layer (SSL), который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека TCP/IP. Этот уровень обеспечивает преобразование данных (кодирование, компрессия и т. п.) прикладного уровня в поток информации для транспортного уровня.

7) Прикладной (Application). Прикладной уровень обеспечивает прикладным процессам средства доступа к области взаимодействия, является верхним (седьмым) уровнем и непосредственно примыкает к прикладным процессам. В действительности прикладной уровень – это набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, таким как файлы, принтеры или гипертекстовые Web-страницы, а также организуют свою совместную работу, например с помощью протокола электронной почты. Специальные элементы прикладного сервиса обеспечивают сервис для конкретных прикладных программ, таких как программы пересылки файлов и эмуляции терминалов. Если, например программе необходимо переслать файлы, то обязательно будет использован протокол

передачи, доступа и управления файлами FTAM (File Transfer, Access, and Management). В модели OSI прикладная программа, которой нужно выполнить конкретную задачу (например, обновить базу данных на компьютере), посылает конкретные данные в виде дейтаграммы на прикладной уровень. Одна из основных задач этого уровня – определить, как следует обрабатывать запрос прикладной программы, другими словами, какой вид должен принять данный запрос. Единица данных, которой оперирует прикладной уровень, обычно называется сообщением (message). К числу наиболее распространенных протоколов верхних уровней относятся: FTP, TFTP, Telnet, SSH, SMTP, SNMP, NFS, HTTP, HTTPS.

1.3 Сетевое оборудование

Сетевое оборудование – устройства, необходимые для работы компьютерной сети [6]. Есть различные классификации сетевого оборудования, например по функциям, выполняемым в сети:

– Устройства пользователя (конечное оборудование). В эту группу входят компьютеры, принтеры, сканеры и другие устройства, которые выполняют функции, необходимые непосредственно пользователю сети.

– Сетевые устройства. Эти устройства позволяют осуществлять связь с другими сетевыми устройствами или устройствами конечного пользователя. В сети они выполняют специфические функции.

Сетевой коммутатор (switch) – устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети. Коммутатор работает на канальном (втором) уровне модели OSI. Коммутаторы были разработаны с использованием мостовых технологий и часто рассматриваются как многопортовые мосты.

Рисунок 3 – Коммутатор Cisco C3550

Коммутатор передаёт данные только непосредственно получателю (исключение составляет широковещательный трафик всем узлам сети и трафик для устройств, для которых неизвестен исходящий порт коммутатора). Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались [8].

Коммутатор хранит в памяти (т.н. ассоциативной памяти) таблицу коммутации, в которой указывается соответствие MAC-адреса узла порту коммутатора. При включении коммутатора эта таблица пуста, и он работает в режиме обучения. В этом режиме поступающие на какой-либо порт данные передаются на все остальные порты коммутатора. При этом коммутатор анализирует фреймы (кадры) и, определив MAC-адрес хоста-отправителя, заносит его в таблицу на некоторое время. Впоследствии, если на один из портов коммутатора поступит кадр, предназначенный для хоста, MAC-адрес которого уже есть в таблице, то этот кадр будет передан только через порт, указанный в таблице. Если MAC-адрес хоста-получателя не ассоциирован с каким-либо портом коммутатора, то кадр будет отправлен на все порты, за исключением того порта, с которого он был получен. Со временем коммутатор строит таблицу для всех активных MAC-адресов, в результате трафик локализуется [8].

Коммутаторы подразделяются на управляемые и неуправляемые (наиболее простые).

Более сложные коммутаторы позволяют управлять коммутацией на сетевом (третьем) уровне модели OSI. Обычно их именуют соответственно, например «Layer 3 Switch» или сокращенно «L3 Switch» [17]. Управление коммутатором может осуществляться посредством Web-интерфейса, интерфейса командной строки (CLI), протокола SNMP, RMON и т. п.

Многие управляемые коммутаторы позволяют настраивать дополнительные функции: VLAN, QoS, агрегирование, зеркалирование. Многие коммутаторы уровня доступа обладают такими расширенными возможностями, как сегментация трафика между портами, контроль трафика на предмет штормов, обнаружение петель, ограничение количества изучаемых MAC-адресов, ограничение входящей/исходящей скорости на портах и т. п.

Сложные коммутаторы можно объединять в одно логическое устройство – стек – с целью увеличения числа портов. Например, можно объединить 4 коммутатора с 24 портами и получить логический коммутатор с 90 портами либо с 96 портами (если для стекирования используются специальные порты).

Маршрутизатор (router) – устройство, которое пересылает пакеты между различными сегментами сети на основе правил и таблиц маршрутизации [11]. Маршрутизатор может связывать разнородные сети различных архитектур. Для принятия решений о пересылке пакетов используется информация о топологии сети и определённые правила, заданные администратором.

Маршрутизаторы работают на «сетевом» (третьем) уровне сетевой модели OSI, нежели коммутатор, который работает соответственно на втором и первом уровнях модели OSI [14].

Рисунок 4 – Маршрутизатор Cisco C2801

Обычно маршрутизатор использует адрес получателя, указанный в заголовке пакета, и определяет по таблице маршрутизации путь, по которому следует передать данные. Если в таблице маршрутизации для адреса нет описанного маршрута, пакет отбрасывается [18].

Существуют и другие способы определения маршрута пересылки пакетов, когда, например, используется адрес отправителя, используемые протоколы верхних уровней и другая информация, содержащаяся в заголовках пакетов сетевого уровня. Нередко маршрутизаторы могут осуществлять трансляцию адресов отправителя и получателя, фильтрацию транзитного потока данных на основе определённых правил с целью ограничения доступа, шифрование/расшифрование передаваемых данных и т. д.

Таблица маршрутизации содержит информацию, на основе которой маршрутизатор принимает решение о дальнейшей пересылке пакетов. Таблица состоит из некоторого числа записей – маршрутов, в каждой из которых содержится идентификатор сети получателя (состоящий из адреса и маски сети), адрес следующего узла, которому следует передавать пакеты, административное расстояние – степень доверия к источнику маршрута и некоторый вес записи – метрика. Метрики записей в таблице играют роль в вычислении кратчайших маршрутов к различным получателям. В зависимости от модели маршрутизатора

и используемых протоколов маршрутизации, в таблице может содержаться некоторая дополнительная служебная информация [21].

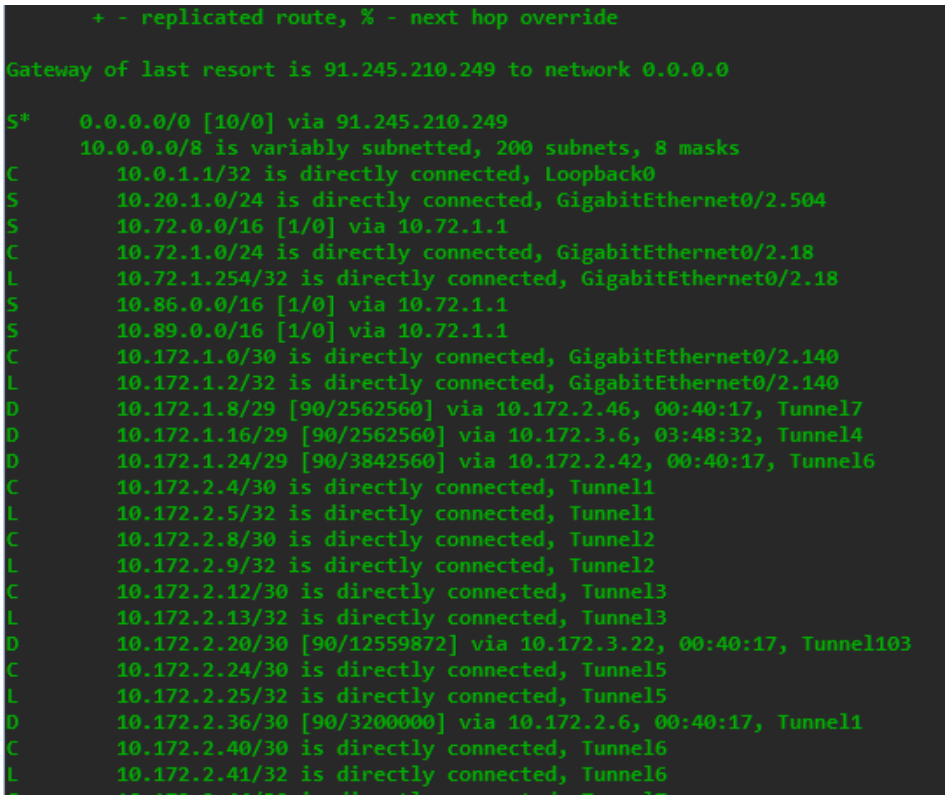

Рисунок 5 – Пример таблицы маршрутизации

Таблица маршрутизации может составляться двумя способами:

1) Статическая маршрутизация – когда записи в таблице вводятся и изменяются вручную. Такой способ требует вмешательства администратора каждый раз, когда происходят изменения в топологии сети. С другой стороны, он является наиболее стабильным и требующим минимума аппаратных ресурсов маршрутизатора для обслуживания таблицы.

2) Динамическая маршрутизация – когда записи в таблице обновляются автоматически при помощи одного или нескольких протоколов маршрутизации – RIP, OSPF, IGRP, EIGRP, BGP, и др. Кроме того, маршрутизатор строит таблицу оптимальных путей к сетям назначения на основе различных критериев – количества промежуточных узлов, пропускной способности каналов, задержки передачи данных и т. п. Критерии вычисления оптимальных маршрутов чаще всего зависят от протокола маршрутизации, а также задаются конфигурацией

маршрутизатора. Такой способ построения таблицы позволяет автоматически держать таблицу маршрутизации в актуальном состоянии и вычислять оптимальные маршруты на основе текущей топологии сети. Однако динамическая маршрутизация оказывает дополнительную нагрузку на устройства, а высокая нестабильность сети может приводить к ситуациям, когда маршрутизаторы не успевают синхронизировать свои таблицы, что приводит к противоречивым сведениям о топологии сети в различных её частях и потере передаваемых данных.

Существует еще несколько видов сетевого оборудования, среди которых: межсетевой экран, сетевой адаптер, медиаконвертер, сетевой трансивер, точка подключения для Wi-Fi и т. п.

1.4 Теория информационной и сетевой безопасности

Информационная безопасность (ИБ) – это состояние информационной системы, при котором она наименее восприимчива к вмешательству и нанесению ущерба со стороны третьих лиц. Безопасность данных также подразумевает управление рисками, которые связаны с разглашением информации или влиянием на аппаратные и программные модули защиты. Безопасность информации, которая обрабатывается в организации, – это комплекс действий, направленных на решение проблемы защиты информационной среды в рамках компании. При этом информация не должна быть ограничена в использовании и динамичном развитии для уполномоченных лиц [2].

Сетевой безопасностью называются действия, направленные на защиту работоспособности и целостности сети и данных. Сюда относятся аппаратные и программные технологии. Эффективность сетевой безопасности выражается в управлении доступом к сетевым ресурсам. Данный комплекс мер ориентирован на множество угроз и позволяет предотвратить их проникновение и распространение в сети [24].

Пренебрежение сетевой безопасностью может стоит предприятию огромных финансовых потерь. По данными НАФИ (Национальное Агенство Финансовых

исследований), в 2017 г. около половины российских компаний сталкивались с различными угрозами, а финансовые потери от атак понесли 22 % из них. Ущерб российских компаний от кибератак составил 116 млрд рублей в 2017 г. «Большинство российских предпринимателей считают, что в будущем их не затронут хакерские атаки, несмотря на объективный рост числа таких атак. В текущих реалиях эти данные свидетельствует, к сожалению, не о том, что компании защищены и эти атаки не произойдут. Напротив, в большинстве российских предприятий нет объективной оценки информационных угроз, и это в итоге препятствует разработке планов действий на случай возможных атак.

В зарубежной и Отечественной литературе существует достаточно много различных методик внедрения, аудита, улучшения сетевой безопасности. В соответствии с одной из методик вначале необходимо классифицировать защищаемую информацию (определить ее конфиденциальность, ценность, жизненный цикл и т. п.), определить риски, разработать политику безопасности, разработать конкретные положения для различных отделов предприятия и т. д.

Проведем классификацию уязвимостей в КСПД:

– Недостатки (упущения) политики безопасности.

– Ошибки дизайна (КСПД и информационных ресурсов).

– Слабости протоколов.

– Уязвимости программного обеспечения.

– Ошибки в конфигурации оборудования.

– Вредоносный код.

– Человеческий фактор.

– Прочие уязвимости.

Классификация контрмер:

– Административные (руководящие документы).

– Технические (корректно сконфигурированные протоколы обеспечения безопасности сети, использование методов защиты протоколов и т. п.).

– Физические (Средства Контроля и Управления Доступом).

Один из лучших подходов для обеспечения сетевой безопасности – Глубокая защита (Defense in Depth). Этот подход подразумевает разбитие защиты на несколько уровней, каждый уровень при этом, должен иметь свои средства защиты. Механизмы защиты уровней должны поддерживать друг друга, при этом быть независимыми, предоставлять разнообразные и даже избыточные методы защиты. Можно провести аналогию данного метода с защитой замка, где есть ров вокруг замка, поднимающиеся ворота, внешний периметр защиты, внутренний периметр защиты, крепость и т. д.

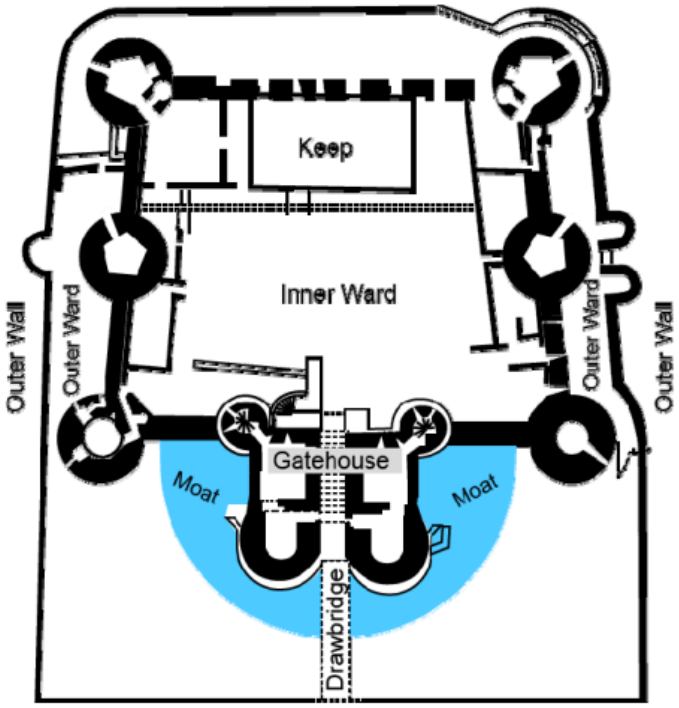

Рисунок 6 – Структура защиты средневекового замка

Общепринятая стратегия защиты КСПД – деление сети на различные зоны, в большинстве своем используются следующие зоны:

– Inside – внутренняя зона (зона подконтрольная предприятию).

– Outside – внешняя зона (зона находящаяся все контроля предприятия).

– DMZ (Demilitarized Zone) – демилитаризованная зона.

Внутренняя зона предприятия подразумевает частную сеть под единым административным началом, с конфиденциальными данными, частными информационными сервисами, серверами, клиентскими устройствами и т. п.

Внешняя зона – зона считающаяся априори не безопасной, все запросы, пакеты из данной зоны необходимо считать потенциально вредоносными и соответствующим образом защищать периметр сети. Пример такой зоны – интернет.

Демилитаризованная зона – зона содержащая информационные сервисы предприятия, которые должны быть доступны из внешней зоны (и обычно из внутренней). В этой зоне могут быть расположены Web-сервера, почтовые сервера и т. п.

Для обеспечения сетевой безопасности необходимо определить устройства, которые будут обеспечивать защиту от сетевых атак – чаще всего это коммутаторы, маршрутизаторы, межсетевые экраны. Данные устройства обеспечивают не только работоспособность сети, но еще и защищают как сеть, так и клиентов сети (пользовательские компьютеры, принтеры и т. п.). Процессы сетевых устройств можно разбить на 3 функциональных плоскости:

– Management Plane – плоскость управления. В данную плоскость попадает трафик для управления и мониторинга сетевого устройства, например SSH, SNMP, telnet. Как правило, данный трафика направляется в сетевое устройство.

– Control Plane – плоскость контроля. В данную плоскость попадает трафик поддерживающий функционирование сети, например BGP, OSPF, EIGRP. Данный трафик обычно направляется в сетевое устройство из другого сетевого устройства.

– Data Plane – плоскость данных. В данную плоскость попадает трафик ассоциированный с пользовательскими данными, данными сервера, системы хранения данных и т. п. Трафик, чаще всего, направляется от одного конечного устройства другому, например от пользователя к серверу баз данных.

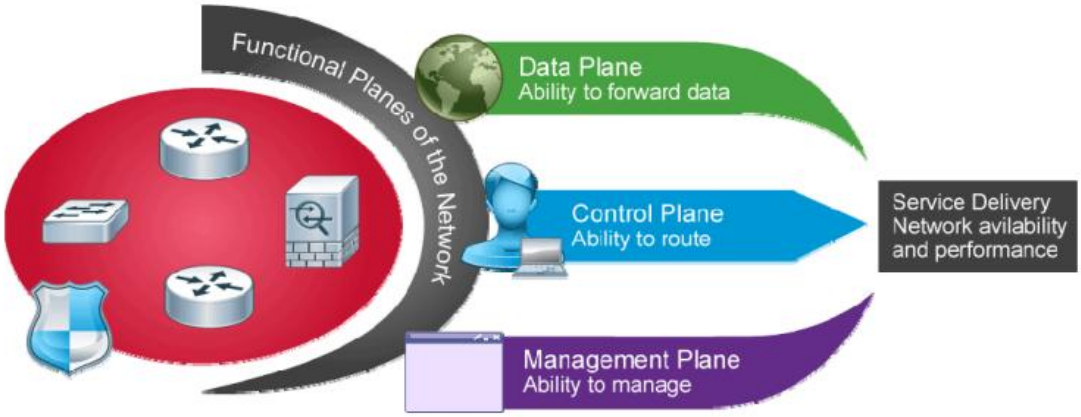

Рисунок 7 – Функциональных плоскости сетевых устройств

Каждая плоскость предоставляет различный функционал, который необходимо защищать, каждый по-своему. Плоскость управления можно защитить внедрив AAA (Authentication Authorization Accounting – аутентификация Авторизация Учет), ACL (Access Control List – Списки Управления Доступом). Для плоскости контроля – аутентификация протоколов динамической маршрутизации, использование SNMP ловушек высоких значений использования ЦПУ или памяти сетевого устройства. В плоскости данных применяются множество разных средств защиты, таких как VPN (Virtual Private Network – Виртуальная частная сеть), ACL, IPS (Intrusion Prevention System – Система Предотвращения Вторжений), шифрование данных и т. п.

1.5 Шифрование данных

Шифрование данных используется для обеспечения целостности, конфиденциальности и доступности получателям этих данных. Часто шифрование применяется при построении виртуальных частных сетей. Виртуальная частная сеть – обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений передаваемых по логической сети сообщений).

VPN крайне удобное средство для предприятий с развитой территориально распределенной КСПД [24]. Например, VPN позволяет прозрачно для пользователя в удаленном филиале обмениваться информацией с центральным офисом, использовать сервисы центрального офиса и т. д.

В настоящее время существует большое разнообразие алгоритмов шифрования разной стойкости ко взлому. Некоторые алгоритмы шифрования могут быть взломаны с помощью использования соответствующих алгоритмов дешифровки, обычно такие алгоритмы шифрования не являются стойкими и их е используют в КСПД. Стоит отметить, что любой зашифрованный пароль можно взломать, применив грубую атаку (brute force), т. е. последовательным перебором всех комбинаций символов и букв. Грубая атака обычно применяется с использованием словарей, где заранее определены некоторые распространенные логины и пароли, например пароль Password могут взломать мгновенно. Поэтому необходимо использовать длинные пароли (включая спецсимволы, верхний и нижний регистры). Важное значение имеет длина ключа шифрования. Современные технологии позволяют взломать слово, зашифрованное на алгоритме шифрования DES (с длинной ключа 56 бит) за несколько часов. В свою очередь при использовании алгоритма AES (с длинной ключа до 256 бит) на взлом (грубой атакой) сложного пароля уйдет около 150 триллионов лет.

Хеширование – механизм, гарантирующий целостность данных. На входе функции может быть слово или файл, на выходе – фиксированный набор букв и цифр. Значение Хэш-функции не обратимо [2]. Например, мы можем подать на вход 128-битной хеш-функции книгу в шестнадцатеричном коде и парольную фразу. В результате на выходе мы в обоих случаях получим разные наборы псевдослучайных шестнадцатеричных цифр вида: cf8a0b923820dcc509a6f75849b. При изменении исходного текста даже на один знак, полностью, непредсказуемо меняется результат хеш-функции. Взломать исходный пароль при этом можно лишь применив грубую атаку. На сегодняшний день в основном используются следующие алгоритмы хэширования: MD5 (Message Digest), SHA1 (Secure Hash

Algorithm), SHA2. Они отличаются скоростью работы, длинной ключа, вероятностью возникновения коллизии. Коллизией называется случай, при котором одна хеш-функция для разных входных блоков возвращает одинаковые хеш-коды. Чем длиннее ключ, тем меньше вероятность возникновения коллизии [24].

Шифрование можно разделить на симметричное (более быстрое, например DES, 3DES, AES) и ассиметричное (менее быстрое в сравнении с симметричным, например RSA, DSA, elliptic curves algorithms). В симметричном шифровании один и тот же ключ используется для шифрования и дешифрования сообщений. Обе стороны должны иметь этот ключ для успешной коммуникации, секретно передать данный ключ может быть проблемой. В ассиметричном: создается (на каждой стороне) два ключа, один называется закрытый (private), другой открытый (public). Закрытый ключ остается у стороны сгенерировавшей его (важно, чтобы закрытый ключ никоим образом не попал злоумышленникам), открытый ключ свободно пересылается адресату (если его перехватит атакующий – безопасность от этого не пострадает). Данную процедуру выполняют обе стороны.

Рисунок 8 – Получение сообщения, с использованием ассиметричного шифрования

Сообщения, зашифрованные открытым ключом, сможет расшифровать лишь соответствующий закрытый ключ. Сообщения, зашифрованный закрытым ключом – дешифрует открытый. Может возникнуть вопрос зачем шифровать сообщения закрытым ключом, которое может расшифровать любой человек

получивший (или перехвативший) открытый ключ. Ответ заключается в следующем. Обычно все сообщение целиком, не шифруется, шифруется хэш от этого сообщения, далее отправляется, в открытом виде, сообщение и шифрованный хэш (так называемая подпись). Таким образом можно однозначно идентифицировать отправителя сообщения, а также понимать, что дошло оригинальное (не перехваченное и измененное злоумышленником) сообщение.

1.6 Распространенные сетевые атаки

DoS и DDoS. DDoS (Distributed Denial of Service) – распределённая атака типа «отказ в обслуживании». Сетевой ресурс выходит из строя в результате множества запросов к нему, отправленных из разных точек. Обычно атака организуется при помощи бот-нетов. Злоумышленник заражает компьютеры ни о чем не подозревающих пользователей Интернета. Такие «зомби» и отправляют бессмысленные запросы на сервер жертвы. Обрабатывая миллионы запросов, сервер сначала «тормозит», а после и вовсе прекращает работать. Например, можно использовать TCP SYN flood, т. е. на сервер (жертву) с множества разных IP адресов идут запросы типа TCP SYN, на которые сервер отвечает TCP SYN ACK и создает при этом запись в своей таблице подключений. Обратного ответа сервер не дождется, так запись в таблице остается до окончания времени существования. На любом устройстве эта таблица не бесконечна, соответственно при достаточном количестве одновременно атакующих бот-нетов, можно достигнуть предела у этой таблицы – сервер не будет воспринимать новые запросы.

Spoofing (подмена). Атакующий отправляет в сеть пакеты с данными других узлов (подмененные). Например, злоумышленник заменяет свой IP адрес (или MAC адрес) на IP адрес жертвы (пользователя, сервера). Другой пример ARP-spoofing изображен на рисунке ниже.

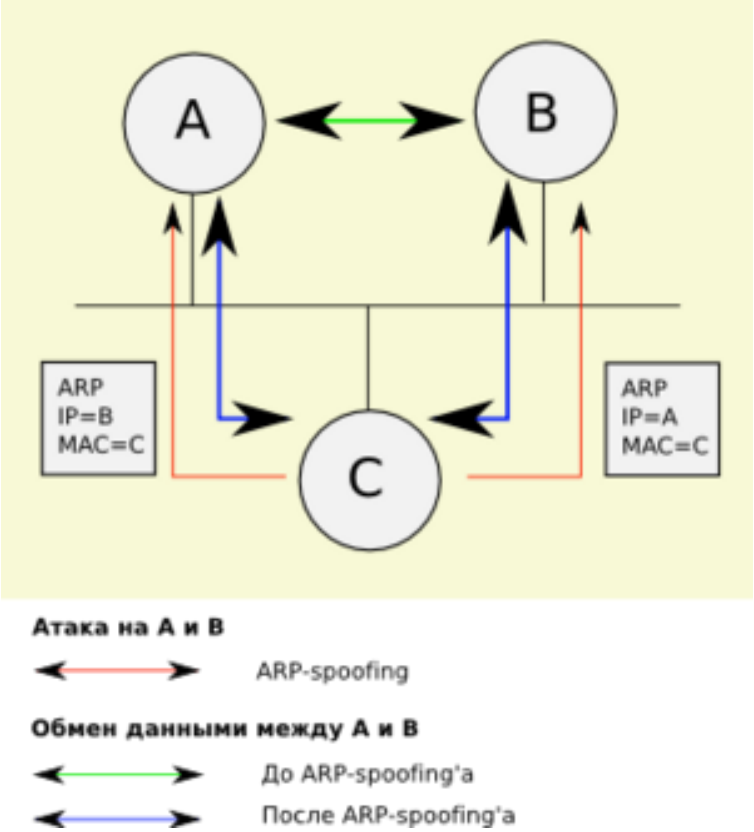

Рисунок 9 – ARP-spoofing

До выполнения ARP-spoofing'a в ARP-таблице узлов A и B существуют записи с IP- и MAC-адресами друг друга. Обмен информацией производится непосредственно между узлами A и B (зелёная стрелка). В ходе выполнения ARP-spoofing'a компьютер C, выполняющий атаку, отправляет ARP-ответы (без получения запросов):

– узлу A: с IP-адресом узла B и MAC-адресом узла C;

– узлу B: с IP-адресом узла A и MAC-адресом узла C.

В силу того что компьютеры поддерживают самопроизвольный ARP (gratuitous ARP), они модифицируют собственные ARP-таблицы и помещают туда записи, где вместо настоящих MAC-адресов компьютеров A и B стоит MAC-адрес компьютера C (красные стрелки). После того как атака выполнена, когда компьютер A хочет передать пакет компьютеру B, он находит в ARP-таблице запись (она соответствует компьютеру C) и определяет из неё MAC-адрес получателя. Отправленный по этому MAC-адресу пакет приходит компьютеру C

вместо получателя. Компьютер C затем ретранслирует пакет тому, кому он действительно адресован – т. е. компьютеру B (синие стрелки).

Reflection and Amplification attack (Атаки отражения и усиления). Атака отражения это разновидность DoS атак, в которой злоумышленник отправляет большое количество запросов жертве. Злоумышленник подменяет свой IP на IP жертвы и посылает различные запросы на адреса отличные от адреса жертвы, все кто принял запрос отправляют ответ уже на IP жертвы, т. е. становятся отражателями (reflectors). Если запрос атакующего вызывает более объемный ответ, то атака считается усиливающей. Часто такие атаки используют протоколы DNS и NTP.

Man-in-the-Middle attack (атака человек по середине). Данная атака представляет из себя определенную концепцию, которая может быть применена в разных сценариях атак. В общем случае, система злоумышленника имеет возможность видеть пакеты передаваемые двумя другими системами, выдавая себя за коммуникационный путь между двумя другими системами. Например, ARP-Poisoning (отравление таблицы ARP). После отравления ARP таблиц жертв, каждое зараженное устройство отправляет пакеты уже через устройство злоумышленника, что ставит устройство злоумышленника посередине пути коммуникации устройств жертв. С полученным злоумышленником траффиком уже можно делать все что угодно, например изменять его, перехватывать пароли и конфиденциальные данные. На рисунке ниже изображена эта атака. Атакующий отравляет ARP таблицу хоста A и B – поэтому оба хоста будут отправлять пакеты через атакующего, при отправке пакетов от хоста A к хосту B и наоборот.

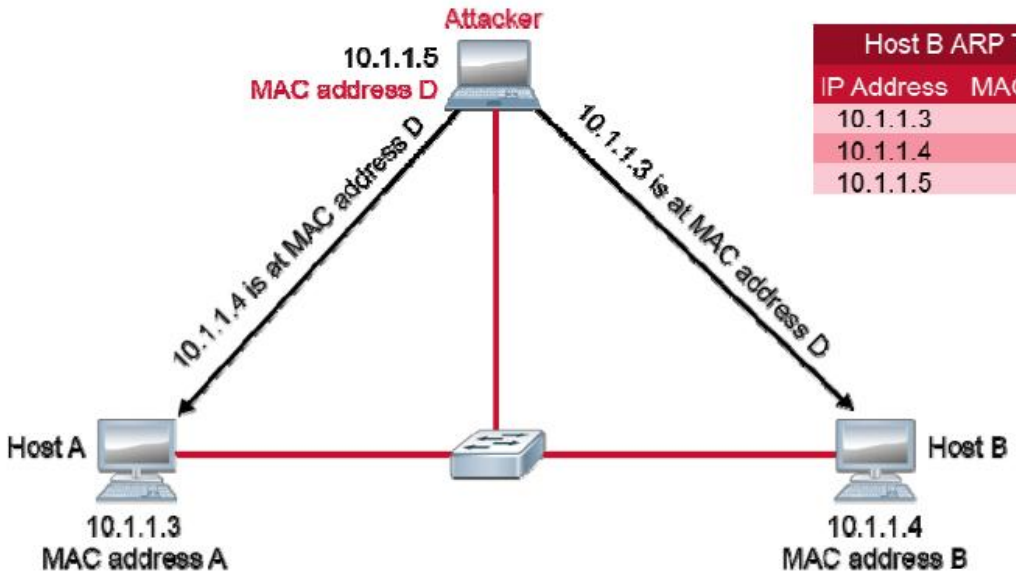

Рисунок 10 – Man-in-the-Middle attack

Существует еще несколько атак и множество их разновидностей, например фишинг, социальная инженерия, атаки на пароли, вредоносное ПО, атаки на переполнение буфера.

1.7 Распространенные методы защиты сети

Методы защиты КСПД:

– Использование Firewall (Межсетевой экран) – программный или программно-аппаратный комплекс, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.

– Использование IPS – система, обеспечивающая глубокий анализ сетевого траффика, ищущая подозрительную сетевую активность и препятствующая прохождению данного траффика.

– Content Security (безопасность контента) – система, осуществляющая анализ контента внутри определенного сетевого объекта (например, такая система может отыскать вредоносное ПО во вложении электронного письма, заблокировать адрес с которого оно пришло, отправить письмо на карантин, а не во входящую папку пользователя).

– Использование VPN.

– Endpoint Security (безопасность конечного устройства) – комплекс мер направленных на защиту конечного оборудования, включает в себя локальный межсетевой экран, антивирус и т. д.

– Ведение журнала событий – при обнаружении подозрительной сетевой активности или действующей атаки необходимо обязательно разбирать каждый инцидент. Без существования баз данных, на которых будут записаны события и время, в которое оно произошло, расследовать инцидент будет крайне сложно.

– Защита сетевых устройств и протоколов, используемых на этих устройствах.

Конечно, желательно применять все доступные методы для защиты КСПД и ее пользователей. Но последний метод требует повышенного внимания к себе, т. к. речь идет о защите протоколов, используемых в активном сетевом оборудовании. Обычно предприятие (даже обладающее небольшим бюджетом) с КСПД имеет у себя в наличии хотя бы управляемый коммутатор и маршрутизатор. Если не уделять должного внимания защите сетевых протоколов и данных устройств, то работоспособность КСПД может быть нарушена, наряду с утечкой конфиденциальной информации.

Чтобы обезопасить сетевые устройства необходимо внедрить AAA, обезопасить Management и Control Plane, вести учет событий на сторонний сервер, использовать NTP (Network Time Protocol), использовать сложные пароли, применять баннеры. Для того, чтобы обезопасить сетевые протоколы (L2 и L3) необходимо использовать соответствующие методы, препятствующие атакам. Также стоит отметить, разные сотрудники занимаются разной работой (имеют разный уровень доступа к различным информационным ресурсам), соответственно необходимо не только на уровне приложения разграничить этот доступ, но и если это возможно, на сетевом уровне. Например, водитель не должен иметь возможности обращаться к серверу 1С Бухгалтерия Предприятия, в свою очередь, главный бухгалтер должен не только иметь доступ до этого сервера, но и обладать почти максимальными правами в соответствующей

информационной системе. Ограничивать сетевую доступность ресурсов, можно применяя, например, списки доступа на маршрутизаторах.

AAA состоит из трёх частей: Аутентификация (проверка личности), Авторизация (предоставление определенных прав в соответствии с ролью, исполняемыми обязанностями, группой аутентифицированного лица), Учет (учет совершенных действий лицом). Возможно настроить локальную AAA, либо внешний сервер AAA (учет действий может производит лишь внешний сервер AAA). Если КСПД имеет хотя бы несколько сетевых устройств и более одного администратора, то рекомендуется использовать внешний сервер AAA. Существует 2 протокола для взаимодействия сетевого устройства и внешнего сервера AAA – TACACS+ (Terminal Access Controller Access Control Server) и RADIUS (Remote Authentication Dial-In User Service). Протокол TACACS+ является разработкой компании Cisco. Протокол использует порт TCP 49, все данные сессии шифруются, а также протокол полностью разграничивает на 3 части понятие AAA. Протокол RADIUS является полностью открытым, работает по порту UDP 1645/1812 для аутентификации и авторизации, для учета используется UDP 1646/1813. В протоколе шифруются только пароли, остальные данные передаются в открытом виде. RADIUS разделяет AAA на 2 части, аутентификацию идет вместе с авторизацией, учет происходит отдельно.

В процессе внедрения безопасности в Management Plane необходимо включить и использовать более защищенные протоколы для осуществления управления и мониторинга сетевого устройства. Обычно любое управляемое устройство поддерживает протокол telnet, но все данные передающиеся в рамках данного протокола (в том числе и пароли) являются открытыми. Альтернатива данному незащищенному протоколу – протокол SSH ver. 2 (Secure Shell). SSH использует ассиметричный алгоритм шифрования RSA. Сетевые устройства использующие telnet не могут считаться защищенными, а значит необходимо включать использование протокола SSH и не забывать использовать сложные пароли.

При организации мониторинга сетевых устройств используется протокол SNMP (Simple Net Management Protocol), обычно используется SNMP ver. 2, который также передает и запрашивает данные в открытом виде. Единственная защита данного протокола это так называемая Community String (слово, зная который сервер мониторинга может запрашивать информацию у сетевого устройства, при этом даже это слово передается в открытом виде). SNMP ver. 3 уже имеет возможность гибкого шифрования трафика (ничего не шифровать, шифровать только данные аутентификации, шифровать все).

Применение баннеров аргументированно судебной практикой США. В судебной практике США были несколько случаев, когда пойманным злоумышленникам удалось избежать ответственности за хакерскую атаку, т. к. при подключении по протоколу telnet или SSH в консоли либо не было никакого баннера, либо был баннер «Welcome». В суде злоумышленники утверждали, что они не знали, что заходят на сетевое устройство им не принадлежащее. Либо они как-бы случайно попадали на сетевое устройство, видели надпись «Welcome», думали, что их приветствуют, а значит, следует зайти на данное устройство. После таких судов, производители сетевого оборудования стали настоятельно рекомендовать использовать баннеры, которые будут отображены, при подключении к сетевому устройству. Причем исключать из баннера приветственные слова, описывать кому принадлежит данное устройство и даже немного запугивать ответственностью, которую человек может понести за неавторизованный доступ к системе. Ниже, на рисунке изображен пример правильно составленного баннера, к нему можно добавить лишь организацию владеющую устройством (хотя эти данные иногда предпочитают не указывать).

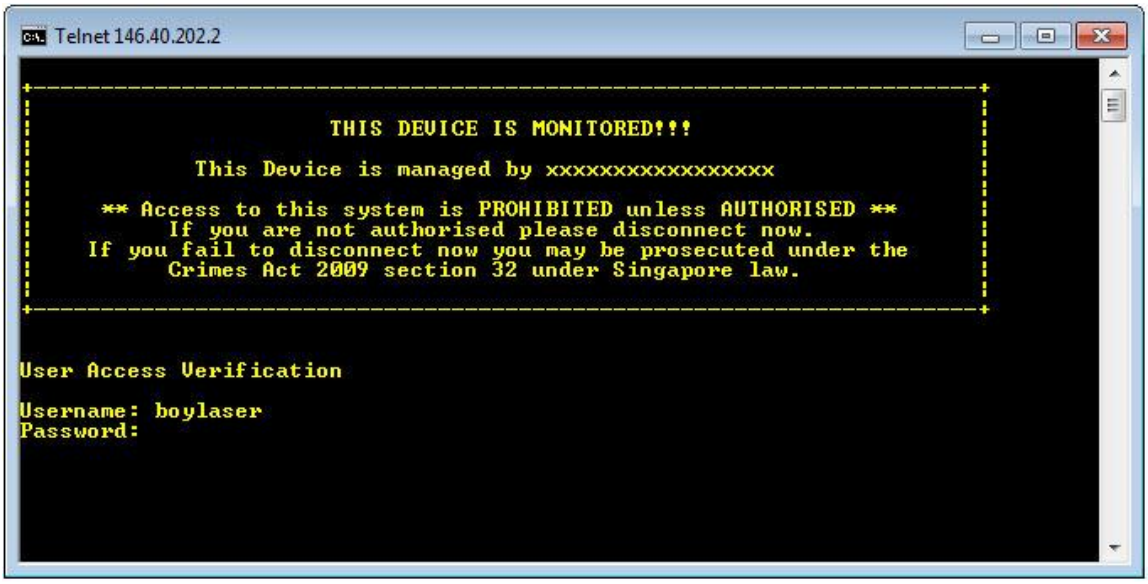

Рисунок 11 – Пример правильного баннера

Control Plane включает в себя аппаратно-программные части устройства, которые помогают обеспечивать функционирование сети. Траффик Control Plane – траффик, отправленный одним сетевым устройством, другому устройству, данный траффик обрабатывает CPU устройства. Например, это траффик маршрутизации, служебные сообщения (BPDU) протокола STP, сообщения протокола CDP и т. д. Многие сетевые атаки воздействуют именно на Control Plane. Чтобы обезопасить данную плоскость, часто применяют Control Plane Policing, т. е. определенную политику для обрабатывания траффика CPU устройства. Для того, чтобы защитить, например, таблицу маршрутизации маршрутизатора – используют аутентификацию протоколов динамической маршрутизации.

Для защиты различных протоколов используют соответствующие механизмы. Обычно эти механизмы общеизвестны и применяются во всех управляемых сетевых устройствах. Ниже описаны некоторые механизмы защиты протоколов:

– Для защиты STP применяют BPDU Guard, BPDU Filtering, Root Guard. Этот механизм позволяет исключить прием нелегитимных BPDU сетевым устройством.

– DHCP snooping. Технологи защиты, при которой создается БД соответствий MAC адреса и IP адреса, а также исключаются DHCP Request злоумышленников.

– Dynamic ARP Inspection (DAI). Защита от ARP-poisoning. DAI проверяет легитимность ARP reply (в соответствии со своей БД, либо статически настроенными значениями) и отклоняет не соответствующие ARP ответы.

Port Security. Механизм позволяющий бороться с атакой на переполнение MAC-таблицы коммутатора. Port Security ограничивает максимальное количество MAC-адресов на порту, может ограничивать какие конкретные MAC-адреса должны быть на определенном сетевом интерфейсе.

2 СРАВНЕНИЕ ОТЕЧЕСТВЕННЫХ И ПЕРЕДОВЫХ ЗАРУБЕЖНЫХ ТЕХНОЛОГИЙ И РЕШЕНИЙ

В настоящее время существует огромное множество компаний производящих активное сетевое оборудование, те или иные производители используют как стандартные открытые протоколы и технологии, так и проприетарные. Производители стремятся захватить нишу сетевого оборудования поэтому стремятся выпустить оборудование со своими фирменными функциями и улучшениями. Среди них, безусловно, выделяется компания Cisco, которая является лидером в области компьютерных сетей.

Cisco – американская транснациональная компания, разрабатывающая и продающая сетевое оборудование, предназначенное в основном для крупных организаций и телекоммуникационных предприятий. Одна из крупнейших в мире компаний, специализирующихся в области высоких технологий. Изначально занималась только корпоративными маршрутизаторами.

Одной из особенностей бизнес-модели компании стала многоуровневая разветвлённая система сертификации инженеров по компьютерным сетям. Благодаря тому, что экзамены этой системы проверяют знание не только продукции Cisco, но и знание сетевых технологий и протоколов, многие организации, даже работающие на сетевом оборудовании других фирм, признают ценность профессиональных сертификатов Cisco. В частности, сертификация на уровне эксперта (CCIE) является одной из самых известных и уважаемых в компьютерной индустрии.

В конце марта 2000, на пике бума доткомов, Cisco стала самой оценённой компанией в мире, с рыночной капитализацией больше 500 млрд долларов США. В июле 2009, имея капитализацию 108,03 млрд долл. США, она остаётся одной из самых больших компаний.

В конце 20-го века и начале 21 века компания Cisco внесла огромный вклад в развитие индустрии компьютерных сетей и интернета. Многие протоколы и технологии, которые она спроектировала (как проприетарные) были взяты за

основу открытыми (не зависящими от производителя) протоколами, которые в настоящее время используются в подавляющем большинстве сетевых устройств. Некоторые проприетарные протоколы компания Cisco публиковала, большинство же оставались конфиденциальными.

На Российском рынке сетевого оборудования можно отметить компанию Zelax. Zelax – российский разработчик и производитель решений для сетей передачи данных. Собственное производство и исследовательский центр, расположенные в Зеленограде, позволяют Zelax осуществлять полный цикл создания современного оборудования: систем оптического уплотнения, маршрутизаторов, коммутаторов, мультиплексоров, модемов, шлюзов TDM через IP, конвертеров, устройств защиты и др.

Компании Zelax также производит оборудование для зарубежных заказчиков, разрабатывает в том числе и специализированное оборудование для ведомственных сетей связи. Zelax одно из немногих предприятий полного цикла – от возникновения идеи изделия или постановки комплексной задачи до сопровождения, когда изделие уже работает у заказчика.

Zelax сотрудничает со многими клиентами по 15-20 лет. Это силовые структуры, операторы стационарной и мобильной связи, добывающие и промышленные предприятия. Сети с участием оборудования Zelax строятся по всей России (более 90 % поставок) и в странах СНГ (около 10 %).

Т. к. компания Cisco является мировым лидером на рынке сетевого оборудования, а компания Zelax зарекомендовавший производитель того же сегмента рынка в РФ – сравнение будет производится между этими производителями. В качестве предмета сравнения будет логичным взять основные виды корпоративного сетевого оборудования, а именно управляемые коммутаторы и маршрутизаторы. Сравнение будет производится лишь по некоторым общим параметрам.

Таблица 1 – Сравнение коммутаторов Cisco и Zelax

Характеристика	Cisco WS-C2960-24LC-S	ZES-2028G
Уровень по модели OSI	2	2
Коммутационная фабрика	32 Гб\с	56 Гб\с
Количество портов	24	24
Таблица MAC адресов	8192	16384
QoS	Auto/Per Port	Auto/Per Port
PoE	Есть	Есть
Основные протоколы L2	Есть	Есть
Протоколы безопасности L2	Есть	Есть
Наличие проприетарных технологий и протоколов	Есть	Отсутсвуют

Из таблицы 1 видно, что коммутатор ZES-2028G превосходит коммутатор C2960 по техническим параметрам почти в 2 раза. Коммутатор C2960 в свою очередь обладает рядом проприетарных протоколов и технологи компании Cisco. Стоит отметить следующий факт: в 2013 г. у коммутатора C2960 закончился жизненный цикл (коммутатор достаточно старый), но он продолжает использоваться и конкурировать с новыми моделями, т. к. отлично зарекомендовал себя, в свое время как ZES-2028G является современным коммутатором.

Таблица 2 – Сравнение маршрутизаторов Cisco и Zelax

Характеристика	Cisco 3945	Zelax-ST MM-1017
Гибридный маршрутизатор-коммутатор	Нет	Да
Количество портов	1 Гбит\с RJ45– 3 шт.	1 Гбит\с RJ45 – 20 шт.
SFP порты	2	4
Осовные протоколы маршрутизации	Есть, в том число проприетарный EIGRP	Есть
Сертификат ФСТЭК	Да	Да

Окончание таблицы 2

Характеристика	Cisco 3945	Zelax-ST MM-1017
Шифрование в соответствии с ГОСТ 28147-89	По умолчанию – нет (возможна покупка плат расширения)	Да
VPN	Да	Да
QoS	Да	Да
Наличие основных протоколов L3	Да	Да
Наличие проприетарных протоколов	Да	Нет

Современный маршрутизатор Zelax-ST MM-1017 представляется из себя гибридный маршрутизатор-коммутатор, с шифрование в соответствии с ГОСТ 28147-89. В свою очередь маршрутизатор Cisco 3945 является классическим маршрутизатором с небольшим количеством портов, но с четкой ролью и наличием проприетарных протоколов. По умолчанию маршрутизатор Cisco 3945 не использует стойкое шифрование в соответствии с ГОСТ 28147-89, не нарушая постановления РФ можно использовать лишь шифрование DES, но при желании возможно приобретение плат расширения с алгоритмами шифрования соответствующими ГОСТ 28147-89. EoL серии маршрутизаторов Cisco 3900 анонсирована в 2012г.

Резюмируя главу, можно сказать, что Российский производитель Zelax не сильно уступает передовому производителю сетевого оборудования Cisco. У каждого решения есть свои плюсы и минусы.

3 РЕАЛИЗАЦИЯ СЕТЕВОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

3.1 Аудит КСПД предприятия

Прежде чем приступать к внедрению сетевой безопасности предприятия, следует провести аудит КСПД этого предприятия. В ходе аудита будет исследована структура КСПД, сетевое оборудование, которое используется на предприятии, какие сетевые протоколы применяются, степень их защищенности от распространенных атак.

Предприятие является филиалом, с территориально-распределенной КСПД. Филиал имеет один центральный офис в г. Тюмень и порядка 20 удаленных офисов (на территории Тюменской области, ХМАО и ЯНАО). Сетевое оборудование используемое на предприятии: коммутаторы Cisco C2960, C3750, C3550; маршрутизаторы Cisco 3945, 2801, 2811. Отдельного программно-аппаратного комплекса межсетевого экрана нет.

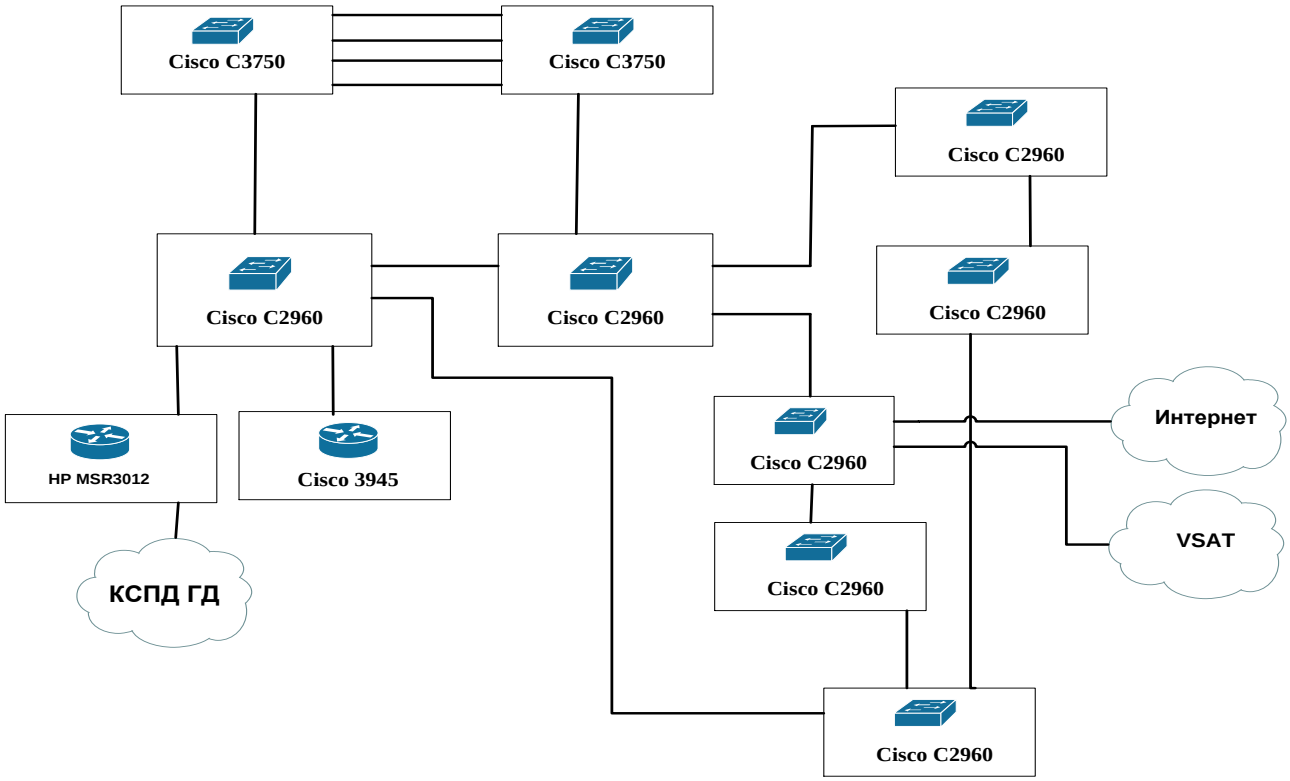

Рисунок 12 – L2 схема КСПД предприятия

Удаленные офисы подключены к КСПД с помощью GRE-туннеля, поверх публичной сети интернет, т. е. шифрование между удаленным офисом и главным офисов отсутствует.

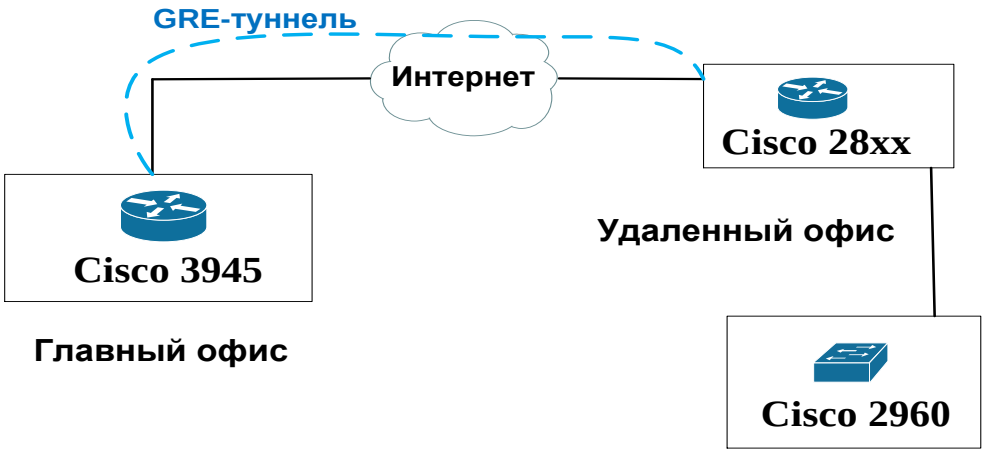

Рисунок 13 – Типовая схема подключения удаленных офисов

Как правило, L2 схема подключения в удаленных офисах состоит из одного маршрутизатора Cisco 2801 или Cisco 2811 и коммутатора Cisco 2960 (24- или 48-портового). Все информационные ресурсы предприятия (например, 1С бухгалтерия предприятия 8, СЭД, IP-телефония и т. п.) расположены в главном офисе, для этого и необходимы GRE-туннели между главным офисом и удаленными.

Филиал насчитывает более 60 сетевых устройств, управление которыми осуществляется с использованием протокола telnet (локальная режим AAA), мониторинг с помощью протокола SNMPv2. В КСПД используется протокол динамической маршрутизации EIGRP, без аутентификации. На интересах маршрутизаторов, граничащих с провайдером интернета используются ACL (которые выполняют роль межсетевого экрана, разделяющего оборудование провайдера и КСПД филиала). На предприятии используется Wi-Fi точки доступа Ubiquiti Unifi AP.

На филиал генеральной дирекцией была выделена подсеть 10.172.0.0/16. Ресурсы генеральной (электронная почта, сервисы 1С, helpdesk и т. д.) дирекции используют подсеть 172.16.0.0/12.

Сотрудниками IT-отдела были замечены посторонние сетевые устройства, на которых часто бывает включен DHCP. Пользовательские ПК иногда получали IP-адреса по протоколу DHCP от этих сетевых устройств, хотя на предприятии организован свой домен-контроллер с DHCP сервером. Никаких руководящих документов о сетевой безопасности в филиале нет, но есть некоторые пожелания руководящего состава. Эти пожелания включат в себя: обеспечение приемлемого уровня сетевой и информационной безопасности; ограничение доступа к некоторым ресурсам большинства пользователей КСПД; ограничение доступа Wi-Fi пользователей к ресурсам филиала и ГД.

3.2 Постановка задачи

В филиале нет никаких документов связанных с политикой безопасности (сетевой), а также составление руководящих документов выходит за рамки ВКР – следует реализовывать сетевую безопасность, учитывая пожелания руководства, использовать распространенные «лучшие практики», закрывать «дыры» безопасности. Сетевая безопасность будет реализовываться изменением конфигурационных файлов сетевых устройств Cisco. Следует учитывать, что руководство филиала выделило сервера, которые можно будет использовать при необходимости.

Задачи заключаются в обеспечении сетевой безопасности:

– Плоскости управления.

– Плоскости контроля.

– Плоскости данных.

– 2 и 3 уровней по модели OSI.

– Виртуальной частной сети филиала (GRE-туннелей между офисами).

– Некоторых информационных сервисов.

3.3 Внедрение сетевой безопасности

Для обеспечения приемлемого уровня безопасности в разрезе плоскости управления, учитывая, что в филиале используется достаточно много сетевых устройств (производителя Cisco) следует использовать внешний, централизованный сервер для AAA, следовательно организовать TACACS+, а также настроить SSH и использовать его вместо протокола telnet.

У компании Cisco есть надежное решение для AAA – Access Control Server (ACS). Следует использовать его. ACS может устанавливаться как физический сервер, так и на виртуальной машину. Установка достаточно простая, поэтому описываться не будет, необходимо просто задать пароль для ACS и IP-адрес. Настройка ACS описана ниже.

В первую очередь создаются клиенты AAA (сетевые устройства), затем группы пользователей и пользователи, далее устанавливаются политики (т. е. какой уровень доступа имеют пользователи).

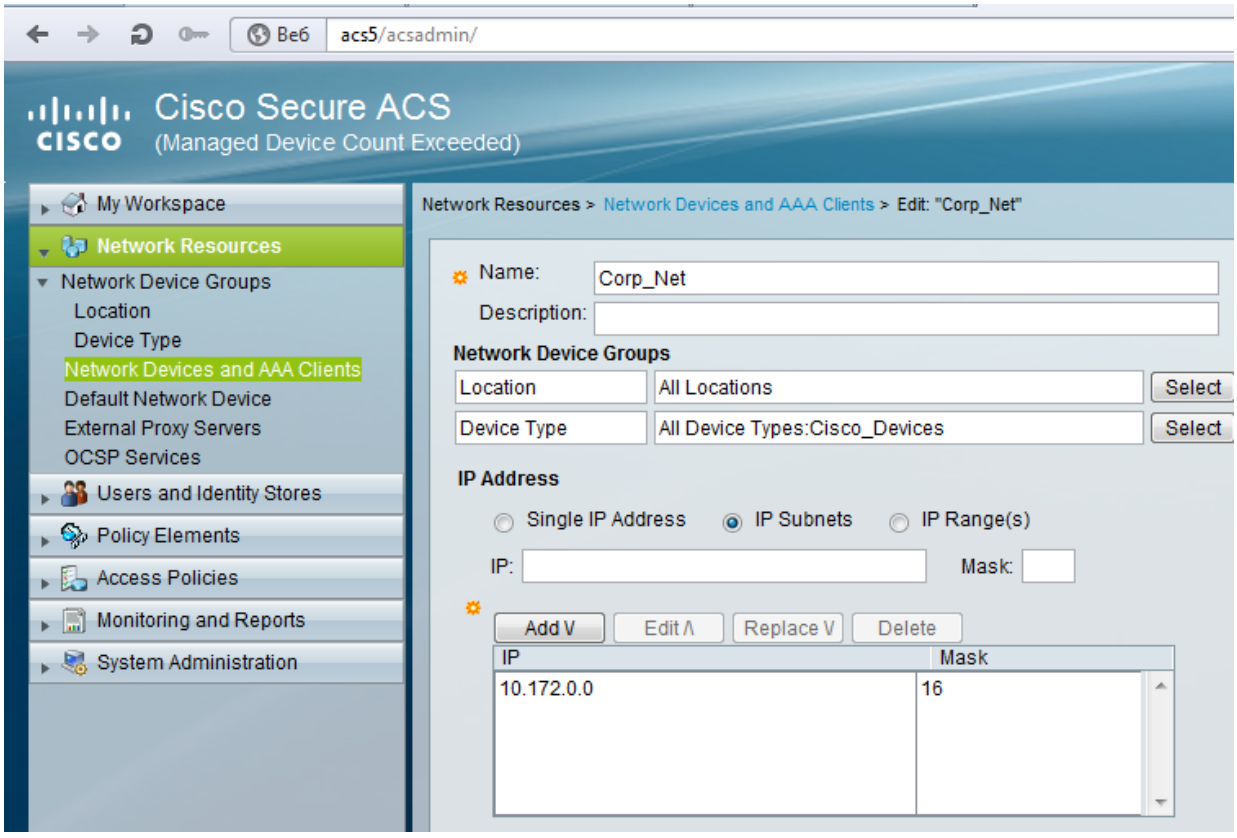

Рисунок 14 – Сетевые устройства и клиенты AAA

Следует обратить внимание на ограничение диапазона IP-адресов, клиентов AAA. Протокол с помощью которого будет производится AAA – TACACS+ (также необходимо указать shared secret).

Т. к. администраторов сетевых устройств немного, то хватит и одной группы (которой в дальнейшем будет присвоены максимальные права).

Рисунок 15 – Группы ACS

Далее необходимо создать пользователей и связать их с группой администраторов.

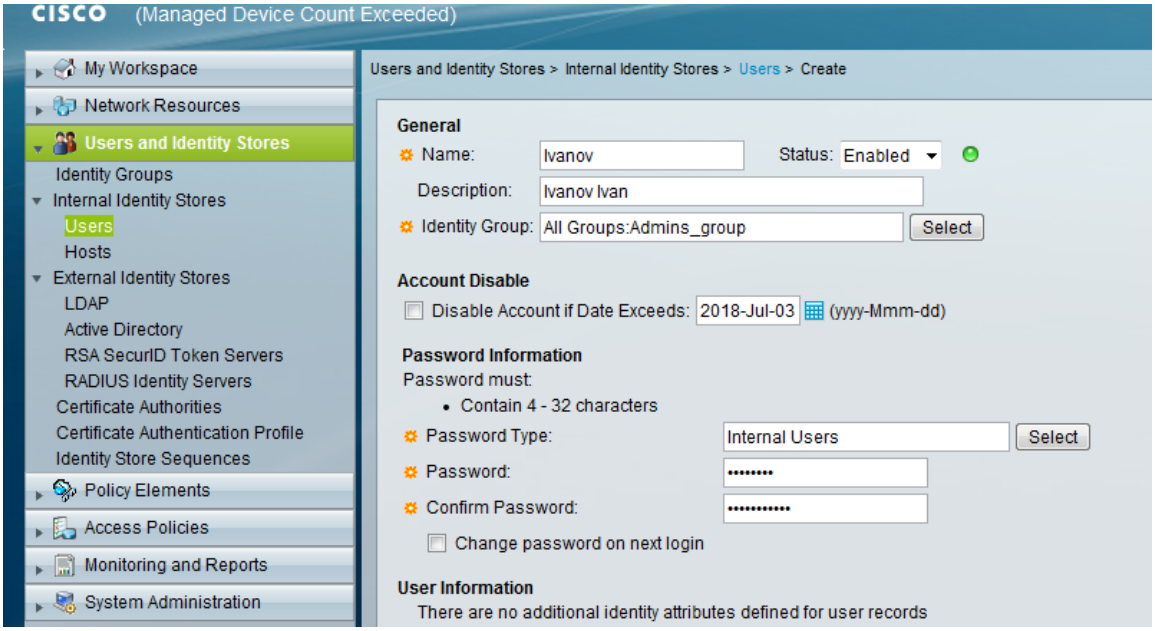

Рисунок 16 – Добавление пользователя

Потом необходимо определить элементы политики (уровни доступа) и политики доступа. Политики представляют собой список правил, которые обрабатываются в порядке нумерации. В ACS есть возможность сделать

несколько разных списков правил, например для Device Administration и для Wireless network access, эти списки называются Access Services. Access Service – это есть некая административная единица, которая в свою очередь в себя включает собственно политики. Service selection rules – определяют в каких случаях какой Access Service будет выбран.

Рисунок 17 – Настройка правил соответствия полномочий пользователю

Заключительным этапом является настройка работы каждого сетевого устройства в связке с ACS. Для этого в конфигурации устройств (с помощью CLI) прописываются следующие строки:

```
tacacs-server host 10.172.8.15 key <shared_key>
tacacs-server directed-request
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
```

Следует обратить внимание, что уже был настроен аккаунт с полными привилегиями (при локальной аутентификации), который будет использоваться при отсутствии доступа к TACACS+. После ввода в эксплуатацию ACS5 и настройки сетевых устройств, в средстве мониторинга и отчетов ACS можно увидеть, что на оборудование постоянно пытаются зайти по протоколу telnet (и ssh) неавторизованные пользователи.

Reload

✔=Pass ✖=Fail =Click for details

ACS View Timestamp	ACS Timestmap	Status	Details	Failure Reason	User Name	Device Name	Network Device Group	Access Service
May 8,18 12:54:18.630 PM	May 8,18 12:54:18.556 PM	✖		22056 Subject not found in the applicable identity store(s).	telecomadmin	Corp_Net	Device Type:All Device Types:Cisco_Devices, Location:All Locations	MyService
May 8,18 12:54:18.626 PM	May 8,18 12:54:18.553 PM	✖		22056 Subject not found in the applicable identity store(s).	telecomadmin	Corp_Net	Device Type:All Device Types:Cisco_Devices, Location:All Locations	MyService
May 8,18 12:54:18.566 PM	May 8,18 12:54:18.546 PM	✖		22056 Subject not found in the applicable identity store(s).	telecomadmin	Corp_Net	Device Type:All Device Types:Cisco_Devices, Location:All Locations	MyService
May 8,18 12:29:49.633 PM	May 8,18 12:29:49.630 PM	✔			[redacted]	Corp_Net	Device Type:All Device Types:Cisco_Devices, Location:All Locations	MyService

Рисунок 18 – Отчет по TACACS+ AAA

Более детальный отчет по одной из попыток входа представлен ниже. Стоит обратить внимание на IP-адрес, с которого была попытка входа, под каким именем и на какое устройство.

AAA Protocol > TACACS+ Authentication Details

Date : May 8, 2018

Generated on May 10, 2018 8:40:17 AM GMT+05:00

Authentication Details	
Status:	Failed
Failure Reason:	22056 Subject not found in the applicable identity store(s).
Logged At:	May 8, 2018 12:54 PM
ACS Time:	May 8, 2018 12:54 PM
ACS Instance:	ACS5
Authentication Method:	PAP_ASCII
Authentication Type:	ASCII
Privilege Level:	1
User	
Username:	telecomadmin
Remote Address:	5.188.10.144
Network Device	
Network Device:	Corp_Net
Network Device IP Address:	10.172.[redacted]
Network Device Groups:	Device Type:All Device Types:Cisco_Devices, Location:All Locations
Access Policy	
Access Service:	MyService

Рисунок 19 – Детальный отчет по попытке входа

Чтобы использовать протокол SSH, вместо telnet, необходимо сгенерировать пару ключей по алгоритму RSA, включить SSHv2. Далее разрешить подключение к сетевому устройству только с помощью SSH (также необходимы домен и имя хоста, которые уже были определены). В дополнение ограничим доступ к сетевым устройствам извне (т. е. доступ будет только из КСПД):

```
crypto key generate rsa general-keys modulus 1024
ip ssh version 2
ip access-list extended SSH_Permit
 permit ip 10.172.0.0 0.0.255.255 any
 deny ip any any
line vty 0 4
 access-class SSH_Permit in
 transport input ssh
```

Можно проверить работоспособность SSH

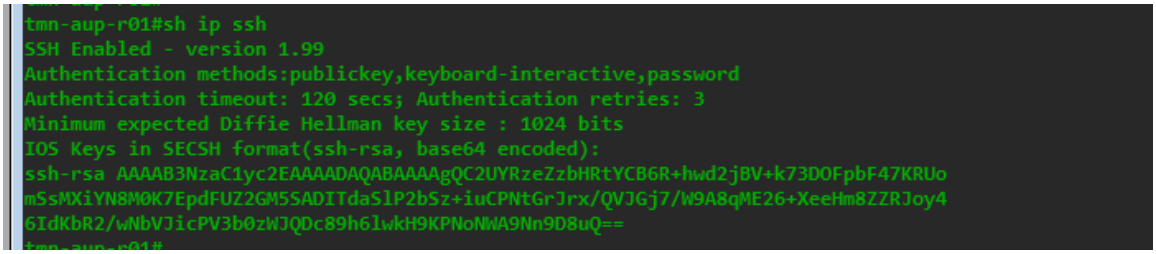

Рисунок 20 – Вывод данных используемого протокола SSH на устройстве

Для обеспечения безопасности плоскости контроля сетевых устройств необходимо настроить аутентификацию протокола динамической маршрутизации EIGRP. Для этого необходимо (на каждом сетевом устройстве) создать единый ключ, включить аутентификацию EIGRP с помощью этого ключа, определить хэш-алгоритм на интерфейсе. Т. к. на предприятии используются GRE туннели, то необходимо настроить каждый туннельный интерфейс:

```
key chain EIGRP-Keys
 key 1
  key-string ParolDlyaEIGRP
interface Tunnel<number>
 ip authentication mode eigrp 107 md5
 ip authentication key-chain eigrp 107  EIGRP-Keys
```

Следует обратить внимание на то, что филиал имеет более 20 удаленных точек, подключенных к главному офису через публичную сеть интернет, с использованием GRE-туннели. GRE (Generic Routing Encapsulation) не предоставляет аутентификации и шифрования инкапсулируемого траффика, т. е.

любой хоп по маршруту следования траффика перехватить конфиденциальные данные. Чтобы исправить огромную брешь в безопасности следует использовать протокол IPsec VPN. Для этого необходимо настроить isakmp, определить ключ для каждого туннеля, сконфигурировать transform-set, создать ipsec profile, назначить на каждом туннельном интерфейсе режим ipsec и ipsec профайл:

```
crypto isakmp policy 1
  encr 3des
  hash md5
  authentication pre-share
  group 2
crypto isakmp key GS#FDGsdgsdvsd34q3KK address <peer_ip-address>
crypto ipsec transform-set 3DES-MD5 esp-3des esp-md5-hmac
  mode tunnel
crypto ipsec profile Tunnel
  set transform-set 3DES-MD5
interface Tunnel<number>
  tunnel mode ipsec ipv4
  tunnel destination <peer_ip>
  tunnel path-mtu-discovery
  tunnel protection ipsec profile Tunnel
```

Теперь весть траффик между удаленными офисами и главным офисом шифруется. IPsec-туннели потребляют больше ресурсов CPU, чем GRE, это связанно со сложностью протоколов хэширования и шифрования. Если ресурсов отдельных устройств не хватает для обработки всех пакетов туннеля, возможно уменьшить стойкость шифрования (изменив политику isakmp и transform-set). На рисунке ниже представлены данные по интерфейсу tunnel 1, как видно используется туннельный протокол IPsec и профиль-защиты Tunnel.

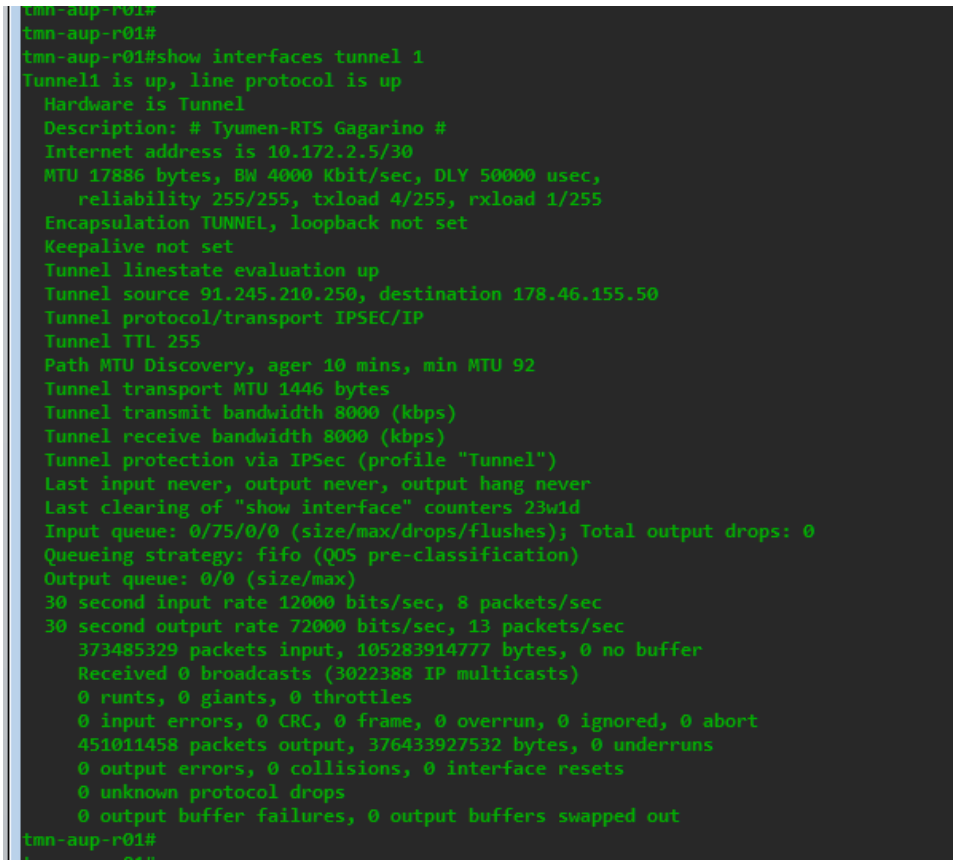

Рисунок 21 – Данные по интерфейсу tunnel 1

Организации IPsec VPN состоит из двух фаз. Сетевые устройства согласуют методы шифрования, хэширования, времени жизни, аутентификации, transform-set, траффик подлежащий шифрования (так называемая криптокарта, в данном примере создается динамически). В первой фазе создается шифрованный SA (Security Associations) для передачи ключа через не доверенные сети, вторая фаза завершается установкой двух IPsec SA (в обоих направлениях). На рисунке ниже представлены данные по IPsec SA одного из туннелей. Установились два IPsec SA (с определенным transorm-set), а также происходит инкапсулирование с шифрование (и деинкапсулирование с дешифрованием), из чего следует успешная работа IPsec VPN.

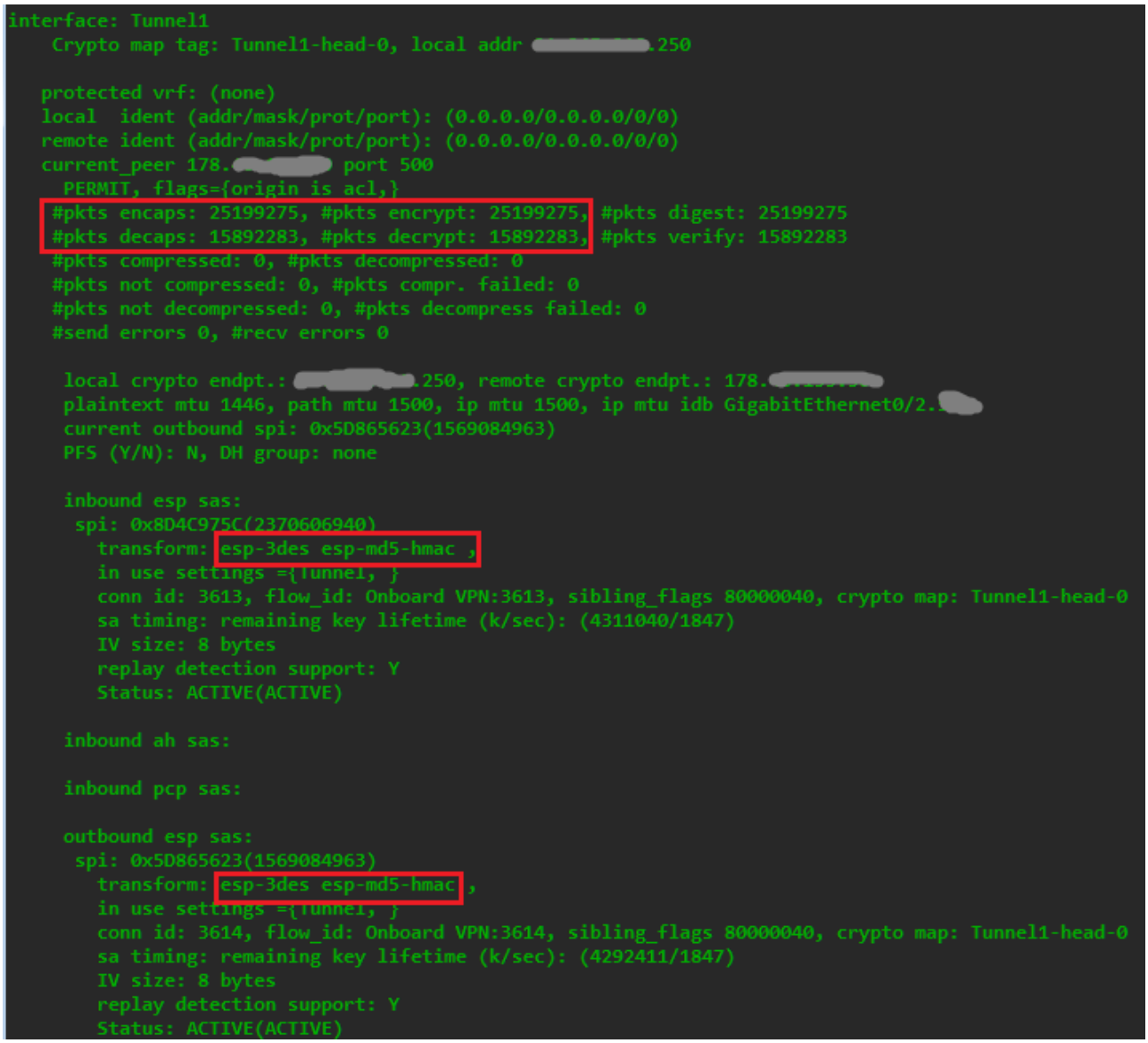

Рисунок 22 – Данные по Tunnel1 IPsec SA

Для того чтобы исключить использование посторонних сетевых устройств, от сторонних DHCP серверов – необходимо обеспечить сетевую безопасность 2 и 3 уровня по модели OSI. Для этого следует внедрить port security, dhcp snooping, dynamic arp inspection. Т. к. в филиале более 200 пользовательских ПК, почти на каждом рабочем месте используется ip-телефоны Cisco, использование статических MAC-адресов в port security будет достаточно проблематичным. Поэтому необходимо использовать динамическое запоминание MAC-адресов в количестве 2 шт. (пользовательский ПК и ip-телефон). Произведем настройку port-security на каждом коммутаторе, использовав режим shutdown (это означает,

что если на порту появляется больше количество MAC-адресов, чем задано – порт отключается и администратор узнает о нарушении безопасности):

```
interface <название_пользовательского_access_порта>
switchport port-security maximum 2
switchport port-security violation shutdown
switchport port-security mac-address sticky
switchport port-security aging time 120
switchport port-security
```

Следует учесть, что при нарушении безопасности порта, следовательно его отключении (error-disabled state) – администраторы должны будут зайти на сетевое устройство и включить порт.

Для борьбы с нелегитимными DHCP-серверами (если такие вдруг появятся) используется dhcp snooping. На каждом коммутаторе следует настроить dhcp snooping, не забывая помечать транковые порты соединящие коммутаторы и маршрутизатор, пример конфигурации для одного из коммутаторов описан ниже. Коммутатор 48 портовый (48 пользовательских портов и 4 SFP), интерфейсы gigabitethernet 0/1 и 0/2 подключены к другим коммутаторам:

```
ip dhcp snooping
ip dhcp snooping vlan 8-35
ip dhcp snooping database flash:/dhcpsnoop
interface range gi0/1 – 2
  ip dhcp snooping trust
interface range fa0/1 – 48
  ip dhcp snooping limit rate 10
```

Интерфейсы gi0/1 и gi0/2 помечены как trusted, соответственно только эти интерфейсы могут принимать DHCP Offer, если же данный пакет придет на другие интерфейсы он будет отброшен. Чтобы при выключении питания сохранить БД DHCP snooping – используется файл на флеш памяти.

Для предотвращения ARP-poisoning атак необходимо использовать DAI, эта технология хорошо сочетается с dhcp snooping, который уже настроен (DAI будет проверять соответствие MAC-to-IP используя БД dhcp snooping). На всех

коммутаторах следует включить функции ARP для соответствующих вланов, при этом настроить «доверие» на транковых портах:

```
ip arp inspection vlan 8-35
interfrace range gi0/1 – 2
 ip arp inspection trust
```

На соответствующих транковых портах DAI не будет проверять соответствие MAC-to-IP, что сэкономит ресурсы устройства.

В лучших практиках написано, что необходимо использовать баннеры, поэтому следует обезопасить предприятие с юридической точки зрения и внедрить баннеры на каждое сетевое устройство. Желательно написать, кому принадлежит данное сетевое устройство, а также, что все действия записываются и доступ неавторизованных пользователей запрещен.

```
tmn-aup-r01#show banner motd
##############################################################################
YOU ARE ACCESSING A RESTRICTED SYSTEM! This it a property of RTRS corporation.
Disconnect IMMIDIATELY if you are not an authorized user! All actions are monitoring and recording!
```

Рисунок 23 – Баннер на сетевых устройствах предприятия

В филиале используются корпоративный Wi-Fi. Он состоит из нескольких точек доступа Ubiquiti Unifi AP. Для пользователей Wi-Fi шлюзом выступает один из сабъинтерфейсов маршрутизатора. На данном сабъинтерфейсе нет списков доступа следовательно пользователи могут свободно получить доступ к любым информационным ресурсам филиала и КСПД. Данное положение вещей руководство филиала не устраивает, устройствам, использующим Wi-Fi необходимо оставить доступ в интернет, и доступ к корпоративной электронной почте, все остальные сервисы запретить. Данная задача решает списки доступа, которые следует повесить на сабъинтерфейс маршрутизатора, выступающий шлюзом для беспроводной сети:

```
ip access-list extended Ban_Wi-Fi_to_CorpNetwork
  permit tcp any host 10.172.8.65 established
  permit tcp any host 10.172.8.65 eq 8080
  permit udp any 10.172.8.48 0.0.0.3 eq domain
```

```
 permit udp any 10.172.8.48 0.0.0.3 eq bootps
 permit udp any 10.172.8.48 0.0.0.3 eq bootpc
 permit icmp any 10.172.0.0 0.0.255.255
 permit tcp 10.172.38.0 0.0.0.255 host 172.31.42.25 eq smtp
 permit tcp 10.172.38.0 0.0.0.255 host 172.31.42.20 eq smtp
 deny   ip any 10.0.0.0 0.255.255.255
 deny   ip any 192.168.0.0 0.0.255.255
 deny   ip any 172.16.0.0 0.15.255.255
 permit ip any any
interface Gi0/2.38
 ip access-group Ban_Wi-Fi_to_CorpNetwork in
```

Списки доступа имеют направление, в котором они будут работать, в данном случае направление входящее. Списки доступа имеют некоторое количество строк, маршрутизатор анализирует пакет на соответствие строкам списка доступа сверху вниз, при соответствии производится определенное действие, если пакет не соответствовал ни одной строке, то пакет отбрасывается. В самом списке доступа в начале разрешается взаимодействие с сервером-контроллером точек доступа Ubiquiti, далее разрешаются DHCP запросы на домен-контроллеры, следом разрешается доступ по протоколу smtp до серверов корпоративной почты, затем блокируются любые пакеты на частные сети (КСПД), в конце разрешаются все остальные ip пакеты. Ниже представлено количество совпадений по данному списку доступа.

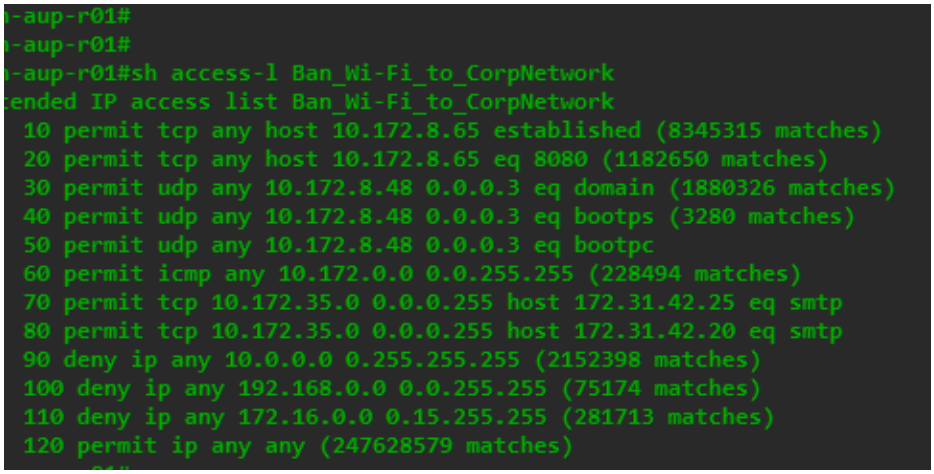

Рисунок 24 – Информация по списку доступа Ban_Wi-Fi_to_CorpNetwork

Обеспечение защиты data plane и некоторых информационных сервисов может заключается в ограничении доступа к определенным БД, серверам, устройствам. В этом случае опять же следует использовать списки доступа. Списками доступа также определяются хосты, траффик, которых следует преобразовать, используя NAT (Network Address Translation).

В КСПД используются сплайсеры (устройства для врезки рекламы в цифровое вещание). К ним также следует ограничить доступ, только IP адреса администраторов должны иметь к ним доступ, а также сервера генеральной дирекции, с которых скачивается необходимый контент для врезки. Для достижения этой цели необходимо составить следующий список доступа и повесить его на интерфейс, выступающий шлюзом для спайсеров в направлении входа:

```
ip access-list extended Splicers
  permit ip any host 10.172.32.197
  permit ip any host 10.172.32.196
  permit ip any host 10.172.8.199
  permit ip any host 172.30.1.253
  permit ip any host 172.30.1.254
  permit ip any 172.31.69.0 0.0.0.255
  permit ip any 172.31.59.0 0.0.0.255
  permit ip any 172.31.197.0 0.0.0.255
  permit ip any 172.31.201.0 0.0.3.255
```

ЗАКЛЮЧЕНИЕ

В рамках выпускной квалификационной работы были реализованы различные аспекты сетевой безопасности на программно-аппаратных решениях компании Cisco.

До внедрения на предприятие различных протоколов и технологий сетевой безопасности, конфиденциальные данные предприятия могли быть перехвачены и использованы в корыстных целях злоумышленников. Также были введены некоторые протоколы, устраняющие бреши в сетевой безопасности (например аутентификация протоколов динамической маршрутизации, DAI, portsecurity). В рамках данной ВКР была не полностью защищена плоскость контроля (не настроены политики для control plane) и плоскость управления (не настроен протокол SNMPv3), а также не были составлены руководящие документы политики безопасности. Следует учесть, что сетевую и информационную безопасность возможно улучшать практически бесконечно (закрывая различные бреши в безопасности, уязвимости протоколов и операционных систем устройств). Если на предприятии не предусмотрены конкретные ставки, занимающиеся лишь информационной и сетевой безопасностью, совершенствование последней может быть крайне проблематично. Вследствие чего предприятие может понести огромные финансовые потери, при нарушении безопасности и утечке конфиденциальных данных.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Анкудинов, Г.И. Сети ЭВМ и телекоммуникации / Г.И. Анкудинов. – Спб.: СЗТУ, 2009. – 92 с.

2 Ачилов, Р. Построение защищенных корпоративных сетей / Р. Ачилов. – М.: ДМК-Пресс, 2012. – 250 с.

3 Блам, Э. Сеть. Как устроен и как работает Интернет / Э. Блам. – М.: АСТ, 2014. – 320 с.

4 Борисенко, А.А. Локальная сеть / А.А. Борисенко. – М.: Эксмо, 2005. – 160 с.

5 Ваняшин, С.А. Сети следующего поколения NGN / С.А. Ваняшин. – М.: Эко-Трендз, 2008. – 424 с.

6 Васин, Н.Н. Основы сетевых технологий на базе коммутаторов и маршрутизаторов / Н.Н. Васин. – М.: Бином, 2011. – 272 с.

7 Ватаманюк, А.И. Создание, обслуживание и администрирование сетей / А.И. Ватаманюк. – СПб.: Питер, 2010. – 288 с.

8 Гольдштейн, Б.С. Сети связи / Б.С. Гольдштейн. – СПб.: БХВ-Петербург, 2010. – 400 с.

9 Гольдштейн, Б.С. Сети связи пост-NGN / Б.С. Гольдштейн. – СПб.: БХВ-Петербург, 2013. – 356 с.

10 Гулевич, Д.С. Сети связи следующего поколения / Д.С. Гулевич. – М.: Бином, 2014. – 242 с.

11 Иртегов, Д.В. Введение в сетевые технологии / Д.В. Иртегов. – СПб.: БХВ-Петербург, 2004. – 176 с.

12 Кенин, А.М. Практическое руководство системного администратора / А.М. Кенин. – СПб.: БХВ-Петербург, 2012. – 314 с.

13 Киселев, С.В. Основы сетевых технологий / С.В. Киселев. – М.: Академия, 2012. – 274 с.

14 Клименко, С.Ю. Компьютерная сеть за один день / С.Ю. Клименко. – М.: Вильямс, 2008. – 148 с.

15 Кузин, А.В. Компьютерные сети / А.В. Кузин. – М.: Инфра-М, 2016. – 167 с.

16 Кузьменко, Н.Г. Компьютерные сети и сетевые технологии / Н.Г. Кузьменко. – СПб.: Наука и техника, 2013. – 202 с.

17 Куроуз, Дж. Ф. Компьютерные сети. Нисходящий подход / Дж.Ф. Куроуз, Кит В. Росс. – М.: Эксмо, 2016. – 296 с.

18 Леммл, Т. CCNP. Маршрутизация. Учебное руководство / Т. Леммл. – М.: Лори, 2015. – 85 с.

19 Ломовицкий, В.В. Основы построения систем и сетей передачи информации / В.В. Ломовицкий, А.И. Михайлов. – М.: Горячая линия-Телеком, 2005. – 336 с.

20 Максимов, Н.В. Компьютерные сети / Н.В. Максимов, И.И. Попов. – М.: Инфра-М, 2013. – 191 с.

21 Мелехин, В.Ф. Вычислительные машины, системы и сети / В.Ф. Мелехин, Е.Г. Павловский. – М.: Академия, 2010. – 326 с.

22 Мельников, Д.А. Системы и сети передачи данных. Учебник / Д.А. Мельников. – М.: РадиоСофт, 2015. – 149 с.

23 Новожилов, Е.О. Компьютерные сети / Е.О. Новожилов. – М.: Академия, 2011. – 238 с.

24 Олифер, В.Г. Безопасность компьютерных сетей / В.Г. Олифер. – Спб.: Питер, 2015. – 644 с.

25 Поляк-Брагинский, А.В. Администрирование сети на примерах / А.В. Поляк-Брагинский. – СПб.: БХВ-Питер, 2010. – 184 с.

26 Поляк-Брагинский, А.В. Локальная сеть. Самое необходимое / А.В. Поляк-Брагинский. – СПб.: БХВ-Питер, 2011. – 124 с.

27 Ручкин, В.Н. Архитектура компьютерных сетей / В.Н. Ручкин, В.А. Фулин. – М.: Диалог-МИФИ, 2008. – 116 с.

28 Самарский, П.А. Основы структурированных кабельных систем / П.А. Самарский. – М.: ДМК Пресс, 2005. – 216 с.

29 Сахнин, А.А. Информационно-телекоммуникационные сети. Технологии. Стандартизация / А.А. Сахнин. – М.: Радиотехника, 2012. – 273 с.

30 Семенов, А.Б. Волоконно-оптические подсистемы современных СКС / А.Б. Семенов. – М.: ДМК Пресс, 2007. – 269 с.

31 Семенов, Ю.А. Алгоритмы телекоммуникационных сетей / Ю.А. Семенов. – М.: Бином, 2007. – 292 с.

32 Сергеев, А.Н. Основы локальных компьютерных сетей. Учебное пособие / А.Н. Сергеев. – СПб.: Лань, 2016. – 137 с.

33 Смирнов, И.Г. Структурированные кабельные системы – проектирование, монтаж и сертификация / И.Г. Смирнов. – М.: Экон-Информ, 2005. – 482 с.

34 Смирнова, Е.В. Технология коммутации и маршрутизации в локальных компьютерных сетях. Учебное пособие / Е.В. Смирнова, А.В. Пролетарский. – М.: МГТУ им. Н. Э. Баумана, 2013. – 186 с.

35 Смирнова, Е.В. Построение коммутируемых компьютерных сетей / Е.В. Смирнова, А.В. Пролетарский. – М.: НОУ «Интуит», 2016. – 174 с.

36 Смирнова, Е.В. Технологии современных сетей Ethernet. Методы коммутации и управления потоками данных / Е.В. Смирнова, П.В. Козик. – СПб.: БХВ-Петербург, 2012. – 272 с.

37 Степанов, А.Н. Информатика. Базовый курс: учебник / А.Н. Степанов. – СПб.: Питер, 2010. – 720 с.

38 Соболь, Б.В. Сети и телекоммуникации. Учебное пособие / Б.В. Соболь, А.А. Манин. – Ростов-на-Дону: Феникс, 2015. – 192 с.

39 Таненбаум, Э. Компьютерные сети / Э. Таненбаум. – СПб.: Питер, 2016. – 992 с.

40 Фейт, С. TCP / IP. Архитектура. Протоколы. Реализация / С. Фейт. – М.: Лори, 2014. – 424 с.

41 Чекмарев, Ю.С. Локальные вычислительные сети. Учебное пособие / Ю.С. Чекмарев. – М.: ДМК Пресс, 2009. – 200 с.