РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

Митюшин Дмитрий Алексеевич

Информационные технологии. Администрирование подсистем защиты информации

Тема 7. Администрирование межсетевых экранов

Вопросы:

1. *Защита периметра корпоративной сети*
2. *Демилитаризованная зона*
3. *Анализ содержимого почтового и веб-трафика*
4. *Обнаружение и устранение уязвимостей. Возможности сканеров безопасности*
5. *Введение в технологию обнаружения атак*

Литература

1. Бондарев, В. В. Введение в информационную безопасность автоматизированных си-стем : учебное пособие / В. В. Бондарев. - Москва : Издательство МГГУ им. Н. Э. Бау-мана, 2016. - 250, [2] с.: ил.
2. Демилитаризованная зона ISA. Windows IT Pro/RE, 2006, № 03 // https://www.osp.ru/winitpro/2006/03/1156406

1. Защита периметра корпоративной сети

1.1. Взаимодействие корпоративной сети с внешним миром

Периметр корпоративной сети должен быть защищён и в то же время иметь взаимодействие с окружающим миром.

Возможными точками взаимодействия с окружающим миром могут быть:

- точка подключения к сети Интернет;
- выделенные каналы, соединяющие филиалы друг с другом или обеспечивающие взаимодействие с сетями партнёров;
- клиентские приложения, нередко имеющие постоянное соединение с ресурсами, расположенными в недоверенных сетях;
- сегменты, обеспечивающие удалённый доступ к сети, включая доступ посредством виртуальных частных сетей (Virtual Private Network, VPN);
- беспроводные сегменты, позволяющие нарушать границы сети на физическом и канальном уровнях.

Виртуальные частные сети позволяют предоставить удалённым мобильным пользователям, где бы они ни находились, безопасный доступ к корпоративным ЛВС, а партнёрам и клиентам – безопасный доступ к определённым внутренним информационным ресурсам организации за счёт создания криптографически защищённых туннелей для пересылки данных из одной конечной точки в другую.

1. Защита периметра корпоративной сети

1.1. Взаимодействие корпоративной сети с внешним миром

В современных условиях границы сетей становятся все более «размытыми». Иногда говорят, что точка периметра находится на границе между двумя сетями с разными политиками безопасности. Возможные названия этих областей приведены на рис. 1.

Рис. 1. Граница между двумя сетями с разными политиками безопасности

1. Защита периметра корпоративной сети

1.1. Взаимодействие корпоративной сети с внешним миром

В статье [Защита периметра и «сеть без границ» https://www.osp.ru/lan/2014/02/13039888] говорится, что, учитывая стремительное распространение мобильных устройств, концепции BYOD, облачных вычислений и различных технологий для удалённой работы, всё чаще приходится слышать об исчезновении периметра корпоративной сети, однако концепция его защиты не устарела, она лишь нуждается в адаптации к современным условиям.

Немногие решатся отказаться от межсетевых экранов и шлюзов безопасности.

Тем не менее использование облачных вычислений, мобильных устройств и виртуализации приводит к размыванию традиционной защиты периметра – ее приходится распространять как за границы, так и внутрь сети.

Это явление получило название «депериметризация»: с расширением способов доступа к корпоративным ресурсам и приложениям у сети больше нет единой точки входа.

К тому же новые технологии и тенденции требуют иных подходов к организации защиты корпоративной сети.

1. Защита периметра корпоративной сети

1.1. Взаимодействие корпоративной сети с внешним миром

«Концепция традиционного периметра как чётко очерченной и неизменяемой границы сети все ещё применяется теми организациями, где с подозрением относятся к новомодным ИТ-течениям – облакам, BYOD, «Интернету вещей» и т. п.

Прежде всего это военные структуры, некоторые государственные органы, а также учреждения, обрабатывающие засекреченные сведения. В более современных организациях понятие традиционного периметра действительно исчезает, ему на смену приходит «нечёткий», или «размытый», периметр: граница сети динамически меняется и проходит по мобильным устройствам и облачной инфраструктуре, где хранятся защищаемые информационные активы», – поясняет Алексей Лукацкий, бизнес-консультант Cisco по информационной безопасности.

«Концепция защиты периметра пока не устарела, но все к этому идёт, – добавляет Андрей Прозоров, ведущий эксперт по информационной безопасности компании InfoWatch. – Ландшафт ИТ-инфраструктуры стремительно меняется, и специалистам по ИТ и ИБ необходимо адаптироваться к этим изменениям.

Надо чётко понимать, у кого есть права удалённого доступа к ресурсам сети,

1. Защита периметра корпоративной сети

1.1. Взаимодействие корпоративной сети с внешним миром

Одни пойдут по пути запрета, а другие организуют мониторинг или предложат пользователям удобные и защищённые сервисы. В целом использование внешних сервисов и персональных устройств для обработки корпоративной информации все ещё не очень распространено в России».

Однако, по данным зарубежной статистики, более половины деловых коммуникаций и транзакций сегодня уже осуществляется вне корпоративной сети. Малые компании могут обойтись и без традиционной ИТ-инфраструктуры, используя облачные сервисы (IaaS) и клиентские устройства, а средние и крупные организации выбирают для себя аутсорсинг ИТ, BYOD, облачные приложения и различные способы доставки приложений и данных. Обеспечить защиту корпоративных данных становится все сложнее. Изменения, происходящие сейчас в данной области, наверно, самые значительные за всю историю информационной безопасности.

На рис. 2 перечислены каналы, через которые в корпоративную сеть может попасть какая-либо информация или, наоборот, уйти из неё.

Разумеется, информация может попасть в сеть (или «уйти» из неё) и через различные портативные устройства (флэш-карты, диски и т. п.), однако эти вопросы касаются физической безопасности и в рамках данного курса не

1. Защита периметра корпоративной сети

1.1. Взаимодействие корпоративной сети с внешним миром

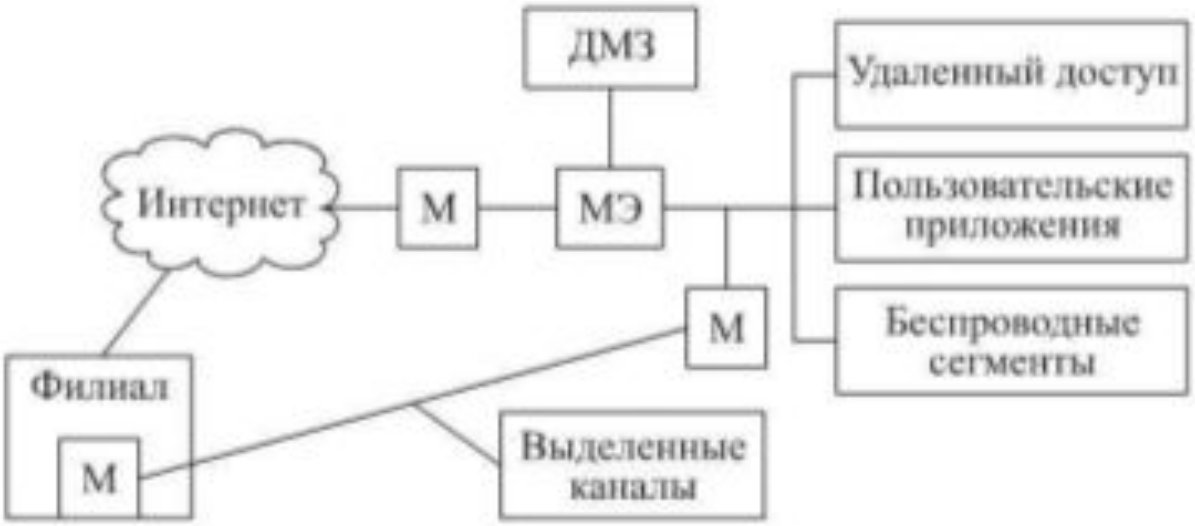

Рис. 2. Каналы поступления информации в корпоративную сеть

1. Защита периметра корпоративной сети

1.2. Угрозы, связанные с периметром корпоративной сети

Задачи, которые требуется решать в ходе защиты периметра сети, вытекают из тех угроз, источником которых и является существование сетевого периметра.

Прежде всего, это атаки на внешние ***ресурсы***, находящиеся в демилитаризованной зоне (рис. 3).

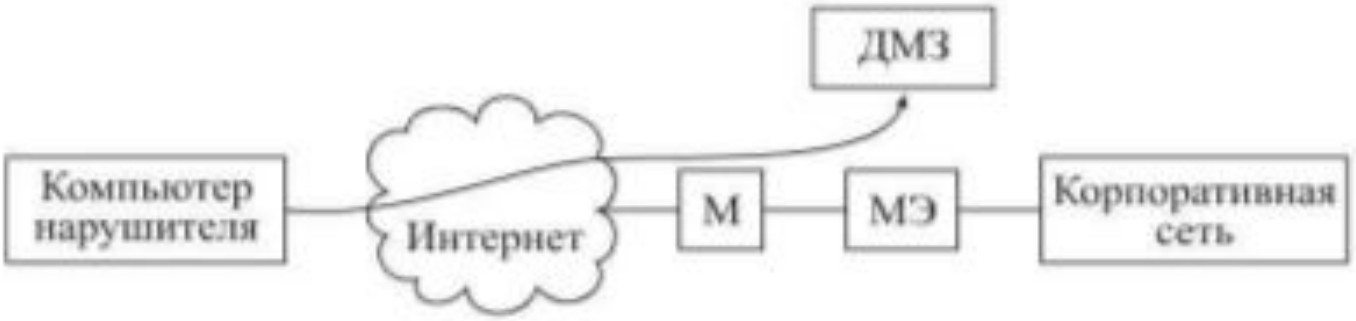

Рис. 3. Атаки на внешние ресурсы

1. Защита периметра корпоративной сети

1.2. Угрозы, связанные с периметром корпоративной сети

К таким ресурсам, например, относят почтовый сервер, DNS-сервер и т. п. Отдельно следует упомянуть проблему ***спама***, которая частично может быть решена средствами защиты периметра.

Поскольку точкой периметра можно считать и клиентские приложения, одной из угроз является возможность проникновения в сеть ***вредоносного кода*** – вирусов, «червей», шпионского ПО (рис. 4).

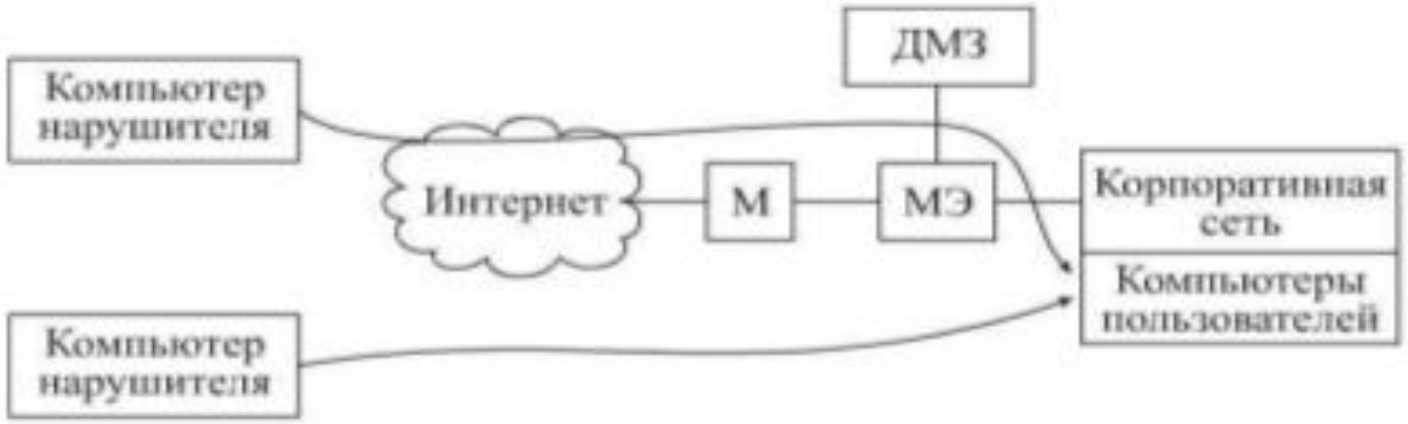

Рис. 4. Атаки на клиентское программное обеспечение

1. Защита периметра корпоративной сети

1.2. Угрозы, связанные с периметром корпоративной сети

Ещё одна точка подключения к корпоративной сети – ***удалённый доступ***, обычно осуществляющийся с использованием технологий VPN. При этом незащищённые клиенты VPN могут представлять собой дополнительную угрозу, поскольку, с одной стороны, они имеют соединение с внутренней сетью, с другой – с той сетью, из которой осуществляется подключение.

Сети, с которыми осуществляется связь по выделенным каналам, могут иметь разный уровень доверия, соответственно, здесь также нужен контроль.

Беспроводные устройства (точка доступа или просто ноутбук, имеющий как проводной, так и беспроводной сетевые интерфейсы) также являются частью сетевого периметра. К тому же они делают возможным нарушение границ на канальном или физическом уровне, поскольку точка доступа может быть «продолжением» коммутатора, а это значит, что для подключения к сети уже не потребуются кабель и розетка.

Наконец, стоит упомянуть и ***угрозу утечки критичной информации***, вследствие того, что точка периметра, как уже отмечалось, лежит на границе между доверенной и недоверенной сетями.

1. Защита периметра корпоративной сети

1.3. Составляющие защиты периметра

Защита периметра – это обеспечение безопасности при осуществлении электронного обмена информацией с другими сетями, разграничение доступа между сегментами корпоративной сети, а также защита от проникновения и вмешательства в работу корпоративной сети нарушителей из внешних систем.

Для нейтрализации угроз механизм защиты периметра имеет несколько составляющих:

- ***фильтрация трафика*** – позволяет «отсечь» лишний трафик и оставить только разрешённые сетевые протоколы. Это своеобразное разграничение доступа, работающее на сетевом уровне. Обычно фильтрация трафика сопровождается также трансляцией сетевых адресов, что позволяет скрыть структуру защищаемой сети. Помимо фильтрации трафика, возникает задача его защиты при передаче по недоверенным сетям, что подразумевает обеспечение его конфиденциальности, аутентичности и целостности. Для этого обычно используются технологии построения виртуальных частных сетей;
- ***противодействие сетевым атакам***, с помощью которого в оставшемся (разрешённом) сетевом трафике осуществляется поиск признаков атак;
- ***анализ содержимого*** (Content Security) – для более тщательного анализа некоторых разновидностей трафика (например, HTTP, POP3, SMTP, FTP).

1. Защита периметра корпоративной сети

1.3. Составляющие защиты периметра

Задача анализа содержимого распадается на несколько подзадач:

- веб-фильтр;
- антивирусная защита;
- защита от спама;
- контроль утечек критичной информации;
- контроль беспроводных сегментов.

Несанкционированно установленная в сети точка доступа позволяет подключиться к корпоративной сети и использовать ее ресурсы в обход средств защиты периметра.

1. Защита периметра корпоративной сети

1.4. Межсетевые экраны

Как было отмечено, задача защиты периметра заключается в контроле его отдельных точек. Обычно для этого устанавливают межсетевые экраны.

Имеется огромное количество определений ***межсетевого экрана***, одно из них, кажущееся вполне логичным, представлено в документе RFC 4949 (Internet Security Glossary), где МЭ (firewall) определяется как шлюз, ограничивающий прохождение сетевого трафика между подключёнными к нему сегментами.

Шлюз (gateway) – устройство, обеспечивающее обмен информацией между двумя или несколькими подключёнными к нему компьютерными сетями (сетевыми сегментами) со схожими функциями, но с различной реализацией (различные сетевые технологии или различные стеки протоколов) и позволяющее узлам из различных сегментов связываться друг с другом.

Необходимо сделать несколько уточнений:

1) взаимодействие может быть как однонаправленным, так и двунаправленным;
2) возможен широкий спектр различий между взаимодействующими сетями – от используемых протоколов до защитных механизмов.

1. Защита периметра корпоративной сети

1.4. Межсетевые экраны

Теоретически шлюзы могут быть реализованы на любом уровне модели OSI. На практике обычно применяют шлюзы канального (мосты), сетевого (маршрутизаторы) и прикладного (прокси-серверы) уровней.

Межсетевой экран в основном защищает небольшую сеть (корпоративную ЛВС или даже отдельный узел) от большой сети (например, Интернет).

С точки зрения ***архитектуры***, МЭ – не всегда отдельный узел (например, МЭ может состоять из двух пакетных фильтров и одного или нескольких посредников (proxy), подключённых к выделенной локальной сети, расположенной между двумя пакетными фильтрами). Внешний пакетный фильтр блокирует атаки на уровне IP, в то время как proxy блокируют атаки на уровнях выше IP. Внутренний маршрутизатор перенаправляет трафик из внутренней сети на посредников различных типов.

С точки зрения защищаемых ресурсов МЭ классифицируют следующим образом:

- периметровые или сетевые (network-based, защищающие целую сеть);
- персональные (host-based, контролирующие трафик отдельного узла).

Помимо МЭ общего характера, имеются специализированные МЭ (например,

1. Защита периметра корпоративной сети

1.4. Межсетевые экраны

Периметровые МЭ выполняют в основном в виде отдельного устройства, имеющего несколько сетевых интерфейсов; персональные МЭ представляют собой программное обеспечение, установленное на защищаемом узле.

Простейшая схема включения периметрового МЭ приведена на рис. 5.

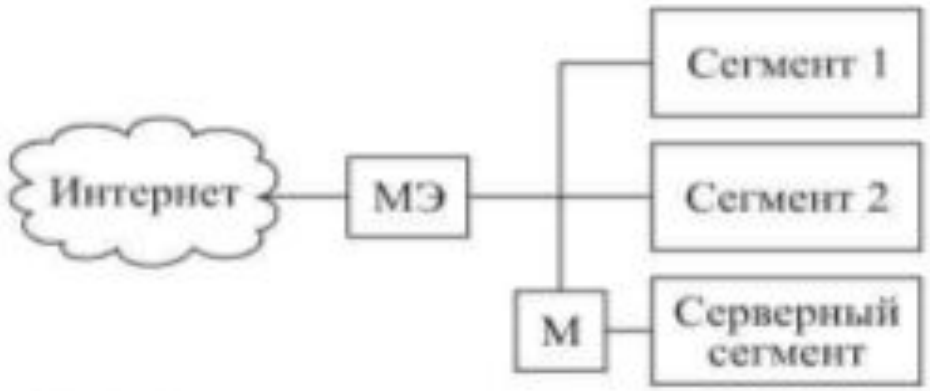

Рис. 5. Схема включения периметрового МЭ

1. Защита периметра корпоративной сети

1.4. Межсетевые экраны

В данном случае один из интерфейсов МЭ подключён к внешней (недоверенной) сети, другой – к внутренней (доверенной) сети. МЭ на данной схеме обеспечивает функции маршрутизатора между внешней и внутренней сетями. Внутренняя сеть состоит из нескольких областей, одна из которых (серверный сегмент) отделена маршрутизатором.

Ещё одна конфигурация (рис. 6) имеет демилитаризованную зону.

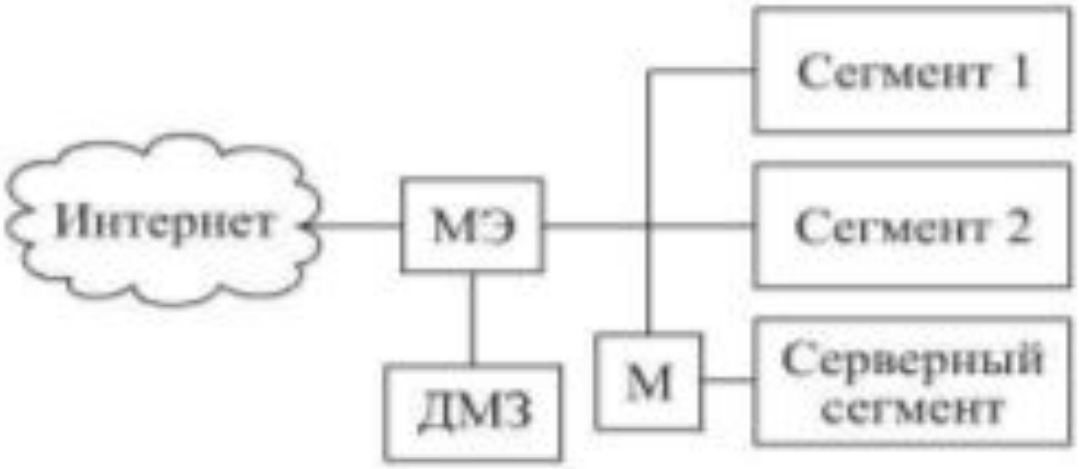

Рис. 6. Схема включения периметрового МЭ с ДМЗ – это изолированный сегмент, прохождение трафика через который регламентируется правилами, заданными на МЭ (или другом устройстве разграничения доступа)

1. Защита периметра корпоративной сети

1.4. Межсетевые экраны

Существует две разновидности ДМЗ:

- граничная сеть (экранированная подсеть, ДМЗ типа «сэндвич») – сетевой сегмент, расположенный между двумя МЭ;
- тупиковая сеть – сетевой сегмент, подсоединённый к отдельному интерфейсу МЭ.

Прохождение трафика через ДМЗ регламентировано правилами установки МЭ, а трафик Интернета и внутренней сети не регулируется.

Основное назначение ДМЗ – предоставление доступа к различным службам клиентов, которые не входят в число доверенных лиц. В качестве примера можно привести:

1) размещение в ДМЗ таких узлов, как веб-сервер, почтовый сервер и разрешение доступа к ним со стороны пользователей;
2) разделение информационных потоков между внутренними сегментами корпоративной сети.

Таким образом, ДМЗ позволяет обеспечить безопасность серверов и разграничение доступа между сегментами внутренней сети. Кроме того, в ДМЗ можно сосредоточить средства обнаружения атак и дополнительно укрепить расположенные там узлы.

1. Защита периметра корпоративной сети

1.4. Межсетевые экраны

С помощью ДМЗ может быть организован гостевой беспроводной доступ. Трафик беспроводных клиентов маршрутизируется в Интернет, а межсетевой экран препятствует подключению к ресурсам внутренней сети.

Периметровые МЭ могут быть дополнены персональными МЭ, установленными на узлах, требующих введения дополнительного уровня защиты:

- отдельные внутренние серверы;
- VPN-клиенты;
- беспроводные клиенты;
- рабочие станции.

Систему персональных МЭ можно использовать, если нет возможности выделить в отдельный сегмент группу узлов, нуждающуюся в таком выделении.

Поскольку МЭ по своей природе это шлюз, который может быть реализован на любом уровне модели OSI, различают следующие типы МЭ по уровню, на котором он «вмешивается» в сетевое взаимодействие:

- мосты (мостовые МЭ);
- пакетные фильтры;
- посредники (шлюзы) уровня соединения;
- посредники (шлюзы) прикладного уровня.

1. Защита периметра корпоративной сети

1.4. Межсетевые экраны

Мостовые МЭ. Мостовые МЭ выполняют анализ фреймов канального уровня и перенаправляют их на нужный сетевой интерфейс. Они подключаются как бы «в разрыв кабеля» и не требуют изменения сетевых настроек (на уровне IP).

К достоинствам мостовых МЭ относят: «прозрачность» (мостовой МЭ просто пересылает фреймы после их анализа между сетевыми интерфейсами, поэтому нет необходимости в изменении существующих сетевых настроек и маршрутизации); защищённость от атак (сетевые интерфейсы мостового МЭ не имеют IP-адреса и поэтому невидимы для окружающего мира).

Пакетные фильтры. Это маршрутизатор, перенаправляющий сетевые пакеты в соответствии с заданной на нем политикой безопасности. Пакетный фильтр «вмешивается» в сетевое взаимодействие на сетевом уровне модели OSI, при этом в качестве критериев фильтрации используется информация из заголовков протоколов сетевого и транспортного уровней (IP, TCP, UDP, ICMP).

Принятие решения происходит на основе правил фильтрации, которые можно представить в виде таблицы. Момент срабатывания правил может варьироваться, обычно это происходит до принятия решения о маршрутизации.

1. Защита периметра корпоративной сети

1.4. Межсетевые экраны

Схема алгоритма работы пакетного фильтра представлена на рис. 7.

Рис. 7. Алгоритм работы пакетного фильтра

1. Защита периметра корпоративной сети

1.4. Межсетевые экраны

После поступления очередного пакета происходит просмотр значимых полей, т. е. тех, которые имеют значение при применении критериев фильтрации (например, это могут быть отдельные поля заголовков сетевого и транспортного уровней).

Затем к пакету применяются имеющиеся правила (по очереди, до первого подошедшего). Если правило явно разрешает прохождение пакета, то просмотр правил прекращается и пакет пропускается. Если правило явно запрещает прохождение пакета, он отбрасывается, просмотр правил прекращается. Если ни одно из имеющихся правил не подошло, пакет также отбрасывается.

Работа алгоритма пакетного фильтра основана на принципе «Запрещено все, что не разрешено».

Правила фильтрации следуют в строго определённом порядке и применяются к пакету в соответствии с этим порядком.

Простейшие пакетные фильтры имеют ряд недостатков, основным из которых является отсутствие контроля соединения (статичность). Это означает, что пакетный фильтр манипулирует отдельными пакетами, не учитывая принадлежности пакета к какому-либо соединению, ни, тем более, сопоставляя

1. Защита периметра корпоративной сети

1.4. Межсетевые экраны

Следующий пример иллюстрирует этот основной недостаток пакетных фильтров (рис. 8).

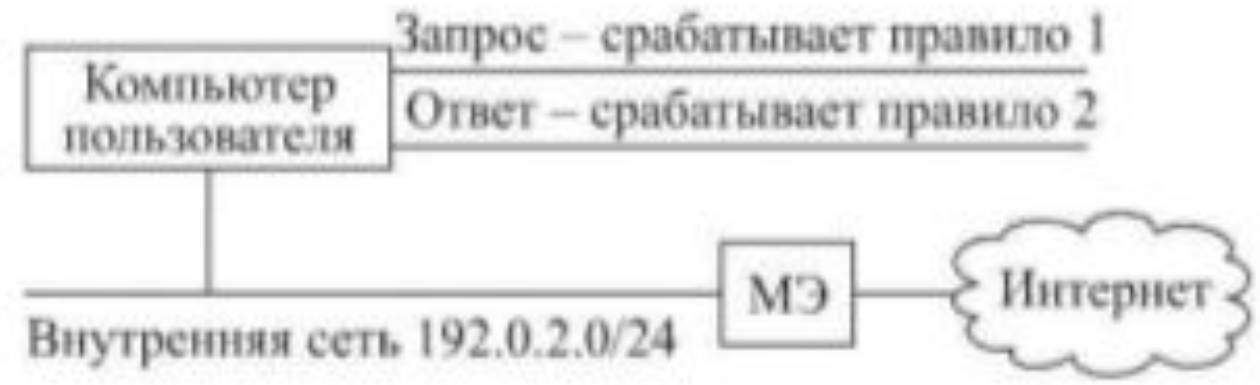

Рис. 8. Статичность пакетного фильтра

1. Защита периметра корпоративной сети

1.4. Межсетевые экраны

Правила, приведённые в табл. 1, обеспечивают возможность отправки почты из сети 192.0.2.0/24 на любой внешний SMTP-сервер.

Таблица 1 Правила фильтрации

Номер правила	Действие	Узел-источник	Порт	Узел-получатель	Порт TCP	Флаги TCP Опции IP	Комментарий
1	Разрешить	192.0.2.0/24	1024-65535	*	25	TCP	Запрос
2	Разрешить	*	25	192.0.2.0/24	1024-65535	TCP АСК-1	Ответ

1. Защита периметра корпоративной сети

1.4. Межсетевые экраны

Несмотря на возможность инициирования соединения только из сети 192.0.2.0/24, прохождение ответов с 25-го порта TCP (с любого внешнего узла) разрешено, даже если не было запроса. Таким образом, нарушитель может посылать большое количество ответов, создавая тем самым ситуацию бесполезного расходования вычислительных ресурсов (рис. 9).

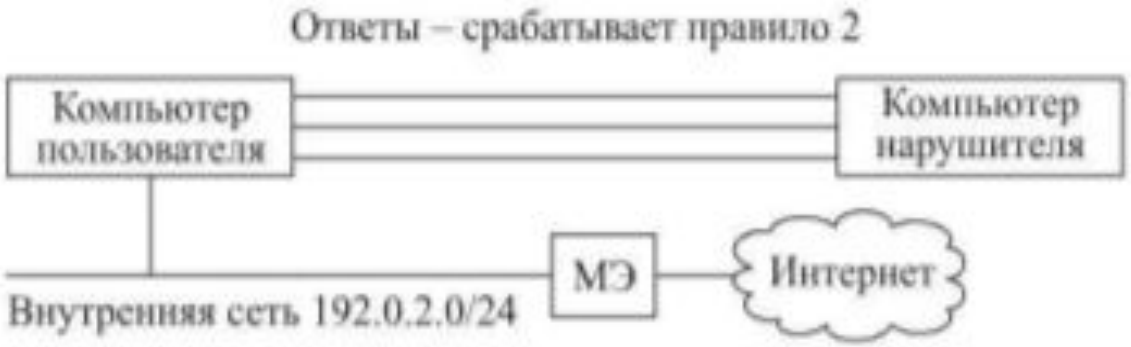

Рис. 9. Бесполезное расходование вычислительных ресурсов

1. Защита периметра корпоративной сети

1.4. Межсетевые экраны

Поскольку пакетный фильтр блокирует подключения к узлу, основываясь на наличии флага SYN в заголовке, пакеты с флагом АСК будут пропущены. Развитие этой идеи в своё время привело к появлению троянцев, клиентская часть которых подключалась к серверной, используя только АСК-пакеты, без флагов SYN.

Пакетная фильтрация свойственна многим операционным системам, а также сетевому оборудованию. В частности, встроенные в ядро возможности пакетных фильтров всегда были сильной стороной UNIX-систем.

Для BSD-систем наиболее популярным в настоящее время является пакетный фильтр pf, а в ОС Linux используется iptables.

Ещё один классический пример – МЭ Checkpoint, архитектура которого базируется на технологии Stateful Inspection. Ядро архитектуры – модуль Fire Wall INSPECT engine, выполняющий перехват и анализ сетевых пакетов, располагаясь между драйвером сетевого адаптера и стеком TCP/IP. Модуль INSPECT работает в режиме ядра ОС (в виде драйвера). Несмотря на то, что Checkpoint выполняет анализ трафика прикладного уровня, дополнительную аутентификацию и содержит «встроенных» посредников, по «своей природе» это пакетный фильтр с технологией Stateful Inspection.

1. Защита периметра корпоративной сети

1.4. Межсетевые экраны

Технология «Stateful Inspection». Очевидно, что для решения проблемы статичности, т.е. принятия окончательного решения о пропуске или запрете очередного анализируемого пакета, недостаточно лишь просматривать отдельные пакеты, должна быть использована информация о предыдущих соединениях.

В зависимости от типа проверяемого пакета, для принятия решения важными могут быть как текущее состояние соединения, которому он принадлежит (полученное из его истории), так и состояние приложения, его использующего.

Технология «Stateful Inspection» обеспечивает сбор информации из пакетов, сохранение и накопление её в специальных контекстных таблицах, которые динамически обновляются.

Таким образом, обработка нового соединения происходит с записью параметров этого соединения в таблицы соединений.

Обработка последующих пакетов соединения осуществляется на основе анализа этих таблиц.

1. Защита периметра корпоративной сети

1.4. Межсетевые экраны

Для разных типов соединений в таблицах запоминается разная информация (табл. 2).

Таблица 2 Запоминаемая информация

Протокол	Тайм-аут	Адреса	Порты	Флаги	SEQ number и ACK number	Идентификаторы
TCP	+	+	+	+	+	-
UDP	+	+	+	+	-	-
ICMP	+	+	-	-	-	+
Другой	+	+	-	-	-	-

1. Защита периметра корпоративной сети

1.4. Межсетевые экраны

Технология «Stateful Inspection» может быть распространена и на прикладной уровень. Если прикладная служба использует несколько взаимосвязанных соединений, то технология «Stateful Inspection» обеспечивает динамическое открытие/закрытие необходимых портов.

Посредники уровня соединения. Решить проблему статичности можно также с помощью посредника (proxy) – узла, выполняющего запрос на установление соединения по инициативе другого узла.

В отличие от пакетных фильтров, посредник не позволяет узлам, находящимся по разные стороны МЭ, связываться напрямую. Вместо этого устанавливаются два соединения: одно между клиентом и посредником, другое – между посредником и сервером.

Посредник (аналогично пакетному фильтру) руководствуется набором правил для определения того, какой трафик разрешён, а какой запрещён, при этом контроль соединения осуществляется «по определению».

1. Защита периметра корпоративной сети

1.4. Межсетевые экраны

Внутреннее устройство посредника упрощённо проиллюстрировано на рис. 10.

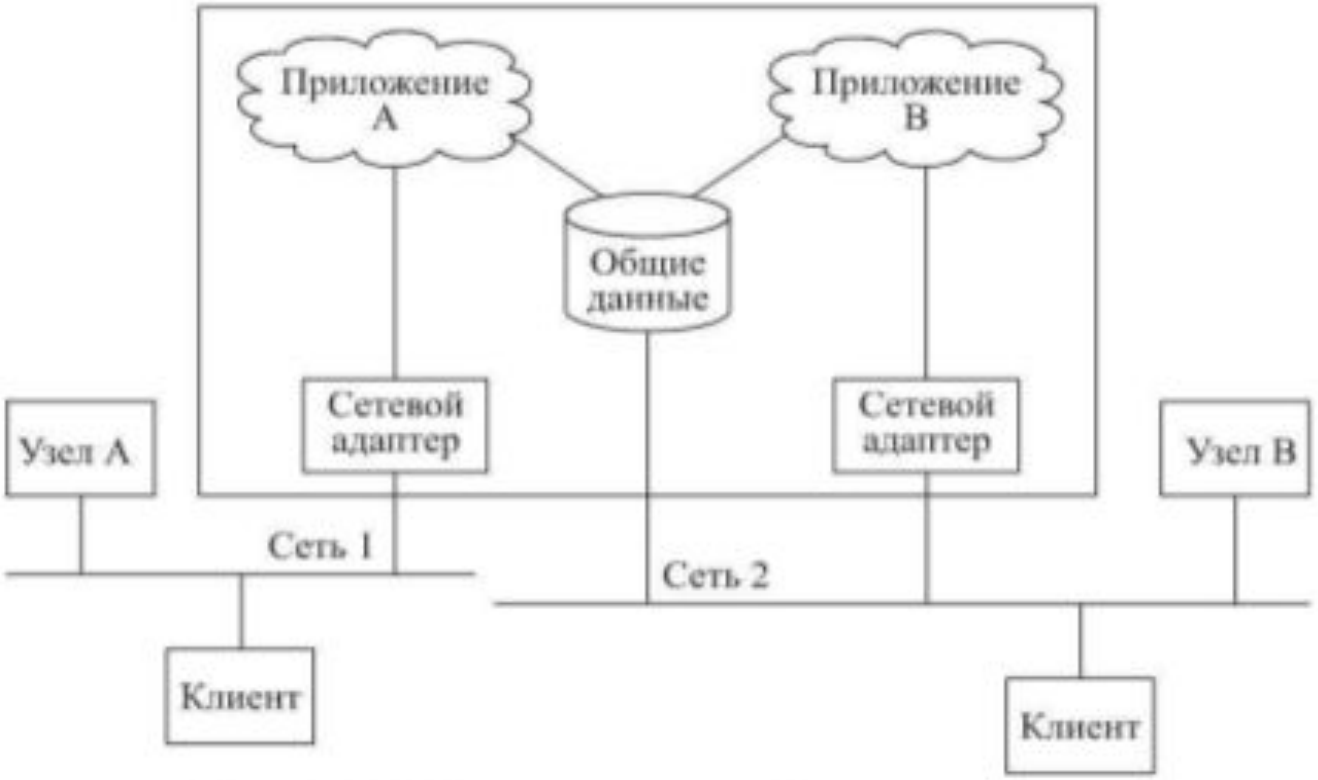

Рис. 10. Внутреннее устройство посредника

1. Защита периметра корпоративной сети

1.4. Межсетевые экраны

Узел A в сети 1 имеет доступ к приложению A на представленном узле, а приложение B – к узлу B. Оба приложения имеют общий буфер, через который узлы A и B могут взаимодействовать.

Когда клиент внутренней сети обращается, например, к веб-серверу, его запрос попадает к посреднику (или перехватывается им).

Последний устанавливает связь с сервером от имени клиента, а полученную информацию передаёт клиенту.

Различают посредники: универсальные – уровня соединения (circuit-level proxy) и специализированные – прикладного уровня (application-level proxy).

Посредник уровня соединения не учитывает особенностей конкретных служб (HTTP, FTP и пр.) и перенаправляет трафик одинаковым образом для любых прикладных сервисов. Для такого посредника прикладной сервис обычно ассоциируется лишь с номером порта (например, протокол SOCKS).

1. Защита периметра корпоративной сети

1.4. Межсетевые экраны

Шлюзы прикладного уровня, называемые также proxy-серверами (рис. 11), контролируют и фильтруют информацию на прикладном уровне модели OSI; различаются по поддерживаемым протоколам прикладного уровня (наиболее часто поддерживаются службы веб (HTTP), FTP, SMTP, POP3/IMAP, NNTP, DNS, RealAudio/RealVideo).

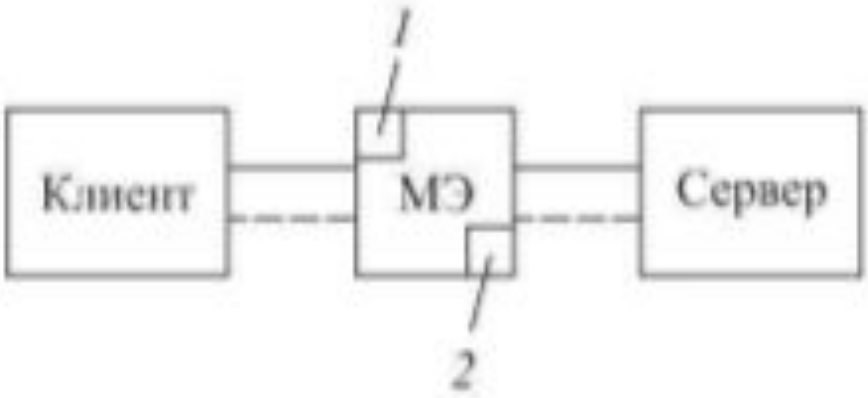

Рис. 11. Шлюзы прикладного уровня: 1,2 – серверная и клиентская часть прикладной службы соответственно

1. Защита периметра корпоративной сети

1.4. Межсетевые экраны

Для внешнего сервера посредник выступает в качестве клиента HTTP, а для внутреннего клиента – в качестве сервера HTTP.

Работа посредников прикладного уровня основана на типе протокола прикладного уровня, в отличие от шлюзов уровня соединения, базирующихся обычно на номерах портов (например, proxy-сервер SQUID).

Посредник, в отличие от пакетного фильтра, «заметен» для клиента, что создаёт некоторые неудобства: необходимость настройки клиентских узлов или приложений. С этой точки зрения посредники подразделяют на классические (classical proxy) и прозрачные (transparent proxy). Классические посредники требуют явной настройки клиентских приложений или установки специального программного обеспечения (например, в настройках браузера можно явно указать адрес и номер порта посредника, рис. 12).

1. Защита периметра корпоративной сети

1.4. Межсетевые экраны

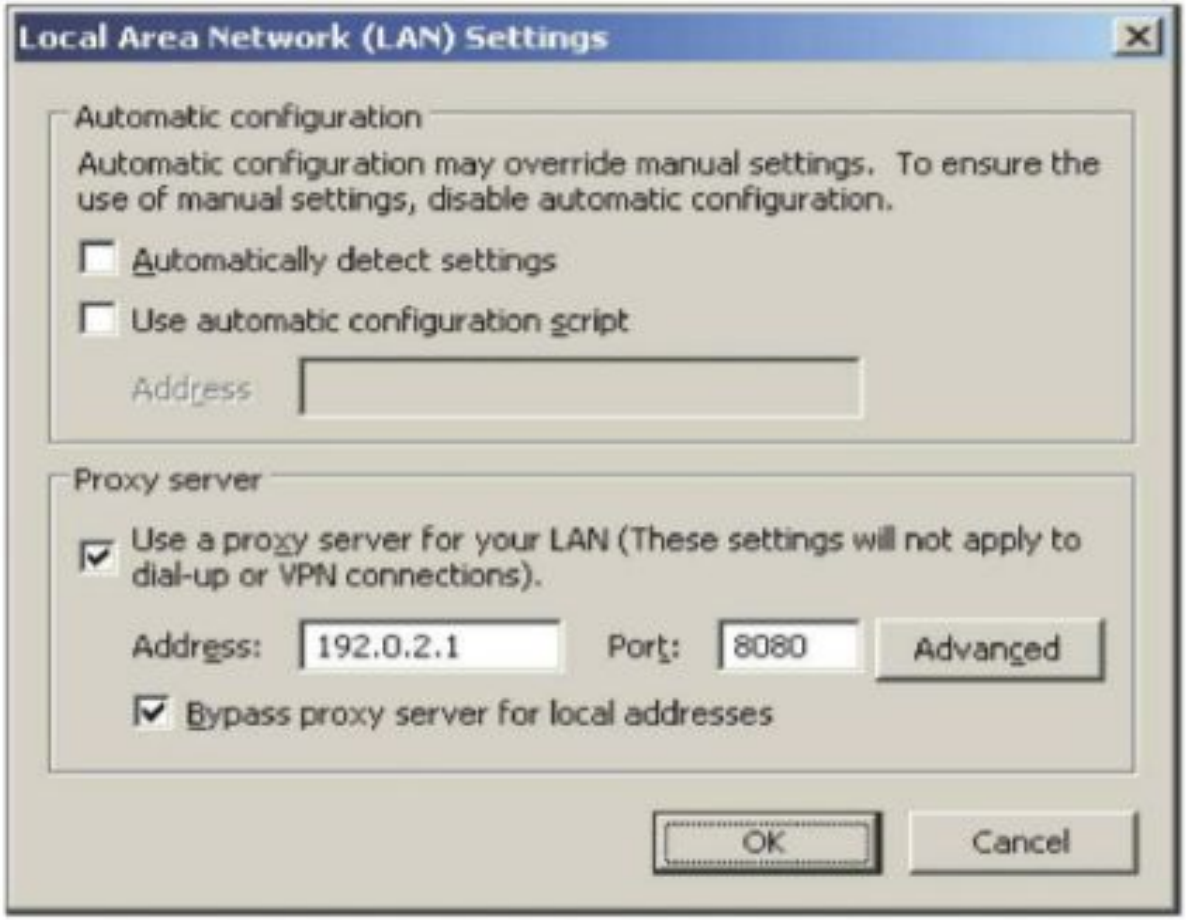

Рис. 12. Windows интерфейс настройки классического посредника

1. Защита периметра корпоративной сети

1.4. Межсетевые экраны

Прозрачный посредник с точки зрения пользователя создаёт иллюзию прямого соединения. Для клиента прозрачный посредник «кажется» пакетным фильтром. Для решения этой задачи стек TCP/IP посредника модифицируется таким образом, что SYN-пакет от клиента обрабатывается именно посредником, и устанавливается соединение с целевым сервером.

В ряде случаев возникает необходимость использования сертифицированных средств защиты, в том числе и МЭ. В России имеется две системы сертификации МЭ: ФС-ТЭК и ФСБ. Первая система сертификации более известна и описана в руководящем документе ФСТЭК России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищённости от несанкционированного доступа к информации», где установлено шесть классов защищённости МЭ, каждый из которых характеризуется определённой минимальной совокупностью требований по защите информации.

Самый низкий класс защищённости – класс 5, самый высокий – класс 1.

1. Защита периметра корпоративной сети

1.5. Администрирование межсетевого экрана

Удалённое администрирование брандмауэра

МЭ – первая линия обороны, видимая для атакующего. Так как МЭ в общем случае тяжело атаковать напрямую из-за их назначения, атакующие часто пытаются получить логин администратора на МЭ. Имена и пароли административных логинов должны быть серьёзно защищены.

Наилучшим методом защиты от такой формы атаки является серьёзная физическая безопасность самого МЭ и его администрирование только с локального терминала. Но в повседневной жизни часто требуется некоторая форма удалённого доступа для выполнения некоторых операций по администрированию МЭ, поэтому для предотвращения перехвата сеансов должно использоваться сквозное шифрование всего трафика удалённого соединения с МЭ.

1. Защита периметра корпоративной сети

1.5. Администрирование межсетевого экрана

МЭ, как и любое другое сетевое устройство, должен кем-то управляться. Политика безопасности должна определять, кто отвечает за управление МЭ.

Должны быть назначены два администратора МЭ (основной и заместитель) ответственным за информационную безопасность, и они должны отвечать за работоспособность МЭ. Основной администратора должен производить изменения в конфигурации МЭ, а его заместитель должен производить любые действия только в отсутствие основного, чтобы не возникало противоречивых установок. Каждый администратор брандмауэра должен сообщить свой домашний телефонный номер, номер пейджера, сотового телефона или другую информацию, необходимую для того, чтобы связаться с ним в любое время.

Обычно рекомендуется иметь двух опытных человек для ежедневного администрирования МЭ. При такой организации администрирования МЭ будет работать практически без сбоев.

Безопасность повседневной деятельности организации требует, чтобы администратор МЭ по-настоящему понимал принципы сетевых технологий и их реализации и имел большой опыт работы с ними. Администратор должен периодически посещать курсы повышения квалификации по теории и практике сетевой безопасности или другими способами поддерживать высокий

2. Демилитаризованная зона

2.1. Защита корпоративной сети с помощью буферной области

Некоторые организации не используют в своих сетях демилитаризованную зону, DMZ. Вместо этого они размещают свои серверы (например, Web-серверы) в той же внутренней сети, где находятся серверы и рабочие станции компании.

Без DMZ, отделяющей общедоступные серверы от внутренней сети, последняя подвергается дополнительному риску. Когда атакующий получит возможность управления Web-сервером, он сможет использовать его для атаки на важные ресурсы, такие как финансовые приложения и файловые серверы.

Именно «когда», а не «если». Потому что независимо от того, как защищён Web-сервер, рано или поздно он подвергнется атаке. Следовательно, необходимо проектировать сеть и рабочие процессы с учётом минимизации ущерба от вторжений и гарантии их быстрого восстановления.

Одной из таких стратегий является стратегия выделения рабочих зон и использование демилитаризованной зоны (DMZ).

2. Демилитаризованная зона

2.1. Защита корпоративной сети с помощью буферной области

При формировании DMZ создаётся две физически разделённые сети: одна – для общедоступных серверов, другая – для внутренних серверов и рабочих станций. В зависимости от типа DMZ и числа используемых брандмауэров, применяется та или иная политика маршрутизации для каждой из сетей и жёстко контролируется доступ между:

- Internet и DMZ;
- Internet и внутренней сетью;
- DMZ и внутренней сетью.

Главное преимущество использования DMZ вместо простого брандмауэра состоит в том, что при атаке на общедоступный сервер риск компрометации внутренних серверов снижается, поскольку общедоступные и внутренние серверы отделены друг от друга. Если скомпрометированный сервер находится в DMZ, злоумышленник не сможет напрямую атаковать другие, более важные серверы, расположенные во внутренней сети. Брандмауэр блокирует любые попытки компьютеров из DMZ подсоединиться к компьютерам внутренней сети, за исключением специально разрешённых соединений. Например, можно настроить брандмауэр так, чтобы разрешить Web-серверу, находящемуся в DMZ, подсоединяться к внутренней системе с *Microsoft SQL* через специальный *TCP*-порт.

2. Демилитаризованная зона

2.1. Защита корпоративной сети с помощью буферной области

Если злоумышленник захватит Web-сервер, он сможет организовать атаку на систему *SQL Server* через этот порт. Однако злоумышленник не сможет атаковать другие службы и порты системы с *SQL Server*, равно как и другие компьютеры во внутренней сети.

Применение DMZ даёт ещё некоторые преимущества.

- Обеспечивается возможность обнаружения вторжений, фильтрации содержимого и мониторинга на уровне приложений. Таким образом брандмауэр обеспечивает защиту внутренней сети от атак не только из Internet, но и с подвергшихся нападению компьютеров из DMZ. Если скомпрометированный компьютер находится в DMZ, а не во внутренней сети, атакующий попытается пройти брандмауэр вновь для получения доступа к внутренней сети.
- DMZ обеспечивает дополнительный уровень защиты от атак, при которых злоумышленники пытаются получить доступ через любые порты, которые непредусмотрительно были оставлены открытыми на общедоступных серверах.
- DMZ позволит контролировать исходящий трафик так, что можно будет остановить распространение различных червей, которые используют Web-сервер для взлома других компьютеров, и атакующие не смогут задействовать Trivial FTP (TFTP) на Web-сервере.

2. Демилитаризованная зона

2.1. Защита корпоративной сети с помощью буферной области

- DMZ защищает серверы от атак типа подмены адресов (spoofing) с использованием протокола Address Resolution Protocol (ARP).

Хотя преимущества использования DMZ велики, возможно, за них придётся заплатить снижением производительности в силу размещения брандмауэра между общедоступными серверами и *Internet*. Возможно, разница и не будет сразу заметна. Это зависит от многих факторов, таких как пропускная способность канала, загрузка канала, используемое программное обеспечение и т.д. Однако некоторым крупным сайтам не удастся избежать ощутимого снижения производительности, и им придётся балансировать между защитой Web-сервера и пассивной системой обнаружения вторжений *Intrusion Detection Systems* (*IDS*). Теперь, когда мы обсудили преимущества и недостатки использования DMZ, давайте рассмотрим факторы, влияющие на выбор того или иного варианта реализации DMZ. Кроме того, следует знать о некоторых опасностях и технических особенностях при разработке DMZ.

Рассмотрим, как создать DMZ на основе *Microsoft Internet Security and Acceleration* (*ISA*) *Server 2000*. В дальнейшем читатели смогут распространить эти принципы и на другие брандмауэры.

2. Демилитаризованная зона

2.2. Типы DMZ

Демилитаризованные зоны могут быть двух типов: так называемые трёхдомные и промежуточные.

DMZ трёхтомного типа (с тремя сетевыми интерфейсами) показана на рис. 13. Она состоит из компьютера с установленным на нем *ISA Server* (т. е. брандмауэром), который имеет три сетевых интерфейса. Интерфейсы соединяют брандмауэр с *Internet*, с сетью DMZ и с внутренней сетью. Если у компании есть средства на дополнительный сервер и лицензию *ISA Server*, можно создать *DMZ* промежуточного типа. Такой тип DMZ предполагает наличие одной системы с установленным на ней *ISA Server* (наружный брандмауэр), соединённой с *Internet* и сетью DMZ, и другой системы с *ISA Server*, соединяющей DMZ и внутреннюю сеть.

DMZ промежуточного типа включает в себя два брандмауэра, которые придётся преодолеть злоумышленнику, поэтому данный тип DMZ обеспечивает более высокий уровень защиты внутренней сети по сравнению с DMZ трёхдомного типа. Другие различия между двумя типами DMZ состоят в уровне защиты общедоступных серверов и стоимости. Некоторые технические проблемы с IP-адресацией и сертификатами также могут повлиять на выбор типа DMZ.

2. Демилитаризованная зона

2.2. Типы DMZ

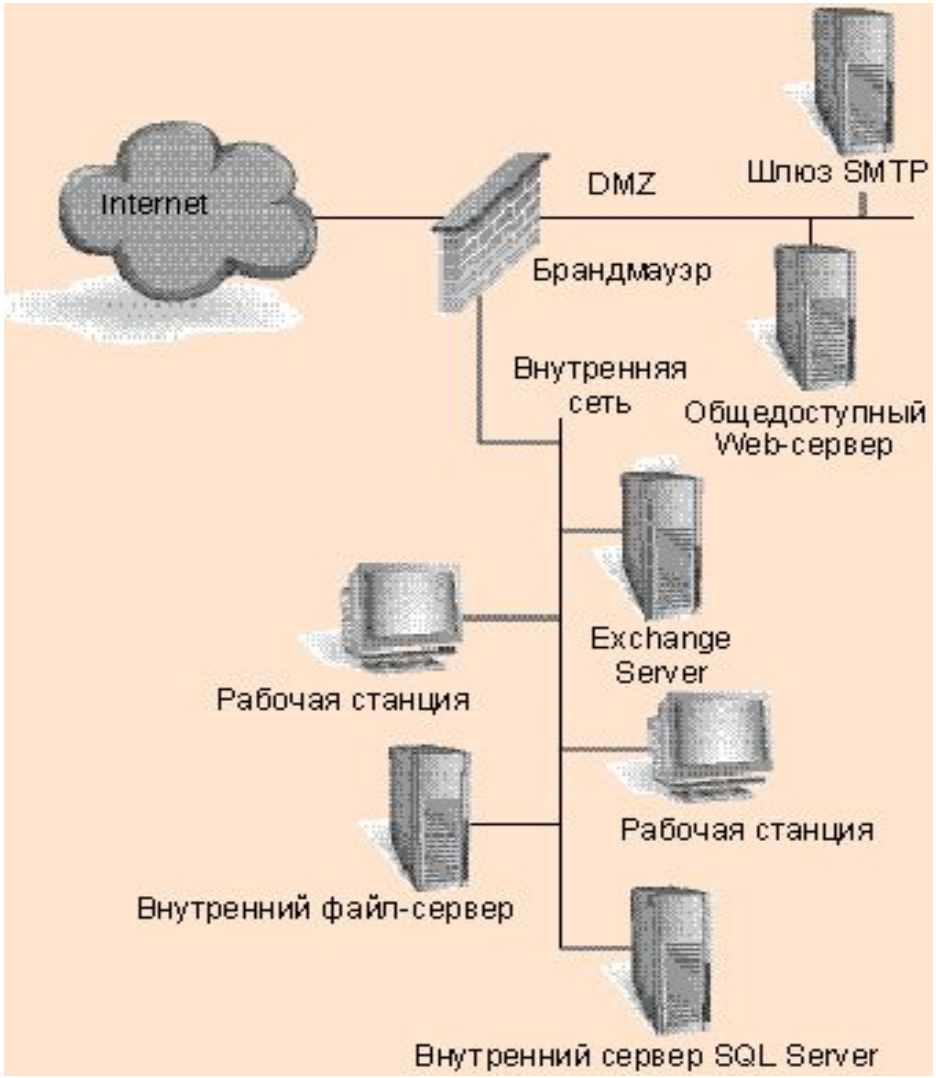

Рис 13. DMZ с тремя интерфейсами

2. Демилитаризованная зона

2.3. DMZ на базе ISA Server с тремя интерфейсами

DMZ, созданная на основе *ISA Server* с тремя сетевыми интерфейсами, является наименее затратной для реализации, поскольку в этом случае понадобится только один сервер, одна лицензия на *Windows* 2000 и выше, одна лицензия на *ISA Server*, три сетевых интерфейса, концентратор или коммутатор для сегмента DMZ и по возможности IP-адреса от поставщика услуг *Internet* для серверов в DMZ. Однако *ISA Server* имеет некоторые важные ограничения, связанные с использованием DMZ с тремя сетевыми интерфейсами.

ISA Server позволяет задать лишь одну сеть в качестве внутренней, полностью защищённой сети. Кроме того, такой тип DMZ обеспечивает проверку на прикладном уровне только для компьютеров внутренней сети. Другими словами, функции *ISA Server* по контролю и проверке на прикладном уровне, т. е. протоколов *HTTP*, *FTP*, *SMTP*, *POP3* и удалённого вызова процедур *RPC Microsoft Exchange Server*, недоступны при использовании такого типа DMZ. *ISA Server* обеспечивает только классическую фильтрацию IP-пакетов для компьютеров в DMZ.

Внутренняя сеть задаётся вводом соответствующего диапазона IP-адресов в таблицу локальных адресов *Local Address Table* (*LAT*) на *ISA Server*. Поскольку *ISA Server* позволяет вести только одну *LAT*, можно будет обеспечить полноценную защиту лишь одной сети (внутренней).

2. Демилитаризованная зона

2.3. DMZ на базе ISA Server с тремя интерфейсами

Другое ограничение *ISA Server* в случае использования трёхдомной DMZ заключается в том, что *ISA Server* для компьютеров в DMZ поддерживает только фильтрацию IP-пакетов. Соответственно, не удастся использовать ни возможности *ISA Server* по трансляции сетевых адресов (*Network Address Translation*, *NAT*), ни функции управления публикацией на серверах, фильтрации приложений и проверки клиентского доступа. Это ограничение также означает, что необходимо будет присвоить серверам в DMZ реальные, полученные от поставщика услуг IP-адреса вместо использования собственных адресов и технологии *NAT*. Таким образом, если преобразовать простую сеть в сеть с DMZ с тремя интерфейсами, потребуется приобрести дополнительные IP-адреса у поставщика услуг *Internet*.

Выделенные IP-адреса, которые будут присваиваться компьютерам в DMZ, должны находиться в диапазоне адресов подсети брандмауэра. Можно использовать для сегмента DMZ адреса, не принадлежащие подсети брандмауэра, но в этом случае необходимо будет поставить в известность поставщика услуг *Internet*, чтобы он маршрутизировал пакеты для DMZ на брандмауэр. В качестве примера допустим, что *ISP* предоставил нам две подсети: подсеть w.x.y.z/24, адреса которой предназначены для общедоступных серверов и которая является частью подсети поставщика услуг (*ISP*), и подсеть a.b.c.d/29. Можно включить внешний интерфейс брандмауэра в подсеть w.x.y.z/24. Затем придется договориться с ISP, чтобы все пакеты, имеющие

2. Демилитаризованная зона

2.3. DMZ на базе ISA Server с тремя интерфейсами

Для создания DMZ с тремя интерфейсами, использующей ISA Server в качестве брандмауэра, для начала понадобится установить на сервер три сетевых интерфейса. Затем необходимо будет установить *Windows* 2000 и более позднюю версию и последний пакет обновлений. Затем потребуется установить ISA *Server* и последний пакет обновлений для него. Далее следует запустить *Windows Update* для установки всех вышедших впоследствии обновлений для *Windows*.

Когда установка будет закончена, появится возможность настроить на *ISA Server* локальную таблицу адресов (*LAT*), содержащую адреса компьютеров внутренней сети. Не стоит включать в эту таблицу какие-либо адреса из DMZ или из *Internet*. Затем нужно активировать фильтрацию пакетов и IP-маршрутизацию. Для управления доступом пользователей внутренней сети в DMZ и *Internet* следует создать соответствующие правила посещения сайтов.

Чтобы разрешить пользователям из *Internet* доступ к серверам, находящимся в DMZ, придётся создать пакетный фильтр, который откроет соответствующие порты на каждом из серверов в DMZ. Например, если имеется Web-сервер и шлюз SMTP в DMZ, нужно будет создать фильтр, который откроет TCP-порт 80 на Web-сервере (или TCP-порт 443, если используется *HTTP Secure*, *HTTPS*). Затем потребуется создать два фильтра, которые разрешат устанавливать входящие соединения к TCP-порту 25 и исходящие соединения от TCP-порта 25 на *SMTP*-

2. Демилитаризованная зона

2.3. DMZ на базе ISA Server с тремя интерфейсами

Далее нужно будет разрешить пакетам протокола SMTP проходить между внутренним сервером *Exchange* (или другим сервером электронной почты) и шлюзом электронной почты, находящимся в DMZ. Чтобы это сделать, следует создать правило публикации, которое позволит шлюзу открывать SMTP-соединения на внутреннем сервере *Exchange* для входящих почтовых сообщений.

Необходимо также создать правило использования протокола, которое позволит серверу *Exchange* открывать SMTP-соединения на шлюзе для отправки исходящей почты. Если Web-серверу нужен доступ к ресурсам сервера внутренней сети, например, к SQL Server, следует создать правило публикации, позволяющее Web-серверу из DMZ получить доступ к системе *SQL Server*.

Создавая правила публикации, мы ограничиваем риск, связанный с уязвимостью внутренних серверов в случае, если атакующий овладеет правами на управление Web-сервером, находящимся в DMZ.

Даже после использования и создания правил публикации серверов и правил использования протоколов у нас все ещё остаются уязвимые места в защите внутренних серверов.

2. Демилитаризованная зона

2.3. DMZ на базе ISA Server с тремя интерфейсами

К счастью, можно использовать дополнительный уровень защиты. Например, чтобы избежать рисков, связанных с внутренним сервером *Exchange*, можно задействовать прекрасный прикладной фильтр для *SMTP* из *ISA Server*, который позволит заблокировать соединения от почтового шлюза к серверу *Exchange*. Можно настроить *SMTP*-фильтр так, чтобы он блокировал доступ к заданным доменам, выполнение определённых *SMTP*-команд и подключений.

Существует возможность сканирования почтовых сообщений на предмет наличия в них определённых ключевых слов. SMTP-фильтр может ограничить размер и длину разрешённых *SMTP*-команд. Эта возможность предотвращает специфический тип *SMTP*-атак, связанных с переполнением буфера.

Избежать рисков, связанных с использованием *SQL Server*, труднее, чем сделать это в *Exchange*, поскольку *ISA Server* не содержит прикладных фильтров для *SQL Server*. Тем не менее можно максимально затруднить взлом *SQL Server*. Например, необходимо использовать хорошие сложные пароли и устранить возможности несанкционированного управления системой с установленным *SQL Server* даже в том случае, если доступ к *SQL Server* разрешён только доверенному Web-серверу.

2. Демилитаризованная зона

2.3. DMZ на базе ISA Server с тремя интерфейсами

Необходимо убедиться, что Web-приложения сохраняют секретность учётной записи и пароля во время соединения с *SQL* Server, другими словами, не позволяйте указывать имя и пароль для доступа к *SQL Server* в коде приложения.

Важно убедиться, что права учётной записи, используемой для доступа к *SQL Server*, ограничены до необходимого минимума. Web-приложения для соединения с *SQL Server* не должны использовать учётную запись системного администратора (*SA*). Вместо этого следует создать для Web-приложений учётную запись с ограниченными правами.

Наконец, предстоит решить, использовать ли протокол защищённого *HTTP* (*HTTPS*) для защиты областей на Web-сайте. Организовать применение *HTTPS* в DMZ с тремя интерфейсами не составляет труда, поскольку *ISA Server* просто маршрутизирует пакеты между *Internet* и DMZ.

Применение *HTTPS* в таком типе DMZ потребует серверного сертификата, который необходимо получить в общедоступном центре сертификатов *Certificate Authority* (*CA*) и установить на Web-сервер в DMZ.

2. Демилитаризованная зона

2.4. Демилитаризованная зона промежуточного типа

При наличии двух брандмауэров мы получаем возможность использовать собственные IP-адреса и функцию трансляции сетевых адресов (*NAT*) для того, чтобы скрыть как сеть DMZ, так и внутреннюю сеть. Как показано на рис. 2, внешний брандмауэр публикует Web-сервер DMZ и шлюз *SMTP* в *Internet*. Внутренний брандмауэр публикует сервер *Exchange* для шлюза *SMTP*.

Для создания промежуточной DMZ, использующей два брандмауэра на базе *ISA Server*, понадобится два сервера, две копии *Windows* 2000 или 2003, две копии *ISA Server*, четыре сетевых интерфейса (по два на каждый сервер) и коммутатор для DMZ. Вначале устанавливается внешний брандмауэр путем установки на одном из серверов Windows 2000 или 2003 и *ISA* Server. В *Control Panel* выбираем ярлык *Network Connection* и настраиваем сетевой интерфейс в Internet на внешнем брандмауэре, задавая на нем все IP-адреса, полученные от поставщика услуг *Internet*. Необходимо выбрать собственную IP-подсеть, например 10.10.*.*, для всех общедоступных серверов в DMZ. Присвоим адрес 10.10.0.1 сетевому интерфейсу DMZ на внешнем брандмауэре, 10.10.0.2 – Web-серверу и 10.10.0.3 – шлюзу SMTP. Внесём эту подсеть (10.10.*.*) в локальную таблицу адресов (LAT) внешнего брандмауэра. Настроим компьютеры в DMZ на использование внешнего брандмауэра в качестве шлюза по умолчанию.

2. Демилитаризованная зона

2.4. Демилитаризованная зона промежуточного типа

Теперь установим внутренний брандмауэр, установив на второй сервер Windows *Server* и *ISA Server*. Присвоим адрес 10.10.0.4 сетевому интерфейсу DMZ на внутреннем брандмауэре, настроим этот интерфейс на использование внешнего брандмауэра в качестве шлюза по умолчанию. Выберем собственную подсеть для внутренней сети, допустим 10.20.*.*. Присвоим адрес 10.20.0.1 интерфейсу внутренней сети на внутреннем брандмауэре. Настроим внутренние компьютеры так, чтобы они использовали в качестве шлюза по умолчанию внутренний брандмауэр. В локальную таблицу адресов (LAT) внесём IP-адреса внутренней сети (10.20.*.*), отделённой от сети 10.10.*.* демилитаризованной зоной.

После присвоения частных IP-адресов клиентским системам можно будет создать правила публикации серверов и правила использования протоколов. Чтобы разрешить клиентам из *Internet* доступ на Web-сервер, следует добавить на внешнем брандмауэре правило, которое опубликует Web-сервер в *Internet*. Чтобы разрешить *SMTP*-серверам из *Internet* передавать сообщения на шлюз, нужно настроить правило публикации серверов, которое будет перенаправлять входящие *SMTP*-соединения, изначально направленные на внешний брандмауэр, на *SMTP*-шлюз в DMZ. Затем на внутреннем брандмауэре необходимо добавить правило публикации сервера, которое опубликует SMTP-службу сервера *Exchange*, и одновременно направит клиентские соединения на шлюз SMTP

2. Демилитаризованная зона

2.4. Демилитаризованная зона промежуточного типа

После этого требуется настроить шлюз SMTP на передачу входящих e-*mail*-сообщений на внутренний брандмауэр, который, в свою очередь, сам перенаправит их на Exch*a*nge-сервер.

Для того чтобы разрешить почтовым сообщениям из внутренней сети достигать адресатов, находящихся в *Internet*, следует настроить правило использования протоколов и пакетный фильтр так, чтобы они разрешали устанавливать исходящие SMTP-соединения через *SMTP*-шлюз. Важно ограничить такие соединения только теми, которые исходят от *Exchange*-сервера. Настроим *Exchange* на передачу исходящих почтовых сообщений на *SMTP*-шлюз. Наконец, если Web-серверу, находящемуся в DMZ, необходим доступ к внутреннему *SQL Server*, следует создать правило публикации сервера на внутреннем брандмауэре, разрешающее Web-серверу доступ к системе с *SQL Server* во внутренней сети через порт 1433.

Использование *HTTPS* для защиты важных областей Web-сайта в DMZ промежуточного типа отличается от применения *HTTPS* в DMZ с тремя сетевыми интерфейсами. Вместо установки на Web-сервере серверного сертификата, полученного от общедоступного центра сертификации (CA), необходимо установить сертификат на ISA Server. Соответственно, когда клиент из *Internet* получает доступ к защищённой области Web-сайта, *Internet Explorer* клиента устанавливает защищённое SSL-соединение (*Secure Sockets Layer*) между клиентским компьютером и *ISA Server*. ISA *Server*, в свою очередь, перенаправляет

2. Демилитаризованная зона

2.4. Демилитаризованная зона промежуточного типа

Можно либо настроить *ISA Server* на перенаправление запросов в текстовом формате обычного *HTTP*, либо установить новое *HTTPS*-соединение с Web-сервером. Если Web-сервер является единственным сервером в DMZ, рекомендую использовать *HTTP* для экономии ресурсов компьютера. Вероятность, что кто-нибудь перехватит соединения, невелика, поскольку Web-сервер находится в защищённой сети DMZ.

Если же Web-сервер – не единственный сервер в DMZ, возможно, придётся устанавливать новые *HTTPS*-соединения. Важно помнить, что процесс шифрования снижает производительность как *ISA Server*, так и Web-серверов. Другой возможностью, позволяющей изолировать трафик между *ISA Server* и Web-сервером, является использование виртуальных сетей *Virtual LAN* (*VLAN*) на коммутаторе сети DMZ.

DMZ с тремя интерфейсами обеспечивает безопасность как внутренней сети, так и общедоступных серверов в DMZ. Кроме того, DMZ такого типа – менее дорогостоящая и более простая в использовании, чем DMZ промежуточного типа. Однако использование промежуточной DMZ даёт возможность полностью задействовать все функции *ISA Server* для защиты как внутренней сети, так и общедоступных серверов в DMZ. В DMZ такого типа внешний брандмауэр проверяет входящий и исходящий трафик к Web-серверу и шлюзу SMTP на

2. Демилитаризованная зона

2.4. Демилитаризованная зона промежуточного типа

Кроме того, DMZ промежуточного типа необходим всего один *Internet*-адрес, полученный от провайдера, который скроет IP-адреса не только внутренней сети, но и серверов, находящихся в DMZ. Вне зависимости от того, какой выбрать тип DMZ, это будет важный шаг в обеспечении безопасности корпоративной сети. Размещение общедоступных серверов в DMZ обеспечит предприятию новый уровень защиты от атак.

2. Демилитаризованная зона

2.5. Установка и использование ISA Server в качестве защитного экрана

Microsoft Internet Security and Acceleration (*ISA*) Server выполняет функции защитного экрана масштаба предприятия и Web-кэша. *ISA Server* может быть установлен в трех режимах: либо в качестве кэширующего сервера (*proxy*-сервера), либо в качестве брандмауэра, либо в интегральном режиме (этот режим обеспечивает как функции кэширования, так и функции защитного экрана). Поскольку мы используем *ISA Server* в качестве брандмауэра, необходимо будет выбрать либо режим *Firewall*, либо *Integrated*. С помощью *ISA Server* можно отслеживать процессы доступа клиентов внутренней сети к ресурсам *Internet*.

Чтобы создать демилитаризованную зону (DMZ), потребуется настроить компьютеры внутренней сети для доступа к *ISA Server* в качестве клиентов *SecureNAT*. Клиенты не должны быть настроены как клиенты брандмауэра или клиенты Web-*proxy*. *SecureNAT* означает, что вы настроили внутреннюю сеть на использование частных IP-подсетей и *ISA Server* применяет технологию *Network Address Translation* (*NAT*) для обслуживания *Internet*-запросов от внутренних клиентов. Использование SecureNAT требует, чтобы компьютеры внутренней сети задействовали *ISA Server* в качестве шлюза по умолчанию. Устанавливать на компьютеры какое-либо специализированное программное обеспечение для работы с *ISA Server* не требуется. Для использования *SecureNAT* необходимо убедиться, что все компьютеры, которым нужен доступ в *Internet*, настроены на IP-адрес сервера *DNS*, выданный *Internet*-провайдером, или внутренний *DNS*-сервер должен перенаправлять неразрешённые запросы на *DNS*-сервер

2. Демилитаризованная зона

2.5. Установка и использование ISA Server в качестве защитного экрана

Чтобы разрешить доступ клиентам из *Internet* к ресурсам, находящимся во внутренней сети, надо будет опубликовать соответствующие внутренние серверы через *ISA Server*. Внешним клиентам *ISA Server* будет представлять эти серверы как доступные. Однако, когда *ISA Server* принимает клиентский запрос, он перенаправляет его внутреннему серверу только после того, как проверит соответствующие политики и проанализирует подозрительные заголовки в запросе.

Для настройки политик использования входящего и исходящего трафика на *ISA Server* применяются правила доступа к сайтам и типу содержимого, правила использования протоколов, фильтры IP-пакетов, правила Web-публикаций и правила публикации серверов. Правила доступа к сайтам и типу содержимого управляют доступом и временем доступа внутренних пользователей к определённым внешним сайтам или их содержимому по типу этого содержимого. Правила протоколов управляют тем, какими протоколами могут пользоваться внутренние клиенты для доступа к компьютерам в *Internet*. Фильтры пакетов IP позволяют управлять тем, какие типы пакетов *ISA Server* будет принимать из *Internet*, а какие – от внутренних компьютеров. Например, можно использовать IP-фильтр, чтобы разрешить прохождение пакетов *Ping* или *PPTP*. Правила Web-публикаций позволят сделать внутренние Web-серверы доступными внешним клиентам из *Internet*.

2. Демилитаризованная зона

2.5. Установка и использование ISA Server в качестве защитного экрана

С помощью этих правил можно управлять входящими Web-запросами в зависимости от соответствующих учётных записей, адресов клиентов, целевых адресов и пути. При помощи правил публикации серверов можно будет сделать доступными для внешнего мира другие серверы (например, *SMTP*-серверы). Правила публикации серверов позволят управлять входящими запросами к этим серверам в зависимости от IP-адреса клиента.

Когда внутренний клиент пытается подсоединиться к компьютеру в *Internet*, *ISA Server* проверяет запрос на соответствие правилам использования протоколов. Если этот запрос является *HTTP* или *HTTP Secure* (*HTTPS*), *ISA Server* дополнительно проверяет его на соответствие правилам доступа к сайтам и по типу содержимого сайтов. Когда *ISA Server* принимает входящий запрос с клиента *Internet*, *ISA Server* проверяет его на соответствие фильтру IP-пакетов.

Если запрос является запросом *HTTP* или *HTTPS*, *ISA Server* дополнительно проверяет его на соответствие правилам Web-публикации; в других случаях *ISA Server* проверяет запрос на соответствие правилам публикации серверов.

3. Анализ содержимого почтового и веб-трафика

Для фильтрации трафика служб прикладного уровня возможностей межсетевых экранов может оказаться недостаточно, особенно для контроля электронной почты и HTTP-трафика. Сложность задачи заключается в том, что для осуществления такого контроля недостаточно анализа заголовков указанных протоколов прикладного уровня, здесь требуется просмотр данных, передаваемых в нескольких пакетах различного формата, и т. д.

Задача анализа содержимого сводится к просмотру передаваемой информации следующего характера:

- содержимое электронной почты (в том числе прикреплённые файлы);
- содержимое HTTP-трафика;
- передаваемые файлы (например, по протоколу FTP).

Для решения этой задачи применяют два подхода (данные подходы могут быть реализованы на базе МЭ Checkpoint Fire Wall-1):

1) анализ содержимого средствами МЭ (многие МЭ имеют возможности фильтрации на основе адреса отправителя, получателя и т. д.);
2) антивирусное программное обеспечение.

Такие решения имеют недостатки, которые заключаются в поддержке небольшого числа критериев фильтрации и форматов передаваемых файлов. Кроме того, немаловажное значение имеет вопрос производительности, поскольку для детального анализа содержимого требуется значительное количество ресурсов.

3. Анализ содержимого почтового и веб-трафика

Электронная почта. Электронная почта, наряду с очевидными преимуществами (удобство для бизнеса, оперативность, продуктивность), имеет ряд недостатков, среди которых возможности:

- создания ситуации отказа в обслуживании (пересылка файлов большого размера, спам, подмена адреса отправителя);
- пересылки вирусов в сообщении или прикреплённых файлах;
- пересылки конфиденциальной информации и информации неэтичного характера;
- использования электронной почты в личных целях.

Таким образом, средства анализа содержимого электронной почты должны противодействовать перечисленным угрозам,

Критериями фильтрации для таких средств должны быть:

- адреса отправителя и получателя;
- параметры прикреплённых файлов (тип, размер);
- наличие вирусов;
- содержимое письма и прикреплённых файлов;
- подлинность адреса отправителя.

3. Анализ содержимого почтового и веб-трафика

HTTP-трафик. С HTTP-трафиком связаны следующие угрозы:

- «опасное» содержимое – мобильный код, вирусы;
- пересылка информации через веб-интерфейс;
- использование трафика в личных целях;
- загрузка материалов недопустимого характера (нелицензионное ПО и т. д.).

Следовательно, критериями фильтрации в данном случае являются:

- параметры загружаемых файлов (имя, тип, размер);
- наличие вирусов;
- содержимое загружаемых файлов;
- URL;
- почта с веб-интерфейсом;
- разрешённые часы работы;
- направление загрузки файлов.

Системы анализа содержимого – это фактически посредники прикладного уровня с расширенными возможностями фильтрации трафика прикладного уровня, работающие аналогично МЭ (фактически это разновидность МЭ).

Размещение такой системы в корпоративной сети зависит от следующих факторов:

- схема подключения к сети Интернет;
- расположение МЭ (пакетного фильтра или посредника).

4. Обнаружение и устранение уязвимостей. Возможности сканеров безопасности

4.1. Управление уязвимостями

Подсистема управления уязвимостями представляет собой комплекс организационно-технических мероприятий, направленных на предотвращение использования известных уязвимостей, потенциально существующих в защищаемой системе или сети. В частности, в рамках управления уязвимостями проводятся такие мероприятия, как периодический мониторинг защищённости информационных систем и устранение обнаруженных уязвимостей.

Контроль состояния защищённости относится к категории так называемых превентивных защитных механизмов, главное назначение которых – своевременно «заметить» уязвимость в защищаемой системе и предотвратить возможные атаки.

Создать абсолютно защищённую систему принципиально невозможно. Согласно статистическим данным, число уязвимостей, обнаруживаемых ежегодно, составляет в среднем 5…6 тыс.:

http://web.uvd.riist.gov

4. Обнаружение и устранение уязвимостей. Возможности сканеров безопасности

4.1. Управление уязвимостями

Число обнаруженных уязвимостей

2005.....4 933
2006.....6 608
2007.....6 514
2008.....5 632
2009.....5 732
2012.....4639
2013.....4 150
2014.....5 289

И это только уязвимости реализации, а есть ещё ошибки проектирования и эксплуатации.

В ходе контроля защищённости информационных систем приходится решать следующие основные задачи:

- инвентаризация информационных активов;
- оценка защищённости;
- контроль соблюдения требований политик и стандартов безопасности.

Средства анализа защищённости (так называемые сканеры безопасности – security scanners) помогают обнаруживать уязвимости на узлах корпоративной сети и своевременно устранять их (до того, как ими воспользуются злоумышленники).

Сканеры безопасности классифицируют по различным критериям.

4. Обнаружение и устранение уязвимостей. Возможности сканеров безопасности

4.2. Архитектура систем управления уязвимостями

Распределённая архитектура систем управления уязвимостями предполагает наличие как минимум двух типов компонентов:

- агенты сканирования;
- компоненты управления.

Агенты сканирования в свою очередь могут быть классифицированы по расположению относительно объекта сканирования:

- ***сетевые*** (network-based) – выполняют проверки дистанционно, не требуя наличия агента на сканируемом узле;
- ***локальные*** (host-based) – устанавливают непосредственно на контролируемый узел, работают от имени учётной записи с максимальными привилегиями и все проверки выполняют локально;
- ***пассивные*** (passive) – в качестве источника данных используют сетевой трафик, а выводы о наличии уязвимостей делаются на основе анализа сетевых взаимодействий (например, Passive Vulnerability Scanner от компании Tenable).

4. Обнаружение и устранение уязвимостей. Возможности сканеров безопасности

4.2. Архитектура систем управления уязвимостями

По назначению агенты сканирования подразделяют на:

- ***специализированные*** – применяются для сканирования таких систем, как СУБД, веб-приложения, ERP-системы и т. п.;
- ***общего назначения*** – содержат проверки разных типов.

Например, в состав решения от компании eEye Digital Security (США) входят два агента сканирования: сканер общего назначения (Retina Network Security Scanner) и специализированный сканер для веб-приложений (Retina Web Security Scanner).

В составе решения от компании Safety. Lab (Россия) используется три типа агентов сканирования: сканер общего назначения (Shadow Security Scanner), сканер веб-приложений (Shadow Web Analyzer), сканер СУБД (Shadow Database Scanner).

В некоторых системах нет явного деления агентов сканирования по назначению (например, агент сканирования от компании Positive Technologies (Россия) содержит различные сканирующие модули, в том числе модули анализа безопасности веб-приложений и СУБД).

4. Обнаружение и устранение уязвимостей. Возможности сканеров безопасности

4.3. Особенности сетевых агентов сканирования

Сетевые сканеры имеют следующие особенности:

- выполняют проверки дистанционно, т. е. по сети, что влияет как на скорость сканирования (сравните, например, удалённый подбор пароля и локальный), так и на достоверность результатов;
- используют разные методы для выявления одной и той же уязвимости (системные сканеры руководствуются только косвенными признаками наличия уязвимости (например, проверкой версий файлов);
- применяют различные учётные записи для подключения к службам сканируемого узла (системные сканеры, как правило, представляют собой сервис, работающий от имени учётной записи с максимальными привилегиями).

Проверки, выполняемые по сети, затрагивают не только сетевые сервисы, но и уровни приложений, сетевых служб, ОС, СУБД.

К наиболее известным программным продуктам для выполнения дистанционного анализа защищённости (network-based) относят:

- Nessus Security Scanner;
- Internet Scanner;
- X Spider и др.

4. Обнаружение и устранение уязвимостей. Возможности сканеров безопасности

4.3. Особенности сетевых агентов сканирования

Задача анализа защищённости на сетевом уровне – ответить на вопрос: «что нарушитель может сделать с узлом, получив доступ к нему по сети (удалённо)?» При этом попутно решаются задачи инвентаризации сетевого оборудования, обнаружения неизвестных устройств, идентификации сетевых служб и т.д.

Проверки (Check), выполняемые сканером безопасности, подразделяют на две категории:

- выводы (Inference) – проверки, выполняемые по косвенным признакам (без «участия» уязвимости);
- тесты (Test) – проверки, выполняемые путём проведения атаки в отношении узла (явное использование уязвимости).

При этом часть проверок второй категории может приводить к выведению из строя тестируемой службы (узла).

Наиболее очевидный способ поиска уязвимости – попытаться применить её, т. е. сымитировать атаку, её использующую, – такие проверки называют тестами.

4. Обнаружение и устранение уязвимостей. Возможности сканеров безопасности

4.3. Особенности сетевых агентов сканирования

С другой стороны, наличие уязвимости в системе можно определить и по косвенным признакам, например, по баннеру сканируемой службы или версии какого-либо файла – такие проверки называют инференцией, что означает умозаключение, вывод, сделанный на основе анализа полученных сообщений, поэтому результаты таких проверок (по косвенным признакам) весьма существенно зависят от результатов сбора информации (идентификация открытых портов, служб, приложений и т. д.).

В некоторых сканерах существует возможность выбора способа выявления уязвимости (например, в сканере безопасности Nessus имеется режим «Safe checks», при включении которого все проверки выполняются по косвенным признакам).

В сканере безопасности Internet Scanner для выявления одной и той же уязвимости может быть предусмотрено две проверки: одна с реализацией атаки (например, проверка WinLsassBo), другая – по косвенным признакам (например, проверка WinMs04011).

4. Обнаружение и устранение уязвимостей. Возможности сканеров безопасности

4.3. Особенности сетевых агентов сканирования

Сетевые сканеры безопасности применяют для решения следующих задач:

1) инвентаризация ресурсов сети: узлов, сетевых служб, приложений. Инвентаризационное сканирование предоставляет обобщённую (базовую) информацию о сети. Параллельно решается задача обнаружения несанкционированно подключённых устройств;
2) тестирование сети на устойчивость к взлому — может осуществляться как внутри сети, так и снаружи. В последнем случае это часто называют анализом защищённости периметра. В процессе проведения такого исследования могут быть использованы и другие инструменты (сетевые анализаторы, «троянцы», «руткиты» и пр.), но сканеры уязвимостей, как правило, используются всегда;
3) аудит безопасности сети или отдельных её областей на соответствие заданным требованиям — осуществляется периодически в целях, например, проверки правильности и своевременности установки обновлений.

Для решения второй задачи, как правило, привлекаются сторонние организации, а первую и третью задачи выполняют обычно собственными силами.

4. Обнаружение и устранение уязвимостей. Возможности сканеров безопасности

4.4. Средства анализа защищённости системного уровня

Сканеры системного уровня выполняют поиск уязвимостей более тщательно и достоверно по сравнению с сетевыми сканерами, поскольку установлены на сканируемом узле и работают от имени учётной записи с максимальными привилегиями (root, SYSTEM).

Сканеры уровня узла помимо проверок, аналогичных проводимым сетевыми сканерами (например, поиск работающих на узле устройств, таких как модемы, обнаружение установленных на узле приложений или контроль режима работы сетевого адаптера — селективный или неселективный), выполняют проверки, которые невозможно или сложно осуществить с использованием сетевых сканеров (например, оценка стойкости паролей, контроль целостности, анализ журналов ОС и приложений для поиска следов нарушителя).

Средства сканирования на уровне узла используются для защиты наиболее важных серверов: почтовых, веб, удалённого доступа, управления базами данных. Эти узлы нередко содержат наиболее критичные данные для ведения бизнеса, и сканирование на системном уровне помогает обнаружить уязвимости высокой степени риска и предоставить администратору информацию для устранения найденных проблем.

4. Обнаружение и устранение уязвимостей. Возможности сканеров безопасности

4.4. Средства анализа защищённости системного уровня

Сканирование на системном уровне применяется и при защите межсетевых экранов, которые содержат известные уязвимости и конфигурации, установленные по умолчанию.

Сканеры уровня узла имеют обычно распределённую архитектуру, состоящую из агентов, расставленных на защищаемых узлах, и консоли, контролирующей работу агентов и осуществляющей сбор данных от них.

Перечислим источники данных для сканеров уровня узла:

- файловая система узла – нередко признаком наличия уязвимости считается номер версии того или иного файла. Кроме того, изменения некоторых важных файлов могут служить признаками следов нарушителя;
- журналы регистрации;
- конфигурация, параметры, влияющие на безопасность, – для ОС Windows основной источник таких данных – реестр. К этой же категории относится информация о пользователях, работающих на узле, службах, установленных приложениях.

4. Обнаружение и устранение уязвимостей. Возможности сканеров безопасности

4.4. Средства анализа защищённости системного уровня

Таким образом, проверки, выполняемые на системном уровне, осуществляют поиск уязвимостей следующим образом;

- сравнением версий файлов или их атрибутов с имеющимися значениями в базе данных проверок;
- поиском файлов или ключей реестра, свидетельствующих о наличии в узле того или иного приложения (вируса и т. п.);
- сравнением текущих значений параметров конфигурации с требуемыми значениями (в этом случае пользователь должен задать эти значения, которые обычно являются частью политики безопасности).

5. Введение в технологию обнаружения атак

5.1. Системы обнаружения атак

Обнаружением атак называют процесс идентификации и реагирования на подозрительную деятельность, направленную на вычислительные ресурсы.

Системы обнаружения атак (Intrusion Detection Systems, IDS) предназначены для своевременного выявления факта нарушения и реагирования на него. Технология обнаружения атак может быть использована либо как часть инфраструктуры мониторинга событий, либо как самостоятельный механизм защиты.

Необходимость использования данной технологии может быть проиллюстрирована следующими примерами.

Ситуация 1. Затруднено или невозможно обращение к расположенному в ДМЗ веб-серверу компании.

Причиной такой ситуации может быть успешно проведённая DDoS-атака с одной из так называемых бот-сетей (ботнетов – от англ. botnet), которые распространяют спам, содержащий вредные вложения.

5. Введение в технологию обнаружения атак

5.1. Системы обнаружения атак

Ситуация 2. Резкий рост нагрузки на межсетевой экран.

Причиной ситуации может быть использование популярных в настоящее время P2P-сетей – файлообменных сетей.

Алгоритм (технология) обнаружения атак имеет три ***составляющие***:

1) признаки атак (понимание ожидаемого поведения контролируемого объекта, знание возможных атак и их модификаций);
2) источники информации об атаках (сетевой график, журналы, действия субъектов и т. д.);
3) механизмы реагирования (оповещение, блокировка, вызов внешней программы и др.).

Рассмотрим механизмы реагирования более подробно.

Возможны следующие варианты оповещения:

- звуковой сигнал;
- электронная почта;
- телефон;
- консоль управления;
- система сетевого управления.

5. Введение в технологию обнаружения атак

5.1. Системы обнаружения атак

Блокировка предполагает «активное вмешательство» системы обнаружения атак и может быть выполнена следующими способами:

- аварийное завершение TCP-соединения;
- посылка ICMP Destination Unreachable для блокировки взаимодействия по протоколу UDP;
- блокировка трафика, содержащего признаки атак;
- карантин.

Механизм блокировки «превращает» систему обнаружения атак в систему противодействия атакам, что накладывает дополнительные ***требования***:

- сценарий действий в случае выхода из строя для Network IPS;
- наличие «мягкого» режима;
- отсутствие влияния на производительность;
- качество сигнатур, минимизация ложных срабатываний;
- понимание ожидаемого поведения контролируемого объекта, знание возможных атак и модификаций.

5. Введение в технологию обнаружения атак

5.2. Классификация систем обнаружения атак

Существует несколько вариантов классификации систем обнаружения атак.

Классификация по источнику данных (по принципу реализации) показывает, что именно защищает система обнаружения атак. Исполнение подобных систем возможно в двух ***вариантах***:

- на базе сетевого сегмента(Network-based) – системы, анализирующей трафик сетевого сегмента (подобно сетевому анализатору) в целях поиска признаков атак. К данному виду относится большая часть систем обнаружения атак;
- на базе узла (host-based) – системы, ориентированной на защиту отдельного узла (в некоторых случаях удобнее поместить систему обнаружения атак непосредственно на защищаемом узле). Входными данными для таких систем являются журналы регистрации и действий пользователей защищаемого узла.

Классификация по технологии обнаружения показывает, произошла атака или нет:

• обнаружение злоупотреблений (Misuse Detection) – известен перечень атак;

• обнаружение аномалий (Anomaly Detection) – известно поведение контролируемого объекта и любое отклонение считается атакой.

Данными для построения профиля поведения могут служить:

• объёмы трафика;