Университет ИТМО

Факультет программной инженерии и компьютерной техники

Лабораторная работа №4 по Администрированию систем и сетей

«Основы сетевой безопасности и доступа к сети»

Работу выполнили студенты группы P34101: Патутин Владимир  
Крюков Андрей

Преподаватель:   
Афанасьев Дмитрий Борисович

Желаемая оценка: 3

Санкт-Петербург

Оглавление

[Топология: 3](#_Toc117609758)

[Шаг 1 Настройте IP-адреса 3](#_Toc117609759)

[Шаг 2 Настройте OSPF для обеспечения возможности сетевого подключения. 4](#_Toc117609760)

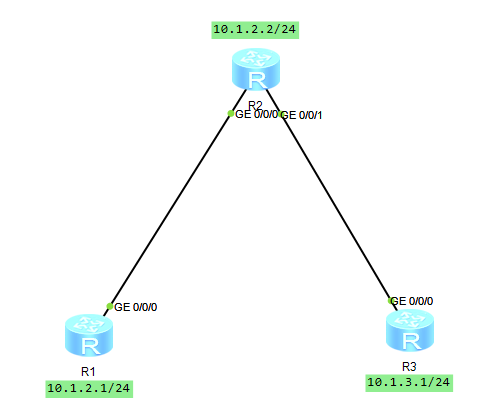
[Шаг 3 Сконфигурируйте R3 в качестве сервера 5](#_Toc117609761)

[Шаг 4 Настройте ACL на основе необходимого трафика. 5](#_Toc117609762)

[Шаг 5 Проверка 6](#_Toc117609763)

[Выводы: 6](#_Toc117609764)

# Топология:



# Шаг 1 Настройте IP-адреса

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

<Huawei>system-view

[Huawei]sysname R1

[R1]interface GigabitEthernet0/0/0

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

[R1-GigabitEthernet0/0/0]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-LoopBack1]quit

[R1]

<Huawei>system-view

[Huawei]sysname R2

[R2]interface GigabitEthernet 0/0/0

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

[R2-GigabitEthernet0/0/0]quit

[R2]interface GigabitEthernet 0/0/1

[R2-GigabitEthernet0/0/1]ip address 10.1.3.2 24

[R2-GigabitEthernet0/0/1]quit

[R2]

<Huawei>system-view

[Huawei]sysname R3

[R3]interface GigabitEthernet 0/0/0

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

[R3-GigabitEthernet0/0/0]quit

[R3]

# Шаг 2 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=100 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=30 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=50 ms

--- 10.1.1.1 ping statistics ---

5 packet(s) transmitted

5 packet(s) received

0.00% packet loss

round-trip min/avg/max = 30/52/100 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=50 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=40 ms

--- 10.1.2.1 ping statistics ---

5 packet(s) transmitted

5 packet(s) received

0.00% packet loss

round-trip min/avg/max = 30/36/50 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=30 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=60 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 = 30/36/60 ms

<R3>

# Шаг 3 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

Error: TELNET server has been enabled

[R3]user-interface vty 0 4

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

[R3-ui-vty0-4]set authentication password cipher Huawei@123

[R3-ui-vty0-4]quit

[R3]

# Шаг 4 Настройте ACL на основе необходимого трафика.

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 inb

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

[R3-ui-vty0-4]quit

Выведите на экран конфигурацию ACL на R3.

[R3]display acl 3000

Advanced ACL 3000, 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

rule 10 deny tcp

[R3]

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

[R2]

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

[R2]interface GigabitEthernet 0/0/0

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

[R2-GigabitEthernet0/0/0]quit

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

rule 10 deny tcp

[R2]

# Шаг 5 Проверка

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

Press CTRL\_] to quit telnet mode

Trying 10.1.3.1 ...

Error: Can't connect to the remote host

<R1>

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:

Password:

Password:

Configuration console exit, please retry to log on

The connection was closed by the remote host

<R1>

# Выводы:

Лаборатория познакомила нас с ACL, механизмом, который позволяет настраивать политики фильтрации пакетов на основе различных критериев. На практике мы блокировали пакеты от одного маршрутизатора к другому и проверяли блокировку с помощью утилиты telnet.