Лабораторная работа № 10. Настройка списков управления доступом (ACL)

10.1. Цель работы

Освоить настройку прав доступа пользователей к ресурсам сети.

10.2. Задание

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. Требуется проверить правильность действия установленных правил доступа.
3. Требуется выполнить задание для самостоятельной работы по настройке прав доступа администратора сети на Павловской.
4. При выполнении работы необходимо учитывать соглашение об именовании (см. раздел 2.5).

10.3. Последовательность выполнения работы

В рабочей области проекта подключите ноутбук администратора с именем `admin` к сети к `other-donskaya-1` с тем, чтобы разрешить ему потом любые действия, связанные с управлением сетью. Для этого подсоедините ноутбук к порту 24 коммутатора `msk-donskaya-sw-4` и присвойте ему статический адрес `10.128.6.200`, указав в качестве gateway-адреса `10.128.6.1` и адреса DNS-сервера `10.128.0.5` (рис. 10.1).

Права доступа пользователей сети (см. рис. 9.2) будем настраивать на маршрутизаторе `msk-donskaya-gw-1`, поскольку именно через него проходит весь трафик сети. Ограничения можно накладывать как на входящий (in), так и на исходящий (out) трафик. По отношению к маршрутизатору накладываемые ограничения будут касаться в основном исходящего трафика.

Различают стандартные (standard) и расширенные (extended) списки контроля доступа (Access Control List, ACL). Стандартные ACL проверяют только адрес источника трафика, расширенные — адрес как источника, так и получателя, тип протокола и TCP/UDP порты.

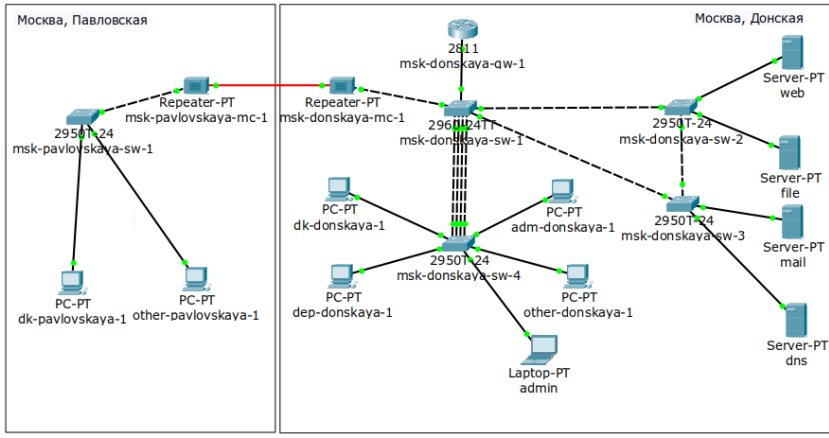

Рис. 10.1. Размещение ноутбука администратора в сети other-donskaya-1

Следует помнить, что на оборудовании Cisco правила в списке доступа проверяются по порядку сверху вниз до первого совпадения — как только одно из правил сработало, проверка списка правил прекращается и обработка трафика происходит на основе сработавшего правила. Поэтому рекомендуется сначала дать разрешение (permit) на какое-то действие, а уже потом накладывать ограничения (deny). Кроме того, после всех правил в конце дописывается неявное запрещение на всё, что не разрешено: `deny ip any any` (implicit deny).

1. Настройка доступа к web-серверу по порту tcp 80:

```
msk-donskaya-gw-1#configure terminal
msk-donskaya-gw-1(config)#ip access-list extended servers-out
msk-donskaya-gw-1(config-ext-nacl)#remark web
msk-donskaya-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.2 eq 80
```

   Здесь: создан список контроля доступа с названием `servers-out` (так как предполагается ограничить доступ в конкретные подсети и по отношению к маршрутизатору это будет исходящий трафик); указано (в качестве комментария-напоминания `remark web`), что ограничения предназначены для работы с web-сервером; дано разрешение доступа (`permit`) по протоколу TCP всем (`any`) пользователям сети (`host`) на доступ к web-серверу, имеющему адрес `10.128.0.2`, через порт `80`.

2. Добавление списка управления доступом к интерфейсу:

```
msk-donskaya-gw-1#configure terminal
msk-donskaya-gw-1(config)#interface f0/0.3
msk-donskaya-gw-1(config-subif)#ip access-group servers-out out
```

   Здесь: к интерфейсу `f0/0.3` подключается список прав доступа `servers-out` и применяется к исходящему трафику (`out`).
   Можно проверить, что доступ к web-серверу есть через протокол HTTP (введя в строке браузера хоста ip-адрес web-сервера). При этом команда

`ping` будет демонстрировать недоступность web-сервера как по имени, так и по ip-адресу web-сервера.

3. Дополнительный доступ для администратора по протоколам Telnet и FTP:

```
msk-donskaya-gw-1#configure terminal
msk-donskaya-gw-1(config)#ip access-list extended servers-out
msk-donskaya-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host
    ↪ 10.128.0.2 range 20 ftp
msk-donskaya-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host
    ↪ 10.128.0.2 eq telnet
```

Здесь: в список контроля доступа servers-out добавлено правило, разрешающее устройству администратора с ip-адресом 10.128.6.200 доступ на web-сервер (10.128.0.2) по протоколам FTP и telnet.
Убедитесь, что с узла с ip-адресом 10.128.6.200 есть доступ по протоколу FTP. Для этого в командной строке устройства администратора введите `ftp 10.128.0.2`, а затем по запросу имя пользователя `cisco` и пароль `cisco` (рис. 10.2).

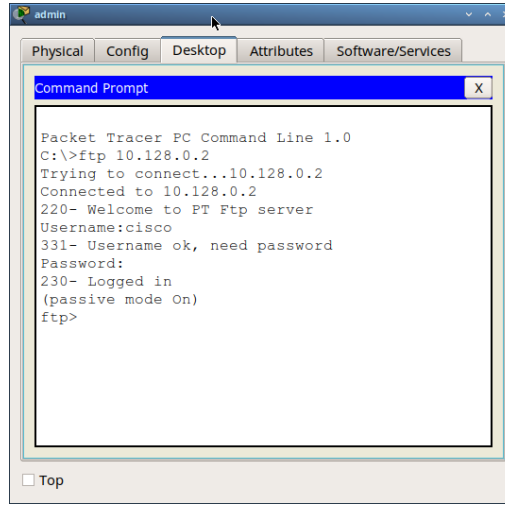

Рис. 10.2. Проверка доступа к web-серверу по протоколу FTP с устройства администратора

Попробуйте провести аналогичную процедуру с другого устройства сети. Убедитесь, что доступ будет запрещён.

4. Настройка доступа к файловому серверу:

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

Здесь: в списке контроля доступа `servers-out` указано (в качестве комментария-напоминания `remark file`), что следующие ограничения предназначены для работы с file-сервером; всем узлам внутренней сети (10.128.0.0) разрешён доступ по протоколу SMB (работает через порт 445 протокола TCP) к каталогам общего пользования; любым узлам разрешён доступ к file-серверу по протоколу FTP. Запись 0.0.255.255 — обратная маска (wildcard mask).

5. Настройка доступа к почтовому серверу:

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

Здесь: в списке контроля доступа `servers-out` указано (в качестве комментария-напоминания `remark mail`), что следующие ограничения предназначены для работы с почтовым сервером; всем разрешён доступ к почтовому серверу по протоколам POP3 и SMTP.

6. Настройка доступа к DNS-серверу:

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

Здесь: в списке контроля доступа `servers-out` указано (в качестве комментария-напоминания `remark dns`), что следующие ограничения предназначены для работы с DNS-сервером; всем узлам внутренней сети разрешён доступ к DNS-серверу через UDP-порт 53.
Проверьте доступность web-сервера (через браузер) не только по ip-адресу, но и по имени.

7. Разрешение icmp-запросов:

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

Здесь демонстрируется явное управление порядком размещения правил — правило разрешения для icmp-запросов добавляется в начало списка контроля доступа. Номера строк правил в списке контроля доступа можно посмотреть с помощью команды

```
msk-donskaya-gw-1#show access-lists
```

8. Настройка доступа для сети Other (требуется наложить ограничение на исходящий из сети Other трафик, который по отношению к маршрутизатору `msk-donskaya-gw-1` является входящим трафиком):

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

Здесь: в списке контроля доступа `other-in` указано, что следующие правила относятся к администратору сети; даётся разрешение устройству с адресом

10.128.6.200 на любые действия (`any`); к интерфейсу `f0/0.104` подключается список прав доступа `other-in` и применяется к входящему трафику (`in`).

9. Настройка доступа администратора к сети сетевого оборудования:

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

Здесь: в списке контроля доступа `management-out` указано (в качестве комментария-напоминания `remark admin`), что устройству администратора с адресом 10.128.6.200 разрешён доступ к сети сетевого оборудования (10.128.1.0); к интерфейсу `f0/0.2` подключается список прав доступа `management-out` и применяется к исходящему трафику (`out`).

10.4. Самостоятельная работа

1. Проверьте корректность установленных правил доступа, попытавшись получить доступ по различным протоколам с разных устройств сети к подсети серверов и подсети сетевого оборудования.
2. Разрешите администратору из сети Other на Павловской действия, аналогичные действиям администратора сети Other на Донской.

10.5. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
   - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
   - подробное описание настроек сетевого оборудования в соответствии с заданием;
   - результаты проверки корректности настроек сетевого оборудования в соответствии с заданием (подтверждённые скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

10.6. Контрольные вопросы

1. Как задать действие правила для конкретного протокола?
2. Как задать действие правила сразу для нескольких портов?
3. Как узнать номер правила в списке прав доступа?
4. Каким образом можно изменить порядок применения правил в списке контроля доступа?

Литература по теме

1. 802.1D-2004 - IEEE Standard for Local and Metropolitan Area Networks. Media Access Control (MAC) Bridges : тех. отч. / IEEE. — 2004. — С. 1—277. — DOI: 10.1109/IEEESTD.2004.94569. — URL: http://ieeexplore.ieee.org/servlet/opac?punumber=9155.
2. 802.1Q - Virtual LANs. — URL: http://www.ieee802.org/1/pages/802.1Q.html.
3. *A J.* Packet Tracer Network Simulator. — Packt Publishing, 2014. — ISBN 9781782170426. — URL: https://books.google.com/books?id=eVOcAgAAQBAJ&dq=cisco+packet+tracer&hl=es&source=gbs_navlinks_s.
4. *Cotton M., Vegoda L.* Special Use IPv4 Addresses : RFC / RFC Editor. — 01.2010. — С. 1—11. — № 5735. — DOI: 10.17487/rfc5735. — URL: https://www.rfc-editor.org/info/rfc5735.
5. *Droms R.* Dynamic Host Configuration Protocol : RFC / RFC Editor. — 03.1997. — С. 1—45. — № 2136. — DOI: 10.17487/rfc2131. — URL: https://www.ietf.org/rfc/rfc2131.txt%20https://www.rfc-editor.org/info/rfc2131.
6. *McPherson D., Dykes B.* VLAN Aggregation for Efficient IP Address Allocation, RFC 3069. — 2001. — URL: http://www.ietf.org/rfc/rfc3069.txt.
7. *Moy J.* OSPF Version 2 : RFC / RFC Editor. — 1998. — С. 244. — DOI: 10.17487/rfc2328. — URL: https://www.rfc-editor.org/info/rfc2328.
8. NAT Order of Operation. — URL: https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/6209-5.html.
9. NAT: вопросы и ответы / Сайт поддержки продуктов и технологий компании Cisco. — URL: https://www.cisco.com/cisco/web/support/RU/9/92/92029_nat-faq.html.
10. *Neumann J. C.* Cisco Routers for the Small Business A Practical Guide for IT Professionals. — Apress, 2009.
11. *Odom S., Nottingham H.* Cisco Switching: Black Book. — The Coriolis Group, 2001. — ISBN 9781576107065. — URL: http://books.google.sk/books?id=GYsLAAAACAAJ.
12. *Tetz E.* Cisco Networking All-in-One For Dummies. — Indianapolis, Indiana : John Wiley & Sons, Inc., 2011. — (For Dummies). — URL: http://www.dummies.com/store/product/Cisco-Networking-All-in-One-For-Dummies.productCd-0470945583.html.
13. ГОСТ Р ИСО/МЭК 7498-1-99. — «ВОС. Базовая эталонная модель. Часть 1. Базовая модель». — ОКС: 35.100.70. — Действует с 01.01.2000. — URL: http://protect.gost.ru/v.aspx?control=7&id=132355.
14. *Кларк К., Гамильтон К.* Принципы коммутации в локальных сетях Cisco. — М. : Вильямс, 2003. — (Cisco Press Core Series). — ISBN 5-8459-0464-1.
15. *Королькова А. В., Кулябов Д. С.* Архитектура и принципы построения современных сетей и систем телекоммуникаций. — М. : Издательство РУДН, 2009.

16. *Королькова А. В.*, *Кулябов Д. С.* Прикладные протоколы Интернет и www. Курс лекций. — М. : РУДН, 2012. — ISBN 9785209049500.

17. *Королькова А. В.*, *Кулябов Д. С.* Прикладные протоколы Интернет и www. Лабораторные работы. — М. : РУДН, 2012. — ISBN 9785209049357.

18. *Королькова А. В.*, *Кулябов Д. С.* Сетевые технологии. Лабораторные работы. — М. : РУДН, 2014. — ISBN 785209056065.

19. *Куроуз Д. Ф.*, *Росс К. В.* Компьютерные сети. Нисходящий подход. — 6-е изд. — М. : Издательство «Э», 2016. — (Мировой компьютерный бестселлер).

20. *Одом У.* Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101. — М. : Вильямс, 2017. — (Cisco Press Core Series). — ISBN 978-5-8459-1906-9.

21. *Одом У.* Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101. Маршрутизация и коммутация. — М. : Вильямс, 2016. — (Cisco Press Core Series).

22. *Олифер В. Г.*, *Олифер Н. А.* Компьютерные сети. Принципы, технологии, протоколы. — 5-е изд. — Питер : Питер, 2017. — (Учебник для вузов). — ISBN 978-5-496-01967-5.

23. Сети и системы передачи информации: телекоммуникационные сети / К. Е. Самуйлов [и др.]. — М. : Изд-во Юрайт, 2016. — ISBN 978-5-9916-7198-9.

24. *Таненбаум Э.*, *Уэзеролл Д.* Компьютерные сети. — 5 изд. — Питер : Питер, 2016. — (Классика Computer Science). — ISBN 978-5-496-00831-0.

25. *Хилл Б.* Полный справочник по Cisco. — М. : Вильямс, 2009. — ISBN 978-5-8459-1309-8.

26. Цикл статей «Сети для самых маленьких». — URL: `http://linkmeup.ru/blog/11.html`.

27. Часто задаваемые вопросы технологии NAT / Сайт поддержки продуктов и технологий компании Cisco. — URL: `https://www.cisco.com/c/ru_ru/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html`.