Network Working Group
Request for Comments: 3882
Category: Informational

D. Turk
Bell Canada

September 2004

Настройка BGP для блокирования DoS-атак

Configuring BGP to Block Denial-of-Service Attacks

Статус документа

В этом документе содержится спецификация протокола, предложенного сообществу Internet. Документ служит приглашением к дискуссии в целях развития и совершенствования протокола. Текущее состояние стандартизации протокола вы можете узнать из документа Internet Official Protocol Standards (STD 1). Документ может распространяться без ограничений.

Авторские права

Аннотация

В этом документе обсуждается практический метод, использующий группы BGP в качестве способа удаленного запуска механизма создания «черной дыры» для определенной сети-адресата с целью блокирования атаки на службы (denial-of-service или DoS). «Черные дыры» могут создаваться для избранных маршрутизаторов, а не для всех понимающих BGP маршрутизаторов в сети. Документ также описывает метод «сливной трубы» (sinkhole tunnel), использующий группы BGP и туннели для того, чтобы направить трафик в специальный маршрутизатор (sinkhole router) для анализа пакетов.

Оглавление

1. Методы активизации «черных дыр» с помощью BGP

Существующие методы организации «черных дыр», запускаемые с помощью BGP[1], основаны на изменении адреса следующего интервала BGP[2] для сети, атакуемой через сеть iBGP. Генерируется специально подготовленный анонс iBGP от маршрутизатора, находящегося в целевой/атакуемой AS, и в этом анонсе адрес следующего интервала для маршрута в атакуемую сеть (или хост) заменяется на адрес RFC 1918 [RFC1918] (приватный адрес). Большинство маршрутизаторов в Internet (особенно краевые маршрутизаторы) имеет статические маршруты, указывающие на адреса RFC 1918 для null-интерфейса. Такие статические маршруты уводят весь трафик, адресованный в атакуемую сеть, на null-интерфейс.

Когда узел iBGP в целевой AS получает обновление iBGP, анонсируемый префикс будет добавляться в таблицу маршрутизации с адресом из какой-либо сети RFC 1918, в качестве следующего интервала (next-hop). Маршрутизатор будет пытаться преобразовать адрес RFC 1918 для следующего интервала, чтобы квалифицировать маршрут и определить интерфейс для пересылки. Этот процесс будет корректно возвращать в качестве следующего интервала null-интерфейс. В предположении, что маршрутизатор корректно настроен для направления адресованного в сеть RFC 1918 трафика в null-интерфейс, весь трафик, направленный в атакуемую сеть, будет в результате отброшен, а сама атакуемая сеть станет недоступной как для атакующего, так и для всех остальных.

Хотя такой метод позволяет экранировать сетевую инфраструктуру от атак, защищая большое число устройств, он имеет нежелательный побочный эффект, делающий атакуемую сеть недоступной для всей AS, в которой находится эта сеть. Даже если статический маршрут, указывающий на адрес RFC 1918 для null-интерфейса, задан не на всех маршрутизаторах AS, измененное значение next hop делает невозможной доставку трафика легитимным адресатам.

Обычно сетевые операторы используют такие методы в течение коротких периодов. Метод приводит к отбрасыванию трафика, адресованного в атакуемую сеть, на всех точках входа в AS. По умолчанию маршрутизаторам, отбрасывающим трафик в null-интерфейс, следует возвращать по адресу отправителя, относящемуся к исходной/атакующей AS, сообщение "ICMP unreachable".

Когда процедура достигнет этой точки[3], один из адресов источников связанного с атакой трафика захватывается путем введения устройства с таким же IP-адресом в домен BGP целевой/атакуемой AS. Устройство, захватившее адрес источника, будет собирать пакеты ICMP unreachable. Адреса отправителей в таких пакетах ICMP будут показывать,

[1]BGP-triggered black-holing.
[2]BGP next hop.
[3]Отправки сообщения ICMP unreachable. *Прим. перев.*

через какие из граничных маршрутизаторов атакуемой AS проходит трафик данной атаки. Оператор после этого может вручную заблокировать этот трафик на определенных таким путем маршрутизаторах.

2. Расширенный метод активизации «черных дыр» с помощью BGP

В этом документе описан метод, позволяющий проинструктировать выбранный набор маршрутизаторов о необходимости изменения адреса следующего интервала для определенного префикса путем использования протокола BGP. В качестве следующего интервала может использоваться null-интерфейс или интерфейс рассмотренной ниже «сливной трубы». Метод не использует списков доступа или средств ограничения трафика для трактовки связанного с атакой трафика, а также не включает изменения адреса следующего интервала для всей сети. Значение next hop будет изменяться только на выбранных маршрутизаторах вспомогательной группы BGP в целевой/атакуемой AS.

Для подготовки сети к использованию этого метода оператору нужно определить уникальную группу (community) для каждого граничного маршрутизатора AS, который может использоваться для доставки в сеть связанного с атакой трафика. Например, сеть с номером автономной системы BGP 65001 имеет два граничных маршрутизатора R1 и R2. Группа 65001:1 создается для идентификации маршрутизатора R1, группа 65001:2 – для R2, а группа 65001:666 используется для идентификации обоих маршрутизаторов.

После определения групп BGP маршрутизаторы R1 и R2 нужно настроить, как показано ниже.

1. Создать статический маршрут, указывающий на сеть RFC 1918 для null-интерфейса.
2. Создать список управления доступом для AS-Path, которому соответствует анонс локального префикса BGP.
3. Создать список управления доступом для BGP community, которому соответствует значение группы, выделенное оператором для соответствующего маршрутизатора (например, 65001:1 для маршрутизатора R1).
4. Создать список управления доступом для BGP community, которому соответствует значение группы, выделенное оператором для всех маршрутизаторов (т. е., 65001:666 для R1 и R2).
5. В BGP следует применять политику импорта маршрутов iBGP к получаемым анонсам iBGP для реализации показанной ниже логики (должны выполняться все приведенные ниже условия - AND)
   a. Правило, разрешающее маршруты, соответствующие перечисленным ниже критериям, и вносящее указанные изменения:
      i. проверить соответствие группе (community) указанной для данного маршрутизатора (т. е., 65001:1 для R1);
      ii. проверить соответствие AS-Path для локально сгенерированных анонсов BGP;
      iii. установить для BGP next hop сеть RFC 1918;
      iv. заменить BGP community на общеизвестную группу no-advertise (не анонсировать).
   b. Правило, разрешающее маршруты, соответствующие перечисленным ниже критериям и вносящее указанные изменения.
      i. проверить соответствие группе, включающей все маршруты (т. е., 65001:666);
      ii. проверить соответствие AS-Path для локально сгенерированных анонсов BGP;
      iii. установить для BGP next hop сеть RFC 1918;
      iv. заменить BGP community на общеизвестную группу no-advertise.

После того, как заданы правила для R1 и R2, сетевой оператор может в случае атаки анонсировать целевую сеть, которая может содержать маршруты к одному или множеству хостов (/32) в iBGP атакуемой AS. Анонсы должны содержать значение группы, связанное с маршрутизатором или маршрутизаторами, через которые проходит атака, в дополнение к общепринятой группе no-export. Использование групп BGP сохраняет исходный адрес next hop целевой сети на всех маршрутизаторах, где не присутствует специальная маршрутная политика. iBGP будет тогда передавать анонс префиксов во все маршрутизаторы атакуемой AS. Все маршрутизаторы в этой AS, за исключением тех, которые соответствуют указанной в префиксе группе, будут устанавливать маршрут с легитимным значением next hop. Маршрутизаторы, соответствующие группе, также будут устанавливать в своей таблице маршрут, но значение next hop будет указывать на сеть RFC 1918 и далее на null-интерфейс, как при настройке политики для маршрутов и рекурсивном просмотре маршрутов. Поиск соответствия среди локально анонсируемых сетей производится для того, чтобы ни один из партнеров eBGP не мог ошибочно воспользоваться этим анонсом и направить какую-либо сеть в null-интерфейс. Рекомендуется создавать «черную дыру» для атакуемых хостов, но не для всего блока, к которому они относятся, чтобы оказывать минимальное воздействие на работу атакуемой сети.

Описанный метод блокирует пересылку трафика легитимным адресатам на маршрутизаторах, которые были идентифицированы, как транзитные, для связанного с атакой трафика и имеют маршруты, соответствующие значению группы, связанному с анонсом. Весь остальной трафик будет нормально пересылаться легитимным адресатам, что позволяет минимизировать негативное влияние на работу атакуемой сети.

3. «Сливные» туннели

Метод Enhanced BGP-Triggered Black-holing может потребовать просмотра связанного с атакой трафика для его дальнейшего анализа. Это требование усложняет задачу. Обычно при использовании интерфейсов в широковещательные среды операторы для анализа сетевого трафика подключают анализатор к порту коммутатора. Другим вариантом будет анонсирование сетевого префикса, который включает адрес атакуемого хоста в iBGP и заменяет значение next hop адресом «сливного устройства[1]», способного сохранять трафик для анализа. Этот метод приводит к недоступности служб, обеспечиваемых атакуемыми адресами IP. Внешний (Inter-AS) трафик будет попадать в «слив» вместе с внутренним (Intra-AS). Анализ на уровне пакетов включает перенаправление трафика

[1]Sinkhole device.

хоста-адресата в анализатор или маршрутизатор. В результате, если в этот поток входит и легитимный трафик, последний просто не попадет к адресату. В конечном итоге для легитимного трафика атакуемый хост становится недоступным.

Более эффективным вариантом будет использование «сливного туннеля[1]». Такой туннель организуется на всех возможных точках входа, через которые связанный с атакой трафик может передаваться в атакуемую AS. Используя группы BGP, можно перенаправить связанный с атакой трафик на специальный путь (туннель), где анализатор протоколов может собирать пакеты для последующего их анализа. После анализа трафика он выходит из туннеля и нормально маршрутизируется к хосту-адресату. Иными словами, трафик будет проходить через сеть к анализатору без изменения значений next hop для атакуемой сети. Все маршрутизаторы в домене iBGP атакуемой AS будут иметь корректный адрес next hop и только маршрутизаторы в точках входа будут иметь измененный адрес следующего интервала.

В сети устанавливается «сливной» маршрутизатор с подключенным к нему анализатором протоколов. Этот маршрутизатор настраивается на участие в IGP и iBGP атакуемой AS. Далее создаются туннели (например, с использованием MPLS TE[2]) от всех маршрутизаторов, через которые может входить связанный с атакой внешний трафик к «сливному» маршрутизатору. При возникновении атаки на хост или сеть передается специально подготовленный анонс iBGP с адресом атакуемого хоста или сети и подходящим адресом next hop, который обеспечит доставку трафика хосту или сети. Этот анонс будет также включать группу (community), которой соответствует набор граничных маршрутизаторов, используемых для передачи в сеть связанного с атакой трафика, как описано в параграфе 2. Новому значению next hop, заданному в правилах всех граничных маршрутизаторов, следует указывать IP-адрес «слива». Этот адрес относится к сети с маской /30, выделенной для «сливного» туннеля, соединяющего граничный маршрутизатор со «сливным».

Маршрутизаторы, которые не соответствуют группе, будут работать как обычно. Отсутствие соответствия в этих маршрутизаторах будет гарантировать, что специальное правило замены значения next hop не будет применено. Трафик, входящий в сеть через граничные маршрутизаторы, которые не соответствуют группе, будет проходить к легитимным адресатам через обычные интерфейсы этих маршрутизаторов. Может также потребоваться передача направленного в туннель трафика адресатам после его анализа. В этом случае создается используемый по умолчанию маршрут к любому интерфейсу, подключенному и сконфигурированному для сети iBGP. Этот маршрут будет также включать физический интерфейс, использованный для создания туннеля. Поскольку адрес next hop не меняется на «сливном» устройстве, попавший в это устройство трафик из туннеля будет передаваться обратно в сеть, благодаря наличию принятого по умолчанию маршрута. Протоколы маршрутизации после этого будут предпринимать попытки корректной маршрутизации трафика адресату (в атакуемую сеть).

Ясно, что этот метод можно использовать не только для анализа трафика, связанного с атаками. Легитимный трафик также можно перенаправить в туннель и вернуть в сеть после анализа без изменения схемы адресации next hop в сети iBGP.

Методы MPLS TE с их широкими возможностями весьма удобны для перенаправления трафика в «сливное» устройство. К связанному с атакой трафику можно применить возможности управления QoS, что позволит сохранить ресурсы для передачи легитимного трафика.

Для изменения адреса next hop на граничном маршрутизаторе подсеть RFC 1918 статически маршрутизируется на интерфейс туннеля. Примером такого маршрута может быть

```
ip route 192.168.0.12 255.255.255.255 Tunnel0
```

Установка в качестве next hop для IP-адреса получателя значения 192.168.0.12/32 будет приводить к направлению трафика в туннель.

Трафик принимается «сливным» интерфейсом через туннель TE. Следовательно, могут использоваться три метода, а именно – правила ограничения скорости, правила QoS и списки управления доступом. Эти правила позволяют ограничить скорость передачи трафика, связанного с атакой, или отбросить этот трафик совсем. Процесс будет полностью выполнен на интерфейсе “сливного» устройства. Другим полезным применением «сливных» маршрутизаторов является направление трафика в туннели при наличии принятого по умолчанию маршрута, который будет пересылать трафик на интерфейс Ethernet. Этот интерфейс подключается к сети iBGP и гарантирует корректную доставку трафика, который при этом остается доступным анализатору для сбора пакетов и последующего анализа связанного с атакой трафика.

Этот метод весьма полезен в тех случаях, когда нет возможности использовать список контроля доступа или ограничение скорости на маршрутизаторе BGP или последнем маршрутизаторе перед атакуемым хостом в силу аппаратных или программных ограничений. Вместо замены интерфейсов в точке входа связанного с атакой трафика последний просто «сливается» в туннель и обрабатываться «сливным» устройством. Эксплуатационные издержки могут быть минимальными, если «сливной» маршрутизатор является достаточно мощным устройством.

4. Вопросы безопасности

Прежде, чем реализовать описанный метод на практике, следует попрактиковаться в контроле партнерских точек eBGP. Пользователи eBGP могут направить в «черную дыру» трафик для той или иной сети, используя группы Blackhole. Для избавления от риска не следует пренебрегать проверкой соответствия для локально генерируемых анонсов BGP с использованием специальной политики маршрутизации.

5. Благодарности

Автор документа благодарит разработчиков механизма удаленного включения «черных дыр» и разработчиков метода backscatter для сбора backscatter-трафика. Автор также благодарен всем членам отдела IP Engineering за помощь, оказанную в проверке функциональности описанного метода.

[1]Sinkhole tunnel.
[2]Traffic Engineering – организация трафика.

6. Литература

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

7. Адрес автора

Doughan Turk

Bell Canada

100 Wynford Drive

EMail: doughan.turk@bell.ca

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

8. Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечивается Internet Society.