Packet Tracer. Настройка расширенных списков контроля доступа. Сценарий 1

# Таблица адресации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Устройство | Интерфейс | IP-адрес | Маска подсети | Шлюз по умолчанию |
| R1 | G0/0 | 172.22.34.65 | 255.255.255.224 | — |
| R1 | G0/1 | 172.22.34.97 | 255.255.255.240 | — |
| R1 | G0/2 | 172.22.34.1 | 255.255.255.192 | — |
| Server | 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 контроля доступа

Часть 2. Настройка, применение и проверка расширенного именованного списка контроля доступа

# Общие сведения/сценарий

Двум сотрудникам предприятия требуется доступ к сервисам, предоставляемым этим сервером. Узлу **PC1** требуется доступ только по FTP, а узлу **PC2** — только доступ в Интернет. Оба компьютера могут получать отчеты на ping-запросы к серверу, но не друг к другу.

# Инструкции

## Настройка, применение и проверка расширенного нумерованного ACL-списка

### Настройте ACL-список на разрешение FTP и ICMP с PC1 LAN.

* + - 1. В режиме глобальной конфигурации на маршрутизаторе **R1** введите следующую команду, чтобы определить первый действительный номер для расширенного списка контроля доступа.

Откройте окно конфигурации

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

<1-99> IP standard access list

<100-199> IP extended access list

* + - 1. Добавьте **100** к команде, а затем поставьте 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 команду **permit** с вопросительным знаком.

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. При настройке и применении этот ACL должен разрешать FTP и ICMP. Протокол ICMP входит в этот список, а протокол FTP — нет. Это связано с тем, что FTP является протоколом уровня приложений, который использует TCP на транспортном уровне. Введите TCP, чтобы уточнить подсказку списка контроля доступа.

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

A.B.C.D Source address

any Any source host

host A single source host

* + - 1. Адрес источника может представлять одно устройство, например PC1, используя ключевое слово **host** , а затем IP-адрес PC1. Использование ключевого слова **any** разрешает любой хост в любой сети. Фильтрацию также можно выполнить по сетевому адресу. В этом случае это любой хост, который имеет адрес, принадлежащий сети 172.22.34.64/27. Введите сетевой адрес со знаком вопроса в конце.

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

A.B.C.D Source wildcard bits

* + - 1. Рассчитайте шаблонную маску, определяющую двоичную противоположность /27 маски подсети.

**11111111.11111111.11111111.111**00000 = 255.255.255.224

00000000.00000000.00000000.000**11111** = 0.0.0.31

* + - 1. Введите сетевой адрес, а после него — знак вопроса.

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 места назначения. В этом сценарии мы фильтруем трафик для единственного места назначения — сервера. Введите ключевое слово host, а после него — 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 на параметр **<cr>** (возврат каретки). Другими словами, вы можете нажать клавишу **ВВОД**, и согласно правилу будет разрешен весь трафик TCP. Однако мы хотим разрешить только трафик FTP. Поэтому введите ключевое слово **eq**, после которого поставьте вопросительный знак, чтобы отобразить доступные параметры. Затем введите **ftp** и нажмите клавишу **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 вторую запись списка контроля доступа, разрешающую передачу трафика ICMP (ping-запрос и др.) от PC1 на Server. Обратите внимание, что номер списка контроля доступа остается прежним и нет необходимости 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. Остальной трафик запрещен по умолчанию.
      2. Выполните команду **show access-list** и убедитесь, что список доступа 100 содержит правильные инструкции. Обратите внимание, что инструкция **deny any** не отображается в конце списка доступа. Выполнение списка доступа по умолчанию заключается в том, что если пакет не соответствует инструкции в списке доступа, он не разрешен через интерфейс.

R1#**show access-lists**

Extended IP access list 100

10 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp

20 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62

### Примените этот список контроля доступа на соответствующем интерфейсе, чтобы фильтровать трафик.

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

Примечание. В реальной операционной сети не рекомендуется применять непроверенный список доступа к активному интерфейсу.

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

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

### Проверьте работу списка контроля доступа.

* + - 1. Отправьте ping-запрос с PC1 на Server. Если ответов на ping-запросы нет, проверьте IP-адреса перед тем, как продолжить.
      2. Отправьте FTP-трафик от PC1 на Server. Имя пользователя и пароль — **cisco**.

PC> **ftp 172.22.34.62**

* + - 1. Выход из службы FTP.

ftp> **quit**

Закройте окно настройки.

* + - 1. Пощлите эхо-запрос от PC1 к PC2. Хост назначения должен быть недоступен, поскольку ACL явно не разрешает трафик.

## Настройка, применение и проверка расширенного именованного ACL-списка

### Настройте список контроля доступа на разрешение доступа по протоколу HTTP и ICMP с PC2 LAN..

* + - 1. Именованные списки контроля доступа начинаются с ключевого слова **ip**. В режиме глобальной настройки маршрутизатора **R1** введите следующую команду, после которой поставьте вопросительный знак.

Откройте окно конфигурации

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

extended Extended Access List

standard Standard Access List

* + - 1. Можно настроить именованные стандартные и расширенные ACL-списки. Посредством этого списка доступа фильтруются как IP-адреса источника, так и IP-адреса узла-назначения; таким образом, список должен быть расширенным. Введите **HTTP\_ONLY** в качестве имени. (Для определения рейтинга Packet Tracer имя чувствительно к регистру, а инструкции списка доступа должны быть в правильном порядке.)

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

* + - 1. Командная строка изменится. Теперь активирован режим настройки именованного расширенного ACL-списка. Всем устройствам в локальной сети хоста **PC2** требуется доступ по TCP. Введите сетевой адрес со знаком вопроса в конце.

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

A.B.C.D Source wildcard bits

* + - 1. Другой способ расчета шаблонной маски заключается в вычитании маски 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. Допишите правило, определив адрес сервера как в части 1 и настроив фильтрацию трафика **www**.

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

* + - 1. Создайте вторую запись списка контроля доступа, разрешающую передачу трафика ICMP (ping-запрос и др.) от **PC2** на **Server.** Примечание. Приглашение остается прежним, и нет необходимости указывать конкретный тип трафика ICMP.

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

* + - 1. Остальной трафик запрещен по умолчанию. Выход из расширенного именованного режима конфигурации ACL.
      2. Выполните команду **show access-list** и убедитесь, что список доступа **HTTP\_ONLY** содержит правильные инструкции.

R1# **show access-lists**

Extended IP access list 100

10 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp

20 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62

Extended IP access list HTTP\_ONLY

10 permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www

20 permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62

### Примените этот список контроля доступа на соответствующем интерфейсе, чтобы фильтровать трафик.

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

В реальной операционной сети не рекомендуется применять непроверенный список доступа к активному интерфейсу. Этого следует избегать, если это возможно.

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

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

### Проверьте работу списка контроля доступа.

* + - 1. Отправьте ping-запрос с **PC2** на **Server**. Если ответы на ping-запросы не приходят, проверьте IP-адреса.
      2. С PC2 откройте веб-браузер и введите IP-адрес Сервера. Должна быть отображена веб-страница Сервера.
      3. Отправьте FTP-трафик от **PC2** на **Server**. Подключение не должно быть успешным. Если нет, устраняйте инструкции списка доступа и конфигурации групп доступа на интерфейсах.

Закройте окно настройки.

Конец документа