УДК 004.056.53

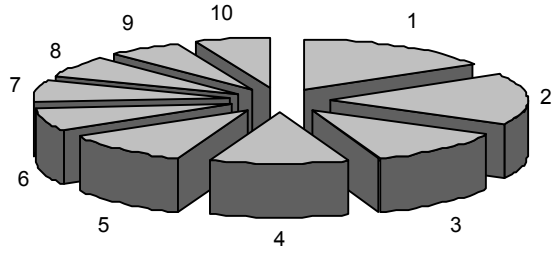
ТЕХНОЛОГИЯ МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ. ОСОБЕННОСТИ РЕАЛИЗАЦИИ ИНСПЕКТОРОВ СОСТОЯНИЯ

Е.А. Васильева

В настоящей статье описаны особенности функционировании межсетевых экранов – одной из самых востребованных технологий защиты сетевого взаимодействия в автоматизированных системах. Предлагается классификация межсетевых экранов по принципу фильтрации сетевого трафика; ставится задача тестирования инспекторов состояния.

На сегодняшний день одними из самых востребованных средств защиты сетевого взаимодействия являются межсетевые экраны (МЭ).

Так, результаты последних исследований в области информационной безопасности (согласно отчету CSI/FBI за 2006 г.) показывают, что на сегодняшний день в качестве средств защиты межсетевые экраны используют порядка 98 % компаний (рис. 1).



1 – межсетевой экран – 98 %
2 – антивирусы – 97 %
3 – серверные списки контроля – 70 %
4 – системы обнаружения вторжений – 69 %
5 – шифрование данных – 63 %
6 – системы аутентификации – 46 %
7 – управление событиями безопасности – 41 %
8 – межсетевые экраны на уровне приложений – 39 %
9 – смарт-карты и токены – 38 %
10 – PKI – 36 %

Рис. 1. Используемые технологии информационной безопасности (по данным отчета CSI/FBI 2006)

Технологии межсетевого экранирования появились практически одновременно с возникновением проблемы защиты компьютерных систем. Первые межсетевые экраны (МЭ) фильтровали сетевой трафик, анализируя его на уровне сетевых пакетов. Основным критерием фильтрации служили адреса источника и получателя пакетов. Пакеты пропускались или отбрасывались МЭ в зависимости от определенных политикой безопасности правил.

Современные МЭ являются сложными многофункциональными системами. Знание их архитектуры позволяет более полно оценить функциональные возможности МЭ как средства защиты. Под архитектурой МЭ понимаются, прежде всего, технические решения разработчиков, принятые за основу реализации разработанного продукта. При этом выделяют базовую платформу (аппаратная часть, операционная система), языки и среду разработки и алгоритмы функционирования, как отдельных модулей, так и МЭ в целом.

МЭ представляет собой программный, аппаратный или программно-аппаратный комплекс, реализующий функции фильтрации сетевого трафика (информационных потоков) между двумя (или более) автоматизированными системами по некоторому набору правил, определяемых политикой безопасности защищаемой сети[1]. Фильтрация трафика – одна из основных функций всех МЭ.

Существует множество различных классификаций МЭ. Несмотря на это, можно выделить основные категории МЭ: пакетные фильтры (packet filter); прикладные посредники (application proxy); инспекторы состояния (stateful inspection firewalls).

Пакетные фильтры. МЭ фильтры пакетов TCP/IP анализируют сетевой трафик на транспортном уровне и уровне межсетевого взаимодействия стека протоколов TCP/IP. Поля каждого пакета данных определены и стандартизованы (например, поле IP-адреса источника, поле IP-адреса получателя, поле транспортного порта источника, поле транспортного порта получателя и проч.). Статические пакетные фильтры анализируют заголовки пакетов, поступающих на сетевые интерфейсы МЭ. При настройке пакетных фильтров определяются правила, использующие в качестве критериев фильтрации поля заголовков пакетов[2]: IP-адрес источника пакета; IP-адрес получателя пакета; транспортный порт источника; транспортный порт получателя; протокол.

В качестве примера классического пакетного фильтра можно привести маршрутизатор, настроенный для использования списков контроля доступа (Access Control Lists, ACL)[3].

Важной особенностью любого пакетного фильтра является то, что он не хранит информацию о текущем соединении. Каждый пакет анализируется пакетным фильтром в соответствии с набором правил, определяемых политикой безопасности. После обработки очередного пакета никакой информации о нем не сохраняется. Следующий пакет обрабатывается точно таким же образом, как и предыдущий.

При получении очередного IP-пакета начинается проверка соответствия пакета правилам (рис. 2). Для каждого пакета правила просматриваются последовательно, начиная с первого. Просмотр правил заканчивается в случае нахождения первого правила, у которого выполняется условие его срабатывания, либо когда просмотрены все правила.

Под условием срабатывания правила понимается совпадение всех контролируемых параметров с указанными в данном правиле.

Выполнение действия, предусмотренного правилом, состоит в разрешении или блокировании пакета (с уведомлением об этом отправителя пакета или без него); трансляции адреса и номера порта; изменении дополнительных параметров TCP/UDP/IP-заголовка; процедуре по учету пакета (протоколирование событий) и в уведомлении администратора безопасности.

Если пакет не удовлетворяет ни одному из правил, то используется политика по умолчанию – либо разрешено все, что не запрещено, либо запрещено все, что не разрешено.

Пакетные фильтры имеют следующие недостатки. Произвольный пакет может быть пропущен, если он соответствует критериям, определенным правилами фильтрации. Фрагментированные пакеты могут быть пропущены через пакетный фильтр. Создание и изменение больших списков правил – достаточно трудоемкий процесс. Не все прикладные сервисы могут быть определены при помощи разрешающих и запрещающих правил (в качестве критерия в правиле можно определить номера транспортных портов, но не во всех современных приложениях – особенно новых мультимедийных приложениях – номера портов известны до установления соединения).

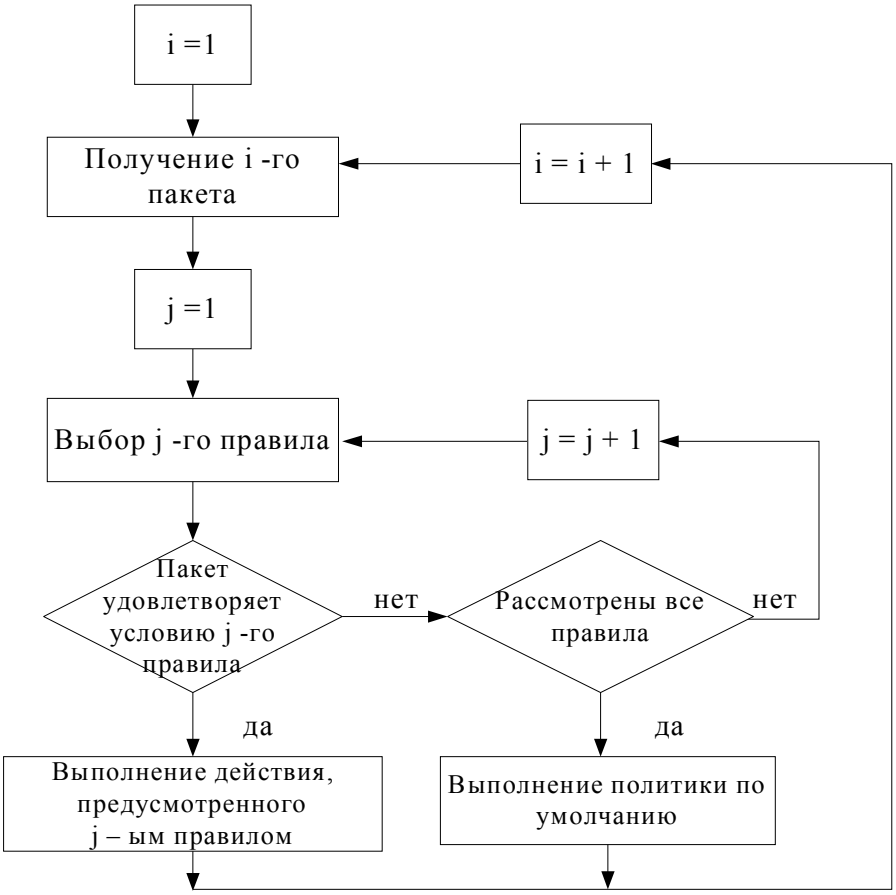


Рис. 2. Алгоритм обработки пакетов пакетным фильтром

Прикладные посредники. Прикладные посредники анализируют сетевой трафик на верхних уровнях эталонной модели взаимодействия открытых систем OSI (как правило, начиная с 4 транспортного уровня и заканчивая 7 прикладным). Очевидно, что прикладные посредники более детально анализируют проходящие через них пакеты[4]. Этот факт является причиной резкого снижения производительности МЭ. Пользователи получают доступ к ресурсам сети только после прохождения процедур установления соединения и их аутентификации. Пользователи подключаются не напрямую к сервисам внешней сети, а к прикладным посредникам, выступающим в роли шлюзов, соединяющих частную сеть с внешней сетью.

Перед соединением с внешней сетью пользователи внутренней сети должны установить соединение с прикладным посредником. Затем пользователи проходят процедуру аутентификации. На основании идентификатора и пароля пользователям предоставляется определенный уровень доступа к ресурсам внешней сети. При использовании прикладных посредников устанавливается два соединения: между пользователем и посредником и между посредником и узлом назначения из внешней сети. Существует вариант прозрачного для пользователя использования прикладного посредника, но и в этом случае устанавливается два соединения. При использовании прикладных посредников выявляются следующие возможные проблемы и недостатки. Прикладной посредник представляет собой единую «точку опасности», что означает компрометацию целой сети при получении несанкционированного доступа к прикладному посреднику. Добавление нового сервиса в МЭ прикладной посредник является сложной, часто невыполнимой задачей. Прикладные посредники обладают низкой производительностью; к тому же она резко снижается при увеличении нагрузки. Прикладные посредники обычно реализуются с использованием операционных систем (ОС) общего назначения и используют сетевые сервисы этих ОС. Это создает дополнительные уязвимости МЭ, связанные с уязвимостями самих ОС.

Инспекторы состояния. Инспекторы состояния – тип МЭ, сочетающий в себе преимущества пакетных фильтров и прикладных посредников. Технология инспекции состояния (stateful inspection) была разработана и впервые реализована в МЭ компанией Check Point.

Практически все производители современных корпоративных МЭ заявляют, что их изделия поддерживают данную технологию. Шлюзы сеансового уровня (session proxy), инспекторы состояния (stateful inspection), динамические пакетные фильтры (stateful packet filter), TCP/UDP-посредники (TCP/UDP proxy) – в большинстве случаев под этими терминами понимается следующее: ни один сетевой пакет не будет пропущен, если он не принадлежит к некоторому виртуальному соединению, ассоциированному МЭ с ранее установленным соединением. Исключение составляют пакеты, разрешенные политикой безопасности и принадлежащие текущей стадии установленного соединения. Информация обо всех виртуальных соединениях хранится в специальной таблице, называемой таблицей состояний.

При передаче данных соединения могут контролироваться следующие параметры: длительность соединения, скорость передачи данных, текущие параметры окна TCP-соединения, большое количество ошибок передачи данных.

Контролирование этих параметров позволяет правильно распределить пропускную способность канала связи между несколькими соединениями, тем самым ограничив максимально возможную загрузку линий связи трафиком злоумышленника, а также позволяет вовремя обнаружить деятельность злоумышленника и закрыть (т.е. завершить по инициативе посредника*)* данное соединение (с протоколированием причины и уведомлением об этом администратора).

Рассмотрим принцип функционирования инспектора состояния в части, реализующей определение допустимости соединения (рис. 3).

При получении очередного запроса на соединение правила просматриваются последовательно, начиная с первого. Просмотр правил заканчивается в случае нахождения первого правила, у которого выполняется условие его срабатывания, либо когда просмотрены все правила.

Под условием срабатывания правила понимается совпадение всех контролируемых параметров с указанными в данном правиле. Комплексное действие правила состоит из действия по разрешению или запрещению данного соединения, условий передачи данных и завершения соединения по инициативе посредника (на основе параметров, контролируемых во время передачи данных). Если подходящее правило не было найдено, то используется политика по умолчанию – соединение запрещается, а соответствующая попытка установления связи протоколируется.

Эффективность инспекторов состояния обусловлена следующими причинами: инспекторы состояния анализируют каждый пакет и проверяют его принадлежность существующему виртуальному соединению; инспекторы состояния обладают хорошей производительностью (сравнимой с производительностью пакетных фильтров); инспекторы состояния хранят в таблице состояний записи для каждого соединения или транзакции используются для передачи данных в протоколах без установления соединения (например, в протоколе UDP). Таблица состояний является ключевым элементом при определении разрешения/запрещения прохождение пакета через МЭ из одной сети в другую.

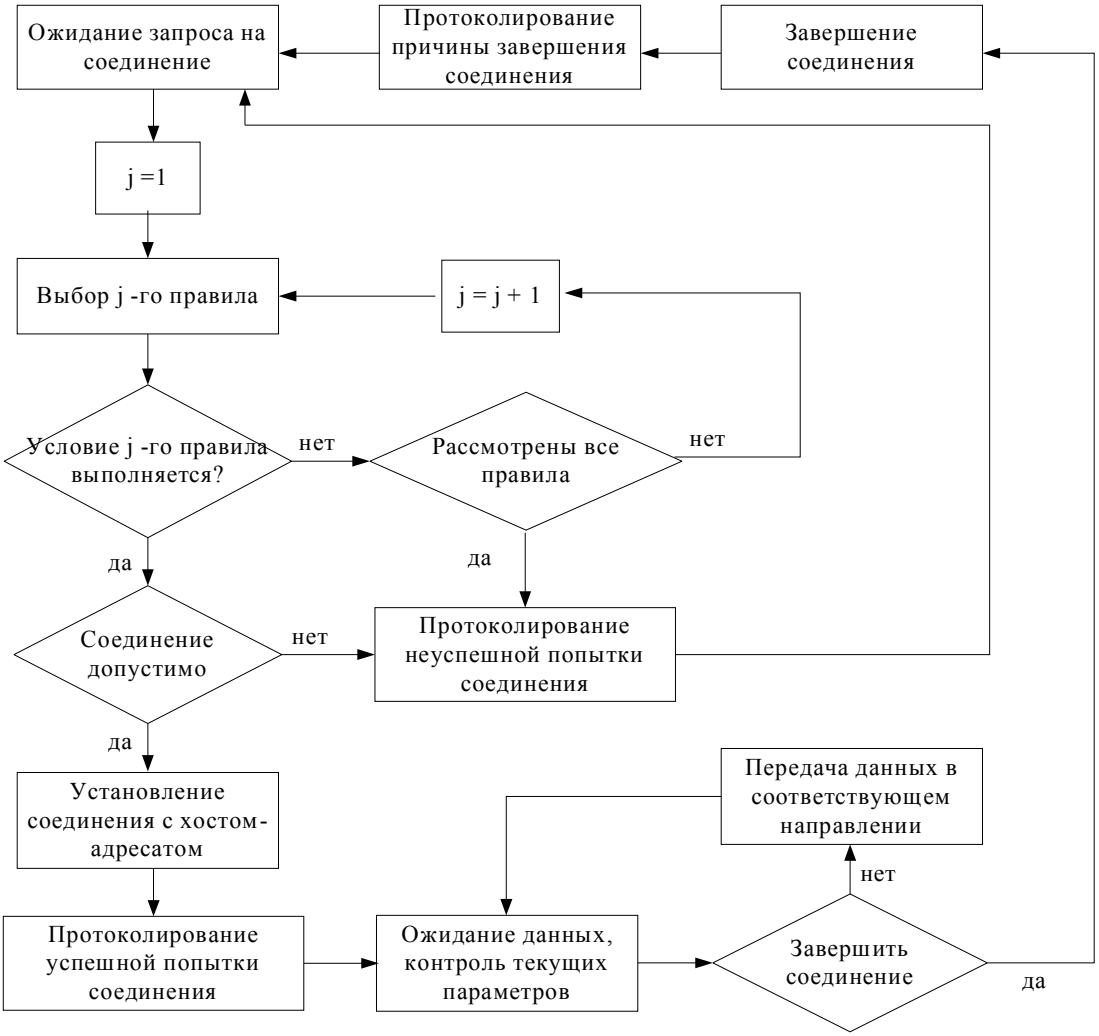


Рис. 3. Алгоритм функционирования посредника уровня соединения

В большинстве случаев проверка и сравнение заявленных возможностей МЭ различных производителей не вызывает проблем. Исследование (тестирование) же инспекторов состояния из-за особенностей функционирования ставит перед специалистами ряд вопросов. Основная сложность заключается в том, что подробные алгоритмы их функционирования являются авторскими разработками и не раскрываются производителями. Ситуация осложняется тем, что на сегодняшний день не существует специальных прикладных средств, предназначенных для проведения таких тестов. Данная проблема является темой для дальнейших исследований.

---

[1] ***Лебедь С.В.*** Межсетевое экранирование. Теория и практика защиты внешнего периметра. М.: Изд-во МГТУ им. Н.Э. Баумана, 2002. 304 с.

[2] ***Оглтри Т.*** Firewalls. Практическое применение межсетевых экранов. М.: Изд-во ДМК, 2001. 400 с.

[3] ***Чемпмен мл. Дэвид***, ***Фокс Энди***. Брандмауэры Cisco Secure PIX.: Пер. с англ. М.: Издательский дом «Вильямс», 2003. 384 с.

[4] ***Шипли Грег***. Прорыв в межсетевом экранировании // Сети и системы связи. 2005. № 9. С. 93–100.