Федеральное агентство по образованию РФ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Факультет информатики
Кафедра теоретических основ информатики

УДК 681

ДОПУСТИТЬ К ЗАЩИТЕ В ГАК
Зав. кафедрой, проф., д.т.н. _____
Ю.Л. Костюк «___» _____ 2006 г.

Кокшенев Владимир Владимирович

ИФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОРПОРАТИВНЫХ МУЛЬТИСЕРВИСНЫХ СЕТЕЙ

Дипломная работа

Научный руководитель,
ведущий инженер ООО «Элекс.Ком» Д. Ю. Белицкий

Исполнитель,
студент группы 1411 В. В. Кокшенев

Электронная версия дипломной работы помещена
в электронную библиотеку. Файл
Администратор

Томск-2006

РЕФЕРАТ

Дипломная работа, 64 страницы, 26 источников, 2 приложения, 19 рисунков.

ИНФОРМЦИОННАЯ БЕЗОПАСНОСТЬ, КОРПОРАТИВНЫЕ МУЛЬТИСЕРВИСНЫЕ СЕТИ, АТАКИ, ТЕХНОЛОГИИ БЕЗОПАСНОСТИ ДАННЫХ, CISCO SAFE, МЕЖСЕТЕВОЙ ЭКРАН, ГЕНЕРАЦИЯ ТРАФИКА, CAM OVERFLOW, MAC ADDRESS MANIPULATION, PACKET SNIFFER SDK

Объект исследования – информационная безопасность корпоративных мультисервисных сетей.

Цель работы – реализация комплексного подхода при обеспечении информационной безопасности корпоративных мультисервисных сетей.

Методы исследования – теоретический анализ мер, предлагаемых компанией Cisco, практическое моделирование в лабораторных условиях предложенного комплекса мер и имитация хакерских атак с целью проверки их работоспособности.

Результат – проанализированы технологии защиты корпоративных сетей, произведено проектирование, реализация, тестирование и обеспечение информационной безопасности сети пресс-центра Российско-Германского саммита. Разработано приложение, осуществляющее атаку на коммутаторы с целью проверки защищенности 2-го уровня.

Содержание

Введение.

В наш век сетевые технологии развиваются с огромной скоростью. Растут вычислительные мощности, пропускная способность, расширяется спектр услуг, предлагаемых ISP, изобретаются все новые механизмы сетевого взаимодействия.

Это нацелено на объединения ресурсов и совместную работу тысяч, миллионов пользователей.

Все острее стоит вопрос защиты ресурсов и разграничения доступа к ним. К сожалению, частенько третьи лица пытаются получить (и получают) доступ к конфиденциальной информации, являющейся интеллектуальной собственностью компаний, к сетевым услугам, или же направляют свои усилия на разрушение работоспособности отдельных хостов или всей сети.

Чем больше ресурсов компания объединяет в своей корпоративной сети, тем больше создается угроз для них, тем труднее обеспечить сетевую безопасность.

Для надежной защиты ресурсов необходимо реализовывать комплексный подход в обеспечение сетевой безопасности корпоративных мультисервисных сетей. Предлагаемые решения перед внедрением должны быть всесторонне (насколько позволяют время и возможности) протестированы в лабораторных условиях. Это касается не только проверки, оборудования и ПО, но и подготовки квалифицированного персонала, способного правильно с ним работать.

Цель данной работы заключается в анализе технологий, предлагаемых компанией Cisco, реализации комплекса мер по защите существующей сети, создании программного средства генерации трафика для частичной проверки защищенности 2-го уровня.

Глава 1. Сетевая безопасность.

§1.1 Основы сетевой безопасности.

Сетевая безопасность – это не цель, а процесс! [1] Колесо безопасности Cisco (Cisco Security Wheel) хорошо описывает эволюцию системы безопасности (см. рис. 1).

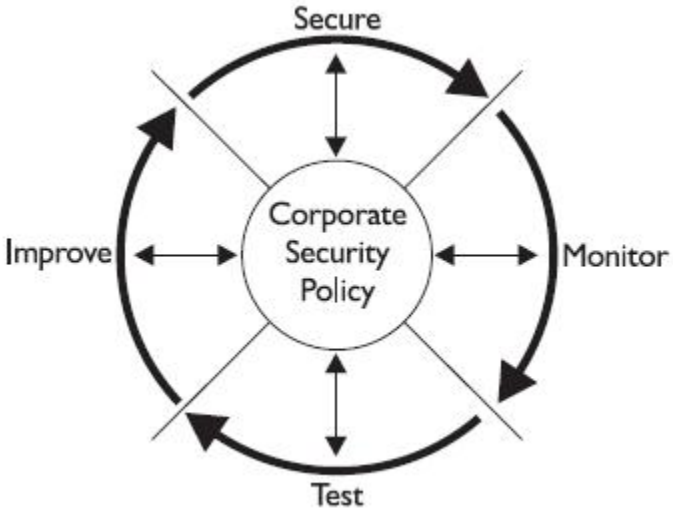


Рис. 1 Cisco Security Wheel

В основе данного представления лежит корпоративная политика безопасности (Corporate Security Policy), на которую опираются четыре составляющие: Secure (Обеспечение безопасности), Monitor (Мониторинг), Test (Проверка), Improve (Улучшение системы).

Согласно [4], прежде чем проектировать реальную схему защиты сети, следует выработать адекватную политику безопасности, определяющую ряд моментов:

1. План приобретений и реализаций по обеспечению безопасности
2. Допустимые и запретные технологии
3. План действий на случай инцидентов
4. Допустимое поведение персонала
5. Санкции на нарушение
6. Иерархию ответственности за реализацию, поддержку, аудит, мониторинг,…
7. Направление дальнейшего развития системы безопасности

Политика безопасности – это формальное изложение правил, которым должны подчиняться лица, получающие доступ к корпоративной технологии и информации [4], это утвержденный документ, являющийся результатом компромисса между безопасностью и простотой использования, безопасностью и предоставляемыми услугами, и, наконец, между ценой системы и рисками потерь[8].

Сам документ разбивается на части – субполитики – описывающие отдельные элементы схемы безопасности, такие, например, как:

1. Удаленный доступ (Remote Access Policy)
2. Аутентификацию (Authentication Policy)

3. Антивирусные средства (Antivirus Policy)
4. Парольная политика (Password Policy) и многое другое.

Следует, однако, отдельно упомянуть позицию компании (организации) в отношении подготовки персонала. Например, статья «Каждый сотрудник как брандмауэр» ([11]) описывает позиции компаний Cisco и SAP по данному вопросу, которые тратят не малых деньги на постоянную переподготовку и проверку персонала. Результатом таких действий является резкое снижение успешности проведения социальной инженерии (см. секцию «Сетевые атаки»), и усиление системы безопасности в отношении внутренних угроз. Какая бы качественная и дорогостоящая ни была система, если персонал не соблюдает правила, закрепленные в политике, то она бесполезна.

Secure – реализация спроектированных процессов и технологий, направленных на обеспечение безопасности.

Monitor – процессы и технологии безопасности нуждаются в мониторинге с целью оценивания работоспособности и эффективности системы безопасности, обнаружение и фиксирования нарушений и вторжений.

Test – фаза тестирования включает проверку процессов на адекватность, устойчивость и предсказуемость. Всегда лучше самому обнаружить слабости в своей системе безопасности, чем позволить это другим.

Improve – разработка нового дизайна сети, внедрение новых технологий, обновление оборудования, его ПО и конфигураций.

Объектами защиты являются:

- Оборудование – сервера, рабочие станции, маршрутизаторы, коммутаторы, IP-телефоны и т.д.
- Программное обеспечение – например, операционная система на сервере или рабочей станции.
- Данные, представляющие коммерческую ценность для компании.

Как бы мы ни старались, и сколько бы средств мы ни вкладывали, абсолютной безопасности добиться невозможно. Безопасность и доступность – в асимптотике вещи обратно пропорциональные. Всегда есть причины, вызывающие трудности в защите. Их можно классифицировать на 3 группы.

Технологические уязвимости – изначально TCP/IP изобретался без учета каких бы то ни было требований по безопасности. Все операционные системы содержат уязвимые места, которые постоянно обнаруживаются и устраняются. Уязвимость ОС несет угрозу ресурсам, которыми она управляет.

Слабость политики безопасности – сюда можно отнести недостаток мониторинга системы, отсутствие плана восстановления в случае сбоя, или же отсутствие политики безопасности как таковой.

Неправильная настройка оборудования – использование паролей по умолчанию или же вообще их отсутствие, оставление ненужных услуг и портов включенными.

§1.2 Сетевые атаки.

1.2.1. Угрозы.

Угроза – это риск потери в результате наступления ряда событий по случайности или же чьих-то преднамеренных действий.

Снятие рисков потерь от случайности осуществляется с помощью избыточности схемы сети. Избыточность достигается за счет добавления дополнительного оборудования, что приводит к увеличению цены проекта. Однако это неизбежно, если мы хотим добиться высокой надежности системы. Например, может потребоваться обеспечить среднее время между сбоями (MTBF – mean time between fail) равное 99.999% [12]. Это примерно 1 час простоя на 11 лет работы.

Риски потерь от чьих-то преднамеренных действий снимаются применением комплексного подхода к обеспечению безопасности корпоративной сети.

Существует четыре основных типа угроз данной категории:

- неподготовленные угрозы (unstructured threats)
- подготовленные угрозы (structured threats)
- внутренние угрозы (internal threats)
- внешние угрозы (external threats)

Неподготовленные угрозы реализуются слабо квалифицированными субъектами, с весьма ограниченными навыками и познаниями в области сетевой безопасности. Они сами не создают и не модифицируют инструментов взлома, а используют чужие, готовые продукты.

Подготовленные угрозы осуществляются высоко квалифицированным, мотивированным взломщиком или же группой лиц. Все их атаки хорошо спланированы и ведутся не в слепую, а по вполне конкретным точкам целевой сети. Они могут сами создавать и модифицировать существующие инструменты взлома.

Основой внутренних угроз является лицо, имеющее доступ к ресурсам организации, то есть являющееся внутренним резидентом компании (обозленный или обманутый служащий). Если ко всему прочему он вступит в сговор с внешней профессиональной группой, то мы получим подготовленную внутреннюю угрозу, защититься от которой крайне сложно, так как практически невозможно избежать потерь. [1] Их степень будет определяться уровнем доступа служащего к ресурсам.

Внешняя угроза исходит от лиц, находящихся вне периметра обороны (может быть как подготовленной, так и нет).

Целью сетевой атаки может быть:

- разведка (reconnaissance attack)
- получение доступа (access attack)
- отказ в обслуживании (DoS attack)
- манипуляция данными (data manipulation attack)

В общем доступе находится множество программ – инструментов взлома. Так, например, любой может достать себе такие известные утилиты подбора паролей как L0pht

Crack, PWLVIEW, Pwlhack, PWL_Key, ntPassword; или же утилиты разведки: NMAP, SATAN, Portscanner, Strobe. Их можно использовать и в созидательных целях – проверка качества пароля или обнаружение недостатков конфигурации аппаратуры и ПО (например, не отключен SNMP там, где не предполагается его использовать).

1.2.2. Классификация сетевых атак и методы противодействия и защиты.

Снифферы пакетов.

Сниффер пакетов представляет собой прикладную программу, которая использует сетевую карту, работающую в режиме promiscuous mode (в этом режиме все пакеты, полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки). При этом сниффер перехватывает все сетевые пакеты, которые передаются через определенный сегмент. В настоящее время снифферы работают в сетях на вполне законном основании. Они используются для диагностики неисправностей и анализа трафика. Однако ввиду того, что некоторые сетевые приложения передают данные в текстовом формате (Telnet, FTP, SMTP, POP3 и т.д.), с помощью сниффера можно узнать полезную, а иногда и конфиденциальную информацию (например, имена пользователей и пароли). Перехват имен и паролей создает большую опасность, так как пользователи часто применяют один и тот же логин и пароль для множества приложений и систем. Многие пользователи вообще имеют один пароль для доступа ко всем ресурсам и приложениям. Если приложение работает в режиме клиент/сервер, а аутентификационные данные передаются по сети в читаемом текстовом формате, эту информацию с большой вероятностью можно использовать для доступа к другим корпоративным или внешним ресурсам.

Смягчить угрозу сниффинга пакетов можно с помощью следующих средств:

Аутентификация. Сильные средства аутентификации являются первым способом защиты от сниффинга пакетов. Примером являются однократные пароли (OTP — One-Time Passwords). OTP — это технология двухфакторной аутентификации, при которой происходит сочетание того, что у вас есть, с тем, что вы знаете. Типичным примером двухфакторной аутентификации является работа обычного банкомата, который опознает вас, во-первых, по вашей пластиковой карточке и, во-вторых, по вводимому вами ПИН-коду. Для аутентификации в системе OTP также требуется ПИН-код и ваша личная карточка. Под «карточкой» (token) понимается аппаратное или программное средство, генерирующее (по случайному принципу) уникальный одномоментный однократный пароль. Если хакер узнает этот пароль с помощью сниффера, эта информация будет бесполезной, потому что в этот момент пароль уже будет использован и выведен из употребления. Заметим, что этот способ борьбы со сниффингом эффективен только для предотвращения перехвата паролей. Снифферы, перехватывающие другую информацию (например, сообщения электронной почты), не теряют своей эффективности.

Коммутируемая инфраструктура. Еще одним способом борьбы со сниффингом пакетов в вашей сетевой среде является создание коммутируемой инфраструктуры. Если, к примеру, во всей организации используется коммутируемый Ethernet, хакеры могут получить доступ только к трафику, поступающему на тот порт, к которому они подключены (результат микросегментации производимой коммутатором). Однако, как мы увидим позже, существуют методы, позволяющие обойти это ограничение (ARP-взлом, CAM переполнение).

Анти-снифферы. Третий способ борьбы со сниффингом заключается в установке аппаратных или программных средств, распознающих снифферы, работающие в вашей сети. Эти средства не могут полностью ликвидировать угрозу, но, как и многие другие средства

сетевой безопасности, они включаются в общую систему защиты. Так называемые «анти-снифферы» измеряют время реагирования хостов и определяют, не приходится ли хостам обрабатывать «лишний» трафик. Одно из таких средств, поставляемых компанией L0pht Heavy Industries, называется AntiSniff.

Криптография – самый эффективный способ борьбы со сниффингом пакетов. Она делает работу снифферов бесполезной. Криптография Cisco на сетевом уровне базируется на протоколе IPSec. IPSec представляет собой стандартный метод защищенной связи между устройствами с помощью протокола IP. К прочим криптографическим протоколам сетевого управления относятся протоколы SSH (Secure Shell) и SSL (Secure Socket Layer).

IP-спуфинг.

IP-спуфинг происходит, когда хакер, находящийся внутри корпорации или вне ее, выдает себя за санкционированного пользователя. Это можно сделать двумя способами. Во-первых, хакер может воспользоваться IP-адресом, находящимся в пределах диапазона санкционированных IP-адресов, или авторизованным внешним адресом, которому разрешается доступ к определенным сетевым ресурсам. Атаки IP-спуфинга часто являются отправной точкой для прочих атак. Классический пример — атака DoS, которая начинается с чужого адреса, скрывающего истинную личность хакера. Обычно IP-спуфинг ограничивается вставкой ложной информации или вредоносных команд в обычный поток данных, передаваемых между клиентским и серверным приложением. Для двусторонней связи хакер должен изменить все таблицы маршрутизации, чтобы направить трафик на ложный IP-адрес. Если ему это удается, он получит все пакеты и сможет отвечать на них так, будто он является санкционированным пользователем.

Угрозу спуфинга можно ослабить (но не устранить) с помощью следующих мер:

Контроль доступа – самый простой способ предотвращения IP-спуфинга. Он заключается в правильной настройке управления доступом. Чтобы снизить эффективность IP-спуфинга, необходимо отсечь любой трафик, поступающей из внешней сети с исходным адресом, который должен располагаться внутри нашей сети. Если же санкционированными являются и некоторые адреса внешней сети, данный метод становится неэффективным.

Фильтрация RFC 2827. Мы можем пресечь попытки спуфинга чужих сетей пользователями нашей сети (и стать добропорядочным «сетевым гражданином»). Для этого необходимо отбраковывать любой исходящий трафик, адрес источника которого не является одним из IP-адресов нашей организации. Этот тип фильтрации, известный под названием «RFC 2827», может выполнять и провайдер (ISP). До тех пор, пока все провайдеры не внедрят этот тип фильтрации, его эффективность будет намного ниже возможной.

Аутентификация. IP-спуфинг может функционировать только при условии, что аутентификация происходит на базе IP-адресов. Поэтому внедрение дополнительных методов аутентификации делает этот вид атак бесполезным.

Отказ в обслуживании (Denial of Service — DoS).

DoS являются наиболее известной формой хакерских атак. Они просты в реализации и могут причинить огромный вред. Кроме того, против атак такого типа труднее всего создать гарантированную защиту. Типы DoS атак:

- TCP SYN Flood
- Ping of Death
- Tribe Flood Network (TFN) и Tribe Flood Network 2000 (TFN2K)

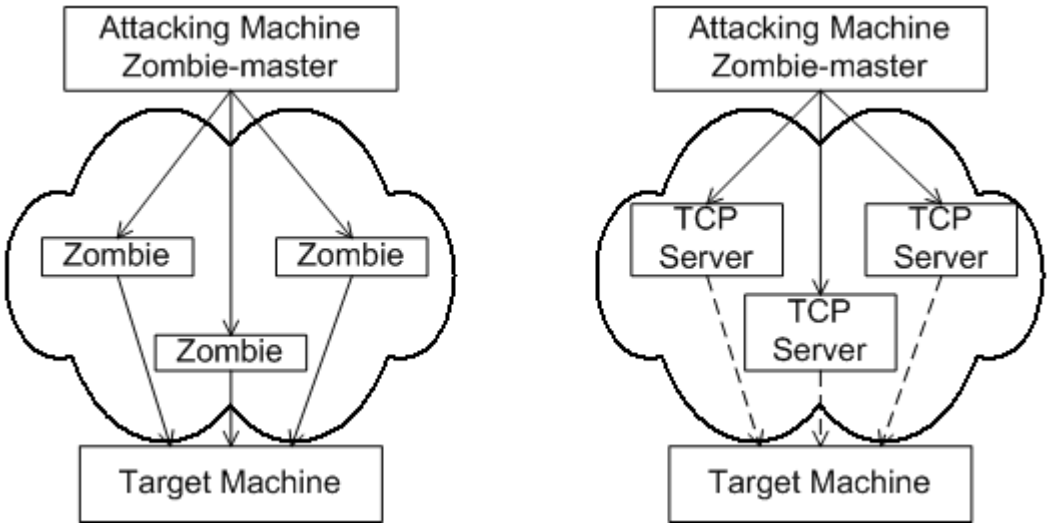
- Trinco
- Stacheldracht
- Trinity

Атаки DoS отличаются от атак других типов. Они не нацелены на получение доступа к вашей сети или на получение из нее какой-либо информации. Атака DoS делает вашу сеть недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения. В случае использования некоторых серверных приложений (таких как web-сервер или FTP-сервер) атаки DoS могут заключаться в том, чтобы занять все соединения, доступные для этих приложений, и держать их в занятом состоянии, не допуская обслуживания обычных пользователей. В ходе атак DoS могут использоваться обычные Интернет-протоколы, такие как TCP и ICMP. Большинство атак DoS опирается не на программные ошибки или бреши в системе безопасности, а на общие слабости системной архитектуры. Некоторые атаки сводят к нулю производительность сети, переполняя ее нежелательными и ненужными пакетами или сообщая ложную информацию о текущем состоянии сетевых ресурсов.

Существует две разновидности атак данного типа: DDoS (distributed denial of service) – распределенный отказ в обслуживании и DRDoS (distributed deflection denial of service) – распределенный отраженный отказ в обслуживании.

Атака типа DDoS начинается с расстановки на разных компьютерах, имеющих высокоскоростное подключение к сети, программ-ботов (Zombie), которые координируются с единой машины (Zombie-master), инициирующей атаку. Задача ботов – осуществлять непрерывную посылку пакетов (флуд) на целевой адрес (это может быть как отдельный хост, так и точка выхода целой сети). Таким образом, осуществляется перекрытие всей доступной пропускной способности (или занятие иных важных ресурсов).

Отличие атаки DRDoS от предыдущей заключается в использовании в качестве посредников между атакующим и целью легальных TCP серверов. Источник (или же несколько источников) посылает на них эхо-запросы (ping) или запросы на TCP соединение со спуфнутым (подмененным) адресом источника, в качестве которого указывает адрес цели. И ответы от многих хостов приходят в единую точку, поглощая всю пропускную способность.



а) б)

Рис. 2. Схема атак типа DoS, а) DDoS, б) DRDoS

Угроза атак типа DoS может снижаться тремя способами:

Функции анти-спуфинга. Правильная конфигурация функций анти-спуфинга на ваших маршрутизаторах и межсетевых экранах поможет снизить риск DoS. Эти функции, как минимум, должны включать фильтрацию RFC 2827. Если хакер не сможет замаскировать свою истинную личность, он вряд ли решится провести атаку.

Функции анти-DoS. Правильная конфигурация функций анти-DoS на маршрутизаторах и межсетевых экранах может ограничить эффективность атак. Эти функции часто ограничивают число полуоткрытых каналов в любой момент времени.

Ограничение объема трафика (traffic rate limiting). Если трафик, предназначенный для переполнения вашей сети, не остановить у провайдера, то на входе в сеть вы это сделать уже не сможете, потому что вся полоса пропускания будет занята. Обычным примером является ограничение объемов трафика ICMP. При заключении договора с провайдером на предоставление услуг (SLA – service level agreement), следует обговорить применение технологии ограничения доступа (CAR – committed access rate). [2]

Парольные атаки.

Хакеры могут проводить парольные атаки с помощью целого ряда методов, таких как простой перебор (brute force attack), «троянский конь», IP-спуфинг и сниффинг пакетов. Если злоумышленник, перехватив пароль, получит привилегированный доступ, он может создать для себя «проход», который будет действовать, даже если пользователь изменит уже раскрытый пароль и логин.

Прежде всего, парольных атак можно избежать, если не пользоваться паролями в текстовой форме. Одноразовые пароли и/или криптографическая аутентификация могут практически свести на нет угрозу таких атак. К сожалению, не все приложения, хосты и устройства поддерживают указанные выше методы аутентификации. При использовании обычных паролей следует придумать такой пароль, который было бы трудно подобрать. Минимальная длина пароля должна быть не менее восьми символов. Пароль должен включать символы верхнего регистра, цифры и специальные символы (#, %, $ и т.д.).

С точки зрения администратора, существует несколько методов борьбы с подбором паролей. Один из них заключается в использовании средства L0phtCrack, которое часто применяют хакеры для подбора паролей в среде Windows NT. Это средство быстро покажет вам, легко ли подобрать пароль, выбранный пользователем.

Атаки на уровне приложений.

Атаки на уровне приложений могут проводиться несколькими способами. Самый распространенный из них состоит в использовании хорошо известных слабостей серверного программного обеспечения (sendmail, HTTP, FTP). Используя их, хакеры могут получить доступ к компьютеру от имени пользователя, работающего с приложением. Сведения об атаках на уровне приложений широко публикуются, чтобы дать возможность администраторам исправить проблему с помощью коррекционных модулей (патчей). К сожалению, многие хакеры также имеют доступ к этим сведениям, что позволяет им учиться.

Главная проблема с атаками на уровне приложений состоит в том, что они часто пользуются портами, по которым разрешен проход через межсетевой экран. К примеру, хакер, эксплуатирующий известную слабость web-сервера, часто использует в ходе атаки TCP порт 80. Поскольку web-сервер предоставляет пользователям web-страницы, межсетевой экран должен предоставлять доступ к этому порту. С точки зрения межсетевого экрана, атака рассматривается как стандартный трафик.

Полностью исключить атаки на уровне приложений невозможно. Хакеры постоянно открывают и публикуют в Интернет все новые уязвимые места прикладных программ. Самое главное здесь — хорошее системное администрирование. Вот некоторые меры, которые можно предпринять, чтобы снизить уязвимость от атак этого типа:

1. Чтение лог-файлов операционных систем и сетевых лог-файлов, их анализ с помощью специальных программ.
2. Оформление подписки на услуги по рассылке данных о слабых местах прикладных программ: Bugtrad (http://www.securityfocus.com) и CERT (http://www.cert.com).
3. Использование самых свежих версий операционных систем и приложений и самых последних коррекционных модулей (патчев).
4. Использование программно-аппаратных систем распознавания атак (IDS).

Сетевая разведка.

Сетевой разведкой называется сбор информации о сети с помощью общедоступных данных и приложений. При подготовке атаки против какой-либо сети хакер, как правило, пытается получить о ней как можно больше информации. Сетевая разведка проводится в форме запросов DNS, эхо-тестирования (ping sweep) и сканирования портов. Запросы DNS помогают понять, кто владеет тем или иным доменом и какие адреса этому домену присвоены. Эхо-тестирование (ping sweep) адресов, раскрытых с помощью DNS, позволяет увидеть, какие хосты реально работают в данной среде. Получив список хостов, хакер использует средства сканирования портов, чтобы составить полный список услуг, поддерживаемых этими хостами. И, наконец, хакер анализирует характеристики приложений, работающих на хостах. В результате добывается информация, которую можно использовать для взлома.

Полностью избавиться от сетевой разведки невозможно. Если, к примеру, отключить ICMP на периферийных маршрутизаторах, вы избавитесь от эхо-тестирования, но потеряете данные, необходимые для диагностики сетевых сбоев. Кроме того, сканировать порты можно и без предварительного эхо-тестирования. Просто это займет больше времени, так как сканировать придется и несуществующие IP-адреса. Системы IDS на уровне сети и хостов обычно хорошо справляются с задачей уведомления администратора о ведущейся сетевой разведке, что позволяет лучше подготовиться к предстоящей атаке и оповестить провайдера (ISP), в сети которого установлена система, проявляющая чрезмерное любопытство.

Злоупотребление доверием.

Собственно говоря, этот тип действий не является «атакой» или «штурмом». Он представляет собой злонамеренное использование отношений доверия, существующих в сети.

Классическим является ситуация в периферийной части корпоративной сети. В этом сегменте часто располагаются серверы DNS, SMTP и HTTP. Поскольку все они принадлежат к одному и тому же сегменту, взлом одного из них приводит к взлому и всех остальных, так как эти серверы доверяют другим системам своей сети.

Другим примером является система, установленная с внешней стороны межсетевого экрана, имеющая отношения доверия с системой, установленной с его внутренней стороны. В случае взлома внешней системы хакер может использовать отношения доверия для проникновения в систему, защищенную межсетевым экраном.

Риск злоупотребления доверием можно снизить за счет более жесткого контроля уровней доверия в пределах своей сети. Системы, расположенные с внешней стороны

межсетевого экрана, никогда не должны пользоваться абсолютным доверием со стороны защищенных экраном систем [4]. Отношения доверия должны ограничиваться определенными протоколами и, по возможности, аутентифицироваться не только по IP-адресам, но и по другим параметрам.

Переадресация портов.

Переадресация портов представляет собой разновидность злоупотребления доверием, когда взломанный хост используется для передачи через межсетевой экран трафика, который в противном случае был бы обязательно отбракован. Представим себе межсетевой экран с тремя интерфейсами, к каждому из которых подключен определенный хост. Внешний хост может подключаться к хосту общего доступа (DMZ), но не к хосту, установленному с внутренней стороны межсетевого экрана. Хост общего доступа может подключаться и к внутреннему, и к внешнему хосту. Если хакер захватит его, он сможет установить на нем программное средство, перенаправляющее трафик с внешнего хоста прямо на внутренний. Хотя при этом не нарушается ни одно правило, действующее на экране, внешний хост в результате переадресации получает прямой доступ в защищенную зону. Примером приложения, которое может предоставить такой доступ, является netcat.
Основным способом борьбы с переадресацией портов является использование надежных моделей доверия. Кроме того, помешать хакеру установить на хосте свои программные средства может хост-система IDS (HIDS).

Несанкционированный доступ.

Большинство сетевых атак проводятся ради получения несанкционированного доступа. Чтобы подобрать логин Telnet, хакер должен сначала получить подсказку Telnet на своей системе. После подключения к порту Telnet на экране появляется сообщение «authorization required to use this resource» (для пользования этим ресурсом нужна авторизация). Если после этого хакер продолжит попытки доступа, они будут считаться несанкционированными. Источник таких атак может находиться как внутри сети, так и снаружи.

Способы борьбы с несанкционированным доступом достаточно просты. Главным здесь является сокращение или полная ликвидация возможностей хакера по получению доступа к системе с помощью несанкционированного протокола. Что же касается межсетевого экрана, то его основной задачей является предотвращение самых простых попыток несанкционированного доступа.

Вирусы и троянские кони.

Рабочие станции конечных пользователей очень уязвимы для вирусов и «троянских коней». Борьба с ними ведется с помощью эффективного антивирусного программного обеспечения, работающего на пользовательском уровне и, возможно, на уровне сети. Антивирусные средства обнаруживают большинство вирусов и «троянских коней» и пресекают их распространение. Получение самой свежей информации о вирусах поможет эффективнее бороться с ними. Необходимо постоянно устанавливать новые версии антивирусных средств и приложений.

Эффективным средством борьбы также можно считать технологию IAS (Intelligent Application Switching) [10]. В основе лежит фильтрация на основании содержания трафика. IAS позволяет вылавливать не только вредоносные программы, но и спам. Согласно

исследованиям, приведенным в [10], некоторые компании, установившие у себя на магистралях средства IAS, освободили до 20% их пропускной способности от «мусора».

Социальная инженерия.

Часто, проектирую сетевую безопасность, забывают защититься от одного из самых простых и в то же время действенных способов взлома – социальной инженерии. Она основана на работе со служащими компании, их подкупе или введения в заблуждения. Например, хакер может позвонить служащему и, выдав себя за сетевого администратора, попросить назвать свой пароль для выполнения каких-либо действий.

Противодействие таким методам может осуществляться лишь через обучения и подготовку персонала, закрепления в политике безопасности правил поведения.

1.2.3 Атаки на втором уровне.

К атакам на 2-ом уровне относит сниффинг пакетов. Это цель, а вот способов ее достижения – несколько.

APR-взлом и CAM-переполнение.

Многие системные администраторы полагают, что подключение сервера через коммутатор является панацеей от перехвата сетевого трафика. Однако это не так. Существует ряд программ – активных снифферов, способных реализовывать такой взлом.

Активный сниффер (например, angst) способен работать в двух режимах. Первый из них называется man-in-the-middle. После старта программа начинает мониторить адреса arp-запросов, а затем включает arp forwanding на станции, где она запущена, посылая на arp-запрос ответ, что mac-адрес псевдофорвардера соответствует всем ip-адресам в данной сети.

Для своей работы коммутатор динамически строит таблицу соответствия MAC – порт. Второй метод заключается в наполнении сети ложными (спуфнутыми) MAC адресам, CAM-память коммутатора переполнится и он переходит в режим работы «концентратор» (hub). Эффект микросегментации устраняется, и сниффер начинает слушать весь трафик на своем порту.

Атака на STP.

Путем подключения устройства с низким приоритетом или при помощи инструмента генерации пакетов STP (BPDU – bridge protocol data unit) можно частично или целиком перевести на себя весь трафик VLAN и успешно его анализировать. Если злоумышленник имеет доступ к 2-ум портам на разных коммутаторах, выдавая себя за корень дерева STP, он получает трафик виртуальной локальной сети.

Если через небольшие промежутки времени хакер будет менять приоритет, заставляя протокол постоянно пересчитывать дерево, получится атака типа DoS.

Для защиты от STP-взлома компания Cisco дополнила ПО для коммутаторов парой опций:

- защита порта – запрещение порта принимать BPDU (bpdu filter)
- защита корня – запрет нахождения за данным портом корня.

Злоумышленник в большинстве случаев сможет подключиться лишь к портам доступа коммутатора. Данные меры полностью блокируют его от каких-либо воздействий на STP.

Атака на HSRP.

Протокол HSRP (Hot Standby Router Protocol) реализует избыточную эксплуатацию нескольких маршрутизаторов, доступных под одним виртуальным IP и MAC. Между собой маршрутизаторы обмениваются многоадресными (multicast) пакетами (224.0.0.2). На основе приоритета определяется активный, отвечающий за обработку и передачу всего трафика.

Если нарушитель может рассылать HSRP-пакеты с наибольшим приоритетом, он способен:

a) перевести все маршрутизаторы в неактивное состояние, реализуя таким образом атаку типа DoS
b) перевести на себя весь трафик

Для защиты рекомендуется использовать протокол IPSec для шифрования трафика HSRP. А в версиях IOS 12.3(2)T и новее применять MD5 аутентификацию.

Наиболее известным инструментом атаки на HSRP и STP является Irpas.

Атака на DTP и VTP.

Обычно администраторы вручную конфигурируют все транковые порты. Однако этот процесс можно автоматизировать применением DTP. Коммутаторы сами будут определять, что за устройства подключены к портам и, при необходимости, переводить его в режим магистрали.

Процесс настройки параметров виртуальных локальных сетей можно автоматизировать применением VTP. Тогда, настроив VLAN на VTP-сервере, на клиентах этого делать уже не придется.

По умолчанию DTP находится в режиме «активирован». Таким образом, подключаясь к порту доступа, хакер завладевает транком. Он способен осуществлять:

a) чтение широковещательного и многоадресного трафика всех виртуальных локальных сетей (в том числе, протоколов маршрутизации OSPF и EIGRP)
b) участие в VTP, изменение настроек VLAN
c) спуфинг ARP

Для защиты необходимо не забывать изменять настройки по умолчанию, блокировать режим магистрали на портах доступа.

§1.3 Технологии безопасности данных.

1.3.1 Технологии аутентификации.

S/Key

Система S/Key, определенная в RFC 1760, представляет собой схему генерирования одноразовых паролей на основе стандартов MD4 и MD5. Она предназначена для борьбы с перехватом паролей.

Протокол S/Key основан на технологии клиент/сервер, где клиентом обычно является персональный компьютер, а сервером — сервер аутентификации. Вначале и клиента, и сервер нужно настроить на единую парольную фразу и счет итерации. Клиент начинает обмен

S/Key, отправляя серверу пакет инициализации, а сервер в ответ отправляет порядковый номер и случайное число – «зерно» (seed). После этого клиент генерирует одноразовый пароль в ходе операции, состоящей из трех этапов:

- подготовительного этапа
- этапа генерирования
- функции выхода

На подготовительном этапе клиент вводит секретную парольную фразу, которая соединяется с «зерном», полученным от сервера в незашифрованном виде.

Далее, на этапе генерирования, клиент многократно использует хэш-функцию и получает 64-разрядную итоговую величину. При каждом новом использовании количество хэш-циклов уменьшается на один, создавая тем самым уникальную последовательность генерируемых паролей. Для совместимости клиента и сервера они должны использовать одну и ту же защищенную хэш-функцию.

Функция выхода воспринимает 64-разрядный одноразовый пароль и переводит его в читаемую форму.

Аутентификация с помощью аппаратных средств.
Token Password Authentication.

Аутентификация с помощью аппаратных средств работает по одной из двух альтернативных схем: запрос-ответ или синхронизация по времени.

В первом случае пользователь подключается к серверу аутентификации, который в свою очередь предлагает ввести персональный аутентификационный номер (PIN). Затем сервер передает случайное число, которое пользователь вводит в специальное аппаратное устройство, где оно шифруется с помощью пользовательского ключа. Далее результат отправляется на сервер аутентификации. Получив ответ от пользователя, сервер сравнивает его с собственным, полученным с помощь пользовательского ключа, хранящегося в базе данных. Если оба результата совпадают, разрешается доступ к сети.

При использовании схемы с синхронизацией по времени на аппаратном устройстве пользователя и на сервере работает секретный алгоритм, который через определенные синхронизированные промежутки времени генерирует идентичные пароли и заменяет старые пароли на новые. Пользователь подключается к серверу аутентификации, который запрашивает у него доступа. После этого пользователь вводит свой PIN в аппаратное устройство, и в результате на экран выводится некоторая величина, которая представляет собой одноразовый пароль. Этот пароль и отправляется на сервер.

Аутентификация PPP.

PPP — это популярное средство инкапсуляции, которое часто используется в глобальных сетях. В его состав входят три основных компонента:

- метод инкапсуляции датаграмм в последовательных каналах
- протокол Link Control Protocol (LCP), который используется для установления, конфигурирования и тестирования связи
- семейство протоколов Network Control Protocols (NCP) для установки и конфигурирования различных протоколов сетевого уровня

Чтобы установить прямую связь между двумя точками по каналу PPP, каждая из этих точек должна сначала отправить пакеты LCP для конфигурирования связи на этапе ее установления. После установления связи и, прежде чем перейти к этапу работы на протоколах сетевого уровня, протокол PPP дает возможность провести аутентификацию.

Протокол PPP PAP (Password Authentication Protocol) не является сильным аутентификационным методом. Он аутентифицирует только вызывающего оператора, а пароли пересылаются по каналу, который считается уже «защищенным». Таким образом, этот метод не дает защиты от использования чужих паролей и неоднократных попыток подбора пароля.

CHAP (Challenge Handshake Authentication Protocol) используется для периодической аутентификации центрального компьютера или конечного пользователя с помощью согласования по трем параметрам. Аутентификация происходит в момент установления связи, но может повторяться и после.

CHAP обеспечивает безопасность сети, требуя от операторов обмена «текстовым секретом». Этот секрет никогда не передается по каналу связи. По завершении этапа установления связи аутентификатор передает вызывающей машине запрос, который состоит из аутентификатора (ID), случайного числа и имени центрального компьютера (для местного устройства) или имени пользователя (для удаленного устройства). Вызывающая машина проводит вычисления с помощью односторонней хэш-функции, на вход которой подаются аутентификатор, случайное число и общий «текстовый секрет». После этого вызывающая машина отправляет серверу ответ, который состоит из хэша и имени центрального компьютера или имени пользователя удаленного устройства. По получении ответа аутентификатор проверяет проставленное в ответе имя и выполняет те же вычисления. Затем результат этих вычислений сравнивается с величиной, проставленной в ответе. Если эти величины совпадают, результат аутентификации считается положительным, система выдает соответствующее уведомление, и LCP устанавливает связь.

PPP EAP (Extensible Authentication Protocol) является общим протоколом аутентификации PPP, который поддерживает множество механизмов (MD5, S/Key, аутентификация с использованием аппаратной карты для генерирования паролей и т.д.). Это развивающийся стандарт.

TACACS+.

TACACS+ пользуется транспортным протоколом TCP. «Демон» сервера «слушает» порт 49, который является зарезервированным для выделенных номеров RFC в протоколах UDP и TCP.

Протокол TACACS+ работает по технологии клиент/сервер, где клиентом обычно является NAS (Network Access Server), а сервером считается «демон». Фундаментальным структурным компонентом протокола TACACS+ является разделение аутентификации, авторизации и учета (AAA — Authentication, Authorization, Accounting). Это позволяет обмениваться аутентификационными сообщениями любой длины и содержания, и, следовательно, использовать для клиентов TACACS+ любой аутентификационный механизм, в том числе PPP PAP, PPP CHAP, аппаратные карты и Kerberos. Аутентификация не является обязательной. Она рассматривается как опция, которая конфигурируется на месте.

Транзакции между клиентом и сервером идентифицируются с помощью общего «секрета», который никогда не передается по каналам связи. Обычно он вручную устанавливается на обоих сторонах. TACACS+ можно настроить на шифрование всего трафика.

RADIUS.

Протокол RADIUS (RFC 2058, 2059) основан на технологии клиент/сервер. Клиентом является NAS, а сервером – «демон». Клиент передает пользовательскую информацию на определенный сервер RADIUS, а затем действует в соответствии с полученными от него инструкциями. Серверы RADIUS принимают запросы пользователей на подключение, проводят аутентификацию пользователей, а затем отправляют всю конфигурационную информацию.

Обычно регистрация пользователя состоит из запроса (Access Request), который поступает от NAS на сервер RADIUS, производящий поиск указанного имени пользователя в базе данных. Если такого имени там нет, то сервер загружает профиль по умолчанию, или отправляет пользователю отрицательный ответ. В положительном ответе приводится список пар атрибутов для данной сессии (авторизация).

Учетные функции RADIUS позволяют в начале и в конце каждой сессии отправлять данные о количестве использованных ресурсов.

Транзакции между клиентом и сервером RADIUS аутентифицируются с помощью общего «секрета», который никогда не передается по сетевым каналам. Кроме того, обмен любыми пользовательскими идет только в зашифрованном виде, что исключает подслушивание чужих паролей.

1.3.2 Технологии целостности и конфиденциальности.

SSL.

SSL (Secure Socket Layer) — это открытый протокол, разработанный компанией Netscape. Он определяет механизм безопасности данных между уровнем приложений (HTTP, Telnet, NNTP, FTP,…) и транспортным протоколом TCP/IP, и поддерживает шифрование данных, аутентификацию серверов, целостность сообщений и (в качестве опции) аутентификацию клиентов в канале TCP/IP.

Основная цель протокола состоит в том, чтобы обеспечить защищенность и надежность связи между двумя подключенными друг к другу приложениями. SSL состоит из двух уровней: нижний располагается поверх надежного транспортного протокола TCP и называется SSL Record Protocol. Он используется для встраивания различных протоколов верхнего уровня, одним из которых является SSL Handshake Protocol, позволяющий серверу и клиенту аутентифицировать друг друга и согласовывать алгоритм шифрования и криптографические ключи.

Протокол SSL поддерживает безопасность связи, придавая ей следующие свойства:

- Защищенность – после первоначального квитирования связи применяются средства шифрования, и определяется секретный ключ. Для шифрования данных используются средства симметричной криптографии (например, DES, RC4 и т.д.).
- Участник сеанса связи может быть аутентифицирован и с помощью общих ключей, то есть средствами асимметричной криптографии (например, RSA, DSS и т.д.).
- Надежность – транспортные средства проводят проверку целостности сообщений с помощью зашифрованного кода, для вычисления которого используются безопасные хэш-функции (SHA, MD5 и т.д.).

SSL принят только в рамках HTTP. Хотя и другие протоколы доказали свою способность работать с ним, используют ее они не часто.

SSH.

Протокол Secure Shell (SSH) предназначен для защиты удаленного доступа и других сетевых услуг. Он поддерживает безопасный удаленный вход в сеть, безопасную передачу файлов и безопасную эстафетную передачу сообщений по протоколам TCP/IP и X11. SSH может автоматически шифровать, аутентифицировать и сжимать передаваемые данные. В настоящее время он достаточно хорошо защищен от криптоанализа и протокольных атак. SSH довольно хорошо работает при отсутствии глобальной системы управления ключами и инфраструктуры сертификатов, а при необходимости может поддерживать существующие инфраструктуры (DNSSEC, X.509 и др.).

Протокол SSH состоит из трех основных компонентов:

- Протокол транспортного уровня, обеспечивающий аутентификацию сервера, конфиденциальность, целостность данных с отличной защищенностью эстафетной передачи, и компрессию.
- Протокол аутентификации пользователя, позволяющий серверу аутентифицировать клиента.
- Протокол соединения, мультиплексирующий зашифрованный туннель, создавая в нем несколько логических каналов.

Для шифрования используются алгоритмы и схемы IDEA, 3DES, DES, RC4-128, Blowfish, AES. Обмен ключами происходит с помощью RSA, а данные, использованные при этом обмене, уничтожаются каждый час (ключи нигде не сохраняются).

S-HTTP.

Клиенты и серверы S-HTTP допускают использование нескольких стандартных форматов криптографических сообщений. Протокол поддерживает только операции с симметричными шифровальными ключами. Хотя S-HTTP может пользоваться преимуществами глобальных сертификационных инфраструктур, для его работы такие структуры не обязательны.

Протокол S-HTTP обеспечивает безопасные сквозные (end-to-end) транзакции, что выгодно отличает его от базовых механизмов аутентификации HTTP, которые требуют, чтобы клиент попытался получить доступ и получил отказ, и лишь затем включают механизм безопасности.

В S-HTTP используется механизм согласования опций, криптографических алгоритмов – RSA или Digital Signature Standard [DSA] для подписи, DES или RC2 для шифрования и т.д.

Протокол не получил широкого распространения.

SOCKS.

SOCKS v4 решает вопрос незащищенного пересечения межсетевых экранов приложениями клиент/сервер, основанными на протоколе TCP, включая Telnet, FTP и популярные информационные протоколы, такие как HTTP, Wide Area Information Server (WAIS) и GOPHER. SOCKS v5, RFC 1928, включает в себя UDP (хотя и не масштабированное решение[4]), расширяет общую рамочную структуру, придавая ей

возможность использования мощных обобщенных схем аутентификации, и расширяет систему адресации, включая в нее имя домена и адреса IP v6.

Функционирование SOCKS заключается в замене стандартных сетевых системных вызовов в приложении их специальными версиями, которые устанавливают связь с прокси-сервером SOCKS (он конфигурируется самим пользователем в приложении или системным файлом конфигурации), подключаясь к хорошо известному порту (обычно это порт 1080/TCP). После установления связи с сервером SOCKS приложение отправляет серверу имя машины и номер порта, к которому хочет подключиться пользователь. Сервер SOCKS реально устанавливает связь с удаленным центральным компьютером, а затем прозрачно передает данные между приложением и удаленной машиной. При этом пользователь даже не подозревает, что в канале связи присутствует сервер SOCKS.

Трудность с использованием SOCKS состоит в том, что кто-то должен проводить работу по замене сетевых системных вызовов версиями SOCKS (этот процесс обычно называется «SOCKS-ификацией» приложения). К счастью, большинство обычных сетевых приложений (Telnet, FTP, finger, whois) уже SOCKS-ифицированы, и многие производители включают поддержку SOCKS в свои коммерческие приложения.

IPSec.

Этот протокол используется для защиты данных и аутентификации на уровне IP. Текущие стандарты IPSec включают независимые от алгоритмов базовые спецификации, RFC 2401 – 2412.

IPSec построен на применении двух протоколов для осуществления взаимодействия: ESP (Encrypting Security Payload), отвечающий за шифрование, и IKE (Internet Key Exchange), используемый для согласования методов и ключей.

Существует два режима работы IPSec: транспортный и туннельный.

В транспортном режиме происходит шифрование лишь поля данных IP-пакета, а заголовок остается нетронутым. Если хакер будет прослушивать сеанс, он получит только адреса сторон, а информация останется закрытой.

В туннельном режиме происходит полное шифрование пакета и добавления нового заголовка. Такую схему взаимодействия удобно использовать для организации связи двух отделений организации с применением технологии VPN. Перехваченные (например, на магистрали провайдера) сообщения не дают возможности злоумышленнику раскрыть даже внутреннюю структуру частной сети.

X.509

X.509 определяет форматы данных и процедуры распределения общих ключей с помощью сертификатов с цифровыми подписями, которые проставляются сертификационными органами CA (Certificate Authority).

Каждый сертификат состоит из трех основных полей: текста сертификата, алгоритма подписи и самой подписи. В тексте сертификата указывается номер версии, серийный номер, имена эмитента и субъекта, общий ключ для субъекта, срок действия (дата и время начала и окончания действия сертификата). Иногда в этом тексте содержится дополнительная опционная информация, которую помещают в уникальные поля, связывающие пользователей или общие ключи с дополнительными атрибутами. Алгоритм подписи – это алгоритм, который использует CA для подписи сертификата. Подпись создается пропусканием текста сертификата через одностороннюю хэш-функцию. Величина, получаемая на выходе,

зашифровывается частным ключом CA. Результат этого шифрования и является цифровой подписью.

CRL представляет собой список отозванных сертификатов с указанием времени. Он подписывается CA и свободно распространяется через общедоступный репозиторий. В списке CRL каждый отозванный сертификат опознается по своему серийному номеру. Когда у какой-то системы возникает необходимость в использовании сертификата (например, для проверки цифровой подписи удаленного пользователя), эта система не только проверяет подпись сертификата и срок его действия, но и просматривает последний из доступных списков CRL, проверяя, не отозван ли этот сертификат.

1.3.3 Технологии удаленного доступа к VPN.

L2F.

Протокол эстафетной передачи на втором уровне (Layer 2 Forwarding — L2F) был разработан компанией Cisco Systems. Он обеспечивает туннелирование протоколов канального уровня (то есть фреймов HDLC, async HDLC или SLIP) с использованием протоколов более высокого уровня, например, IP. С помощью таких туннелей можно разделить местоположение сервера удаленного доступа, к которому подключается пользователь, используя местные коммутируемые линии связи, и точки, где происходит непосредственная обработка протокола удаленного доступа (SLIP, PPP), и пользователь получает доступ в сеть.

Построенные на L2F туннели дают возможность использовать приложения, требующие удаленного доступа с частными адресами IP, IPX и AppleTalk через протокол SLIP/PPP по существующей инфраструктуре Интернет.

PPTP.

Сквозной туннельный протокол Point-to-Point Tunneling Protocol (PPTP) создан корпорацией Microsoft. Он никак не меняет PPP, но предоставляет для него новое транспортное средство. В рамках этого протокола определяется архитектура клиент/сервер, предназначенная для разделения функций, которые существуют в текущих NAS (Network Access Server), и для поддержки виртуальных частных сетей (VPN). Сервер сети PPTP (PNS – PPTP Network Server) должен работать под управлением операционной системы общего назначения, а клиент, который называется концентратором доступа к PPTP (PAC – PPTP Access Concentrator), работает на платформе удаленного доступа.

PPTP определяет протокол управления вызовами, который позволяет серверу управлять удаленным коммутируемым доступом через телефонные сети общего пользования (PSTN) или цифровые каналы ISDN или инициализировать исходящие коммутируемые соединения. PPTP использует механизм общей маршрутной инкапсуляции GRE (Generic Routing Encapsulation) для передачи пакетов PPP, обеспечивая при этом контроль потоков и сетевых заторов. Безопасность данных в PPTP может обеспечиваться при помощи протокола IPSec.

L2TP.

Протоколы L2F и PPTP имеют сходную функциональность. Компании Cisco и Microsoft согласились вместе (в рамках IETF) разработать единый стандартный протокол, который получил название туннельного протокола второго уровня (Layer 2 Tunneling Protocol

— L2TP). Обе компании будут и далее поддерживать свои собственные решения для виртуальных частных сетей (L2F и PPTP), а также путь перехода от этих решений к L2TP.

§1.4 Безопасный дизайн Cisco SAFE

1.4.1 Обзор архитектуры

SAFE представляет собой архитектуру безопасности, которая призвана предотвратить нанесение хакерами серьезного ущерба ценным сетевым ресурсам. Данный подход к проектированию корпоративных сетей является устойчивым и масштабируемым. Устойчивость достигается за счет избыточности на физическом уровне, а масштабируемость обеспечивается иерархическим подходом. Принцип модульности позволяет учитывать политики безопасности, складывающиеся между различными функциональными блоками сети. [1,4,5] .

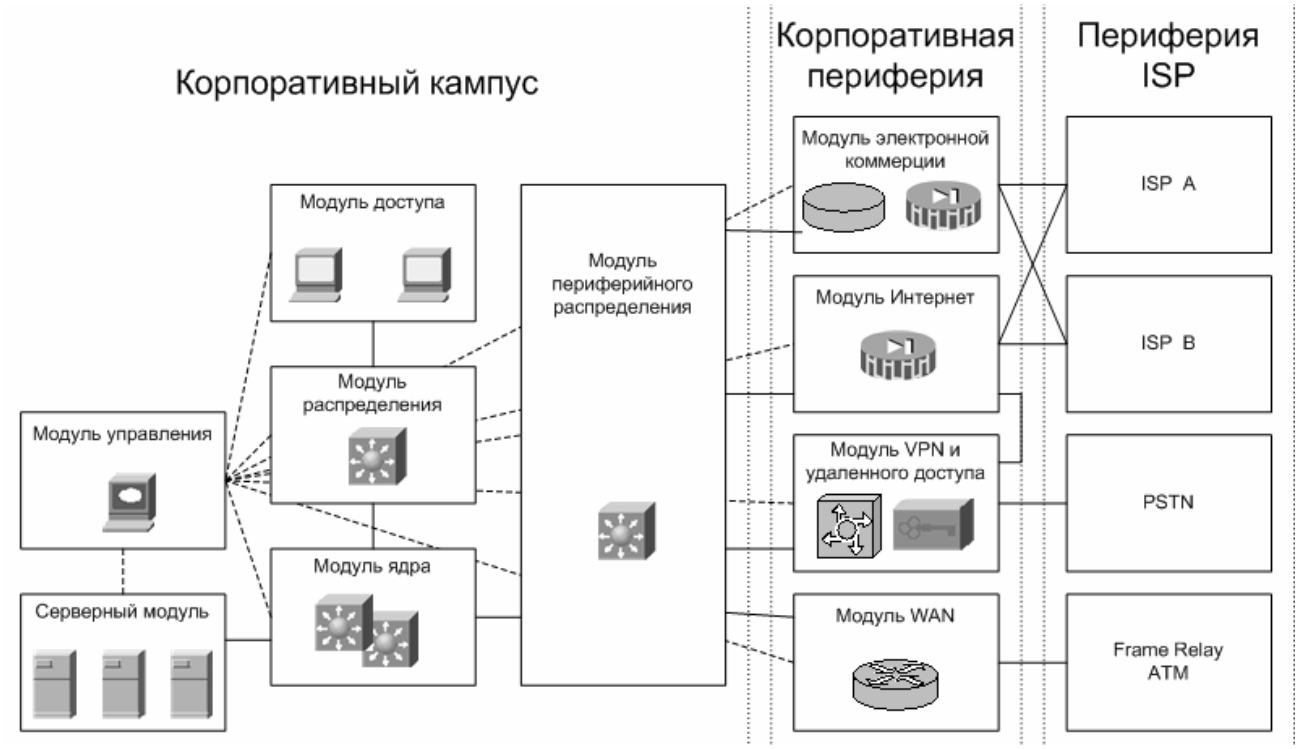


Рис. 3. Модульная схема корпоративной системы SAFE.

1.4.2 Корпоративный кампус.

Модуль управления.

Главная цель данного модуля состоит в обеспечении безопасного управления всеми устройствами в корпоративной архитектуре SAFE. Хосты управления принимают потоки отчетности и информации для лог-файлов и отправляют обновления конфигурации и ПО.

Основные устройства:

1. Хост управления SNMP — поддерживает функции управления устройствами по протоколу SNMP
2. Хост NIDS — собирает сигналы тревоги по всем устройствам NIDS в сети
3. Хост(ы) Syslog — получают информацию от межсетевого экрана и хостов NIDS
4. Сервер контроля доступа — обеспечивает аутентификацию доступа к сетевым устройствам с помощью однократных паролей
5. Сервер одноразовых паролей — авторизует информацию по однократным паролям, поступающую с сервера контроля доступа
6. Хост системного администратора — обеспечивает изменение конфигурации устройств и их ПО
7. Устройство NIDS — позволяет мониторить потоки трафика между хостами управления и управляемыми устройствами
8. Коммутатор Уровня 2 – обеспечивает передачу данных с управляемых устройств только на маршрутизатор с функциями межсетевого экрана.

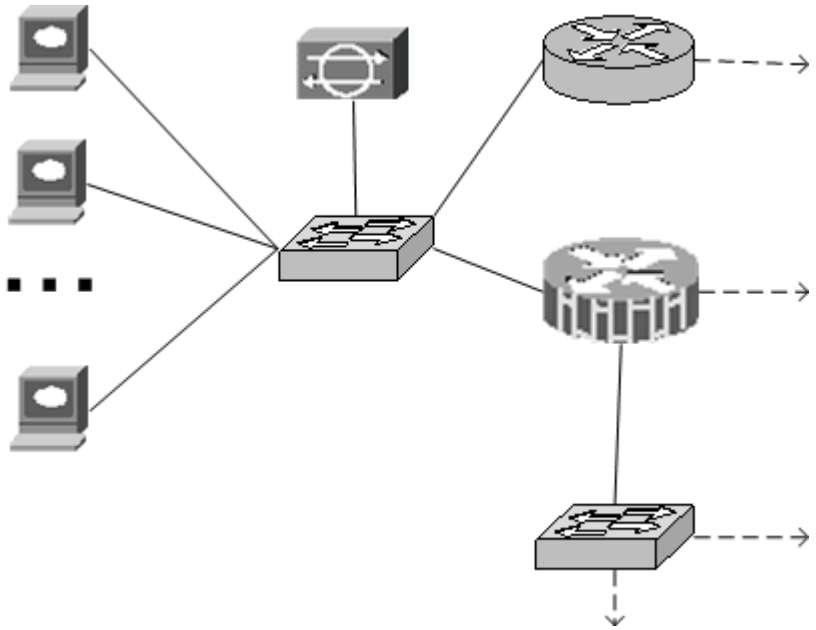


Рис. 4. Модуль управления.

Корпоративная сеть управления имеет два сетевых сегмента, которые разделены маршрутизатором, выполняющим роль межсетевого экрана и устройства терминирования VPN. Сегмент, находящийся с внешней стороны, соединяется со всеми устройствами, нуждающимися в управлении. Сегмент, находящийся с внутренней стороны, включает хосты управления и маршрутизаторы, которые выступают в качестве терминальных серверов. Другой интерфейс подключается к производственной сети, но лишь для передачи защищенного средствами IPSec трафика управления с заранее определенных хостов.

Сети управления и производственная работают в разных адресных пространствах. В результате протоколы маршрутизации не распространяют данные о сети управления.

Устройства производственной сети блокируют любой трафик, попадающий из сети управления в производственные сегменты.

Хосты, не подключенные к сети управления напрямую, связываются с ней через туннели IPSec, которые идут от маршрутизатора управления.

Поскольку сеть управления имеет доступ с правами администратора практически ко всем областям сети, она может стать весьма привлекательной целью для хакеров. Поэтому в модуль управления встроено сразу несколько технологий, специально предназначенных для смягчения подобных рисков.

Сниффинг паролей вообще оказывается неэффективным, поскольку они являются одноразовыми. Кроме того, в подсети управления устанавливаются системы HIDS и NIDS, которые настраиваются на очень жесткий режим. Поскольку в этой подсети передается весьма ограниченное количество типов трафика, любое совпадение сигнатуры должно вызывать немедленную реакцию.

Даже если хакеру удастся захватить один из хостов управления, технология private VLAN помешает ему атаковать с него остальные.

Большое значение для правильного управления сетью имеет сбор и анализ системной информации (syslog). Syslog предоставляет важные данные о нарушениях безопасности и изменениях конфигурации.

Модуль ядра.

Задача модуля ядра состоит в маршрутизации и коммутации межсетевого трафика с как можно более высокой скоростью.

Основным устройством является коммутатор уровня 3.

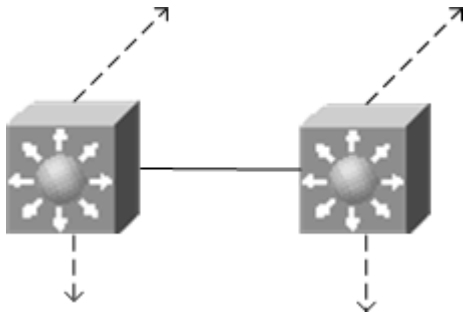


Рис. 5. Модуль ядра (распределительный модуль, модуль периферийного распределения).

Архитектура SAFE не предъявляет никаких особенных требований к данному модулю. Крайне важным является правильная настройка оборудования, но не в ущерб производительности.

Модуль распределения.

Этот модуль предоставляет услуги доступа коммутаторам здания, включающие маршрутизацию, поддержку QoS и контроль доступа. Запросы о предоставлении данных поступают на коммутаторы и далее в базовую сеть (ядро). Ответный трафик следует по тому же маршруту в обратном направлении.

Основными устройствами также являются коммутаторы 3 уровня.

Распределительный модуль представляет собой первую линию обороны и предотвращения атак, источник которых находится внутри корпорации. С помощью средств

контроля доступа снижается вероятность получения одним отделом конфиденциальной информации с сервера другого отдела.

Модуль доступа.

Главная цель этого модуля состоит в предоставлении услуг конечным пользователям.

Основные устройства:

1. Коммутатор Уровня 2
2. Пользовательская рабочая станция
3. IP-телефон

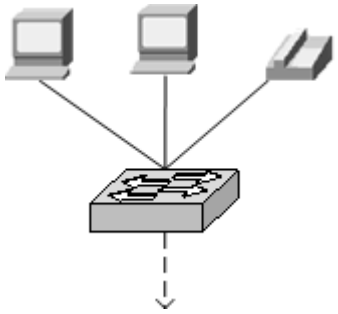


Рис. 6. Модуль доступа.

На рабочих станциях осуществляется сканирование программ на наличие вирусов. На коммутаторах реализуются требования по безопасности 2-го уровня (port-security, правильная настройка режимов работы портов и т.д.).

Серверный модуль.

Основная задача серверного модуля состоит в предоставлении прикладных услуг устройствам и конечным пользователям. Потоки трафика в проверяются средствами IDS, встроенными в коммутаторы Уровня 3.

Основные устройства:

1. Коммутатор Уровня 3
2. CallManager — выполняет функции маршрутизации вызовов для устройств IP-телефонии, установленных на предприятии.
3. Корпоративные серверы и серверы отделов — оказывают рабочим станциям услуги по обработке файлов, услуги печати и DNS.
4. Сервер электронной почты — оказывает корпоративным пользователям услуги SMTP и POP3.

Надежную защиту дает сочетание систем HIDS, NIDS, частных виртуальных локальных сетей (PVLAN), средств контроля доступа и эффективных процедур системного администрирования (включая установку самых свежих версий ПО и коррекционных модулей).

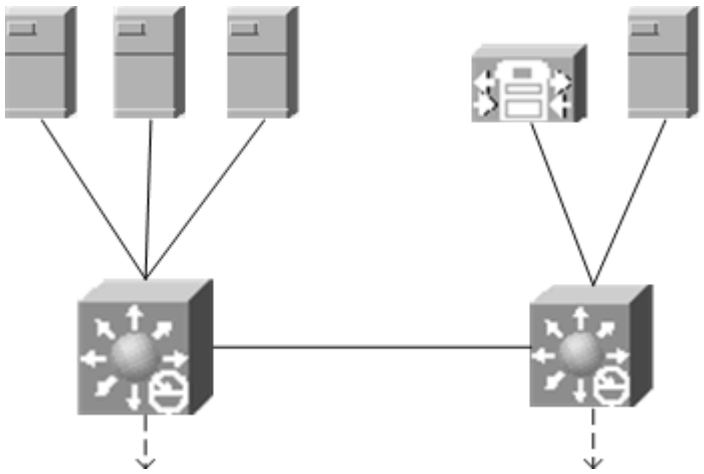


Рис. 7. Серверный модуль.

Поскольку системы NIDS могут анализировать ограниченный объем трафика, очень важно отправлять для анализа лишь тот, который в наибольшей степени подвержен хакерским атакам. В разных сетях этот трафик может быть разным, но, как правило, он включает SMTP, Telnet, FTP и WWW.

Модуль периферийного распределения.

Задача этого модуля состоит в агрегации соединений разных элементов на сетевой периферии. Трафик фильтруется и направляется с периферийных модулей в базовую сеть.

Основные устройства:

Коммутаторы Уровня 3 — агрегируют периферийные соединения и предоставляют продвинутые услуги.

По своей общей функциональности периферийный распределительный модуль похож на распределительный модуль здания. Оба модуля пользуются средствами контроля доступа для фильтрации трафика, хотя ряд возможностей сетевой периферии позволяет периферийному распределительному модулю поддерживать дополнительные функции безопасности. Для поддержки высокой производительности оба модуля пользуются коммутацией Уровня 3, но периферийный распределительный модуль обладает дополнительными возможностями в области безопасности, поскольку на сетевой периферии требования к производительности не столь высоки. Периферийный распределительный модуль представляет собой последнюю линию обороны для всего трафика, который передается с периферийного модуля на кампусный модуль. Эта линия должна пресекать попытки передачи пакетов с ложных адресов и несанкционированного изменения маршрутов, а также обеспечивать контроль доступа на уровне сети.

1.4.3 Корпоративная периферия.

Интернет модуль.

Интернет-модуль предоставляет внутрикорпоративным пользователям доступ к интернет услугам и информации, расположенной на серверах общего доступа. Трафик отсюда передается также на модуль VPN и удаленного доступа.

Основные устройства:

1. Сервер SMTP — является мостом между Интернет и почтовыми серверами, проверяет содержание.
2. Сервер DNS — служит внешним сервером DNS для предприятия, передает в Интернет запросы внутренних пользователей.
3. Сервер FTP/HTTP — предоставляет открытую информацию об организации.
4. Межсетевой экран — защищает ресурсы на уровне сети и производит фильтрацию трафика.
5. Устройство NIDS — поддерживает мониторинг ключевых сетевых сегментов модуля на Уровнях 4–7.
6. Сервер фильтрации URL — отсеивает несанкционированные запросы URL, исходящие от предприятия.

В основе модуля лежит пара отказоустойчивых межсетевых экранов, защищающих общедоступные услуги Интернет и внутренних пользователей. Они гарантируют пропускание только санкционированного трафика.

Начиная с маршрутизатора ISP, происходит реализация технологии CAR (ограничение уровня доступа), что в значительной степени снижает угрозу атак типа (D)DoS. Кроме того, на выходе маршрутизатора ISP производится фильтрация RFC 1918 и 2827, что снижает угрозу спуфинга.

На входе первого маршрутизатора корпоративной сети производится базовая фильтрация, пропускающая только ожидаемый по адресам и IP-услугам трафик. Любой трафик IPSec, адресованный на модуль VPN/удаленного доступа, передается по назначению.

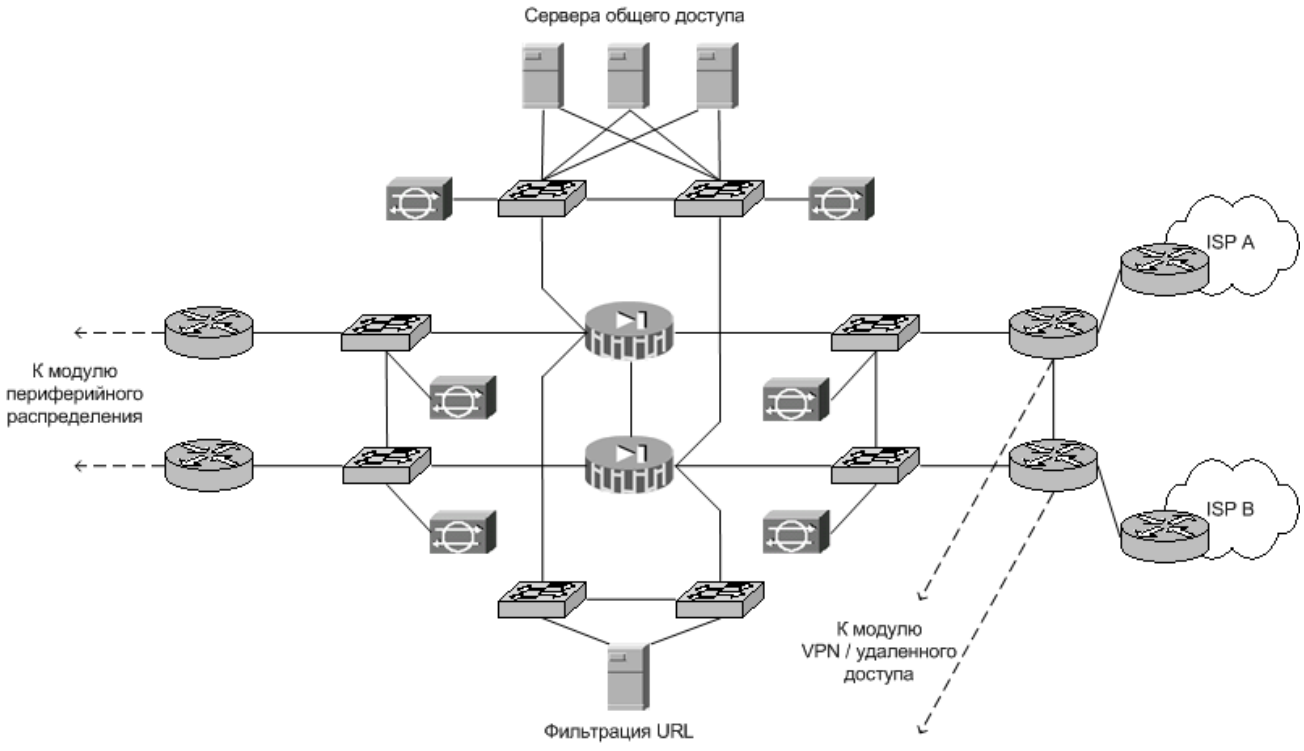


Рис. 8. Интернет модуль.

Устройство NIDS, которое находится с внешней стороны межсетевого экрана, производит мониторинг атак, анализируя Уровни 4–7 и сравнивая результаты с известными

сигнатурами. Поскольку ISP и периферийный маршрутизатор корпоративной сети отфильтровывают некоторые диапазоны адресов и портов, NIDS может сконцентрировать усилия на борьбе с более изощренными атаками. И все же это устройство NIDS работает в менее строгом режиме, чем аналогичные устройства, находящиеся с внутренней стороны межсетевого экрана. Это происходит, потому, что замеченная им несанкционированная активность представляет собой не прорыв обороны, а лишь попытку.

Межсетевой экран контролирует состояние соединения и производит тщательную фильтрацию проходящих через него сессий во всех направлениях. Серверы общего доступа получают некоторую защиту от переполнения TCP_SYN за счет использования лимитов полуоткрытых соединений на межсетевом экране.

Устройство URL-фильтрации проверяет исходящий трафик на наличие несанкционированных запросов WWW (данные предоставляются третьей стороной). Это устройство напрямую связывается с межсетевым экраном и одобряет или отклоняет запросы URL, которые тот передает своему механизму URL-инспекции

На каждом сервере устанавливаются программные средства для обнаружения атак, пресекающие любую несанкционированную активность на уровне операционной системы и на уровне обычных серверных приложений (HTTP, FTP, SMTP и т.д.).

Модуль VPN и удаленного доступа.

Базовыми задачам модуля являются аутентификация и терминирования трех типов услуг для внешних пользователей: VPN удаленного доступа, пользователи с модемным доступом и VPN для связи между сайтами.

Основные устройства:

1. Концентратор VPN — аутентифицирует удаленных пользователей с помощью средства расширенной аутентификации XAUTH и терминирует их туннели IPSec.
2. Маршрутизатор VPN — аутентифицирует доверенные удаленные сайты и обеспечивает связь через туннели GRE/IPSec.
3. Сервер модемного доступа — аутентифицирует индивидуальных удаленных пользователей с помощью TACACS+ и терминирует их аналоговые соединения.
4. Межсетевой экран — поддерживает свой уровень безопасности для каждого из трех типов удаленного доступа.
5. Устройство NIDS — поддерживает мониторинг ключевых сетевых сегментов данного модуля на Уровнях 4–7.

VPN удаленного доступа

Трафик VPN передается с маршрутизаторов доступа, являющихся частью корпоративного Интернет-модуля. На выходе этих маршрутизаторов трафик фильтруется по IP-адресам и протоколам, входящим в состав услуг VPN. Современные виртуальные частные сети с удаленным доступом могут пользоваться несколькими протоколами туннелирования и безопасности (IPSec, PPTP, L2TP). Трафик VPN с удаленным доступом будет направляться на единый адрес общего доступа с помощью протокола IKE. Технология XAUTH, являющаяся одним из расширений IKE, создает дополнительный механизм аутентификации пользователя, прежде чем ему будут присвоены какие-либо параметры IP. Концентратор VPN «подключается» к серверу контроля доступа через подсеть управления и интерфейс управления. При этом надежную защиту с помощью паролей предоставляет сервер однократных паролей.

После аутентификации удаленный пользователь получает доступ. Для этого ему присваиваются IP-параметры с помощью MODCFG, еще одного расширения IKE.

После терминации туннеля VPN трафик передается через межсетевой экран, где происходит необходимая фильтрация пользователей VPN.

Пользователи с модемным доступом

Традиционные пользователи с модемным доступом терминируются на одном из двух маршрутизаторов доступа, где имеются встроенные модемы. После установления связи между пользователем и сервером на Уровне 1 для аутентификации применяется протокол CHAP. Для аутентификации и предоставления паролей используются сервер AAA и сервер однократных паролей. После аутентификации пользователей им присваиваются IP-адреса, которые выбираются из IP-пула при установлении соединения протокола PPP.

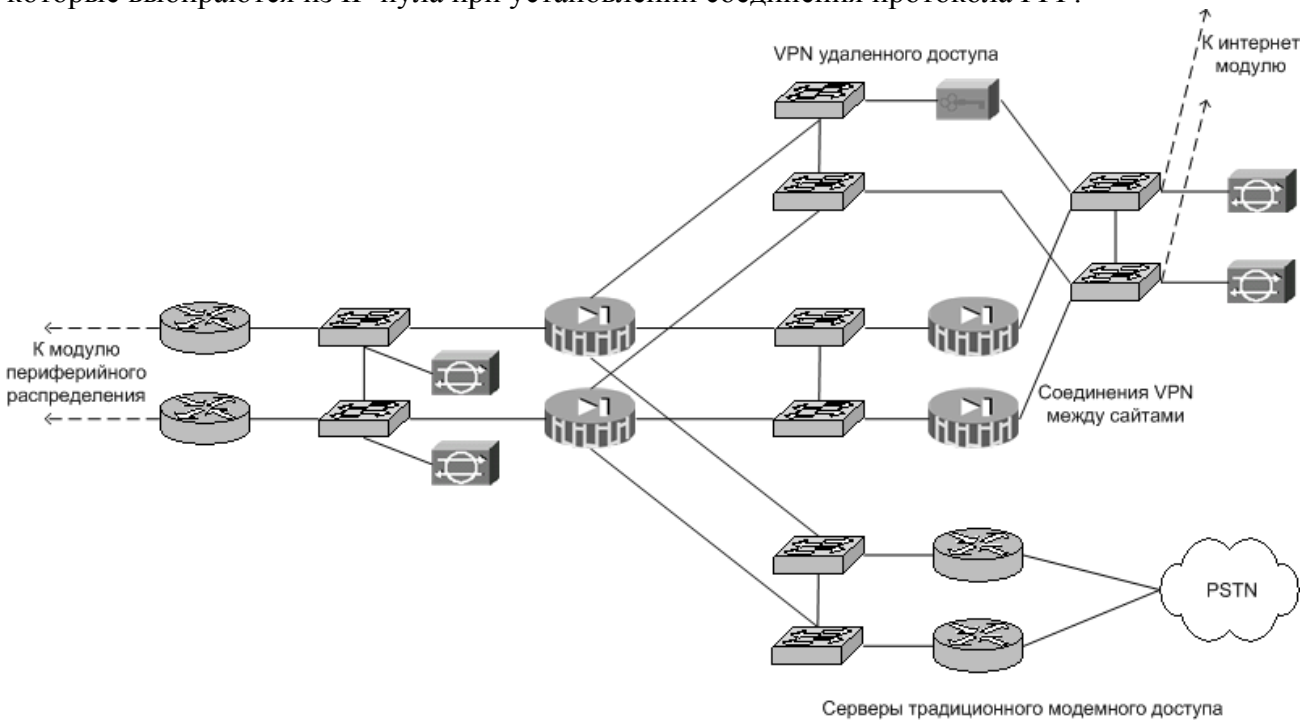


Рис. 9. Модуль VPN и удаленного доступа.

VPN для связи между сайтами

Трафик VPN, предназначенный для связи между сайтами, состоит из туннелей GRE, защищенных протоколом IPSec в транспортном режиме с использованием технологии ESP (Encapsulated Security Payload). Единственными ожидаемыми протоколами в этом канале являются ESP и протокол IKE.

Протокол GRE используется для обеспечения полнофункционального маршрутизируемого канала, по которому передается многопротокольный трафик. Здесь же поддерживаются протоколы маршрутизации и режим многоадресной передачи.

Как и в случае с VPN удаленного доступа, максимальная безопасность с приемлемым ущербом для производительности достигается с помощью алгоритмов шифрования и контроля целостности 3DES и SHAHMAC.

На маршрутизаторах VPN могут использоваться аппаратные акселераторы IPSec.

Остальные компоненты модуля

Межсетевой экран агрегирует трафик всех трех типов и направляет его на внутренний интерфейс, а затем — через пару маршрутизаторов — в периферийный распределительный модуль. На маршрутизаторе должен быть правильно настроен контроль доступа, чтобы пропускать к внутреннему интерфейсу экрана только санкционированный трафик. С внешней стороны межсетевого экрана устанавливается пара устройств NIDS для обнаружения любой «разведывательной» деятельности, направленной против устройств терминирования VPN. В этом сегменте может передаваться только трафик IPSec (IKE/ESP).

Модуль WAN.

Основными устройствами являются маршрутизаторы.

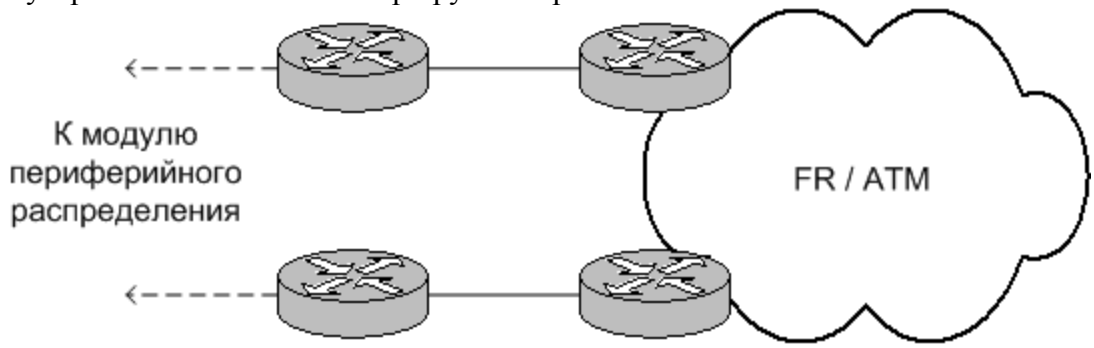


Рис. 10. Модуль WAN

Устойчивость обеспечивается двойным соединением, идущим от сервис-провайдера через маршрутизаторы к периферийному распределительному модулю. Безопасность поддерживается с помощью функций IOS. Для блокирования всего нежелательного трафика, поступающего от отделений компании, используются списки контроля доступа на входе.

Модуль электронной коммерции.

В основе архитектуры данного модуля лежит идея разделения транзакции электронной коммерции на 3 части.

Основные устройства:

1. Web-сервер — служит основным пользовательским интерфейсом для навигации по магазину электронной коммерции.
2. Сервер приложений — является платформой для различных приложений, которые требуются web-серверу.
3. Сервер баз данных — содержит критически важную информацию, которая служит основой для электронной коммерции.
4. Межсетевой экран — управляет уровнями безопасности и доступа в системе.
5. Устройство NIDS — поддерживает мониторинг ключевых сетевых сегментов в модуле.
6. Коммутатор Уровня 3 с модулем ISP — масштабируемое устройство ввода для электронной коммерции с интегрированными средствами мониторинга безопасности.

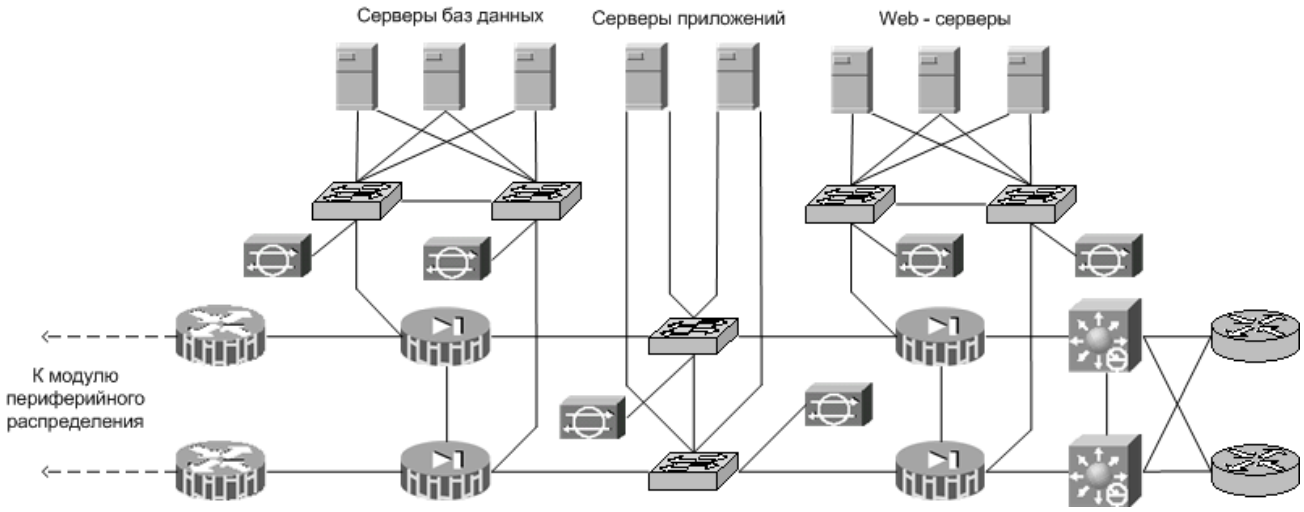


Рис. 11. Модуль электронной коммерции.

Схема данного модуля сходна с дизайном модулей интернет и VPN. Отличие заключается в использовании двух пар отказоустойчивых межсетевых экранов. Такой подход позволяет обеспечить фильтрацию каждой части транзакции.

Глава 2. Проектирование и реализация информационной безопасности.

§2.1 Схема сети. Оборудование. Адресация.

Требования к сети пресс-центра Российско-Германского саммита:

1. 30 стационарных рабочих станций
2. проводная и радио телефонная связь
3. организация радио сети (WiFi) для подключения пользователей с ноутбуками
4. создания резервных кабельных подключений для ноутбуков на случай конфликта оборудования или отсутствия сетевых карт 802.11.
5. простота и удобство подключения новых хостов
6. надежность сети

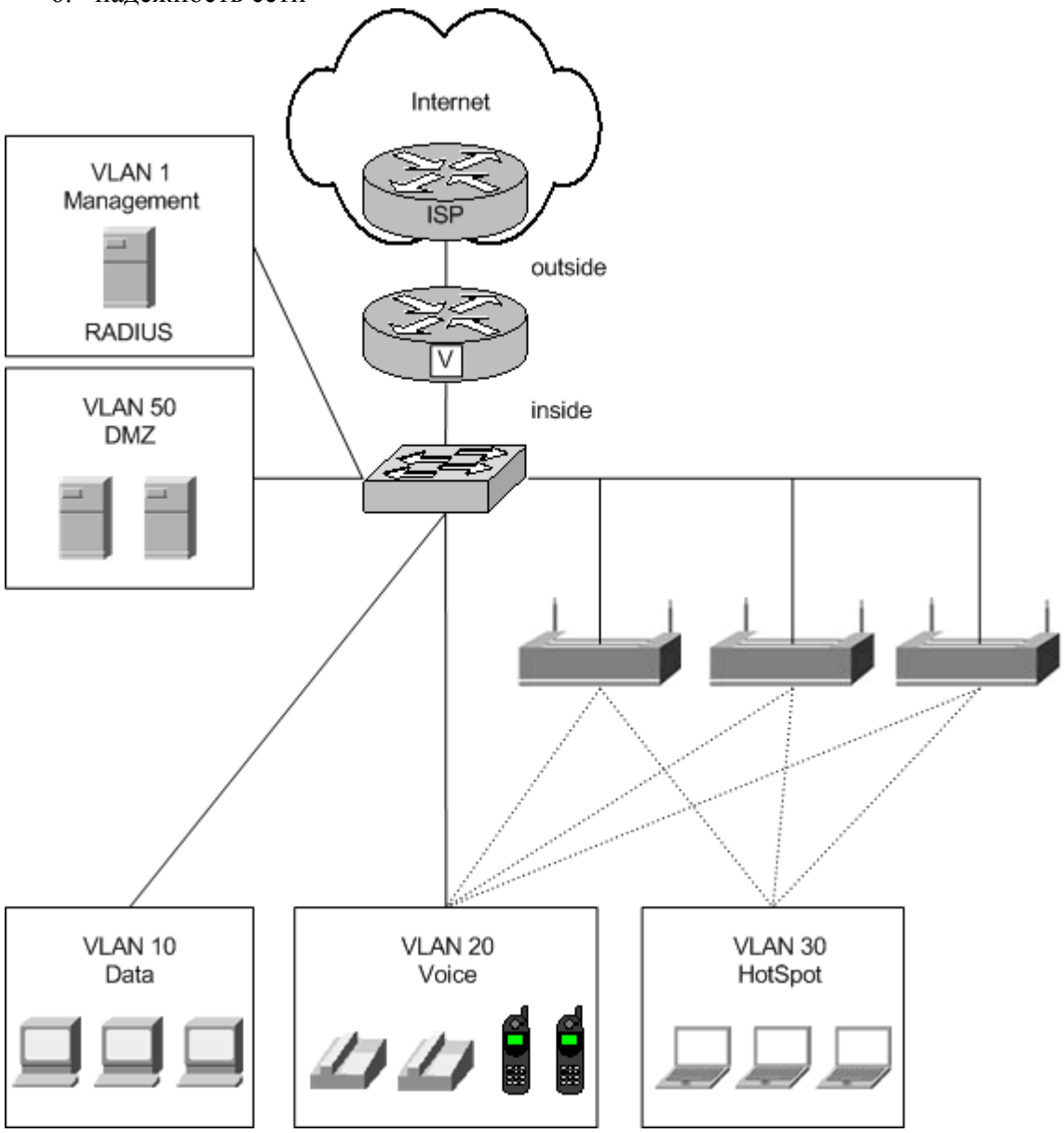


Рис. 12. Схема сети Российско-Германского саммита.

В соответствии с данными требования была разработана сеть, схема которой представлена на рисунке 12.

Маршрутизатор выполняет функции маршрутизации трафика между VLAN-ами, отвечает за управление установлением соединения телефонных вызовов, является межсетевым экраном и файерволлит внутренний и внешний трафик.

Коммутатор осуществляет подключение точек приема, устройств доступа (рабочие станции и IP-телефоны), организует виртуальные ЛВС, предоставляет функции QoS, обеспечивает безопасность на уровне портов.

Точки приема осуществляют подключение устройств доступа (рабочие станции и IP-телефоны), предоставляют функции QoS и безопасности.

В соответствии с требуемой функциональностью было принято решение использовать следующее **оборудование**:

маршрутизатор – Cisco 2811 Integrated Services Router
коммутатор – Cisco 2960 Catalyst Switch
точки приема – Cisco Aironet 1231 Access Point

Cisco 2811 Router[19]:

- обеспечивает производительность различных услуг (таких как Голос и Безопасность) на скорости носителя
- продвинутая модульность и производительность системы в целом
- поддержка более 90 существующих модулей
- 2 интегрированных порта 10/100 Fast Ethernet
- опциональная поддержка PoE (Power over Ethernet - питание по Ethernet)
- встроенное шифрование
- поддержка SDM (Security Device Manager) для простоты управления
- поддержка до 1500 VPN туннелей при использовании модуля AIM-EPII-PLUS
- антивирусная защита с помощью NAC (Network Admission Control)
- функции обнаружения и предотвращения вторжения – система IPS (Intrusion Preventing System)
- функции программного межсетевого экрана (IOS Firewall)
- поддержка аналоговых и цифровых голосовых звонков
- опциональная поддержка голосовой почты
- опциональная поддержка Cisco CME (CallManager Express) для локальной обработки вызовов (до 36 IP-телефонов)
- опциональная поддержка SRST (Survivable Remote Site Telephony) для локальной поддержки голосовых вызовов (до 36 IP-телефонов)

Cisco 2960 Catalyst Switch[20]:

- интегрированная безопасность, включая NAC (Network Admission Control)
- поддержка QoS
- 48 интегрированных портов 10/100 Fast Ethernet
- 2 интегрированных порта Gigabit Ethernet

Cisco Aironet 1231 Access Point[21]:

- поддержка стандартов IEEE 802.11a/b/g
- поддержка питания по Ethernet

- поддержка средств управления
- интегрированные функции безопасности

Адресация:

№	Название	Адрес	Описание
VLAN 1	Management	192.168.0.0/24	Управляющий доступ к оборудованию производится только из Management VLAN, здесь же располагается RADIUS сервер.
VLAN 10	Data	192.168.10.0/24	Сеть для стационарных рабочих станций по кабельному подключениею
VLAN 20	Voice	192.168.20.0/24	Сеть для голосового трафика (кабельные и радиор IP-телефоны)
VLAN 30	HotSpot	192.168.30.0/24	Сеть горячего беспроводного доступа для посетителей с ноутбуками
VLAN 40	Unused	–	VLAN для неиспользуемых портов коммутатора (как составной компонент системы безопасности)
VLAN 50	DMZ	217.80.159.0/29	Сеть для серверов публичного доступа (в частности, Proxy-сервер).

§2.2 AAA и защищенный доступ к оборудованию.

Для аутентификации доступа пользователей к оборудованию, авторизации прав и аудита действий необходимо специальным образом настраивать устройства.

Существует несколько способов реализации механизма AAA:

1. В сети управления устанавливается отдельный ACS (access control server) сервер, и все устройства проводят функции AAA через него.
2. На одном из устройств (маршрутизаторе, коммутаторе, точке доступа) запускается локальный ACS сервер, через который все устройства проводят функции AAA.
3. AAA производится на основе локальной базы данных на каждом устройстве отдельно.

AAA на основе локальной БД.

Для реализации данной технологии необходимо [1]:

1. Включить AAA на устройстве
2. Добавить учетную запись пользователя с соответствующими параметрами (имя, пароль, уровень привилегий).
3. Создать листы AAA.
4. Применить листы AAA в нужных местах.

```
Router#conf terminal
Router(config)#aaa new-model
Router(config)#username test privilege 15 secret test
Router(config)#aaa authentication login logina1 local
Router(config)#aaa authorization exec execa2 local
Router(config)#line vty 0 4
```

```
Router(config-line)#login authentication logina1
Router(config-line)#authorization exec execa2
```

AAA с отдельным ACS сервером.

Для реализации данной технологии необходимо [1]:

1. Установить в сети и настроить ACS сервер.
2. Создать на нем учетные записи пользователей.
3. На устройстве включить AAA.
4. Прописать адрес ACS сервера (серверов, если их несколько).
5. Создать листы AAA.
6. Применить листы AAA.

```
Router#conf terminal
Router(config)#aaa new-model
Router(config)#radius-server host 192.168.5.100 key test
Router(config)#username test privilege 15 secret test
Router(config)#aaa authentication login logina1 group radius
Router(config)#aaa authorization exec execa2 group radius
Router(config)#aaa accounting exec execa3 wait-start group radius
Router(config)#line vty 0 4
Router(config-line)#login authentication logina1
(Router(config-line)#authorization exec execa2
```

AAA с ACS сервером, запускаемом на отдельном устройстве (маршрутизаторе, точке доступа).

Для реализации данной технологии необходимо [15, 18]:

1. Включить на устройстве RADIUS сервер.
2. Прописать в его настройках все NAS (Network Access Server), которые должны пользоваться его услугами и их ключи доступа.
3. Создать группы пользователей (опционально).
4. Создать учетные записи пользователей, распределив их по группам.
5. В настройках AAA всех NAS использовать адрес только что созданного сервера, как ACS сервер.
6. Создать листы AAA.
7. Применить листы AAA.

```
AP1# configure terminal
AP1(config)# radius-server local
AP1(config-radsrv)# nas 192.168.0.252 key test
AP1(config-radsrv)# nas 192.168.0.251 key test
AP1(config-radsrv)# nas 192.168.0.250 key test

AP1(config-radsrv)# group voicegroup
AP1(config-radsrv-group)# vlan 20
AP1(config-radsrv-group)# ssid voice
AP1(config-radsrv-group)# reauthentication time 1800
```

```
AP1(config-radsrv-group)# group hotspotgroup
AP1(config-radsrv-group)# vlan 30
AP1(config-radsrv-group)# ssid hotspot
AP1(config-radsrv-group)# reauthentication time 1800

AP1(config-radsrv-group)# exit

AP1(config-radsrv)# user test password test group voicegroup

AP1(config)# radius-server host 192.168.0.252 key test
```

В тестовой лаборатории было проверены все три механизма. Начальным рабочим вариантом было использование отдельного ACS сервера, расположенного в сети управления. И, как частичная альтернатива, настройка одной из трех точек доступа как ACS для функций AAA для пользователей сети горячего доступа – беспроводный радио доступ для посетителей с ноутбуками.

Однако от них пришлось отказаться для снижения административных усилий при подключении новых пользователей и обеспечения удобства пользования сетью и простоты подключения.

В итоге были созданы локальные базы данных для аутентификации доступа на управление.

Для аутентификации подключения пользователей (по проводной сети к коммутатору или же через радио доступ к точкам приема) предполагалось использование протокола портовой аутентификация 802.1x.

В лабораторной конфигурации была произведена настройка коммутатора соответствующим образом. Суть протокола заключается в том, что коммутатор блокирует любые кадры кроме 802.1x от вновь подключившегося пользователя до момента окончания проведения успешной аутентификации. Также существует возможность проведения повторной аутентификации и отслеживания периода молчания хоста.

Для реализации данной технологии необходимо [6, 16]:

1. Включить 802.1x глобально на коммутаторе
2. Произвести настройку всех интерфейсов, где необходимо выставить режим работы, таймеры и опции.
3. Создать лист аутентификации через 802.1x

```
Switch(config)# aaa authentication dot1x  dot1xa1 group radius

Switch(config)# dot1x system-auth-control

Switch(config-if)# dot1x port-control  auto
Switch(config-if)# dot1x multi-hosts
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 60
Switch(config-if)# dot1x timeout quiet-period 60
Switch(config-if)# dot1x max-reauth-req 5
```

Однако от данной технологии пришлось отказаться для снижения административных усилий при подключении новых пользователей и обеспечения удобства пользования сетью и простоты подключения.

Управляющий доступ к оборудованию происходит только из Management сети. Запрещается использования открытых средств взаимодействия, таких как http и telnet.

На всех устройствах отключается http сервер:

```
Router#conf terminal
Router(config)#no ip http server
```

Разрешается лишь использование защищенного сервера по протоколу S-HTTP. И настраивается аутентификация доступа.

```
Router(config)#ip http secure-server
Router(config)#ip http authentication local
```

Вместо telnet используется протокол ssh. Для этого единственным транспортом по линиям устанавливается ssh, а telnet таким образом отключается. Настраивается аутентификация доступа.

```
Router(config)#line vty 0 4
Router(config-line)#transport input ssh
Router(config-line)#login authentication logina1
```

На межсетевом экране сеть управления закрывается от всех остальных. В нее не должны попадать пакеты из других сетей, и из нее не должно ничего исходит. Для этого необходимо добавить следующие фильтрующие правила:

```
Router(config)#access-list 101 permit ip 192.168.0.0 0.0.0.255 192.168.0.0 0.0.0.255
Router(config)#access-list 101 deny ip 192.168.0.0 0.0.0.255 any
Router(config)#access-list 101 deny ip any 192.168.0.0 0.0.0.255
```

Необходимо не забывать о следующем: все устройства (коммутатор, маршрутизатор, точки доступа) подключаются к сети управления. Соответствующая ей VLAN присутствует во всех транках (от коммутатора к маршрутизатору и точкам приема). Но ни в коем случае нельзя оставлять порты коммутатора в ней (подробнее смотри в параграфе «Безопасность на 2 уровне»), или же отдавать ее в эфир на точке доступа.

В данной сети ввиду ее компактности не были использованы протоколы маршрутизации. На маршрутизаторе был объявлен статический маршрут по умолчанию до интерфейса провайдера.

Однако не следует забывать, что в случае использования динамических протоколов необходимо предотвращать попадание в динамические обновления маршрутной информации о сети управления. В частности это можно добиться при настройке протокола маршрутизация путем не объявления в них данной сети.

§2.3 Безопасность на 2 уровне.

Вопрос безопасности на 2-ом уровне обычно касается требований, предъявляемых к настройке коммутаторов 2-го и 3-го уровней.

Во-первых, необходимо бороться со спуфингом MAC-адресов, т.к. на нем основаны многие эффективные и простые в реализации атаки. Например, установка посредничества в коммутируемой среде (см. рис. 13).

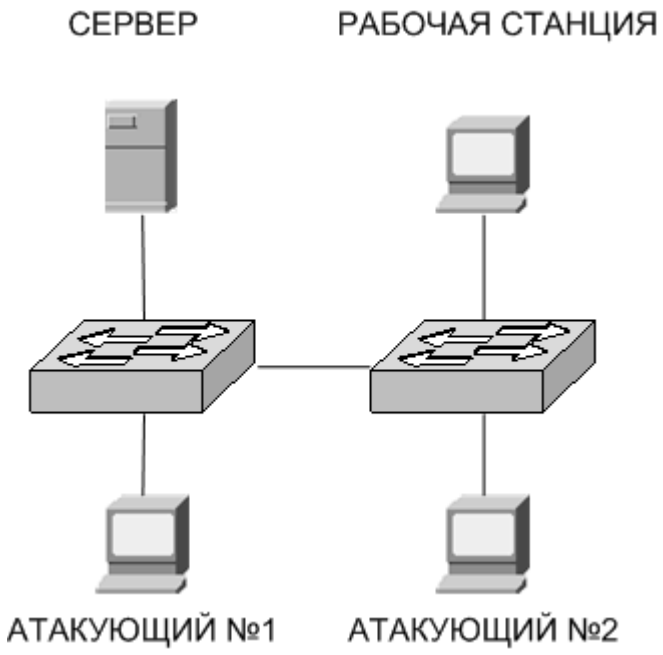


Рис. 13. Установление посредничества в коммутируемой среде.

Представим ситуацию, в которой нам необходимо стать посредником между рабочей станцией и сервером. Для этого необходимо 2 компьютера, подключенных к разным коммутаторам. Атакующий 1 вводит в заблуждение свой коммутатор относительно того, где находится рабочая станция, путем спуфинга ее MAC-адреса. Атакующий 2 вводит в заблуждение дугой коммутатор относительно местонахождения сервера путем спуфинга MAC-адреса сервера.

Таким образом, когда рабочая станция пытается что-то отправить серверу, ее коммутатор направляет эту информацию атакующему 2, тот передает ее своем напарнику 1, а тот серверу. Легко убедится, что данная цепочка работает и в обратном направлении.

Еще более простая атака через спуфинг адресов называется CAM-переполнение. CAM – это память коммутатора, где он хранит информацию о выученных соответствиях MAC-адрес – порт. Если на одном порту генерировать очень много несуществующих адресов, то вскоре память коммутатора переполнится, и он перейдет в режим концентратора. Таким образом, атакующий получит доступ ко всему сегменту сети, подключенному к коммутатору, и сможет прослушивать чужие переговоры.

Для борьбы с данной атакой были использованы возможности, предоставляемые технологией port-security, реализованной на коммутаторах Cisco.

Данная технология позволяет ограничить количество MAC адресов, которые коммутатор может выучить с определенного интерфейса, ввести штрафные санкции на нарушения, разрешить только определенным станциям подключаться к данному порту.

В качестве санкций могут быть использоваться несколько альтернатив:

1. Перевод порта в состояние errdisable, в котором он не работает и восстанавливается либо администратором вручную, либо с помощью механизма errdisable recovery.
2. Блокировка всех пакетов с MAC адресами источника, когда количество MAC-ов, засветившихся на интерфейсе, больше установленного порога. При этом разрешенные MAC-и продолжают работать.
3. Посылка «ловушки» на устройства сбора лог-информации.

В данном конкретном случае было принято решение использовать блокировку лишних MAC-адресов, т.к. перевод порта в состояние errdisable недопустимо. Ведь оно препятствует работе санкционированных станций. А посылка ловушки лишь предупреждает, но не предотвращает атаку.

Кроме того устанавливается таймер устаревания выученных MAC-адресов, чтоб информация об уже отключившихся рабочих станциях не находилась в памяти слишком долго.

```
Switch(config-if)#switchport port-security
Switch (config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security violation protect
Switch (config-if)#switchport port-security aging static
Switch (config-if)#switchport port-security aging type inactivity
Switch (config-if)#switchport port-security aging time 1
```

Данные настройки касаются лишь портов доступа. На транках port-security отключается.

Во-вторых, узким местом в коммутируемой среде является протокол VTP. Для предотвращения несанкционированных изменений VLAN-информации, необходимо аутентифицировать VTP-сообщения. Это достигается путем настройки VTP пароля для домена.

```
Switch#vlan database
Switch(vlan-data)#vtp password test
Switch(vlan-data)#apply
```

VTP может работать на устройстве в 3 режимах:

- клиент – не может создавать, удалять, модифицировать информацию о VLAN-ах, а использует для этого информацию, получаемую от сервера.
- сервер – может создавать, удалять и модифицировать информацию о VLAN-ах, и распространять эти изменения на другие сервера и клиенты.
- прозрачный – может локально создавать, удалять, модифицировать информацию о VLAN-ах, получаемые VTP обновления не применяет на свою базу данных, лишь пересылает их дальше.

В данном случае было принято решение отключить VTP, то есть перевести коммутатор в режим transparent (прозрачный) для предотвращения манипуляций VLAN информацией со стороны возможных нарушителей.

```
Switch#vlan database
Switch(vlan-data)#vtp mode transparent
```

Злоумышленник, получивший в свое распоряжение магистраль (транк) представляет огромную опасность (см. 1.2.3 «атака на DTP»). Это достигается посредством того, что рабочая станция атакующего способна эмулировать работу протокола DTP и инкапсуляция 802.1q. После того, как магистраль получена, можно просматривать всю информацию, текущую через эту VLAN, и манипулировать VTP обновлениями. Если получить в свое распоряжение 2 магистрали (подобно тому, как это описано в 1.2.3), можно являться посредником между разными VLAN-ами.

Также одним из механизмов атаки является двойная инкапсуляция, когда злоумышленник вставляет сразу 2 заголовка 802.1q в кадр (см. рис. 14).

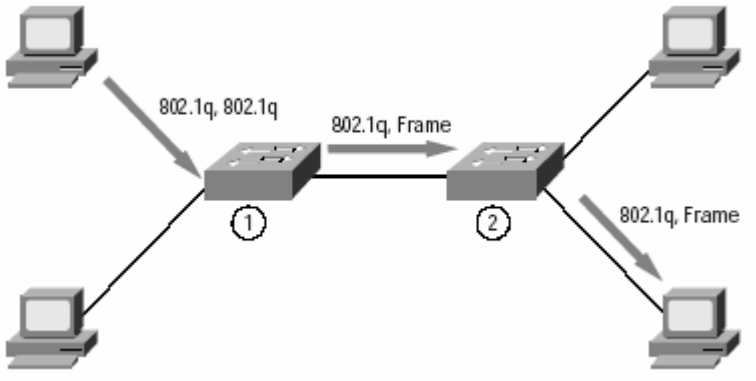


Рис. 14. Атака через двойную инкапсуляцию 802.1q.

Первый коммутатор, сталкиваясь с двойной инкапсуляцией, извлекает первый заголовок и передает кадр дальше. Второй коммутатор смотрит на оставшийся заголовок и действует в соответствии с информацией, размещенной в нем. Таким образом, если во втором заголовке 802.1q указать номер чужой VLAN, можно связаться с хостом, находящемся в ней.

Для борьбы с этими двумя угрозами необходимо правильно настраивать порты коммутатора. Было принято решение все неиспользуемые порты отключить административно (на случай страховки от административных ошибок), поместить в отдельную VLAN под название unused, и установить им тип – порт доступа (access).

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 40
Switch(config-if)#shut
```

Всем портам доступа явно выставить режим access и определить их в правильную VLAN. Также для них отключается DTP.

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#switchport nonegotiate
```

Все порты, являющиеся магистральными, на всякий случай определяются в неиспользуемую VLAN. Это делается для страховки на случай перевода порта в режим доступа административно, когда администратор забывает определить VLAN для него.
Switch(config-if)#switchport access vlan 40

Много опасностей несет в себе протокол 2-го уровня CDP, так как он сообщает соседним устройствам много частной информации. Вот пример вывода информации о соседних устройствах командой #show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
device1.cisco.com	Eth 0/1	122	T S	WS-C2900	2/11
device2.cisco.com	Eth 0/1	179	R	4500	Eth 0
device3.cisco.com	Eth 0/1	155	R	2500	Eth 0
device4.cisco.com	Eth 0/1	155	R	2509	Eth 0

Вывод команды #show cdp neighbors detail:

Device ID: device2.cisco.com
Entry address(es):
IP address: 171.68.162.134
Platform: cisco 4500, Capabilities: Router
Interface: Ethernet0/1, Port ID (outgoing port): Ethernet0
Holdtime : 156 sec
Version :
Cisco Internetwork Operating System Software
IOS(tm) 4500 Software(C4500-J-M),Version 11.1(10.4),MAINTENANCE INTERIM SOFTWARE
Copyright (c) 1986-1997 by Cisco Systems, Inc.
Compiled Mon 07-Apr-97 19:51 by dschwart

Очевидно, что такая информация не должна попасть в чужие руки. Для этого было принято решение отключить CDP на всех устройствах.

Switch(config)#no cdp run

Для повышения надежности сети необходимо создавать резервные линки. Но это приводит к образованию физических циклов в топологии. Протокол STP строит логическую древовидную структуру для поддержания работоспособности коммутируемой среды. В случае выхода из строя активных линий протокол перестраивает дерево и задействует резервные.

Если злоумышленник обладает средством генерации BPDU (Bridge Protocol Data Unit), он может наделать много бед (см. 1.2.3). В частности он может стать корнем дерева STP и гнать трафик через себя, и, манипулирую приоритетом, добиться постоянного пересчета дерева STP, что приводит к отказу работоспособности сети (DoS атака).

Для защиты от данного посягательства было принято решение отключить STP во VLAN-ах.

```
Switch(config)#no spanning-tree vlan 10
Switch(config)#no spanning-tree vlan 20
Switch(config)#no spanning-tree vlan 30
Switch(config)#no spanning-tree vlan 40
Switch(config)#no spanning-tree vlan 50
```

Кроме того, были использованы механизм защиты STP под названием bpdufilter. Смысл заключается в объявлении портов доступа как тупиковых, т.е. за которыми не находится коммутаторов, а, значит, на данном порту будут отбрасываться все полученные BPDU.

```
Switch(config-if)#spanning-tree bpdufilter enable
```

В данной сети принято решение использовать протокол DHCP для выдачи параметров настройки динамически подключаемым пользователям в сетях HotSpot, Data, Voice. Каждый протокол имеет свои уязвимости, в том числе и DHCP.

Существует ряд атак, направленных против данного протокола. Одной из самых распространенных является так называемое «DHCP голодание».

Для ее реализации машина злоумышленника, подключившегося к сети, постоянно отправляет сообщения DHCP request, заставляя сервер выдавать все новые и новые адреса. В какой-то момент наступает истощение DHCP пула. Далее злоумышленник объявляет себя новым DHCP сервером и начинает выдавать ложные настроечные данные.

Для борьбы с данной угрозой было принято решение использовать технологию DHCP Snooping. Ее методами является ограничение количества DHCP сообщений, проходящих через интерфейс, а также объявление надежных интерфейсов, т.е. тех, за которыми может находиться DHCP сервер.

Для использования данной технологии необходимо [14]:

1. Включить DHCP snooping глобально на коммутаторе.
2. Указать VLAN-ы, где это применять.
3. Выставить дополнительные опции (такие, например, как проверка MAC-адреса)
4. Объявить надежные и ненадежные интерфейсы.
5. Установить пороги на количество DHCP сообщений на интерфейсе.

```
ip dhcp snooping
ip dhcp snooping vlan 20
ip dhcp snooping information option
ip dhcp snooping verify mac-address

! на интерфейсе fast 0/1, к которому подключен маршрутизатор, являющийся DHCP сервером.
 ip dhcp snooping trust
 ip dhcp snooping limit rate 200

! на любом интерфейсе уровня доступа
 ip dhcp snooping limit rate 20
```

На случай создания демилитаризованной зоны был проработан вариант создания приватных виртуальных локальных сетей (private VLAN).

Для реализации данной технологии необходимо [6]:

1. Создать Private VLANs.

2. Создать первичную VLAN и проассоциировать с ней частные.
3. Сконфигурировать порты коммутатора, к которым будут подключаться сервера.

```
Switch(config)# vlan 51
Switch(config-vlan)# private-vlan isolated

Switch(config)# vlan 50
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# private-vlan association 51

Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 50  51
```

Однако данная технология доступна лишь на коммутаторах 3-го уровня (а Cisco Catalyst Switch 2960 таким не является), поэтому данная разработка так и осталась на стадии проектирования.

Иногда из-за ошибок в реализации стека протоколов или же в результате чьих-то преднамеренных действий рабочая станция, подключенная к сети, начинает генерировать слишком большое количество широковещательных кадров.

Для борьбы с широковещательным штормом следует использовать механизм storm-control, настраиваемый на интерфейсной базе коммутаторов.

Было принято решение ограничить возможности широковещания на портах доступа уровнем 5 % производительности. Ввиду требований к сети в качестве санкций оставлено поведение по умолчанию – фильтрация штрафных пакетов. Однако не следует забывать, что в некоторых случаях может потребоваться их усиление, например, перевод порта в состояние errdisable или хотя бы отправка лог сообщения.

```
Switch(config-if)# storm-control broadcast level 5
```

§2.4 Безопасность на 3 уровне.

Крайне действенным механизмом защиты на 3-м уровне являются системы предотвращения вторжений IPS (Intrusion Preventing System).

Cisco IOS IPS просматривает пакеты и сессии, проходящие через маршрутизатор, и сканирует их на совпадение с одной из известных ей сигнатур. Когда обнаруживается подозрительная активность, происходит генерация лог-события через механизм SDEE (Security Device Event Exchange).

В качестве защитных мер IPS может принимать следующие:

1. Послать тревогу на syslog сервер
2. Отбросить пакет
3. Сбросить соединение
4. Запретить трафик с IP атакующего на определенное время

При необходимости ненужные сигнатуры можно выключать. Все сигнатуры находятся в специальном файле – SDF (Signature Detection File). Информация хранится в нем в форме XML. Вот пример описания сигнатуры:

```
<entry nda="false" dontDelete="true">

        <var name="SigName" default="HTTP 1.1 Chunked Encoding Transfer"
        protected="true"></var>
        <var name="SIGID" default="5245" protected="true"></var>
        <var name="SubSig" default="0" protected="true"></var>
        <var name="AlarmSeverity" default="medium"></var>
        <var name="Enabled" default="True"></var>
        <var name="EventAction" default="alarm|drop|reset"></var>
        <var name="SigVersion" default="S21"></var>
        <var name="SigStringInfo" default="Transfer-Encoding: chunked"></var>
        <var name="AlarmThrottle" default="Summarize"></var>
        <var name="MinHits" default="1"></var>
        <var name="Protocol" default="TCP"></var>
        <var name="StorageKey" default="STREAM"></var>
        <var name="SummaryKey" default="AaBb"></var>
        <var name="ThrottleInterval" default="15"></var>
        <var name="DeObfuscate" default="True" protected="true"></var>
        <var name="HeaderRegex" default="[Tt][Rr][Aa][Nn][Ss][Ff][Ee][Rr]-
        [Ee][Nn][Cc][Oo][Dd][Ii][Nn][Gg][:][ /t]?[Cc][Hh][Uu][Nn][Kk][Ee][Dd]"
        protected="true"></var>
        <var name="ServicePorts" default="80,3128,8000,8010,8080,8888,24326"></var>

</entry>
```

Переписав sdf файл с маршрутизатора на компьютер, можно регулировать и менять поведение IPS при обнаружении атаки, манипулируя полем EventAction. Однако делать это следует осторожно. Не стоит сбрасывать флаги reset и drop там, где они установлены, т.к. это приводит к ослаблению безопасности.

Для обмена файлами между маршрутизатором и компьютером используется, например, протокол tftp. Необходимо запустить tftp-server на ПК. Далее использовать команды:

- copy flash tftp – для перегонки sdf файла с маршрутизатора на ПК
- copy tftp flash – для обратной операции

Для запуска системы IPS необходимо осуществить следующие шаги [17,22]:

1. Загрузить в модуль IPS sdf файл
2. Создать именованное правило IPS
3. Включить механизм SDEE и настроить размеры буферов сообщение.
4. Применить правило IPS на нужных интерфейсах и необходимых направлениях.

```
Router(config)#ip ips sdf location flash:128MB.sdf
Router(config)#ip ips name testIPS

Router(config)#ip ips notify SDEE
Router(config)#ip sdee messages 111
Router(config)#ip sdee alerts 555

Router(config)#interface fast 0/1
Router(config-if)#ip ips testIPS in
```

Router(config-if)#ip ips testIPS out

На случай размещения в демилитаризованной зоне web-сервера в лаборатории была проработана технология перехвата TCP – TCP intercept. Этот механизм создан для борьбы с очень распространенной и эффективной DoS атакой TCP SYN FLOOD.

Существует 2 режима работы TCP intercept:

- перехват (intercept) – в этом режиме, прежде чем передать запрос на подключение серверу, межсетевой экран пытается сам установить соединение с хостом. В том случае, если это атакующий – ответа не последует, и запрос будет отброшен. Если же ответ приходит – маршрутизатор проводит запрос дальше. Кроме того отслеживается статистика полуоткрытых соединений, и в случае надобности происходит их сброс.
- наблюдение (watch) – межсетевой экран отслеживает статистику полуоткрытых соединений, и в случае надобности происходит их сброс.

Для реализации данной технологии необходимо [17, 23]:

1. Создать расширенный список контроля доступа, в котором необходимо определить трафик, подлежащий перехвату.
2. Связать этот ACL с технологией TCP Intercept.
3. Выставить режим работы (intercept или watch)
4. Выставить режим отбора кандидатов на сброс (случайного или самого старого)
5. Выставить защитные пороги.

```
Router(config)#ip access-list 125 permit tcp any host 217.80.159.1
Router(config)#ip tcp intercept list 125

Router(config)#ip tcp intercept mode intercept
Router(config)#ip tcp intercept drop-mode old

! время, за которое полуоткрытое соединение должно перейти в полное.
Router(config)#ip tcp intercept watch-timeout 30
! интервал неактивности соединения
ip tcp intercept connection-timeout 10

! количество полуоткрытых соединений, при котором нужно начинать агрессивное
! сбрасывание
ip tcp intercept max-incomplete high 100

! количество полуоткрытых соединений, при котором нужно прекращать агрессивное
! сбрасывание
ip tcp intercept max-incomplete low 20

! количество полуоткрытых соединений за минуту, при котором нужно начинать агрессивное
! сбрасывание
ip tcp intercept one-minute high 50

! количество полуоткрытых соединений за минуту, при котором нужно прекращать
! агрессивное сбрасывание
ip tcp intercept one-minute low 10
```

Надежным механизмом защиты является фильтрация сессий с помощью технологии Reflexive ACL. Решения о фильтрации принимаются на основе информации верхних уровней. Настраивается Reflexive ACL на пограничном маршрутизаторе.

Reflexive ACL содержат временные правила, добавляемые маршрутизатором автоматически. Например, пользователь вашей сети пытается установить соединения с внешним адресатом, в обычных условиях трафик от которого был бы отброшен. Но Reflexive ACL создает временный обратный проход для него.

Временные правила обладают рядом свойств, которые ограничивают область их применения:

1. Это всегда permit-правила
2. Они объявляют тот же протокол, который указан в исходящем пакете.
3. Прописывают те же адреса источника и адресата, что и в исходном пакете.
4. Устанавливают те же порты, что и в исходном пакете (это для TCP и UDP). В случае использования ICMP используется тип сообщения.
5. Пункт будет удален после прохождения последнего сессионного пакета.
6. Если в течение установленного интервала времени сессия неактивна, пункт удаляется.

В случае, когда ответ приходит на другой порт, а не на указанный в запросе, он будет отфильтрован.

Для реализации данного механизма необходимо [17, 24]:

1. Создать именованный ACL для исходящего потока, в котором указать трафик, подлежащий фильтрации.
2. Создать именованный ACL для входящего потока, в котором указать ссылку на динамический лист, определенный в 1.
3. Установить таймаут неактивности сессии.
4. Применить листы контроля доступа на интерфейсах.

```
ip access-list extended OutBoundFilter
 permit tcp any any reflect TCPtrafic

ip access-list extended InBoundFilter
 evaluate TCPtrafic
! здесь могут размещаться другие разрешающие/запрещающие правила
 deny ip any any

ip reflexive-list timeout 180
```

Еще более мощным механизмом защиты является CBAC (Context-Based Access Control). CBAC фильтрует TCP и UDP пакеты, основываясь на информации уровня приложения. С помощью данной технологии можно блокировать Java, обнаруживать нелегальные инструкции в управляющем канале SMTP, пропускать только те соединения, которые исходят из защищаемой сети, производить фильтрацию в обоих направлениях (внутрь и наружу).

CBAC фильтрует только заданные протоколы. Он включается только если обычные листы контроля доступа пропускают пакет через межсетевой экран (см. рис 15.)

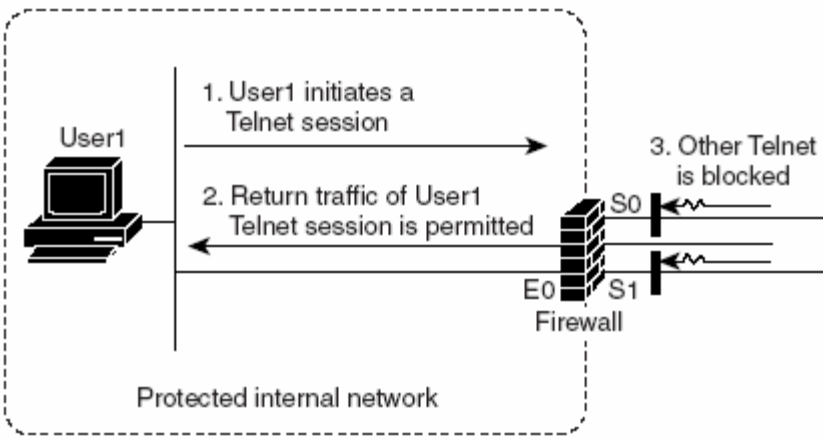


Рис. 15. CBAC – открытие временных обратных дыр.

CBAC подобно Reflexive ACL открывает для исходящих соединений обратные дыры.
Когда CBAC обнаруживает атаку, он способен предпринять ряд действий:

1. Сгенерировать сообщение тревоги.
2. Защитить системные ресурсы, которые необходимы для хорошей производительности.
3. Заблокировать пакеты, исходящие от вероятного злоумышленника.

Также CBAC предоставляет 3 порога против DoS атак:

1. Общее количество полуоткрытых TCP и UDP сессий.
2. Количество полуоткрытых сессий в единицу времени.
3. Количество полуоткрытых TCP-сессий, приходящихся на хост.

При достижении порога CBAC в зависимости от настроек либо посылает команду сброса по самой старой полуоткрытой сессии, либо на время блокирует прохождение пакетов TCP SYN.

В нашем случае было принято решение настраивать фильтрацию TCP, UDP, FTP, вести мониторинг фрагментированных пакетов и осуществлять Java-блокировку от заданных серверов.

Для включения механизма CBAC необходимо [17, 25]:

1. Установить глобальные таймеры и пороги.
2. Создать именованное инспекционное правило, где обозначит фильтруемые протоколы.
3. Создать списки контроля доступа.
4. Применить списки контроля доступа на интерфейсах.
5. Применить инспекционное правило.

```
ip inspect max-incomplete low 200
ip inspect max-incomplete high 400
ip inspect one-minute low 100
ip inspect one-minute high 400
ip inspect udp idle-time 20
ip inspect dns-timeout 6
ip inspect tcp idle-time 600
ip inspect tcp finwait-time 6
ip inspect tcp synwait-time 18
ip inspect tcp max-incomplete host 20 block-time 0
```

```
ip inspect name testinspect ftp timeout 20
ip inspect name testinspect http java-list FriendlySites
ip inspect name testinspect tcp
ip inspect name testinspect udp
ip inspect name testinspect fragment maximum 20

ip access-list standart FriendlySites
  ! permit trafic from friendlySites
  permit 213.213.213.213
  permit 217.80.217.40

! create an ACL to permit inspecting trafic to leave inside network
access-list 101 permit tcp 192.168.0.0 0.0.255.255 any
access-list 101 permit udp 192.168.0.0 0.0.255.255 any
access-list 101 permit icmp any any
access-list 101 deny   ip any any

! create an ACL to deny inspecting trafic to enter inside network from outside
access-list 111 deny   tcp any 192.168.0.0 0.0.255.255
access-list 111 deny   udp any 192.168.0.0 0.0.255.255
access-list 111 permit ip any any
…
! on outside interface
ip access-group 111 in
ip access-group 101 out
ip inspect testinspect in
```

Однако не следует забывать, что CBAC имеет те же ограничения, что и Reflexive ACL.

§2.5 Дополнительная безопасная конфигурация устройств.

Во-первых следуют отключить все неиспользуемые службы. В том числе различные TCP и UDP сервисы, службу finger, отключить протокол bootp, отключить snmp, т.к. не предполагается его использование.

```
no service finger
no service pad
no service tcp-small-servers
no service udp-small-servers
no snmp-server

no ip bootp server
```

Следует отключить так же маршрутизацию по адресу источника.

```
no ip source-route
```

Ряд служб следует включить:

1. Шифрование паролей.
2. Входящие и исходящие TCP keepalive сообщения.
3. Службу временных отметок (необходимо для датирования лог-информации).
4. Службу простановки sequence number в лог сообщениях.
5. Технологию cef (Cisco express forwarding).

```
service password encryption
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debuf datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
service sequence-numbers
ip cef
```

Обязательно следует настроить баннеры, появляющиеся при входе на устройство.

```
banner # <message> #
banner motd # <message> #
banner login # <message> #
```

В качестве сообщения, выводимого в баннере, рекомендуется использовать следующее: “Authorized access only! This system is the property of <company name> Enterprise. Disconnect IMMEDIATELY as you are not an authorized user! Contact <administrator email address> <administrator phone number>”.

Так же следует наложить ограничения на возможные пароли и вести учет ошибочных попыток аутентификации.

```
security passwords min-length 8
security authentication failure rate 3 log
```

Настроить параметры сбора лог-информации.

```
logging on
logging 192.168.5.100 ! log-server
logging console critical
logging trap debugging
logging buffered 32000
```

На интерфейсной базе следует:

1. Отключить направленные широковещания.
2. Отключить proxy-arp.
3. Отключить перенаправления.
4. Включить опцию обратной проверки (RPF – reverse pass forwarding).

```
no ip directed-broadcast
no ip proxy-arp
no ip redirects
ip verify unicast reachable-via rx
```

Использования RPF является крайне важным моментом, т.к. это частично помогает бороться со спуфингом IP адресов. Суть данной технологии заключается в том, что маршрутизатор проверяет, есть ли сеть, соответствующая IP адресу источника, в таблице маршрутизации и на правильном ли интерфейсе получен пакет. Если согласно маршрутизирующей информации сеть источника находиться за другим интерфейсом, пакет отбрасывается.

Проверка происходить не по таблицам маршрутизации, т.к. это очень долго, а по специальной базе данных, созданной технологией CEF.

§2.6 Мониторинг сети.

Чисто теоретически была разработана модель, позволяющая организовать мониторинг сети. Также она предоставляет возможность подключения к сети дополнительных анализаторов (например, систем IDS таких как Snort), и организации выборочного мониторинга трафика (от отдельных хостов, или от целой VLAN).

Идея заключается в создании зеркальных портов на коммутаторе, куда будет переправляться трафик из демилитаризованной зоны. Анализатор будет снимать этот поток с зеркального порта и осуществлять его разбор.

Следует, однако, заранее оговорить некоторые ограничения. В случае пиковой нагрузки на серверах, суммарный их трафик может превзойти возможности порта, к которому подключен анализатор. Тогда происходит отбрасывание не поместившихся кадров.

Схему подключения рабочей станции с функциями мониторинга и анализа см. на рисунке 16.

Рис. 16. Подключение рабочей станции с функциями мониторинга.

Для реализации SPAN технологии необходимо [6]:

1. Объявить источник сессия мониторинга.
2. Объявить назначение сессии мониторинга.

```
Switch(config)# monitor session 1 source vlan 50 both
Switch(config)# monitor session 1 destination interface fast 0/44
```

При обнаружении подозрительного хоста в сети необходимо создать еще одну сессию, которая весь его трафик будет отправлять прямиком на анализатор.

```
Switch(config)# monitor session 2 source interface fast 0/23 both
Switch(config)# monitor session 2 destination interface fast 0/44
```

Данная методология позволяет обнаружить нарушителей и зафиксировать их действия.

Глава 3. Разработка средства атаки коммутаторов.

§3.1 Архитектура Packet Sniffer SDK.

Чтобы эффективно обрабатывать сетевой траффик, программа захвата пакетов должна взаимодействовать непосредственно с сетевым оборудованием. По этой причине ОС должна предоставлять набор действий по коммуникации с сетевым адаптером. Здесь существует большая системная зависимость, поэтому реализация подобных действий различна на разных ОС.

Одна из наиболее перспективних технологий в этой области представлена в продукте компании MicroOLAP (c) Packet Sniffer SDK[26]. Packet Sniffer SDK представляет собой библиотеку для захвата и анализа сетевого трафика для платформы Win32.

В соответствии с типовой архитектурой анализаторов сетевого трафика, на самом нижнем уровне иерархии лежит сетевой адаптер. Он используется для захвата пакетов, которые циркулируют в сети. Во время захвата сетевой адаптер обычно работает в особенном режиме, который заставляет адаптер принимать все пакеты (Promiscuous mode).

Драйвер захвата пакетов – низший программный уровень иерархии захвата. Эта часть работает в «режиме ядра» системы и взаимодействует с сетевым адаптером для обмена пакетами. Он предоставляет программным приложениям набор функций для чтения и записи данных адаптера.

PSSDK (Packet Sniffer SDK) – работает в пользовательском режиме. Однако в отличие от стандартной архитектуры, данная библиотека содержит свой собственный динамически загружаемый драйвер, предоставляющий приложениям высокого уровня мощный инструментарий. PSSDK представляет собой статически или динамически присоединяемую библиотеку, которая является частью приложения захвата пакетов.

Основными особенностями Packet Sniffer SDK являются:

- Полноценная поддержка сетей 1GBit;
- Наличие внутреннего динамически загружаемого драйвера пакетов, что обуславливает отсутствие необходимости в предустановленных драйверах;
- Поддержка мультипроцессорных (SMP) систем;
- Поддержка новой технологии фильтрации пакетов – FastBPF, обеспечивающей в среднем в 6 раз большую производительность по сравнению с обычными BPF фильтрами;
- Поддержка BPF ассемблера для написания BPF/FastBPF фильтров.

На базе данной архитектуры студентом факультета информатики ТГУ Кравченко А.В. было разработано средство анализа сетевого трафика.

В основу собственного инструмента атаки коммутаторов я заложил его программу Sniffer, к которой приделал модуль, отвечающий за отправку пакетов и реализующий атаки CAM-overflow и FloodNetwork.

В будущем планируется нарастить возможности данного атакующего средства. Многие эффективные сетевые атаки реализуются относительно просто: путем генерации и выброса в сеть определенных пакетов. То есть они не предусматривают обратной связи и какой-то интеллектуальной обработки ответов, т.к. вообще их не получают. Атаки данного типа и планируется реализовать.

§3.2 Теоретическая основа использованных механизмов взлома.

Комплексная атака, реализованная в программном продукте, названа «Манипулирование MAC адресами». Она основана на использовании двух полей в заголовке кадра:

1. MAC адрес источника
2. MAC адрес назначения

Генерируя поток кадров, с выставленными определенным образом значениями этих полей, можно получить 3 результата:

1. Атака CAM переполнение
2. DoS атака на сетевой сегмент, подключенных к коммутатору
3. Комбинированная атака

Атака CAM-overflow нацелена на использование правил работы коммутаторов. Саму работу по продвижению трафика можно разделить на две стадии:

- обучение (происходит на ходу)
- продвижение

У коммутатора есть CAM память, в которой он хранит соответствия [MAC адрес, порт], необходимые ему для работы. При получении кадра на одном из интерфейсов он анализирует поле MAC адреса назначения и производит коммутацию на основе данных из CAM. Если они там отсутствуют, коммутатор производит пересылку кадра во все порты, кроме порта источника.

При получении на каком-либо интерфейсе кадра с неизвестным MAC адресом источника коммутатор производит запись соответствия в CAM память.

CAM память ограничена. Если она переполняется, то для сохранения своей работоспособности коммутатор переход в режим концентратора. Таким образом, эффект микросегментации устраняется, коллизионный домен расширяется, и. каждый его член получает доступ ко всему трафику.

Цель атаки CAM переполнения – получение доступа к чужому трафику. Достигается это за счет генерации трафика с множеством неизвестных коммутатору MAC адресов источника. Таким образом, достигается забитие CAM памяти.

Манипулируя MAC адресом назначения, можно реализовать DoS атаку на сетевой сегмент, подключенный к коммутатору. Добиться этого можно двумя способами. Во-первых, в качестве MAC адреса назначения указать широковещание. Однако данная альтернатива легко блокируется опцией storm-control на интерфейсах. Во-вторых, MAC адреса назначения можно динамически генерировать как случайную величину. Пакеты такого типа являются одноадресные и в большинстве случаев фильтром storm-control отброшены не будут.

В программе реализованы 4 опции генерации MAC адреса назначения:

- Random Dynamic – Случайный динамический – для каждого генерируемого кадра будет создавать свой случайный адрес. Используется для организации DoS атаки.
- Random Static – Случайный статический – перед началом атаки будет сгенерирован случайным MAC адрес, который будет проставлен во все отправляемые пакеты. Используется для обхода storm-control.
- Broadcast – Широковещательный – в качестве MAC адреса назначения будет использован широковещательный адрес “FFFF.FFFF.FFFF”. Используется для организации DoS атаки.
- Defined Static – Статический, заданный пользователем заранее. Используется для обхода storm-control.

Также существует 2 возможности для задания MAC адреса источника:

- Random Dynamic – Случайный динамический – необходим в случае реализации атаки CAM переполнение.
- Defined Static – Статический, заданный пользователем заранее. Может использоваться для обхода защитной технологии port-security при организации DoS атаки.

Подробное описание программы, реализующей комплексную атаку манипулирования MAC адресами, находится в приложении 2 «Руководство программиста», а правила использования данного ПО находятся в приложении 1 «Руководство пользователя».

§3.3 Тестирования атакующего генератора пакетов.

Схема лаборатории, в которой проводились испытания, представлена на рисунке 17.

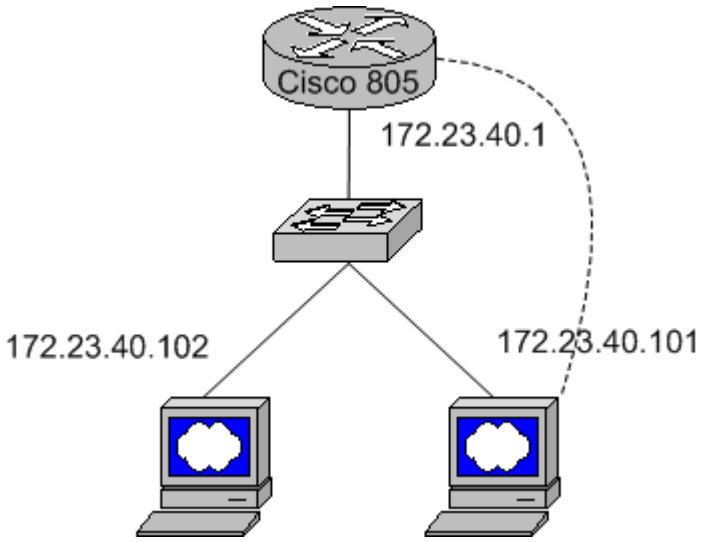


Рис. 17. Домашняя лаборатория.

Рабочая станция 172.23.40.101 имеет консольное подключение к маршрутизатору Cisco 805. NIC карта рабочей станции 172.23.40.102 имеет 100 Мб/сек подключение к сети, остальные хосты – 10 Мб/сек. подключение. Коммутатор поддерживает технологию Fast Ethernet и использует механизм авто переговоров при установлении канала связи с хостами, т.е. происходит согласование режима передачи (full duplex, half duplex) и скорости (10/100 Мб/сек.).

172.23.40.102 – хост А.

172.23.40.101 – хост Б.

Атакующие генератор пакетов был размещен на самой быстрой рабочей станции, т.е. на хосте А.

Для тестирования ПО использовался неуправляемый коммутатор DLink DES-1024D(C1/C2), корой имеет следующие характеристики:

1. 24 порта 10/100Base-TX Fast Etherent.
2. Коммутационная фабрика 4.8 Гбит/с.

3. Соответствие RoHS.
4. Размер таблицы MAC-адресов 8К.
5. Буфер RAM 160 Кб
6. MTBF – 32274 часа.
7. Режим Store and Forward.

В соответствии с испытаниями для 100% нагрузки исходящей линии атакующей станции в 100 МБит/с рекомендуется выставлять параметры:

- интервал – 100 миллисекунд
- количество – 50000-100000 кадров в пачке

Однако, как показала практика, в данных условиях для хорошей нагрузки хостов в 10 МБит/с вполне хватает нагрузки в 21% исходящей линии:

- интервал – 100 миллисекунд
- количество – 10000 кадров в пачке

В случае реализации атаки FloodNetwork путем использования в качестве MAC адреса назначения широковещания или же динамически случайно генерируемый можно нагрузить все хосты, подключенные к сети. Есть возможность нагрузить трафиком отдельный хост в сети путем указания его MAC-а в поле адреса назначения.

При нагрузке сети 10 Мегабитные хосты имеют явные ограничения в сетевом ресурсе. Так процент потерь составляет 73%, а задержка на получение ответа на эхо запрос возрастает в 5-15 раз против ненагруженного состояния (нагрузка давалась в 21% как 100,10000). В обычных условиях время ответа составляет менее 10 миллисекунд, а в нагруженном оно составило 55-157 миллисекунд.

Попытка реализовать атаку CAM переполнения окончилась неудачей. В соответствии с заявленными техническими параметрами, CAM память должна была кончиться уже после 1-2 секунд атаки, однако перехода коммутатора в режим концентратора не произошло, что говорит о наличии каких-то дополнительных средств защиты на этот случай. Предположительно, здесь может использоваться одна из двух альтернатив:

1. Отбрасывание пакетов с неизвестными MAC адресами, когда скорость их появления на интерфейсе превышает порог.
2. Динамическая очистка CAM памяти, т.е. постоянное удаление старых позиций для записи новых (данная гипотеза является наиболее вероятной).

Проверить данные гипотезы в лаборатории не получилось по ряду причин. Во-первых, трафик, генерируемый на атакующей станции, имеет пульсирующий характер и не представляет собой непрерывный поток. Такой эффект получается как из-за архитектуры самого генератора пакетов, так и из-за архитектуры библиотек PSSDK, на основе которых он разрабатывался. Во-вторых, количество пакетов просто огромно и достигает порой десятков миллионов. Поэтому, даже запуская сниффер пакетов на другой рабочей станции, не удается понять, какая из предложенных технологий препятствует атаке.

В случае замены коммутатора на управляемый Cisco Catalyst Switch 2960 (технические характеристики изложены в 2.1) происходит ряд изменений. А именно – опция storm-control препятствует заполнению сети широковещательным трафиком. Опция port-security исключает возможность проведения атаки CAM переполнения. Единственная атакующая возможность для программы – это нагрузка отдельного хоста. Однако это придется делать с

разрешенного MAC адреса (MAC спуффинг исключается), а, значит, это легко будет обнаружить.

Таким образом, чтобы организовать хоть какую-то атаку необходимо:

1. Получить доступ к порту коммутатора.
2. Установить MAC адрес, являющийся разрешенным для данного порта (таких адресов может быть несколько).
3. Установить MAC адрес атакуемой станции.

При этом все, чего удается добиться, это нагрузить входящую линию целевого хоста на 95-97%. Защитить хост в данном случае можно лишь с помощью введения для него технологии CAR.

Остается еще 1 непроверенная на управляемых коммутаторах опция – генерирование трафика с динамическим случайным MAC адресом назначения, что приведет к ситуации похожей на широковещательный шторм. Однако защита storm-control, настроенная на блокирование лишних широковещаний, теоретически должна пропустить данный поток.

Заключение.

В ходе работы был произведен глубокий анализ существующих подходов к обеспечению безопасности корпоративных мультисервисных сетей. Был рассмотрен ряд передовых технологий в данной области. В частности произведено ознакомление с архитектурой безопасности “SAFE” от компании Cisco Systems.

Был проработан ряд существенных моментов:

- Обеспечение безопасного доступа к устройствам
- Безопасность на 2-ом уровне
- Безопасность на 3-м уровне

Результатом работы стала сеть Российско-Германского саммита. В ходе ее эксплуатации успешных попыток взлома обнаружено не было. Все требования, предъявленные к сети, были выполнены.

Произведена также двухдневное сервисное обеспечение работы данной сети. В течение данного интервала времени каких-либо ошибок в настройке оборудования обнаружено не было.

Кроме того, было разработано средство атаки коммутаторов – агрессивный генератор пакетов, и произведено его тестирование на оборудовании фирмы DLink и Cisco.

Список использованных источников литературы.

1. CCSP: Cisco Certified Security Professional Certification All-in-One Exam Guide, Robert E. Larson, Lance Cockcroft, Osborn/McGraw-Hill, 2003
2. CCDP: Cisco Internetwork Design Study Guide, unknown author.
3. Routing TCP/IP (CCIE Professional Development, a detailed examination of interior routing protocols), Jeff Doyle, Cisco Press, 1998
4. Решения компании Cisco Systems по обеспечению безопасности корпоративных сетей, составитель М. Кадер, Cisco Press, 2004
5. Решения Cisco для обеспечения информационной безопасности (издание 4), составитель А. Лукацкий, Cisco Press, 2005
6. CCNP BCMSN Exam Certification Guide, David Hucaby (Building Cisco Multilayer Switching Networks), Osborne/McGraw-Hill, 2000
7. CCNP BCRAN Remote Access Study Guide, Osborne/McGraw-Hill, 2000
8. Best Damn Cisco Internetworking Book Period, Michael E. Flannagan, Ron Fuller, Umer Khan, Wayne A. Lowson II, Keith O`Brien, Martin Walshaw, Syngress, 2003
9. Журнал «Информ-Курьер-Связь», июль 2005.
10. Журнал сетевых решений «LAN», сентябрь 2005.
11. «Администрирование информационно-вычислительных сетей», Н. Т. Кустов, учебное пособие, Томск 2004
12. Построение виртуальных частных сетей (VPN) на базе технологии MPLS, составитель М. Захватов, Cisco Press, 2004
13. «Настройка маршрутизаторов», электронный ресурс, Белицкий Д. Ю.
14. “SAFE Layer 2 Security In-Depth”, Ido Dubrawsky, 2004, электронный ресурс на www.cisco.com.
15. “Cisco IOS Software Configuration Guide for Cisco Aironet Access Points”, 2005, эклетронный ресурс на www.cisco.com.
16. “Catalyst 2960 Switch Configuration Guide”, 2005, эклетронный ресурс на www.cisco.com.
17. “Cisco IOS Security Configuration Guide”, 2005, эклетронный ресурс на www.cisco.com.
18. “Cisco IOS Wireless LAN Configuration Guide”, 2005, эклетронный ресурс на www.cisco.com.
19. “Cisco 2811 Integrated Services Router”, электронный ресурс на www.cisco.com.
20. “Cisco Catalyst 2960 Series Switches”, электронный ресурс на www.cisco.com.
21. “Cisco Aironet 1200 Series Access Points”, электронный ресурс на www.cisco.com.
22. “Cisco IOS IPS Configuration”, электронный ресурс на www.cisco.com.
23. “Cisco IOS TCP Intercept” , электронный ресурс на www.cisco.com.
24. “IP Session Filtering” , электронный ресурс на www.cisco.com.
25. “Context-Based Access Control”, электронный ресурс на www.cisco.com.
26. “Построение и анализ мультисервисных сетей передачи данных, голоса и видео”, Кравченко А.В., электронный ресурс.

ПРИЛОЖЕНИЕ 1. РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Приложение Sniffer представляет собой форму, отображаемую поверх остальных окон.

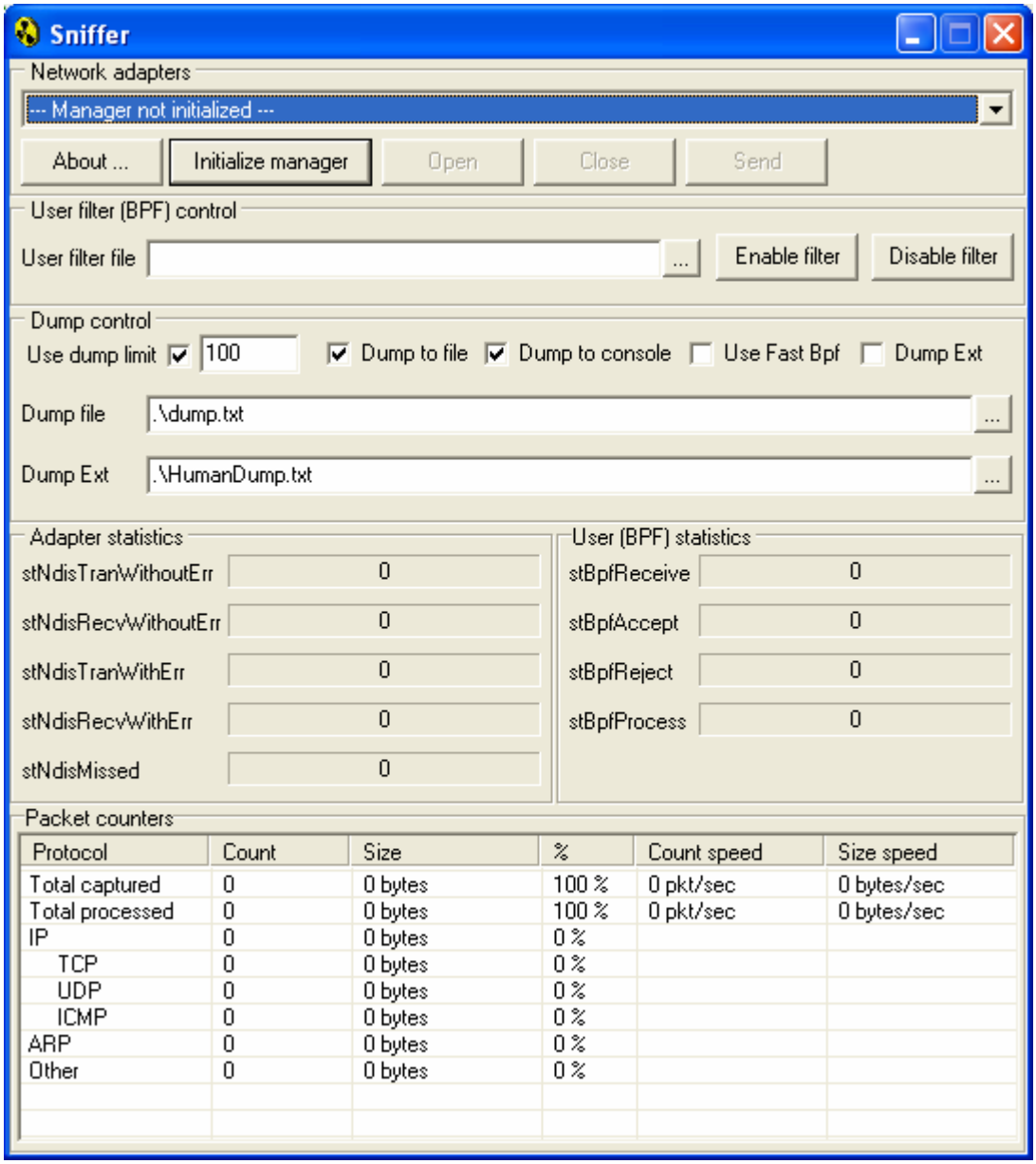


Рис. 18. Главное окно программы Sniffer.

Для начала работы пользователю необходимо нажать кнопку инициализации - "Initialize Manager", в результате чего будет заполнен список активных сетевых адаптеров. После заполнения списка пользователь имеет возможность выбора адаптера, который будет осуществлять захват/передачу пакетов. Приложение может работать только с одним адаптером одновременно, при необходимости захватывать пакеты с нескольких сетевых адаптеров одновременно, следует открыть несколько – по числу отслеживаемых адаптеров – экземпляров приложения, каждый из которых захватывает пакеты со своего адаптера.

Выбрав адаптер из полученного списка, пользователь для начала захвата должен нажать кнопку "Open". Перед этим следует указать в какой форме и куда логировать захваченные пакеты:

- Строка "Dump to file" – задаёт путь к файлу, использующемуся для записи полученных пакетов. Если файл с указанным в строке именем не существует – он будет создан. При каждом запуске программы всё существовавшее до этого содержимое файла уничтожается, это сделано для удобства работы пользователя, поскольку присутствие избыточной информации затрудняет анализ;
- Строка "Dump Ext" – задаёт путь к файлу, использующемуся для записи полученных пакетов в удобной для человека форме. Если файл с указанным в строке именем не существует – он будет создан. При каждом запуске программы всё существовавшее до этого содержимое файла также уничтожается.
- "Use dump limit" – определяет следует ли использовать лимит на количество обработанных пакетов, при достижении которого прекращается захват пакетов;
- "Dump to file" – определяет следует ли логировать захваченные пакеты в файл в шестнадцатеричной форме;
- "Dump to console" – определяет следует ли логировать захваченные пакеты в консоль приложения;
- "Use fast bpf" – определяет следует ли приложению использовать FastBPF фильтры
- "Dump Ext" – определяет следует ли логировать захваченные пакеты в файл в форме удобной для восприятия человеком – при этом, пакеты неопознанного типа также логируются в шестнадцатеричной форме. При использовании расширенного логирования, логирование в файл стандартного дампа не производится.

Более подробную информацию можно получить в [26] в главе «Руководство пользователя».

Для перехода в режим генератора пакетов после инициализации необходимо нажать кнопку “Send”. В результате появиться окно генератора пакетов, показанное на рисунке 18.

В верхнем текстовом поле можно вручную создать пакет и отправить его. При этом значение поля “Send counter” будет использовано в качестве параметра, определяющего количество экземпляров пакета, которые будут переданы. Для отправки необходимо использовать кнопки “Sync send” и “Async send” для синхронной и асинхронной передачи соответственно.

Для организации атаки необходимо сначала выставить опции:

1. Указать интервал отправки порций в поле “Interval”.
2. Указать размер порций в поле “Count”.
3. Указать, стоит ли использовать введенный пользователем текс как поле нагрузки в генерируемых кадрах.
4. Выставить режим генерации MAC адреса назначения.
5. Выставить режим генерации MAC адреса источника.

В качестве MAC адреса назначения есть возможность использовать одну из 4-х альтернатив:

- Random Dynamic – Случайный динамический – для каждого генерируемого кадра будет создавать свой случайный адрес. Используется для организации DoS атаки.
- Random Static – Случайный статический – перед началом атаки будет сгенерирован случайным MAC адрес, который будет проставлен во все отправляемые пакеты. Используется для обхода storm-control.
- Broadcast – Широковещательный – в качестве MAC адреса назначения будет использован широковещательный адрес “FFFF.FFFF.FFFF”. Используется для организации DoS атаки.

- Defined Static – Статический, заданный пользователем заранее. Используется для обхода storm-control.

В качестве MAC адреса источника можно использовать:

- CAM overflow – Random Dynamic – Случайный динамический – необходим в случае реализации атаки CAM переполнение.
- Flood Network – Defined Static – Статический, заданный пользователем заранее. Может использоваться для обхода защитной технологии port-security при организации DoS атаки.

Для начала атаки необходимо нажать кнопку “Attack”. Для прекращения – кнопку “Stop”.

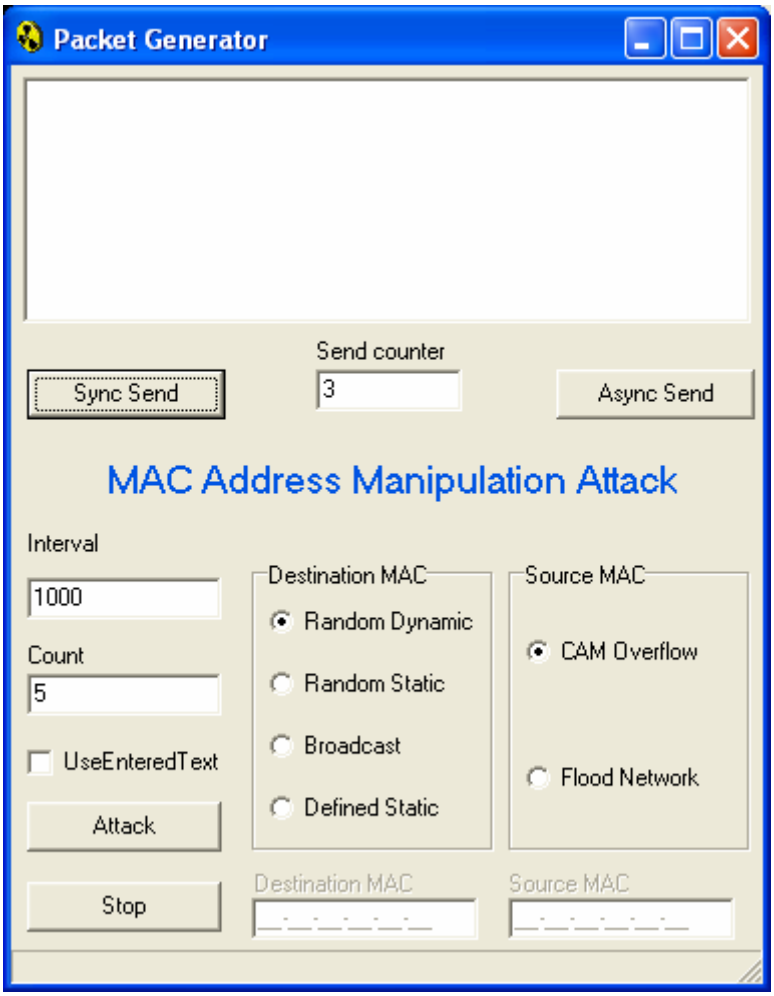


Рис. 19. Генератор пакетов

ПРИЛОЖЕНИЕ 2. РУКОВОДСТВО ПРОГРАММИСТА

Понять структуру приложения поможет заголовочный файл “SendUnit.h”.

```
#ifndef SendUnitH
#define SendUnitH
//---------------------------------------------------------------------------
#include <Classes.hpp>
#include <Controls.hpp>
#include <StdCtrls.hpp>
#include <Forms.hpp>
#include "HNAdapter.hpp"
#include <ExtCtrls.hpp>
#include <ComCtrls.hpp>
#include <stdlib.h>

//Данные константы задают режимы генерирования MAC адреса назначения
#define DM_RANDOMDYNAMIC 0      //случайный, динамически создаваемый
#define DM_RANDOMSTATIC  1      //случайный статический
#define DM_BROADCAST     2      //широковещательный - FFFF.FFFF.FFFF
#define DM_DEFINEDSTATIC 3      //предопределенный статический

//Варианты генерирования MAC адреса источника
#define SM_CAMOVERFLOW   0  //случайный, динамически создаваемый
#define SM_FLOODNETWORK  1  //предопределенный статический

//---------------------------------------------------------------------------
class TSendForm : public TForm
{
__published:   // IDE-managed Components
   //кнопка синхронной отправки
   TButton *SyncSend_Btn;
   //кнопка асинхронной отправки
   TButton *AsyncSend_Btn;
   //текстовое поле для ввода пакета к отправке вручную
   TMemo *PacketsContent_Edit;
   //VCL-контрол, соответствующий адаптеру
   THNAdapter *HNAdapter;
   //поле для ввода количества отправляемых пакетов
   TLabeledEdit *SendCount_Edit;
   //кнопка начала атаки
   TButton *Button1;
   //кнопка остановки атаки
   TButton *Button2;
   //таймер, генерирующий прерывания в соответствии с заданным интервалом
   TTimer *Timer1;
   //полоса отображения статуса
   TStatusBar *StatusBar1;
```

```
    //флаг, обозначающий необходимость использования текстового поля
    TCheckBox *CheckBox2;
    //поле для ввода значения интервала
    TEdit *Edit1;
    TLabel *Label1;
    //поле для ввода размера порции
    TEdit *Edit2;
    TLabel *Label2;
    //альтернативы выбора способа генерирования MAC назначения
    TRadioGroup *RadioGroup1;
    //шаблонное поле для ввода MAC адреса назначения
    TMaskEdit *MaskEdit1;
    TLabel *Label3;
    //альтернативы выбора способа генерирования MAC адреса источника
    TRadioGroup *RadioGroup2;
    //шаблонное поле для ввода MAC адреса источника
    TMaskEdit *MaskEdit2;
    TLabel *Label4;
    TLabel *Label5;
    //обработчик события нажатия на кнопку синхронной отправки
    void __fastcall SyncSend_BtnClick(TObject *Sender);
    //обработчик события нажатия на кнопку асинхронной отправки
    void __fastcall AsyncSend_BtnClick(TObject *Sender);
    //обработчик события сигнала от таймера
    void __fastcall OnTimerEvent(TObject *Sender);
    //обработчик события нажатия на кнопку начала атаки
    void __fastcall Button1Click(TObject *Sender);
    //обработчик события нажатия на кнопку прекращения атаки
    void __fastcall Button2Click(TObject *Sender);
    //обработчик, отвечающий за блокирование/разблокирование полей ввода MAC
    //адресов в соответствии с указанными пользователем опциями
    void __fastcall OnRadioClick(TObject *Sender);
private:        // User declarations
public:         // User declarations
    //конструктор формы
    __fastcall TSendForm(TComponent* Owner);
    //строковая переменная, содержащая значение MAC адреса назначения
    AnsiString DestMAC;
    //строковая переменная, содержащая MAC адрес источника
    AnsiString SrcMAC;
    //целочисленная переменная, содержащая размер порции к отправке
    int sendcnt;
};
//---------------------------------------------------------------------------
extern PACKAGE TSendForm *SendForm;
//---------------------------------------------------------------------------
#endif
```

Архитектура атакующего генератора построена на идее периодического выброса порций пакетов в сеть. Для гибкого управления этим процессом вводятся 2 целочисленные величины:

- Interval – интервал выброса
- Count – количество пакетов в порции

Интервал используется в качестве значения свойства Interval класса TTimer. По каждому событию, генерируемому таймером на истечение интервала, происходит создания порции пакетов и сброс их в сеть.

Поле MAC адреса назначения кадра генерируется в соответствии с выбранной пользователем альтернативой. Всего их 4:

- Random Dynamic (DM_RANDOMDYNAMIC) – Случайный динамический – для каждого генерируемого кадра будет создавать свой случайный адрес. Используется для организации DoS атаки.
- Random Static (DM_RANDOMSTATIC) – Случайный статический – перед началом атаки будет сгенерирован случайным MAC адрес, который будет проставлен во все отправляемые пакеты. Используется для обхода storm-control.
- Broadcast (DM_BROADCAST) – Широковещательный – в качестве MAC адреса назначения будет использован широковещательный адрес “FFFF.FFFF.FFFF”. Используется для организации DoS атаки.
- Defined Static (DM_DEFINEDSTATIC) – Статический, заданный пользователем заранее. Используется для обхода storm-control

Поле MAC адреса источника кадра генерируется в 2-х вариантах:

- CAM overflow (SM_CAMOVERFLOW) – Random Dynamic – Случайный динамический – необходим в случае реализации атаки CAM переполнение.
- Flood Network (SM_FLOODNETWORK) – Defined Static – Статический, заданный пользователем заранее. Может использоваться для обхода защитной технологии port-security при организации DoS атаки.