

# Фильтрация на входе в сеть для защиты от DoS-атак с использованием обманных адресов IP (IP Spoofing)

## Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

### Статус документа

Этот документ содержит информацию для сообщества Internet. Документ может распространяться без ограничений.

### Авторские права

Copyright (C) The Internet Society (1998). All Rights Reserved.

### Аннотация

Недавно наблюдавшиеся DoS-атаки<sup>1</sup> с использованием подмены адреса отправителя показали наличие серьезной опасности для провайдеров Internet (ISP) и сообщества Internet в целом. В этом документе рассматривается простой и эффективный метод борьбы с такими атаками путем фильтрации входящего трафика с целью блокировки DoS-атак, в которых используются адреса IP, не относящиеся к точкам агрегирования ISP.

## Оглавление

1. Введение.....	1
2. Основы.....	1
3. Ограничение фальсифицированного трафика.....	3
4. Дополнительные возможности сетевого оборудования.....	3
5. Недостатки.....	3
6. Заключение.....	4
7. Вопросы безопасности.....	4
8. Благодарности.....	4
9. Литература.....	4
10. Адреса авторов.....	4
11. Полное заявление авторских прав.....	5

## 1. Введение

Организация DoS-атак на различные сайты Internet [1] заставляет провайдеров и организации, связанные с безопасностью, искать новые методы ослабления таких атак. Достижение этой цели сопряжено с многочисленными трудностями, однако существует ряд простых средств, позволяющих ограничить эффективность и область распространения таких атак. Эти средства борьбы с атаками реализованы пока недостаточно широко.

Данный тип атак известен уже достаточно давно. Однако защита от них еще находится на этапе становления. В статье [2] сказано, что Билл Чесвик (Bill Cheswick) - автор книги «Firewalls and Internet Security<sup>2</sup>» [3] - заявил, что в последний момент он исключил из своей книги главу с описанием таких атак, поскольку у администратора атакуемой системы нет эффективных способов защиты, а описывая метод [атаки], следует учитывать возможность его практического применения.

Хотя предложенный здесь метод ничуть не поможет при лавинных атаках с использованием корректных<sup>3</sup> IP-адресов, возможности использования атакующими подставных адресов будут ограничены правилами фильтрации сетей, из которых организуются атаки. Всем провайдерам настоятельно рекомендуется реализовать описанные в данном документе фильтры для того, чтобы лишить атакующих возможности использовать подставные адреса за пределами легитимно анонсируемых префиксов. Иными словами, если ISP агрегирует маршрутные анонсы для множества обслуживаемых им сетей<sup>4</sup>, этот провайдер должен использовать строгую фильтрацию для предотвращения трафика, переданного с указанием адресов отправителя за пределами агрегируемого блока адресов.

Дополнительным преимуществом предложенного метода является простота отслеживания источников атак, поскольку атакующие будут вынуждены использовать в поле отправителя легитимные адреса.

## 2. Основы

Ниже показана упрощенная схема атаки путем создания лавины пакетов TCP SYN.

204.69.207.0/24

<sup>1</sup>Denial of Service – атака на службу в целях отказа последней.

<sup>2</sup>Межсетевые экраны и безопасность Internet.

<sup>3</sup>Корректность адреса в данном контексте совершенно не означает, что атакующий использует реальный адрес своего хоста. Просто подставные адреса относятся к реально распределенным блокам адресов IP. *Прим. перев.*

<sup>4</sup>В оригинале - downstream networks. Прим. перев.

хост <----- маршрутизатор <--- Internet <----- маршрутизатор <-- атакующий

```

      TCP/SYN
      <-----
      Source: 192.168.0.4/32
SYN/ACK
no route
      TCP/SYN
      <-----
      Source: 10.0.0.13/32
SYN/ACK
no route
      TCP/SYN
      <-----
      Source: 172.16.0.2/32
SYN/ACK
no route
[и т. п.]

```

В этой схеме использовался ряд допущений:

- Хост является атакуемым узлом.
- Атакуемый находится в сети с корректным префиксом 204.69.207.0/24.
- Атакующий использует случайные значения адреса отправителя; в данном примере они случайно выбираются адреса из частных блоков [4], которые в общем случае не присутствуют в глобальных таблицах маршрутизации Internet и, следовательно, не являются доступными. Однако в реальных атаках могут применяться любые недоступные адреса.

Следует принимать во внимание и случаи использования обманных адресов отправителя, которые относятся к легитимным сетям, присутствующим в глобальных таблицах маршрутизации. Например, атакующий, используя корректный сетевой адрес, может создавать видимость того, что атака организована из сети организации, которая, по сути, не имеет к этой атаке никакого отношения. В таких случаях администратор атакуемой системы может активизировать фильтрацию трафика из сети, которую атакующий использовал для выбора подставных адресов. Такие фильтры будут приводить к блокированию трафика от легитимных узлов. И в этом случае администратор атакуемой системы становится невольным помощником атакующего.

Дополнительную сложность во время лавинных атак TCP SYN вызывает поток откликов SYN/ACK, которые передаются одному или множеству хостов<sup>1</sup>, не имеющих отношения к атаке, но становящихся ее дополнительными жертвами. Это позволяет атакующему наносить вред одновременно множеству систем..

Предпринимались попытки организации подобных атак с использованием лавины потоков UDP и ICMP. Вариант с лавиной UDP использует обманные пакеты для попыток «подключения» к сетевым службам chargen, что должно приводить к передаче потока символов в адрес хоста, чей адрес был использован в запросах. Системные администраторы **должны** блокировать пакеты UDP, адресованные в диагностические порты системы и приходящие извне административного домена. Другой вариант атаки (ICMP flooding) использует хитрость в механизме репликации широковещательных пакетов IP, адресованных в подсеть. Эти атаки базируются на том, что маршрутизаторы, обслуживающие крупные широковещательные сети<sup>2</sup>, преобразуют широковещательные адреса IP (например, 10.255.255.255 для пакетов, адресованных всем хостам сети 10.0.0.0/8) в широковещательные кадры уровня 2 (например для Ethernet, FF:FF:FF:FF:FF:FF). Сетевые адаптеры Ethernet (MAC-уровень) при нормальной работе прослушивают ограниченное число адресов. Одним из адресов, прослушиваемых каждым устройством Ethernet в нормальном режиме, является широковещательный адрес FF:FF:FF:FF:FF:FF. При обнаружении такого пакета в среде передачи устройство будет принимать его и инициировать прерывание для обработки полученного кадра. Таким образом, лавина подобных широковещательных кадров может поглотить все доступные ресурсы конечной системы [9]. Представляется разумным рассмотрение системными администраторами вопроса о приеме и пересылке адресованных всей сети широковещательных пакетов на граничных маршрутизаторах и отключение принятой по умолчанию обработки таких пакетов<sup>3</sup>.

При организации атаки TCP SYN с использованием недостижимых адресов в поле отправителя, атакуемый хост пытается сохранять выделенные ресурсы в ожидании отклика. Атакующие безостановочно меняют обманные адреса для каждого генерируемого пакета, что достаточно быстро приводит к исчерпанию ресурсов атакуемого хоста.

Если же атакующий указывает в пакетах легитимные адреса отправителя, атакуемая система будет слать большое число пакетов SYN/ACK предполагаемым инициаторам соединений. В этом случае атакующий нарушает работу двух систем – непосредственного объекта атаки и хоста, адрес которого используется в качестве подставного.

В результате оба варианта атаки существенно снижают производительность атакуемой системы и в некоторых случаях могут привести к полной потере работоспособности объекта атаки.

В результате возникновения таких атак производители большинства операционных систем обновили свои программы, чтобы обеспечить устойчивость серверов к атакам с высокой частотой попыток организации соединения. Эти обновления весьма полезны и являются одной из необходимых компонент решения проблемы в целом. Распространение систем фильтрации на входе (Ingress filtering) займет некоторое время, а обновить операционные системы можно значительно быстрее. Комбинация этих способов позволит обеспечить эффективную защиту от атак с подменой адресов. Сведения о программных обновлениях для ОС различных производителей можно найти в документе [1].

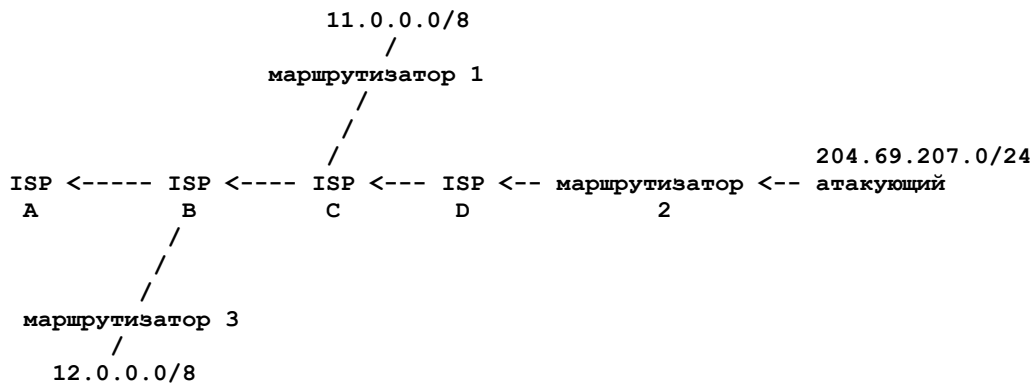
<sup>1</sup>Чьи адреса использованы в качестве подставных. *Прим. перев.*

<sup>2</sup>Например, Ethernet. *Прим. перев.*

<sup>3</sup>Этот вопрос рассматривается в [RFC 2644](#). *Прим. перев.*

### 3. Ограничение фальсифицированного трафика

Проблемы, связанные с этим типом атак, достаточно многочисленны и включают недостатки реализации используемых хостами программ, методов маршрутизации и стеков TCP/IP в целом. Однако, ограничение транзитного трафика из обслуживаемых сетей известными и осознанно анонсируемыми префиксами адресов позволит существенно снизить возможность организации атак с подменой адресов.



В приведенном примере атакующий находится в сети 204.69.207.0/24, подключение которой к Internet обеспечивает провайдер ISP D. Фильтрация входящего трафика на интерфейсе маршрутизатора 2, обеспечивающего связь с сетью атакующего, которая позволит принимать лишь те пакеты, где адрес отправителя относится к блоку 9.0.0.0/8, заблокирует возможность атаки с использованием подставных адресов из другого блока.

Фильтр входящих пакетов на маршрутизаторе 2 работает по следующему алгоритму:

```

IF    адрес отправителя в пакете относится к сети 204.69.207.0/24
THEN  пакет пересылается в направлении получателя
IF    адрес отправителя в пакете относится к любому другому блоку
THEN  пакет отбрасывается (drop).
  
```

Администраторы должны вести журнал отбрасываемых пакетов, который обеспечит постоянный мониторинг любых подозрительных действий.

### 4. Дополнительные возможности сетевого оборудования

Следует рассмотреть дополнительные функции, которые могут использоваться в новых реализациях. Ниже кратко описана одна из таких возможностей:

- Реализация автоматических фильтров на серверах доступа. В большинстве случаев доступ по коммутируемым линиям обеспечивается для индивидуальных пользователей, которые работают с одним ПК. **Единственным** корректным адресом отправителя в таких случаях является адрес, выделенный провайдером для этой сессии. Сервер удаленного доступа может проверять каждый пакет на входе для предотвращения возможности применения пользователем подставных адресов. Обычно в таких устройствах должна быть предусмотрена и возможность удаленного подключения не отдельного компьютера, а сети, использующей свой маршрутизатор. Такая возможность может быть реализована, как опция. Некоторые провайдеры и производители оборудования уже сообщают о реализации фильтров на серверах доступа.

Рассматривался также вариант проверки IP-адреса отправителя, предложенный в [8], но этот метод недостаточно хорошо работает в реальных сетях. Метод заключается в просмотре адресов отправителя на предмет соответствия принявшего пакет интерфейса пути, через который обеспечивается доставка отправителю данного пакета. При наличии в Internet асимметричных маршрутов использование такой проверки представляется проблематичным.

### 5. Недостатки

Фильтрация по своей природе может нарушать работу некоторых «специальных» служб. Для поставщиков подобных типов сервиса целесообразно рассмотреть другие варианты организации работы этих служб, чтобы избежать влияния входных фильтров.

Одной из служб, на которые оказывает влияние фильтрация на входе, является Mobile IP [6]. Трафик в направлении мобильных узлов передается с использованием туннелей, но трафик от мобильных узлов туннелирования не использует. В результате пакеты от мобильного узла могут содержать адрес отправителя, не соответствующий принявшей пакет сети. Рабочая группа Mobile IP для решения этой проблемы предложила «обратные туннели<sup>1</sup>» [7]. Метод основан на том, что мобильная станция сначала туннелирует данные домашнему агенту (home agent) и только после этого информация передается в Internet. Дополнительным преимуществом такой схемы является повышение эффективности обработки группового трафика, что является добавочным стимулом реализации обратных туннелей в мобильных системах IP.

Как было отмечено выше, фильтрация на входе существенно осложняет проведение атак с подменой адресов, но такая фильтрация не может помешать атакующему использовать подставные адреса хостов из корректного для сети атакующего блока адресов. Однако в таких случаях наличие входных фильтров дает администратору достоверные сведения о местонахождении источника атаки и значительно упрощает поиск атакующего. По крайней мере, администратор всегда может заблокировать диапазон адресов, в который входит используемый атакующим подставной адрес или адреса, пока конкретный источник атаки не будет обнаружен.

Если входные фильтры применяются в средах, где используется протокол DHCP или BOOTP, администратор должен обеспечить корректную доставку пакетов с адресом отправителя 0.0.0.0 и пакетов с адресом получателя

<sup>1</sup>Reverse tunnel.

255.255.255.255. Область распространения пакетов directed broadcast должна быть контролируемой, а их произвольная пересылка недопустима<sup>1</sup>.

## 6. Заключение

Входная фильтрация трафика на периферии подключенных к Internet сетей будет снижать эффективность DoS-атак с подменой адреса отправителя. Провайдеры и администраторы корпоративных сетей уже начали использование этого типа фильтрации на периферийных маршрутизаторах. Всем сервис-провайдерам рекомендуется реализовать такие фильтры, как можно скорее. В дополнение к избавлению сообщества Internet от атак этого типа предложенный метод также помогает провайдерам локализовать источник атаки в своей сети, если входные фильтры реализованы на маршрутизаторах, используемых для подключения заказчиков.

Администраторам корпоративных сетей также следует реализовать такие фильтры, чтобы предотвратить возможность организации атак из своей сети. Фильтрация также позволит избавиться от проблем, связанных с некорректным подключением систем к сети.

На всех сетевых администраторов ложится ответственность за предотвращение атак с подменой адресов отправителей из контролируемых ими сетей.

## 7. Вопросы безопасности

Основной задачей данного документа является повышение уровня осведомленности и безопасности сообщества Internet в целом. Чем больше провайдеров Internet и корпоративных пользователей реализует в своих маршрутизаторах входные фильтры, тем сложнее будет организовать атаки с подменой адресов отправителей в пакетах. Фильтрация также упрощает поиск источников атак. Снижение числа атак в сети Internet позволит более эффективно использовать ресурсы для отслеживания атак, которые все-таки будут происходить время от времени.

## 8. Благодарности

Авторы благодарят группу NANOG<sup>2</sup> [5] за активное обсуждение вопроса и участие в поисках возможных решений. Благодарим также Justin Newton [Priori Networks] и Steve Bielagus [IronBridge Networks] за их комментарии и вклад в работу.

## 9. Литература

- [1] CERT Advisory CA-96.21; TCP SYN Flooding and IP Spoofing Attacks; September 24, 1996.
- [2] B. Ziegler, "Hacker Tangles Panix Web Site", Wall Street Journal, 12 September 1996.
- [3] "Firewalls and Internet Security: Repelling the Wily Hacker"; William R. Cheswick and Steven M. Bellovin, Addison-Wesley Publishing Company, 1994; ISBN 0-201-63357-4.
- [4] Rekhter, Y., Moskowitz, R., Karrenberg, D., de Groot, G., and E. Lear, "Address Allocation for Private Internets", [RFC 1918](#), February 1996.
- [5] The North American Network Operators Group; <http://www.nanog.org>.
- [6] Perkins, C., "IP Mobility Support", RFC 2002, October 1996.
- [7] Montenegro, G., "Reverse Tunneling for Mobile IP", RFC 2344, May 1998.
- [8] Baker, F., "Requirements for IP Version 4 Routers", [RFC 1812](#), June 1995.
- [9] Спасибо Craig Huegen; См. сайт: <http://www.quadrunner.com/~chuegen/smurf.txt>.

## 10. Адреса авторов

### Paul Ferguson

Cisco Systems, Inc.  
13625 Dulles Technology Dr.  
Herndon, Virginia 20170 USA  
E-Mail: [ferguson@cisco.com](mailto:ferguson@cisco.com)

### Daniel Senie

Amaranth Networks Inc.  
324 Still River Road  
Bolton, MA 01740 USA  
E-Mail: [dts@senie.com](mailto:dts@senie.com)

### Перевод на русский язык

#### Николай Малых

[nmalykh@protokols.ru](mailto:nmalykh@protokols.ru)

<sup>1</sup>См. [RFC 2644](#). Прим. перев.

<sup>2</sup>North American Network Operators Group – Группа Сетевых Операторов Северной Америки. Прим. перев.

## **11. Полное заявление авторских прав**

Copyright (C) The Internet Society (2000). Все права защищены.

Этот документ и его переводы могут копироваться и предоставляться другим лицам, а производные работы, комментирующие или иначе разъясняющие документ или помогающие в его реализации, могут подготавливаться, копироваться, публиковаться и распространяться целиком или частично без каких-либо ограничений при условии сохранения указанного выше уведомления об авторских правах и этого параграфа в копии или производной работе. Однако сам документ не может быть изменён каким-либо способом, таким как удаление уведомления об авторских правах или ссылок на Internet Society или иные организации Internet, за исключением случаев, когда это необходимо для разработки стандартов Internet (в этом случае нужно следовать процедурам для авторских прав, заданных процессом Internet Standards), а также при переводе документа на другие языки.

Предоставленные выше ограниченные права являются бессрочными и не могут быть отозваны Internet Society или правопреемниками.

Этот документ и содержащаяся в нем информация представлены "как есть" и автор, организация, которую он/она представляет или которая выступает спонсором (если таковой имеется), Internet Society и IETF отказываются от каких-либо гарантий (явных или подразумеваемых), включая (но не ограничиваясь) любые гарантии того, что использование представленной здесь информации не будет нарушать чьих-либо прав, и любые предполагаемые гарантии коммерческого использования или применимости для тех или иных задач.