Internet Engineering Task Force (IETF)
Request for Comments: 8212
Updates: 4271
Category: Standards Track
ISSN: 2070-1721

J. Mauch
Akamai
J. Snijders
NTT
G. Hankins
Nokia

July 2017

Распространение маршрутов EBGP без политики

Default External BGP (EBGP) Route Propagation Behavior without Policies

Тезисы

Этот документ обновляет RFC 4271, определяя принятое по умолчанию поведение поведение узлов BGP при отсутствии политики импорта или экспорта, связанной с сессией External BGP.

Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошел открытое обсуждение и был одобрен для публикации IESG[2]. Не все одобренные IESG документы претендуют на статус Internet Standard (см. раздел 2 в RFC 7841).

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке http://www.rfc-editor.org/info/rfc8212.

Оглавление

1. Введение

Для обеспечения более стабильной работы Internet требуется решить вопросы защиты маршрутизации BGP. Утечки маршрутов [RFC7908] являются частью этой проблемы, но в нее могут вносить свой вклад дефекты программ и ошибки операторов. Данный документ обновляет [RFC4271] так, что экспорта и импорта маршрутов не происходит, пока это не будет явно разрешено в конфигурации. Это смягчает последствия упомянутой проблемы и повышает устанавливаемый по умолчанию уровень безопасности маршрутизации Internet.

Многие из развернутых узлов BGP (speaker) передают и воспринимают по умолчанию любые и все маршруты, анонсируемые между соседями BGP. Такая практика возникла на ранних этапах развития Internet, когда операторам было разрешено передавать маршрутную информацию для того, чтобы все сети могли обмениваться данными между собой. По мере роста плотности соединений в Internet риск некорректного поведения узлов BGP начал вызывать значительный риск для маршрутизации Internet в целом.

Данная спецификация предназначена для решения указанной выше проблемы за счет требования явной конфигурации правил импорта и экспорта BGP для любой внешней (EBGP) сессии с заказчиками, партнерами или границами

[1]Internet Engineering Task Force.
[2]Internet Engineering Steering Group.

конфедераций для всех разрешенных семейств адресов. За счет кодификации этого требования операторы получат преимущество в результате согласования поведения разных реализаций BGP.

Узлы BGP, соответствующие данной спецификации не используют и не передают маршрутов в сессии EBGP, пока это явно не задано в конфигурации.

2. Терминология

В [RFC4271] описана информационная база правил (PIB[1]), содержащая локальные правила, применяемые к информации из базы маршрутных данных RIB[2]. Данный документ разделяет типы правил (политики) на основе их применения.

Политика импорт — локальные правила, применяемые к информации, содержащейся в Adj-RIBs-In. Как описано в параграфе 3.2 [RFC4271], Adj-RIBs-In содержит информацию, полученную от других узлов BGP и применение этой политики дает в результате маршруты, которые будут учитываться в процессе принятия решений (Decision Process) данным узлом BGP.

Политика экспорта применяется при выборе информации, содержащейся в Adj-RIBs-Out. Как указано в параграфе 3.2 [RFC4271], Adj-RIBs-Out содержит информацию, выбранную для анонсирования другим узлам BGP.

2.1. Уровни требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они набраны заглавными буквами, как показано здесь.

3. Отличия от RFC 4271

Этот раздел обновляет [RFC4271] с целью указания конкретного поведения узлов BGP при отсутствии правил импорта или экспорта, связанных с конкретной сессией EBGP. Узел BGP **может** поддерживать конфигурационные параметры, обеспечивающие отличное от описанного ниже поведение.

Приведенный ниже абзац добавляется в параграф 9.1 «Процесс выбора маршрутов (Decision Process)» после пятого абзаца, который заканчивается словами «объединение маршрутов и снижение объема маршрутной информации»[3].

> Маршруты из Adj-RIB-In, связанные с данным партнером EBGP, **не следует** рассматривать, как желательные (eligible) в Decision Process, если к ним не была явно применена политика импорта (Import Policy).

Приведенный ниже абзац добавляется в параграф 9.1.3 «Фаза 3: Распространение маршрутов (Route Dissemination)» после третьего абзаца, который заканчивается словами «с помощью сообщения UPDATE (см. параграф 9.2)».

> Маршруты **не следует** добавлять в Adj-RIB-Out, связанную с данным партнером EBGP, если к ним не была явно применена политика экспорта.

4. Вопросы безопасности

Политика маршрутизации с разрешением по умолчанию может приводить к нежелательным эффектам типа утечки маршрутов [RFC7908], что в общем случае ведет к маршрутизации трафика по неожиданным путям. Хотя операторы могут применять мониторинг для обнаружения неожиданных потоков, для этого не существует сколь-либо общей модели. Такие правила также могут раскрывать некоторые программные дефекты или некорректные конфигурации, что может давать нежелательные технические и экономические эффекты.

Обновление [RFC4271], описанное в этом документе, предназначено для ослабления этих нежелательных эффектов. Операторы должны явно задавать политику импорта и экспорта для достижения своих целей. Естественно, что это не может обеспечить защиты от конфигурационных ошибок и злонамеренных воздействий.

Вопросы безопасности, рассмотренные в [RFC4271], и анализ уязвимостей в [RFC4272] применимы и к данному документу.

5. Согласование с IANA

Этот документ не требует каких-либо действий IANA.

6. Литература

6.1. Нормативные документы

[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>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <http://www.rfc-editor.org/info/rfc8174>.

[1] Policy Information Base.
[2] Routing Information Base — база данных о маршрутизации.
[3] Это последний абзац параграфа, п с). *Прим. перев.*

6.2. Дополнительная литература

[RFC4272] Murphy, S., "BGP Security Vulnerabilities Analysis", RFC 4272, DOI 10.17487/RFC4272, January 2006, <http://www.rfc-editor.org/info/rfc4272>.

[RFC7908] Sriram, K., Montgomery, D., McPherson, D., Osterweil, E., and B. Dickson, "Problem Definition and Classification of BGP Route Leaks", RFC 7908, DOI 10.17487/RFC7908, June 2016, <http://www.rfc-editor.org/info/rfc7908>.

Приложение A. Вопросы перехода для разработчиков BGP

Это приложение не является нормативным.

Для разработчиков создание совместимых с данным документом реализаций BGP может потребовать нескольких лет.

Понятно и подтверждено, что операторы, использующие преимущества неопределенного поведения, будут удивляться изменениям этого поведения.

A.1. Стратегия N+1 N+2

Разработчики могут использовать модель, описанную, как стратегия выпуска «N+1 и N+2». В выпуске N+1 вводятся новые конфигурационные параметры, используемые по умолчанию для индикации работы узла BGP в небезопасном режиме (ebgp insecure-mode). Кроме добавление нового параметра разработчики могут добавить выдачу оператору предупреждений о том, что в некоторых частях конфигурация не полна. В выпуске N+1 операторы такой реализации BGP будут знать, что имеется возможность настройки конфигурации и могут соответствующим образом ее сделать. В выпуске N+2 или позднее может быть введен используемый по умолчанию параметр, с обратным по отношение к N+1 смыслом.

В результате новые инсталяции выпуска N+2 будут соответствовать данному документу. Инсталяции выпуска N+1 будут следовать прежнему, незащищенному поведению, если конфигурационный параметр ebgp insecure-mode не будет изменен.

Благодарности

Авторы благодарны за рецензии, комментарии и поддержку Shane Amante, Christopher Morrow, Robert Raszuk, Greg Skinner, Adam Chappell, Sriram Kotikalapudi, Brian Dickson, Jeffrey Haas, John Heasley, Ignas Bagdonas, Donald Smith, Alvaro Retana, John Scudder b Dale Worley.

Участники

Ниже перечислены люди, которые внесли свой вклад в успешное развертывание описанного в этом документе решения.

Jakob Heitz
Cisco
Email: jheitz@cisco.com

Ondrej Filip
CZ.NIC
Email: ondrej.filip@nic.cz

Адреса авторов

Jared Mauch
Akamai Technologies
8285 Reese Lane
Ann Arbor Michigan 48103
United States of America
Email: jared@akamai.com

Job Snijders
NTT Communications
Theodorus Majofskistraat 100
Amsterdam 1065 SZ
The Netherlands
Email: job@ntt.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