实验 7：防火墙和 SSL 实验

一、实验内容

1. 防火墙实验

防火墙实验在虚拟仿真环境下完成，要求如下：

（1）了解包过滤防火墙的基本配置方法、配置命令和配置过程。

（2）利用标准 ACL，将防火墙配置为只允许某个网络中的主机访问另一个网络。

（3）利用扩展 ACL，将防火墙配置为拒绝某个网络中的某台主机访问网络中的 Web 服务器。

（4）将防火墙配置为允许内网用户自由地向外网发起 TCP 连接，同时可以接收外网发回的 TCP 应答数据包。但是，不允许外网的用户主动向内网发起 TCP 连接。

2. SSL 实验（选做）

SSL 实验在实体环境下完成，要求如下：

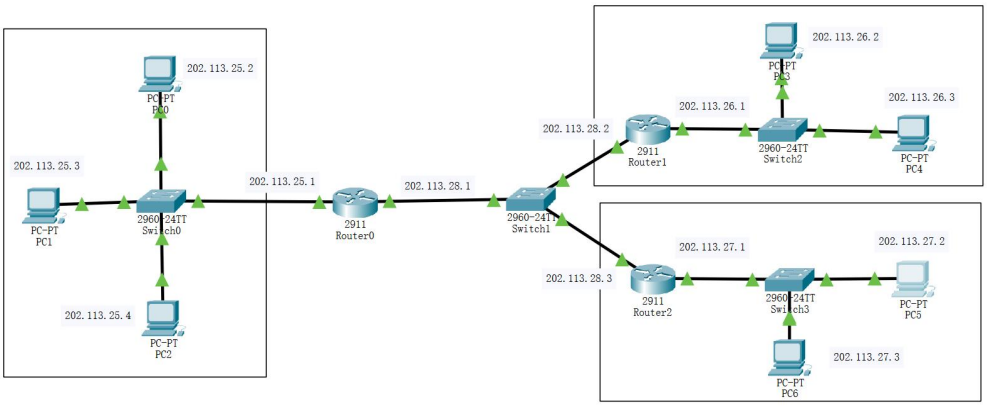
（1）完成 Web 服务器的证书生成、证书审批、证书安装、证书允许等整个过程。

（2）实现浏览器与 Web 服务器的安全通信。

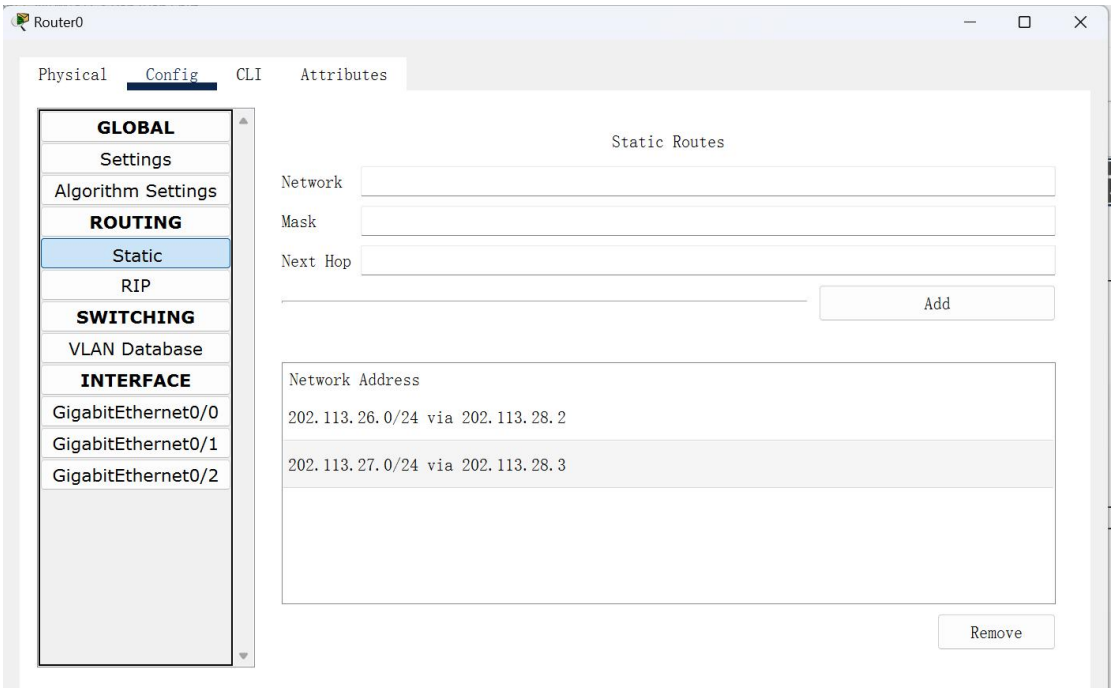
二、实验步骤

在虚拟仿真软件 packet tracer 中，利用路由器实现包过滤防火墙，可以使用 ACL（Access Control List）来实现包过滤防火墙的功能。ACL 用于过滤路由器上的数据流，可应用于网络接口的入站和出站方向，以允许或拒绝特定的数据包通过。需要特别注意的是，本实验所用的思科路由器采用的是默认丢弃的方式处理数据包，也就是说如果没有被设置规则的数据包，路由器是默认丢弃的。

1.使用标准 ACL，将防火墙配置为只允许某个网络中的主机访问另一个网络。网络拓扑图如下，其中共包含四个网络。



首先需要配置主机和路由器的 IP 地址和子网掩码，在路由器中并添加静态路由（这里以 router0 为例）。

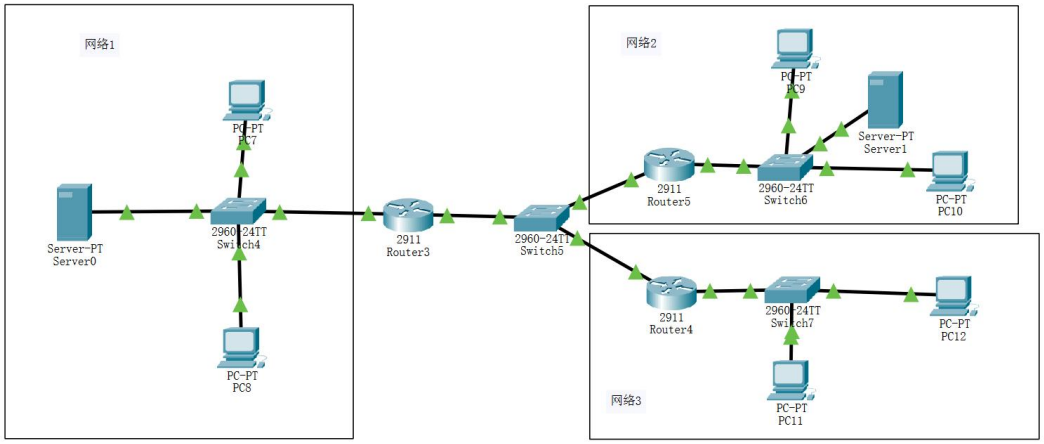


在此互联网中，我们只允许网络 3（202.113.26.0）访问网络 1（202.113.25.0），因此需要在 router0 的右端口设置包过滤防火墙，使用命令 access-list 6 permit 202.113.26.0 0.0.0.255 创建访问控制列表（ACL），然后使用命令 access-list 6 deny any 阻止其他的数据包通过路由器，这里也可以不使用此命令，因为思科路由器会默认自动丢弃其他数据包。最后使用命令 ip access-group 6 in 设置在路由器的 gig0/1 端口过滤数据包。

```
Router#
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 6 permit 202.113.26.0 0.0.0.255
Router(config)#access-list 6 deny any
Router(config)#
Router(config)#
Router(config)#interface fa0/1
%Invalid interface type and number
Router(config)#interface gig0/1
Router(config-if)#ip access-group 6 in
Router(config-if)#
```

2.利用扩展 ACL，将防火墙配置为拒绝某个网络中的某台主机访问网络中的 Web 服务器。网络拓扑图如下，和标准 ACL 的网络拓扑图基本一致，不同的是将 PC1 换成了一台服务器，并在网络 2 中增加了一台服务器用于测试。主机和路由

器的 IP 地址以及静态路由均一致。



在此互联网中，拒绝 PC9 主机访问服务器，因此也需要在 router3 处设置防火墙，使用命令 access-list 106 deny tcp host 202.113.26.2 host 202.113.25.3 eg 80 创建扩展 ACL，拒绝 PC9 主机的 TCP 连接，80 指的是服务器的端口号。由于只是拒绝 PC9 主机，因此还需要使用命令 access-list 106 permit ip any any 允许其他的数据包通过。由于思科路由器的默认丢弃处理，此命令不可省略。最后对路由器的 gig0/1 端口进行设置即可实现扩展 ACL 的配置。

```
Router(config)#access-list 106 deny tcp host 202.113.26.2 host 202.113.25.3 eq 80
Router(config)#access-list 106 permit ip any any
Router(config)#interface gig0/1
Router(config-if)#ip access-group 106 in
Router(config-if)#exit
Router(config)#
```

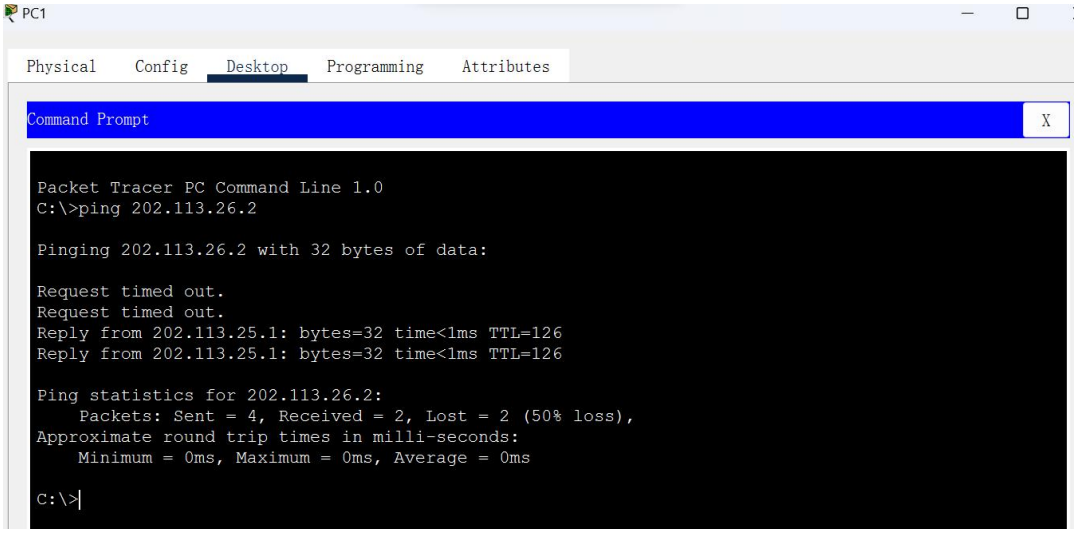
3.将防火墙配置为允许内网用户自由地向外网发起 TCP 连接，同时可以接收外网发回的 TCP 应答数据包。但是，不允许外网的用户主动向内网发起 TCP 连接。在此网络中，规定网络 1 为内网，网络 2，3 为外网。因此仍需要在 router3 中设置 ACL 来过滤数据包。网络拓扑图与之前一致。

首先使用命令 access-list 110 permit tcp any any established 允许所有的 TCP 连接，防止思科路由器的默认丢弃处理。使用 access-list 110 permit tcp 202.113.25.0 0.0.0.255 any 命令创建扩展 ACL，允许网络 1 中的任何数据包通过。然后使用命令 access-list 110 deny tcp any 202.113.25.0 0.0.0.255，拒绝任何外网对网络 1 的 TCP 连接数据包。最后设置服务器的两个端口为进站过滤数据包。此时防火墙配置成功。

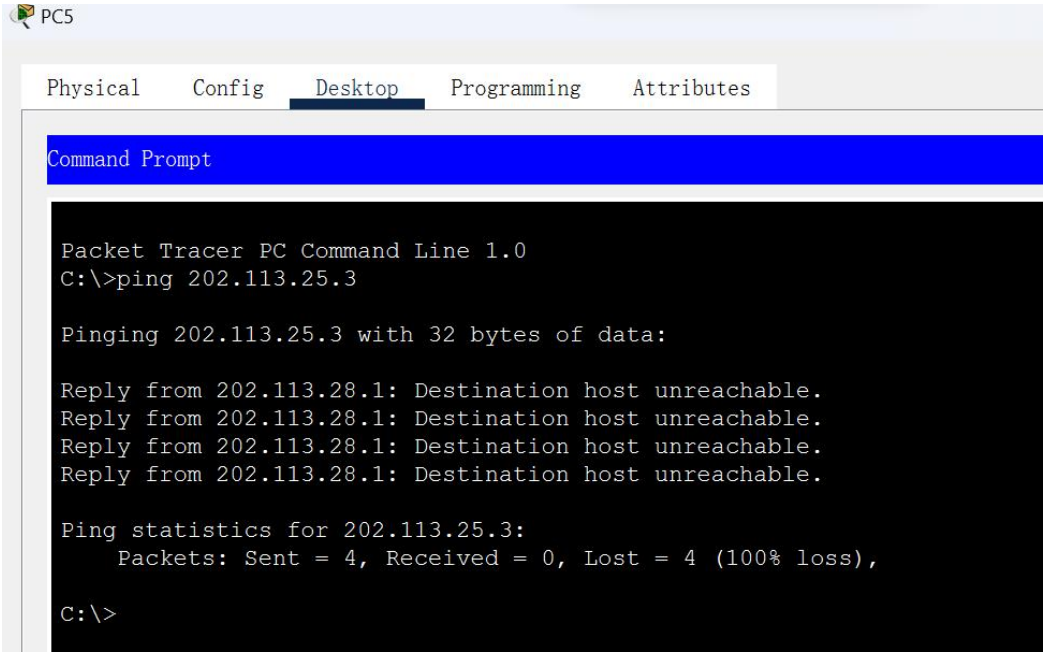
```
Router>
Router>enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 110 permit tcp any any established
Router(config)#access-list 110 permit tcp 202.113.25.0 0.0.0.255 any
Router(config)#access-list 110 deny tcp any 202.113.25.0 0.0.0.255
Router(config)#interface gig0/1
Router(config-if)#ip access-group 110 in
Router(config-if)#exit
Router(config)#interface gig0/0
Router(config-if)#ip access-group 110 in
Router(config-if)#exit
```

三、实验结果分析

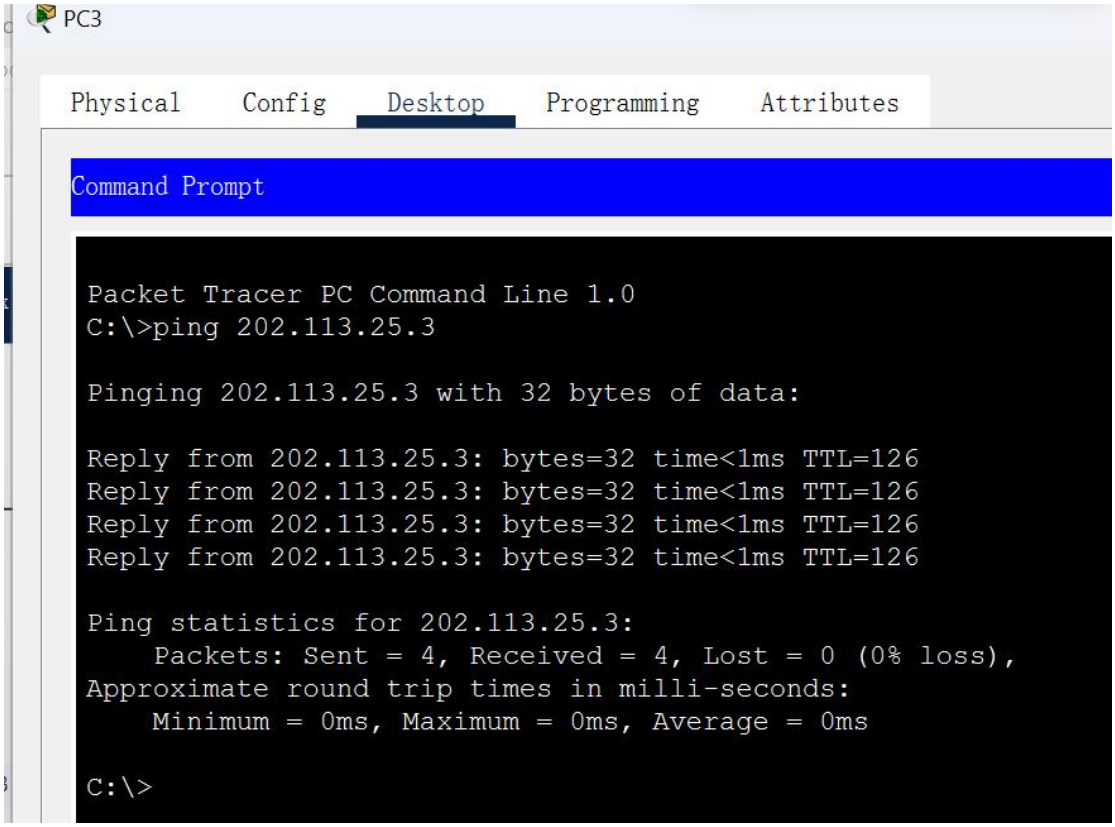
1. 使用 ping 命令检查网络连通性。



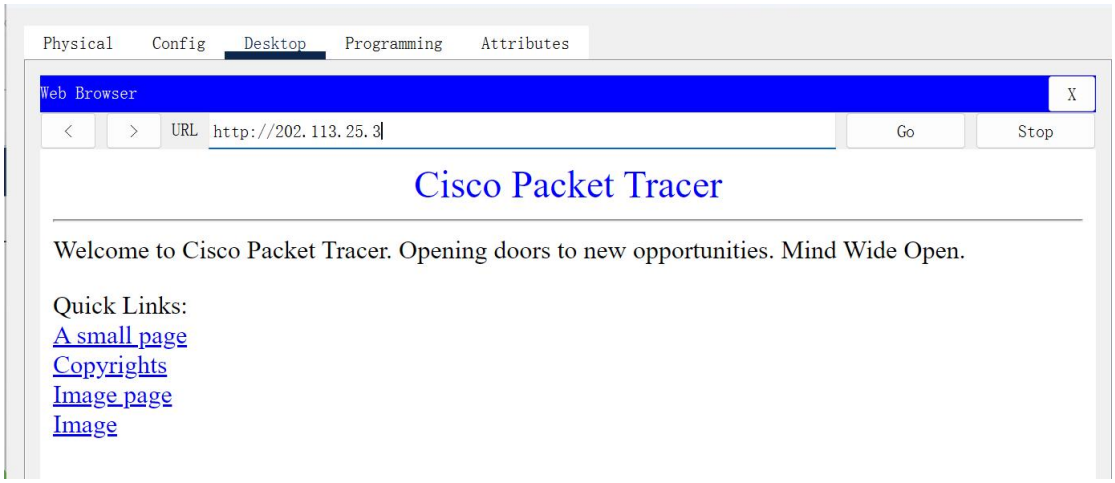
设置防火墙后在 PC5 中使用 ping 命令访问网络 1，可以发现显示了路径不可达。



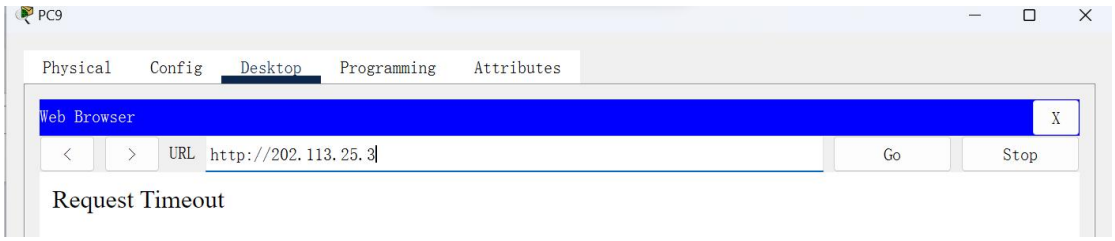
在网络 2 中使用 ping 命令访问网络 1，发现可以访问网络 1，说明包过滤防火墙设置成功。



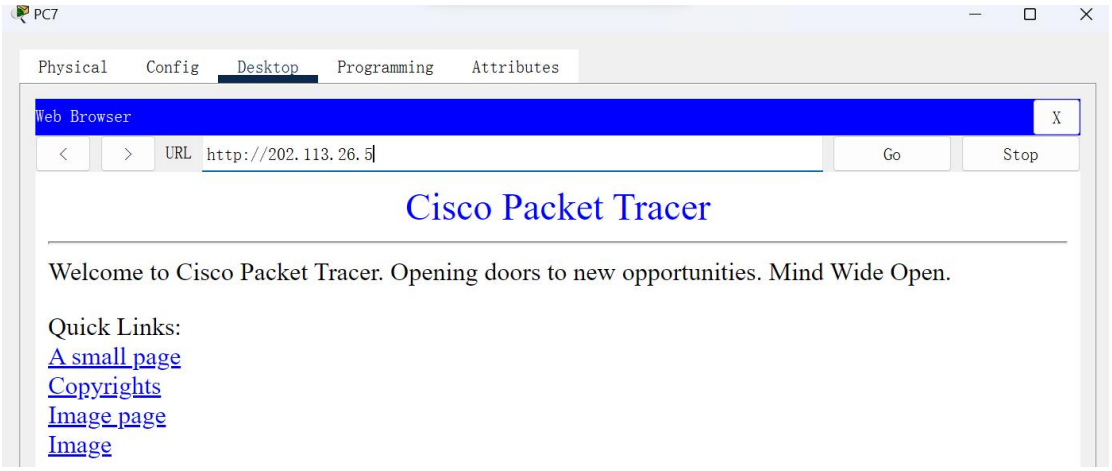
2. 未配置防火墙前，检查网络连通性，在网络 2 的主机中使用浏览器访问服务器网址，发现访问成功。



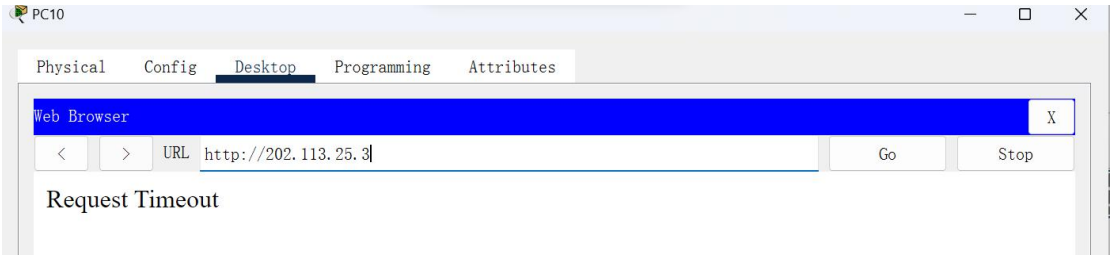
配置好防火墙后，在 PC9 中使用浏览器访问服务器网址，发现访问超时，说明包过滤防火墙设置成功。



3. 为了测试 TCP 连接，在外网中增加了一台服务器 2，其地址为 202.113.26.5 在内网中使用浏览器访问服务器 2 网址。如下图，访问成功。



在外网中使用浏览器访问服务器 1 网址。如下图，访问超时，说明包过滤防火墙设置成功。



四、实验感想与研讨

1. 实验中的问题

对于实验中助教的提问，查阅资料后发现理解有偏差。

access-list ListNum {permit deny} Protocol SrcIPAddr SrcPort DesIPAddr DesPort 这句命令中最后四个字段中的前两个字段应表示的是源 IP 地址和端口号，在检查实验时理解反了。也就是说在设置内网拒绝访问外网时是通过路由器的右端口过滤掉源 IP 地址为内网 IP 地址的数据包。因此这里为源 IP 地址和端口号。

扩展ACL

可按照源IP地址、目的IP地址、源端口、目的端口等条件进行ACL规则定义

access-list ListNum {permit|deny} Protocol SrcIPAddr SrcPort DesIPAddr DesPort

ListNum：列表号，101~199

动作：permit、deny

Protocol：该条规则适用的协议类型，如ip、icmp、tcp、udp等

SrcIPAddr：源IP地址范围

SrcPort：源TCP或UDP端口范围

DesIPAddr：目的IP地址范围

DesPort：目的TCP或UDP端口范围

2. 实验感想

通过实验中的包过滤防火墙设置，我深刻认识到了网络安全中配置防火墙规则的重要性。学会使用 ACL 在 Cisco Packet Tracer 中配置规则，不仅使我能够掌握基本的命令语法，还加深了我对网络策略的理解。实验中，我思考了何时应该允许或拒绝特定流量，这为我制定更严谨的网络安全策略提供了启示。调试和验证已配置规则的过程让我学到了如何确保规则按照预期工作，提高了网络安全的可靠性。通过这次实验提升了对 ACL 的熟练度，也加深了对网络安全的认识，为网络安全的学习打下了坚实基础。