Пояснение, почему мало баллов
Все работает, как нужно, но pkt не засчитывает мое решение. Вероятнее всего ошибка в самом pkt

Packet Tracer. Реализацией ACL IPv4 (повышенный уровень сложности)

Таблица адресации

Устройство	Интерфейс	IP-адрес
Branch	G0/0/0	192.168.1.1/26
	G0/0/1	192.168.1.65/29
	S0/1/0	192.0.2.1/30
	S0/1/1	192.168.3.1/30
HQ	G0/0/0	192.168.2.1/27
	G0/0/1	192.168.2.33/28
	S0/1/1	192.168.3.2/30
PC-1	NIC	192.168.1.10/26
PC-2	NIC	192.168.1.20/26
PC-3	NIC	192.168.1.30/26
Admin	NIC	192.168.1.67/29
Enterprise Web Server	NIC	192.168.1.70/29
Branch PC	NIC	192.168.2.17/27
Branch Server	NIC	192.168.2.45/28
Internet User	NIC	198.51.100.218/24
External Web Server	NIC	203.0.113.73/24

Задачи

- Настройка маршрутизатора со стандартными именованными ACL.
- Настройка маршрутизатора с расширенными именованными ACL.
- Настройте маршрутизатор с расширенными ACL в соответствии с конкретными требованиями
- Настройка ACL для управления доступом к терминальным линиям сетевых устройств.
- Настройте соответствующие интерфейсы маршрутизатора с ACL в соответствующем направлении.
- Проверка работы настроенных списков ACL.

Общие сведения и сценарий

В этом задании будут настроены расширенные, стандартные именованные и расширенные именованные списки ACL в соответствии с указанными требованиями к связи.

Инструкция

Шаг 1: Проверка подключения в новой сети компании

Прежде чем настраивать списки ACL, проверьте подключение к сети в том виде, в каком она есть. Все хосты должны иметь возможность выполнить пинг до всех остальных узлов.

Шаг 2. Настройка стандартных и расширенных списков управления доступом в соответствии с требованиями.

Настройте ACL для соответствия следующим требованиям.

Важные руководящие принципы:

- **Не** используйте неявную deny any в конце списков ACL.
- Используйте сокращения (**host** и **any**), когда это возможно.
- Напишите инструкции ACL соответсвующие требований в том порядке, в котором они указаны здесь.
- Разместите списки ACL в наиболее эффективное местоположение и направление.

Требования ACL 1

- Создать ACL **101**.
- Явно блокировать доступ FTP к Enterprise Web Server из Интернета.
- Никакой трафик ICMP из Интернета не должен быть разрешен любым хостам в сети LAN 1 HQ
- Разрешить весь оставшийся трафик.

```
  <cr>
HQ(config)#ip access-list extended 101
HQ(config-ext-nacl)#deny tcp any host 192.168.1.70 eq 21
HQ(config-ext-nacl)#permit ip any host 192.168.1.70

HQ(config)#int g0/0/1
HQ(config-if)#ip access-group 101 out
```

Требования ACL 2

- Использовать номер ACL **111**
- Ни один хост в сети LAN 1 HQ не должен иметь доступа к Branch Server.
- Все остальные виды трафика должны быть разрешены.

```
Branch(config)#ip access-list extended 111
Branch(config-ext-nacl)#deny ip 192.168.1.0 0.0.0.63 host 192.168.2.45
Branch(config-ext-nacl)#permit ip any host 192.168.2.45

Branch(config)#int g0/0/1
Branch(config-if)#ip access-group ?
  <1-199>  IP access list (standard or extended)
  WORD     Access-list name
Branch(config-if)#ip access-group 111
% Incomplete command.
Branch(config-if)#ip access-group 111 ?
  in   inbound packets
  out  outbound packets
Branch(config-if)#ip access-group 111 out
Branch(config-if)#
```

ACL 3: Требования

- Создайте именованный стандартный ACL. Используйте имя **vty_block**. Имя ACL должно точно совпадать с этим именем.
- Только адреса из сети HQ LAN 2 должны иметь доступ к линиям VTY маршрутизатора HQ.

```
HQ(config)#ip access-list standard vty_block
HQ(config-std-nacl)#permit 192.168.1.64 0.0.0.7
HQ(config-std-nacl)#deny any
HQ(config)#line vty 0 15
HQ(config-line)#access-class vty_block in
```

ACL 4: Требования

- Создайте именованный расширенный ACL с именем **branch_to_hq**. Имя ACL должно точно совпадать с этим именем.
- Ни один хосты ни в одной из ветвей LAN не должны иметь доступа к локальной сети HQ 1. Используйте одну инструкцию списка доступа для из каждой сети Branch LAN .
- Весь остальной трафик IP должен быть разрешен.

```
HQ(config)#ip access-list extended branch_to_hq
HQ(config-ext-nacl)#deny ip 192.168.1.64 0.0.0.7 ?
  A.B.C.D  Destination address
  any      Any destination host
  host     A single destination host
HQ(config-ext-nacl)#deny ip 192.168.1.64 0.0.0.7 192.168.1.0 0.0.0.63
HQ(config-ext-nacl)#deny ip 192.168.2.0 0.0.0.31 192.168.1.0 0.0.0.63
HQ(config-ext-nacl)#deny ip 192.168.2.32 0.0.0.15 192.168.1.0 0.0.0.63
HQ(config-ext-nacl)#exit
HQ(config)#int g0/0/0
HQ(config-if)#ip access-group ?
  <1-199>  IP access list (standard or extended)
  WORD     Access-list name
HQ(config-if)#exit
HQ(config)#ip access-list extended branch_to_hq
HQ(config-ext-nacl)#permit ip any
% Incomplete command.
HQ(config-ext-nacl)#permit ?
  ahp    Authentication Header Protocol
  eigrp  Cisco's EIGRP routing protocol
  esp    Encapsulation Security Payload
  gre    Cisco's GRE tunneling
  icmp   Internet Control Message Protocol
  ip     Any Internet Protocol
  ospf   OSPF routing protocol
  tcp    Transmission Control Protocol
  udp    User Datagram Protocol
HQ(config-ext-nacl)#permit ip ?
  A.B.C.D  Source address
  any      Any source host
  host     A single source host
HQ(config-ext-nacl)#permit ip any any
HQ(config-ext-nacl)#exit
HQ(config)#int g0/0/0
HQ(config-if)#access-group branch_to_hq
                ^
% Invalid input detected at '^' marker.

HQ(config-if)#access-group branch_to_hq out
                ^
% Invalid input detected at '^' marker.

HQ(config-if)#ip access-group branch_to_hq out
HQ(config-if)#
```

Шаг 3. Проверка операции ACL.

a. Выполните следующие тесты на связность между устройствами в топологии. Обратите внимание, являются ли они успешными или нет.

Примечание. Используйте команду **show ip access-lists для проверки работы ACL. Используйте команду clear access list counters для сброса счетчиков совпадений.**

Отправьте запрос ping от Branch PC на Enterprise Web Server. Была ли проверка успешной? Дайте пояснение. Не было запрета на отправку icmp пакетов из LAN Branch PC

```
C:\>ping 192.168.1.70

Pinging 192.168.1.70 with 32 bytes of data:

Reply from 192.168.1.70: bytes=32 time=12ms TTL=126
Reply from 192.168.1.70: bytes=32 time=14ms TTL=126
Reply from 192.168.1.70: bytes=32 time=20ms TTL=126
Reply from 192.168.1.70: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.1.70:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 20ms, Average = 12ms

C:\>
```

Какое заявление ACL разрешало или отклоняло пинг между этими двумя устройствами? Перечислите имя или номер списка доступа, маршрутизатор, на котором он был применен, и конкретную строку, сопоставляемую трафиком.

ACL 101 permit ip any any

Попытка выполнить эхо-запрос с PC-1 на HQ LAN 1 на сервер Branch Server. Была ли проверка успешной? Дайте пояснение. ACL branch_to_hq запрещает запрос

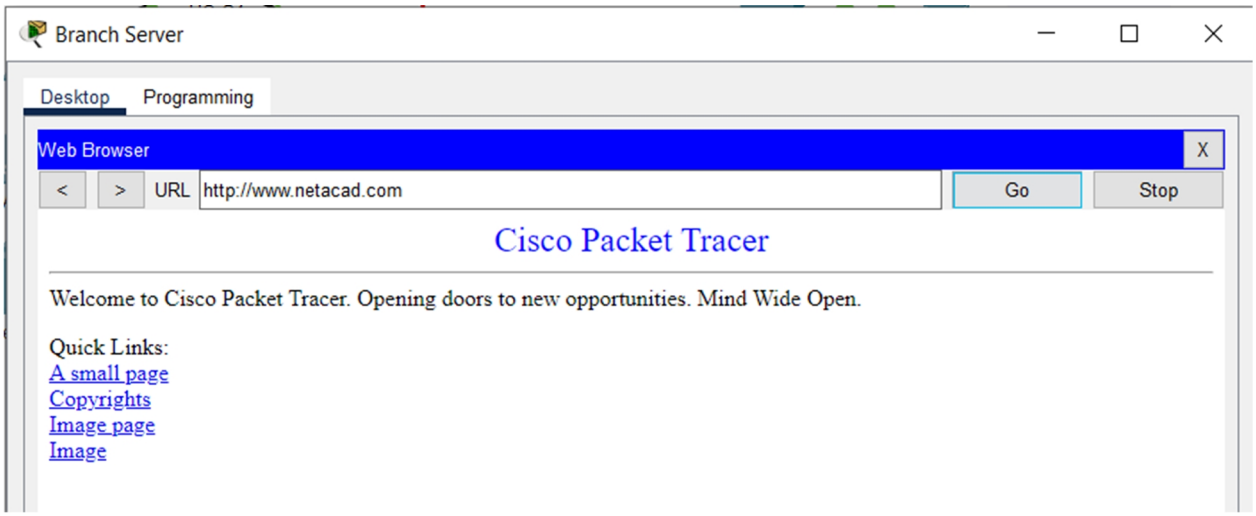
```
C:\>ping 192.168.2.45

Pinging 192.168.2.45 with 32 bytes of data:

Reply from 192.168.3.2: Destination host unreachable.
Reply from 192.168.3.2: Destination host unreachable.
Reply from 192.168.3.2: Destination host unreachable.
Reply from 192.168.3.2: Destination host unreachable.

Ping statistics for 192.168.2.45:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Какое заявление ACL разрешало или отклоняло пинг между этими двумя устройствами?

ACL branch_to_hq

```
HQ(config-ext-nacl)#deny ip 192.168.2.32 0.0.0.15 192.168.1.0 0.0.0.63
```

Откройте веб-браузер на внешнем сервере и попытайтесь открыть веб-страницу, хранящуюся на корпоративном веб-сервере. Успешно? Дайте пояснение.



Нет запрета на такие действия

Какая инструкция ACL разрешала или отклоняла пинг между этими двумя устройствами?

ACL 111 permit ip any any

б. Проверьте подключения к внутреннему серверу из Интернета.

В командной строке на компьютере Internet User PC попытайтесь установить FTP-соединение с сервером филиала. Успешно ли FTP-соединение? Нет

Какой список доступа следует изменить, чтобы пользователи из Интернета не могли подключаться к серверу филиалов по FTP?

```
HQ(config-ext-nacl)#deny tcp any host 192.168.1.70 eq 21
```

Какие операторы должны быть добавлены в список доступа, чтобы запретить этот трафик?