СПИСОК ЛИТЕРАТУРЫ

1. Руководящий документ. Защита от несанкционированного доступа к информации. Государственная техническая комиссия при Президенте Российской Федерации. 1999 г. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей.

Е. А. Васильева, Н. В. Медведев (к. т. н., доцент)
Московский государственный технический университет им. Н. Э. Баумана

МЕТОДИКА ТЕСТИРОВАНИЯ МЕЖСЕТЕВЫХ ЭКРАНОВ

Рассматриваются особенности реализации межсетевых экранов с инспекцией состояния, и предлагается подход к их тестированию.

Введение

На сегодняшний день одними из самых востребованных средств защиты сетевого взаимодействия являются межсетевые экраны. Межсетевой экран (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. Существует множество различных классификаций МЭ [1–3]. Несмотря на это, можно выделить основные категории МЭ: пакетные фильтры (packet filter), прикладные посредники (application proxy), инспекторы состояния (stateful inspection firewalls).

В большинстве случаев проверить и сравнить заявленные возможности МЭ различных производителей не вызывает проблем [4]. 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.

Основной принцип работы инспектора состояния заключается в следующем [1]: ни один сетевой пакет не будет пропущен, если он не принадлежит к некоторому виртуальному соединению, ассоциированному МЭ с ранее установленным соединением (рис. 1). Исключение составляют пакеты, разрешенные политикой безопасности и принадлежащие текущей стадии установленного соединения. Информация обо всех виртуальных соединениях хранится в специальной таблице, называемой таблицей состояний.

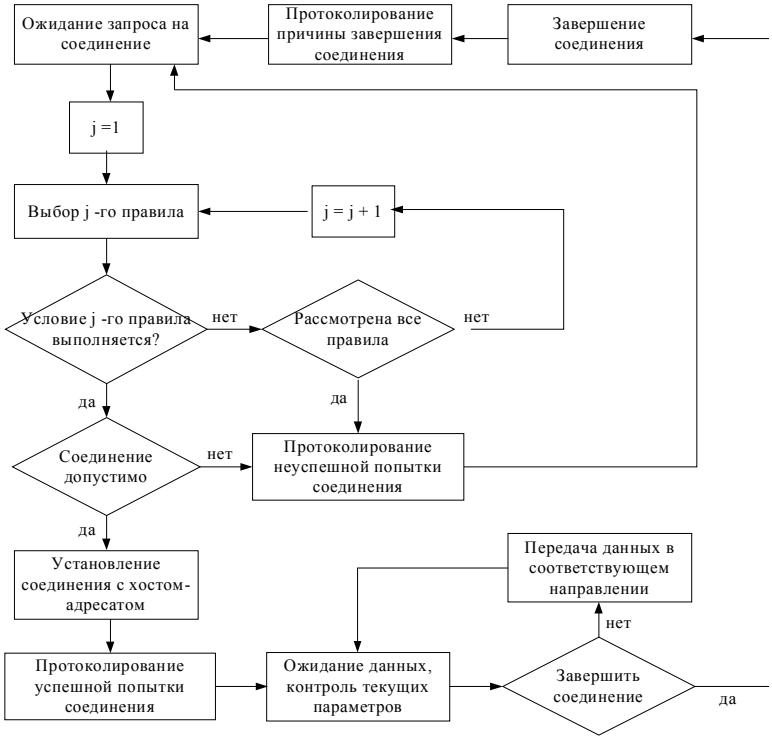

Рис. 1. Алгоритм функционирования посредника уровня соединения

1. Структура стенда тестирования

Анализ основных функций и схемы работы инспекторов состояния позволяет разработать структуру аппаратно-программного стенда тестирования для исследования инспекторов состояния межсетевых экранов. Логическая схема стенда тестирования представлена на рис. 2.

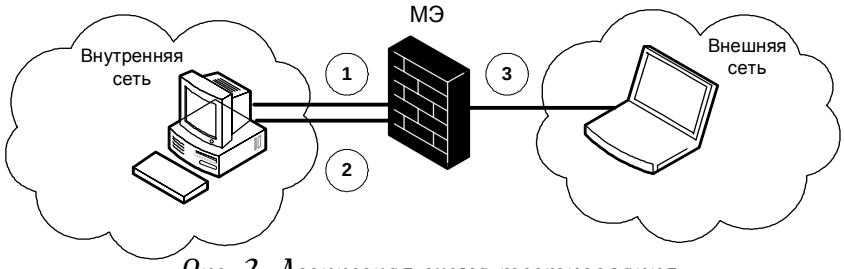

Рис. 2. Логическая схема тестирования

Логически структура стенда делится на внутреннюю (защищаемую) и внешнюю сети, которые взаимодействуют через МЭ (1 — внутренний интерфейс МЭ, 2 — внешний интерфейс, 3 — интерфейс управления).

Во внутренней сети необходимо выделить сервер (это может быть web-сервер, почтовый сервер, Telnet-сервер и др.); анализатор трафика; сервер протоколирования (Syslog). Во внешней сети необходимо выделить клиента (с установленными клиентами прикладных служб) и анализатор трафика. Сервер внутренней сети используется для обслуживания запросов клиента внешней сети. Взаимодействие может быть организовано с использованием любого протокола прикладного уровня (например, HTTP, FTP, SMTP, Telnet).

Анализаторы трафика служат для регистрации и разбора пакетов, передающихся через МЭ, а также для регистрации изменений, вносимых в пакеты межсетевым экраном. Для тестирования инспектора состояния анализаторы трафика должны поддерживать функцию генерации трафика.

Сервер Syslog во внутренней сети служит для получения, сохранения и анализа системного журнала событий МЭ.

2. Получение тестовых наборов

Непосредственно перед проведением тестов необходимо выполнить следующие предварительные шаги:

— запустить анализаторы трафика во внутренней и внешней сети;

— открыть разрешенное соединение между клиентом и сервером; при этом регистрируется сетевой трафик в обоих сегментах сети;

— закрыть соединение с клиентом обычным образом на прикладном уровне;

— остановить регистрацию трафика сетевыми анализаторами.

В результате выполнения этих действий получаются «снимки» разрешенного соединения во внутреннем и внешнем сегментах. Полученные снимки будут использовать в качестве тестовых пакетов. Очевидно преимущество данного метода: набор тестовых пакетов был получен автоматически, и данные пакеты принадлежали разрешенному политикой безопасности соединению.

3. Допущения о работе инспектора состояния

Полноценная инспекция состояния реализуется только для протокола TCP, поэтому тестирование логично проводить с использованием этого протокола.

Так как МЭ в процессе данного тестирования представляет собой «черный ящик», т. е. точные алгоритмы инспекции состояния производителем не раскрываются, тестирование организуем на основе предположений. Логично предположить, что любой МЭ, фильтрующий пакеты на основе данных состояния проходящих через него сессий TCP, должен, как минимум,

— просматривать IP-адреса взаимодействующих узлов;

— просматривать номера транспортных портов на каждом конце соединения;

— просматривать установленные флаги заголовка протокола TCP — SYN, ACK, RST, FIN, используемые при установлении, квитировании, синхронизации и закрытии соединения;

– контролировать поток пакетов, открывающих, поддерживающих и завершающих соединение;

– анализировать порядковые номера TCP-последовательностей (TCP Sequence Numbers).

4. Методика тестирования

Основываясь на сделанных предположениях, можно предложить комплексный набор тестов для выявления особенностей реализации инспектора состояния в МЭ. Тестирование инспектора состояния предлагается проводить в двух режимах:

– при отсутствии активных сессий через МЭ;

– при наличии активной сессии, установленной через МЭ между клиентом внешней сети и сервером внутренней сети.

Тест при отсутствии активных сессий заключается в проверке прохождения через МЭ произвольного пакета (параметры пакета разрешены политикой безопасности МЭ) из полученного «снимка» при отсутствии открытых соединений. МЭ не должен пропустить ни один такой пакет, кроме SYN-пакета, открывающего соединение и добавляющего запись в таблицу состояний. Правильное прохождение МЭ данного теста говорит о самом факте наличия в МЭ реализованной технологии межсетевого экранирования. Корректность же реализации и отсутствие уязвимостей позволяет установить тестирование при наличии активных сессий.

Тест при наличии активных сессий проверяет, будут ли пропущены сетевые пакеты, принадлежащие текущему открытому TCP-соединению, но с измененными параметрами, например отправленные «не в свое время». Сложность этого теста заключается в том, что изначально отсутствуют данные о параметрах виртуального соединения, создаваемого МЭ. Особенно важным и неизвестным параметром в данном случае является диапазон допустимых номеров TCP-последовательностей. В предположении, что диапазон номеров последовательностей начинается с начальных номеров инициализации TCP-соединения, предлагается следующий алгоритм действия:

1) запустить оба анализатора трафика;

2) открыть разрешенное TCP-соединение;

3) поддерживать соединение открытым (это можно сделать, например, путем передачи команд или данных на прикладном уровне);

4) остановить анализатор трафика внешней сети;

5) выбрать пакет из «снимка», изменив при необходимости номера последовательностей или другие параметры (в зависимости от теста);

6) отправить выбранный пакет через МЭ, при этом TCP-соединение остается открытым;

7) остановить анализатор трафика внутренней сети.

Для проведения комплексного тестирования предлагается следующий набор тестов при наличии активных сессий (Таблица 1).

Таблица 1. Набор тестов.

№ теста	Содержание теста	Реакция эталонного МЭ
1	Проверка блокирования пакетов ACK с корректными номерами портов, но неправильными порядковыми номерами	блокируются
2	Проверка разрешения приема пакетов ACK с номерами пакетов, не выходящими за границы окна	пропускаются
3	Проверка блокирования пакетов RST с корректными номерами портов, но неверными порядковыми номерами	блокируются
4	Проверка прохождения пакетов RST с корректными номерами портов и порядковыми номерами, не выходящими за границы окна	пропускаются
5	Проверка блокирования пакетов FIN с корректными номерами портов, но неверными номерами последовательностей	блокируются
6	Проверка прохождения пакетов RST с корректными номерами портов и порядковыми номерами, не выходящими за границы окна	пропускаются
7	Проверка ограничения (блокирования) SYN-пакетов, принадлежащих текущему соединению	блокируются или ограничиваются
8	Проверка ограничения количества FIN-пакетов, принадлежащих текущему соединению, без пакетов подтверждения FIN-ACK	ограничиваются
9	Проверка блокирования пакетов ACK с неправильными номерами портов отправителя и неправильными номерами последовательностей	блокируются
10	Проверка блокирования пакетов с некорректными комбинациями флагов	блокируются

Результаты тестирования МЭ сравниваются с поведением эталонного инспектора состояния, и делаются выводы об особенностях реализации функции инспекции состояния, наличии или отсутствии уязвимостей.

Выводы

Предложенная методика подходит для проведения испытаний на этапе внедрения (выбора) МЭ, а также для проведения сертификационных испытаний для проверки корректности реализации технологии инспекции состояния.

СПИСОК ЛИТЕРАТУРЫ

1. *Лебедь С. В.* Межсетевое экранирование. Теория и практика защиты внешнего периметра. М., 2002. – 304 с.
2. *Лапонина О. Р.* Межсетевое экранирование. М., 2007. – 343 с.
3. *Оглтри Т.* Firewalls. Практическое применение межсетевых экранов. М., 2001. – 400 с.
4. *Васильева Е. А.* Классификация современных подходов к тестированию межсетевых экранов // Научная сессия МИФИ-2008. XV Всероссийская научная конференция «Проблемы информационной безопасности в системе высшей школы». Сборник научных трудов. М., 2008.

С. А. Давыдов
ВНИИ Проблем вычислительной техники и информатизации

ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРЕДАЧИ ЮРИДИЧЕСКИ ЗНАЧИМЫХ ОТЧЕТНЫХ ДАННЫХ

Развитие экономики России сопровождается значительным ростом крупных территориально распределенных компаний, эффективность бизнеса которых в значительной степени зависит от использования ими информации для принятия управленческих решений. В таких компаниях широко развита региональная сеть представительств, в частности, такой является территориально распределенная компания ОАО «Аэрофлот». В ее состав входят более ста представительств в России и за рубежом, в обязанности которых входят выполнение работ по обеспечению авиаперевозок и представление интересов авиакомпании. В этих условиях руководству компании для принятия управленческих решений необходимо иметь юридически значимую оперативную информацию о деятельности всех подразделений компании, причем важны не только исходные данные о работе каждого представительства, но и агрегированная аналитическая информация по каждому представительству в отдельности и всем вместе.

Юридическая значимость электронных документов обеспечивается информационной технологией их изготовления и фиксацией в них сведений, заверенных с помощью электронной цифровой подписи (ЭЦП). Вопросы выработки и проверки ЭЦП, организации пространства PKI достаточно хорошо изучены. При этом вопросам разработки информационных технологий формирования электронных документов традиционно уделяется недостаточно внимания. Задача еще более усложняется, если система собирается из разнородных информационных систем, обменивающихся данными в разных форматах.

Проектирование такой системы, которая должна обеспечить юридическую значимость электронных документов, необходимо осуществлять с учетом как самих бизнес-процессов, так и организации взаимодействия со смежными информационными системами.

Одному из примеров такого проектирования посвящена настоящая работа.

Для решения этой проблемы предлагается следующая технология проектирования информационной системы обеспечения передачи юридически значимых отчетных документов, которая включает следующие разделы.