УДК 621.391

МЕТОДЫ ИСПОЛЬЗОВОНИЯ МЕХАНИЗМА ПОИСКА ОБРАТНОГО МАРШРУТА ДЛЯ ЗАЩИТЫ ЛОКАЛЬНЫХ СЕТЕЙ ОТ АТАКИ СПУФИНГА

М.Н. БОБОВ*, Ф.О. МОХАММЕД

** Научно-исследовательский институт средств автоматизации*
пр. Независимости, 117, Минск 220023, Беларусь

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

Поступила в редакцию 1 октября 2010

Механизм поиска обратного маршрута (Reverse Path Forwarding (RPF)) используется межсетевыми экранами для предотвращения злонамеренного трафика на внутреннюю сеть, и включает в себя проверку правильности адреса источника в получаемых пакетах. Если адрес источника не действителен, пакет отбрасывается.

Ключевые слова: межсетевой экран, поиск обратного маршрута, свободный способ, строгий способ.

Введение

Межсетевые экраны используют механизм поиска обратного маршрута для защиты локальных сетей от атаки подделки адреса отправителя (атаки спуфинга). Этот механизм проверяет все типы пакетов, которые проходят через межсетевой экран. Когда обрабатываются TCP или UDP пакеты то, МСЭ проверяет адрес источника только в первом пакете сессии. Если пакет разрешен, то сессия добавляется в таблицу соединения, которая потом используется для разрешения прохождения следующих пакетов. Так как если пакет запрещен, то его прохождение блокируется. ICMP трафик является некоммутируемым, и у его нет сессии, МСЭ проверяет адрес источника и принимает решение для каждого приходящего пакета.

Основная часть

Механизм поиска обратного маршрута включает два способа проверки: свободный и строгий, а также их комбинацию. Кроме того, он поддерживает проверку маршрута по умолчанию. Выбор используемого способа на каждом интерфейсе межсетевого экрана зависит от реализации сегмента сети, связанного с этим интерфейсом.

Свободный способ RPF

В свободном способе RPF пакет должен быть получен от интерфейса, который будет использоваться межсетевым экраном для отправки возвращаемого пакета. При свободном способе механизм RPF может блокировать законный трафик, если он поступает через интерфейс, который выбран межсетевым экраном для отправки возвращаемых пакетов. Эта проблема возникает тогда, когда в сети присутствуют асимметричные маршруты. Рис. 1 поясняет алгоритм этого способа. Реализация способа включает следующие шаги:

Шаг 1. Правильность адреса источника проверяется следующим образом:

- Блокируются пакеты с адресами источников (SA=255.255.255.255).

- Блокируются пакеты с нулевыми адресами источников (SA=0.0.0.0) и адресами назначения (DA≠255.255.255.255). (Пакет с адресом источника SA=0.0.0.0, и адресом назначения DA=255.255.255.255, может быть пакетом DHCP или BOOT протоколов и таким образом не отбрасываются).

Шаг 2. Анализируется таблица FIB, если адрес источника входящего пакета найден, пакет пропускается.

Шаг 3. Если адрес источника не найден в таблице FIB, RPF принимает решение, основанное на маршруте по умолчанию и ключевом слове «маршрут по умолчанию разрешён».

- Если маршрут по умолчанию не установлен, пакет блокируется.

- Если маршрут по умолчанию доступен, но ключевое слово «маршрут по умолчанию разрешён» не сформировано, то пакет блокируется.

- Если маршрут по умолчанию доступен и ключевое слово «маршрут по умолчанию разрешён» сформировано, то пакет пропускается.

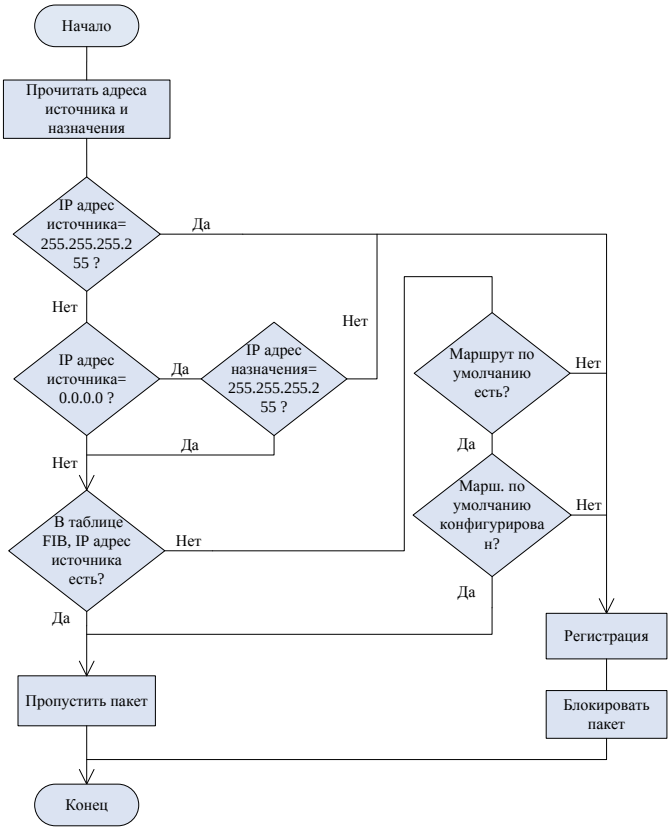

Рис. 1. Алгоритм свободного способа RPF

Строгий способ RPF

В строгом способе RPF, адрес источника должен находиться в таблице маршрутизации. Администраторы могут изменить это поведение, используя выбор «разрешено по умолчанию», который позволяет использование маршрута по умолчанию в процессе проверки источника. Кроме того, если обратный маршрут до любого источника указывает на нулевой интерфейс, то все пакеты содержащие адрес этого источника блокируются. Рис. 2 поясняет алгоритм этого способа.

Строгий способ RPF на практике используется в сетях, которые содержат асимметричные маршруты. Межсетевые экраны реализуют этот способ следующими шагами:

Шаг 1. Правильность адреса источника проверяется следующим образом:

- Блокируются пакеты с адресами источников (SA=255.255.255.255).

- Блокируются пакеты с нулевыми адресами источников (SA=0.0.0.0) и адресами назначения (DA≠255.255.255.255). (Пакет с адресом источника SA=0.0.0.0, и адресом назначения

DA=255.255.255.255, может быть пакетом DHCP или BOOT протоколов и таким образом не блокируются).

Шаг 2. Анализируется таблица FIB, если адрес источника входящего пакета найден, то осуществляется поиск обратных маршрутов (reverse route lookup) к адресу источника. Если, по крайней мере, один исходящий интерфейс из таких маршрутов соответствует интерфейсу получения, пакет пропускается, иначе пакет блокируется.

Шаг 3. Если адрес источника не найден в таблице FIB, принимается решение, основанное на маршруте по умолчанию и ключевом слове «allow-default-route».

- Если маршрут по умолчанию отсутствует, пакет блокируется.

- Если маршрут по умолчанию имеется, но ключевое слово, «allow-default-route» не формируется, пакет блокируется.

- Если маршрут по умолчанию имеется, ключевое слово «allow-default-route» сформировано, и исходящий интерфейс маршрута по умолчанию является интерфейсом получения, то пакет пропускается. В противном случае, пакет блокируется.

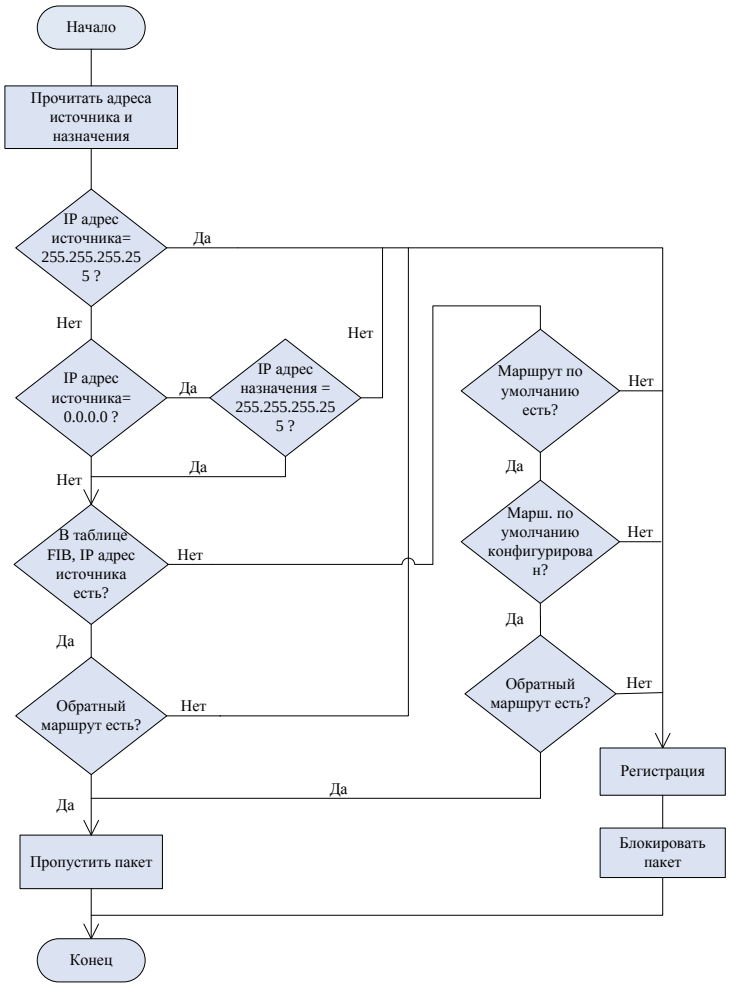

Рис. 2. Алгоритм строгого способа RPF

Заключение

Механизм поиска обратного маршрута обеспечивает эффективную защиту локальных сетей от атаки спуфинга и блокирует пакеты с подделками адресами от прохождения на внутреннюю сеть.

С помощью данного механизма и другими последовательно выполняемыми функциями и механизмами, межсетевой экран обеспечивает полномасштабную защиту локальных сетей от несанкционированного доступа и сетевых атак.

METHODS OF USING REVERSE PATH FORWARDING FOR PROTECTING LOCAL NETWORKS FROM SPOOFING ATTACK

M.N. BOBOF, F.O. MOHAMMED

Abstract

The reveres path forwarding (RPF) is a technology used by firewalls to prevent the malicious traffic in local networks by verifying the reality of the source address in received packets. To protect local networks from spoofed addresses appearance, RPF blocks any packet that don't pass RPF test.

Литература

1. *В.Г. Олифер, Н.А. Олифер*, Компьютерные сети, принципы, технологии, протоколы. СПб. 2007.
2. *Richard A. Deal*. Cisco ASA Configuration. USA, 2009.
3. *Ray Blair, Arvind Durai*. Cisco Secure Firewall Services Module (FWSM). USA, 2009.
4. *David Hucaby*. Cisco ASA, PIX, and FWSM Firewall Handbook. USA, 2008.