

Packet Tracer - Наглядное представление работы списка контроля доступа

Задачи

Часть 1. Проверка локального подключения и тестирование работы списка контроля доступа

Часть 2. Удаление списка контроля доступа и проверка подключения

Общие сведения

В рамках этого задания вы получите представление о том, как можно использовать список контроля доступа (ACL) для запрещения ping-запросов, отправленных на хосты удаленных сетей. После удаления ACL-списка из конфигурации ping-запросы будут успешными.

Таблица адресации

Устройство	Интерфейс	IP адрес/префикс
R1	G0/0	192.168.10.1/24
	G0/1	192.168.11.1/24
	S0/0/0	10.1.1.1/30
R2	S0/0/0	10.10.1.2/30
	S0/0/1	10.10.1.5/30
R3	G0/0	192.168.30.1/24
	G0/1	192.168.31.1/24
	S0/0/1	10.10.1.6/24
PC1	NIC	192.168.10.10/24
PC2	NIC	192.168.10.11/24
PC3	NIC	192.168.11.10/24
PC4	NIC	192.168.30.12/24
DNS Server	NIC	192.168.31.12/24

Инструкция

Часть 1: Проверка локального подключения и проверка списка управления доступом

Шаг 1: Ping устройств в локальной сети для проверки подключения.

- Из командной строки **PC1** отправьте ping-запрос на **PC2**.

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:

Reply from 192.168.10.11: bytes=32 time=6ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 1ms

C:\>A|

```

- б. Из командной строки узла **PC1** отправьте эхо-запрос на **PC3**.

```

C:\>ping 192.168.11.10

Pinging 192.168.11.10 with 32 bytes of data:

Reply from 192.168.11.10: bytes=32 time<1ms TTL=127
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.11.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

Почему ping-запросы прошли успешно?

PC1 и PC2 в одной сети, PC1 и PC3 находятся в разных сетях, но маршрутизатор доставляет пакет в другую сеть

Шаг 2. Отправьте ping-запросы в удаленные сети, чтобы протестировать работу списка контроля доступа.

- а. Из командной строки **PC1** отправьте ping-запрос на **PC4**.

```

C:\>ping 192.168.30.12

Pinging 192.168.30.12 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.30.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>

```

- б. Из командной строки узла **PC1** отправьте эхо-запрос на **DNS-сервер**.

```
C:\>ping 192.168.31.12

Pinging 192.168.31.12 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.31.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Почему возникает сбой при отправке ping-запросов? (Подсказка. Для анализа используйте режим моделирования или просмотрите конфигурации маршрутизатора.)
У маршрутизатора нет пути до другой сети

Часть 2. Удалите ACL и повторите тест.

Шаг 1: Используйте команды show для изучения конфигурации ACL.

- а. Перейдите к интерфейсу командной строки R1. Используйте команды **show run** и **show access-lists**, чтобы просмотреть текущие ACL-списки. Для быстрого просмотра текущих ACL-списков используйте команду **show access-lists**. Введите команду **show access-lists**, после которой нажмите ПРОБЕЛ и поставьте вопросительный знак (?), чтобы просмотреть доступные параметры.

```
R1# show access-lists ?
<1-199> ACL number
Имя ACL-списка СЛОВО
```

Если вы знаете номер или имя ACL-списка, вы можете дополнительно отфильтровать выходные данные команды **show**. Однако на маршрутизаторе **R1** применен только один ACL-список, поэтому будет достаточно команды **show access-lists**.

```
R1#show access-lists
Standard IP access list 11
10 deny 192.168.10.0 0.0.0.255
20 permit any
```

Первая строка ACL блокирует любые пакеты, которые исходят из сети **192.168.10.0/24**, которая включает в себя эхо-сигналы протокола управления сообщениями Интернета (ICMP) (запросы ping). Вторая строка списка контроля доступа разрешает прохождение через маршрутизатор всего **остального трафика по протоколу IP** от **любого** источника.

```
R1#show access-lists
Standard IP access list 11
 10 deny 192.168.10.0 0.0.0.255 (11 match(es))
 20 permit any
```

- б. Для того чтобы список контроля доступа влиял на работу маршрутизатора, он должен быть применен к интерфейсу в определенном направлении. В этом сценарии список контроля доступа используется для фильтрации исходящего трафика на интерфейсе. Поэтому весь трафик, покидающий указанный интерфейс на маршрутизаторе R1, будет проверяться на соответствие списку ACL 11.

Несмотря на возможность просмотра сведений об IP с помощью команды **show ip interface**, в некоторых случаях эффективнее использовать команду **show run**. Чтобы получить полный список интерфейсов, к которым может применяться ACL, и список всех настроенных списков ACL, используйте следующую команду:

```
R1# show run | include interface|access
interface GigabitEthernet0/0
interface GigabitEthernet0/1
```

```

interface Serial0/0/0
ip access-group 11 out
interface Serial0/0/1
interface Vlan1
access-list 11 deny 192.168.10.0 0.0.0.255
access-list 11 permit any

```

Второй символ канала '|' создает условие OR, соответствующее интерфейсу 'OR 'access'. Важно, чтобы в условии OR не включались пробелы. Используйте одну или обе из этих команд для поиска сведений о ACL.

К какому интерфейсу и в каком направлении применяется ACL?

От S0/0/0 R1

Шаг 2. Удаление списка контроля доступа 11 из конфигурации

ACL-списки можно удалить из конфигурации, применив команду **no access list** [номер ACL-списка]. Команда **no access-list** при использовании без аргументов удаляет все списки ACL, настроенные на маршрутизаторе. Команда **no access-list** [номер ACL-списка] удаляет только указанный список контроля доступа. Удаление списка ACL с маршрутизатора не приводит к удалению списка ACL из интерфейса. Команда, применяющая ACL к интерфейсу, должна быть удалена отдельно.

- Для интерфейса Serial0/0/0 удалите список контроля доступа 11, который был ранее применен к интерфейсу в качестве **исходящего** фильтра.

```

R1(config)# interface s0/0/0
R1(config-if)# no ip access-group 11 out

```

- В режиме глобальной конфигурации удалите ACL-список, применив следующую команду:

```

R1(config)# no access-list 11

R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int s0/0/0
R1(config-if)#no ip access-group 11
% Incomplete command.
R1(config-if)#no ip access-group 11
% Incomplete command.
R1(config-if)#exit
R1(config)#no access-list 11
      ^
% Invalid input detected at '^' marker.

R1(config)#no access-list 11
R1(config)#int s0/0/0
R1(config-if)#no ip access-group 11
% Incomplete command.
R1(config-if)#no ip access-group ?
<1-199>  IP access list (standard or extended)
WORD      Access-list name
R1(config-if)#no ip access-group 11
% Incomplete command.
R1(config-if)#

```

- Убедитесь, что теперь ping-запросы с компьютера **PC1** успешно достигают **DNS-сервера** и **PC4**.

```
Pinging 192.168.31.12 with 32 bytes of data:

Request timed out.
Reply from 192.168.31.12: bytes=32 time=2ms TTL=125
Reply from 192.168.31.12: bytes=32 time=2ms TTL=125
Reply from 192.168.31.12: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.31.12:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
```