

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

Copyright (C) The Internet Society (1999). All Rights Reserved.

1. Введение

В требованиях к маршрутизаторам [1] указано, что эти устройства должны принимать и пересылать широковещательный трафик directed broadcast¹. 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 службы² 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 сыграло 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 не задано явно конечным пользователем.

Второй абзац параграфа 5.3.5.2 заменить на:

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

²Denial 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 заблокировать 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 1812¹, June 1995.

[2] Ferguson, P. and D. Senie, "Ingress Filtering", RFC 2267², 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 Progress³.

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

E-Mail: dts@senie.com

Перевод на русский язык

Николай Малых

nmalykh@protocols.ru

8. Полное заявление авторских прав

Copyright (C) The Internet Society (1999). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.

¹На сайте www.protocols.ru имеется перевод этого документа на русский язык. *Прим. перев.*

²На сайте www.protocols.ru имеется перевод этого документа на русский язык. Там же опубликован перевод более современного варианта этого документа - RFC 2827. *Прим. перев.*

³Этот документ опубликован как RFC 2794 - Mobile IP Network Access Identifier Extension for IPv4. *Прим. перев.*