Лаборатория работа 10

Настройка списков управления доступом (ACL)

ПОДГОТОВИЛА: КИМ РЕАЧНА
ГРУППА: НПИБД-02-20

Цель работы:

Освоить настройку прав доступа пользователей к ресурсам сети.

Задание:

1. Требуется настроить следующие правила доступа:
    - web-сервер
    - файловый сервер
    - почтовый сервер:
    - DNS-сервер: открыть порт 53 протокола UDP для доступа из внутренней сети;
    - разрешить icmp-сообщения, направленные в сеть серверов;
    - запретить для сети Other любые запросы за пределы сети, за исключением администратора;
    - разрешить доступ в сеть управления сетевым оборудованием только администратору сети.
2. Требуется проверить правильность действия установленных правил доступа.

Настройка доступа к web-серверу

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

```
msk-donskaya-kim-gw-1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-kim-gw-1(config)#interface f0/0.3
msk-donskaya-kim-gw-1(config-subif)#ip access-group servers-out out
```

```
msk-donskaya-kim-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-kim-gw-1(config)#ip access-list extended servers-out
msk-donskaya-kim-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp
msk-donskaya-kim-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host 10.128.0.2 eq telnet
```

```
C:\>
C:\>ftp 10.128.0.2
Trying to connect...10.128.0.2
Connected to 10.128.0.2
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
```

```
C:\>ping 10.128.0.2

Pinging 10.128.0.2 with 32 bytes of data:

Reply from 10.128.6.1: Destination host unreachable.
Reply from 10.128.6.1: Destination host unreachable.
Reply from 10.128.6.1: Destination host unreachable.
Reply from 10.128.6.1: Destination host unreachable.

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

C:\>ping 10.128.0.5

Pinging 10.128.0.5 with 32 bytes of data:

Reply from 10.128.6.1: Destination host unreachable.
Reply from 10.128.6.1: Destination host unreachable.
Reply from 10.128.6.1: Destination host unreachable.
Reply from 10.128.6.1: Destination host unreachable.

Ping statistics for 10.128.0.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Настройка доступа к файловому серверу

```
msk-donskaya-kim-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-kim-gw-1(config)#ip access-list extended servers-out
msk-donskaya-kim-gw-1(config-ext-nacl)#remark file
msk-donskaya-kim-gw-1(config-ext-nacl)#permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3 eq 445
msk-donskaya-kim-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.3 range 20 ftp
```

Настройка доступа к почтовому серверу

```
msk-donskaya-kim-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-kim-gw-1(config)#ip access-list extended servers-out
msk-donskaya-kim-gw-1(config-ext-nacl)#remark mail
msk-donskaya-kim-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.4 eq smtp
msk-donskaya-kim-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.4 eq pop3
```

Настройка доступа к DNS-серверу

```
msk-donskaya-kim-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-kim-gw-1(config)#ip access-list extended servers-out
msk-donskaya-kim-gw-1(config-ext-nacl)#remark dns
msk-donskaya-kim-gw-1(config-ext-nacl)#permit udp 10.128.0.0 0.0.255.255 host 10.128.0.5 eq 53
```

Разрешить icmp-сообщения

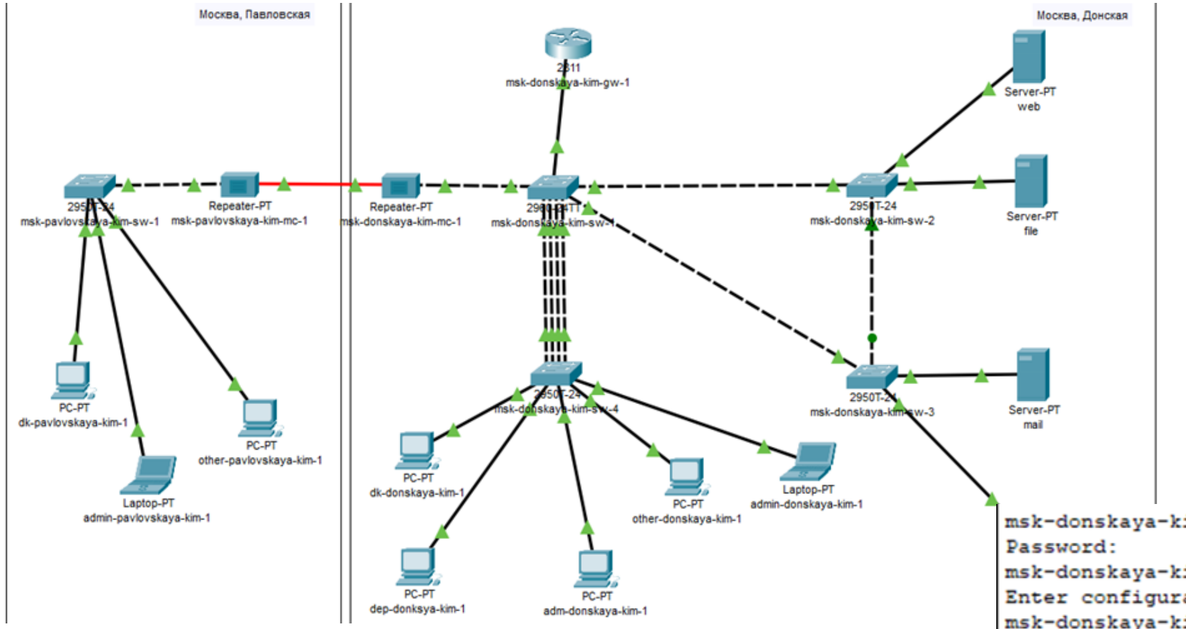
```
msk-donskaya-kim-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-kim-gw-1(config)#ip access-list extended servers-out
msk-donskaya-kim-gw-1(config-ext-nacl)#1 permit icmp any any
```

Настройка доступа для сети Other

```
msk-donskaya-kim-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-kim-gw-1(config)#ip access-list extended other-in
msk-donskaya-kim-gw-1(config-ext-nacl)#remark admin
msk-donskaya-kim-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 any
msk-donskaya-kim-gw-1(config-ext-nacl)#exit
msk-donskaya-kim-gw-1(config)#int f0/0.104
msk-donskaya-kim-gw-1(config-subif)#ip access-group other-in in
```

Настройка доступа администратора к сети

```
msk-donskaya-kim-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-kim-gw-1(config)#ip access-list extended management-out
msk-donskaya-kim-gw-1(config-ext-nacl)#remark admin
msk-donskaya-kim-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 10.128.1.0 0.0.0.255
msk-donskaya-kim-gw-1(config-ext-nacl)#exit
msk-donskaya-kim-gw-1(config)#int f0/0.2
msk-donskaya-kim-gw-1(config-subif)#ip access-group management-out out
```




```
msk-donskaya-kim-gw-1>en
Password:
msk-donskaya-kim-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-kim-gw-1(config)#ip access-list extended servers-out
msk-donskaya-kim-gw-1(config-ext-nacl)#permit tcp host 10.128.6.201 host 10.128.0.2 range 20 ftp
msk-donskaya-kim-gw-1(config-ext-nacl)#permit tcp host 10.128.6.201 host 10.128.0.2 eq telnet
msk-donskaya-kim-gw-1(config-ext-nacl)#exit
msk-donskaya-kim-gw-1(config)#ip access-list extended other-in
msk-donskaya-kim-gw-1(config-ext-nacl)#remark admin
msk-donskaya-kim-gw-1(config-ext-nacl)#permit ip host 10.128.6.201 any
msk-donskaya-kim-gw-1(config-ext-nacl)#exit
msk-donskaya-kim-gw-1(config)#int f0/0.104
msk-donskaya-kim-gw-1(config-subif)#ip access-group other-in in
msk-donskaya-kim-gw-1(config-subif)#exit
msk-donskaya-kim-gw-1(config)#ip access-list extended management-out
msk-donskaya-kim-gw-1(config-ext-nacl)#remark admin
msk-donskaya-kim-gw-1(config-ext-nacl)#permit ip host 10.128.6.201 10.128.1.0 0.0.0.255
msk-donskaya-kim-gw-1(config-ext-nacl)#exit
msk-donskaya-kim-gw-1(config)#int f0/0.2
msk-donskaya-kim-gw-1(config-subif)#ip access-group management-out out
msk-donskaya-kim-gw-1(config-subif)#^Z
msk-donskaya-kim-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-kim-gw-1#wr m
```

Вывод

Освоила настройку прав доступа пользователей к ресурсам сети.

Спасибо за внимание!