Packet Tracer. Настройка стандартных именованных списков контроля доступа IPv4

Топология

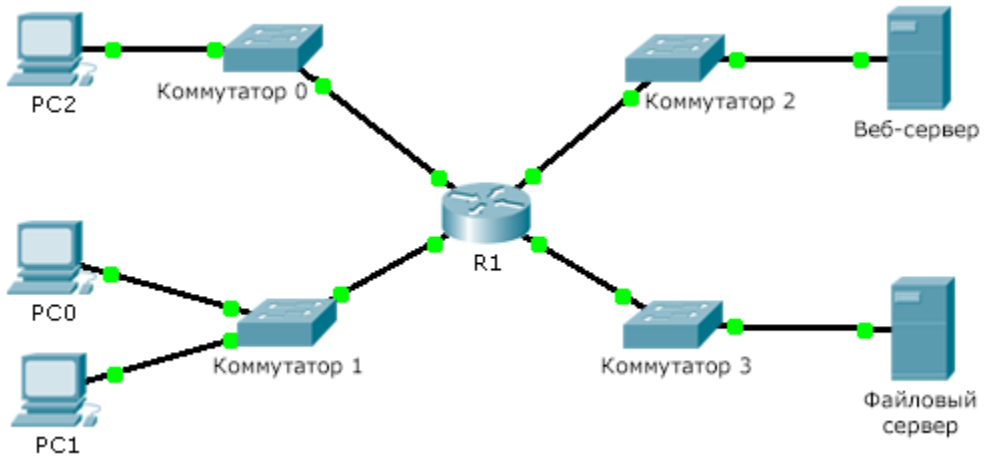

Таблица адресации

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	—
Файловый сервер	NIC	192.168.200.100	255.255.255.0	192.168.200.1
Веб-сервер	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 поставил перед вами задачу создать стандартный именованный ACL-список для предотвращения доступа к файловому серверу. Доступ должен быть запрещен всем клиентам одной сети и определенной рабочей станции другой сети.

Часть 1: Настройка и применение стандартного именованного списка контроля доступа

Шаг 1: Проверьте подключение перед настройкой и применением ACL-списка.

Проверка связи всех трех рабочих станций с **веб-сервером** и **файловым сервером** с помощью утилиты ping должна выполняться успешно.

Шаг 2: Настройте стандартный именованный ACL-список.

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)# deny any
```

Примечание. В рамках присвоения баллов за выполнение задания имя ACL-списка следует создавать с учетом регистра.

Шаг 3: Примените именованный ACL-список.

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

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

b. Сохраните конфигурацию.

Часть 2: Проверка реализации списка контроля доступа

Шаг 1: Проверьте конфигурацию ACL-списка и его размещение на интерфейсе.

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.

Шаг 2: Поверьте работоспособность ACL-списка.

Все три рабочие станции должны осуществлять эхо-запросы к **веб-серверу**, но только компьютер **PC1** должен осуществлять эхо-запросы к **файловому серверу**.