2 Network Security Basics and Network Access

2.1 Lab 1: ACL Configuration

2.1.1 Introduction

2.1.1.1 About This Lab

An Access Control List (ACL) is a collection of one or more rules. A rule refers to a judgment statement that describes a packet matching condition, which may be a source address, destination address, or port number.

An ACL is a rule-based packet filter. Packets matching an ACL are processed based on the policy defined in the ACL.

2.1.1.2 Objectives

Upon completion of this task, you will be able to:

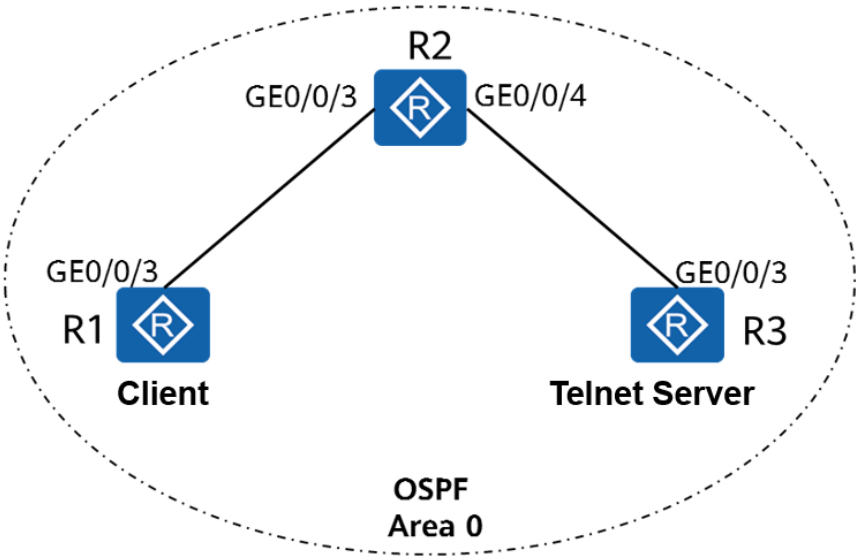
- Learn how to configure ACLs
- Learn how to apply an ACL on an interface
- Understand the basic methods of traffic filtering

2.1.1.3 Networking Topology

As shown in the networking diagram, R3 functions as the server, R1 functions as the client, and they are reachable to reach other. The IP addresses of the physical interfaces connecting R1 and R2 are 10.1.2.1/24 and 10.1.2.2/24 respectively, and the IP addresses of the physical interfaces connecting R2 and R3 are 10.1.3.2/24 and 10.1.3.1/24, respectively. In addition, two logical interfaces LoopBack 0 and LoopBack 1 are created on R1 to simulate two client users. The IP addresses of the two interfaces are 10.1.1.1/24 and 10.1.4.1/24, respectively.

One user (Loopback 1 of R1) needs to remotely manage R3. You can configure Telnet on the server, configure password protection, and configure an ACL to ensure that only the user that meets the security policy can log in to R3.

Figure 2-1 Lab topology for ACL configuration



2.1.2 Lab Configuration

2.1.2.1 Configuration Roadmap

1. Configure IP addresses.
2. Configure OSPF to ensure network connectivity.
3. Create an ACL to match desired traffic.
4. Configure traffic filtering.

2.1.2.2 Configuration Procedure

Step 1 Configure IP addresses.

Configure IP addresses for R1, R2, and 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
```

Step 2 Configure OSPF to ensure network connectivity.

Configure OSPF on R1, R2, and R3 and assign them to area 0 to enable connectivity.

```
[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
```

Run the ping command on R3 to test network connectivity.

```
<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
```

Step 3 Configuration R3 as a server.

Enable the Telnet function on R3, set the user level to 3, and set the login password to Huawei@123.

```
[R3]telnet server enable
```

The **telnet server enable** command enables the Telnet service.

```
[R3]user-interface vty 0 4
```

The **user-interface** command displays one or multiple user interface views.

The Virtual Type Terminal (VTY) user interface manages and monitors users logging in using Telnet or 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
```

Step 4 Configure an ACL to match desired traffic.

Method 1: Configure an ACL on the VTY interface of R3 to allow R1 to log in to R3 through Telnet using the IP address of loopback 1.

Configure an ACL on 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
```

Filter traffic on the VTY interface of R3.

```
[R3]user-interface vty 0 4
[R3-ui-vty0-4]acl 3000 inbound
```

Display the ACL configuration on R3.

```
[R3]display acl 3000
```

The **display acl** command displays the ACL configuration.

```
Advanced ACL 3000, 2 rules
```

An advanced ACL is created. It is numbered 3000 and contains two rules.

```
Acl's step is 5
```

The step between ACL rule numbers is 5.

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

Rule 5 allows matched traffic to pass through. If no packet matches the rule, the **matches** field is not displayed.

```
 rule 10 deny tcp
```

Method 2: Configure an ACL on the physical interface of R2 to allow R1 to log in to R3 through Telnet from the IP address of the physical interface.

Configure an ACL on 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
```

Filter traffic on GE0/0/3 of R3.

```
[R2]interface GigabitEthernet0/0/3
```

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

Display the ACL configuration on 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)
```

Rule 5 allows matched traffic to pass through, and 21 packets have matched the rule.

```
rule 10 deny tcp (1 matches)
```

----End

2.1.3 Verification

Test the Telnet access and verify the ACL configuration.

1. On R1, telnet to the server with the source IP address 10.1.1.1 specified.

```
<R1>telnet -a 10.1.1.1 10.1.3.1
```

The **telnet** command enables a user to use the Telnet protocol to log in to another device.

-a *source-ip-address*: specifies the source IP address. Users can communicate with the server from the specified IP address.

```
 Press CTRL_] to quit telnet mode
 Trying 10.1.3.1 ...
 Error: Can't connect to the remote host
```

2. On R1, telnet to the server with the source IP address 10.1.4.1 specified.

```
<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
```

2.1.4 Configuration Reference (Method 1)

Configuration on 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
```

Configuration on 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
```

Configuration on 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
```

2.1.5 Configuration Reference (Method 2)

Configuration on 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
```

Configuration on 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
```

Configuration on 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
```

2.1.6 Quiz

R3 functions as both a Telnet server and an FTP server, the IP address of loopback 0 on R1 must be used to access only the FTP service, and the IP address of loopback 1 on R1 must be used to remotely manage R3 using Telnet.

Configure an ACL to meet the requirements.