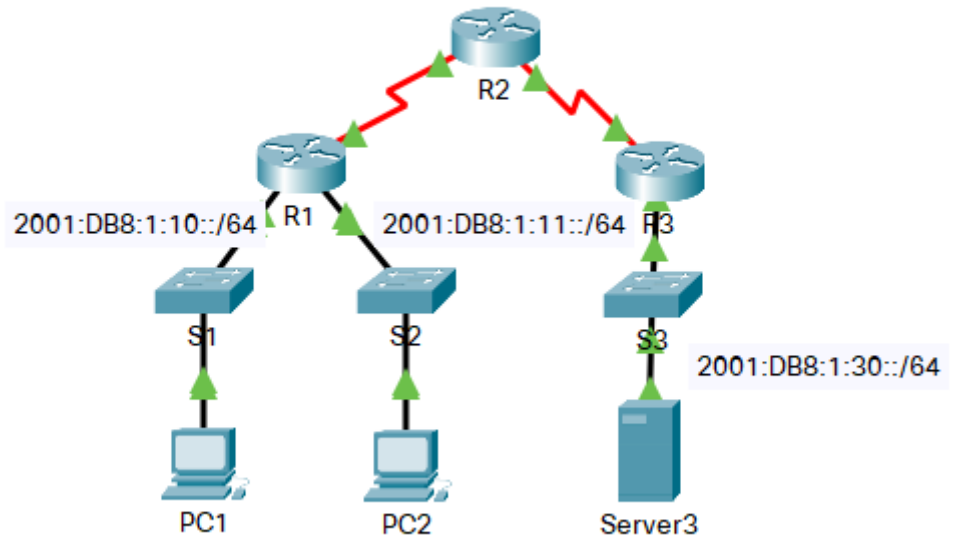
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»
ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
Кафедра компьютерной инженерии и моделирования

Настройка ACL-списков IPv6

Отчет по лабораторной работе № 9
по дисциплине «Компьютерные сети»
студента 2 курса группы ИВТ-б-о-202(1)
Шор Константина Александровича

Направления подготовки 09.03.01«Информатика и вычислительная техника»

Симферополь, 2022



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

Для начала работы настроим eigrp для этого нужно дать роутерам router-id сам eigrp уже настроен

R1

```
ipv6 router eigrp 1
 eigrp router-id 1.1.1.1
 no shutdown
```

R2

```
ipv6 router eigrp 1
 eigrp router-id 2.2.2.2
 no shutdown
```

R3

```
ipv6 router eigrp 1
 eigrp router-id 3.3.3.3
 no shutdown
```

Часть 1. Настройте, примените и проверьте ACL-список 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.

HTTPS к этой сети с помощью списка доступа.

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

Настройте для ACL-списка с именем **BLOCK_ICMP** на маршрутизаторе **R1** следующие правила:

a. Запретите 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 прохождение всего остального трафика IPv6.

```
R1>ena
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ipv6 acc
R1(config)#ipv6 access-list BLOCK_HTTP
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq www
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq 443
R1(config-ipv6-acl)#permit ipv6 any any
```

Шаг 2. Примените ACL-список на соответствующем интерфейсе.

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

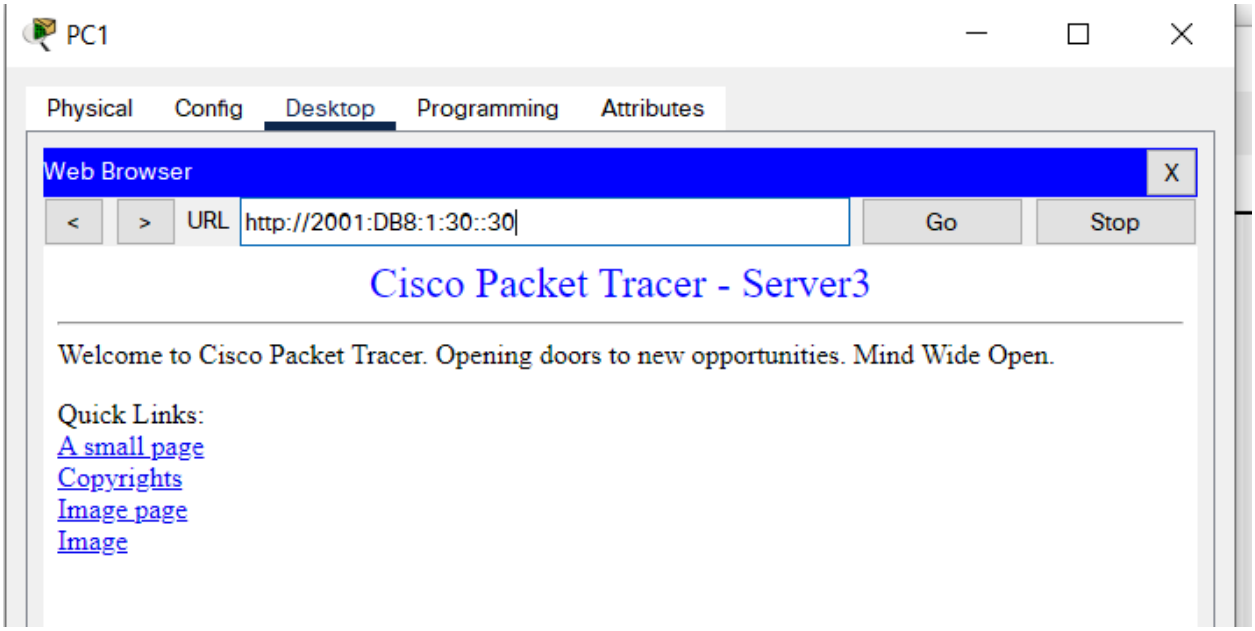
```
R1(config-if)# ipv6 traffic-filter BLOCK_HTTP in
```

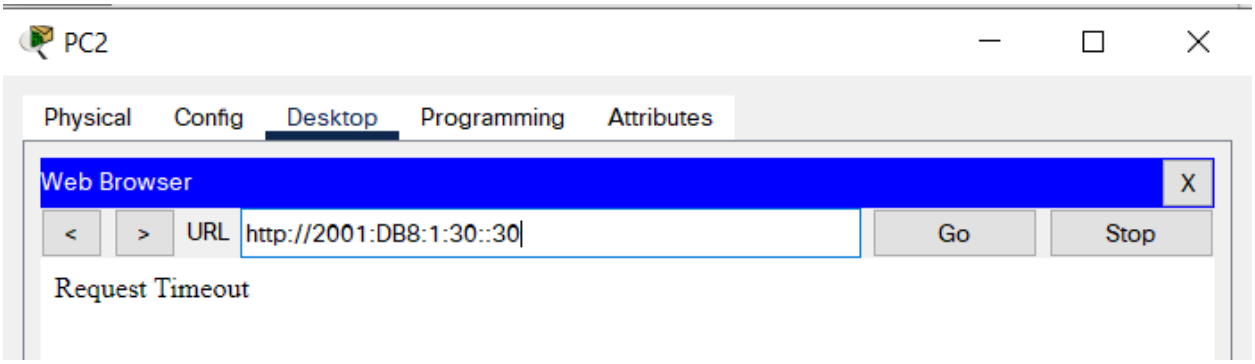
```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int
R1(config)#interface gig
R1(config)#interface gigabitEthernet 0/1
R1(config-if)#ipv6 traffic-filter  BLOCK_HTTP in
```

Шаг 3. Проверьте работу 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 от **PC2** на 2001:DB8:1:30::30. Эхо-запрос должен быть успешным.





```
C:\>ping 2001:DB8:1:30::30

Pinging 2001:DB8:1:30::30 with 32 bytes of data:

Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125

Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

Часть 2. Настройка, применение и проверка второго ACL-списка 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 эхо-запросы ICMP, поступающие на ваш сервер.

Шаг 1. Создайте список доступа для запрещения ICMP.

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.

```
  unicast-routing  Enable unicast routing
R3(config)#ipv6 acc
R3(config)#ipv6 access-list ?
  WORD  User selected string identifying this access list
R3(config)#ipv6 access-list BLOCK_ICMP
R3(config-ipv6-acl)#deny ?
  icmp  Internet Control Message Protocol
  ipv6  Any IPv6
  tcp   Transmission Control Protocol
  udp   User Datagram Protocol
R3(config-ipv6-acl)#deny ecmp ?
% Unrecognized command
R3(config-ipv6-acl)#deny icmp ?
  X:X:X:X::X/<0-128>  IPv6 source prefix x:x::y/<z>
  any                 Any source prefix
  host                A single source host
R3(config-ipv6-acl)#deny icmp any any
R3(config-ipv6-acl)#permit ?
  icmp  Internet Control Message Protocol
  ipv6  Any IPv6
  tcp   Transmission Control Protocol
  udp   User Datagram Protocol
R3(config-ipv6-acl)#permit ipv6 any any
R3(config-ipv6-acl)#
```

Шаг 2. Примените ACL-список на соответствующем 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.

```
R3(config)#interface gig
R3(config)#interface gigabitEthernet 0/0
R3(config-if)#ipv6
R3(config-if)#ipv6 tr
R3(config-if)#ipv6 traffic-filter BLOCK_ICMP in
R3(config-if)#no ipv6 traffic-filter BLOCK_ICMP in
R3(config-if)#ipv6 traffic-filter BLOCK_ICMP out
R3(config-if)#
```

Шаг 3. Проверьте правильность работы списка доступа.

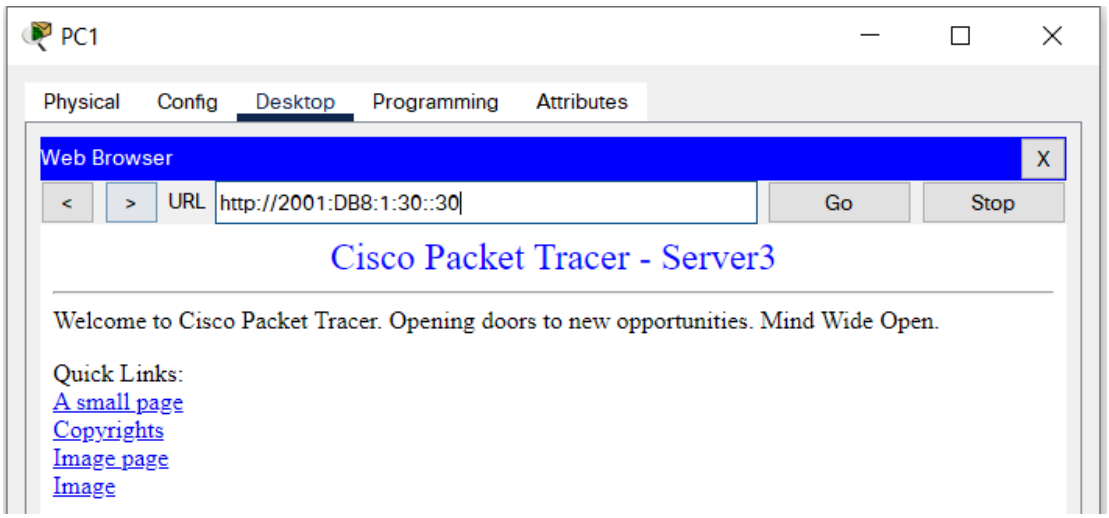
a. Отправьте эхо-запрос от **PC2** на 2001:DB8:1:30::30. Эхо-запрос завершится неудачей.

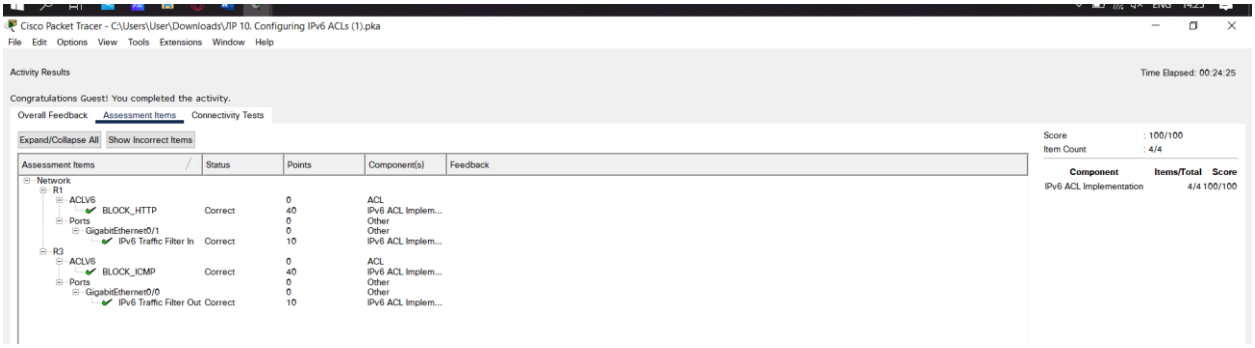
b. Отправьте эхо-запрос от **PC1** на 2001:DB8:1:30::30. Эхо-запрос завершится неудачей.

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

```
C:\>ping 2001:DB8:1:30::30

Pinging 2001:DB8:1:30::30 with 32 bytes of data:

Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.

Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
Packet Tracer PC Command Line 1.0
C:\>ping 2001:DB8:1:30::30

Pinging 2001:DB8:1:30::30 with 32 bytes of data:

Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.
Reply from 2001:DB8:1:2::1: Destination host unreachable.

Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```


PC1
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://2001:DB8:1:30::30
Go
Stop
Cisco Packet Tracer - Server3
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image


Cisco Packet Tracer - C:\Users\User\Downloads\JIP 10. Configuring IPv6 ACLs (1).pka
File Edit Options View Tools Extensions Window Help
Activity Results
Time Elapsed: 00:24:25
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Show Incorrect Items
Assessment Items
Status
Points
Component(s)
Feedback
Network
R1
ACLV6
BLOCK_HTTP
Correct
40
IPv6 ACL Implem...
Ports
0
Other
GigabitEthernet0/1
IPv6 Traffic Filter In
Correct
10
IPv6 ACL Implem...
R3
ACLV6
BLOCK_ICMP
Correct
40
IPv6 ACL Implem...
Ports
0
Other
GigabitEthernet0/0
IPv6 Traffic Filter Out
Correct
10
IPv6 ACL Implem...
Score
: 100/100
Item Count
: 4/4
Component
Items/Total
Score
IPv6 ACL Implementation
4/4
100/100