Internet Engineering Task Force (IETF)
Request for Comments: 7999
Category: Informational
ISSN: 2070-1721

T. King
C. Dietzel
DE-CIX
J. Snijders
NTT
G. Doering
SpaceNet AG
G. Hankins
Nokia

October 2016

Группа BLACKHOLE

BLACKHOLE Community

Тезисы

В этом документе описано использование общеизвестной группы (community) BGP[1]) для создания «черных дыр» по адресам получателей в сетях IP. Эта переходная консультативная группа BGP, называемая BLACKHOLE, позволяет исходной AS[2] указать, что соседним сетям следует отбрасывать весь трафик, адресованный в указанный префикс IP.

Статус документа

Этот документ является проектом стандарта Internet (Internet Standards Track).

Документ является результатом работы IETF[3] и представляет согласованное мнение сообщества IETF. Документ был представлен на общее обозрение и одобрен для публикации IESG[4]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 документа RFC 5741.

Информация о текущем статусе данного документа, обнаруженных ошибках и способах обратной связи приведена на странице http://www.rfc-editor.org/info/rfc7999.

Оглавление

[1]Border Gateway Protocol — протокол граничного шлюза.
[2]Autonomous System — автономная система.
[3]Internet Engineering Task Force.
[4]Internet Engineering Steering Group.

1. Введение

Сетевая инфраструктура все чаще подвергается воздействию DDoS-атак. Для демпфирования воздействий таких атак в сетях IP предложена организация «черных дыр» BGP [RFC4271] с использованием разных механизмов типа описанных в [RFC3882] и [RFC5635].

DDoS-атаки, направленные на тот или иной адрес IP, могут вызывать перегрузки на каналах, ведущих в смежные с атакуемой сети. Для ограничения воздействия таких атак на легитимный трафик в сетях предложено использовать механизм, названный «черной дырой BGP» (BGP blackholing). Сеть, в которой принято решение об использовании «черной дыры», должна понимать, как будет включаться этот механизм у ее соседей. Разные сети используют разные механизмы активизации «черных дыр», включая предопределенные адреса следующего интервала для них (blackhole next-hop IP address), специальные группы BGP, отдельные сессии BGP со специальными узлами BGP и др.

Использование различных механизмов активизации «черных дыр» порождает ненужные сложности и ошибки, осложняющие работу сетевых операторов. По это причине в [RFC1997] определена специальная группа BGP.

Наличие общеизвестной группы BGP для организации «черных дыр» дополнительно упрощает работу операторов:

- реализация и мониторинг «черных дыр» упрощается за счет стандартизованного способа их активизации;
- снижается число запросов от клиентов в службу поддержки по вопросам активизации «черных дыр» благодаря использованию общеизвестных механизмов.

1.1. Урони требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с [RFC2119], если они выделены жирным шрифтом. При отсутствии такого выделения эти слова не имеют нормативного значения.

2. Группа BLACKHOLE

В этом документе описано применение новой общеизвестной переходной группы BGP BLACKHOLE.

Семантика этой группы позволяет сети интерпретировать наличие данной группы, как рекомендацию отбрасывать любой трафик, отправленный в направлении указанного префикса.

3. Рекомендации по применению

3.1. Анонсирование префиксов IP с добавлением группы BLACKHOLE

Вопрос восприятия или игнорирования группы BLACKHOLE каждый оператор решает самостоятельно. Эта группа **может** применяться во всех двухсторонних и многосторонних сценариях развертывания BGP. В двухсторонних партнерских отношениях использование группы BLACKHOLE **должно** быть согласовано между двумя сетями до того, как любая из них начнет анонсировать эту группу. В многосторонних партнерских отношениях решение о восприятии или игнорировании группы BLACKHOLE может приниматься на основе политики маршрутизации оператора. Группу **следует** игнорировать, если она получена сетью, не использующей «черных дыр».

Когда сеть подвержена DDoS-атаке, она **может** анонсировать префикс IP, включающий атакуемые адреса IP, для того, чтобы сообщить соседним сетям о том, что весь трафик, направленный в этот адрес(а) IP, следует отбрасывать. В этом случае оператору **следует** добавить в анонс группу BLACKHOLE.

Группа BLACKHOLE **может** использоваться также в качестве одного из триггеров в конфигурациях RTBH[1] [RFC5635], работающих по адресам получателей.

3.2. Локальное действие «черной дыры»

Узлу BGP, получившему анонс, помеченный группой BLACKHOLE, **следует** добавить в него группу NO_ADVERTISE или NO_EXPORT, как определено в [RFC1997], или аналогичную группу для предотвращения выхода этого префикса за пределы локальной AS. Группу для предотвращение нелокального распространения анонсов **следует** выбирать в соответствии с политикой маршрутизации оператора.

Непреднамеренное распространение более специфичных префиксов IP в соседние сети может иметь неблагоприятные последствия. Следует соблюдать передельную осторожность при целенаправленном распространении префиксов IP, помеченных группой BLACKHOLE, за пределы локального домена маршрутизации, если политика явно не указывает на такое распространение.

3.3. Восприятие префиксов IP с «черными дырами»

Сети провайдеров, использующих протокол BGP, зачастую не воспринимают анонсы префиксов IP длиннее /24 для IPv4 и /48 для IPv6 (см. параграф 6.1.3 в [RFC7454]). Однако префикс для «черной дыры» следует делать максимально длинным для предотвращения отбрасывания трафика, адресованного узлам IP, не затронутым DDoS-атакой. В предельном случае могут применяться префиксы /32 для IPv4 и /128 для IPv6, задающие один адрес.

Узлы BGP в двухсторонних партнерских отношениях с использованием группы BLACKHOLE **должны** воспринимать и обрабатывать анонсы BGP с группой BLACKHOLE только при выполнении приведенных ниже двух условий.

- Анонсируемый префикс перекрывается префиксом, который не длиннее префикса, который разрешено анонсировать соседней сети.
- Принимающая сторона согласна обрабатывать группу BLACKHOLE для данной сессии BGP.

[1] Remote Triggered Blackhole — удаленно активизируемая «черная дыра».

В топологии с сервером маршрутов или иными многосторонними партнерскими связями узлам BGP **следует** воспринимать и обрабатывать анонсы BGP при тех же условиях.

Операторы **должны** быть уверены, что методы проверки источника анонсов (типа описанного в [RFC6811]) не будут неадекватно блокировать легитимные анонсы с группой BLACKHOLE.

Группа BLACKHOLE не предназначена для использования с NLRI[1] [RFC5575] для распространения спецификаций потоков трафика.

Обработка ошибок для этой группы выполняется в соответствии с процессом, описанным в [RFC7606], где группы с некорректным форматом трактуются, как отзыв маршрута.

Операторам предлагается сохранять все обновления BGP из своей сети с группой BLACKHOLE для последующего анализа и внутреннего аудита.

4. Рекомендации для разработчиков

Без явного конфигурационного параметра, заданного оператором, элементам сети **не следует** отбрасывать трафик, направленный в адреса префикса IP, помеченного группой BLACKHOLE. Предполагается, что операторы явно указывают сетевым элементам необходимость обработки группы BLACKHOLE совместимым с его политикой маршрутизации способом.

Производители оборудования **могут** предлагать в своем языке настройки конфигурации сокращенные обозначения для общеизвестной группы BLACKHOLE. Предлагаемый полный вариант - blackhole.

5. Согласование с IANA

Агентство IANA включило группу BLACKHOLE в реестр BGP Well-known Communities

```
BLACKHOLE (= 0xFFFF029A)
```

Два младших октета дают десятичное значение 666, уже связанное сетевыми операторами с «черными дырами» BGP.

6. Вопросы безопасности

Протокол BGP не включает конкретных механизмов для предотвращения несанкционированного изменения информации пересылающими узлами. Это позволяет менять или удалять пересылаемую маршрутную информацию, а также вносить ложные данные на пересылающих агентах. Получатели маршрутных данных не имеют возможности обнаружить такие изменения. Расширение BGPsec [BGPSEC] также не позволяет решить эту проблему, поскольку даже при использовании BGPsec пересылающий агент может менять, добавлять или удалять группы BGP.

Несанкционированное добавление группы BLACKHOLE для префикса IP позволяет организовать DoS-атаку[2], объявив ложную недоступность префикса.

Для дальнейшего ограничения воздействий несанкционированных анонсов BGP с группой BLACKHOLE принимающим узлам BGP **следует** проверять с помощью строгой фильтрации (см. параграф 6.2.1.1.2 в [RFC7454]) полномочия анонсирующего префикс партнера. Если полномочия превышены партнером, анонс BGP следует отфильтровать.

Анонсы BGP с группой BLACKHOLE следует воспринимать и обрабатывать только в тех случаях, когда соседней сети разрешено анонсировать данный префикс. Метод проверки анонсов выбирается в соответствии с политикой маршрутизации оператора.

Операторам **рекомендуется** использовать для защиты своих сессий BGP проверенные на практике средства типа описанных в [RFC7454].

7. Литература

7.1. Нормативные документы

[RFC1997] Chandra, R., Traina, P., and T. Li, "BGP Communities Attribute", RFC 1997, DOI 10.17487/RFC1997, August 1996, <http://www.rfc-editor.org/info/rfc1997>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <http://www.rfc-editor.org/info/rfc4271>.

[RFC7606] Chen, E., Ed., Scudder, J., Ed., Mohapatra, P., and K. Patel, "Revised Error Handling for BGP UPDATE Messages", RFC 7606, DOI 10.17487/RFC7606, August 2015, <http://www.rfc-editor.org/info/rfc7606>.

7.2. Дополнительная литература

[BGPSEC] Lepinski, M., Ed. and K. Sriram, Ed., "BGPsec Protocol Specification", Work in Progress, draft-ietf-sidr-bgpsec-protocol-18, August 2016.

[RFC3882] Turk, D., "Configuring BGP to Block Denial-of-Service Attacks", RFC 3882, DOI 10.17487/RFC3882, September 2004, <http://www.rfc-editor.org/info/rfc3882>.

[RFC5575] Marques, P., Sheth, N., Raszuk, R., Greene, B., Mauch, J., and D. McPherson, "Dissemination of Flow Specification Rules", RFC 5575, DOI 10.17487/RFC5575, August 2009, <http://www.rfc-editor.org/info/rfc5575>.

[RFC5635] Kumari, W. and D. McPherson, "Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF)", RFC 5635, DOI 10.17487/RFC5635, August 2009, <http://www.rfc-editor.org/info/rfc5635>.

[1]Network Layer Reachability Information — информация о доступности на сетевом уровне.
[2]Denial-of-service — атака с целью вызвать «отказ служб».

[RFC6811] Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R. Austein, "BGP Prefix Origin Validation", RFC 6811, DOI 10.17487/RFC6811, January 2013, <http://www.rfc-editor.org/info/rfc6811>.

[RFC7454] Durand, J., Pepelnjak, I., and G. Doering, "BGP Operations and Security", BCP 194, RFC 7454, DOI 10.17487/RFC7454, February 2015, <http://www.rfc-editor.org/info/rfc7454>.

Благодарности

The authors would like to gratefully acknowledge many people who have contributed discussions and ideas to the development of this document. They include Petr Jiran, Yordan Kritski, Christian Seitz, Nick Hilliard, Joel Jaeggli, Christopher Morrow, Thomas Mangin, Will Hargrave, Niels Bakker, David Farmer, Jared Mauch, John Heasley, and Terry Manderson.

Адреса авторов

Thomas King

DE-CIX Management GmbH

Lichtstrasse 43i

Cologne 50825

Germany

Email: thomas.king@de-cix.net

Christoph Dietzel

DE-CIX Management GmbH

Lichtstrasse 43i

Cologne 50825

Germany

Email: christoph.dietzel@de-cix.net

Job Snijders

NTT Communications

Theodorus Majofskistraat 100

Amsterdam 1065 SZ

The Netherlands

Email: job@ntt.net

Gert Doering

SpaceNet AG

Joseph-Dollinger-Bogen 14

Munich 80807

Germany

Email: gert@space.net

Greg Hankins

Nokia

777 E. Middlefield Road

Mountain View, CA 94043

United States of America

Email: greg.hankins@nokia.com

Перевод на русский язык

Николай Малых

nmalykh@gmail.com