Network Working Group
Request for Comments: 3704
Updates: 2827
BCP: 84
Category: Best Current Practice

F. Baker
Cisco Systems
P. Savola
CSC/FUNET

March 2004

Фильтрация на входе в многодомные сети

Ingress Filtering for Multihomed Networks

Статус документа

Этот документ относится к категории обмена опытом (Best Current Practice) в сообществе Internet и служит приглашением к дискуссии и внесению предложений в целях дальнейшего развития. Документ может распространяться свободно.

Аннотация

Документ BCP 38 (RFC 2827) был разработан с целью ограничения возможностей организации распределенных атак на службы (DDoS[1]) за счёт фильтрации трафика с подменными адресами на входе в сеть и оказания помощи в трассировке источников такого трафика. Кроме защиты Internet от таких атак реализующие это решение сети также обеспечивают для себя защиту от этих и других атак типа обманного доступа к системам управления сетевым оборудованием. Возможны ситуации (например, многодомные сети), когда будут возникать проблемы. В данном документе описаны современные механизмы фильтрации на входе и рассмотрены основные проблемы, связанные с такой фильтрацией (в частности, с учётом многодомных подключений). Документ служит обновлением RFC 2827.

Оглавление

1. Введение....1
2. Различные способы фильтрации на входе....2
2.1. Входные списки доступа....2
2.2. Строгая проверка по обратному пути....2
2.3. Проверка по доступности обратного пути....3
2.4. Проверка по наличию маршрута....3
2.5. Проверка по наличию маршрута, кроме маршрута по умолчанию....3
3. Разъяснения о применимости входной фильтрации....4
3.1. Многоуровневая фильтрация....4
3.2. Входная фильтрация для защиты инфраструктуры....4
3.3. Входная фильтрация на партнерских соединениях....4
4. Решения для входной фильтрации в многодомных сетях....4
4.1. Не применяйте Loose RPF без необходимости....5
4.2. Убедитесь в полноте входных фильтров каждого ISP....5
4.3. Передавайте трафик, использующий префикс ISP, только этому ISP....5
5. Вопросы безопасности....5
6. Заключение и планы на будущее....6
7. Благодарности....6
8. Литература....6
8.1. Нормативные документы....6
8.2. Дополнительная литература....6
9. Адреса авторов....7
10. Полное заявление авторских прав....7

1. Введение

Документ BCP 38 (RFC 2827) [1] был разработан с целью ограничения возможностей организации распределенных атак на службы (DDoS) за счёт фильтрации трафика с подменными адресами на входе в сеть и оказания помощи в трассировке источников такого трафика. Кроме защиты Internet от таких атак реализующие это решение сети также обеспечивают для себя защиту от этих и других атак типа обманного доступа к системам управления сетевым оборудованием. Возможны ситуации (например, многодомные сети), когда будут возникать проблемы. В данном документе описаны современные механизмы фильтрации на входе, рассмотрены основные проблемы, связанные с такой фильтрацией (в частности, с учётом многодомных подключений).

RFC 2827 рекомендует сервис-провайдерам (ISP[2]) контролировать трафик своих заказчиков, отбрасывая на входе в сеть пакеты, отправленные с адресов, которые не могут легитимно использоваться в сети заказчика. Фильтрация включает трафик (но никоим образом не ограничивается им) с так называемыми «марсианскими адресами» (Martian Address), которые зарезервированы в [3] (включая все адреса из блоков 0.0.0.0/8, 10.0.0.0/8, 127.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 224.0.0.0/4, 240.0.0.0/4).

[1]Distributed denial of service attack.
[2]Internet Service Provider. *Прим. перев.*

Потребность во входной фильтрации обусловлена тем, что при распределенных DoS-атаках зачастую в качестве подставных адресов отправителей используются случайные адреса. В некоторых случаях такие случайные адреса попадают в блок адресов атакуемой сети и кроме атаки на один или множество хостов этой сети вызывают со стороны этих хостов «атаки» других хостов данной сети сообщениями ICMP или иным трафиком откликов. В таких случаях атакуемые сайты могут защитить самих себя с помощью подходящей фильтрации, проверяя, не указаны ли адреса из данной сети в поле отправителя пакетов, приходящих из Internet. В других атаках в качестве адресов отправителей используются случайные 32-битовые значения для осложнения поиска источника атаки. Если трафик, исходящий из оконечной сети и входящий в ISP ограничивать путём проверки принадлежности адресов отправителей к данной оконечной сети, возможности организации таких атак можно существенно снизить, а источник атак будет проще отследить (по крайней мере, определить сеть злоумышленников).

Этот документ адресован ISP и операторам оконечных сетей, которые 1) хотят расширить свои знания в области фильтрации на входе или 2) уже используют входную фильтрацию, но хотят расширить её применение, избежав ошибок при организации фильтров в многодомных/асимметричных средах.

В разделе 2 описано несколько способов реализации входных фильтров, проверенных в типичных средах. В разделе 3 приведены некоторые разъяснения в части применимости фильтрации на входе. В разделе 4 приведён подробный анализ фильтрации на входе в многодомные сети, а раздел 5 посвящён перспективам работ в этом направлении.

2. Различные способы фильтрации на входе

Этот раздел содержит вводные описания различных методов входной фильтрации, используемых на практике к моменту написания этого документа. Механизмы описаны и проанализированы для общего случая, а специфические для многодомных систем вопросы рассматриваются в разделе 4.

Имеется по крайней мере пять вариантов реализации RFC 2827, различающихся по уровню влияния, включая (даны общепринятые названия):

- Ingress Access Lists - входные списки доступа;
- Strict Reverse Path Forwarding - строгая
- Feasible Path Reverse Path Forwarding - мягкая
- Loose Reverse Path Forwarding - мягкая
- Loose Reverse Path Forwarding ignoring default routes - мягкая с игнорированием принятых по умолчанию маршрутов

Возможны и другие механизмы, а также есть множество которые могли быть полезны после дополнительного изучения, спецификации, реализации и развёртывания. Эти методы перечислены в разделе, но их рассмотрение выходит за рамки этого документа.

2.1. Входные списки доступа

Ingress Access List представляет собой фильтр, который проверяет адрес отправителя в каждом сообщении, принятом сетевым интерфейсом, сравнивая его со списком разрешённых префиксов и отбрасывая не соответствующие списку пакеты. Хотя это не единственный способ фильтрации на входе, он является одним из предложенных в RFC 2827 [1] и, в некотором смысле, наиболее определенным.

Обычно списки Ingress Access List поддерживаются вручную и это может служить причиной некоторых проблем (например, не обновленный вовремя список префиксов ISP, может приводить к потере части пакетов).

Эта проблема присуща не только входным спискам доступа - она может возникать при любом методе фильтрации на входе, если фильтры заданы не полностью. Однако при использовании Ingress Access Lists поддержка фильтров более сложна по сравнению с другими методами и использование устаревшего списка может приводить к потере легитимного трафика.

2.2. Строгая проверка по обратному пути

Strict RPF[1] обеспечивает простой способ реализации входных фильтров. Концептуально этот метод идентичен использованию списков доступа, но эти списки формируются динамически. Метод также позволяет избежать дублирования конфигураций (например, поддержки фильтров для статических маршрутов или префиксов BGP и списков доступа на интерфейсах). Процедура фильтрации заключается в поиске адреса отправителя по базе FIB[2] - пакет считается приемлемым, если он был получен интерфейсом, который используется для пересылки пакетов по адресу отправителя.

Strict RPF является разумным решением для любых краевых сетей и значительно превосходит Ingress Access List для случаев, когда сеть анонсирует множество префиксов, используя BGP. Этот метод служит для создания простых, быстрых и недорогих динамических фильтров.

Однако этому методу присущи свои проблемы. Во-первых, этот метод применим только в тех местах, где маршрутизация симметрична (дейтаграммы IP и отклики на них детерминировано проходят по одному пути). Для краевых сетей такая ситуация является, подключённых к ISP, такая ситуация достаточно типична, но в соединениях между ISP обычно возникает асимметричная маршрутизация (hot potato). Кроме того, если для передачи префиксов применяется BGP и некоторые легитимные префиксы не анонсируются или не воспринимаются в соответствии с политикой ISP, такая фильтрация будет приводить к эффектам, аналогичным тем, что возникают при неполных списках доступа - часть легитимного трафика будет фильтроваться по причине отсутствия маршрута в фильтруемой базе FIB.

Есть методы повышения эффективности Strict RPF для случаев асимметричной маршрутизации и многодомных систем, рассчитанные, прежде всего, на BGP, но в той или иной степени применимы и с другими протоколами

[1] Strict Reverse Path Forwarding - строгая проверка обратного пути.
[2] Forwarding Information Base - база данных о пересылке.

маршрутизации. ISP задаёт лучшую метрику (которая не распространяется за пределы маршрутизатора) с помощью фирменного «веса» или «протокольной дальности», чтобы отдать предпочтение полученным напрямую маршрутам. При использовании BGP и достаточных ресурсах установку предпочтений можно автоматизировать, используя группы BGP [2]. Это позволяет сделать маршрут лучшим в FIB даже в тех случаях, когда реально используется только основное соединение и обычно через интерфейс пакеты даже не передаются. Этот метод предполагает отсутствие фильтрации Strict RPF между основным и вторичным краевыми маршрутизаторами (для многодомных подключений к разным ISP это допущение может быть неверным).

2.3. Проверка по доступности обратного пути

Feasible RPF[1] является расширением Strict RPF. Адреса отправителей по-прежнему отыскиваются в FIB (или эквивалентной таблице RPF), но вместо использования одного лучшего маршрута добавляются дополнительные пути (если они есть), которые также принимаются во внимание. Список маршрутов создаётся с использованием зависящих от протокола маршрутизации методов, например, путём включения всех или N (части) доступных путей BGP из таблицы RIB[2]. Иногда такой метод используют, как часть реализации Strict RPF.

В случае асимметричной маршрутизации и/или многодомного подключения краевой сети, такой подход обеспечивает сравнительно простое решение проблем, присущих Strict RPF.

Важно понимать контекст, в котором работает Feasible RPF. Метод полагается на согласованные анонсы маршрутов (т.е., одни и те же префиксы через все пути), распространяемые всеми маршрутизаторами, применяющими проверки Feasible RPF. Например, этот метод может не работать в случае, когда вторичный ISP не распространяет анонс BGP первичному ISP (в результате использования route-map или других правил для маршрутов). Результаты отказов похожи на описанные в конце предыдущего параграфа для «улучшенного» варианта Strict RPF.

В общем случае фильтрация анонсов будет приводить к фильтрации соответствующих пакетов.

Отметим в заключение, что корректно заданные фильтры Feasible RPF являются очень мощным средством для входной фильтрации при асимметричных маршрутах, но важно понимать их функционирование и применимость.

2.4. Проверка по наличию маршрута

Метод Loose RPF[3] алгоритмически похож на Strict RPF, но отличается тем, проверяется только наличие маршрута (даже маршрута по умолчанию, если он подходит). Практически этот метод можно трактовать, как «проверку наличия маршрута» (термин Loose RPF не вполне корректен, поскольку в первую очередь проверяется отсутствие «обратного пути»).

Неочевидное преимущество Loose RPF возникает в случаях асимметричной маршрутизации - пакеты отбрасываются, если маршрута к их отправителю нет совсем (например, «марсианский адрес» или немаршрутизируемый в данный момент адрес), но не отбрасываются при наличии какого-либо маршрута.

Однако методу Loose RPF присущи и проблемы. Поскольку этот механизм не принимает во внимание направление маршрута, он теряет способность отсекать нелегитимный трафик из той или иной сети и в большинстве случаев механизм становится бесполезным для использования в качестве средства входной фильтрации.

Кроме того, многие ISP поддерживают с теми или иными целями (например, сбор нелегитимного трафика в специальные «ловушки» (Honey Pot) или отбрасывание любого трафика, для которого нет иного пути), а небольшие ISP могут покупать у более крупных транзит трафика и использовать маршрут к большому провайдеру по умолчанию. По крайней мере часть реализаций Loose RPF проверяет, куда ведёт маршрут по умолчанию. Если этот маршрут ведёт на интерфейс, где механизм Loose RPF разрешён, все пакеты с этого интерфейса принимаются. Если не маршрут ведёт в «никуда» или на какой-то другой интерфейс, пакеты с фиктивными адресами будут отбрасываться на интерфейсе Loose RPF даже при наличии используемого по умолчанию маршрута. Если такая усовершенствованная проверка не выполняется, наличие маршрута по умолчанию делает фильтрацию Loose RPF полностью бесполезной.

Loose RPF будет работать достаточно хорошо у ISP, фильтрующих трафик от вышестоящего провайдера для отбрасывания пакетов с «марсианскими» или немаршрутизируемыми адресами.

Если другие варианты фильтрации не подходят, Loose RPF можно применить в качестве средства проверки соответствия контракту - другая сеть заранее подтверждает, что она обеспечивает приемлемую фильтрацию на входе, так что данной сети достаточно лишь проверять этот факт и реагировать при обнаружении каких-либо пакетов, не соответствующих контракту. Естественно, что этот механизм будет лишь обнаруживать пакеты с «марсианскими» и другими немаршрутизируемыми адресами, не реагируя на пакеты с адресами из других пространств.

2.5. Проверка по наличию маршрута, кроме маршрута по умолчанию

Пятый метод фильтрации можно назвать Loose RPF с игнорированием маршрута по умолчанию (т. е., проверкой наличия явного маршрута). В этой модели маршрутизатор ищет адрес отправителя в таблице маршрутизации и пропускает соответствующие пакеты. Однако при просмотре таблицы используемый по умолчанию маршрут не принимается во внимание. Следовательно, этот метод лучше всего подходит для сетей, где маршрут по умолчанию используется только для захвата трафика с фиктивными адресами отправителей, а для легитимного трафика имеется список (возможно, полный) явных маршрутов к отправителям.

Подобно Loose RPF, этот метод подходит для систем с асимметричной маршрутизацией (например, соединения между ISP). Однако, как и Loose RPF, этот метод не принимает во внимание направление, что ведёт к невозможности идентифицировать трафик, легитимно приходящий из той или иной сети.

[1] Feasible Path Reverse Path Forwarding - доступен обратный путь.
[2] Routing Information Base - база маршрутной информации.
[3] Loose Reverse Path Forwarding - проверка наличия маршрута для обратного пути.

3. Разъяснения о применимости входной фильтрации

Не очевидно, что применение входной фильтрации не ограничивается лишь интерфейсами «последней мили» между ISP и конечным пользователем. Будет правильным решением (и рекомендуется) использовать входную фильтрацию также на периметре ISP (где это подходит), на маршрутизаторах, соединяющих ЛВС с корпоративной сетью и т. п. - это обеспечит глубоко эшелонированную защиту.

3.1. Многоуровневая фильтрация

Широкое применение входной фильтрации обуславливает итерационное решение задачи. Входная фильтрация работает везде, где она применяется, а не только между двумя сторонами. Т. е., если пользователь заключил соглашение о входной фильтрации со своим ISP, он должен иметь гарантии того, что аналогичное соглашение заключено между этим ISP с сервис-провайдером восходящего направления и партнерскими ISP. Аналогичная ситуация наблюдается и далее в восходящем направлении.

Следовательно, модели с ручной настройкой фильтров, не обеспечивающие автоматического распространения информации между участниками, снижают уровень эффективности многоуровневой системы входной фильтрации и даже могут сделать её бессмысленной.

3.2. Входная фильтрация для защиты инфраструктуры

Другие особенности, связанные с более широким развёртыванием входной фильтрации, могут быть не очевидными. Маршрутизаторы и другие компоненты архитектуры ISP уязвимы для разных типов атак. Снижение уровня угроз обычно обеспечивается ограничением доступа к системам.

Однако, пока входная фильтрация (или хотя бы часть её) не внедрена на каждом граничном маршрутизаторе (в сторону заказчиков, партнёров и провайдеров) с блокировкой внешних пакетов, содержащих локальные адреса в поле отправителя, у атакующих сохраняются шансы преодолеть защиту инфраструктуры.

Следовательно, развёртывая фильтрацию на входе, вы не только обеспечиваете помощь Internet в целом, но и организуете защиту от некоторых классов атак для своей инфраструктуры.

3.3. Входная фильтрация на партнерских соединениях

Входная фильтрация на партнерских соединениях между ISP или оконечными сетями не имеет существенных отличий от типичной фильтрации на входе в восходящего или нисходящего направления.

Однако следует отметить, что в смешанных ситуациях с восходящими/нисходящими и партнерскими соединениями свойства разных каналов могут различаться (например, в части ограничений, доверия, жизнестойкости механизмов входной фильтрации и т.п.). В наиболее типичном случае простое применение механизма входной фильтрации (например, Strict RPF) будет работать достаточно хорошо, если маршрутизация между партнёрами достаточно симметрична. Это может быть полезно даже для фильтрации по адресам отправителей на восходящем соединении, проходящем через канал к партнёру (предполагается использование в восходящем направление чего-нибудь типа Strict RPF), однако эта ситуация более сложна и выходит за рамки документа (см. раздел 6).

4. Решения для входной фильтрации в многодомных сетях

Сначала следует выяснить причины многодомности сайта. Например, оконечная сеть может

- использовать двух ISP для резервирования своего подключения к Internet в целях повышения отказоустойчивости;
- выбирать ISP, обеспечивающего в данный момент более быстрый сервис TCP;
- иметь потребность в точках доступа в Internet в тех местах, где нет ISP;
- менять ISP (многодомность является временной).

Можно предложит множество вариантов решения проблем, связанных с ограничениями входной фильтрации в многодомных сетях, включая:

1. отказ от многодомности;
2. отказ от входной фильтрации;
3. согласие с неполным обслуживанием;
4. ослабить на некоторых интерфейсах входную фильтрацию, используя подходящую форму Loose RPF, как описано в параграфе 4.1;
5. обеспечить с помощью BGP или контракта полноту входной фильтрации у каждого ISP, как описано в параграфе 4.2;
6. обеспечить, чтобы оконечная сеть только доставляла трафик своим ISP, которые будут осуществлять входную фильтрацию, как описано в параграфе 4.3.

Первые три варианта указаны лишь для полноты, поскольку они не обеспечивают реального решения задачи. Три оставшихся варианта более подробно рассмотрены ниже.

Варианты 4 и 5 должны быть реализованы и у вышестоящих ISP, как описано в параграфе 3.1.

Далее будут рассмотрены практические способы преодоления побочных эффектов фильтрации на входе.

4.1. Не применяйте Loose RPF без необходимости

Когда асимметрия в маршрутизации предпочтительна или неизбежна, могут возникать сложности с использованием механизмов типа Strict RPF, которым нужны симметричные пути. Во многих случаях использование методов, описанных в конце параграфа 2.2 или механизма Feasible RPF позволяет обеспечить полноту входной фильтрации, подобно описанному ниже. Если же это не удаётся, реальными вариантами будут лишь отказ от входной фильтрации, использование создаваемых вручную списков доступа (возможно, дополненных другими механизмами) или применение той или иной формы проверки Loose RPF.

Отказ от входной фильтрации с переносом её в сети нисходящего направления не представляется разумным решением. Однако, особенно для очень больших сетей с сотнями и тысячами префиксов, поддержка списков доступа вручную может оказаться чересчур трудоёмкой.

Использование Loose RPF на границе между оконечной сетью и ISP не представляется разумным решением, поскольку в этом случае утрачивается направление проверки. Это является аргументом в пользу полной фильтрации в сети восходящего направления или обеспечением в сети нисходящего направления того, что отвергаемые вышестоящей сетью пакеты никогда не будут достигать её.

Следовательно, применение Loose RPF не рекомендуется за исключением случаев, когда оно служит для фильтрации «марсианских» и других немаршрутизируемых адресов.

4.2. Убедитесь в полноте входных фильтров каждого ISP

Для оконечной сети, где множественные подключения служат для обеспечения надёжности или изменения маршрутизации в зависимости от поведения ISP, простейшим решением будет убедиться в том, что их ISP фактически передают адреса сети в маршрутизацию. Для этого оконечной сети зачастую требуется не связанный с провайдерами адресный префикс и обмен маршрутами с ISP по протоколу BGP, чтобы обеспечить передачу префикса в восходящем направлении основным транзитным ISP. Это требует от оконечной сети соответствия требованиям по размеру и техническому уровню специалистов, предъявляемым региональным регистратором (RIR) для выделения независимого префикса и номера автономной системы.

Упростить процесс обеспечения полноты входной фильтрации у ISP можно множеством способов. Методы Feasible RPF и Strict RPF с расширениями достаточно хорошо работают для многодомных подключений или асимметричной маршрутизации между ISP и оконечной сетью.

Если протоколы маршрутизации не применяются, а информация берётся из баз данных типа Radius, TACACS или Diameter, входную фильтрацию можно обеспечить и актуализировать при использовании Strict RPF или Ingress Access List на основании информации из таких базе данных.

4.3. Передавайте трафик, использующий префикс ISP, только этому ISP

Для небольших оконечных сетей, использующих адресное пространство ISP, которые применяют входные фильтры (им следует делать это), третьим вариантом является маршрутизация трафика, исходящего с адресов того или иного провайдера только данном ISP.

Эта процедура несложна, но требует аккуратного планирования и настройки. Для обеспечения отказоустойчивости оконечная сеть может выбрать подключение к каждому из своих ISP через две или более точки POP[1], чтобы при возникновении проблем в одной POP или линии можно было использовать другое подключение к тому же ISP. Можно также организовать набор туннелей вместо множества подключений к одному ISP [4][5]. В этом случае граничные маршрутизаторы настраиваются так, чтобы сначала проверялся адрес отправителя в пакетах, предназначенных для ISP, а после этого пакет направлялся на туннельный интерфейс в направлении данного ISP.

При полной реализации сценария с выбором выходного маршрутизатора оконечной сети для каждого используемого в сети префикса, пакеты из другого префикса могут полностью отбрасываться вместо их передачи ISP.

5. Вопросы безопасности

Входная фильтрация обычно служит для того, чтобы убедиться в том, что полученный на сетевом интерфейсе трафик легитимно поступил от компьютера, который относится к сети, доступной через данный интерфейс.

Чем ближе к реальному источнику пакета выполняется входная фильтрация, тем более она эффективна. Было бы хорошо, если бы первый маршрутизатор на пути пакета гарантировал, что приходящий из соседней по отношению к нему оконечной сети трафик использует корректные адреса отправителей. Следующий маршрутизатор тогда может проверять лишь возможность наличия систем в адресном пространстве с указанным префиксом. Следовательно, входную фильтрацию нужно выполнять на множестве уровней с различной гранулярностью.

Следует принимать во внимание, что хотя одной из целей входной фильтрации является отслеживание источников атак, те не менее нет возможности знать будет ли с её помощью отфильтрован трафик конкретного злоумышленника, находящегося где-то в Internet. Следовательно, можно лишь определить является ли адрес отправителя подставным. В любом случае эта информация полезна (например, для контакта с возможным источником атаки) и представляет ценность, тем более, что использование фильтрации на входе продолжает расширяться.

Поэтому каждому администратору домена следует постараться обеспечить достаточный уровень входной фильтрации на границах своего домена.

Защитные свойства и применимость различных типов входной фильтрации достаточно сильно различаются.

- Списки Ingress Access List обычно требуют поддержки вручную, но при правильной настройке являются очень мощным средством. Такие списки хорошо подходят на границе между оконечной сетью и ISP, когда конфигурация достаточно статична и не используется вариант Strict RPF, между сетями ISP, если число используемых ими префиксов невелико, а также в качестве дополнительного уровня защиты.

[1] Points of Presence - точка присутствия.

- Strict RPF обеспечивает очень просто и надёжный способ реализации входных фильтров. Обычно этот метод применяется между оконечной сетью и ISP. Во многих случаях простые фильтры Strict RPF могут быть усилены дополнительными процедурами для асимметричной картины трафика или методом Feasible RPF, если имеется множество путей.

- Feasible Path RPF работает, как расширение Strict RPF. Этот метод работает во всех случаях, где применим метод Strict RPF, но особенно подходит для многодомных систем и случаев с асимметрией трафика. Однако следует помнить, что Feasible RPF предполагает согласованное создание и распространение маршрутной информации. Особенно важно принимать это во внимание для случаев, когда анонсы префиксов проходят через «третьи руки».

- Loose RPF отфильтровывает немаршрутизируемые префиксы типа «марсианских» адресов. Этот метод можно применять на восходящих интерфейсах для снижения интенсивности DoS-атак с немаршрутизируемыми адресами отправителей. На нисходящих интерфейсах этот метод может применяться лишь для проверки соответствия контрактам о применении фильтрации на входе.

При сравнении возможностей разных методов фильтрации на входе следует рассмотреть защитные свойства наиболее мягкого варианта до его применения на практике. Особенно важно это в случаях применения фильтров ISP в направлении оконечной сети, поскольку здесь может существовать множество причин для отказа от более жёсткой фильтрации.

6. Заключение и планы на будущее

В этом документе описаны методы входной фильтрации в целом и варианты для многодомных сетей, в частности.

Для ISP использование входной фильтрации важно в плане предотвращения использования обманных адресов отправителей с целью блокировки DoS-атак и отслеживания их источников, а также для защиты своей инфраструктуры. В этом документе описаны механизмы, которые позволяют решить эти задачи, а также указаны недостатки отдельных механизмов.

В качестве резюме отметим, что:

- входную фильтрацию всегда следует использовать между ISP и оконечными сетями с одним каналом;

- метод Feasible RPF или Strict RPF почти всегда применим между ISP и многодомными оконечными сетями;

- как ISP, так и оконечным сетям следует проверять, что их собственные адреса не указаны в поле отправителя приходящих извне пакетов;

- некоторые формы входной фильтрации разумно использовать и между ISP (особенно при небольшом числе префиксов).

Этот документ будет «снижать планку» адаптации входных фильтров, особенно для случаев многодомных и асимметричных подключений, для которых принято считать такую фильтрацию трудно реализуемой.

Можно отметить ряд направлений, в которых будет полезна дополнительная работа.

- Более подробная спецификация механизмов, поскольку в реализациях используются разные варианты (например, передавать ли групповой трафик во всех случаях через фильтр Strict RPF). Формальная спецификация механизмов поможет согласовать разные реализации.

- Дополнительное изучение и спецификация механизмов фильтрации на базе RIB (например, Feasible Path RPF). В частности, следует рассмотреть допущения, при которых механизмы работают должным образом.

- Подготовить более общее (по сравнению с данным документом) описание механизмов входной фильтрации после того, как будут конкретизированы упомянутые выше детали или механизмы и их систематизация.

- Рассмотрение более сложных случаев сетевых подключений с меняющимися свойствами (например, смена партнёров или провайдеров восходящего направления), когда требуется обеспечить фильтрацию партнерского трафика, если он приходит из восходящего соединения.

7. Благодарности

Rob Austein, Barry Greene, Christoph Reichert, Daniel Senie, Pedro Roque и Iljitsch van Beijnum просмотрели этот документ и помогли улучшить его. Thomas Narten, Ted Hardie и Russ Housley предоставили отклики, которые помогли улучшить окончательный вариант документа.

8. Литература

8.1. Нормативные документы

[1] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, May 2000.

8.2. Дополнительная литература

[2] Chandrasekeran, R., Traina, P. and T. Li, "BGP Communities Attribute", RFC 1997, August 1996.

[3] IANA, "Special-Use IPv4 Addresses", RFC 3330, September 2002.

[4] Bates, T. and Y. Rekhter, "Scalable Support for Multi-homed Multi-provider Connectivity", RFC 2260, January 1998.

[5] Hagino, J. and H. Snyder, "IPv6 Multihoming Support at Site Exit Routers", RFC 3178, October 2001.

9. Адреса авторов

Fred Baker

Cisco Systems

Santa Barbara, CA 93117

US

EMail: fred@cisco.com

Pekka Savola

CSC/FUNET

Espoo

Finland

EMail: psavola@funet.fi

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

10. Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.