利用 ZBF 做流量控制

一、拓扑

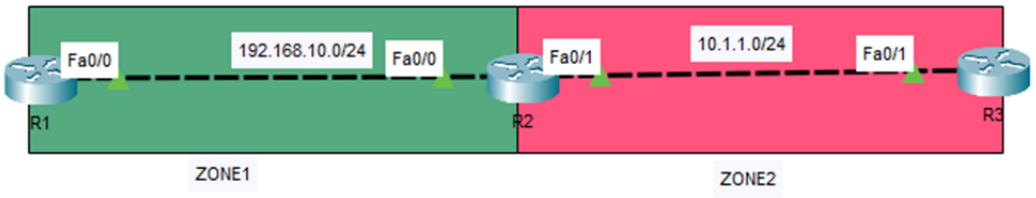

图-1 拓扑

要求：

1. R1、R3 分别以 R2 为网关，实现路由可达，其中 R2 的地址都为 254，R1、R3 都为 1。
2. R1、R3 上分别开启 telnet 登录功能，使 R1、R3 可以互相登录。
3. 实现 R1 可以 telnet 到 R3 上，但不能通过 icmp 方式访问 R3。
4. 实现 R3 可以通过 icmp 访问 R1，但不能 telnet 到 R1 上。

二、配置

1.基本 IP 地址配置（省略）。

2.配置

⑴配置 zone

```
R2(config)#zone security ZONE1
R2(config-sec-zone)#exit
R2(config)#zone security ZONE2
R2(config-sec-zone)#exit
```

⑵将 zone 和接口关联

```
R2(config)#inter f0/0
R2(config-if)#zone-member security ZONE1
R2(config-if)#exit
R2(config)#inter f0/1
R2(config-if)#zone-member security ZONE2
R2(config-if)#exit
```

当路由器上配置完 zone，并将接口关联到 zone 后，不同 zone 之间是不能通信的，现用 R1 访问 R3，结果如下：

```
R1#telnet 10.1.1.1
Trying 10.1.1.1 ...
% Connection timed out; remote host not responding
R1#
```

明显可以看到 R1 不能访问 R3，同样 R3 也不能访问 R1。

```
R3#ping 192.168.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R3#
```

⑶配置策略完成 R1 到 R3 的单向通

①配置 ACL，用于放行 R1 对 R3 的 telnet

```
R2(config)#ip access-list extend R1_TO_R3
R2(config-ext-nacl)#permit tcp host 192.168.10.1 host 10.1.1.1 eq telnet
R2(config-ext-nacl)#exit
```

②配置 class map

```
R2(config)#class-map type inspect match-any ZONE_TO_ZONE2_CLASS
R2(config-cmap)#match access-group name R1_TO_R3
R2(config-cmap)#exit
```

③配置 policy-map

```
R2(config)#policy-map type inspect ZONE1_TO_ZONE2_POLICY
R2(config-pmap)#class type inspect ZONE_TO_ZONE2_CLASS
R2(config-pmap-c)#inspect
```

④配置 zone-pair

```
R2(config)#zone-pair security R1_TO_R3 source ZONE1 destination ZONE2
R2(config-sec-zone-pair)#service-policy type inspect ZONE1_TO_ZONE2_POLICY
R2(config-sec-zone-pair)#exit
```

⑷配置策略完成 R3 到 R1 的单向通

①配置 ACL

```
R2(config)#ip access-list extend R3_TO_R1
R2(config-ext-nacl)#permit icmp host 10.1.1.1 host 192.168.10.1
R2(config-ext-nacl)#exit
```

②配置 class-map

```
R2(config)#class-map type inspect match-any ZONE2_TO_ZONE1_CLASS
R2(config-cmap)#match access-group name R3_TO_R1
R2(config-cmap)#exit
```

③配置 policy-map

```
R2(config)#policy-map type inspect ZONE2_TO_ZONE1
R2(config-pmap)#class type inspect ZONE2_TO_ZONE1_CLASS
R2(config-pmap-c)#inspect
```

④配置 zone-pair

```
R2(config)#zone-pair security ZONE2_TO_ZONE1 source ZONE2 destination ZONE1
R2(config-sec-zone-pair)#service-policy type inspect ZONE2_TO_ZONE1
R2(config-sec-zone-pair)#exit
```

三、测试

1.R1 到 R3 的访问

①R1 通过 telnet 访问 R3

```
R1#telnet 10.1.1.1
Trying 10.1.1.1 ...Open


R3#
```

②R1 通过 icmp 访问 R3

```
R1#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R1#
```

2.R3 到 R1 的访

①R3 通过 telnet 访问 R1

```
R3#telnet 192.168.10.1
Trying 192.168.10.1 ...
% Connection timed out; remote host not responding
R3#
```

②R3 通过 icmp 访问 R1

```
R3#ping 192.168.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

R3#
```

从上面的测试中，可以看到，在 R2 上配置 ZBF，使流量实现了单向通。