УДК 621.391

РЕАЛИЗАЦИЯ ФУНКЦИИ КОНТРОЛЯ СОЕДИНЕНИЯ В МЕЖСЕТЕВОМ ЭКРАНЕ

М.Н. БОБОВ, Ф.О. МОХАММЕД

ОАО «АГАТ – системы управления»
пр. Независимости, 117, Минск, 220023, Беларусь

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 1 июня 2011

Межсетевой экран (МСЭ) проверяет и следит за изменением состояния каждого соединения, проходящего через него. Если соединение разрешено (поток трафика разрешен списком доступа), то каждое изменение состояния регистрируется в таблице соединений МСЭ. После начала соединения и выполнения входа в таблице соединений разрешается передача пакетов от источника к получателю. Обратная связь от получателя к источнику через МСЭ также разрешена.

Ключевые слова: межсетевой экран, таблица соединения, полуоткрытое соединение, рандомизация, порядковый номер.

Введение

Состояние соединения и движение пакетов от источника к получателю должны соответствовать правилам используемого протокола. При любых отклонениях от разрешенных действий соединение удаляется с регистрацией в журнале. Каждое подключение, заносимое в таблицу соединений, содержит следующие параметры:

- используемый протокол (TCP, UDP или ICMP),
- локальный и глобальный адреса,
- номер локального и глобального порта,
- флаги состояния соединения,
- счетчик времени простоя (увеличивается, если ни один из пакетов не использует соединение),
- счетчик байтов (общий объем трафика, используемый соединением),
- локальный и глобальный порядковые номера.

Поддерживаемое количество сессий МСЭ зависит от модели устройства и установленной лицензии. МСЭ разрешает подключение только для количества пользователей, указанных в лицензии. Подключение дополнительных пользователей запрещено, даже если кто-либо из разрешенных пользователей не отправляет пакеты.

Для отслеживания соединений, когда пользователь начинает соединение, МСЭ вычитает данное соединение из количества соединений, разрешенных лицензией. После завершения соединения МСЭ добавляет единицу к счетчику доступных соединений.

Принцип работы МСЭ

На рис. 1 представлен пример проверки соединения, выполняемого МСЭ. Ниже описывается последовательность действий, отображенных на рис. 1.

1. Пользователь А (ПК-А) внутри сети отправляет HTML-запрос на внешний сервер через МСЭ.

2. МСЭ собирает информацию о пользователе, отправившем запрос: адреса источника и получателя, протокол, номера портов источника и получателя, и сохраняет их в новой таблице входящего соединения.

3. МСЭ направляет HTTP-запрос на целевой веб-сервер.

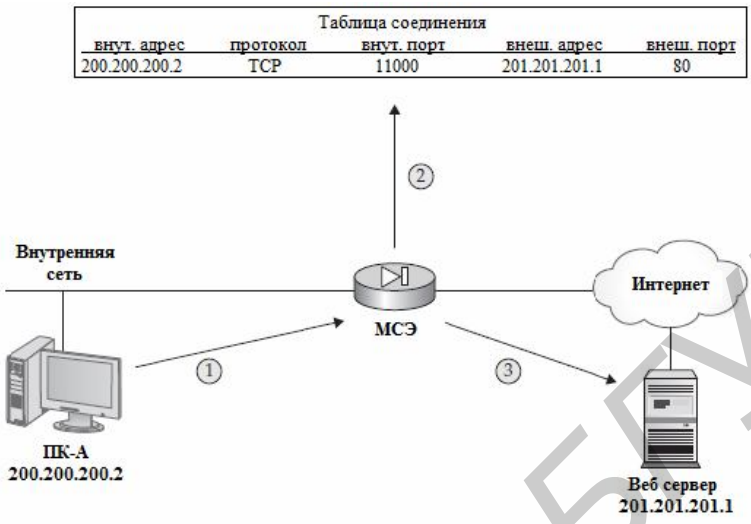

Рис. 1. МСЭ добавляет соединение в таблицу соединений

На рис. 2 показан возвращаемый трафик от HTTP-сервера к пользователю. Ниже представлена последовательность возврата трафика.

1. Веб-сервер отправляет соответствующую веб-страницу пользователю.

2. МСЭ принимает ответ HTTP-сервера и сравнивает его со входами таблицы состояния:

А) если в таблице состояния найден соответствующий вход, то получение пакетов разрешено;

В) если в таблице состояния соответствующий вход не найден, то переходящие пакеты отбрасываются.

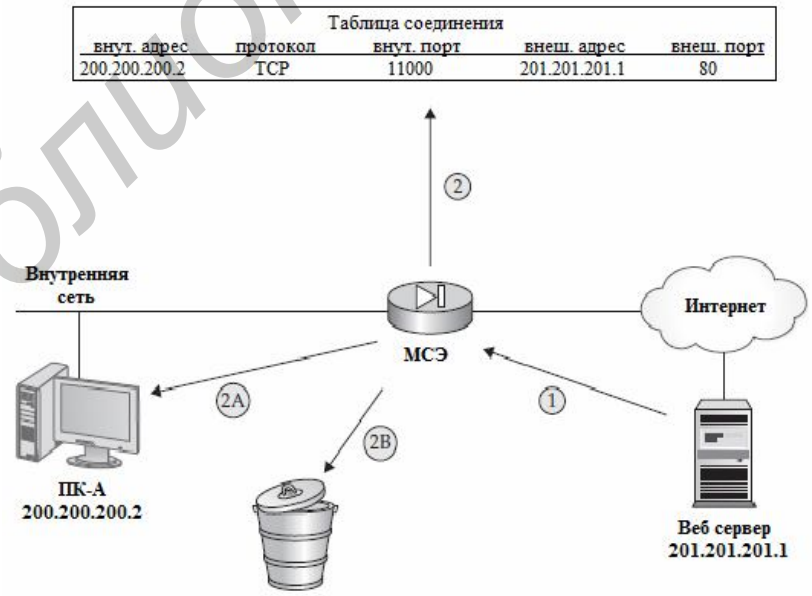

Рис. 2. Сверка МСЭ возвращаемого трафика с информацией из таблицы соединений

МСЭ сохраняет данную таблицу соединения до обнаружения запроса о прекращении соединения между источником и получателем. При получении такого сообщения он удаляет соответствующие данные из таблицы соединения. Если соединение некоторое время не ис-

пользуется и установленное время простоя истекло, то данные о подключении также удаляются из таблицы соединения.

На рис. 3. показан алгоритм проверки таблицы соединения в МСЭ.

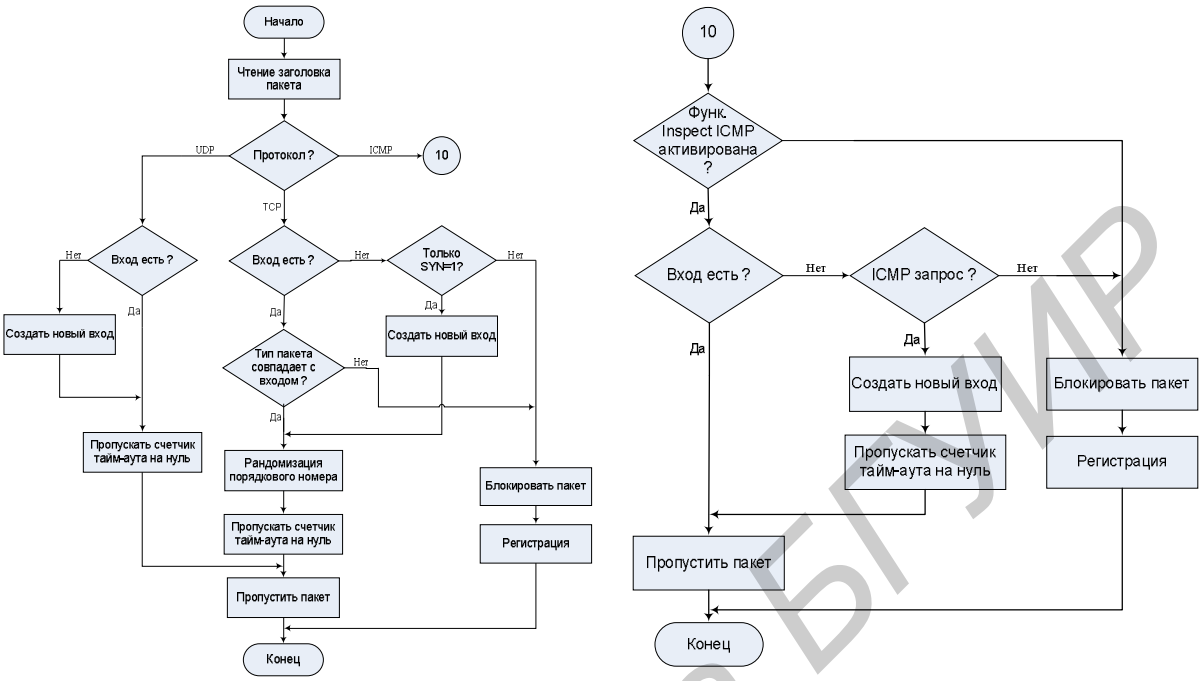

Рис. 3. Алгоритм проверки таблицы соединения в МСЭ

Рандомизация порядкового номера

Функция рандомизации порядкового номера используется для защиты пользователя от проникновения и кражи информации во время TCP-сессии. Проблемой протокола TCP является то, что в большинстве стеков протокола TCP/IP используется предсказуемый метод отбора порядковых номеров – порядковый номер в заголовке TCP указывает количество отправленных байт. Опытные хакеры могут использовать данную информацию для внедрения в сессии своих запросов.

Функция рандомизации порядкового номера в МСЭ решает эту проблему посредством рандомизации порядковых номеров. МСЭ сохраняет старый и новый порядковые номера в таблице соединений. Когда трафик возвращается через МСЭ от получателя к источнику, МСЭ ищет данную информацию и производит откат изменений.

Например, TCP-сегмент может пройти через МСЭ, поскольку порядковый номер в сегменте равен 578, как показано на рис. 4. Функция рандомизации порядкового номера заменяет данный порядковый номер случайным номером и сохраняет его в таблице состояний (в данном случае – номер 992), а затем отправляет сегмент к получателю. Получатель принимает сегмент, не замечая изменения порядкового номера, он отправляет источнику номер подтверждения (acknowledgment number) 993. После получения отклика, МСЭ проводит откат процесса рандомизации порядкового номера посредством замены значения 993 на 579, потому что процесс подтверждения TCP увеличивает порядковый номер на один и использует получившееся значение в качестве номера подтверждения. Рис. 4. иллюстрирует процесс рандомизации порядкового номера в МСЭ.

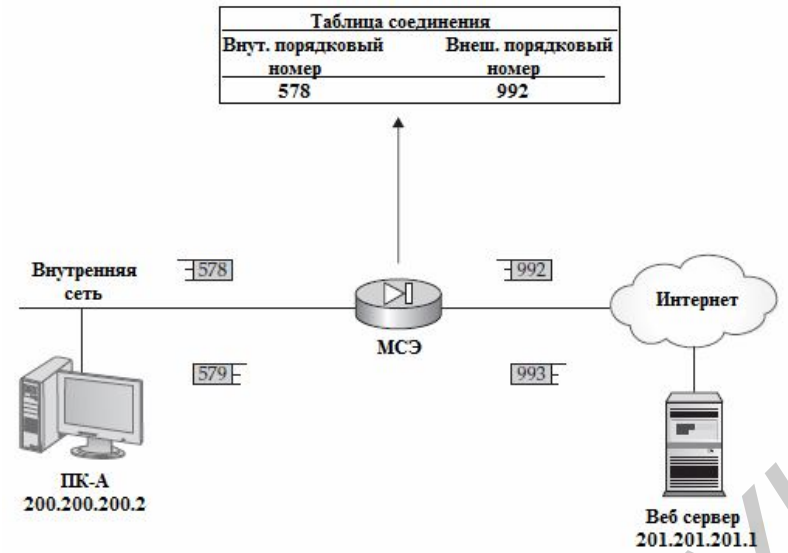

Рис. 4. Рандомизация порядкового номера в МСЭ

Ограничение полуоткрытых соединений

Для создания TCP-соединения необходимо произвести обмен сообщениями (three-way handshake SYN-SYN/ACK-ACK) между двумя компьютерами. Если обмен сообщениями не закончен, то соединение называется полуоткрытым (начатое, но не установленное).

Полуоткрытое соединение может также появиться при задержке или потере пакетов в режиме установления соединения. Таким образом, при нормальных условиях ПК сохраняет полуоткрытое соединение во время ожидания завершения процесса обмена сообщениями. В этом случае хакер может начать создавать множество полуоткрытых соединений к получателю, что приводит к отказу ПК от обслуживания подключений.

МСЭ может ограничивать количество полуоткрытых соединений, направленных определенному получателю. Это касается исключительно входящих соединений, когда внешние пользователи начинают соединения с внутренними пользователями.

До достижения предела подключений МСЭ проверяет каждый SYN-пакет и добавляет новый вход в таблице соединения (помечается полуоткрытое соединение), а затем направляет SYN-пакет к получателю. Если внутренний ПК ответил сообщением SYN/ACK, за которым следует сообщение ACK от внешнего пользователя, соединение установлено правильно. Если обмен пакетами не окончен в течение 30 с, то МСЭ удаляет соответствующий вход автоматически из-за истечения времени простоя (SYN timeout).

В случае, когда установленный предел превышен, МСЭ начинает перехватывать новые SYN-пакеты и отвечать отправителю вместо внутреннего ПК. Данные действия не добавляются в таблицу соединений МСЭ. Вместо этого МСЭ отправляет внешнему ПК пустой SYN/ACK-пакет, отправленный от имени внутреннего ПК. Если внешний ПК отправляет сообщение ACK, то между инициатором и внутренним ПК создается соединение. Таким образом, МСЭ работает как прокси-сервер.

Удаление соединений

Определение момента завершения соединения и удаление его из таблицы состояния зависит от используемого протокола: TCP, UDP, или ICMP. Для удаления входящего соединения TCP используются следующие критерии:

- флаги FIN и FIN/ACK в поле управления заголовка TCP;
- флаг RST в поле управления заголовка TCP;
- соединение TCP не используется более 3600 секунд (1 часа по умолчанию);
- соединение удаляется из таблиц соединения командой clear xlate.

Для протокола UDP используются следующие критерии удаления входа из таблицы состояния:

- соединение UDP не используется более 120 с (2-х мин по умолчанию);
- для запроса DNS указывается соответствующий отклик DNS;
- соединение удаляется из таблиц сетевого экрана командой clear xlate.

Для протокола ICMP используются следующие критерии удаления входа из таблицы состояния:

- соединение ICMP не используется более 2 с (по умолчанию);
- соединение удаляется из таблиц сетевого экрана командой clear xlate.

Заключение

Проверка соединения является современной и самой эффективной функцией, используемой МСЭ для защиты локальных сетей. Она обеспечивает прохождение только пакетов, являющихся частью одного соединения, пропуская их потоками. Таким образом, функция проверки соединения сокращает общее время обработки пакетов МСЭ и повышает пропускную способность МСЭ.

REALIZATION OF CONNECTION CONTROL FUNCTION IN FIREWALL

M.N. BOBOF, F.O. MOHAMMED

Abstract

A Cisco firewall examines and keeps track of the state of each connection attempting to go through it. This is often called stateful inspection. If a connection is allowed to form (the access list permits the traffic flow), each state change is updated in the firewall's connection table. As soon as a connection initiates and a connection table entry is created, traffic from the source to the destination is allowed to pass. As well, the return traffic for that connection is allowed back through the firewall toward the source.

Литература

1. *David Hucaby*. Cisco ASA, PIX, and FWSM Firewall Handbook // USA, 2008.
2. *Richard A. Deal.* Cisco ASA Configuration // USA, 2009.
3. *Ray Blair, Arvind Durai* // Cisco ASA 5500 Series Configuration Guide using the CLI, Software Version 8.2. USA, 2009.
4. RFC 793 – Transmission Control Protocol.
5. RFC 768 – User Datagram Protocol.
6. RFC 792 – Internet Control Message Protocol.