Packet Tracer. Настройка ACL-списков IPv6

Топология

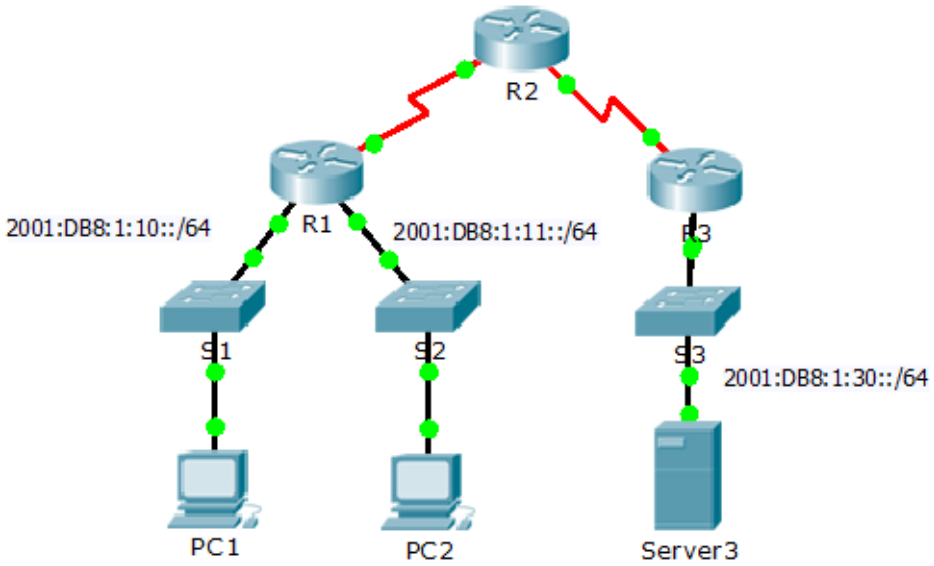

Таблица адресации

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

Задачи

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

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

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

Согласно записям сетевого журнала, компьютер в сети 2001:DB8:1:11::0/64 постоянно обновляет свою веб-страницу, из-за чего на сервере **Server3** происходит отказ в обслуживании (DoS). Пока клиент не обнаружен, и не очищены его настройки, необходимо запретить доступ через HTTP и HTTPS к этой сети с помощью списка доступа.

Шаг 1: Настройте ACL-список, который запрещает доступ к HTTP и HTTPS.

Настройте ACL-список с именем **BLOCK_HTTP** на маршрутизаторе **R1** со следующими правилами.

a. Запретите доступ трафика HTTP и HTTPS к серверу **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 прохождение всего остального трафика IPv6.

Шаг 2: Примените ACL-список на подходящем интерфейсе.

Примените ACL-список на интерфейсе, расположенном максимально близко к источнику трафика, подлежащего запрету.

```
R1(config-if)# ipv6 traffic-filter BLOCK_HTTP in
```

Шаг 3: Проверьте работу ACL-списка.

Убедитесь, что ACL-список работает должным образом, выполнив следующие тесты:

- Откройте в **веб-браузере** на **PC1** страницу http:// 2001:DB8:1:30::30 или https://2001:DB8:1:30::30. Веб-сайт должен отображаться.
- Откройте в **веб-браузере** на **PC2** страницу http:// 2001:DB8:1:30::30 или https://2001:DB8:1:30::30. Данный веб-сайт требуется заблокировать.
- Отправьте эхо-запрос с **PC2** на 2001:DB8:1:30::30. Эхо-запрос должен быть успешным.

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

Записи в журналах теперь указывают на то, что ваш сервер получает эхо-запросы с различных адресов IPv6 в виде атаки типа распределённая атака DDoS. Необходимо отфильтровать ICMP-запросы, приходящие на ваш сервер.

Шаг 1: Создайте список доступа, который запретит ICMP-трафик.

Настройте ACL-список с именем **BLOCK_ICMP** на **R3**, создав в нём следующие правила:

a. Заблокируйте весь трафик ICMP в любом направлении от всех узлов.

b. Разрешите прохождение всего остального трафика IPv6.

Шаг 2: Примените ACL-список на подходящем интерфейсе.

В данном случае трафик ICMP может исходить от любого источника. Чтобы убедиться, что трафик ICMP заблокирован независимо от его источника или изменений, возникающих в топологии сети, примените ACL-список максимально близко к узлу назначения.

Шаг 3: Убедитесь в правильной работе списка контроля доступа.

a. Отправьте эхо-запрос с **PC2** на 2001:DB8:1:30::30. Эхо-запрос завершится неудачей.

b. Отправьте эхо-запрос с **PC1** на 2001:DB8:1:30::30. Эхо-запрос завершится неудачей.

Откройте в **веб-браузере** на **PC1** страницу http:// 2001:DB8:1:30::30 или https://2001:DB8:1:30::30. Веб-сайт должен отображаться.