Настройте обычно используемые ACL IP

Содержание

[Введение](#)
[Предварительные условия](#)
[Требования](#)
[Используемые компоненты](#)
[Настройка](#)
[Разрешите избранному узлу доступ к сети](#)
[Запретить выбранному хосту доступ к сети](#)
[Разрешить доступ к диапазону смежных IP-адресов](#)
[Запрет трафика Telnet (TCP, порт 23)](#)
[Инициирование сеанса TCP только внутренними сетями](#)
[Отрицание трафика FTP (TCP, порт 21)](#)
[Позвольте трафик FTP (активный FTP)](#)
[Позвольте трафик FTP (пассивный FTP)](#)
[Разрешить программу эхо-тестирования (ICMP)](#)
[Разрешение HTTP, Telnet, Mail, POP3, FTP](#)
[Позвольте DNS](#)
[Разрешить обновление маршрутизации](#)
[Трафик отладки на основе ACL](#)
[Фильтрация MAC-адресов](#)
[Проверка](#)
[Устранение неполадок](#)
[Дополнительные сведения](#)

Введение

В данном документе описываются простые конфигурации для распространенных списков управления доступом IP Access Control Lists (ACL), которые фильтруют IP-пакеты в зависимости от следующих данных:

- Исходный адрес
- Адрес получателя
- Тип пакета
- Любая комбинация этих элементов

Для фильтрации сетевого трафика контроль за ACL, переданы ли пакеты для маршрутизации или заблокированы в интерфейсе маршрутизатора. Ваш маршрутизатор исследует каждый пакет, чтобы определить, передать ли или отбросить пакет на основе критериев, которые вы задаете в ACL. Критерии ACL включают:

- Адрес источника трафика
- Адрес назначения (DA) трафика
- Протокол высшего уровня

Выполните эти шаги для построения ACL, поскольку примеры в этом документе показывают:

1. Создайте список управления доступом.
2. Примените список ACL к интерфейсу.

ACL IP является последовательным набором разрешения, и запретите условия, которые применяются к пакету IP. Маршрутизатор проверяет пакеты на соответствие условиям ACL по одному за раз.

Первое соответствие определяет, будет ли программное обеспечение Cisco IOS® принимать или отвергать пакет. Поскольку программное обеспечение Cisco IOS останавливает проверку по условиям после первого совпадения, то порядок условий становится критически важен. Если совпадений нет, маршрутизатор отвергает пакет из-за неявного условия deny all.

Вот примеры того, как IP ACL могут быть настроены в программном обеспечении Cisco IOS:

- Стандартные списки управления доступом
- Расширенные списки управления доступом
- Динамичный (Технология Lock and Key (замок и ключ)) ACL
- Именованные списки ACL для протокола IP
- Рефлексивные списки управления доступом (ACL)
- Списки управления доступом (ACL) с временным критерием то использование временные диапазоны
- Откомменированные записи списка прав доступа (ACL) IP
- Основанные на контексте ACL
- Прокси-сервер аутентификации
- Расширенные списки управления доступом
- Распределенные списки управления доступом с временным критерием

В этом документе описываются некоторые общеупотребительные стандартные и расширенные списки ACL. Подробнее о различных типах ACL, которые поддерживает программное обеспечение Cisco IOS, и об их настройке и редактировании см. "Настройка списков доступов IP".

Формат синтаксиса команды стандартного ACL выглядит следующим образом: access-list access-list-number {permit|deny} {host|source source-wildcard|any}.

Стандартные ACL сравнивают адрес источника пакетов IP к адресам, настроенным в ACL чтобы к контрольному трафику.

Расширенные списки ACL сравнивают адреса источника и назначения пакетов IP к адресам, настроенным в ACL чтобы к контрольному трафику. Работу расширенных ACL можно сделать более детализированной, с фильтрацией трафика по следующим критериям:

- Протокол
- Номера портов
- Значение точки кода дифференцированных услуг (DSCP)
- Значение приоритета
- Состояние синхронизировать порядкового номера (SYN) укусило

Форматы синтаксиса команды расширенных списков ACL:

IP

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
  {deny | permit} protocol source source-wildcard destination
    destination-wildcard
  [precedence precedence] [tos tos] [log | log-input]
    [time-range time-range-name][fragments]
```

Internet Control Message Protocol (ICMP)

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit}
 icmp source source-wildcard destination destination-wildcard [icmp-type
 [icmp-code] | [icmp-message]] [precedenceprecedence] [tos tos] [log |
 log-input] [time-range time-range-name][fragments]
```

Transport Control Protocol (TCP)

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} tcp
 source source-wildcard [operator [port]] destination destination-wildcard
 [operator [port]] [established] [precedence precedence] [tos tos] [log |
 log-input] [time-range time-range-name][fragments]
```

Протокол дейтаграммы пользователя (UDP)

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} udp
 source source-wildcard [operator [port]] destination destination-wildcard
 [operator [port]] [precedence precedence] [tos tos] [log | log-input]
 [time-range time-range-name][fragments]
```

Предварительные условия

Требования

Перед попыткой применения конфигурации убедитесь в том, что следующие требования выполняются:

- Основное понимание IP-адресации

См. IP-адресацию и Разделяющий на подсети для Новых пользователей для дополнительных сведений.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

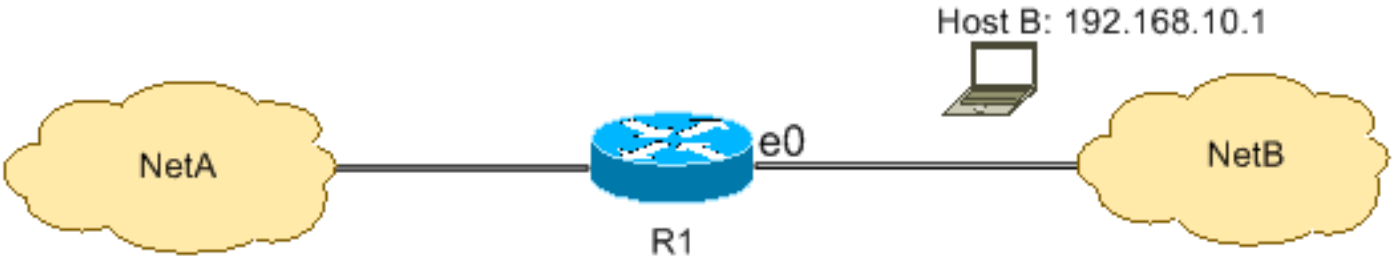
Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Настройка

Следующие примеры конфигурации используют наиболее распространенные IP ACL.

Разрешите избранному узлу доступ к сети

Эти данные показывают выбор узла, данный разрешение для доступа к сети. Весь трафик из узла B, направленный к NetA, принимается, в то время как весь другой трафик из NetB, направленный к NetA, отвергается.



Выходные данные в таблице R1 показывают, как сеть выдает узлу право на доступ. Эти выходные данные таковы:

- Эта конфигурация допускает только узел с IP-адресом 192.168.10.1 через интерфейс Ethernet 0 на R1.
- У этого узла есть доступ к IP-службам NetA.
- Никакие другие узлы в NetB не имеют доступа к NetA.
- В ACL не настроены никакие инструкции запрета.

По умолчанию в конце каждого ACL есть неявное условие deny all (запретить все). Все, что не разрешается явно, отвергается.

_____ M1

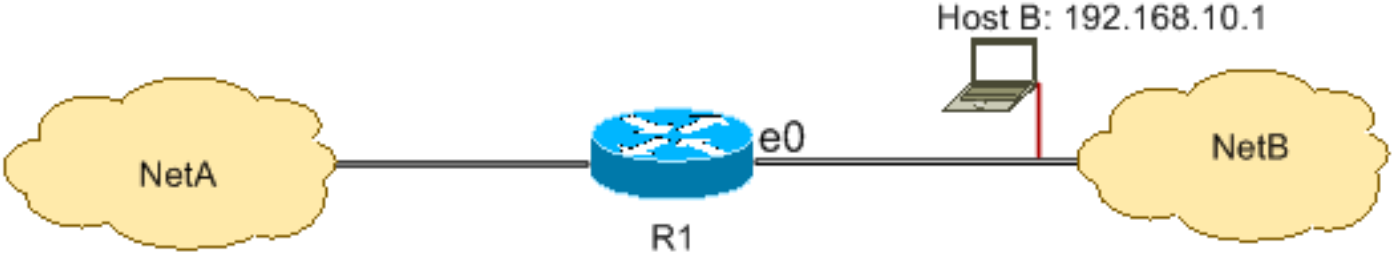
```
hostname R1
!
interface ethernet0
ip access-group 1 in
!
access-list 1 permit host 192.168.10.1
```

> **Примечание:** ACL фильтрует пакеты IP от NetB до NetA, кроме пакетов из источника от NetB. Пакеты из источника от Хоста B до NetA все еще разрешены.

> **Примечание:** ACL **разрешение access-list 1 192.168.10.1 0.0.0.0** является другим способом настроить то же правило.

Запретить выбранному хосту доступ к сети

Эти данные показывают, что трафик, полученный от Хоста B, предназначенного к NetA, запрещен, в то время как разрешен весь другой трафик от NetB для доступа к NetA.



Следующая конфигурация запрещает получение всех пакетов от узла 192.168.10.1/32 через Ethernet 0 или R1 и разрешает получение всех остальных пакетов. **Для того чтобы явно**

разрешить все остальные пакеты, следует использовать команду access list 1 permit any, поскольку в каждом ACL есть неявное условие "deny all".

_____ M1

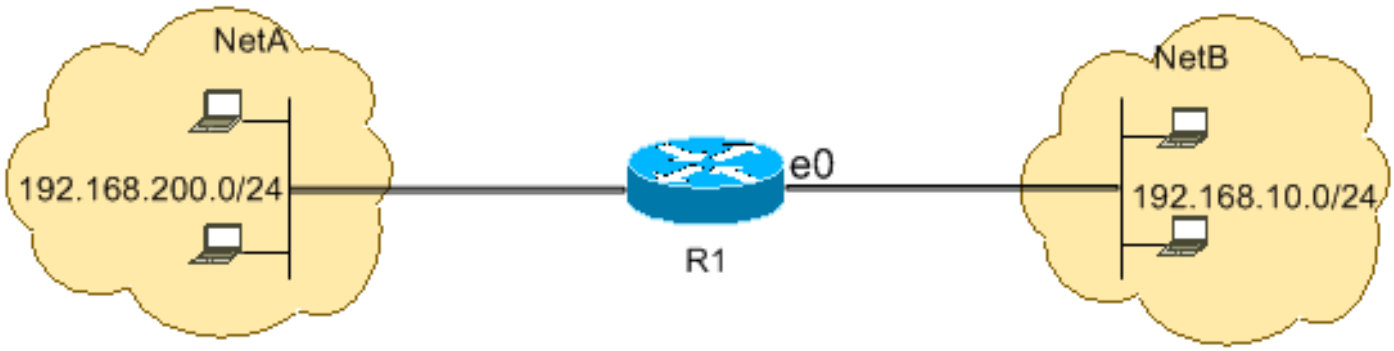
```
hostname R1
!
interface ethernet0
ip access-group 1 in
!
access-list 1 deny host 192.168.10.1
access-list 1 permit any
```

> **Примечание:** Порядок операторов критичен для функционирования списка ACL. Если порядок записей является обратным, как показано в данной команде, первая строка сопоставляет адрес источника пакета. Таким образом, ACL не сможет блокировать доступ узла 192.168.10.1/32 к NetA.

```
access-list 1 permit any
   access-list 1 deny host 192.168.10.1
```

Разрешить доступ к диапазону смежных IP-адресов

Эти данные показывают, что все хосты в NetB с сетевым адресом 192.168.10.0/24 могут доступ к сети 192.168.200.0/24 в NetA.



Эта конфигурация позволяет IP-пакетам, чьи заголовки IP содержат адрес источника в сети 192.168.10.0/24 и адрес назначения в сети 192.168.200.0/24, получить доступ к NetA. Неявное условие "deny all" в конце ACL запрещает прохождение всего трафика, не удовлетворяющего разрешающим условиям, через входящий Ethernet 0 на R1.

_____ M1

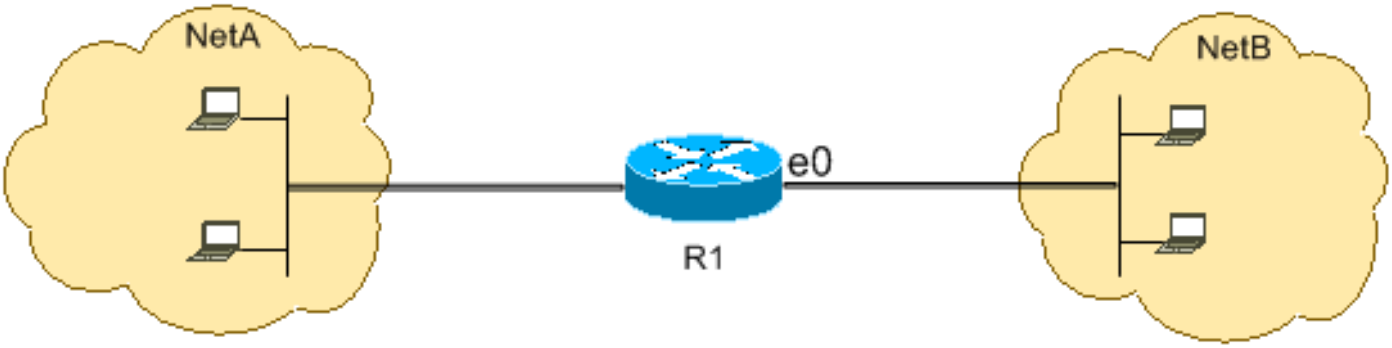
```
hostname R1
!
interface ethernet0
ip access-group 101 in
!
access-list 101 permit ip 192.168.10.0  0.0.0.255
  192.168.200.0  0.0.0.255
```

> **Примечание:** В команде access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.200.0 0.0.0.255, эти "0.0.0.255" обратная маска сети 192.168.10.0 с маской 255.255.255.0. ACL используют обратную маску, чтобы знать, сколько битов в адресе сети требуют сопоставления. В таблице ACL разрешает все узлы с адресами источника в сети 192.168.10.0/24 и адресами назначения в сети 192.168.200.0/24.

Подробнее о маске сетевого адреса и о том, как вычислить обратную маску, необходимую для ACL, см. раздел "Маски" в документе "Настройка списков доступа IP".

Запрет трафика Telnet (TCP, порт 23)

Для совещания проблем более высокой безопасности вам, возможно, придется отключить доступ Telnet к вашей частной сети от открытой сети. Данный рисунок показывает, как трафик Telnet из сети NetB (публичной), направленный в NetA (частную), отвергается, что позволяет NetA инициировать и установить сеанс Telnet с NetB, при этом разрешая весь другой IP-трафик.



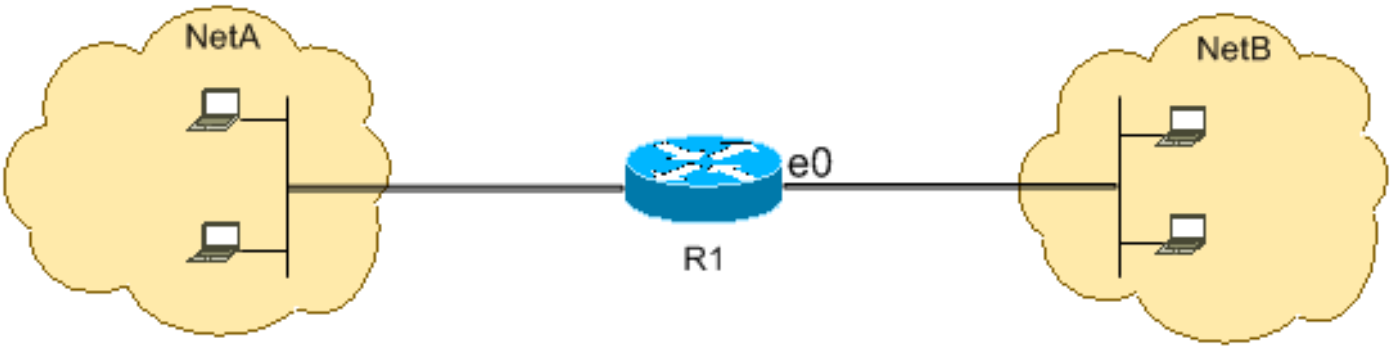
Telnet использует TCP, порт 23. Следующая конфигурация показывает, что весь TCP-трафик, направленный в NetA для порта 23, заблокирован, а остальной IP-трафик разрешен.

M1

```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
access-list 102 deny tcp any any eq 23
access-list 102 permit ip any any
```

Инициирование сеанса TCP только внутренними сетями

Эти данные показывают, что Трафик TCP, полученный от NetA, предназначенного к NetB, разрешен, в то время как запрещен Трафик TCP от NetB, предназначенного к NetA.



Назначением ACL в данном примере является следующее:

- Разрешить узлам в NetA инициировать и устанавливать сеанс TCP к узлам в NetB.
- Запретить узлам в NetB инициировать и устанавливать сеанс TCP к узлам в NetA.

Эта конфигурация разрешает дейтаграмме проходить через внутренний интерфейс Ethernet 0 на R1, если у нее есть:

- Подтвержденный (ACK) или сброс (RST) набор битов (указание на установленный сеанс TCP)
- Значение порта назначения, больше, чем 1023

_____ M1

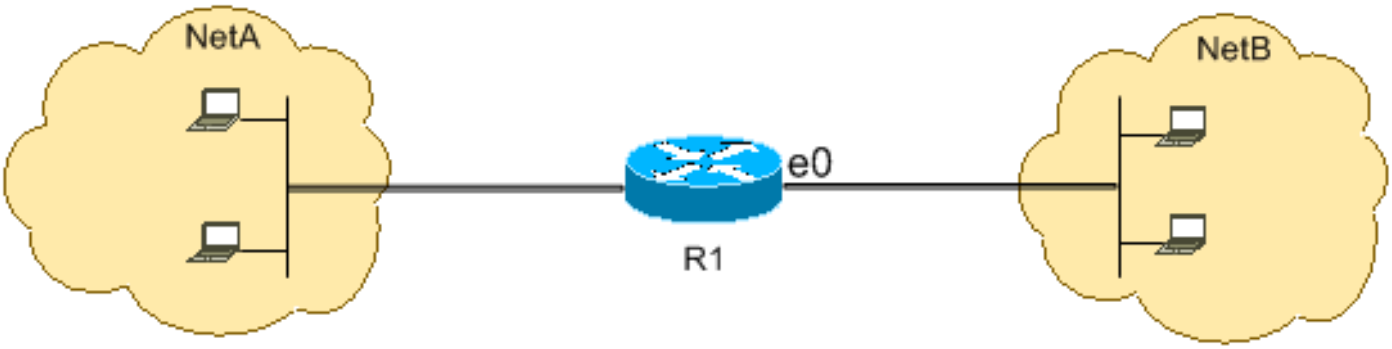
```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
access-list 102 permit tcp any any gt 1023 established
```

Начиная с большинства известных портов для использования IP-сервисов оценивает меньше чем 1023, любая дейтаграмма с портом назначения, меньше чем 1023 или ACK/RST укусили "not set", запрещена ACL 102. Поэтому, когда хост от NetB инициирует TCP - подключение путем передачи первого пакета TCP (без Набора битов синхронизированного/стартового пакета (SYN/RST)) для номера порта меньше чем 1023, это запрещено и сбои сеанса TCP. Сеансы TCP, инициированные NetA к NetB, разрешаются, поскольку у них есть набор битов ACK/RST для возврата пакетов, и они используют значения портов ниже 1023.

Полный список портов см. в RFC 1700 .

Отрицание трафика FTP (TCP, порт 21)

Эти данные показывают, что FTP (TCP, порт 21) и данные FTP (порт 20), трафик, полученный от NetB, предназначенного к NetA, запрещен, в то время как разрешен весь другой IP - трафик.



FTP использует порты 21 и 20. Трафик TCP, предназначенный для порта 21 и порта 20, отвергается, а все остальное явным образом разрешается.

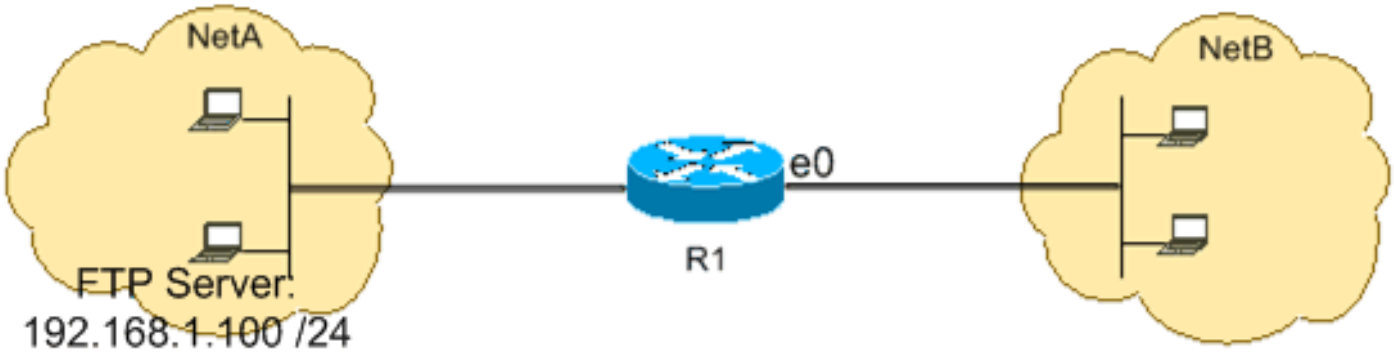
_____ M1

```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
access-list 102 deny tcp any any eq ftp
access-list 102 deny tcp any any eq ftp-data
access-list 102 permit ip any any
```

Позвольте трафик FTP (активный FTP)

FTP может работать в двух других режимах, названных активными и пассивными. Общие сведения о работе активного и пассивного FTP см. в разделе "Функционирование FTP".

Когда FTP работает в активном режиме, сервер FTP использует порт 21 для управления и порт 20 для данных. Сервер FTP (192.168.1.100) расположен NetA. В следующем примере показано, что трафик FTP (TCP, порт 21) и данных FTP (порт 20), пересылаемый из NetB на сервер FTP (192.168.1.100), разрешается, а весь остальной IP-трафик отвергается.



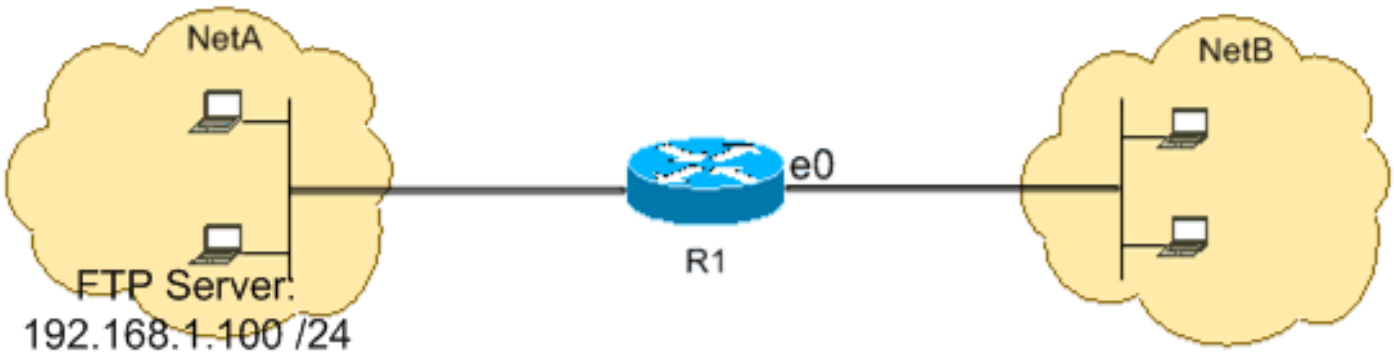
_____ M1

```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
access-list 102 permit tcp any host 192.168.1.100 eq ftp
access-list 102 permit tcp any host 192.168.1.100 eq ftp-data established
!
interface ethernet1
 ip access-group 110 in
!
access-list 110 permit host 192.168.1.100 eq ftp any established
access-list 110 permit host 192.168.1.100 eq ftp-data any
```

Позвольте трафик FTP (пассивный FTP)

FTP может работать в двух других режимах, названных активными и пассивными. Общие сведения о работе активного и пассивного FTP см. в разделе "Функционирование FTP".

Когда FTP работает в пассивном режиме, сервер FTP использует порт 21 для управления и динамические порты, начиная с 1024 и выше, для данных. Сервер FTP (192.168.1.100) расположен NetA. В следующем примере показано, что трафик FTP (TCP, порт 21) и данных FTP (порты, начиная с 1024 и выше), пересылаемый из NetB на сервер FTP (192.168.1.100), разрешается, а весь остальной IP-трафик отвергается.

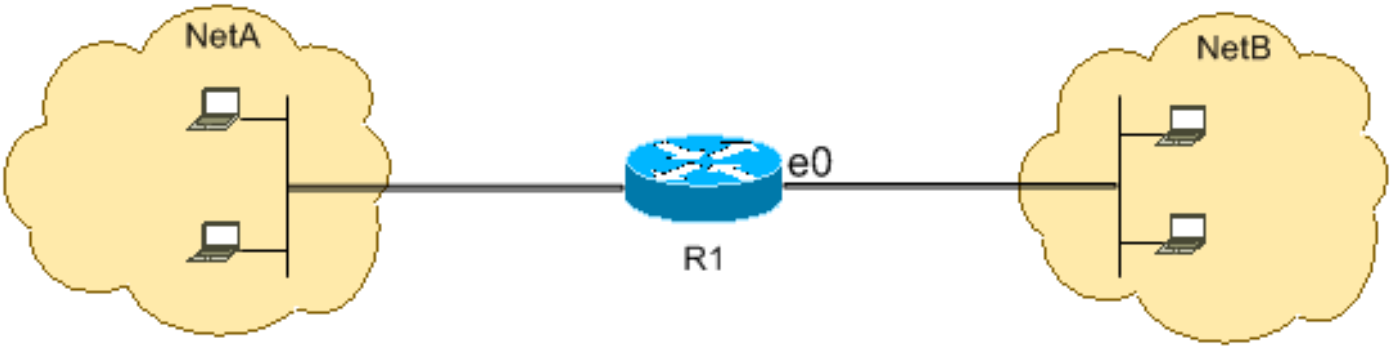


_____ M1

```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
access-list 102 permit tcp any host 192.168.1.100 eq ftp
access-list 102 permit tcp any host 192.168.1.100 gt 1024
!
interface ethernet1
 ip access-group 110 in
!
access-list 110 permit host 192.168.1.100 eq ftp any established
access-list 110 permit host 192.168.1.100 gt 1024 any established
```

Разрешить программу эхо-тестирования (ICMP)

Эти данные показывают, что ICMP, исходящий из NetA от NetA, предназначенного к NetB, разрешен и пропинговывает полученный от NetB, предназначенного к NetA, запрещены.



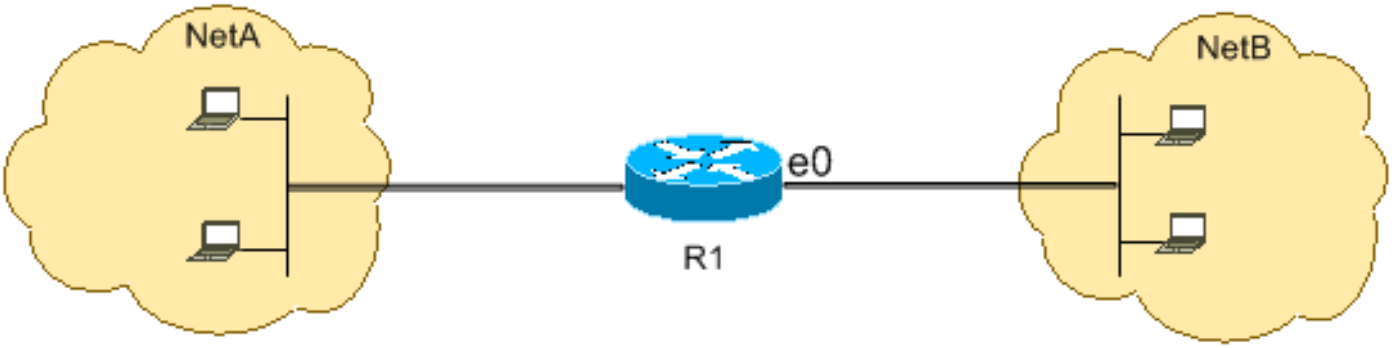
Эта конфигурация разрешает проходить по интерфейсу Ethernet 0 из NetB в NetA только пакетам эхо-ответа (отклика эхо-теста). Но конфигурация блокирует все пакеты эхо-запроса ICMP, когда эхо-тесты исходят из NetB и направляются в NetA. Таким образом, хосты в сети NetA могут выполнять эхо-тестирование хостов в сети NetB, но хосты в сети NetB не могут выполнять эхо-тестирование хостов в сети NetA.

_____ M1

```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
access-list 102 permit icmp any any echo-reply
```

Разрешение HTTP, Telnet, Mail, POP3, FTP

Эти данные показывают, что только HTTP, Telnet, Протокол SMTP, POP3 и трафик FTP разрешены, и остаток трафика, полученного от NetB, предназначенного к NetA, запрещен.



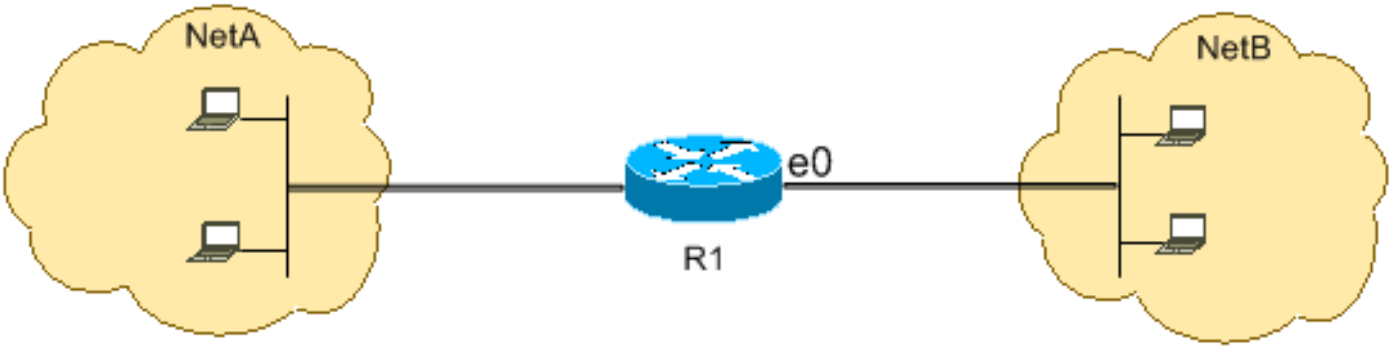
Эта конфигурация разрешает трафик TCP со значениями порта назначения, которые соответствуют WWW (порт 80), Telnet (порт 23), SMTP (порт 25), POP3 (порт 110), FTP (порт 21) или данным FTP (порт 20). Следует помнить, что неявное условие "deny all" в конце ACL запрещает весь трафик, не удовлетворяющий разрешающим условиям.

_____ M1

```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
access-list 102 permit tcp any any eq www
access-list 102 permit tcp any any eq telnet
access-list 102 permit tcp any any eq smtp
access-list 102 permit tcp any any eq pop3
access-list 102 permit tcp any any eq 21
access-list 102 permit tcp any any eq 20
```

Позвольте DNS

Эти данные показывают, что только трафик Системы доменных имен (DNS) разрешен, и остаток трафика, полученного от NetB, предназначенного к NetA, запрещен.



Эта конфигурация разрешает TCP-трафик со значением порта назначения 53. Неявное условие "deny all" в конце ACL запрещает весь трафик, не удовлетворяющий разрешающим условиям.

_____ M1

```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
access-list 112 permit udp any any eq domain
access-list 112 permit udp any eq domain any
access-list 112 permit tcp any any eq domain
access-list 112 permit tcp any eq domain any
```

Разрешить обновление маршрутизации

Когда вы применяете входящий ACL на интерфейс, гарантируете, что не отфильтрованы обновления маршрута. Используйте необходимые ACL из этого списка, чтобы разрешить пакеты протокола маршрутизации:

Введите эту команду для разрешения Протокола RIP:

```
access-list 102 permit udp any any eq rip
```

Введите эту команду для разрешения Протокола IGRP:

```
access-list 102 permit igrp any any
```

Введите эту команду для разрешения Расширенного IGRP (EIGRP):

```
access-list 102 permit eigrp any any
```

Введите эту команду для разрешения Протокола OSPF:

```
access-list 102 permit ospf any any
```

Введите эту команду для разрешения Протокола BGP:

```
access-list 102 permit tcp any any eq 179
access-list 102 permit tcp any eq 179 any
```

Трафик отладки на основе ACL

Использование **команд отладки** требует выделения ресурсов системы как память, и питание для обработки и в экстренных ситуациях может заставить в-большой-степени-загружаемую-систему останавливаться. **Используйте команды debug с осторожностью. Воспользуйтесь ACL, чтобы отобрать трафик, который следует проверить, и снизить таким образом воздействие команд debug**. В такой конфигурации фильтрация пакетов не выполняется.

Эта конфигурация включает команду debug ip packet только для пакетов между хостами 10.1.1.1 и 172.16.1.1.

```
R1(config)#access-list 199 permit tcp host 10.1.1.1 host 172.16.1.1
   R1(config)#access-list 199 permit tcp host 172.16.1.1 host 10.1.1.1
   R1(config)#end
   R1#debug ip packet 199 detail
   IP packet debugging is on (detailed) for access list 199
```

Подробнее о воздействии команд отладки см. "Важные сведения о командах отладки".

Подробнее об использовании ACL с командами отладки см. раздел "Использование команды debug" документа "Общие сведения о командах Ping и Traceroute".

Фильтрация MAC-адресов

Можно фильтровать кадры с определенным адресом источника или назначения станции MAC - уровня. Любое количество адресов может быть настроено в систему без снижения производительности. Для фильтрации Адресом MAC-уровня используйте эту команду в режиме глобальной конфигурации:

```
Router#config terminal
       bridge irb
       bridge 1 protocol ieee
```

```
       bridge 1 route ip
```

Примените протокол мостовой передачи к интерфейсу, в котором вы нуждаетесь к трафику фильтрации наряду с созданным списком доступа:

```
Router#int fa0/0
       no ip address
       bridge-group 1 {input-address-list 700 | output-address-list 700}
       exit
```

Создайте Виртуальный интерфейс моста и примените IP-адрес, который назначен на Интерфейс Ethernet:

```
Router#int bvi1
       ip address
       exit
!
!
       access-list 700 deny <mac address> 0000.0000.0000
       access-list 700 permit 0000.0000.0000 ffff.ffff.ffff
```

С этой конфигурацией маршрутизатор только позволяет MAC-адреса, настроенные на access-list 700. Со списком доступа запретите MAC adddress, который не может иметь доступа и затем разрешить остальным.

Примечание: Создайте каждую линию списка доступа для каждого MAC-адреса.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Configuring IP Access Lists
- Страница поддержки списков доступа
- Страница поддержки IP-маршрутизации
- Протоколы маршрутизируемые по IP
- Cisco Systems – техническая поддержка и документация