Лабораторная работа № 10

Настройка списков управления доступом (ACL)

Танрибергенов Эльдар

2024 г.

Российский университет дружбы народов, Москва, Россия

Цели и задачи

Цель лабораторной работы

Освоить настройку прав доступа пользователей к ресурсам сети.

Задачи

1. Требуется настроить следующие правила доступа:
    1) web-сервер: разрешить доступ всем пользователям по протоколу HTTP через порт 80 протокола TCP, а для администратора открыть доступ по протоколам Telnet и FTP;
    2) файловый сервер: с внутренних адресов сети доступ открыт по портам для общедоступных каталогов, с внешних — доступ по протоколу FTP;
    3) почтовый сервер: разрешить пользователям работать по протоколам SMTP и POP3 (соответственно через порты 25 и 110 протокола TCP), а для администратора — открыть доступ по протоколам Telnet и FTP;
    4) DNS-сервер: открыть порт 53 протокола UDP для доступа из внутренней сети;
    5) разрешить icmp-сообщения, направленные в сеть серверов;
    6) запретить для сети Other любые запросы за пределы сети, за исключением администратора;
    7) разрешить доступ в сеть управления сетевым оборудованием только администратору сети.
2. Проверить правильность действия установленных правил доступа.

Выполнение работы

Размещение ноутбука администратора в сети other-donskaya

- IP-адрес устройства - 10.128.6.200, шлюз - 10.128.6.1, DNS-сервер - 10.128.0.5, подсоединён к порту 24 коммутатора msk-donskaya-etanribergenov-sw-4

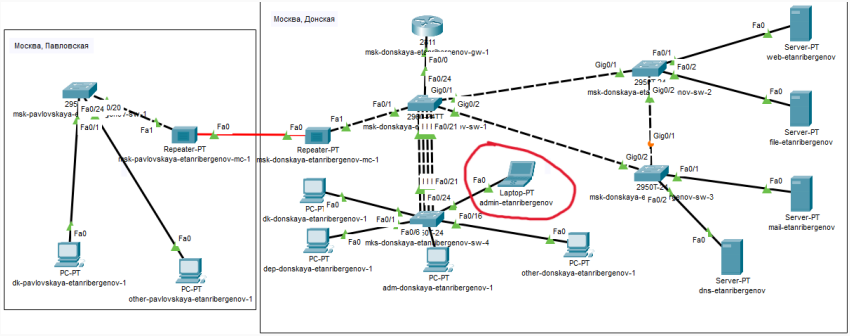

Рис. 1: Размещение ноутбука администратора в сети other-donskaya

Настройка доступа к web-серверу по порту tcp 80

- *ip access-list extended servers-out* - переход к настройке расширенного (extended) списка управления доступом servers-out
- *remark <текст>* - комментарий-напоминание
- *permit <протокол> <адрес источника> <адрес назначения> eq <порт>* - разрешение хосту <адрес источника> отправлять сообщения по протоколу <протокол> хосту <адрес назначения> на порт <порт>

```
msk-donskaya-etanribergenov-gw-1>enable
Password:
msk-donskaya-etanribergenov-gw-1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-etanribergenov-gw-1(config)#ip access-list extended servers-out
msk-donskaya-etanribergenov-gw(config-ext-nacl)#remark web
msk-donskaya-etanribergenov-gw(config-ext-nacl)#permit tcp any host 10.128.0.2 eq 80
msk-donskaya-etanribergenov-gw(config-ext-nacl)#
```

Рис. 2: Настройка доступа к web-серверу по порту http (tcp 80)

Добавление списка управления доступом к интерфейсу

```
msk-donskaya-etanribergenov-gw-1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-etanribergenov-gw-1(config)#interface f0/0.3
msk-donskaya-etanribergenov-gw-1(config-subif)#ip access-group servers-out out
msk-donskaya-etanribergenov-gw-1(config-subif)#^Z
msk-donskaya-etanribergenov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-etanribergenov-gw-1#wr mem
Building configuration...
[OK]
```

Рис. 3: Подключение списка прав доступа к интерфейсу и применение к исходящему трафику

Проверка работы правила

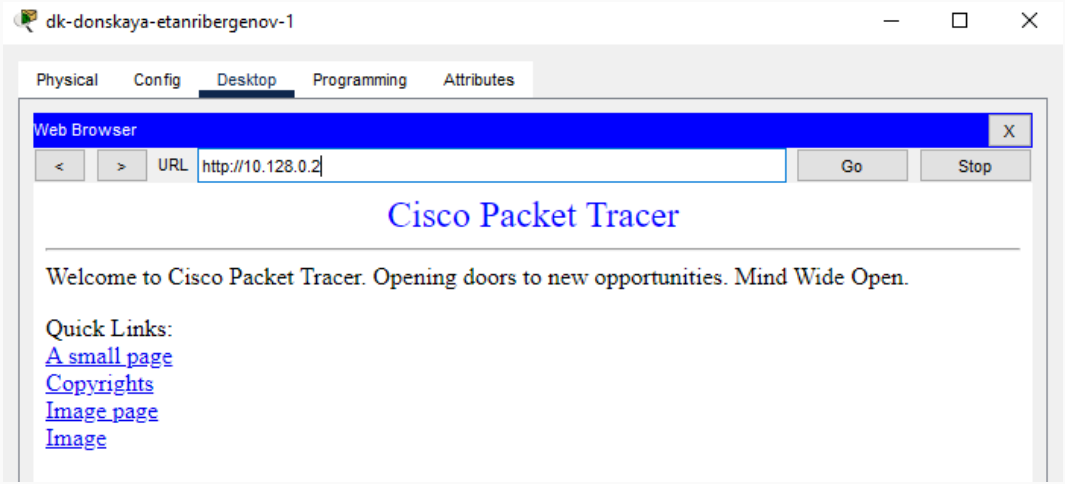

Рис. 4: Проверка доступа к web-серверу через протокол HTTP

Проверка работы правила

```
C:\>ping 10.128.0.2

Pinging 10.128.0.2 with 32 bytes of data:

Reply from 10.128.3.1: Destination host unreachable.
Reply from 10.128.3.1: Destination host unreachable.
Reply from 10.128.3.1: Destination host unreachable.
Reply from 10.128.3.1: Destination host unreachable.

Ping statistics for 10.128.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
C:\>ping www-etanribergenov.donskaya.rudn.edu
C:\>
```

Рис. 5: Проверка недоступности web-сервера по команде ping

```
msk-donskaya-etanribergenov-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-etanribergenov-gw-1(config)#ip access-list extended servers-out
msk-donskaya-etanribergenov-gw(config-ext-nacl)#permit tcp host 10.128.6.200 host
10.128.0.2 range 20 ftp
msk-donskaya-etanribergenov-gw(config-ext-nacl)#permit tcp host 10.128.6.200 host
10.128.0.2 eq telnet
msk-donskaya-etanribergenov-gw(config-ext-nacl)#^Z
msk-donskaya-etanribergenov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-etanribergenov-gw-1#wr mem
Building configuration...
[OK]
```

Рис. 6: Добавление разрешения устройству администратора на доступ к web-серверу по протоколам FTP и telnet

Проверка работы правила

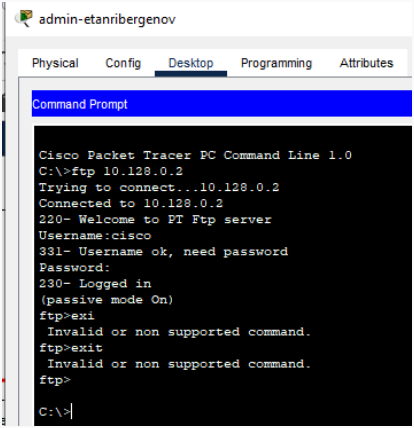

Рис. 7: Проверка доступа администратора к web-серверу по протоколу FTP

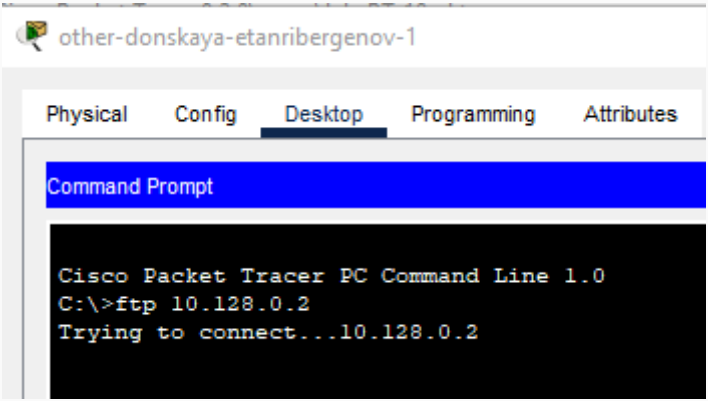

Рис. 8: Проверка доступа другого устройства сети к web-серверу по протоколу FTP

Настройка доступа к файловому серверу

```
msk-donskaya-etanribergenov-gw-1(config)#ip access-list extended servers-out
msk-donskaya-etanribergenov-gw(config-ext-nacl)#remark file
msk-donskaya-etanribergenov-gw(config-ext-nacl)#permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3
eq 445
msk-donskaya-etanribergenov-gw(config-ext-nacl)#permit tcp any host 10.128.0.3 range 20 ftp
msk-donskaya-etanribergenov-gw(config-ext-nacl)#
```

Рис. 9: Настройка доступа к файловому серверу

Настройка доступа к почтовому серверу

```
msk-donskaya-etanribergenov-gw-1(config)#ip access-list extended servers-out
msk-donskaya-etanribergenov-gw(config-ext-nacl)#remark mail
msk-donskaya-etanribergenov-gw(config-ext-nacl)#permit tcp any host 10.128.0.4 eq smtp
msk-donskaya-etanribergenov-gw(config-ext-nacl)#permit tcp any host 10.128.0.4 eq pop3
msk-donskaya-etanribergenov-gw(config-ext-nacl)#
```

Рис. 10: Настройка доступа к почтовому серверу

Настройка доступа к DNS-серверу

```
msk-donskaya-etanribergenov-gw-1(config)#ip access-list extended servers-out
msk-donskaya-etanribergenov-gw(config-ext-nacl)#remark dns
msk-donskaya-etanribergenov-gw(config-ext-nacl)#permit udp 10.128.0.0 0.0.255.255 host 10.128.0.5
eq 53
msk-donskaya-etanribergenov-gw(config-ext-nacl)#^Z
```

Рис. 11: Настройка доступа к DNS-серверу

Проверка работы правила

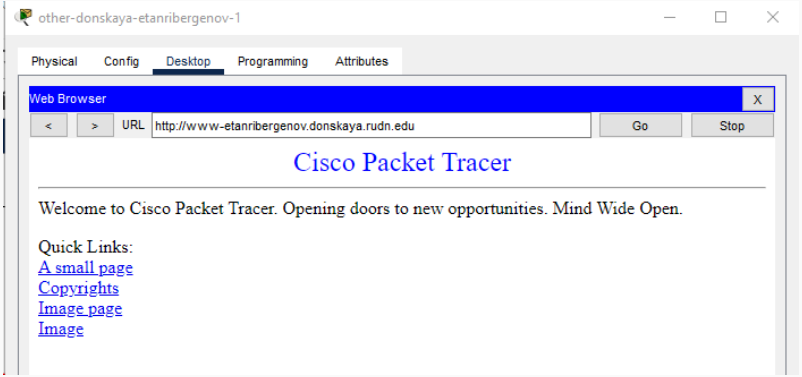

Рис. 12: Проверка доступа к DNS-серверу

Разрешение icmp-запросов

```
msk-donskaya-etanribergenov-gw-1(config)#ip access-list extended servers-out
msk-donskaya-etanribergenov-gw(config-ext-nacl)#1 permit icmp any any
```

Рис. 13: Разрешение icmp-запросов всем узлам в сети

Проверка работы правила

```
C:\>ping www-etanribergenov.donskaya.rudn.edu

Pinging 10.128.0.2 with 32 bytes of data:

Reply from 10.128.0.2: bytes=32 time=1ms TTL=127
Reply from 10.128.0.2: bytes=32 time<1ms TTL=127
Reply from 10.128.0.2: bytes=32 time<1ms TTL=127
Reply from 10.128.0.2: bytes=32 time=9ms TTL=127

Ping statistics for 10.128.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 9ms, Average = 2ms

C:\>
```

Рис. 14: Проверка доступности icmp-запросов в сети

Настройка доступа для сети Other

- наложение ограничения на исходящий из сети Other трафик, который по отношению к маршрутизатору является входящим трафиком

```
msk-donskaya-etanribergenov-gw-1(config)#ip access-list extended other-in
msk-donskaya-etanribergenov-gw(config-ext-nacl)#remark admin
msk-donskaya-etanribergenov-gw(config-ext-nacl)#permit ip host 10.128.6.200 any
msk-donskaya-etanribergenov-gw(config-ext-nacl)#exit
msk-donskaya-etanribergenov-gw-1(config)#
msk-donskaya-etanribergenov-gw-1(config)#interface f0/0.104
msk-donskaya-etanribergenov-gw-1(config-subif)#ip access-group other-in in
msk-donskaya-etanribergenov-gw-1(config-subif)#
```

Рис. 15: Настройка доступа для сети other

```
msk-donskaya-etanribergenov-gw-1(config)#ip access-list extended management-out
msk-donskaya-etanribergenov-gw(config-ext-nacl)#remark admin
msk-donskaya-etanribergenov-gw(config-ext-nacl)#permit ip host 10.128.6.200
% Incomplete command.
msk-donskaya-etanribergenov-gw(config-ext-nacl)#permit ip host 10.128.6.200 10.128.1.0 0.0.0.255
msk-donskaya-etanribergenov-gw(config-ext-nacl)#exit
msk-donskaya-etanribergenov-gw-1(config)#
msk-donskaya-etanribergenov-gw-1(config)#interface f0/0.2
msk-donskaya-etanribergenov-gw-1(config-subif)#ip access-group management-out out
```

Рис. 16: Настройка доступа администратора к сети сетевого оборудования

Проверка работы правила

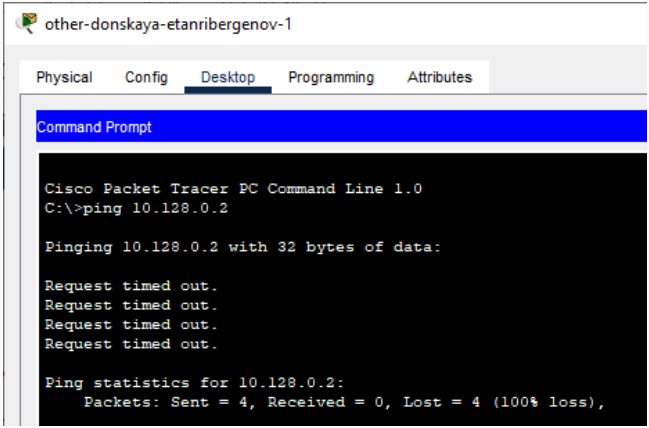

Рис. 17: Проверка доступа к web-серверу устройства из сети other

Проверка работы правила

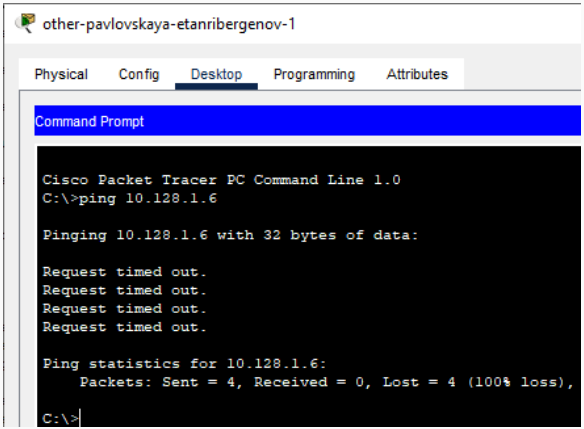

Рис. 18: Проверка доступа к сетевому оборудованию устройства из сети other

```
C:\>ping www-etanribergenov.donskaya.rudn.edu

Pinging 10.128.0.2 with 32 bytes of data:

Request timed out.
Reply from 10.128.0.2: bytes=32 time=1ms TTL=127
Reply from 10.128.0.2: bytes=32 time<1ms TTL=127
Reply from 10.128.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 10.128.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Рис. 19: Проверка доступа администратора ко всем устройствам сети

Проверка работы правила

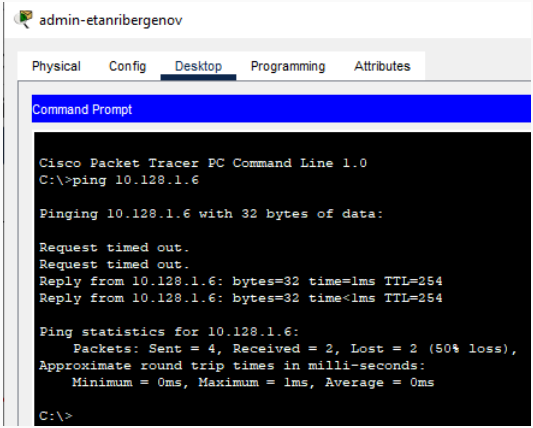

Рис. 20: Проверка доступа администратора к сети сетевого оборудования

Размещение ноутбука администратора в сети other-pavlovskaya (на Павловской)

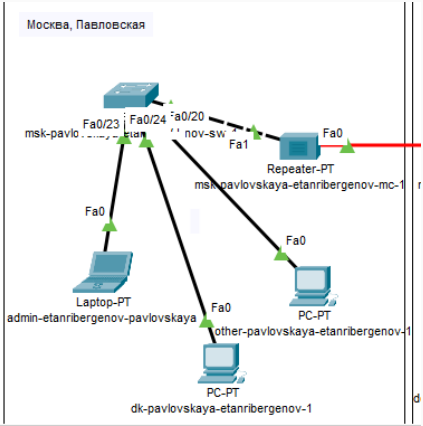

Рис. 21: Размещение ноутбука администратора на Павловской

Добавление правил для ноутбука администратора в списки управления доступом

```
ip access-list extended other-in
 remark admin
 permit ip host 10.128.6.200 any
 permit ip host 10.128.6.201 any
ip access-list extended management-out
 remark admin
 permit ip host 10.128.6.200 10.128.1.0 0.0.0.255
 permit ip host 10.128.6.201 10.128.1.0 0.0.0.255
!
```

Рис. 22: Правила для администратора на Павловской в списках доступа

Проверка работы правила

```
C:\>ping mail-etanribergenov.donskaya.rudn.edu

Pinging 10.128.0.4 with 32 bytes of data:

Reply from 10.128.0.4: bytes=32 time<1ms TTL=127
Reply from 10.128.0.4: bytes=32 time<1ms TTL=127
Reply from 10.128.0.4: bytes=32 time<1ms TTL=127
Reply from 10.128.0.4: bytes=32 time<1ms TTL=127

Ping statistics for 10.128.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
C:\>ping 10.128.1.6

Pinging 10.128.1.6 with 32 bytes of data:

Reply from 10.128.1.6: bytes=32 time<1ms TTL=254
Reply from 10.128.1.6: bytes=32 time=1ms TTL=254
Reply from 10.128.1.6: bytes=32 time<1ms TTL=254
Reply from 10.128.1.6: bytes=32 time=15ms TTL=254

Ping statistics for 10.128.1.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 4ms
```

Рис. 23: Проверка правильности работы правил

Результаты

Результат

- Созданы правила доступа к разным устройствам сети.
- В сеть добавлены ноутбуки администраторов и разрешён доступ к сетевому оборудованию только администраторам.

Вывод

Вывод

Я освоил настройку прав доступа пользователей к ресурсам сети.