Packet Tracer. Настройка списков контроля доступа (ACL) для IPv6

Топология

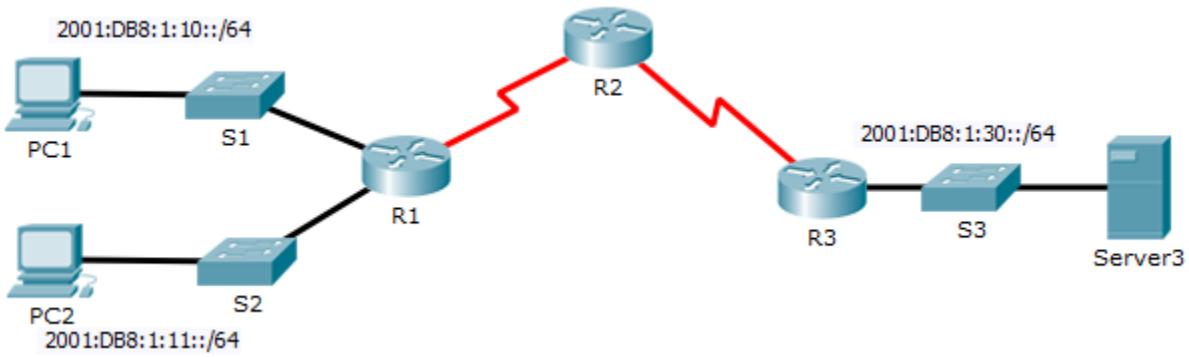

Таблица адресации

Устройство	Интерфейс	Адрес IPv6/префикс	Шлюз по умолчанию
Server3	NIC	2001:DB8:1:30::30/64	FE80::30

Задачи

Часть 1. Настройка, применение и проверка списка ACL для IPv6

Часть 2. Настройка, применение и проверка второго списка ACL для IPv6

Часть 1: Настройка, применение и проверка списка ACL для IPv6

Данные журналов свидетельствуют о том, что компьютер в сети 2001:DB8:1:11::0/64 многократно обновляет веб-страницу. Это вызывает атаку «Отказ в обслуживании» (DoS) на сервер **Server3**. Пока не удастся идентифицировать клиент и решить проблему, необходимо блокировать HTTP- и HTTPS-доступ к этой сети с помощью списка контроля доступа.

Шаг 1: Создайте список ACL, блокирующий HTTP- и HTTPS-доступ.

Создайте список ACL с именем **BLOCK_HTTP** на маршрутизаторе **R1** со следующими операторами.

a. Блокируйте передачу трафика HTTP и HTTPS на сервер **Server3**.

```
R1(config)# deny tcp any host 2001:DB8:1:30::30 eq www
R1(config)# deny tcp any host 2001:DB8:1:30::30 eq 443
```

b. Разрешите передачу всего остального трафика IPv6.

Шаг 2: Примените список ACL к нужному интерфейсу.

Примените список ACL на интерфейсе, ближайшем к источнику трафика, который требуется заблокировать.

Шаг 3: Проверьте реализацию списка ACL.

Убедитесь, что список ACL работает правильно, с помощью следующих тестов.

- Откройте в **браузере** на компьютере **PC1** адрес http://2001:DB8:1:30::30 или https://2001:DB8:1:30::30. Сайт должен открыться.
- Откройте в **браузере** на компьютере **PC2** адрес http://2001:DB8:1:30::30 или https://2001:DB8:1:30::30. Сайт должен быть заблокирован.

- Отправьте эхо-запрос с компьютера **PC2** по адресу 2001:DB8:1:30::30. Эхо-запрос должен быть успешным.

Часть 2: Настройка, применение и проверка второго списка ACL для IPv6

Теперь данные журналов показывают, что ваш сервер получает эхо-запросы со множества разных IPv6-адресов в ходе распределенной атаки DDoS. Вы должны отфильтровать эхо-запросы ICMP к вашему серверу.

Шаг 1: Создайте список контроля доступа для блокировки ICMP.

Создайте список ACL с именем **BLOCK_ICMP** на маршрутизаторе **R3** со следующими операторами.

a. Заблокируйте весь трафик ICMP со всех хостов к любому месту назначения.

b. Разрешите передачу всего остального трафика IPv6.

Шаг 2: Примените список ACL к нужному интерфейсу.

В данном случае трафик ICMP может поступать из любого источника. Чтобы заблокировать трафик ICMP независимо от его источника и изменений в топологии сети, примените список ACL, ближайший к месту назначения.

Шаг 3: Проверьте работоспособность списка контроля доступа.

a. Отправьте эхо-запрос с компьютера **PC2** по адресу 2001:DB8:1:30::30. Эхо-запрос должен завершиться неудачно.

b. Отправьте эхо-запрос с компьютера **PC1** по адресу 2001:DB8:1:30::30. Эхо-запрос должен завершиться неудачно.

   Откройте в **браузере** на компьютере **PC1** адрес http://2001:DB8:1:30::30 или https://2001:DB8:1:30::30. Сайт должен открыться.

