Министерство науки и высшего образования
Российской Федерации

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Тульский государственный университет»

Интернет-институт ТулГУ

Кафедра ИБ

ОТЧЕТ ПО КОНТРОЛЬНОЙ РАБОТЕ

по дисциплине

«**Методы и средства защиты компьютерной информации**»

на тему

«Основные компоненты межсетевых экранов»

Вариант № 5

Выполнил:

студент группы ИБ262521-ф
Артемов Александр Евгеньевич

Проверил:

канд. техн. наук, доц.
Сафронова Марина Алексеевна

Тула, 2025

Содержание

Задание на работу

1. Изучить теоретический и дополнительный материал по данной дисциплине.
2. Выбрать тему индивидуального задания (Приложение А). Номер темы определяется по последней цифре в номере Вашей зачетке.
3. Оформить КРЗ и сдать преподавателю.

Введение

Интенсивное развитие глобальных компьютерных сетей, появление новых технологий поиска информации привлекают все больше внимания к сети Internet со стороны частных лиц и различных организаций. Многие организации принимают решение об интеграции своих локальных и корпоративных сетей в глобальную сеть. Использование глобальных сетей в коммерческих целях, а также при передаче информации, содержащей сведения конфиденциального характера, влечет за собой необходимость построения эффективной системы защиты информации. В настоящее время в России глобальные сети применяются для передачи коммерческой информации различного уровня конфиденциальности, например для связи с удаленными офисами из головной штаб-квартиры организации или создания Web-страницы организации с размещенной на ней рекламой и деловыми предложениями.

Вряд ли нужно перечислять все преимущества, которые получает современное предприятие, имея доступ к глобальной сети Internet. Но, как и многие другие новые технологии, использование Internet имеет и негативные последствия. Развитие глобальных сетей привело к многократному увеличению количества пользователей и увеличению количества атак на компьютеры, подключенные к сети Internet. Ежегодные потери, обусловленные недостаточным уровнем защищенности компьютеров, оцениваются десятками миллионов долларов. При подключении к Internet локальной или корпоративной сети необходимо позаботиться об обеспечении информационной безопасности этой сети.

Глобальная сеть Internet создавалась как открытая система, предназначенная для свободного обмена информацией. В силу открытости своей идеологии Internet предоставляет для злоумышленников значительно большие возможности по сравнению с традиционными информационными системами. Через Internet нарушитель может:

- вторгнуться во внутреннюю сеть предприятия и получить несанкционированный доступ к конфиденциальной информации;
- незаконно скопировать важную и ценную для предприятия информацию;
- получить пароли, адреса серверов, а подчас и их содержимое;
- входить в информационную систему предприятия под именем зарегистрированного пользователя и т.д.

С помощью полученной злоумышленником информации может быть серьезно подорвана конкурентоспособность предприятия и доверие его клиентов.

Ряд задач по отражению наиболее вероятных угроз для внутренних сетей способны решать межсетевые экраны. В отечественной литературе до последнего времени использовались вместо этого термина другие термины иностранного происхождения: брандмауэр и firewall. Вне компьютерной сферы брандмауэром (или firewall) называют стену, сделанную из негорючих материалов и препятствующую распространению пожара. В сфере компьютерных сетей межсетевой экран представляет собой барьер, защищающий от фигурального пожара – попыток злоумышленников вторгнуться во внутреннюю сеть для того, чтобы скопировать, изменить или стереть информацию либо воспользоваться памятью или вычислительной мощностью работающих в этой сети компьютеров. Межсетевой экран призван обеспечить безопасный доступ к внешней сети и ограничить доступ внешних пользователей к внутренней сети.

Межсетевой экран

Межсетевой экран – это система межсетевой защиты, позволяющая разделить общую сеть на две части или более и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую.

Как правило, эта граница проводится между корпоративной (локальной) сетью предприятия и глобальной сетью Internet, хотя ее можно провести и внутри корпоративной сети предприятия. МЭ пропускает через себя весь трафик, принимая для каждого проходящего пакета решение – пропускать его или отбросить. Для того чтобы МЭ мог осуществить это, ему необходимо определить набор правил фильтрации.

Обычно межсетевые экраны защищают внутреннюю сеть предприятия от «вторжений» из глобальной сети Internet, однако они могут использоваться и для защиты от «нападений» из корпоративной интрасети, к которой подключена локальная сеть предприятия. Ни один межсетевой экран не может гарантировать полной защиты внутренней сети при всех возможных обстоятельствах. Однако для большинства коммерческих организаций установка межсетевого экрана является необходимым условием обеспечения безопасности внутренней сети. Главный довод в пользу применения межсетевого экрана состоит в том, что без него системы внутренней сети подвергаются опасности со стороны слабо защищенных служб сети Internet, а также зондированию и атакам с каких-либо других хост-компьютеров внешней сети.

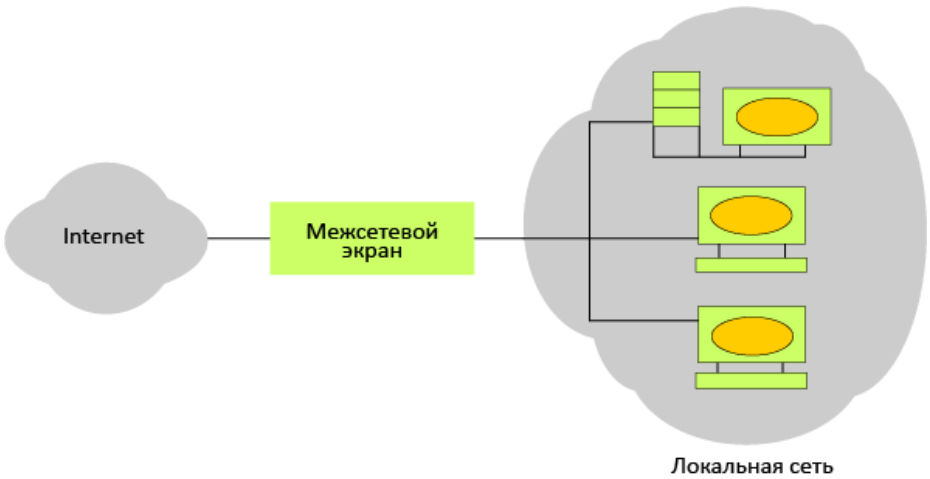

Рисунок 1: Схема установления межсетевого экрана

Проблемы недостаточной информационной безопасности являются «врожденными» практически для всех протоколов и служб Internet. Большая часть этих проблем связана с исторической зависимостью Internet от

операционной системы UNIX. Известно, что сеть Arpanet (прародитель Internet) строилась как сеть, связывающая исследовательские центры, научные, военные и правительственные учреждения, крупные университеты США. Эти структуры использовали операционную систему UNIX в качестве платформы для коммуникаций и решения собственных задач. Поэтому особенности методологии программирования в среде UNIX и ее архитектуры наложили отпечаток на реализацию протоколов обмена и политики безопасности в сети. Из-за открытости и распространенности система UNIX стала любимой добычей хакеров. Поэтому совсем не удивительно, что набор протоколов TCP/IP, который обеспечивает коммуникации в глобальной сети Internet и в получающих все большую популярность интрасетях, имеет «врожденные» недостатки защиты. То же самое можно сказать и о ряде служб Internet.

Набор протоколов управления передачей сообщений в Internet (Transmission Control Protocol/Internet Protocol – TCP/IP) используется для организации коммуникаций в неоднородной сетевой среде, обеспечивая совместимость между компьютерами разных типов. Совместимость – одно из основных преимуществ TCP/IP, поэтому большинство локальных компьютерных сетей поддерживает эти протоколы. Кроме того, протоколы TCP/IP предоставляют доступ к ресурсам глобальной сети Internet. Поскольку TCP/IP поддерживает маршрутизацию пакетов, он обычно используется в качестве межсетевого протокола. Благодаря своей популярности TCP/IP стал стандартом де-факто для межсетевого взаимодействия.

В заголовках пакетов TCP/IP Оказывается информация, которая может подвергнуться нападениям хакеров. В частности, хакер может подменить адрес отправителя в своих «вредоносных» пакетах, после чего они будут выглядеть, как пакеты, передаваемые авторизированным клиентом.

Отметим «врожденные слабости» некоторых распространенных служб Internet.

Простой протокол передачи электронной почты (Simple Mail Transfer Protocol – SMTP) позволяет осуществлять почтовую транспортную службу Internet. Одна из проблем безопасности, связанная с этим протоколом, заключается в том, что пользователь не может проверить адрес отправителя в заголовке сообщения электронной почты. В результате хакер может послать во внутреннюю сеть большое количество почтовых сообщений, что приведет к перегрузке и блокированию работы почтового сервера.

Sendmail. Популярная в Internet программа электронной почты Sendmail использует для работы некоторую сетевую информацию – IP-адрес отправителя. Перехватывая сообщения, отправляемые с помощью Sendmail, хакер может употребить эту. информацию для нападений, например для спуфинга (подмены адресов).

Протокол передачи файлов (File Transfer Protocol – FTP) обеспечивает передачу текстовых и двоичных файлов, поэтому его часто используют в Internet для организации совместного доступа к информации. Его обычно рассматривают как один из методов работы с удаленными сетями. На FTP-серверах хранятся документы, программы, графика и другие виды информации, К данным этих файлов на FTP-серверах нельзя обратиться напрямую. Это можно сделать, только переписав их целиком с FTP-сервера на локальный сервер. Некоторые FTP-серверы ограничивают доступ пользователей к своим архивам данных с помощью пароля, другие же предоставляют свободный доступ (так называемый анонимный FTP-сервер). При использовании опции анонимного FTP для своего сервера пользователь должен быть уверен, что на нем хранятся только файлы, предназначенные для свободного распространения.

Служба сетевых имен (Domain Name System – DNS) представляет собой распределенную базу данных, которая преобразует имена пользователей и хост-компьютеров в IP-адреса, указываемые в заголовках пакетов, и наоборот. DNS также хранит информацию о структуре сети компании, например количестве компьютеров с IP-адресами в каждом домене. Одной из проблем DNS является то, что эту базу данных очень трудно «скрыть» от неавторизированных пользователей. В результате DNS часто используется хакерами как источник информации об именах доверенных хост- компьютеров.

Служба эмуляции удаленного терминала (TELNET) употребляется для подключения к удаленным системам, присоединенным к сети; применяет базовые возможности по эмуляции терминала. При использовании этого сервиса Internet пользователи должны регистрироваться на сервере TELNET, вводя свои имя и пароль. После аутентификации пользователя его рабочая станция функционирует в режиме «тупого» терминала, подключенного к внешнему хост-компьютеру. С этого терминала пользователь может вводить команды, которые обеспечивают ему доступ к файлам и запуск программ. Подключившись к серверу TELNET, хакер может сконфигурировать его программу таким образом, чтобы она записывала имена и пароли пользователей.

Всемирная паутина (World Wide Web – WWW) – это система, основанная на сетевых приложениях, которые позволяют пользователям просматривать содержимое различных серверов в Internet или интрасетях. Самым полезным свойством WWW является использование гипертекстовых документов, в которые встроены ссылки на другие документы и Web-узлы, что дает пользователям возможность легко переходить от одного узла к другому. Однако это же свойство является и наиболее слабым местом системы WWW, поскольку ссылки на Web-узлы, хранящиеся в гипертекстовых документах, содержат информацию о том, как осуществляется доступ к соответствующим узлам. Используя эту информацию, хакеры могут разрушить Web-узел или получить доступ к хранящейся в нем конфиденциальной информации.

К уязвимым службам и протоколам Internet относятся также протокол копирования UUCP, протокол маршрутизации RIP, графическая оконная система X Windows и др.

Решение о том, фильтровать ли с помощью межсетевого экрана конкретные протоколы и адреса, зависит от принятой в защищаемой сети политики безопасности. Межсетевой экран является набором компонентов, настраиваемых таким образом, чтобы реализовать выбранную политику безопасности. В частности, необходимо решить, будет ли ограничен доступ пользователей к определенным службам Internet на базе протоколов TCP/IP и если будет, то до какой степени.

Политика сетевой безопасности

Политика сетевой безопасности каждой организации должна включать две составляющие:

- политику доступа к сетевым сервисам;
- политику реализации межсетевых экранов.

В соответствии с политикой доступа к сетевым сервисам определяется список сервисов Internet, к которым пользователи должны иметь ограниченный доступ. Задаются также ограничения на методы доступа, например, на использование протоколов SLIP (Serial Line Internet Protocol) и PPP (Point-to-Point Protocol). Ограничение методов доступа необходимо для того, чтобы пользователи не могли обращаться к «запрещенным» сервисам Internet обходными путями. Например, если для ограничения доступа в Internet сетевой администратор устанавливает специальный шлюз, который не дает возможности пользователям работать в системе WWW, они могли бы установить PPP-соединения с Web-серверами по коммутируемой линии.

Политика доступа к сетевым сервисам обычно основывается на одном из следующих принципов:

- запретить доступ из Internet во внутреннюю сеть, но разрешить доступ из внутренней сети в Internet;
- разрешить ограниченный доступ во внутреннюю сеть из Internet, обеспечивая работу только отдельных «авторизированных» систем, например почтовых серверов.

В соответствии с политикой реализации межсетевых экранов определяются правила доступа к ресурсам внутренней сети. Прежде всего необходимо установить, насколько «доверительной» или «подозрительной» должна быть система защиты. Иными словами, правила доступа к внутренним ресурсам должны базироваться на одном из следующих принципов:

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

Реализация межсетевого экрана на основе первого принципа обеспечивает значительную защищенность. Однако правила доступа, сформулированные в соответствии с этим принципом, могут доставлять большие неудобства пользователям, а кроме того, их реализация обходится достаточно дорого. При реализации второго принципа внутренняя сеть оказывается менее защищенной от нападений хакеров, однако пользоваться ей будет удобнее и потребуется меньше затрат.

Эффективность защиты внутренней сети с помощью межсетевых экранов зависит не только от выбранной политики доступа к сетевым сервисам и ресурсам внутренней сети, но и от рациональности выбора и использования основных компонентов межсетевого экрана.

Функциональные требования к межсетевым экранам включают:

- требования к фильтрации на сетевом уровне;
- требования к фильтрации на прикладном уровне;
- требования по настройке правил фильтрации и администрированию;
- требования к средствам сетевой аутентификации;
- требования по внедрению журналов и учету.

Основные компоненты межсетевых экранов

Межсетевые экраны состоят из множества компонентов, которые работают вместе для обеспечения безопасности сети. Они фильтруют трафик, контролируют соединения, анализируют данные на уровне приложений и защищают от атак. Современные решения объединяют эти функции для комплексной защиты.

Компоненты межсетевых экранов:

1. Фильтры пакетов (Фильтрующие маршрутизаторы, Packet Filters): анализируют входящие и исходящие пакеты на основе заданных правил (например, IP-адресов, портов, протоколов), пропускают или блокируют пакеты в зависимости от соответствия правилам.
2. Шлюз сеансового уровня (Шлюз сетевого уровня, система трансляции сетевых адресов, Circuit-Level Gateway): контролирует установление соединений между внутренней и внешней сетями, проверяет легитимность сеансов связи, не анализируя содержимое пакетов.
3. Шлюз прикладного уровня (Application-Level Gateway, прокси-сервер): анализирует трафик на уровне приложений (например, HTTP, FTP, SMTP), перехватывает запросы от клиентов, проверяет их и передает на сервер от своего имени.
4. Инспектор состояния (Stateful Inspection): отслеживает состояние активных соединений и анализирует пакеты в контексте этих соединений, охраняет информацию о текущих сеансах и проверяет, соответствуют ли пакеты ожидаемому состоянию.
5. Система предотвращения вторжений (Intrusion Prevention System, IPS): обнаруживает и блокирует попытки атак или несанкционированного доступа., анализирует трафик на наличие известных сигнатур атак или аномального поведения
6. Система обнаружения вторжений (Intrusion Detection System, IDS): выполняет мониторинг сетевого трафика для выявления подозрительной активности, анализирует трафик и уведомляет администратора о потенциальных угрозах.
7. Межсетевой экран следующего поколения (Next-Generation Firewall, NGFW): объединяет функции традиционного межсетевого экрана с дополнительными возможностями, такими как анализ на уровне приложений, интеграция с IPS, фильтрация контента и защита от угроз, использует глубокий анализ пакетов (Deep Packet Inspection, DPI) для выявления сложных угроз.

8. База правил (Rule Base): содержит набор правил, определяющих, какой трафик разрешен, а какой заблокирован, правила применяются последовательно, и первое совпадение определяет действие (разрешить или запретить).

9. Журналы и отчеты (Logs and Reporting): регистрирует все события, связанные с работой межсетевого экрана, сохраняет информацию о попытках доступа, блокировках, атаках и других событиях.

10. Интерфейсы управления: позволяют администраторам настраивать и управлять работой межсетевого экрана через веб-интерфейс, командную строку или специализированное ПО.

Рассмотрим каждый компонент более подробно.

Фильтры пакетов (фильтрующие маршрутизаторы)

Фильтрующий маршрутизатор представляет собой маршрутизатор или работающую на сервере программу, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Фильтрация пакетов осуществляется на основе ин формации, содержащейся в TCP- и IP-заголовках пакетов. Процесс инкапсуляции передаваемых данных и формирования TCP- и IP-заголовков пакетов с данными в стеке протоколов TCP/IP показан на рисунке 2.

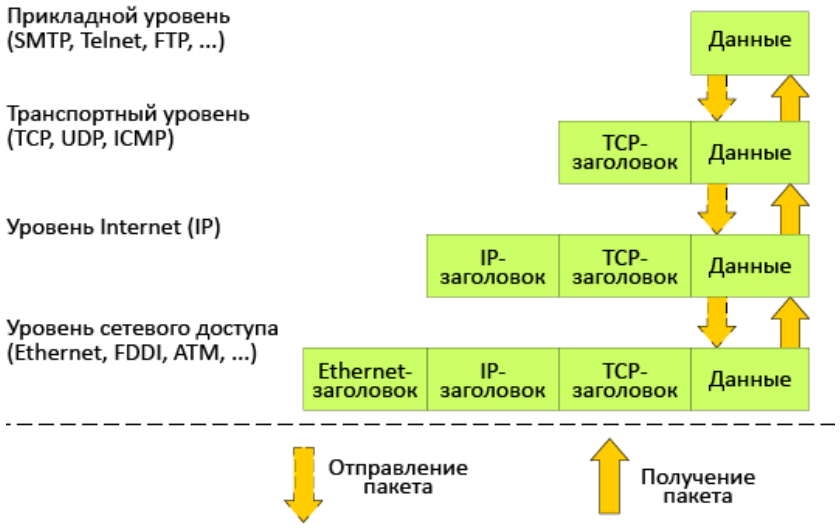

Рисунок 2: Схема инкапсуляции данных в стеке протоколов TCP

Фильтрующий маршрутизатор обычно может фильтровать IP-пакеты на основе группы следующих полей заголовка пакета:

- IP-адрес отправителя (адрес системы, которая послала пакет);
- IP-адрес получателя (адрес системы, которая принимает пакет);
- порт отправителя (порт соединения в системе-отправителе);

– порт получателя (порт соединения в системе-получателе).

Порт – это программное понятие, которое используется клиентом или сервером для посылки или приема сообщений; порт идентифицируется 16-битовым числом.

В настоящее время не все фильтрующие маршрутизаторы фильтруют пакеты по TCP/UDP-порту отправителя, однако многие производители маршрутизаторов начали обеспечивать такую возможность. Некоторые маршрутизаторы проверяют, с какого сете вого интерфейса маршрутизатора пришел пакет, и затем используют эту информацию как дополнительный критерий фильтрации.

Фильтрация может быть реализована различным образом для блокирования соединений с определенными хост-компьютерами или портами. Например, можно блокировать соединения, идущие от конкретных адресов тех хост-компьютеров и сетей, которые считаются враждебными или ненадежными.

Добавление фильтрации по портам TCP и UDP к фильтрации по IP-адресам обеспечивает большую гибкость. Известно, что такие серверы, как демон TELNET, обычно связаны с конкретными портами (например, порт 23 протокола TELNET). Если межсетевой экран может блокировать соединения TCP или UDP с определенными портами или от них то можно реализовать политику безопасности, при которой некоторые виды соединений устанавливаются только с конкретными хост-компьютерами.

Например, внутренняя сеть может блокировать все входные соединения со всеми хост-компьютерами за исключением нескольких систем. Для этих систем могут быть разрешены только определенные сервисы (SMTP для одной системы и TELNET или FTP – для другой). При фильтрации по портам TCP и UDP эта политика может быть реализована фильтрующим маршрутизатором или хост-компьютером с возможностью фильтрации пакетов (см. рисунок 3).

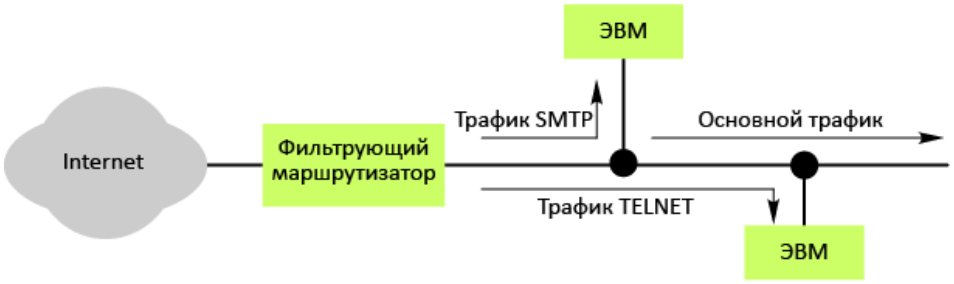

Рисунок 3: Схема фильтрации трафика

В качестве примера работы фильтрующего маршрутизатора рассмотрим реализацию политики безопасности, допускающей определенные соединения с внутренней сетью с адресом 123.4.*.* Соединения TELNET

разрешаются только с одним хост-компьютером с адресом 123.4.5.6, который может быть прикладным TELNET-шлюзом, а SMTP-соединения – только с двумя хост-компьютерами с адресами 123.4.5.7 и 123.4.5.8, которые могут быть двумя шлюзами электронной почты. Обмен по NNTP (Network News Transfer Protocol) разрешается только от сервера новостей с адресом 129.6.48.254 и только с NNTP-сервером сети с адресом 123.4.5.9, а протокол NTP (сетевого времени)-для всех хост-компьютеров. Все другие серверы и пакеты блокируются. Соответствующий набор правил сведен в таблице:

Тип	Адрес отправителя	Адрес получателя	Порт отправителя	Порт получателя	Действие
TCP	*	123.4.5.6	>1023	23	Разрешить
TCP	*	123.4.5,7	>1023	25	Разрешить
TCP	*	123.4.5.8	>1023	25	Разрешить
TCP	129.6.48.254	123.4.5.9	>1023	119	Разрешить
UDP	*	123.4.*.*	>1023	123	Разрешить
*	*	*	*	*	Запретить

Первое правило позволяет пропускать пакеты TCP из сети Internet от любого источника с номером порта большим, чем 1023, к получателю с адресом 123.4.5.6 в порт 23. Порт 23 связан с сервером TELNET, а все клиенты TELNET должны иметь непривилегированные порты с номерами не ниже 1024.

Второе и третье правила работают аналогично и разрешают передачу пакетов к получателям с адресами 123.4.5.7 и 123.4.5.8 в порт 25, используемый SMTP.

Четвертое правило пропускает пакеты к NNTP-серверу сети, но только от отправителя с адресом 129.6.48.254 к получателю с адресом 123.4.5.9 с портом назначения 119 (129.6.48.254 – единственный NNTP-сервер, от которого внутренняя сеть получает новости, поэтому доступ к сети для выполнения протокола NNTP ограничен только этой системой).

Пятое правило разрешает трафик NTP, который использует протокол UDP вместо TCP, от любого источника к любому получателю внутренней сети.

Наконец, шестое правило блокирует все остальные пакеты. Если бы этого правила не было, маршрутизатор мог бы блокировать, а мог бы и не блокировать другие типы пакетов. Выше был рассмотрен очень простой пример фильтрации пакетов. Реально используемые правила позволяют осуществить более сложную фильтрацию и являются более гибкими.

Правила фильтрации пакетов формулируются сложно, и обычно нет средств для тестирования их корректности, кроме медленного ручного тестирования. У некоторых фильтрующих маршрутизаторов нет средств протоколирования, поэтому, если правила фильтрации пакетов все-таки позволят опасным пакетам пройти через маршрутизатор, такие пакеты не смогут быть выявлены до обнаружения последствий проникновения.

Даже если администратору сети удастся создать эффективные правила фильтрации, их возможности остаются ограниченными. Например, администратор задает правило, в соответствии с которым маршрутизатор будет отбраковывать все пакеты с неизвестным адресом отправителя. Однако хакер может использовать в качестве адреса отправителя в своем «вредоносном» пакете реальный адрес доверенного (авторизированного) клиента. В этом случае фильтрующий маршрутизатор не сумеет отличить поддельный пакет от настоящего и пропустит его. Практика показывает, что подобный вид нападения, называемый подменой адреса, довольно широко распространен в сети Internet и часто оказывается эффективным.

Межсетевой экран с фильтрацией пакетов, работающий только на сетевом уровне эталонной модели взаимодействия открытых систем OSI-ISO, обычно проверяет информацию, содержащуюся только в IP-заголовках пакетов. Поэтому обмануть его несложно: хакер создает заголовок, который удовлетворяет разрешающим правилам фильтрации. Кроме заголовка пакета, никакая другая содержащаяся в нем информация межсетевыми экранами данной категории не проверяется.

К положительным качествам фильтрующих маршрутизаторов следует отнести:

- сравнительно невысокую стоимость;
- гибкость в определении правил фильтрации;
- небольшую задержку при прохождении пакетов.

Недостатками фильтрующих маршрутизаторов являются:

- внутренняя сеть видна (маршрутизируется) из сети Internet;
- правила фильтрации пакетов трудны в описании и требуют очень хороших знаний технологий TCP и UDP;
- при нарушении работоспособности межсетевого экрана с фильтрацией пакетов все компьютеры за ним становятся полностью незащищенными либо недоступными;
- аутентификацию с использованием IP-адреса можно обмануть путем подмены IP-адреса (атакующая система выдает себя за другую, используя ее IP-адрес);
- отсутствует аутентификация на пользовательском уровне.

Шлюз сеансового уровня (шлюз сетевого уровня)

Шлюз сетевого уровня иногда называют системой трансляции сетевых адресов или шлюзом сеансового уровня модели OSI. Такой шлюз исключает прямое взаимодействие между авторизированным клиентом и внешним хост-компьютером.

Шлюз сетевого уровня принимает запрос доверенного клиента на конкретные услуги и после проверки допустимости запрошенного сеанса устанавливает соединение с внешним хост-компьютером. После этого шлюз копирует пакеты в обоих направлениях, не осуществляя их фильтрации.

Шлюз следит за подтверждением (квитированием) связи между авторизированным клиентом и внешним хост-компьютером, определяя, является ли запрашиваемый сеанс связи допустимым. Чтобы выявить допустимость запроса на сеанс, связи, шлюз выполняет следующую процедуру.

Когда авторизированный клиент запрашивает некоторый сервис, шлюз принимает этот запрос, проверяя, удовлетворяет ли этот клиент базовым критериям фильтрации (например, может ли DNS-сервер определить IP-адрес клиента и ассоциированное с ним имя). Затем, действуя от имени клиента, шлюз устанавливает соединение с внешним хост-компьютером и следит за выполнением процедуры квитирования связи по протоколу TCP. Эта процедура состоит из обмена TCP-пакетами, которые помечаются флагами SYN (синхронизировать) и ACK (подтвердить) (см. рисунок 4).

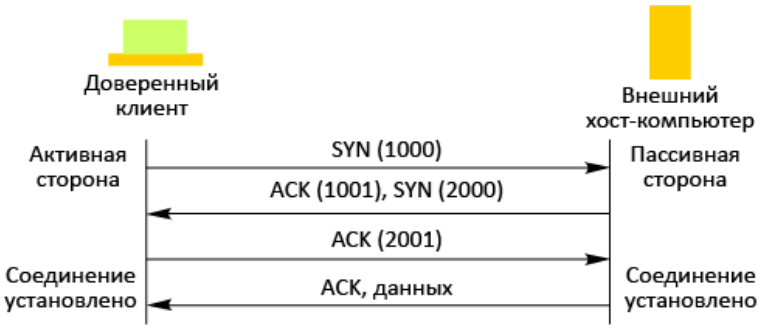

Рисунок 4: Последовательность передачи пакетов

Первый пакет сеанса TCP, помеченный флагом SYN и содержащий произвольное число, например 1000, является запросом клиента на открытие сеанса. Внешний хост-компьютер, получивший этот пакет, посылает в ответ пакет, помеченный флагом ACK и содержащий число, на единицу большее, чем в принятом пакете (в нашем случае 1001), подтверждая тем самым прием пакета SYN от клиента.

Далее осуществляется обратная процедура: хост-компьютер посылает клиенту пакет SUN с исходным числом (например, 2000), а клиент

подтверждает его получение передачей пакета ACK, содержащего число 2001. На этом процесс квитирования связи завершается.

Шлюз сетевого уровня признает запрошенное соединение допустимым только в том случае, если при выполнении процедуры квитирования связи флаги SYN и ACK., а также числа, содержащиеся в TCP-пакетах, оказываются логически связанными между собой.

После того как шлюз определил, что доверенный клиент и внешний хост-компьютер являются авторизированными участниками сеанса TCP, и проверил допустимость этого сеанса, он устанавливает соединение. Начиная с этого момента, шлюз копирует и перенаправляет пакеты туда и обратно, не проводя никакой фильтрации. Он поддерживает таблицу установленных соединений, пропуская данные, относящиеся к одному из сеансов связи, зафиксированных в этой таблице. Когда сеанс завершается, шлюз удаляет соответствующий элемент из таблицы и разрывает цепь, использовавшуюся в данном сеансе.

Для копирования и перенаправления пакетов в шлюзах сетевого уровня применяются специальные приложения, которые называют канальными посредниками, поскольку они устанавливают между двумя сетями виртуальную цепь или канал, а затем разрешают пакетам, которые генерируются приложениями TCP/IP, проходить по этому каналу. Канальные посредники поддерживают несколько служб TCP/IP, поэтому шлюзы сетевого уровня могут использоваться для расширения возможностей шлюзов прикладного уровня, работа которых основывается на программах-посредниках конкретных приложений.

Фактически большинство шлюзов сетевого уровня не являются самостоятельными продуктами, а поставляются в комплекте со шлюзами прикладного уровня. Примерами таких шлюзов являются Gauntlet Internet Firewall компании Trusted Information Systems, Alta Vista Firewall компании DEC и ANS Interlock компании ANS. Например, Alta Vista Firewall использует канальные посредники прикладного уровня для каждой из шести служб TCP/IP, к которым относятся, в частности, FTP, HTTP (Hyper Text Transport Protocol) и TELNET. Кроме того, межсетевой экран компании DEC обеспечивает шлюз сетевого уровня, поддерживающий другие общедоступные службы TCP/IP, такие как Gopher и SMTP, для которых межсетевой экран не предоставляет посредников прикладного уровня.

Шлюз сетевого уровня выполняет еще одну важную функцию защиты: он используется в качестве сервера-посредника. Этот сервер-посредник выполняет процедуру трансляции адресов, при которой происходит преобразование внутренних IP-адресов в один «надежный» IP-адрес. Этот

адрес ассоциируется с межсетевым экраном, из которого передаются все исходящие пакеты. В результате в сети со шлюзом сетевого уровня все исходящие пакеты оказываются отправленными из этого шлюза, что исключает прямой контакт между внутренней (авторизированной) сетью и потенциально опасной внешней сетью. IP-адрес шлюза сетевого уровня становится единственно активным IP-адресом, который попадает во внешнюю сеть. Таким образом, шлюз сетевого уровня и другие серверы-посредники защищают внутренние сети от нападений типа подмены адресов.

После установления связи шлюзы сетевого уровня фильтруют пакеты только на сеансовом уровне модели OSI, т.е. не могут проверять содержимое пакетов, передаваемых между внутренней и внешней сетью на уровне прикладных программ. И поскольку эта передача осуществляется «вслепую», хакер, находящийся во внешней сети, может «протолкнуть» свои «вредоносные» пакеты через такой шлюз. После этого хакер обратится напрямую к внутреннему Web-серверу, который сам по себе не может обеспечивать функции межсетевого экрана. Иными словами, если процедура квитирования связи успешно завершена, шлюз сетевого уровня установит соединение и будет «слепо» копировать и перенаправлять все последующие пакеты независимо от их содержимого.

Чтобы фильтровать пакеты, генерируемые определенными сетевыми службами, в соответствии с их содержимым необходим шлюз прикладного уровня.

Шлюз прикладного уровня

Для устранения ряда недостатков, присущих фильтрующим маршрутизаторам, межсетевые экраны должны использовать дополнительные программные средства для фильтрации сообщений сервисов типа TELNET и FTP. Такие программные средства называются полномочными серверами (серверами-посредниками), а хост-компьютер, на котором они выполняются, – шлюзом прикладного уровня.

Шлюз прикладного уровня исключает прямое взаимодействие между авторизированным клиентом и внешним хост-компьютером. Шлюз фильтрует все входящие и исходящие пакеты на прикладном уровне. Связанные с приложениями серверы-посредники перенаправляют через шлюз информацию, генерируемую конкретными серверами.

Для достижения более высокого уровня безопасности и гибкости шлюзы прикладного уровня и фильтрующие маршрутизаторы могут быть объединены в одном межсетевом экране. В качестве примера рассмотрим сеть, в которой с помощью фильтрующего маршрутизатора блокируются

входящие соединения TELNET и FTP. Этот маршрутизатор допускает прохождение пакетов TELNET или FTP только к одному хост-компьютеру – шлюзу прикладного уровня TELNET/FTP. Внешний пользователь, который хочет соединиться с некоторой системой в сети, должен сначала соединиться со шлюзом прикладного уровня, а затем уже с нужным внутренним хост-компьютером. Это осуществляется следующим образом:

1. сначала внешний пользователь устанавливает TELNET-соединение со шлюзом прикладного уровня с помощью протокола TELNET и вводит, имя интересующего его внутреннего хост-компьютера;
2. шлюз проверяет IP-адрес отправителя и разрешает или запрещает соединение в соответствии с тем или иным критерием доступа;
3. пользователю может потребоваться аутентификация (возможно, с помощью одноразовых паролей);
4. сервер-посредник устанавливает TELNET-соединение между шлюзом и внутренним хост-компьютером;
5. сервер-посредник осуществляет передачу информации между этими двумя соединениями;
6. шлюз прикладного уровня регистрирует соединение.

Этот пример наглядно показывает преимущества использования полномочных серверов-посредников.

1. Полномочные серверы-посредники пропускают только те службы, которые им поручено обслуживать. Иначе говоря, если шлюз прикладного уровня наделен полномочиями (и полномочными серверами-посредниками) для служб FTP и TELNET, то в защищаемой сети будут разрешены только FTP и TELNET, а все другие службы будут полностью блокированы. Для некоторых организаций такой вид безопасности имеет большое значение, так как он гарантирует, что через межсетевой экран будут пропускаться только те службы, которые считаются безопасными.
2. Полномочные серверы-посредники обеспечивают возможность фильтрации протокола. Например, некоторые межсетевые экраны, использующие шлюзы прикладного уровня, могут фильтровать FTP-соединения и запрещать использование команды FTP put, что гарантированно не позволяет пользователям записывать информацию на анонимный FTP-сервер.

В дополнение к фильтрации пакетов многие шлюзы прикладного уровня регистрируют все выполняемые сервером действия и, что особенно важно, предупреждают сетевого администратора о возможных нарушениях защиты. Например, при попытках проникновения в сеть извне BorderWare Firewall Server компании Secure Computing позволяет фиксировать адреса

отправителя и получателя пакетов, время, в которое эти попытки были предприняты, и используемый протокол. Межсетевой экран Black Hole компании Milkyway Networks регистрирует все действия сервера и предупреждает администратора о возможных нарушениях, посылая ему сообщение по электронной почте или на пейджер. Аналогичные функции выполняют и ряд других шлюзов прикладного уровня.

Шлюзы прикладного уровня позволяют обеспечить наиболее высокий уровень защиты, поскольку взаимодействие с внешним миром реализуется через небольшое число прикладных полномочных программ-посредников, полностью контролирующих весь входящий и выходящий трафик.

Шлюзы прикладного уровня имеют ряд серьезных преимуществ по сравнению с обычным режимом, при котором прикладной трафик пропускается непосредственно к внутренним хост-компьютерам. Перечислим эти преимущества.

3. Невидимость структуры защищаемой сети из глобальной сети Internet. Имена внутренних систем можно не сообщать внешним системам через DNS, поскольку шлюз прикладного уровня может быть единственным хост-компьютером, имя которого должно быть известно внешним системам.

4. Надежная аутентификация и регистрация. Прикладной трафик может быть аутентифицирован, прежде чем он достигнет внутренних хост-компьютеров, и может быть зарегистрирован более эффективно, чем с помощью стандартной регистрации.

5. Оптимальное соотношение между ценой и эффективностью. Дополнительные программные или аппаратные средства для аутентификации или регистрации нужно устанавливать только на шлюзе прикладного уровня.

6. Простые правила фильтрации. Правила на фильтрующем маршрутизаторе оказываются менее сложными, чем они были бы, если бы маршрутизатор сам фильтровал прикладной трафик и отправлял его большому числу внутренних систем. Маршрутизатор должен пропускать прикладной трафик, предназначенный только для шлюза прикладного уровня, и блокировать весь остальной трафик.

7. Возможность организации большого числа проверок. Защита на уровне приложений позволяет осуществлять большое количество дополнительных проверок, что снижает вероятность взлома с использованием «дыр» в программном обеспечении.

К недостаткам шлюзов прикладного уровня относятся:

– более низкая производительность по сравнению с фильтрующими маршрутизаторами; в частности, при использовании клиент-

серверных протоколов, таких как TELNET, требуется двухшаговая процедура для входных и выходных соединений;

– более высокая стоимость по сравнению с фильтрующими маршрутизаторами.

Помимо TELNET и FTP шлюзы прикладного уровня обычно используются для электронной почты, X Windows и некоторых других служб.

Инспектор состояния.

Инспектор состояния – это технология, используемая в современных межсетевых экранах для анализа сетевого трафика с учетом состояния активных соединений. В отличие от простых фильтров пакетов, которые анализируют каждый пакет независимо, инспектор отслеживает состояние сеансов связи и принимает решения на основе контекста соединения.

Основное назначение инспектора состояния это:

контроль состояния соединений, т.е. отслеживание установленных соединений и их параметров (например, IP-адреса, порты, протоколы, флаги TCP);

повышение безопасности – блокировка несанкционированного трафика, который не соответствует ожидаемому состоянию соединения;

оптимизация работы – уменьшение нагрузки на межсетевой экран за счет анализа только значимых пакетов;

Инспектор состояния обладает такими преимуществами как высокая безопасность (блокировка несанкционированных пакетов, которые не соответствуют ожидаемому состоянию соединения), эффективность (уменьшение нагрузки на межсетевой экран за счет анализа только значимых пакетов), гибкость (поддержка сложных протоколов и приложений, которые используют динамические порты (например, FTP, SIP)), защита от атак (предотвращение атак, таких как SYN-флуд, подделка пакетов и сканирование портов).

Недостатки инспектора состояния

сложность настройки: требуется тщательная настройка правил для корректной работы;

зависимость от состояния: если информация о состоянии соединения потеряна (например, из-за сбоя), это может привести к блокировке легитимного трафика;

ограниченная защита: инспектор не анализирует содержимое пакетов на уровне приложений, что делает его уязвимым для сложных атак.

Система предотвращения вторжений.

Система предотвращения вторжений (Intrusion Prevention System, IPS) — это технология, предназначенная для активного мониторинга и блокировки сетевого трафика с целью предотвращения кибератак. В отличие от систем обнаружения вторжений (IDS), которые только обнаруживают угрозы и уведомляют администратора, IPS активно вмешивается в трафик, блокируя подозрительные действия в реальном времени. Это делает IPS важным компонентом современной сетевой безопасности.

IPS работает на основе анализа сетевого трафика и сравнения его с базой данных известных сигнатур атак или с использованием методов анализа аномалий. Сигнатурный анализ позволяет обнаруживать известные угрозы, такие как эксплойты уязвимостей или вредоносное ПО. Анализ аномалий, в свою очередь, выявляет подозрительное поведение, которое может указывать на новые или неизвестные атаки. Например, IPS может блокировать попытки сканирования портов или подозрительные запросы к серверам.

Одним из ключевых преимуществ IPS является ее способность работать в режиме реального времени. Это позволяет предотвращать атаки до того, как они нанесут ущерб. Например, если злоумышленник пытается эксплуатировать уязвимость в веб-сервере, IPS может заблокировать этот трафик до того, как он достигнет цели. Однако для эффективной работы IPS требует регулярного обновления сигнатур и настройки, чтобы минимизировать ложные срабатывания.

IPS может быть реализована как отдельное устройство, встроенный модуль в межсетевой экран или программное решение. Она часто используется в сочетании с другими технологиями, такими как межсетевые экраны и системы обнаружения вторжений, для создания многоуровневой защиты. В современных сетях IPS играет критическую роль в предотвращении атак, таких как DDoS, SQL-инъекции, распространение вредоносного ПО и другие угрозы, обеспечивая безопасность данных и инфраструктуры.

Система обнаружения вторжений.

Система обнаружения вторжений (Intrusion Detection System, IDS) — это технология, предназначенная для мониторинга сетевого трафика или активности на хостах с целью выявления подозрительных действий или атак. В отличие от систем предотвращения вторжений (IPS), IDS не блокирует трафик, а только обнаруживает потенциальные угрозы и уведомляет

администратора. Это делает IDS важным инструментом для анализа и реагирования на инциденты безопасности.

IDS работает на основе двух основных методов: сигнатурного анализа и анализа аномалий. Сигнатурный анализ сравнивает сетевой трафик или действия на хостах с базой данных известных шаблонов атак, таких как эксплойты уязвимостей или вредоносное ПО. Анализ аномалий, в свою очередь, выявляет отклонения от нормального поведения, что позволяет обнаруживать новые или неизвестные угрозы. Например, IDS может обнаружить подозрительную активность, такую как сканирование портов или необычные запросы к серверу.

Одним из ключевых преимуществ IDS является ее способность работать в пассивном режиме, не влияя на производительность сети. Это позволяет использовать IDS для мониторинга крупных сетей без риска блокировки легитимного трафика. Однако IDS требует регулярного обновления сигнатур и настройки для минимизации ложных срабатываний, которые могут затруднить анализ и реагирование на реальные угрозы.

IDS может быть реализована как сетевая (NIDS), отслеживающая трафик на уровне сети, или как хоставая (HIDS), мониторящая активность на отдельных устройствах. Она часто используется в сочетании с другими системами безопасности, такими как межсетевые экраны и системы предотвращения вторжений, для создания комплексной защиты. В современных сетях IDS играет важную роль в раннем обнаружении атак, таких как DDoS, SQL-инъекции, распространение вредоносного ПО и другие угрозы, помогая предотвратить потенциальный ущерб.

Межсетевой экран следующего поколения.

Объединяет функции традиционного межсетевого экрана с дополнительными возможностями, такими как анализ на уровне приложений, интеграция с IPS, фильтрация контента и защита от угроз, использует глубокий анализ пакетов (Deep Packet Inspection, DPI) для выявления сложных угроз.

База правил.

База правил (Rule Base) — это набор предопределенных правил, которые используются в межсетевых экранах и других системах безопасности для контроля сетевого трафика. Эти правила определяют, какие действия должны быть выполнены с пакетами данных: разрешить, заблокировать или перенаправить. База правил является основным

механизмом, который позволяет администраторам гибко настраивать политики безопасности в зависимости от потребностей сети.

Каждое правило в базе обычно содержит критерии, такие как IP-адреса, порты, протоколы и направление трафика (входящий/исходящий). Например, правило может разрешать HTTP-трафик (порт 80) для определенного IP-адреса, но блокировать SSH-трафик (порт 22) из внешних сетей. Правила применяются последовательно, и первое совпадение определяет действие, которое будет выполнено с пакетом. Это требует тщательного планирования и упорядочивания правил для избежания конфликтов.

Эффективность базы правил зависит от ее актуальности и корректности. Администраторы должны регулярно обновлять и оптимизировать правила, чтобы адаптироваться к изменяющимся угрозам и требованиям сети. Например, добавление правил для блокировки новых типов атак или удаление устаревших правил, которые больше не актуальны. Хорошо настроенная база правил обеспечивает баланс между безопасностью и производительностью сети, минимизируя риски и ложные срабатывания.

Журналы и отчеты.

Журналы и отчеты − это важные компоненты систем безопасности, которые фиксируют все события, связанные с работой межсетевых экранов, систем обнаружения вторжений и других защитных механизмов. Журналы содержат подробную информацию о попытках доступа, блокировках, атаках и других событиях, что позволяет администраторам анализировать активность в сети и выявлять потенциальные угрозы. Они являются ключевым инструментом для аудита и расследования инцидентов безопасности.

Отчеты формируются на основе данных из журналов и предоставляют структурированную информацию о состоянии безопасности сети. Они могут включать статистику по атакам, списки заблокированных IP-адресов, данные о попытках несанкционированного доступа и другие метрики. Отчеты помогают администраторам оценивать эффективность текущих политик безопасности, выявлять уязвимости и принимать обоснованные решения для улучшения защиты. Регулярный анализ журналов и отчетов является важной частью поддержания высокого уровня безопасности в сети.

Интерфейсы управления.

Позволяют администраторам настраивать и управлять работой межсетевого экрана через веб-интерфейс, командную строку или

специализированное программного обеспечения. Интерфейсы управления предоставляют удобный доступ к настройкам правил фильтрации, мониторингу трафика, обновлению сигнатур и другим функциям, что делает их незаменимыми для эффективного администрирования.

Удобство и функциональность интерфейсов управления напрямую влияют на производительность работы администраторов. Современные интерфейсы часто включают визуализацию данных, такие как графики и диаграммы, что упрощает анализ сетевой активности и выявление угроз. Кроме того, они поддерживают удаленное управление, что особенно важно для крупных распределенных сетей. Хорошо разработанные интерфейсы управления помогают минимизировать время настройки и повышают общую эффективность систем безопасности.

Заключение

Межсетевые экраны являются важнейшим инструментом для обеспечения безопасности сетей, защищая их от несанкционированного доступа, атак и утечек данных. Их эффективность достигается за счет взаимодействия различных компонентов, каждый из которых выполняет свою уникальную функцию. Основные компоненты, такие как фильтры пакетов, инспекторы состояния, шлюзы прикладного уровня и системы предотвращения вторжений, работают вместе, чтобы обеспечить многоуровневую защиту.

Фильтры пакетов и инспекторы состояния обеспечивают базовую защиту на сетевом и транспортном уровнях, контролируя трафик на основе IP-адресов, портов и состояния соединений. Шлюзы прикладного уровня и системы предотвращения вторжений (IPS) добавляют более глубокий анализ, работая на уровне приложений и блокируя сложные атаки, такие как SQL-инъекции или распространение вредоносного ПО. Эти компоненты позволяют адаптировать защиту под конкретные угрозы и требования сети.

База правил, журналы и отчеты, а также интерфейсы управления играют ключевую роль в настройке и администрировании межсетевых экранов. База правил определяет политики безопасности, журналы и отчеты помогают анализировать события и выявлять угрозы, а интерфейсы управления обеспечивают удобство настройки и мониторинга. Эти компоненты делают работу администраторов более эффективной и позволяют оперативно реагировать на изменения в сетевой среде.

Современные межсетевые экраны, такие как Next-Generation Firewalls (NGFW), объединяют все эти компоненты в единое решение, добавляя дополнительные функции, такие как глубокий анализ пакетов (DPI), интеграция с облачными сервисами и защита от угроз нулевого дня. Это делает их универсальными инструментами для защиты как традиционных, так и современных сетевых инфраструктур.

В заключение можно сказать, что компоненты межсетевых экранов образуют комплексную систему, которая обеспечивает безопасность сети на всех уровнях. Их правильная настройка и взаимодействие позволяют эффективно противостоять как известным, так и новым угрозам, обеспечивая защиту данных, ресурсов и репутации организации. Постоянное развитие технологий и адаптация к изменяющимся условиям делают межсетевые экраны неотъемлемой частью любой системы информационной безопасности.

Список литературы

1. Назначение и принцип работы межсетевого экрана https://www.bfn.by/naznachenie-i-princzip-raboty-mezhsetevogo-ekrana

2. В. Ф. Шаньгин. Защита информации в компьютерных системах и сетях — ДМК Пресс. 2012. -593 с.

3. Поговорим об NGFW https://habr.com/ru/companies/otus/articles/734770/

4. Сергеева Т.И. Методы и средства защиты компьютерной информации: учеб. пособие / Т.И. Сергеева, М.Ю. Сергеев. Воронеж: ГОУВПО «Воронежский государственный технический университет», 2011. 230 с.