Настройка распространённых ACL IP

Содержание

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:

- адрес источника
- адрес назначения
- тип пакета
- любая комбинация данных пунктов

Для фильтрации сетевого трафика ACL проверяют, пересылаются ли передаваемые пакеты или же блокируются на интерфейсе маршрутизатора. Маршрутизатор проверяет каждый пакет и на основании критериев, указанных в ACL, определяет, что с ним нужно сделать: переслать или сбросить. Критерии ACL включают:

- адреса источника трафика
- адрес назначения трафика
- протокол верхнего уровня

Выполните следующие действия, чтобы создать такой же ACL, как в приведенных в этом документе примерах:

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

IP ACL – последовательный набор состояний разрешения и отказа, применяемый к IP-пакету. Маршрутизатор проверяет пакеты на соответствие условиям ACL по одному.

Первое соответствие определяет, что программное обеспечение Cisco IOS® сделает с пакетом: примет или отвергнет его. 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 ACL
- расширенные ACL
- динамические ACL (замок и ключ)
- именованные IP-списки ACL
- рефлексивные ACL
- синхронизируемые списки ACL, использующие временные диапазоны
- откомментированные записи IP ACL
- контекстно-ориентированные ACL
- прокси-аутентификации
- Turbo ACL
- распределенные синхронизируемые ACL

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. в разделе 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 (только для зарегистрированных клиентов) управляют трафиком, сравнивая адрес источника IP-пакетов с адресами, заданными в списке.

Расширенные ACL (только для зарегистрированных клиентов) управляют трафиком, сравнивая адреса источника и назначения IP-пакетов с адресами, заданными в списке. Работу расширенных ACL можно сделать более детализированной: можно использовать фильтрацию трафика по следующим критериям:

- протокол
- номера порта
- значение DSCP
- значение приоритета
- состояние бита SYN

Форматы синтаксиса команд расширенных ACL следующие:

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]
```

User Datagram Protocol (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]
```

Справочник по командам ACL см. в разделе Команды IP-служб.

Предварительные условия

Требования

Прежде чем использовать эту конфигурацию, убедитесь, что выполняются следующие требования:

- Имеются основные сведения об IP-адресации

Подробнее см. в разделе IP-адресация и создание подсетей для новых пользователей.

Используемые компоненты

Данный документ не ограничен отдельными версиями программного и аппаратного обеспечения.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в разделе Технические советы Cisco. Условные обозначения.

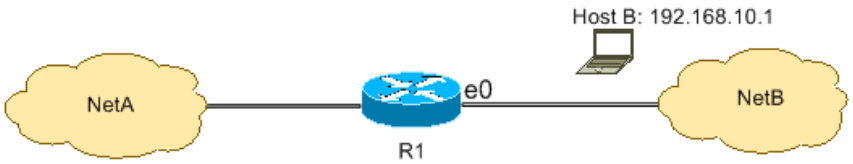
Примеры конфигурации

Следующие примеры конфигурации используют наиболее распространенные ACL для IP.

Примечание: Для поиска дополнительной информации о командах, упоминаемых в данном документе, используйте средство Command Lookup Tool (только для зарегистрированных клиентов).

Разрешение доступа выбранного узла к сети

На данном рисунке показывается, как выбранный узел получает разрешение на доступ в сеть. Весь трафик из узла B, направленный к сети 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. 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 сети 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.

R1

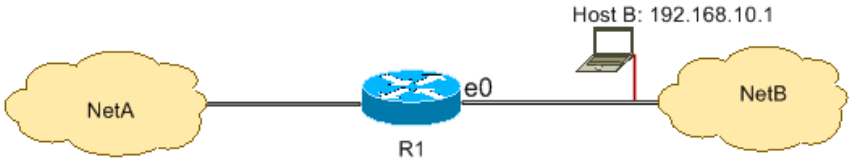
`hostname R1`
`!`
`interface ethernet0`
`ip access-group 1 in`
`!`
`access-list 1 permit host 192.168.10.1`

Примечание: ACL фильтрует IP-пакеты от NetB к NetA – кроме пакетов, исходящих из NetB. Пакеты, направляющиеся в узел B из NetA, разрешаются.

Примечание: другой способ настроить то же самое правило – ACL **access-list 1 permit 192.168.10.1 0.0.0.0**.

Запрет доступа выбранного узла к сети

На данном рисунке показано, как весь трафик из узла B, направленный к NetA, отвергается, в то время как весь другой трафик из NetB, направленный к NetA, разрешается.



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.

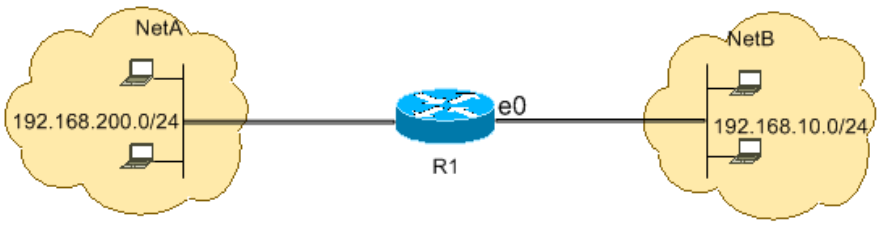
R1
hostname R1 ! interface ethernet0 ip access-group 1 in ! access-list 1 deny host 192.168.10.1 access-list 1 permit any

Примечание: Порядок условий критичен для функционирования списка ACL. Если расположить записи в обратном порядке, как показано в данной команде, первая строка соответствует адресу любого источника пакета, поэтому 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
```

Разрешение доступа к диапазону смежных IP-адресов

На данном рисунке показано, как всем узлам NetB с сетевым адресом 192.168.10.0/24 разрешается доступ к сети 192.168.200.0/24 в NetA.



Эта конфигурация позволяет IP-пакетам, IP-заголовки которых 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.

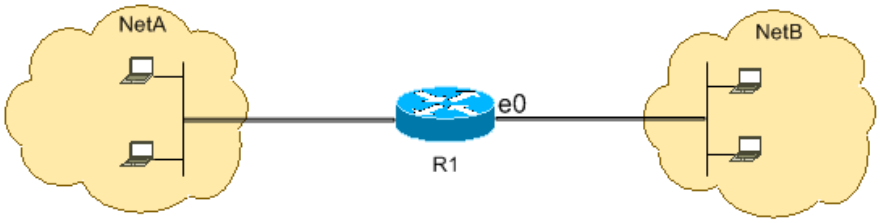
R1
hostname R1 ! interface ethernet0 ip access-group 101 in ! access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.200.0 0.0.0.255

Примечание: В команде **access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.200.0 0.0.0.255** параметр 0.0.0.255 – это 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 соответствия более высоким требованиям безопасности может быть необходимым отключение доступа Telnet к частной сети из публичной. Данный рисунок показывает, как трафик Telnet из сети NetB (публичной), направленный в сеть NetA (частную), отвергается, что позволяет NetA инициировать и установить сеанс Telnet с NetB, при этом разрешая весь другой IP-трафик.

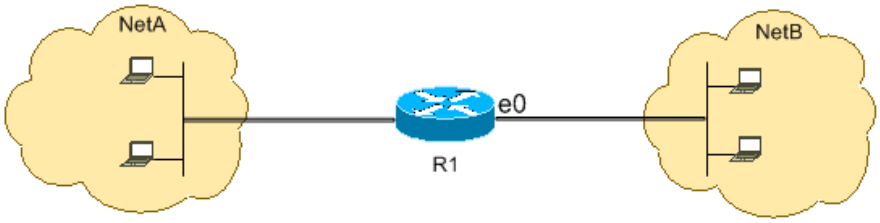


Telnet использует TCP, порт 23. Следующая конфигурация показывает, что весь TCP-трафик, направленный в NetA для порта 23, заблокирован, а остальной IP-трафик разрешен.

R1
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

Разрешение инициировать сеансы TCP только внутренним сетям

На данном рисунке показано, как весь TCP-трафик из NetA, направленный к NetB, разрешается, в то время как TCP-трафик из NetB, направленный к NetA, отвергается.



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 датаграмме проходить через внутренний интерфейс Ethernet 0 на R1, если у нее есть:

- подтвержденный (ACK) или сброшенный (RST) набор данных (указывающий на установленный сеанс TCP);
- значение конечного порта больше 1023.

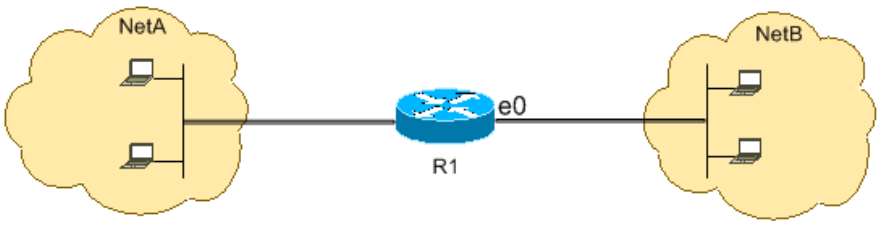
R1
hostname R1 ! interface ethernet0 ip access-group 102 in ! access-list 102 permit tcp any any gt 1023 established

Поскольку большинство портов IP-служб используют значения ниже 1023, все датаграммы с портом назначения, предшествующим 1023, и незаданным битом ACK/RST отклоняются списком ACL 102, поэтому, когда хост из сети NetB инициирует соединение TCP, отправив первый пакет TCP (без установленного бита синхронизации/начального пакета (SYN/RST)) в порт, номер которого меньше 1023, этот пакет будет отвергнут, и сеанс TCP не установится. 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 документе RFC 1700 .

Запрет трафика FTP (TCP, порт 21)

На следующем рисунке показано, что трафик FTP (TCP, порт 21) и данных FTP (порт 20), пересылаемый из NetB в NetA, отвергается, а весь остальной IP-трафик разрешается.



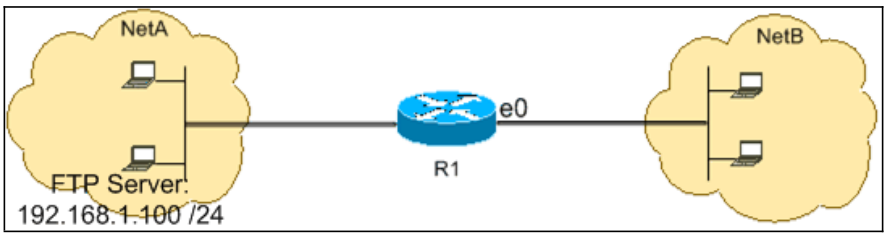
FTP использует порты 21 и 20. Трафик TCP, предназначенный для порта 21 и порта 20, отвергается, а все остальное явным образом разрешается.

R1
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

Разрешение трафика FTP (активного FTP)

FTP может работать в двух различных режимах: активном и пассивном. 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 в сети 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.



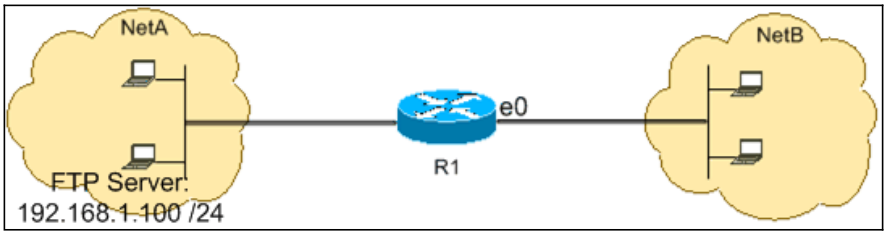
R1

```
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
```

Разрешение трафика FTP (пассивного FTP)

FTP может работать в двух различных режимах: активном и пассивном. 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 в сети 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.



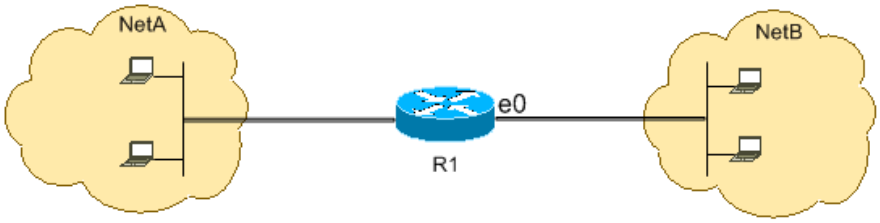
R1

```
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
```

Разрешение эхо-тестирования (ICMP)

На следующем рисунке показано, что трафик ICMP, пересылаемый из NetA в NetB, разрешается, а эхо-тесты из NetB в NetA отвергаются.



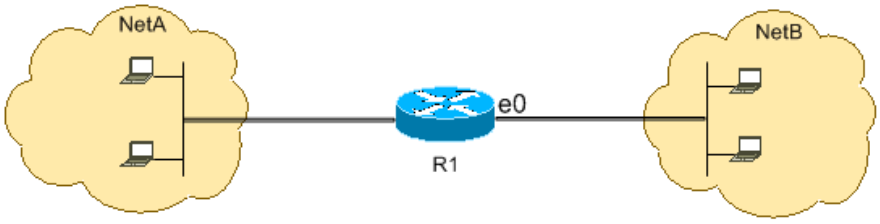
Эта конфигурация разрешает проходить по интерфейсу Ethernet 0 из NetB в NetA только пакетам эхо-ответа (отклика эхо-теста). Конфигурация блокирует все пакеты эхо-запроса ICMP, когда эхо-тесты исходят из NetB и направляются в NetA. Таким образом, узлы в сети NetA могут выполнять эхо-тестирование узлов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

R1

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

Разрешение HTTP, Telnet, Mail, POP3, FTP

На следующем рисунке показывается ситуация, в которой разрешен только трафик по протоколам HTTP, Telnet, SMTP, POP3 и FTP, и запрещен весь остальной трафик, идущий из NetB в NetA.



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.

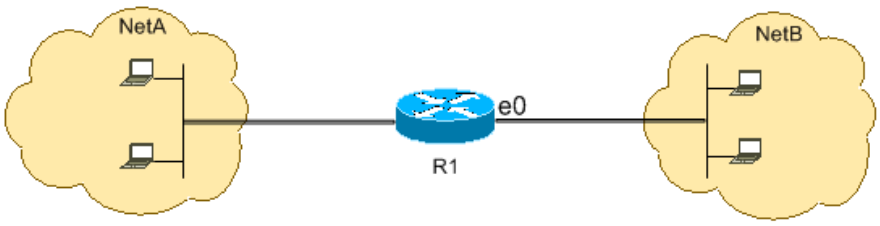
R1

```
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 pop3
access-list 102 permit tcp any any eq 21
access-list 102 permit tcp any any eq 20
```

Разрешение DNS

На следующем рисунке показывается ситуация, в которой разрешен только трафик Domain Name System (DNS), и запрещен весь остальной трафик, идущий из NetB в NetA.



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

R1

```
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
```

Разрешение обновлений маршрутизации

При применении внутреннего ACL к интерфейсу убедитесь, что обновления маршрутизации не отфильтрованы. Используйте необходимые ACL из этого списка, чтобы разрешить пакеты протокола маршрутизации:

Выполните эту команду, чтобы разрешить использование протокола RIP:

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

Выполните эту команду, чтобы разрешить использование протокола IGRP:

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

Выполните эту команду, чтобы разрешить использование протокола EIGRP:

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

Выполните эту команду, чтобы разрешить использование OSPF:

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

Выполните эту команду, чтобы разрешить использование протокола BGP:

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

Отладка трафика с помощью ACL

Использование команд **debug** требует выделения системных ресурсов, например ресурсов памяти и процессора, и в экстремальных ситуациях может привести к зависанию сильно загруженной системы. 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. в разделе Важные сведения о командах отладки.

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

Проверка

Для этой конфигурации отсутствует процедура проверки.

Поиск и устранение неисправностей

Для этой конфигурации отсутствуют данные о поиске и устранении неисправностей.

Дополнительные сведения

- **Настройка списков доступа IP**
- **Страница поддержки списков доступа**
- **Страница поддержки IP-маршрутизации**
- **Страница поддержки маршрутизируемых IP-протоколов**
- **Техническая поддержка и документация – Cisco Systems**