Network Working Group D. Senie
Request for Comments: 2644 Amaranth Networks Inc.
Updates: 1812 August 1999
BCP: 34
Category: Best Current Practice

Смена принятого по умолчанию поведения маршрутизаторов по отношению к пакетам Directed Broadcast

Changing the Default for Directed Broadcasts in Routers

Статус документа

В этом документе приведена основанная на обобщении опыта информация, которая может быть полезна сообществу Internet. Документ служит приглашением к дискуссии в целях дальнейшего совершенствования и может распространяться без ограничений.

Авторские права

1. Введение

В требованиях к маршрутизаторам [1] указано, что эти устройства должны принимать и пересылать широковещательный трафик directed broadcast[1]. В этом же документе указано, что маршрутизаторы **должны** иметь опцию, позволяющую запретить эту функцию, и по умолчанию функция приема и пересылки directed broadcast должна быть включена. Однако поддержка пересылки таких пакетов обеспечивает возможность организации эффективных атак на другие сети.

Смена принятого по умолчанию поведения маршрутизаторов позволит при подключении новых маршрутизаторов к сети Internet не усугублять уже существующую проблему.

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с RFC 2119.

2. Обсуждение

Разрушительные атаки на службы[2] привели к необходимости разработки системы фильтрации входящего трафика - Ingress Filtering [2]. Фильтрация на входе сейчас используется многими сетевыми операторами, а также в корпоративных сетях для предотвращения DOS-атак.

Недавние Smurf-атаки [3] были направлены против сетей, которые поддерживают directed broadcast из внешних сетей. Поддержка directed broadcast делала такие сети «усилителями» Smurf-атак.

Реализация ingress-фильтров является наилучшим решением проблемы, однако ограничение использования directed broadcast также сыграет позитивную роль.

Провайдеры и корпоративные пользователи хотят оградить свои сети от пакетов directed broadcast, приходящих из внешних сетей.

Mobile IP [4] предлагает использовать directed broadcast в мобильных узлах для динамического детектирования сетей. Хотя такая функция применяется в некоторых реализациях, польза ее совершенно не очевидна. В работе [5] предложены другие способы решения таких задач. Имеет смысл рассмотреть вопрос об отмене использования directed broadcast в Mobile IP, пока рассматривается вопрос о принятии стандарта.

3. Рекомендации

Внести в документ [1] следующие изменения:

Параграф 4.2.2.11 (d) заменить на:

> **(d) { <Network-prefix>, -1 }**
>
> Directed Broadcast – широковещательный адрес для сети с указанным префиксом. **Недопустимо** использование таких адресов в поле отправителя. Маршрутизатор может генерировать пакеты Network Directed Broadcast. Маршрутизатор **может** иметь конфигурационную опцию, разрешающую прием пакетов directed broadcast, однако эта опция **должна** быть отключена по умолчанию и, таким образом, для маршрутизаторов **недопустимо** принимать пакеты Network Directed Broadcast, пока это на задано явно конечным пользователем.

Второй абзац параграфа 5.3.5.2 заменить на:

---

[1] Directed Broadcast - широковещательный пакет, направленный в сеть с заданным префиксом (номер сети). *Прим. перев.*

[2] Denial of Service - DOS. *Прим. перев.*

Маршрутизатор **может** иметь опцию, разрешающую прием широковещательных пакетов для заданной префиксом сети (network-prefix-directed broadcast) на уровне интерфейсов и **может** иметь опцию для разрешения пересылки таких пакетов. Эти опции по умолчанию **должны** быть отключены, чтобы блокировать прием и передачу пакетов network-prefix-directed broadcast.

4. Вопросы безопасности

Задача этого документа состоит в снижении эффективности некоторых типов атак на службы (DoS).

5. Литература

[1] Baker, F., "Requirements for IP Version 4 Routers", RFC 1812[1], June 1995.

[2] Ferguson, P. and D. Senie, "Ingress Filtering", RFC 2267[2], January 1998.

[3] Публикация Craig Huegen на сайте http://www.quadrunner.com/~chuegen/smurf.txt и документ CERT http://www.cert.org/advisories/CA-98.01.smurf.html

[4] Perkins, C., "IP Mobility Support", RFC 2002, October 1996.

[5] P. Calhoun, C. Perkins, "Mobile IP Dynamic Home Address Allocation Extensions", Work in Progress[3].

6. Благодарности

Автор благодарит Брэндона Росса (Brandon Ross) из Mindspring и Гэбриела Монтенегро (Gabriel Montenegro) из Sun за их вклад в работу.

7. Адрес автора

Daniel Senie

Amaranth Networks Inc.

324 Still River Road

Bolton, MA 01740

Phone: (978) 779-6813

EMail: dts@senie.com

Перевод на русский язык

Николай Малых

nmalykh@protocols.ru

8. Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.

[1]На сайте www.protocols.ru имеется перевод этого документа на русский язык. *Прим. перев.*
[2]На сайте www.protocols.ru имеется перевод этого документа на русский язык. Там же опубликован перевод более современного варианта этого документа - RFC 2827. *Прим. перев.*
[3]Этот документ опубликован как RFC 2794 - Mobile IP Network Access Identifier Extension for IPv4. *Прим. перев.*