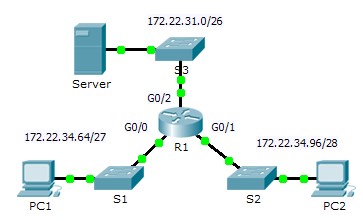
**Packet Tracer. Настройка расширенных списков контроля доступа (ACL). Сценарий 1**

**Топология**



**Таблица адресации**



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Устройство** | **Интерфейс** | **IP-адрес** | **Маска подсети** | **Шлюз по умолчанию** |
| R1 | G0/0 | 172.22.34.65 | 255.255.255.224 | Н/П |
| G0/1 | 172.22.34.97 | 255.255.255.240 | Н/П |
| G0/2 | 172.22.34.1 | 255.255.255.192 | Н/П |
| Сервер | NIC | 172.22.34.62 | 255.255.255.192 | 172.22.34.1 |
| PC1 | NIC | 172.22.34.66 | 255.255.255.224 | 172.22.34.65 |
| PC2 | NIC | 172.22.34.98 | 255.255.255.240 | 172.22.34.97 |

**Задачи**

**Часть 1. Настройка, применение и проверка расширенного нумерованного списка ACL**

**Часть 2. Настройка, применение и проверка расширенного именованного списка ACL**

**Исходные данные/сценарий**

Двум сотрудникам требуется доступ к сервисам, которые предоставляет сервер. Компьютеру PC1 нужен только FTP-доступ, а компьютеру PC2 – только веб-доступ. Оба компьютера могут отправлять эхо-запросы серверу, но не друг другу.

# Часть 1: Настройка, применение и проверка расширенного нумерованного списка ACL

**Шаг 1: Настройте список ACL, разрешающий трафик FTP и ICMP.**

1. На маршрутизаторе R1 введите следующую команду в режиме глобальной настройки, чтобы определить первый допустимый номер для расширенного списка контроля доступа.

R1(config)# **access-list ?**

<1-99> IP standard access list

<100-199> IP extended access list

1. Добавьте в команду число **100** изатем вопросительный знак.

R1(config)# **access-list 100 ?** deny Specify packets to reject permit Specify packets to forward remark Access list entry comment

1. Чтобы разрешить трафик FTP, введите **permit** изатем вопросительный знак.

R1(config)# **access-list 100 permit ?**  ahp Authentication Header Protocol eigrp Cisco's EIGRP routing protocol esp Encapsulation Security Payload gre Cisco's GRE tunneling icmp Internet Control Message Protocol ip Any Internet Protocol ospf OSPF routing protocol tcp Transmission Control Protocol udp User Datagram Protocol

1. Этот список ACL разрешает трафик FTP и ICMP. ICMP указан выше, а FTP – нет, так как FTP использует TCP.

Поэтому введите **tcp**, чтобы уточнить справку по ACL.

R1(config)# **access-list 100 permit tcp ?**

A.B.C.D Source address any Any source host host A single source host

1. Обратите внимание, что можно было бы выполнить фильтрацию только по **PC1** с помощью ключевого слова **host** либо разрешить любой хост (**any** host). В данном случае разрешен трафик любого устройства с адресом в сети 172.22.34.64/27. Введите сетевой адрес, а затем вопросительный знак.

R1(config)# **access-list 100 permit tcp 172.22.34.64 ?**

A.B.C.D Source wildcard bits

1. Рассчитайте шаблонную маску как двоичную противоположность маски подсети.

11111111.11111111.11111111.11100000 = 255.255.255.224

00000000.00000000.00000000.00011111 = 0.0.0.31

1. Введите шаблонную маску и затем вопросительный знак.

R1(config)# **access-list 100 permit tcp 172.22.34.64 0.0.0.31 ?**

A.B.C.D Destination address any Any destination host

eq Match only packets on a given port number gt Match only packets with a greater port number host A single destination host lt Match only packets with a lower port number neq Match only packets not on a given port number range Match only packets in the range of port numbers

1. Настройте адрес назначения. В этом сценарии выполняется фильтрация трафика для одного адреса назначения (сервера). Введите ключевое слово **host**, а затем IP-адрес сервера.

R1(config)# **access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 ?**

dscp Match packets with given dscp value eq Match only packets on a given port number established established gt Match only packets with a greater port number lt Match only packets with a lower port number neq Match only packets not on a given port number precedence Match packets with given precedence value range Match only packets in the range of port numbers

<cr>

1. Обратите внимание, что один из параметров – **<cr>** (символ возврата каретки). Другими словами, вы можете нажать **Enter**, и оператор разрешит весь трафик TCP. Однако мы разрешаем только трафик FTP; поэтому введите ключевое слово **eq** и знак вопроса, чтобы отобразить доступные варианты. Затем введите **ftp** инажмите **Enter**.

R1(config)# **access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ?**

<0-65535> Port number ftp File Transfer Protocol (21) pop3 Post Office Protocol v3 (110) smtp Simple Mail Transport Protocol (25) telnet Telnet (23)

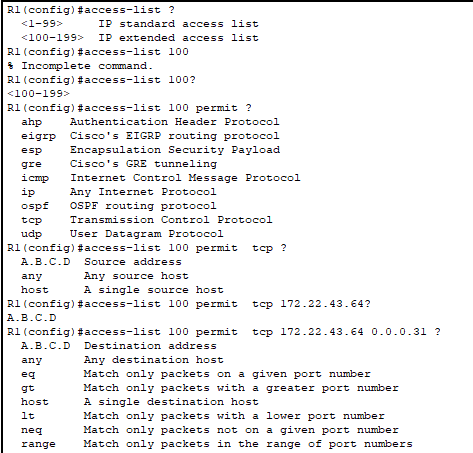
www World Wide Web (HTTP, 80)

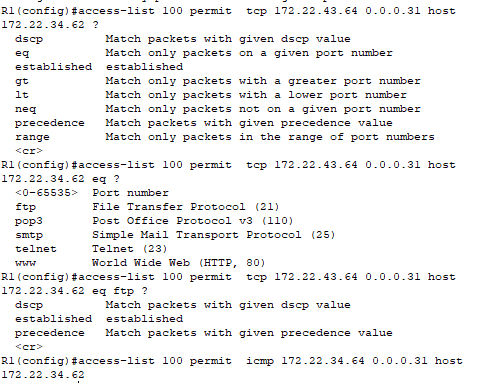
R1(config)# **access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp**

1. Создайте второй список контроля доступа, разрешающий трафик ICMP (эхо-запросы и т. п.) с компьютера **PC1** на сервер **Server.** Обратите внимание, что номер списка контроля доступа остается прежним и что не нужно указывать конкретный тип трафика ICMP.

R1(config)# **access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62**

1. Весь прочий трафик отклоняется по умолчанию.





**Шаг 2: Примените список ACL на нужном интерфейсе для фильтрации трафика.**

С точки зрения маршрутизатора **R1** трафик, к которому применяется список ACL 100, поступает из сети, подключенной к интерфейсу Gigabit Ethernet 0/0. Войдите в режим интерфейсной настройки и примените список ACL.

R1(config)# **interface gigabitEthernet 0/0**

R1(config-if)# **ip** **access-group 100 in**

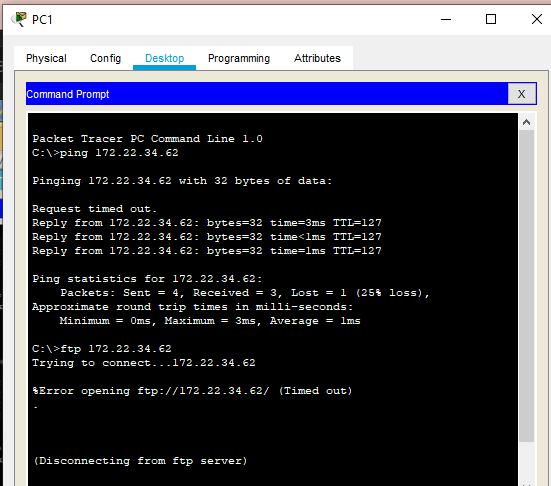


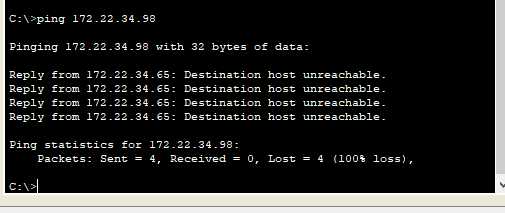
**Шаг 3: Проверьте реализацию списка ACL.**

* 1. Отправьте эхо-запрос с компьютера **PC1** на сервер **Server**. Если эхо-запросы завершаются неудачно, проверьте IP-адреса, прежде чем продолжить.
  2. Установите FTP-подключение с компьютера **PC1** к серверу **Server**. Имя пользователя и пароль **cisco**.

PC> **ftp 172.22.34.62**

* 1. Выйдите из FTP-сервиса сервера **Server**. ftp> **quit**
  2. Отправьте эхо-запрос с компьютера **PC1** на компьютер **PC2**. Хост назначения должен быть недоступен, потому что трафик не был явно разрешен.





# Часть 2: Настройка, применение и проверка расширенного именованного списка ACL

**Шаг 1: Настройте список ACL, разрешающий доступ по протоколам HTTP и ICMP.**

1. Именованные списки ACL начинаются с ключевого слова **ip**. На маршрутизаторе **R1** введите следующую команду и затем вопросительный знак.

R1(config)# **ip** **access-list ?**

extended Extended Access List standard Standard Access List

1. Можно настроить именованные стандартные и расширенные списки ACL. Этот список контроля доступа выполняет фильтрацию по IP-адресам источника и назначения, поэтому он должен быть расширенным.

Введите имя **HTTP\_ONLY**. (Для оценки в Packet Tracer имя вводится с учетом регистра.)

R1(config)# **ip** **access-list extended HTTP\_ONLY**

1. Строка приглашения изменит вид. Теперь вы находитесь в режиме настройки расширенного именованного списка ACL. Всем устройствам в локальной сети **PC2** требуется доступ по TCP. Введите сетевой адрес, а затем вопросительный знак.

R1(config-ext-nacl)# **permit tcp 172.22.34.96 ?**

A.B.C.D Source wildcard bits

1. Альтернативный способ вычислить шаблонную маску – вычесть маску подсети из 255.255.255.255.

255.255.255.255

- 255.255.255.240

-----------------

= 0. 0. 0. 15

R1(config-ext-nacl)# **permit tcp 172.22.34.96 0.0.0.15 ?**

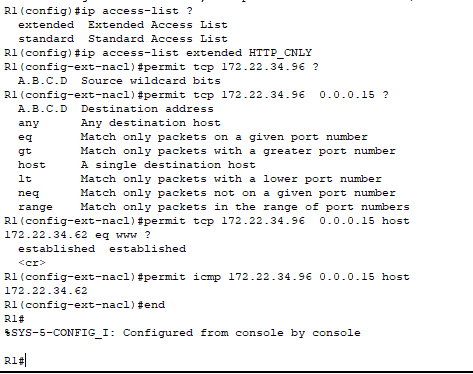
1. Закончите оператор, указав адрес сервера, как в части 1, и отфильтровав трафик **www**.

R1(config-ext-nacl)# **permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www**

1. Создайте второй список контроля доступа, разрешающий трафик ICMP (эхо-запросы и т. п.) с компьютера **PC2** на сервер **Server.** Примечание. Командная строка останется прежней, и конкретный тип трафика ICMP указывать не нужно..

R1(config-ext-nacl)# **permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62**

1. Весь прочий трафик отклоняется по умолчанию. Выйдите из режима настройки расширенного именованного списка ACL.



**Шаг 2: Примените список ACL на нужном интерфейсе для фильтрации трафика.**

С точки зрения маршрутизатора **R1** трафик, к которому применяется список контроля доступа **HTTP\_ONLY**, поступает из сети, подключенной к интерфейсу Gigabit Ethernet 0/1. Войдите в режим интерфейсной настройки и примените список ACL.

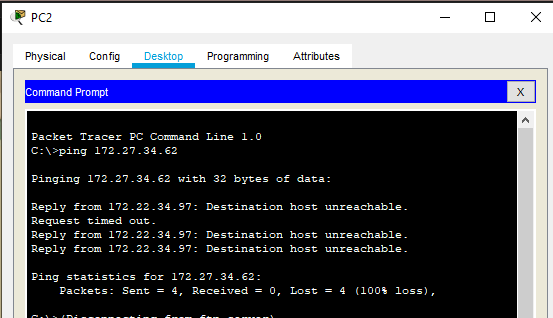
R1(config)# **interface gigabitEthernet 0/1**

R1(config-if)# **ip** **access-group HTTP\_ONLY in**

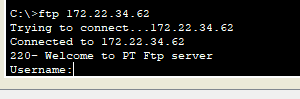


**Шаг 3: Проверьте реализацию списка ACL.**

1. Отправьте эхо-запрос с компьютера **PC2** на сервер **Server**. Эхо-запрос должен завершиться успешно, в противном случае проверьте IP-адреса, прежде чем продолжить.



1. Установите FTP-подключение с компьютера **PC2** к серверу **Server**. Должен произойти сбой подключения.





1. Откройте браузер на компьютере **PC2** ивведите IP-адрес сервера **Server.** Подключение должно быть установлено успешно.

