Packet Tracer. Настройка именованных стандартных списков контроля доступа (ACL) IPv4.

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	F0/0	192.168.10.1	255.255.255.0	—
	F0/1	192.168.20.1	255.255.255.0	
	E0/0/0	192.168.100.1	255.255.255.0	
	E0/1/0	192.168.200.1	255.255.255.0	
File Server	NIC	192.168.200.100	255.255.255.0	192.168.200.1
Web server	NIC	192.168.100.100	255.255.255.0	192.168.100.1
PC0	NIC	192.168.20.3	255.255.255.0	192.168.20.1
PC1	NIC	192.168.20.4	255.255.255.0	192.168.20.1
PC2	NIC	192.168.10.3	255.255.255.0	192.168.10.1

Задачи

Часть 1. Настройка и применение стандартного именованного списка контроля доступа

Часть 2. Проверка реализации списка контроля доступа

Общие сведения/сценарий

Старший сетевой администратор попросил вас создать стандартный именованный список контроля доступа (ACL) для запрета доступа к файловому серверу. Файловый сервер содержит базу данных для веб-приложений. Доступ к файловому серверу требуется только рабочая станция Web Manager PC1 и веб-сервер. Весь остальной трафик файлового сервера должен быть отклонен.

Инструкция

Часть 1. Настройка и применение именованного стандартного ACL

Шаг 1: Проверка подключения до настройки и применения ACL.

Проверка связи всех трех рабочих станций с **Web Server** и **File Server** с помощью утилиты ping должна выполняться успешно.

Шаг 2. Настройте стандартный именованный список контроля доступа.

a. Настройте следующий именованный ACL-список на маршрутизаторе **R1**.

```
R1(config)# ip access-list standard File_Server_Restrictions
R1(config-std-nacl)# permit host 192.168.20.4
R1(config-std-nacl)# permit host 192.168.100.100
R1(config-std-nacl)# deny any
```

Примечание. Для целей оценки имя ACL чувствительно к регистру, и инструкции должны быть в том же порядке, как показано на рисунке.

б. Используйте команду **show access-lists** для проверки содержимого списка доступа перед его применением к интерфейсу. Убедитесь, что вы не ввели неправильные IP-адреса и что инструкции находятся в правильном порядке.

```
R1# show access-lists
Standard IP access list File_Server_Restrictions
10 permit host 192.168.20.4
20 permit host 192.168.100.100
30 deny any
```

```
R1>enable
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip access-list standard File_Server_Restrictions
R1(config-std-nacl)#permit host 192.168.20.4
R1(config-std-nacl)#permit host 192.168.100.100
R1(config-std-nacl)#deny any
R1(config-std-nacl)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show access-lists
Standard IP access list File_Server_Restrictions
    10 permit host 192.168.20.4
    20 permit host 192.168.100.100
    30 deny any

R1#
```

Шаг 3. Примените именованный список контроля доступа.

а. Примените ACL-список к исходящему трафику на интерфейсе Fast Ethernet 0/1.

Примечание. В реальной операционной сети применение списка доступа к активному интерфейсу не является хорошей практикой, и его следует избегать, если это возможно.

```
R1(config-if)# ip access-group File_Server_Restrictions out
```

б. Сохраните конфигурацию.

Часть 2. Проверка реализации ACL.

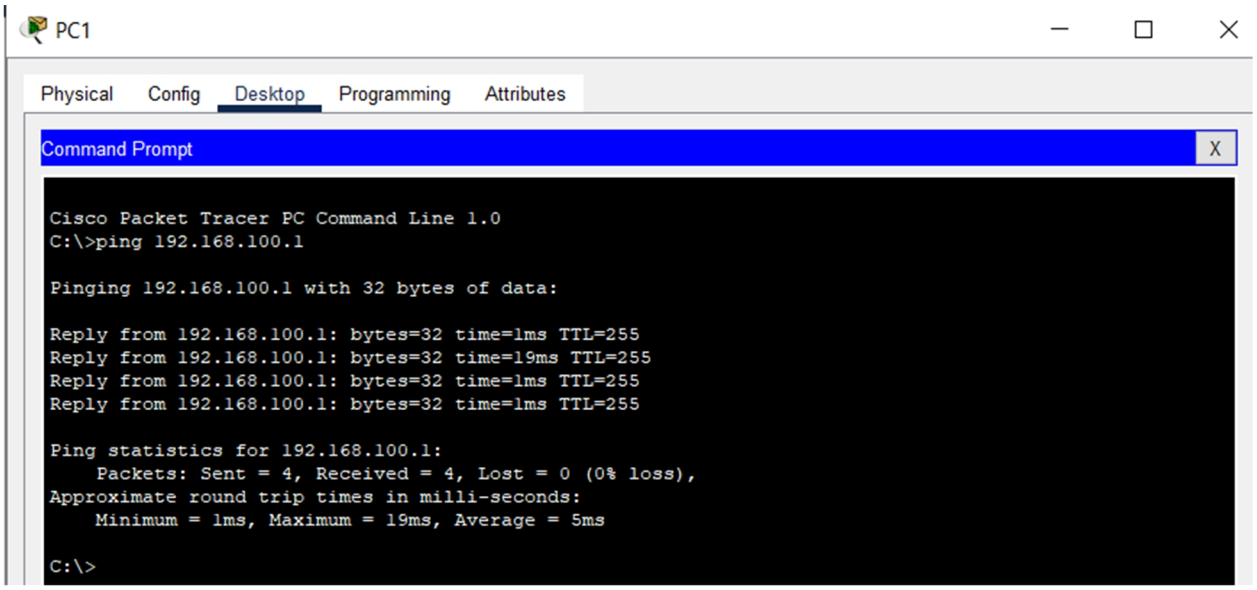
Шаг 1. Проверка конфигурации и применение ACL к интерфейсу.

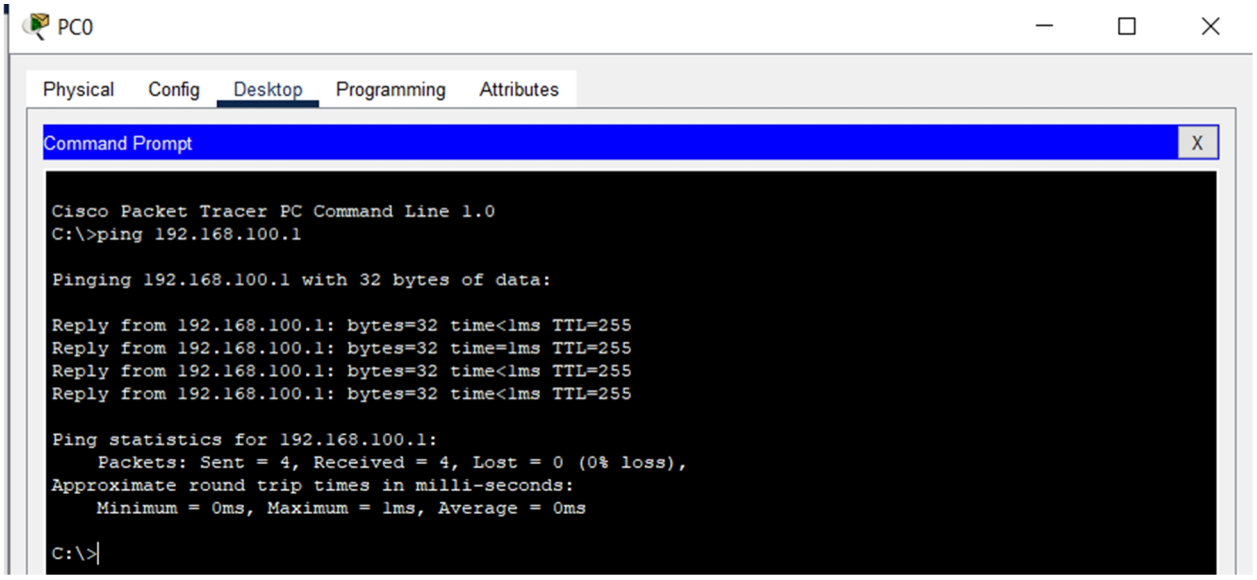
Для проверки конфигурации списка контроля доступа используйте команду **show access-lists**. Используйте команду **show run** или **show ip interface fastethernet 0/1**, чтобы проверить правильность применения ACL-списка на интерфейсе.

```
R1(config-if)#int f0/1
R1(config-if)#ip access-group File_Server_Restrictions out
R1(config-if)#
```

Шаг 2.Проверьте правильность работы списка контроля доступа.

Все три рабочие станции должны иметь возможность пинговать **Web Server**, но только **PC1** и **Web Server** должны иметь возможность пинговать **File Server**. Повторите команду **show access-lists**, чтобы увидеть количество пакетов, соответствующих каждой инструкции.


PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.100.1
Pinging 192.168.100.1 with 32 bytes of data:
Reply from 192.168.100.1: bytes=32 time=1ms TTL=255
Reply from 192.168.100.1: bytes=32 time=19ms TTL=255
Reply from 192.168.100.1: bytes=32 time=1ms TTL=255
Reply from 192.168.100.1: bytes=32 time=1ms TTL=255
Ping statistics for 192.168.100.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 19ms, Average = 5ms
C:\>


PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.100.1
Pinging 192.168.100.1 with 32 bytes of data:
Reply from 192.168.100.1: bytes=32 time<1ms TTL=255
Reply from 192.168.100.1: bytes=32 time=1ms TTL=255
Reply from 192.168.100.1: bytes=32 time<1ms TTL=255
Reply from 192.168.100.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.100.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>