# Лабораторная работа Настройка ACL

### Общая информация

#### О лабораторной работе

Список контроля доступа (Access Control List, ACL) — это набор правил, разрешающих или запрещающих доступ. В каждом правиле определяется условие сопоставления пакетов. Это может быть адрес источника, адрес пункта назначения или номер порта.

ACL — это механизм фильтрации пакетов на основе правил. Пакеты, соответствующие списку ACL, обрабатываются на основе политики, определенной в ACL.

#### Цели

Лабораторная работа помогает получить практические навыки по изучению следующих тем:

* Настройка списков ACL
* Применение ACL на интерфейсе
* Основные методы фильтрации трафика

#### Топология сети

В сети, показанной на схеме, маршрутизатор R3 выполняет функции сервера, маршрутизатор R1 выполняет функции клиента, и они доступны для связи. Физические интерфейсы, соединяющие R1 и R2, имеют IP-адреса 10.1.2.1/24 и 10.1.2.2/24 соответственно, а физические интерфейсы, соединяющие R2 и R3, —   
IP-адреса 10.1.3.2/24 и 10.1.3.1/24. Кроме того, на маршрутизаторе R1 созданы два логических интерфейса LoopBack 0 и LoopBack 1 для имитации двух пользователей-клиентов. Два интерфейса имеют IP-адреса 10.1.1.1/24 и 10.1.4.1/24 соответственно.

Один пользователь (LoopBack 1 на R1) должен удаленно управлять R3. Для гарантии того, что вход в R3 будет разрешен только пользователю, который соответствует политике безопасности, можно настроить Telnet на сервере, задать защиту паролем и сконфигурировать ACL.

Топология сети для конфигурирования ACL, используемая в данной лабораторной работе

Изображение выглядит как текст, устройство

Автоматически созданное описание

### Лабораторная работа

#### План работы

Настройка IP-адресов.

Настройка OSPF для обеспечения возможности сетевого подключения.

Создание ACL на основе необходимого трафика.

Настройка фильтрации трафика.

#### Процедура конфигурирования

Настройте IP-адреса.

# Настройте IP-адреса для маршрутизаторов R1, R2 и R3.

[R1]interface GigabitEthernet0/0/3

[R1-GigabitEthernet0/0/3]ip address 10.1.2.1 24

[R1-GigabitEthernet0/0/3]quit

[R1]interface LoopBack 0

[R1-LoopBack0]ip address 10.1.1.1 24

[R1-LoopBack0]quit

[R1]interface LoopBack 1

[R1-LoopBack1]ip address 10.1.4.1 24

[R1-LoopBack0]quit

[R2]interface GigabitEthernet 0/0/3

[R2-GigabitEthernet0/0/3]ip address 10.1.2.2 24

[R2-GigabitEthernet0/0/3]quit

[R2]interface GigabitEthernet 0/0/4

[R2-GigabitEthernet0/0/4]ip address 10.1.3.2 24

[R2-GigabitEthernet0/0/4]quit

[R3]interface GigabitEthernet0/0/3

[R3-GigabitEthernet0/0/3]ip address 10.1.3.1 24

[R3-GigabitEthernet0/0/3]quit

Настройте OSPF для обеспечения возможности сетевого подключения.

# Настройте OSPF на маршрутизаторах R1, R2 и R3 и назначьте их в область 0, чтобы обеспечить возможность подключения.

[R1]ospf

[R1-ospf-1]area 0

[R1-ospf-1-area-0.0.0.0]network 10.1.1.1 0.0.0.0

[R1-ospf-1-area-0.0.0.0]network 10.1.2.1 0.0.0.0

[R1-ospf-1-area-0.0.0.0]network 10.1.4.1 0.0.0.0

[R1-ospf-1-area-0.0.0.0]return

[R2]ospf

[R2-ospf-1]area 0

[R2-ospf-1-area-0.0.0.0]network 10.1.2.2 0.0.0.0

[R2-ospf-1-area-0.0.0.0]network 10.1.3.2 0.0.0.0

[R2-ospf-1-area-0.0.0.0]return

[R3]ospf

[R3-ospf-1]area 0

[R3-ospf-1-area-0.0.0.0]network 10.1.3.1 0.0.0.0

[R3-ospf-1-area-0.0.0.0]return

# Выполните команду ping на маршрутизаторе R3, чтобы проверить возможность подключения к сети.

<R3>ping 10.1.1.1

PING 10.1.1.1: 56 data bytes, press CTRL\_C to break

Reply from 10.1.1.1: bytes=56 Sequence=1 ttl=254 time=40 ms

Reply from 10.1.1.1: bytes=56 Sequence=2 ttl=254 time=40 ms

Reply from 10.1.1.1: bytes=56 Sequence=3 ttl=254 time=20 ms

Reply from 10.1.1.1: bytes=56 Sequence=4 ttl=254 time=40 ms

Reply from 10.1.1.1: bytes=56 Sequence=5 ttl=254 time=30 ms

--- 10.1.1.1 ping statistics ---

5 packet(s) transmitted

5 packet(s) received

0.00% packet loss

round-trip min/avg/max = 20/34/40 ms

<R3>ping 10.1.2.1

PING 10.1.2.1: 56 data bytes, press CTRL\_C to break

Reply from 10.1.2.1: bytes=56 Sequence=1 ttl=254 time=30 ms

Reply from 10.1.2.1: bytes=56 Sequence=2 ttl=254 time=30 ms

Reply from 10.1.2.1: bytes=56 Sequence=3 ttl=254 time=30 ms

Reply from 10.1.2.1: bytes=56 Sequence=4 ttl=254 time=30 ms

Reply from 10.1.2.1: bytes=56 Sequence=5 ttl=254 time=50 ms

--- 10.1.2.1 ping statistics ---

5 packet(s) transmitted

5 packet(s) received

0.00% packet loss

round-trip min/avg/max = 30/34/50 ms

<R3>ping 10.1.4.1

PING 10.1.4.1: 56 data bytes, press CTRL\_C to break

Reply from 10.1.4.1: bytes=56 Sequence=1 ttl=254 time=50 ms

Reply from 10.1.4.1: bytes=56 Sequence=2 ttl=254 time=30 ms

Reply from 10.1.4.1: bytes=56 Sequence=3 ttl=254 time=40 ms

Reply from 10.1.4.1: bytes=56 Sequence=4 ttl=254 time=30 ms

Reply from 10.1.4.1: bytes=56 Sequence=5 ttl=254 time=30 ms

--- 10.1.4.1 ping statistics ---

5 packet(s) transmitted

5 packet(s) received

0.00% packet loss

round-trip min/avg/max = 30/36/50 ms

Сконфигурируйте R3 в качестве сервера.

# Включите функцию Telnet на R3, установите для уровня пользователя значение 3 и задайте для входа пароль — Huawei@123.

[R3]telnet server enable

Команда **telnet server enable** позволяет включить службу Telnet.

[R3]user-interface vty 0 4

Команда **user-interface** позволяет перейти в режим интерфейса одного или нескольких пользователей.

Пользовательский интерфейс терминала виртуального типа (Virtual Type Terminal, VTY) осуществляет управление и мониторинг входа пользователей в систему с помощью Telnet или SSH.

[R3-ui-vty0-4]user privilege level 3

[R3-ui-vty0-4] set authentication password cipher

Warning: The "password" authentication mode is not secure, and it is strongly recommended to use "aaa" authentication mode.

Enter Password(<8-128>):Huawei@123

Confirm password:Huawei@123

[R3-ui-vty0-4] quit

Настройте ACL на основе необходимого трафика.

Способ 1. Настройте ACL на интерфейсе VTY маршрутизатора R3, чтобы разрешить вход с R1 в R3 через Telnet, используя IP-адрес LoopBack 1.

# Настройте ACL на R3.

[R3]acl 3000

[R3-acl-adv-3000]rule 5 permit tcp source 10.1.4.1 0.0.0.0 destination 10.1.3.1 0.0.0.0 destination-port eq 23

[R3-acl-adv-3000]rule 10 deny tcp source any

[R3-acl-adv-3000]quit

# Выполните фильтрацию трафика на интерфейсе VTY маршрутизатора R3.

[R3]user-interface vty 0 4

[R3-ui-vty0-4]acl 3000 inbound

# Выведите на экран конфигурацию ACL на R3.

[R3]display acl 3000

Команда **display acl** позволяет вывести на экран конфигурацию ACL.

Advanced ACL 3000, 2 rules

Создан расширенный ACL. Он имеет номер 3000 и содержит два правила.

Acl's step is 5

Правила ACL пронумерованы с шагом 5.

rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq telnet

Правило 5 разрешает прохождение соответствующего трафика. Если пакетов, соответствующих правилу, нет, поле **matches** не отображается.

rule 10 deny tcp

Способ 2. Настройте ACL на физическом интерфейсе маршрутизатора R2, чтобы разрешить вход с R1 в R3 через Telnet, используя IP-адрес физического интерфейса.

# Настройте ACL на R2.

[R2]acl 3001

[R2-acl-adv-3001]rule 5 permit tcp source 10.1.4.1 0.0.0.0 destination 10.1.3.1 0.0.0.0 destination-port eq 23

[R2-acl-adv-3001]rule 10 deny tcp source any

[R2-acl-adv-3001]quit

# Выполните фильтрацию трафика на интерфейсе GE0/0/3 маршрутизатора R3.

[R2]interface GigabitEthernet0/0/3

[R2-GigabitEthernet0/0/3]traffic-filter inbound acl 3001

# Выведите на экран конфигурацию ACL на R2.

[R2]display acl 3001

Advanced ACL 3001, 2 rules

Acl's step is 5

rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq telnet (21 matches)

Правило 5 разрешает прохождение соответствующего трафика. Поле **matches** показывает 21 соответствие пакетов правилу.

rule 10 deny tcp (1 matches)

----Конец

### Проверка

Протестируйте доступ через Telnet и проверьте конфигурацию ACL.

На маршрутизаторе R1 подключитесь через Telnet к серверу, используя указанный IP-адрес источника 10.1.1.1.

<R1>telnet -a 10.1.1.1 10.1.3.1

Команда **telnet** позволяет использовать протокол Telnet для входа на другое устройство.

-a *source-ip-address*: определяет IP-адрес источника. Пользователи могут связываться с сервером, используя указанный IP-адрес.

Press CTRL\_] to quit telnet mode

Trying 10.1.3.1 ...

Error: Can't connect to the remote host

На маршрутизаторе R1 подключитесь через Telnet к серверу, используя указанный IP-адрес источника 10.1.4.1.

<R1>telnet -a 10.1.4.1 10.1.3.1

Press CTRL\_] to quit telnet mode

Trying 10.1.3.1 ...

Connected to 10.1.3.1 ...

Login authentication

Password:

<R3>quit

### Справочные конфигурации (Способ 1)

Конфигурация на R1

#

sysname R1

#

interface GigabitEthernet0/0/3

ip address 10.1.2.1 255.255.255.0

#

interface LoopBack0

ip address 10.1.1.1 255.255.255.0

#

interface LoopBack1

ip address 10.1.4.1 255.255.255.0

#

ospf 1

area 0.0.0.0

network 10.1.1.1 0.0.0.0

network 10.1.2.1 0.0.0.0

network 10.1.4.1 0.0.0.0

#

return

Конфигурация на R2

#

sysname R2

#

interface GigabitEthernet0/0/3

ip address 10.1.2.2 255.255.255.0

#

interface GigabitEthernet0/0/4

ip address 10.1.3.2 255.255.255.0

#

ospf 1

area 0.0.0.0

network 10.1.2.2 0.0.0.0

network 10.1.3.2 0.0.0.0

#

return

Конфигурация на R3

#

sysname R3

#

acl number 3000

rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq telnet

rule 10 deny tcp

#

interface GigabitEthernet0/0/3

ip address 10.1.3.1 255.255.255.0

#

ospf 1

area 0.0.0.0

network 10.1.3.1 0.0.0.0

#

telnet server enable

#

user-interface vty 0 4

acl 3000 inbound

authentication-mode password

user privilege level 3

set authentication password cipher %^%#Z5)H#8cE(YJ6YZ:='}c-;trp&784i>HtKl~pLnn>2zL16cs<6E}xj.FmK5(8%^%#

#

return

### Справочные конфигурации (Способ 2)

Конфигурация на R1

#

sysname R1

#

interface GigabitEthernet0/0/3

ip address 10.1.2.1 255.255.255.0

#

interface LoopBack0

ip address 10.1.1.1 255.255.255.0

#

interface LoopBack1

ip address 10.1.4.1 255.255.255.0

#

ospf 1

area 0.0.0.0

network 10.1.1.1 0.0.0.0

network 10.1.2.1 0.0.0.0

network 10.1.4.1 0.0.0.0

#

return

Конфигурация на R2

#

sysname R2

#

acl number 3001

rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq telnet

rule 10 deny tcp

#

interface GigabitEthernet0/0/3

ip address 10.1.2.2 255.255.255.0

traffic-filter inbound acl 3001

#

interface GigabitEthernet0/0/4

ip address 10.1.3.2 255.255.255.0

#

ospf 1

area 0.0.0.0

network 10.1.2.2 0.0.0.0

network 10.1.3.2 0.0.0.0

#

return

Конфигурация на R3

#

sysname R3

#

interface GigabitEthernet0/0/3

ip address 10.1.3.1 255.255.255.0

#

ospf 1

area 0.0.0.0

network 10.1.3.1 0.0.0.0

#

telnet server enable

#

user-interface vty 0 4

authentication-mode password

user privilege level 3

set authentication password cipher %^%#Z5)H#8cE(YJ6YZ:='}c-;trp&784i>HtKl~pLnn>2zL16cs<6E}xj.FmK5(8%^%#

#

return

### Вопросы

R3 выполняет функции как сервера Telnet, так и FTP-сервера, IP-адрес LoopBack 0 на R1 должен использоваться только для доступа к службе FTP, а IP-адрес LoopBack 1 на R1 должен использоваться для удаленного управления R3 через Telnet.

Настройте ACL в соответствии с приведенными требованиями.