

Packet Tracer. Настройка расширенных ACL-списков. Сценарий 3

Топология

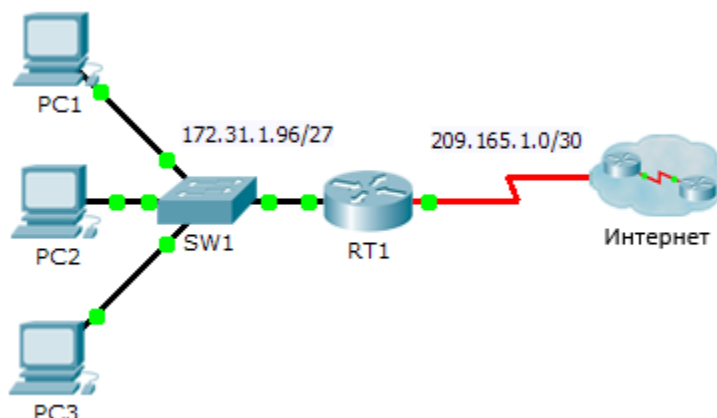


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
RT1	G0/0	172.31.1.126	255.255.255.224	N/A
	S0/0/0	209.165.1.2	255.255.255.252	N/A
PC1	NIC	172.31.1.101	255.255.255.224	172.31.1.126
PC2	NIC	172.31.1.102	255.255.255.224	172.31.1.126
PC3	NIC	172.31.1.103	255.255.255.224	172.31.1.126
Server1	NIC	64.101.255.254		
Server2	NIC	64.103.255.254		

Задачи

Часть 1. Настройка расширенного именованного ACL-списка

Часть 2. Применение и проверка расширенного ACL-списка

Исходные данные/сценарий

В этом сценарии конкретным устройствам сети LAN разрешается доступ к нескольким службам серверов, размещённых в сети Интернет.

Часть 1. Настройка расширенного именованного ACL-списка

Используйте один именованный ACL-список для реализации следующих правил:

- Запретите доступ через протоколы HTTP и HTTPS с **PC1** на серверы **Server1** и **Server2**. Эти серверы находятся внутри облака, известны только их IP-адреса.

- Запретите доступ для FTP-трафика к **Server1** и **Server2** от узла **PC2**.
- Запретите доступ для ICMP-трафика к **Server1** и **Server2** от узла **PC3**.

Примечание. Чтобы получить больше баллов, вы должны создать записи ACL-списка в порядке, указанном ниже.

Шаг 1: Запретите узлу PC1 доступ к сервисам HTTP и HTTPS на серверах Server 1 и Server2.

- a. Создайте расширенный именованный список доступа по протоколу IP, который запретит узлу **PC1** доступ к сервисам HTTP и HTTPS серверов **Server1** и **Server2**. Поскольку невозможно напрямую наблюдать за подсетями серверов в сети Интернет, требуется использование четырёх правил.

С какой команды начинается именованный ACL-список?

- b. Создайте правило, запрещающее доступ от **PC1** к **Server1**, только для HTTP (порт 80).

- c. Создайте правило, запрещающее доступ от **PC1** к **Server1**, только для HTTPS (порт 443).

- d. Создайте правило, запрещающее доступ от **PC1** к **Server2**, только для HTTP.

- e. Создайте правило, запрещающее доступ от **PC1** к **Server2**, только для HTTP.

Шаг 2: Запретите узлу PC2 доступ к сервисам FTP и на серверах Server1 и Server2.

- a. Создайте правило, запрещающее доступ от **PC2** к **Server1**, только для FTP (только порт 21).

- b. Создайте правило, запрещающее доступ от **PC2** к **Server2**, только для FTP (только порт 21).

Шаг 3: Запретите узлу PC3 отправлять эхо-запросы на Server1 и Server2.

- a. Создайте правило, запрещающее ICMP-доступ от **PC3** к серверу **Server1**.

- b. Создайте правило, запрещающее ICMP-доступ от **PC3** к серверу **Server2**.

Шаг 4: Разрешите весь остальной трафик.

По умолчанию список доступа отклоняет весь трафик, который не соответствует любому правилу, указанному в списке. С помощью какой команды разрешается весь остальной трафик?

Часть 2. Применение и проверка расширенного ACL-списка

Трафик, который должен фильтроваться, поступает от сети 172.31.1.96/27 и предназначен для удалённых сетей. Соответствующее размещение ACL-списка также зависит от отношений трафика к **RT1**.

Шаг 1: Примените ACL-список на соответствующем интерфейсе и направлении.

- a. С помощью каких команд ACL-список применяется на правильном интерфейсе и правильном направлении?

Шаг 2: Протестируйте доступ для каждого ПК.

- a. Перейдите на веб-сайты **Server1** и **Server2**, используя веб-браузер на узле **PC1** и протоколы HTTP и HTTPS.
- b. Войдите в сервис FTP серверов **Server1** и **Server2** с помощью узла **PC1**. Имя пользователя и пароль — **cisco**.
- c. От узла **PC1** отправьте эхо-запросы на серверы **Server1** и **Server2**.
- d. Повторите шаги 2a – 2c для узлов **PC2** и **PC3**, чтобы убедиться в правильной работе списка контроля доступа.