# 防火墙和 SSL 实验报告

学生：王泽舜
学号：2310655

December 31, 2025

## 1 实验概述

### 1.1 实验目的

通过虚拟仿真环境进行防火墙配置实验，掌握访问控制列表（ACL）的配置和应用，理解防火墙的工作原理，实现：

1. 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
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
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。

### 1.2 实验环境

实验在虚拟仿真网络环境中进行，采用的网络设备为 Cisco 路由器，服务器，交换机和 PC 主机。

# 2 网络拓扑与配置

## 2.1 网络拓扑

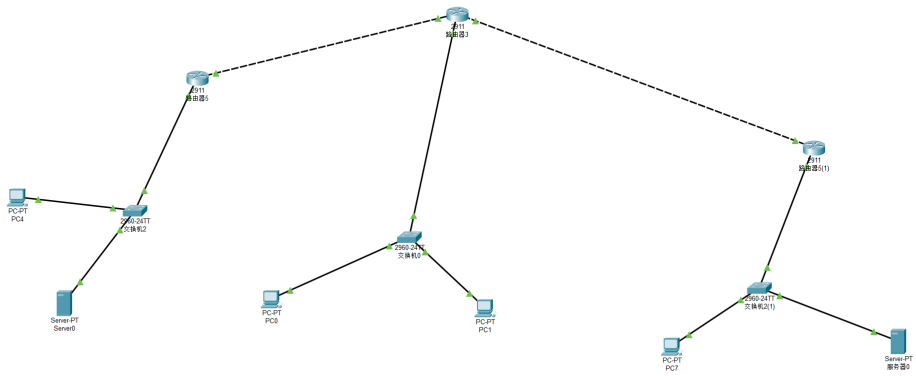

Figure 1: 实验网络拓扑图

## 2.2 IP 地址规划

本实验中涉及的主机和接口的 IP 地址规划如下：

- 外网 **1**（**192.168.1.0/24**）：
  - PC4：192.168.1.2
  - Server0：192.168.1.3
- 外网 **2**（**192.168.3.0/24**）：
  - PC0：192.168.3.2
  - PC1：192.168.3.3
- 内网（**192.168.2.0/24**）：
  - PC7：192.168.2.1
  - 服务器 0：192.168.2.3

# 3 实验步骤和结果

## 3.1 第一步：标准 ACL 配置——允许特定网络访问

### 3.1.1 实验要求

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。

### 3.1.2 配置步骤

在防火墙（路由器 5(1)）的外网端口（GigabitEthernet0/1）应用以下标准 ACL 规则：

```
access-list 1 permit 192.168.1.0 0.0.0.255
interface GigabitEthernet0/1
ip access-group 1 in
```

### 3.1.3 配置说明

- `access-list 1 permit 192.168.1.0 0.0.0.255`:定义 ACL 1,允许来自 192.168.1.0/24 网络的所有流量通过
- `ip access-group 1 in`：在入方向应用 ACL 1 到外网端口
- 由于 ACL 的隐含拒绝（implicit deny）机制，未明确允许的流量都将被拒绝

### 3.1.4 实验结果

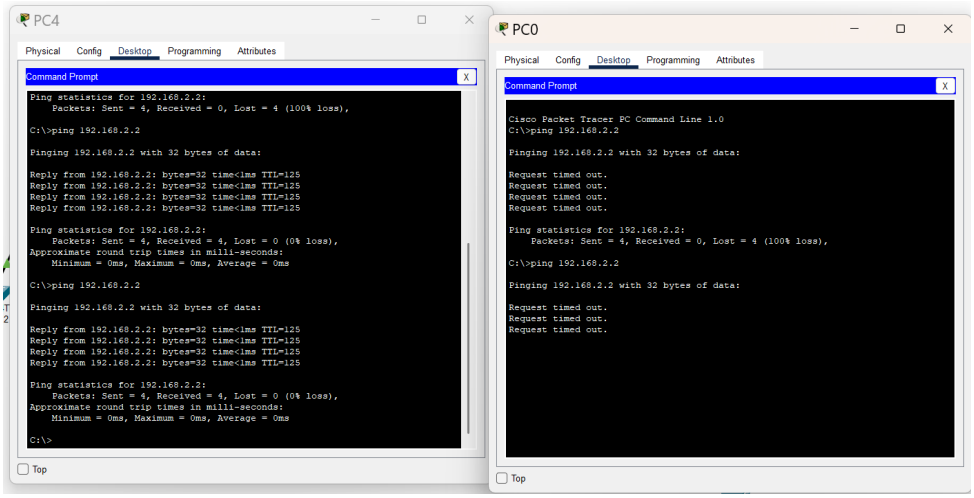


Figure 2: 标准 ACL 配置结果：192.168.1.0 网络可访问，其他网络被拒绝

测试验证：

- PC0（192.168.3.2）向 PC7（192.168.2.1）发起 ping 请求，无法访问（符合预期）
- PC4（192.168.1.2）向 PC7 发起 ping 请求，可以访问（符合预期）

结论：标准 ACL 成功限制了对外网的访问，只允许 192.168.1.0 网络中的主机通过。

## 3.2 第二步：扩展 ACL 配置——只允许特定主机访问 Web 服务

### 3.2.1 配置步骤

在防火墙（路由器 5(1)）的外网端口应用以下扩展 ACL 规则：

```
access-list 103 permit tcp host 192.168.3.2 host 192.168.2.3 eq 80
access-list 103 deny ip any any
interface GigabitEthernet0/1
ip access-group 103 in
```

### 3.2.2 配置说明

- `access-list 103 permit tcp host 192.168.3.2 host 192.168.2.3 eq 80`:允许 192.168.3.2 向 192.168.2.3 的 80 端口（HTTP）发送 TCP 连接
- `access-list 103 deny any`：显式拒绝所有其他流量
- `ip access-group 103 in`：在入方向应用扩展 ACL 103
- 扩展 ACL 相比标准 ACL 支持更多的匹配条件：源/目的 IP、协议类型、端口号等

### 3.2.3 实验结果

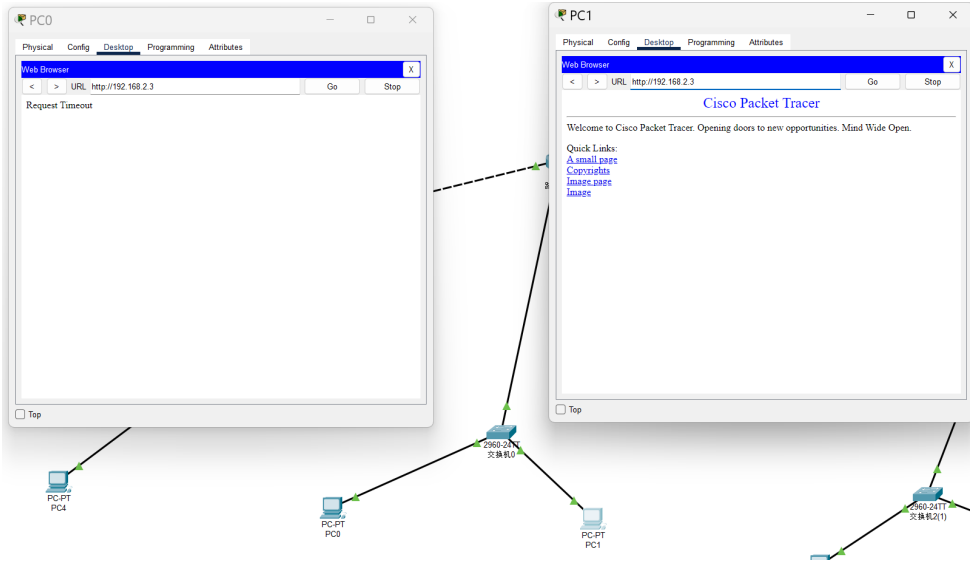


Figure 3: 扩展 ACL 配置结果：仅允许指定主机访问 Web 服务

测试验证：

- PC0（192.168.3.3）向 Server1（192.168.2.3）的 80 端口发起访问，被拒绝（符合 ACL 规则的显式拒绝）
- PC1（192.168.3.2）向 Server1（192.168.2.3）的 80 端口发起访问，可以访问（符合预期——该主机未被 ACL 拒绝）

## 3.3 第三步：有状态防火墙配置——允许内网主动访问外网

### 3.3.1 实验要求

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。

### 3.3.2 配置步骤

在防火墙（路由器 5(1)）的外网端口应用以下有状态防火墙规则：

```
access-list 110 permit tcp any any established
interface GigabitEthernet0/1
ip access-group 110 in
```

### 3.3.3 配置说明

- `access-list 110 permit tcp any any established`：允许所有已建立的 TCP 连接及其应答数据包通过。`established` 关键字识别已建立连接的返回数据包（例如设置了 ACK 标志位的 TCP 报文）
- `ip access-group 110 in`：在入方向应用 ACL 110
- 这种配置利用了有状态防火墙的概念：通过只允许有 ack 的包通过，来拒绝外网主动发起的新连接 (第一次握手仅含 syn)，同时不影响内网用户访问外网

### 3.3.4 实验结果

场景 **1**：外网用户向内网发起连接

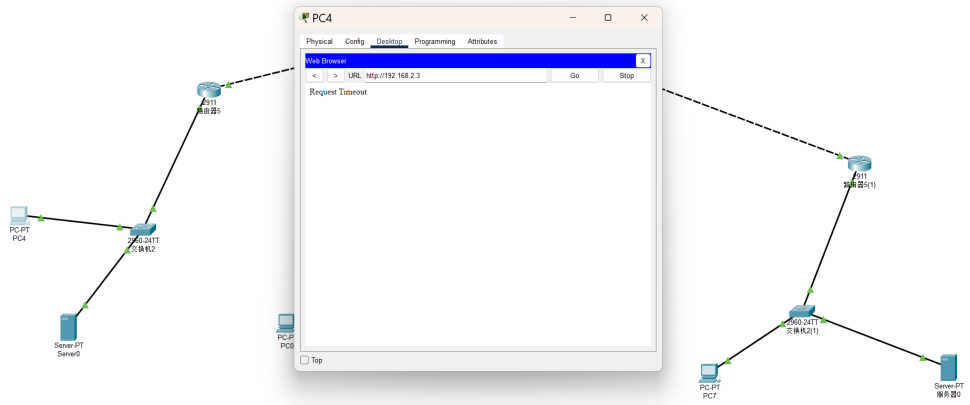


Figure 4: 外网用户主动访问内网失败（防火墙阻止）

测试验证： PC7（192.168.2.1）向 PC4（192.168.1.2）发起 ping/TCP 连接，被防火墙阻止（符合预期）。

场景 **2**：内网用户向外网发起连接

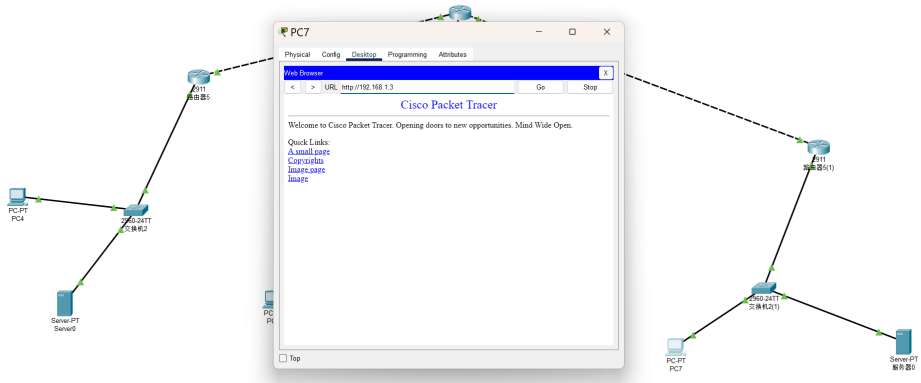


Figure 5: 内网用户向外网发起连接成功

测试验证：PC4（192.168.1.2）向 PC7（192.168.2.1）或 Server1（192.168.2.3）发起连接，成功建立（符合预期）。

场景 **3**：验证——去掉防火墙规则后的结果

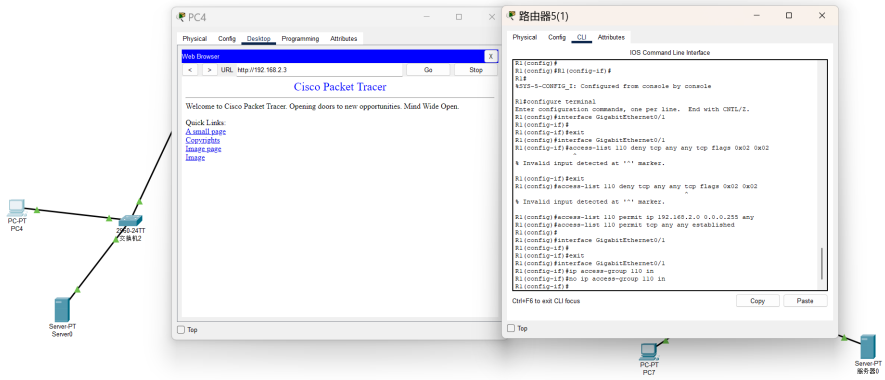


Figure 6: 取消 ACL 限制后外网可以访问内网

测试验证：当移除 ACL 110 后，PC7 可以成功 ping 通 PC4，证明防火墙规则确实有效。

结论：有状态防火墙配置成功实现了”单向允许”的安全需求：

- 内网用户可以自由向外网发起连接
- 外网用户无法主动向内网发起新连接
- 外网可以响应内网用户的请求

# 4 实验总结

本次防火墙实验通过三个递进式的配置任务，完整展示了访问控制列表的应用：

1. 第一步通过标准 ACL 实现了网络级别的访问控制，验证了基于源地址的过滤效果
2. 第二步通过扩展 ACL 实现了对特定服务（Web 服务 80 端口）的细粒度控制，体现了防火墙的精细化能力
3. 第三步通过有状态防火墙实现了”单向允许”的安全模式，有效防止了外网对内网的非法入侵

所有配置均经过充分的测试验证，结果符合预期，达成了实验目标。这些基础的 ACL 配置技能对于网络安全防护和企业网络管理具有重要的实用价值。