Министерство образования и науки РФ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Уральский государственный педагогический университет»
Институт математики, информатики и информационных технологий
Кафедра информационно-коммуникационных технологий в образовании

СИСТЕМА ФИЛЬТРАЦИИ ТРАФИКА В КОМПЬЮТЕРНОЙ СЕТИ ОРГАНИЗАЦИИ

Выпускная квалификационная работа бакалавра по направлению подготовки 09.03.02 – Информационные системы и технологии

Исполнитель: студент группы БС-41
ИМИ и ИТ
Гудюшкина А.А.

Руководитель: к.п.н., доцент кафедры ИКТО
Стариченко Е.Б.

Работа допущена к защите
« 12 » мая 2016 г.
Зав. кафедрой _____

Екатеринбург – 2016

Реферат

Гудюшкина А.А. СИСТЕМА ФИЛЬТРАЦИИ ТРАФИКА В КОМПЬЮТЕРНОЙ СЕТИ ОРГАНИЗАЦИИ, выпускная квалификационная работа: 42 стр., рис. 1, табл. 1, библ. 30 назв.

Ключевые слова: фильтрация трафика, компьютерная сеть, Cisco Packet Tracer.

Объект разработки – система фильтрация трафика компьютерной сети организации.

Цель работы – разработка системы фильтрации трафика, обеспечивающей разграничение доступа разных групп пользователей к внутренним и внешним ресурсам.

В работе описаны результаты проектирования и настройки системы фильтрации трафика для готовой компьютерной сети с помощью средств программного комплекса Cisco Packet Tracer 6.0.

Оглавление

Введение

С появлением сети Интернет произошло множество изменений в жизни людей. Интернет представляет собой хранилище разнообразнейшей информации и сервисов. Часто возникает необходимость ограничения доступа к различным ресурсам сети. Это может быть связано с нерациональным использованием рабочего времени и стремлением работодателя оптимизировать деятельность своих сотрудников, желанием родителей ограничить детей от определённого контента и т.д.

Оптимизация использования сетевых ресурсов находится в списке обязанностей системного администратора. Можно выделить несколько основных проблем, с которыми сталкивается администратор корпоративной сети:

- чрезмерная нагрузка на сеть, вызванная неконтролируемым скачиванием пользователями больших файлов из глобальной сети;
- нерациональное использование ресурсов сети и рабочего времени в результате деятельности любителей онлайн-игр;
- снижение уровня безопасности сети предприятия – именно внутренние ресурсы и данные организации часто становятся объектом угроз и рисков при отсутствии полноценного контроля за посещением сотрудниками сайтов той или иной тематики.

Немаловажной также является проблема заполнения пропускной способности канала сети Интернет.[1]

Исходя из всего вышесказанного, можно увидеть насколько актуальной является проблема фильтрации трафика.

Объект разработки – система фильтрация трафика компьютерной сети организации.

Цель работы – разработка системы фильтрации трафика, обеспечивающей разграничение доступа разных групп пользователей к внутренним и внешним ресурсам.

Задачи:

1. Произвести анализ состояния проблемы и подходов к ее решению.
2. Произвести анализ и обосновать выбор технологий реализации и необходимых программных платформ.
3. В соответствии с техническим заданием провести разработку системы фильтрации трафика.

Глава 1. Фильтрация сетевого трафика, как средство разграничения доступа к ресурсам

1.1 Организация фильтрации сетевого трафика

Фильтрация трафика − основная функция систем межсетевых экранов (или брандмауэров), которая позволяет сетевому администратору распределить пользователям как доступ из внешней сети к службам компьютеров, находящимся внутри сети предприятия, или к защищенному сегменту сети, так и доступ пользователей из внутренней сети к соответствующим ресурсам внешней сети.[1]

Фильтрация обычно осуществляется на четырех уровнях OSI:

1. Канальном (Ethernet).
2. Сетевом (IP).
3. Транспортном (TCP, UDP).
4. Прикладном (FTP, TELNET, HTTP, SMTP и т. д.)

Фильтрация сетевого трафика является основной функцией межсетевых экранов и позволяет администратору безопасности сети централизованно осуществлять необходимую сетевую политику безопасности в выделенном сегменте IP-сети. Настроив соответствующим образом брандмауэр, можно разрешить или запретить пользователям как доступ из внешней сети к соответствующим службам хостов или к хостам, находящихся в защищаемом сегменте, так и доступ пользователей из внутренней сети к соответствующим ресурсам внешней сети. Можно провести аналогию с администратором локальной операционной системы, который для осуществления политики безопасности в системе назначает необходимым образом соответствующие отношения между субъектами (пользователями) и объектами системы (файлами, например), что позволяет разграничить доступ субъектов системы к ее объектам в соответствии с заданными администратором правами доступа. Те же рассуждения применимы к брандмауэр-фильтрации: в качестве субъектов взаимодействия будут выступать

IP-адреса хостов пользователей, а в качестве объектов, доступ к которым необходимо разграничить, - IP-адреса хостов, используемые транспортные протоколы и службы предоставления удаленного доступа.[3]

Многие страны мира решили разрабатывать свои национальные подходы, регулирующие использование Интернета. Подобные попытки имели разную степень успеха, а иногда и неожиданные последствия. Это можно наблюдать в растущем числе стран, в которых в последние годы было принято решение просто ограничить доступ к Интернет-контенту. Кроме того, все большее число стран пытается применять фильтры в Интернете – технический подход к контролю доступа к контенту. Как правило, используется три способа блокировки доступа к веб-сайтам: блокировка по IP-адресам, фильтрация DNS и блокировка URL-адресов с помощью прокси-сервера. Блокировка по ключевым словам, при которой блокируется доступ к веб-сайтам на основе ключевых слов, найденных на запрошенных URL-адресах, или блокировка поиска на основе «черного» списка терминов является более совершенным способом, который применяется во все большем числе стран. Указанные методы можно применять в разных точках, например: у поставщика услуг Интернета, на уровне организации или отдельного устройства, подключенного к Интернету. [20]

Существует множество разных способов фильтрации, все они направлены на ограничение доступа к определенным веб-сайтам. Ряд из них основан на списке «плохих сайтов», который создают поставщики услуг Интернета или органы власти и внедряют на уровне сети, однако родители, преподаватели или другие полномочные органы также имеют доступ к программам и инструментам, способным осуществлять мониторинг, отслеживать и блокировать доступ к определенным действиям в Интернете на устройствах, используемых их детьми; например:

- прокси-серверы и программы, разрешающие или блокирующие доступ к определенным сайтам и протоколам (включая защиту от вирусов, фильтры нежелательной электронной почты, блокировка

всплывающих окон, антишпионские программы, программы для удаления файлов «cookie» и т. д.);

- программы для фильтрации контента, которые находят и блокируют определенный контент или веб-сайты;
- параметры конфигурации, которые задают уровень конфиденциальности и мониторинга сайтов (например, фильтр Google SafeSearch, Privolock).

Однако фильтрация не может быть эффективной на 100%. Технологии фильтрации часто склонны к двум характерным недостаткам: недостаточная и избыточная блокировка. Под недостаточной блокировкой понимается неспособность заблокировать доступ ко всему целевому контенту. С другой стороны технологии фильтрации часто блокируют контент, который они не должны блокировать, что называется избыточным блокированием. Оба указанных недостатка появляются вследствие создания множества «черных» списков с использованием сочетания ручных настроек и автоматизированных поисковых систем, которые часто содержат веб-сайты, классифицированные неправильно. Дополнительные проблемы возникают, когда контент размещается под тем же IP-адресом или в том же домене. Более того, методы фильтрации не удаляют незаконное содержимое из Интернета, и их зачастую можно обойти. Они также могут случайным образом ограничить свободное и открытое общение и тем самым ограничить права отдельных людей или групп меньшинств.

Могут высказываться мнения, что фильтрация на уровне сети, например фильтрация DNS, также приводит к нестабильности сети, способствует разобщенности и подрывает основы Интернета. Другие подходы к контролю контента, такие как наложение ареста на имя домена, подвержены большинству тех же проблем, что и при использовании фильтрации DNS, включая простой обход, неспособность решить проблему, которая лежит в основе, а также подталкивание к созданию теневой сети, которая будет недоступной для правоохранительных органов.

Несмотря на то, что программы могут блокировать доступ к высокопрофильным веб-сайтам, в настоящее время не существует решения, которое будет неизменно надежным и абсолютно эффективным. Технологии позволяют точно идентифицировать и выделить определенные категории контента, находящегося на миллионах веб-сайтов и в других интернет-приложениях, таких как группы новостей, списки электронной почты, чаты, мгновенные сообщения и социальные сети. В любом случае эти методы не позволяют удалить предосудительный или незаконный контент из Интернета; они только затрудняют к нему доступ.[2]

1.2 Средства и способы фильтрации трафика

1.2.1 Структура IP-пакета

Основу транспортных средств стека протоколов TCP/IP составляет протокол межсетевого взаимодействия (Internet Protocol, *IP*). Он обеспечивает передачу дейтаграмм от отправителя к получателям через объединенную систему компьютерных сетей.

Имеется прямая связь между функциональной сложностью протокола и сложностью заголовка пакетов, которые этот протокол использует. Это объясняется тем, что основные служебные данные, на основании которых протокол выполняет то или иное действие, переносятся между двумя модулями, реализующими этот протокол на разных машинах, именно в полях заголовков пакетов. Поэтому очень полезно изучить назначение каждого поля заголовка IP-пакета, и это изучение дает не только формальные знания о структуре пакета, но и объясняет все основные режимы работы протокола по обработке и передаче IP-дейтаграмм.

IP-пакет состоит из заголовка и поля данных. Заголовок, как правило, имеющий длину 20 байт, имеет следующую структуру (Рисунок 1)

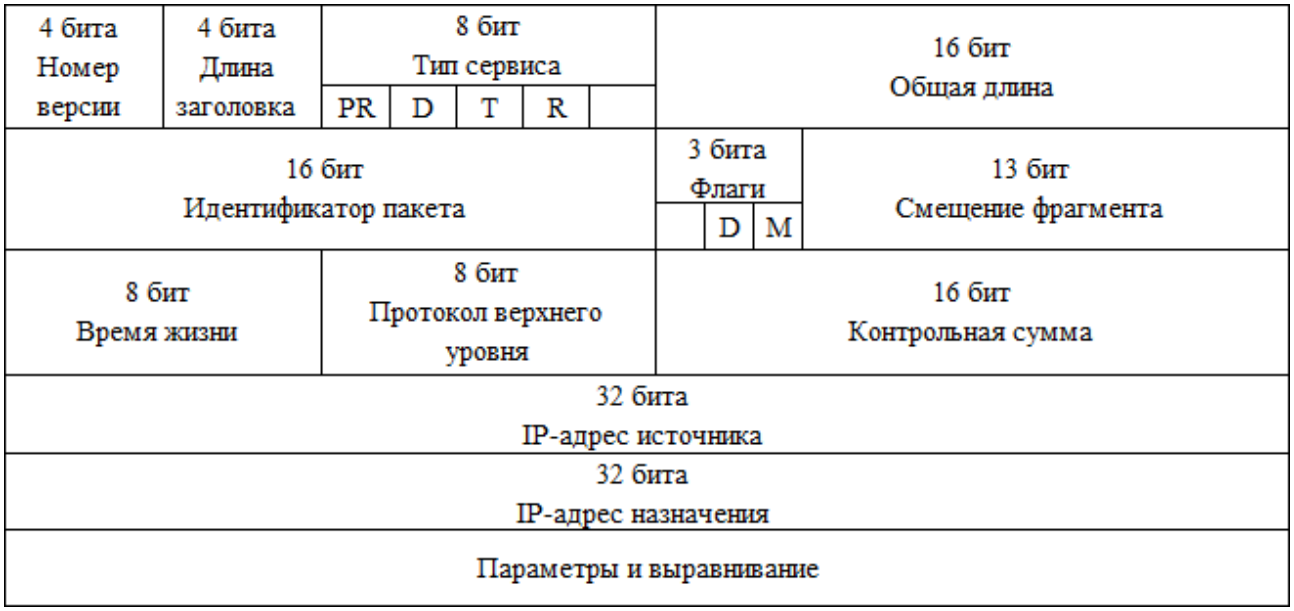

Рисунок 1. Структура заголовка IP-пакета

Поле Номер версии (Version), занимающее 4 бит, указывает версию протокола IP. Сейчас повсеместно используется версия 4 (IPv4) и версия 6 (IPv6).

Поле Длина заголовка (IHL) IP-пакета занимает 4 бит и указывает значение длины заголовка, измеренное в 32-битовых словах. Обычно заголовок имеет длину в 20 байт (пять 32-битовых слов), но при увеличении объема служебной информации эта длина может быть увеличена за счет использования дополнительных байт в поле Опции (IP Options). Наибольший заголовок занимает 60 октетов.

Поле Тип сервиса (Type of Service) занимает один байт и задает приоритетность пакета и вид критерия выбора маршрута. Первые три бита этого поля образуют подполе приоритета пакета (Precedence), Приоритет может иметь значения от самого низкого - 0 (нормальный пакет) до самого высокого - 7 (пакет управляющей информации). Маршрутизаторы и компьютеры могут принимать во внимание приоритет пакета и обрабатывать более важные пакеты в первую очередь. Поле Тип сервиса содержит также три бита, определяющие критерий выбора маршрута. Реально выбор осуществляется между тремя альтернативами: малой задержкой, высокой достоверностью и высокой пропускной способностью. Установленный бит D (delay) говорит о том, что маршрут должен вы-

бираться для минимизации задержки доставки данного пакета, бит T - для максимизации пропускной способности, а бит R - для максимизации надежности доставки. Во многих сетях улучшение одного из этих параметров связано с ухудшением другого, кроме того, обработка каждого из них требует дополнительных вычислительных затрат. Поэтому редко, когда имеет смысл устанавливать одновременно хотя бы два из этих трех критериев выбора маршрута. Зарезервированные биты имеют нулевое значение.

Поле Общая длина (Total Length) занимает 2 байта и означает общую длину пакета с учетом заголовка и поля данных. Максимальная длина пакета ограничена разрядностью поля, определяющего эту величину, и составляет 65 535 байт, однако в большинстве хост-компьютеров и сетей столь большие пакеты не используются.

Поле Идентификатор пакета (Identification) занимает 2 байта и используется для распознавания пакетов, образовавшихся путем фрагментации исходного пакета. Все фрагменты должны иметь одинаковое значение этого поля.

Поле Флаги (Flags) занимает 3 бита и содержит признаки, связанные с фрагментацией. Установленный бит DF (Do not Fragment) запрещает маршрутизатору фрагментировать данный пакет, а установленный бит MF (More Fragments) говорит о том, что данный пакет является промежуточным (не последним) фрагментом. Оставшийся бит зарезервирован.

Поле Смещение фрагмента (Fragment Offset) занимает 13 бит и задает смещение в байтах поля данных этого пакета от начала общего поля данных исходного пакета, подвергнутого фрагментации. Используется при сборке/разборке фрагментов пакетов при передачах их между сетями с различными величинами MTU. Смещение должно быть кратно 8 байт.

Поле Время жизни (Time to Live) занимает один байт и означает предельный срок, в течение которого пакет может перемещаться по сети. Время жизни данного пакета измеряется в секундах и задается источником передачи. На маршрутизаторах и в других узлах сети по истечении каждой секунды из теку-

щего времени жизни вычитается единица; единица вычитается и в том случае, когда время задержки меньше секунды. Поскольку современные маршрутизаторы редко обрабатывают пакет дольше, чем за одну секунду, то время жизни можно считать равным максимальному числу узлов, которые разрешено пройти данному пакету до того, как он достигнет места назначения. Если параметр времени жизни станет нулевым до того, как пакет достигнет получателя, этот пакет будет уничтожен. Время жизни можно рассматривать как часовой механизм самоуничтожения. Значение этого поля изменяется при обработке заголовка IP-пакета.

Идентификатор Протокол верхнего уровня (Protocol) занимает один байт и указывает, какому протоколу верхнего уровня принадлежит информация, размещенная в поле данных пакета (например, это могут быть сегменты протокола TCP, дейтаграммы UDP, пакеты ICMP или OSPF). Значения идентификаторов для различных протоколов приводятся в документе RFC «Assigned Numbers».

Контрольная сумма (Header Checksum) занимает 2 байта и рассчитывается только по заголовку. Поскольку некоторые поля заголовка меняют свое значение в процессе передачи пакета по сети (например, время жизни), контрольная сумма проверяется и повторно рассчитывается при каждой обработке IP-заголовка. Контрольная сумма - 16 бит - подсчитывается как дополнение к сумме всех 16-битовых слов заголовка. При вычислении контрольной суммы значение самого поля «контрольная сумма» устанавливается в нуль. Если контрольная сумма неверна, то пакет будет отброшен, как только ошибка будет обнаружена.

Поля IP-адрес источника (Source IP Address) и IP-адрес назначения (Destination IP Address)имеют одинаковую длину - 32 бита - и одинаковую структуру.

Поле Опции (IP Options) является необязательным и используется обычно только при отладке сети. Механизм опций предоставляет функции управления,

которые необходимы или просто полезны при определенных ситуациях, однако он не нужен при обычных коммуникациях. Это поле состоит из нескольких подполей, каждое из которых может быть одного из восьми предопределенных типов. В этих подполях можно указывать точный маршрут прохождения маршрутизаторов, регистрировать проходимые пакетом маршрутизаторы, помещать данные системы безопасности, а также временные отметки. Так как число подполей может быть произвольным, то в конце поля Опции должно быть добавлено несколько байт для выравнивания заголовка пакета по 32-битной границе.

Поле Выравнивание (Padding) используется для того, чтобы убедиться в том, что IP-заголовок заканчивается на 32-битной границе. Выравнивание осуществляется нулями.[21]

1.2.2 Межсетевые экраны

Межсетевые экраны (брандмауэр, firewall) защищают компьютеры и сети от попыток несанкционированного доступа с использованием уязвимых мест, существующих в семействе протоколов TCP/IP. Дополнительно они помогают решать проблемы безопасности, связанные с использованием уязвимых систем и с наличием большого числа компьютеров в локальной сети. Существует несколько типов брандмауэров, начиная от пакетных фильтров, встроенных в пограничные роутеры, которые могут обеспечивать управление доступом для IP-пакетов, до мощных брандмауэров, которые могут закрывать уязвимости в большом количестве уровней семейства протоколов TCP/IP, и еще более мощных, которые могут фильтровать трафик на основании всего содержимого пакета.

1.2.2.1 Пакетные фильтры

Самый основной, базовый, первоначально разработанный тип брандмауэра называется пакетным фильтром. Пакетные фильтры в основном являются частью устройств роутинга, которые могут управлять доступом на уровне сис-

темных адресов и коммуникационных сессий. Функциональность управления доступом обеспечивается с помощью множества директив, называемых ruleset или rules (правила).

Вначале пакетные фильтры функционировали на уровне 3 модели OSI. Данная функциональность разработана для обеспечения управления сетевым доступом, основываясь на нескольких блоках информации, содержащихся в сетевом пакете. В настоящее время все пакетные фильтры также анализируют и уровень 4.

Пакетные фильтры анализируют следующую информацию, содержащуюся в заголовках пакетов 3-го и 4-го уровней:

- адрес источника пакета, например, адрес уровня 3 системы или устройства, откуда получен исходный сетевой пакет (IP-адрес, такой как 192.168.1.1);
- адрес назначения пакета, например, адрес уровня 3 пакета, который он пытается достигнуть (например, 192.168.1.2);
- тип коммуникационной сессии, т.е. конкретный сетевой протокол, используемый для взаимодействия между системами или устройствами источника и назначения (например, TCP, UDP или ICMP);
- возможно некоторые характеристики коммуникационных сессий уровня 4, такие как порты источника и назначения сессий (например, TCP:80 для порта назначения, обычно принадлежащий web-серверу, TCP:1320 для порта источника, принадлежащий персональному компьютеру, который осуществляет доступ к серверу);
- иногда информацию, относящуюся к интерфейсу роутера, на который пришел пакет, и информацию о том, какому интерфейсу роутера она предназначена; это используется для роутеров с тремя и более сетевыми интерфейсами;

- иногда информацию, характеризующую направление, в котором пакет пересекает интерфейс, т.е. входящий или исходящий пакет для данного интерфейса;
- иногда можно также указать свойства, относящиеся к созданию логов для данного пакета.

Пакетные фильтры обычно размещаются в сетевой инфраструктуре, использующей TCP/IP. Однако они могут также быть размещены в любой сетевой инфраструктуре, которая имеет адресацию уровня 3, например, IPX (Novell NetWare) сети. В современных сетевых инфраструктурах брандмауэры на уровне 2 могут также использоваться для обеспечения балансировки нагрузки в приложениях с высокими требованиями к доступности, в которых два или более брандмауэра используются для увеличения пропускной способности или для выполнения восстановительных операций.

Некоторые пакетные фильтры, встроенные в роутеры, могут также фильтровать сетевой трафик, основываясь на определенных характеристиках этого трафика, для предотвращения DoS- и DDoS-атак.

Пакетные фильтры могут быть реализованы в следующих компонентах сетевой инфраструктуры:

- пограничные роутеры;
- ОС;
- персональные брандмауэры.

1.2.2.2 Прокси-сервер прикладного уровня

Прокси прикладного уровня являются более мощными межсетевыми экранами, которые комбинируют управление доступом на низком уровне с функциональностью более высокого уровня (уровень 7 – Application). При использовании межсетевого экрана прикладного уровня обычно, как и в случае пакетного фильтра не требуется дополнительное устройство для выполнения роутинга: межсетевой экран выполняет его сам. Все сетевые пакеты, которые поступают

на любой из интерфейсов межсетевого экрана, находятся под управлением этого прикладного прокси. Прокси-сервер имеет набор правил управления доступом для определения того, какому трафику может быть разрешено проходить через межсетевой экран.

Аутентификация пользователя может иметь много форм, например такие:

- с помощью User ID и пароля;
- с помощью аппаратного или программного токена;
- по адресу источника;
- биометрическая аутентификация.

Прокси-сервер, который анализирует конкретный протокол прикладного уровня, называется агентом прокси.

1.2.2.3 Выделенные прокси-серверы

Выделенные прокси-серверы отличаются от прикладных прокси в том, что они анализируют трафик только конкретного прикладного протокола и не обладают возможностями анализа всего трафика, что все-таки характерно для межсетевого экрана прикладного уровня. По этой причине они обычно развертываются позади межсетевых экранов прикладного уровня. Типичное использование таково: основной межсетевой экран получает входящий трафик, определяет, какому приложению он предназначен, и затем передает обработку конкретного типа трафика соответствующему выделенному прокси-серверу, например, e-mail прокси серверу. Выделенный прокси-сервер при этом выполняет операции фильтрации и логирования трафика и затем перенаправляет его во внутренние системы. Этот сервер может также принимать исходящий трафик непосредственно от внутренних систем, фильтровать трафик и создавать логи, а затем передавать его межсетевому экрану для последующей доставки. Обычно выделенные прокси-серверы используются для уменьшения нагрузки на межсетевой экран и выполнения более специализированной фильтрации и создания логов.

Как и в случае прикладных прокси, выделенные прокси позволяют выполнить аутентификацию пользователей. В случае использования выделенного прокси легче более точно ограничить исходящий трафик или проверять весь исходящий и входящий трафик, например, на наличие вирусов. Выделенные прокси-серверы могут также помочь в отслеживании внутренних атак или враждебного поведения внутренних пользователей. Фильтрация всего исходящего трафика сильно загружает общий межсетевой экран прикладного уровня и увеличивает стоимость администрирования.

В дополнение к функциям аутентификации и создания логов, выделенные прокси-серверы используются для сканирования web и e-mail содержимого, включая следующие функции:

- фильтрование Java-апплетов или приложений;
- фильтрование управлений ActiveX;
- фильтрование JavaScript;
- блокирование конкретных MIME-типов – например, "application/msword";
- сканирование и удаление вирусов;
- блокирование команд, специфичных для приложения, например, блокирование HTTP-команды PUT;
- блокирование команд, специфичных для пользователя, включая блокирование некоторых типов содержимого для конкретных пользователей.

1.2.3 Реализация набора правил брандмауэра

Большинство реализаций межсетевых экранов используют наборы правил в качестве механизма для реализации управления трафиком. Возможная совокупность этих правил определяет реальную функциональность межсетевого экрана. В зависимости от архитектуры реализации межсетевого экрана набор правил может включать в себя различные блоки информации. Тем не менее все они содержат как минимум следующие поля:

- адрес источника пакета, например, адрес 3 уровня компьютерной системы или устройства, откуда получен сетевой пакет (IP-адрес);
- адрес назначения пакета, например, адрес 3-го уровня компьютерной системы или устройства, куда пакет должен быть доставлен;
- тип трафика, т.е. конкретный сетевой протокол, используемый для взаимодействия систем или устройств источника или получателя, – например, IP на 3-м уровне или TCP и UDP на 4-м уровне;
- возможно, некоторые характеристики коммуникационных сессий 4-го уровня – протокол, такой, как TCP, и порты источника и назначения;
- иногда информация, относящаяся к интерфейсу роутера, с которого пришел пакет, и к интерфейсу роутера, для которого пакет предназначен, – используется для роутеров с тремя и более сетевыми интерфейсами;
- действие, такое как Deny или Block пакета, или Drop пакета, когда пакет отбрасывается и отправителю пакета не возвращается ответ, содержащий информацию о том, что ему запрещена пересылка; либо Allow, Pass или Accept, когда пакет пропускается через межсетевой экран.

Набор правил может быть создан после определения трафика приложений. В зависимости от межсетевого экрана это может выполняться с использованием интерфейса в стиле web; в случае пакетных фильтров набор обычно является текстовым файлом. Набор должен быть создан как можно более конкретно в соответствии с трафиком, который он контролирует. Он должен быть как можно более простым, чтобы случайно не появилось "дырок" в межсетевом экране, которые могут допустить прохождение неавторизованного или нежелательного трафика через межсетевой экран.

По умолчанию политика обработки входящего трафика должна блокировать все пакеты и соединения, за исключением того типа трафика и тех соединений, которые были специально разрешены. Данный подход является более безопасным, чем другой подход, при котором по умолчанию разрешаются все

соединения и весь трафик и затем блокируется конкретный трафик и соединения.

Набор правил межсетевого экрана должен всегда блокировать следующие типы трафика:

- входящий трафик от неаутентифицированного источника с адресом назначения самого межсетевого экрана. Данный тип пакета обычно является некоторым типом зондирования или атакой, направленной на сам межсетевой экран. Одним общим исключением из этого правила может служить случай, когда межсетевой экран обеспечивает доставку входящего e-mail (SMTP на порт 25). Тогда межсетевой экран должен разрешить входящие соединения к самому себе, но только на порт 25;
- входящий трафик из внешней сети с адресом источника, указывающим, что пакет получен из сети, расположенной позади межсетевого экрана. Данный тип пакета обычно представляет собой некоторый тип попыток spoofing'a (подделки);
- входящий трафик, содержащий ICMP-трафик. Так как ICMP может использоваться для определения расположенных позади межсетевого экрана сетей, ICMP не должен передаваться внутрь из Интернета или из любой недоверяемой внешней сети;
- входящий или исходящий трафик от системы, использующей адрес источника из множества диапазонов адресов, которые в соответствии с RFC 1918 зарезервированы для частных сетей.[4]

1.3 Области применения фильтрации трафика

Существует множество областей применения фильтрации трафика.

По масштабу можно разделить их на несколько категорий:

1. Фильтрация на отдельном компьютере.
2. Фильтрация в сети компьютеров предприятия.
3. Фильтрация в масштабах государства.

1.3.1 Фильтрация на отдельном компьютере

У родителей часто возникает потребность обезопасить своего ребенка от «плохого» контента в интернете. Существует несколько способов это осуществить.

Заблокировать определенные сайты можно с помощью антивируса, который установлен на компьютере (если он имеет встроенный брандмауэр), так и в файле hosts. Эти способы хороши тогда, когда Вы подключаетесь к интернету напрямую, через кабель, или беспроводной модем. Если нужно запретить доступ к некоторым сайтам, или же наоборот разрешить доступ только к определенным сайтам и при этом используется Wi-Fi роутер для доступа к интернету, то можно непосредственно на роутере настроить родительский контроль.

Плюс родительского контроля на уровне Wi-Fi роутера в том, что можно создавать правила доступа к сайтам для каждого компьютера или мобильного устройства, которое подключается через точку доступа (устройства распознаются по MAC адресу). Можно так же запретить доступ к определенным сайтам, или разрешить только к некоторым для всех устройств, которые работают через один и тот же роутер. Минус в том, что можно ограничить или разрешить доступ только к 8 сайтам.

Также можно использовать специализированный DNS-сервер. Например, Яндекс.DNS. Если доступ к интернету идет через точку доступа, он же Wi-Fi роутер, то достаточно в настройках прописать DNS, которые Яндекс предлагает в рамках сервиса Яндекс.DNS. И все устройства, которые будут подключаться к интернету через этот роутер, будут защищены от опасных сайтов.

Если пользователь не использует точку доступа, то можно указать DNS в настройках самого компьютера, телефона, планшета и т. д. Все настройки делаются очень просто.

1.3.2 Фильтрация в сети компьютеров предприятия

Основным механизмом организации общего доступа к ресурсам внешней сети (в т.ч. интернет) является преобразование сетевых адресов (NAT), суть которого сводится к подмене адреса источника (во внутренней сети) адресом внешнего интерфейса сервера и обратной заменой для ответного пакета. Это позволяет осуществить доступ к внешним ресурсам для всей внутренней сети и в то же время закрыть внутреннюю сеть от попыток доступа извне.

В Ubuntu Server функции NAT выполняет встроенный брандмауэр iptables. Главным достоинством NAT является его прозрачность, любое приложение использующее любой сетевой протокол с легкостью получит доступ во внешнюю сеть, если это разрешено правилами брандмауэра. [19]

Кроме организации доступа в сеть интернет требуется осуществлять фильтрацию контента и первичную антивирусную проверку. Львиная доля интернет трафика приходится на протокол HTTP, все, с чем пользователи работают через браузер, использует этот протокол.

Для работы с HTTP трафиком предназначены прокси-сервера, которые обрабатывают запросы пользователей и, в зависимости от результатов обработки, либо отвечают сами, либо перенаправляют запрос во внешнюю сеть или отклоняют его. Прокси-сервера могут представлять собой каскады, каждый элемент которого осуществляет свои функции анализа и обработки запросов.

Для работы через прокси-сервер, как правило, следует явно указать его адрес и порт в настройках приложения, однако можно сделать так, чтобы все HTTP запросы автоматически отдавались прокси-серверу, такая схема называется прозрачным прокси.

Основное назначение прокси-сервера это снижение нагрузки на канал и увеличение скорости работы в интернет за счет кэширования веб-документов имеющих статичное содержимое. Так если несколько пользователей в течение дня обратились к какому-нибудь ресурсу, то все его содержимое, включая оформление будет загружено из сети только один раз, при следующих обращениях клиент будет получать содержимое кэша прокси-сервера. Как показывает

практика, экономия трафика за счет использования прокси-сервера может достигать 30-40%, в основном выигрыш идет за счет статичной графики и статичных документов. Также прокси-сервер может осуществлять фильтрацию трафика, авторизацию пользователей, ограничение скорости доступа.

Кроме того существуют специализированные прокси-серверы основная задача которых именно фильтрация трафика, к ним относятся контент-фильтры, антивирусные прокси, фильтры рекламы и т.п.[23]

Еще одним рубежом обороны может быть использование фильтрующих DNS. Запрашивая какой-либо материал из сети интернет пользователь набирает в браузере символьное имя сайта, например mail.ru. Однако символьное имя не несет информации, какому именно серверу в сети следует посылать запрос, для этого необходимо знать IP адрес сервера, обслуживающего данное доменное имя, такую информацию предоставляют DNS сервера.

Итак, пользователь набрал в адресной строке имя сайта. Следующим шагом будет отправка запроса DNS серверу, указанному в сетевых настройках. Он может выдать результат из кэша или перенаправить запрос вышестоящему серверу. В результате мы получим ответ, что введенному нами символьному имени mail.ru соответствует IP адрес 94.100.191.204. Запрос по данному адресу будет направлен к роутеру, который в свою очередь сравнит адрес назначения с текущими правилами брандмауэра и либо отклонит его, либо передаст дальше. Сервер назначения, получив запрос, сформирует ответ и передаст его запросившему клиенту, в данном случае роутеру. Произведя необходимую фильтрацию, роутер передаст ответ тому ПК, с которого был сделан запрос и пользователь увидит на своем экране содержимое веб-страницы (либо страницу блокировки, если запрошенная страница по какой-то причине не прошла фильтрацию).

Основными службами роутера являются NAT и брандмауэр, именно они, в тесном взаимодействии, отвечают за все сетевые соединения. Так, например,

все инициированные извне соединения будут отклонены, а из внутренней сети будут пропущены только те, которые явно разрешены.

Последнее звено прокси-сервера контент-фильтр, он производит фильтрацию полученного из сети содержимого и либо отдает его клиенту, либо выдает страницу блокировки. Будучи правильно настроенной подобная схема сочетает удобство для пользователя, который может получать сетевые настройки автоматически по DHCP, и высокую степень защиты сети и получаемого пользователями контента.[20]

1.3.3 Фильтрация в масштабах государства.

В качестве примеров фильтрации в масштабах страны можно привести блокировку сайтов по решению Роскомнадзора в России и firewall «Золотой щит» в Китае.

1.3.3.1 Китайский «Золотой щит»

В 1998 году, министр общественной безопасности Китая представил документ, в котором говорилось о том, что Коммунистическая Партия Китая должна иметь возможность контролировать информацию, которую получает население. После глубоких исследований и проведения ряда встреч с органами общественной безопасности, министром общественной безопасности было принято решение об осуществлении проекта, направленного на обеспечение общественной безопасности информационных технологий. Проекту дали название “Golden Shield Project”.

Согласно официальному законодательству для этого проекта, веб-сайты, базирующиеся на территории Китая не могут ссылаться и публиковать новости взятые из зарубежных новостных сайтов, или СМИ без специального одобрения. Существует список медиа-сайтов “licensed print publishers”, которые имеют разрешение публиковать новости в Интернете. Все другие веб-сайты могут предоставлять только ту информацию, которая уже обнародована уполномоченным СМИ. Они также должны получить одобрение со стороны информаци-

онного агентства Государственного Совета и несут ответственность за законность транслирования информации. Каждый интернет-провайдер информационных услуг «должен сохранять копии записей в течение 60 дней» и быть готовым предоставить эту информацию для органов государственной власти по первому требованию. Провайдеры, также, обязаны ограничивать информацию, которую они публикуют. Несоблюдение любого из этих требований приводит к блокированию веб-сайта.

Главная цель «Золотого щита» контроль всего трафика, как в стране, так и за ее пределами. И эта сложная задача выполняется очень простым и эффективным способом.

Зеркальная технология

Первое, что власти используют для контроля над деятельностью своих пользователей интернета является зеркалирование (mirroring) – то есть то, что обычно используется для простого или резервного копирования. Большинство интернет-соединений между Китаем и остальным миром проводится очень небольшим количеством опто-волоконных кабелей, которые вводятся в страну через три основных пункта — в северной области, на центральном побережье и на юге страны. На каждом из этих шлюзов есть устройства, называемые сетевыми анализаторами трафика (network sniffer), которые отражают каждый входящий в страну или исходящий из нее пакет данных.

DNS блокировка

Помимо зеркальной технологии, интересны и другие методы, взятые на вооружение китайскими властями для ограничения доступа к потенциально опасной информации.

Первое препятствие, на которое обычный пользователь может натолкнуться — DNS блокировка. Существует список сайтов, содержание которых полностью закрыто для просмотра случайным интернет-пользователям. Большинство сайтов активно проверяются на наличие потенциально запрещенных ключевых слов, и списки этих слов постоянно обновляются.

Если DNS работает корректно, и доставки происходят по правильному IP-адресу, происходит зеркалирование. Пока пользователь посылает информационный запрос к корректному IP- адресу, информация отражается и IP-адрес проверяется в списках запрещенных IP-адресов. Если адрес соответствует записи в этом списке, шлюз посылает команду разрыва связи на оба компьютера: и на пользовательский, и на тот, которого он хотел достичь.

Блокировка по URL

Если пользователю удастся преодолеть первые две блокировки, есть еще одна проверка, которую необходимо пройти для того, чтобы добраться до выбранного ресурса. Это блокировка по URL. Если IP сайта, к которому пользователь пытается получить доступ, не в черном списке, то его доменное имя проверяется на наличие потенциально опасных ключевых слов. Если запрашиваемый URL содержит запрещенные термины, соединение будет сброшено.

Другие методы

Другим популярным методом для предотвращения доступа пользователей к запрещенному контенту является, так называемая «black-hole loop». Это означает, что запрос попадает в ловушку из серии задерживаемых команд. Когда браузер обнаруживает вход в цикл такого типа, он просто посылает пользователю сообщение об ошибке, заявляя тем самым, что запрос перенаправлен по пути, который не может быть завершен.

Ну и последний этап включает в себя проверку фактического содержания, что и делается при помощи зеркалирования. Пока пользователь просматривает страницу, система контроля доступа сканирует содержание, в поисках слов, фраз и терминов, которые ей не нравятся. Если система находит их — она разрывает соединение и пользователь уже не может делать какие-либо дальнейшие запросы к этому серверу. Затем «Золотой щит» блокирует соединение между компьютером и сервером сайта. Сначала это только в течение 2-3 минут. Но, если пользователь пытается получить доступ к сайту в течение этого времени, следующим будет уже пятиминутный тайм-аут. С третьей попытки, тайм-

аут может уже достигнуть 30-ти минут, или более. С каждой попыткой, которая последует, тайм-аут будет увеличиваться.[18]

1.3.3.2 Роскомнадзор

Блокировки по решению Роскомнадзора осуществляются в соответствии с законами «О связи» и «Об информации, информационных технологиях и защите информации», вводящим обязанность для интернет-провайдеров блокировать доступ к незаконным ресурсам.[5]

Роскомнадзор ведет единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено.

Запрет доступа к сайту может быть вынесен на основании решения суда или уполномоченных органов в отдельных случаях. В реестр включают адрес и доменное имя запрещенного интернет-ресурса, информацию о хостинг-провайдере, решение уполномоченного органа о запрете данного сайта, заверенную копию запрещенной информации и другие данные. Получив решение уполномоченного органа о запрете того или иного сайта, Роскомнадзор обязан в течении суток определить его хостинг-провайдера, направить ему соответствующее уведомление и внести сайт в реестр. Если в течение 3 суток с момента отправки уведомления доступ к запрещенной информации по-прежнему будет возможен по указанному домену или адресу, Роскомнадзор вносит в реестр сетевой адрес ресурса. Операторы связи должны в течение суток заблокировать к нему доступ.

Интернет провайдеры осуществляют блокировку несколькими способами, которые уже были описаны выше:

- Блокировка по IP-адресу;
- Блокировка по доменному имени;
- Блокировка по URL.

1.4 Вывод по главе 1

Подводя итог по первой главе можно сделать несколько выводов.

Существуют различные способы фильтрации трафика, например зеркальная технология, DNS-блокировка, блокировка по URL. Одни из них более эффективны, другие менее, но ни один из способов не является эффективным на 100%.

Существует множество областей применения фильтрации трафика. По масштабу их можно разделить на 3 типа: отдельный компьютер, сеть компьютеров, государственный уровень.

Глава 2. Моделирование системы фильтрации в сети организации

2.1 Задачи фильтрации

При отсутствии гибкой фильтрации доступа к сети Интернет на долю ненужных и опасных сайтов, ежедневно посещаемых сотрудниками, приходится чуть ли не половина общего трафика.

Лидерами в списке нежелательных ресурсов являются социальные сети, порталы, выкладывающие контент непристойного содержания, серверы онлайновых игр, а также сайты, генерирующие так называемый "тяжелый" трафик и предлагающие посетителям загружать и просматривать видеоролики и флэш-баннеры.[16]

Потенциальные угрозы, возникающие в результате посещения сотрудниками различных не относящихся к выполняемой ими работе сайтов, помимо нецелевого использования рабочего времени, могут выглядеть как:

- чрезмерная нагрузка на сеть, вызванная неконтролируемым скачиванием сотрудниками объемных файлов из Интернет-сети. В случае, когда речь идет о постоянном или выделенном подключении с фиксированной скоростью канала от провайдера, просмотр или загрузка пользователями видеофайлов негативно скажется на распределении ресурсов сети и загрузке Интернет-канала в целом, а также на стоимости нецелевого трафика;
- нерациональное использование ресурсов сети и рабочего времени в результате деятельности любителей онлайновых игр с видео- или голосовыми чатами;
- неконтролируемые удаленные соединения сотрудников с рабочими серверами корпоративных сетей посредством VPN-соединений или утилит, связанные с риском заражения локальной сети вирусами, потенциально находящимися на удаленном компьютере;
- снижение уровня безопасности корпоративной сети.[17]

Задачи фильтрации:

1) Ограничение доступа внешних (по отношению к защищаемой сети) пользователей к внутренним ресурсам корпоративной сети. К таким пользователям могут быть отнесены партнеры, удаленные пользователи, хакеры и даже сотрудники самой компании, пытающие получить доступ к серверам баз данных, защищаемых межсетевым экраном.
2) Разграничение доступа пользователей защищаемой сети к внешним ресурсам. Решение этой задачи позволяет, например, регулировать доступ к серверам, не требуемым для выполнения служебных обязанностей, а также ввести следующие ограничения сайтов для сотрудников:
    - ограничение сайтов по поиску работы;
    - ограничение сайтов для просмотра видео роликов;
    - ограничение сайтов созданных для общения;
    - ограничение сайтов для скачивания аудио и видео файлов;
    - ограничение сайтов для online игр.
3) Ограничение скорости интернет-соединения. При одновременной работе в интернете всех сотрудников, значительно падает скорость интернет соединения для каждого пользователя. Ограничение доступа в интернет позволит осуществить:
    - ограничение интернета по скорости для каждого пользователя;
    - ограничение интернета по объему трафика для каждого пользователя;
    - ограничение доступа в интернет для нежелательных программ (например, ICQ);
    - ограничение доступа в интернет для скачивания файлов (например, MP3, AVI, JPG, EXE).[4]

2.2 Техническое задание

1. Общие сведения

1.1.Название системы

Разработка и создание системы фильтрации трафика для структурированной кабельной системы в учебном здании «Уральского государственного педагогического университета».

1.2.Область использования

Системное администрирование и управление сетью передачи данных.

1.3.Место внедрения

Сеть передачи данных ФГБОУ ВПО УрГПУ.

1.4.Данные об авторах

Гудюшкина А.А., ст. группы БС-41

1.5.Руководитель

Стариченко Е.Б.

2. Цели создания системы фильтрации

Цель создания данной системы – создание правил разграничения доступа разных групп пользователей к внешним и внутренним ресурсам сети, мониторинг и контроль использования интернет-ресурсов.

3. Требования к разработке системы фильтрации

3.1.Сетевая инфраструктура организации

Для разработки системы фильтрации требуется функционирующая структурированная кабельная система иерархического типа, на основе оптических каналов связи с пропускной способностью до 1Гб/с.

3.2.Оборудование

Система фильтрации должна быть построена на базе существующего активного оборудования: ядро сети коммутатор Cisco Catalist WS-4503, программный маршрутизатор на базе сервера HP Proliant ML 350 Gen7, коммутаторы доступа Cisco Catalist WS-2650.

3.3.Настройка коммутаторов

Должны быть созданы VLAN для нескольких групп пользователей, включая пользователей, подключающихся через открытую сеть WiFi. Для организации фильтрации должны использоваться штатные средства коммутационного оборудования и операционных систем.

4. Разработка системы фильтрации

4.1.Логические группы VLAN

- Управление
- Бухгалтерия
- Управление институтов
- Методисты
- Остальные
- WiFi

4.2.Настройка правил

Доступ к внутренним ресурсам:

- Полный
- Частичный
- Отсутствует.

Доступ в интернет.

Скорость.

4.3.Списки доступа

Группа	**Доступ к внутренним ресурсам**	**Доступ в интернет**	**Скорость**
Бухгалтерия	**Частичный**	**да**	**средняя**
Управление институтов	**Частичный**	**да**	**средняя**
Методисты	**Полный**	**нет**	**-**
Остальные	**Полный**	**да**	**средняя**

Wi-Fi	**Отсутствует**	**да**	**низкая**

2.3 Моделирование в Cisco Packet Tracer

Технологии фирмы Cisco Systems широко используются для построения защищенных компьютерных сетей. Аппаратно-программные комплексы Cisco можно встретить в сетях практически любых организаций. Соответственно, растет потребность в специалистах, способных не только эксплуатировать данное оборудование, но и разрабатывать на его базе сложные защищенные сетевые проекты, а также осуществлять анализ информационной безопасности таких сетей. Известно, что подобные специалисты весьма ценятся и могут рассчитывать на высокооплачиваемую работу.[13]

2.3.1 Списки доступа

Списки доступа позволяют создавать правила управления трафиком, по которым будет происходить межсетевое взаимодействие как в локальных, так и в корпоративных сетях.

Существует шестнадцать типов списков доступа, но наиболее часто используются два типа: standart – стандартные (номера с 1 по 99) и extended – расширенные (номера с 100 по 199 или с 2000 по 2699). Различия между этими двумя списками заключаются в возможности фильтровать пакеты не только по IP – адресу, но и по другим различным параметрам.

Стандартные списки обрабатывают только входящие IP адреса источников, т.е. ищут соответствие только по IP адресу отправителя. Расширенные списки работают со всеми адресами корпоративной сети и дополнительно могут фильтровать трафик по портам и протоколам.[14]

Работа списка доступа напрямую зависит от порядка следования строк в этом списке, где в каждой строке записано правило обработки трафика. Просматриваются все правила списка с первого до последнего по порядку, но просмотр завершается, как только было найдено первое соответствие, т.е. для при-

шедшего пакета было найдено правило, под которое он подпадает. После этого остальные правила списка игнорируются. Если пакет не подпал ни под одно из правил, то включается правило по умолчанию:

```
access-list номер_списка deny any
```

которое запрещает весь трафик по тому интерфейсу сетевого устройства, к которому данный список был применен.

Для того, чтобы начать использовать список доступа, необходимо выполнить следующие три этапа:

1 – создать список;

2 – наполнить список правилами обработки трафика;

3 – применить список доступа к интерфейсу устройства на вход или на выход этого интерфейса.

Этап первый – создание списка доступа:

Стандартный список:

```
Switch3(config)#ip access-list standart 10
```

(создается стандартный список доступа под номером 10, в данном случае создается на коммутаторе)

Расширенный список:

```
Router1(config)#ip access-list extended 100
```

(создается расширенный список доступа под номером 100, в данном случае создается на маршрутизаторе).

Этап второй – ввод правил в список доступа:

Каждое, правило в списке доступа сдержит три важных элемента:

1 - число, идентифицирующее список при обращении к нему в других частях конфигурации маршрутизатора или коммутатора третьего уровня;

2 - инструкцию deny (запретить) или permit (разрешить);

3 - идентификатор пакета, который задается по одному из трех вариантов:

- адрес сети (например 192.168.2.0 0.0.0.255) – где вместо маски подсети указывается шаблон маски подсети;
- адрес хоста (host 192.168.2.1);
- любой IP адрес (any).

Пример стандартного списка доступа №10:

```
access-list 10 deny host 11.0.0.5
access-list 10 deny 12.0.0.0  0.255.255.255
access-list 10 permit any
```

В этом списке:

- запрещен весь трафик хосту с IP адресом 11.0.0.5;
- запрещен весь трафик в сети 12.0.0.0/8 (в правиле указывается не реальная маска подсети, а ее шаблон);
- весь остальной трафик разрешен.

В расширенных списках доступа вслед за указанием действия ключами permit или deny должен находиться параметр с обозначением протокола (возможны протоколы IP, TCP, UDP, ICMP), который указывает, должна ли выполняться проверка всех пакетов IP или только пакетов с заголовками ICMP, TCP или UDP. Если проверке подлежат номера портов TCP или UDP, то должен быть указан протокол TCP или UDP (службы FTP и WEB используют протокол TCP).

Пример расширенного списка доступа №111:

Запретить трафик на порту 80 (www-трафик)

```
ip access-list 111 deny tcp any any eq 80
ip access-list 111 deny ip host 10.0.0.15  host 12.0.0.5
ip access-list 111 permit ip any any

interface ethernet0
```

Применить список доступа 111 к исходящему трафику

```
ip access-group 111 out
```

В этом списке внешние узлы не смогут обращаться на сайты внутренней сети, т.к. список доступа был применен на выход (для внешних узлов) интерфейса, а так же узлу 10.0.0.15 запрещен доступ к узлу 12.0.0.5. Остальной трафик разрешен.

Этап третий – применение списка доступа.

Списки доступа могут быть использованы для двух типов устройств:

1 – на маршрутизаторе;

2 - на коммутаторе третьего уровня.

На каждом интерфейсе может быть включено два списка доступа: только один список доступа для входящих пакетов и только один список для исходящих пакетов.

Каждый список работает только с тем интерфейсом, на который он был применен и не действует на остальные интерфейсы устройства, если он там не применялся. Однако один список доступа может быть применен к разным интерфейсам.[9]

Применение списка доступа к устройству осуществляется следующими командами:

```
interface ethernet0/0/0
ip access-group 1 in
ip access-group 2 out
```

В данном случае к интерфейсу ethernet0/0/0 применили два списка доступа:

список доступа №1 – на вход интерфейса (т.е. для внутренних адресов);

список доступа №2 – на выход интерфейса (применение к внешней сети).

2.3.1.1 Листинги ACL использованных в работе

Создаем список доступа к внутренним ресурсам

```
ip access-list extended Servers-out
```

Разрешаем доступ от некоторых VLAN'ов к почтовому серверу

```
remark MAIL
```

```
permit ip 192.168.22.0 0.0.0.255 host 192.168.77.2
permit ip 192.168.33.0 0.0.0.255 host 192.168.77.2
permit ip 192.168.44.0 0.0.0.255 host 192.168.77.2
permit ip 192.168.55.0 0.0.0.255 host 192.168.77.2
```

Разрешаем доступ от некоторых VLAN'ов к веб-серверу

```
remark WEB
permit tcp any host 192.168.77.3 eq www
permit ip host 192.168.55.5 host 192.168.77.3
permit ip host 192.168.55.5 host 192.168.77.3
```

Разрешаем доступ от некоторых VLAN'ов к файловому серверу

```
remark FILE
permit ip 192.168.44.0 0.0.0.255 host 192.168.77.4
permit ip 192.168.55.0 0.0.0.255 host 192.168.77.4
```

Запускаем список доступа на исходящий трафик

```
int fa0/0.11
ip access-group Servers-out out
```

2.3.2 Служба NAT

NAT (Network Address Translation) — трансляция сетевых адресов, технология, которая позволяет преобразовывать (изменять) IP адреса и порты в сетевых пакетах.

NAT используется чаще всего для осуществления доступа устройств из сети предприятия(дома) в Интернет, либо наоборот для доступа из Интернет на какой-либо ресурс внутри сети.

Сеть предприятия обычно строится на частных IP адресах. Согласно RFC 1918 под частные адреса выделено три блока:

10.0.0.0 — 10.255.255.255 (10.0.0.0/255.0.0.0 (/8))

172.16.0.0 — 172.31.255.255 (172.16.0.0/255.240.0.0 (/12))

192.168.0.0 — 192.168.255.255 (192.168.0.0/255.255.0.0 (/16))

Эти адреса не маршрутизируются в Интернете, и провайдеры должны отбрасывать пакеты с такими IP адресами отправителей или получателей.

Для преобразования частных адресов в Глобальные (маршрутизируемые в Интернете) применяют NAT.

Помимо возможности доступа во внешнюю сеть (Интернет), NAT имеет ещё несколько положительных сторон. Так, например, трансляция сетевых адресов позволяет скрыть внутреннюю структуру сети и ограничить к ней доступ, что повышает безопасность. А ещё эта технология позволяет экономить Глобальные IP адреса, так как под одним глобальным адресом в Интернет может выходить множество хостов.

Настройка NAT на маршрутизаторах Cisco под управлением IOS включает в себя следующие шаги

1. Назначить внутренний (Inside) и внешний (Outside) интерфейсы

Внутренним интерфейсом обычно выступает тот, к которому подключена локальная сеть. Внешним — к которому подключена внешняя сеть, например сеть Интернет провайдера.

2. Определить для кого (каких ip адресов) стоит делать трансляцию.

3. Выбрать какой вид трансляции использовать

4. Осуществить проверку трансляций

Существует три вида трансляции Static NAT, Dynamic NAT, Overloading.

Static NAT — Статический NAT, преобразование IP адреса один к одному, то есть сопоставляется один адрес из внутренней сети с одним адресом из внешней сети.

Dynamic NAT — Динамический NAT, преобразование внутреннего адреса/ов в один из группы внешних адресов. Перед использованием динамической трансляции, нужно задать nat-пул внешних адресов

Overloading — позволяет преобразовывать несколько внутренних адресов в один внешний. Для осуществления такой трансляции используются порты, поэтому иногда такой NAT называют PAT (Port Address Translation). С помощью PAT можно преобразовывать внутренние адреса во внешний адрес, заданный через пул или через адрес на внешнем интерфейсе.[6]

2.3.2.1 Листинги настроек NAT использованных в работе

Настраиваем NAT на исходящий трафик

```
int fa0/1
ip nat outside
```

Настраиваем NAT на входящий трафик

```
int fa0/0.2
ip nat inside
int fa0/0.3
ip nat inside
int fa0/0.5
ip nat inside
int fa0/0.6
ip nat inside
```

Создаем список доступа VLAN'ов к интернету

```
ip access list standard FOR-NAT
permit 192.168.22.0 0.0.0.255
permit 192.168.33.0 0.0.0.255
permit 192.168.55.0 0.0.0.255
permit 192.168.66.0 0.0.0.255
```

Запускаем NAT в режиме PAT

```
ip nat inside source list FOR-NAT interface fa0/1 overload
```

2.4 Заключение о построенной модели

Разработка схемы произведена в программе Cisco Packet Tracer. За основу была взята схема сети, дополненная для произведения фильтрации трафика. Были добавлены сервера внутренних ресурсов и выход в интернет через провайдера к серверу внешнего ресурса. Настроены списки управления доступом, определяющие какие группы и конкретные пользователи могут иметь доступ к внутренним и внешним ресурсам ресурсам. Настроен механизм NAT, позволяющий соединить нашу локальную сеть с интернетом, а также ограничить к нему доступ.

Заключение

В рамках выпускной квалификационной работы мною была смоделирована система фильтрации трафика для конкретной структурированной кабельной системы. Проектом предусматривается настройка VLAN и ACL для нескольких групп пользователей. В качестве эмулятора сети был выбран Cisco Packet Tracer, так как он наиболее прост в освоении.

Список информационных источников

1. Чемодуров А. С., Карпутина А. Ю. Обзор средств фильтрации трафика в корпоративной сети // Научно-методический электронный журнал «Концепт». 2015. №2 (февраль). С. 71–75. URL: http://e-koncept.ru/2015/15039.htm
2. Дети и Интернет // internetsociety.org URL: http://www.internetsociety.org/sites/default/files/bp-childrenandtheinternet-20129017-en_RU.pdf (дата обращения: январь 2016).
3. Медведовский И. Д., Семьянов П. В., Леонов Д. Г. Атака на Internet. 2-е изд., перераб. и доп. изд. М.: ДМК, 2002.
4. Лапонина О. Р. Межсетевое экранирование. М.: Бином. Лаборатория знаний, 2007.
5. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 № 149-ФЗ // с изм. и допол. в ред. от 13.07.2015
6. Cisco ICND 1 Руководство для студента. изд. Cisco, 2009.
7. Д. Бони Руководство по Cisco IOS. СПб.: Русская редакция, 2008.
8. К. Кеннеди, К. Гамильтон Принципы коммутации в локальных сетях Cisco. изд. Вильямс, 2003.
9. Джером Ф. Димарцио Маршрутизаторы CISCO. Пособие для самостоятельного изучения. Символ-Плюс, 2003.
10. И.В. Руденко Маршрутизаторы CISCO для IP-сетей. КУДИЦ-ОБРАЗ, 2003.
11. Вито Амато Основы организации сетей Cisco. Том 1. Вильямс, 2002.
12. Тодд Леммл, Кевин Хейлз CCNP: Настройка коммутаторов CISCO. Лори, 2002.
13. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс : учеб. пособие / А. Н. Андрончик, А. С. Коллеров, Н. И. Синадский, М. Ю. Щербаков, Под ред. Н. И. Синадского. Екатеринбург: Изд-во Урал. ун-та, 2014.

14. Уэнделла Одома Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1. 3-е изд., серия Cisco Press. Вильямс, 2013.
15. Компания Cisco Systems URL: www.cisco.com
16. Олег Слепов Контентная фильтрация // Jet Info. 2005. №10 (149).
17. Алексей Отт О контентной фильтрации. Продолжение темы // Jet Info. 2006. №10 (161).
18. Великий китайский золотой щит // Habrahabr URL: https://habrahabr.ru/company/websitepulse/blog/136072/ (дата обращения: 14.05.2016).
19. В.В. Глазкова, В.А. Масляков, И.В. Машечкин, М.И. Петровский Система фильтрации интернет трафика на основе методов машинного обучения // Вопросы современной науки и практики. 2008. №2 (12). С. 155-167.
20. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. СПб.: Питер, 2010.
21. Э. Таненбаум, Уэзеролл Д. Компьютерные сети. 5-е изд. СПб.: Питер, 2012.
22. Ермаков А.Е Основы конфигурирования корпоративных сетей Cisco . ФГБОУ «УМЦ ЖДТ», 2013.
23. Максимов Н.В., Попов И.И. Компьютерные сети. 4-е изд., перераб. и доп. М.: Форум, 2010.
24. Боллапрагада В., Мэрфи К., Уайт Р Структура операционной системы Cisco IOS. М.: Издательский дом Вильямс, 2002.

25. Хилл Б. Полный справочник по Cisco. М.: Издательский дом Вильямс, 2004.
26. Хабракен Д. Как работать с маршрутизаторами Cisco. М.:ДМК Пресс,2005.
27. Амато В. Основы организации сетей Cisco, том 2. М.: Издательский дом Вильямс, 2004.
28. Чепмен Д., Фокс Э. Брандмауэры Cisco Secure PIX М.: Издательский дом Вильямс, 2003.
29. НОУ Интуит URL: http://www.intuit.ru
30. Одом У. Компьютерные сети. М.: Издательский дом Вильямс, 2006