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	—
	G0/1	172.22.34.97	255.255.255.240	
	G0/2	172.22.34.1	255.255.255.192	
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 контроля доступа

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

Общие сведения и 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

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

Шаг 1: Настройка ACL для разрешения FTP и ICMP из локальной сети PC1.

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

```
R1(config)# access-list ?
<1-99> IP standard access list
<100-199> IP extended access list
```

б. 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
```

в. 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
```

г. 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 приложения , использующим 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
```

д. Исходный адрес может представлять одно устройство, например PC1, используя ключевое слово **host**, а затем IP-адрес PC1. Использование ключевого слова **any** позволяет любому хосту в любой сети. Фильтрация также может быть выполнена 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
```

е. Рассчитайте шаблонную маску, определяющую двоичную противоположность маски подсети /27.

11111111.11111111.11111111.11100000 = 255.255.255.224
00000000.00000000.00000000.000**11111** = 0.0.0.31

ж. 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
```

з. Настройте адрес узла-назначения. В этом сценарии мы фильтруем трафик для единственного места назначения — сервера. Введите ключевое слово , 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
```

и. Обратите внимание на параметр (возврат каретки). Другими словами, вы можете нажать клавишу **Enter** (Ввод). Эта запись разрешит 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
```

к. 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
```

л. Остальной трафик запрещен по умолчанию.

м. Выполните команду **show access-list** и убедитесь, что список доступа 100 содержит правильные инструкции. Обратите внимание, что инструкция **deny any 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
```

```
R1>enable
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
R1(config)#access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show access-list
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

R1#
```

Шаг 2.Применение списка контроля доступа на соответствующем интерфейсе для фильтрации трафика.

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.

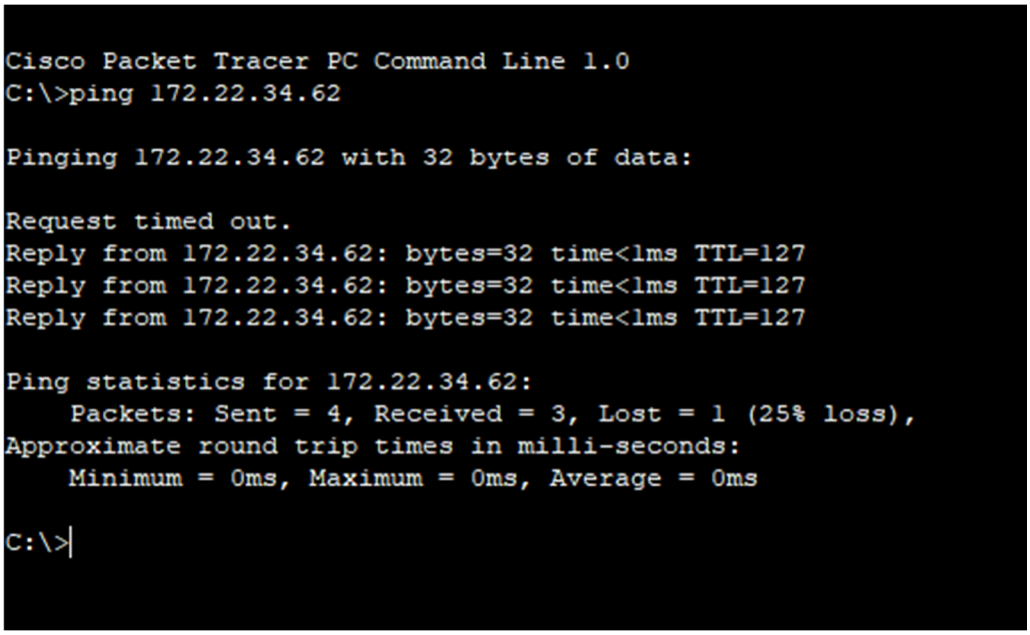
Примечание. В реальной операционной сети применение непроверенного списка доступа к активному интерфейсу не рекомендуется.

```
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ip access-group 100 in
```

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ip access-group 100 in
R1(config-if)#
```

Шаг 3.Проверка реализации списка контроля доступа.

a. Отправьте ping-запрос с PC1 на Server. Если ответов на ping-запросы нет, проверьте IP-адреса перед тем, как продолжить.



б. FTP с PC1 на сервер. Имя пользователя и пароль — **cisco**.

```
PC> ftp 172.22.34.62
```

в. Выйдите из службы FTP.

```
ftp> quit
```

г. Запустите Ping от PC1 до PC2. Хост назначения должен быть недоступен, поскольку ACL явно не разрешает трафик.

```
Pinging 172.22.34.62 with 32 bytes of data:

Request timed out.
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127

Ping statistics for 172.22.34.62:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ftp 172.22.34.62
Trying to connect...172.22.34.62
Connected to 172.22.34.62
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:

%Error ftp://172.22.34.62/ (No such Account)
332- Need account for login




C:\>ftp 172.22.34.62
Trying to connect...172.22.34.62
Connected to 172.22.34.62
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>quit

221- Service closing control connection.
C:\>ping 172.22.34.66

Pinging 172.22.34.66 with 32 bytes of data:

Reply from 172.22.34.66: bytes=32 time<1ms TTL=128
Reply from 172.22.34.66: bytes=32 time=14ms TTL=128
Reply from 172.22.34.66: bytes=32 time=17ms TTL=128
Reply from 172.22.34.66: bytes=32 time=14ms TTL=128

Ping statistics for 172.22.34.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 17ms, Average = 11ms

C:\>
```

Часть 2. Настройка, применение и проверка расширенного именованного ACL

Шаг 1: Настройка ACL для разрешения доступа HTTP и ICMP из локальной сети PC2.

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

```
R1(config)# ip access-list ?
extended Extended Access List
standard Standard Access List
```

б. 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 оценки Packet Tracer имя чувствительно к регистру, а инструкции списка доступа должны быть правильным.)

```
R1(config)# ip access-list extended HTTP_ONLY
```

в. 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
```

г. 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
```

д. 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
```

е. 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
```

ж. Остальной трафик запрещен по умолчанию. Выход из расширенного именованного режима конфигурации ACL.

з. 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
```

```
R1>enable
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
R1(config)#access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show access-list
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

R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ip access-group 100 in
R1(config-if)#exit
R1(config)#ip access-list extended HTTP_ONLY
R1(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
R1(config-ext-nacl)#permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
R1(config-ext-nacl)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

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 (19 match(es))
    20 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62 (4 match(es))
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

R1#
```

Шаг 2.Применение списка контроля доступа на соответствующем интерфейсе для фильтрации трафика.

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.

Примечание. В реальной операционной сети применение непроверенного списка доступа к активному интерфейсу не рекомендуется. Его следует избегать, если это возможно.

```
R1(config)# interface gigabitEthernet 0/1
R1(config-if)# ip access-group HTTP_ONLY in
```

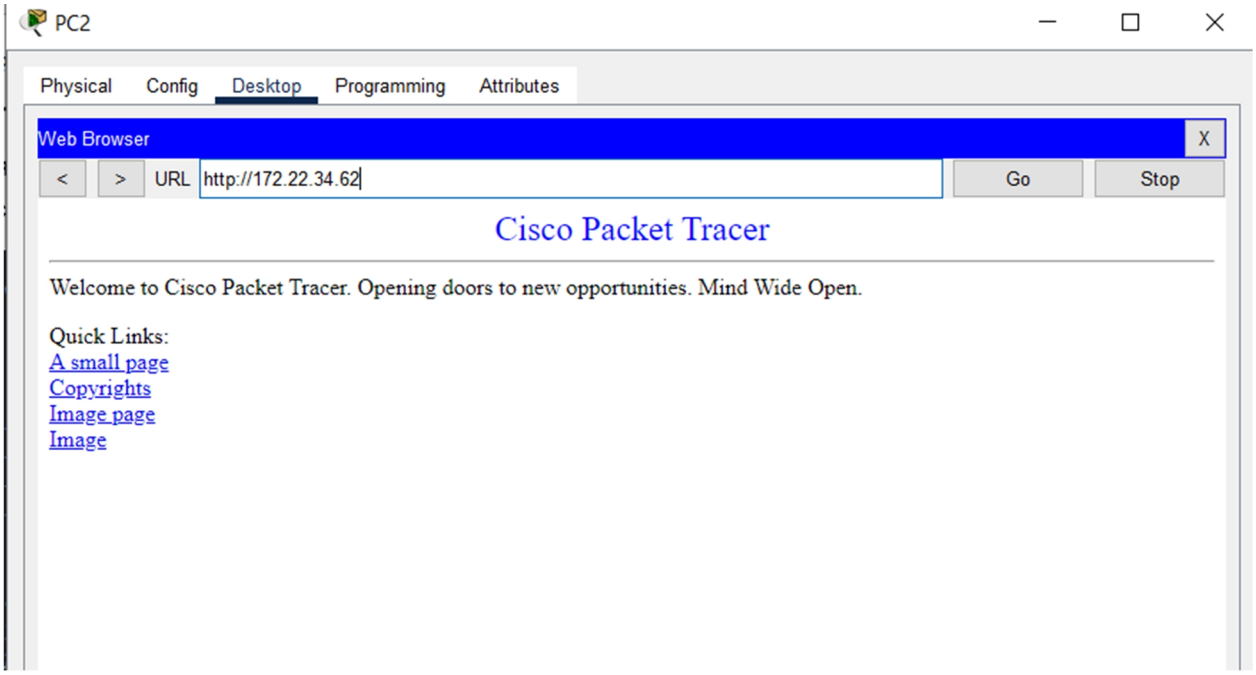
```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int g 0/1
R1(config-if)#ip access-group HTTP_ONLY
% Incomplete command.
R1(config-if)#ip access-group HTTP_ONLY in
R1(config-if)#
```

Шаг 3.Проверка реализации списка контроля доступа.

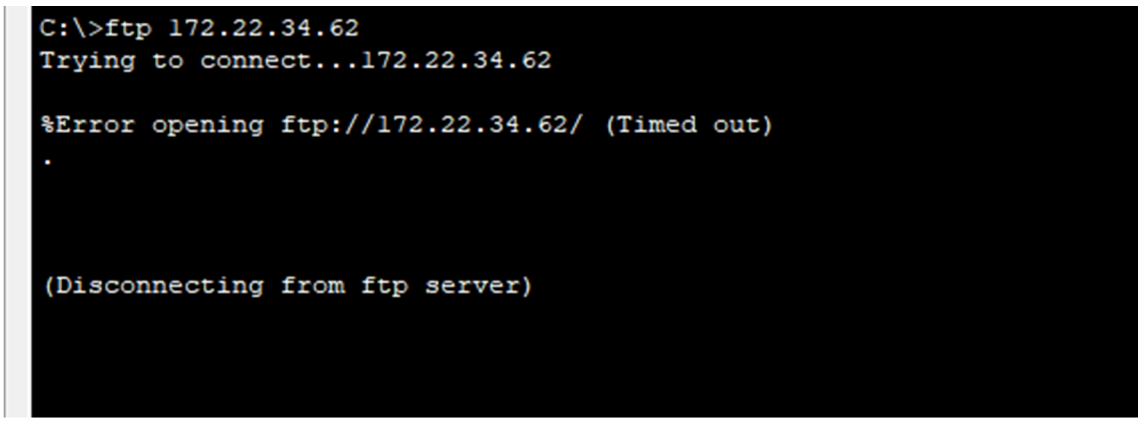
а. Отправьте ping-запрос с PC2 на Server. Если ответы на ping-запросы не приходят, проверьте IP-адреса.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.22.34.62

Pinging 172.22.34.62 with 32 bytes of data:

Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127

Ping statistics for 172.22.34.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

б. С PC2 откройте веб-браузер и введите IP-адрес Сервера. Должна быть отображена веб-страница Сервера.



в. FTP с PC2 на сервер. Подключение не должно быть успешным. Если нет, то устраните проблемы с инструкциями списка доступа и конфигурациями групп доступа на интерфейсах.


C:\>ftp 172.22.34.62
Trying to connect...172.22.34.62
%Error opening ftp://172.22.34.62/ (Timed out)
.
(Disconnecting from ftp server)