南開大學
Nankai University

南　　开　　大　　学

网 络 空 间 安 全 学 院

网络技术与应用

实验 7：防火墙和 SSL 实验

姓名：郑盛东

学号：2010917

年级：2020 级

专业：信息安全、法学双学位班

指导教师：张建忠、徐敬东

2023 年 12 月 17 日

目录

一、 实验内容说明

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。

二、 实验准备

(一) 标准 ACL

网络连接如图1。

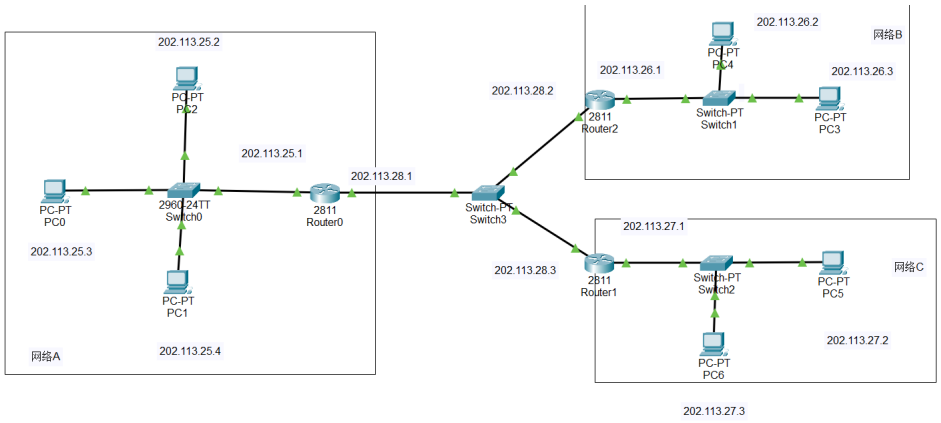

图 1: 标准 ACL 网络连接图

对路由器 0 进行标准 ACL 配置, 对进入 FaO/1 接口的数据报进行检查和过滤。首先, 在路由器的全局配置模式下建立一个标号为 6 的标准 ACL O 该列表包含两条规则,access-list 6 permit 202. 113. 26. 0 0. 0. 0. 255 允许网络 B 中的主机发送的数据报通过, 其后输入 access-list 6 deny any 拒绝所有其他网络的数据报送来的数据报。由于 Cisco 的 ACL 默认情况下拒绝所有的数据包, 因此, access-list 6 deny any 这条规则也可以省略。接下来, 进入 FaO/1 接口配置模式, 利用 ip access-group 6 in 将 6 号 ACL 绑定在 FaO/1 的入站上。

```
Router(config)#access-list 6 permit 202.113.26.0 0.0.0.255
Router(config)#
Router(config)#access-list 6 deny any
Router(config)#
Router(config)#interface fa0/1
Router(config-if)#ip access-group 6 in
Router(config-if)#
```

图 2: 路由器 1 的配置

(二) 扩展 ACL

网络连接如图5。

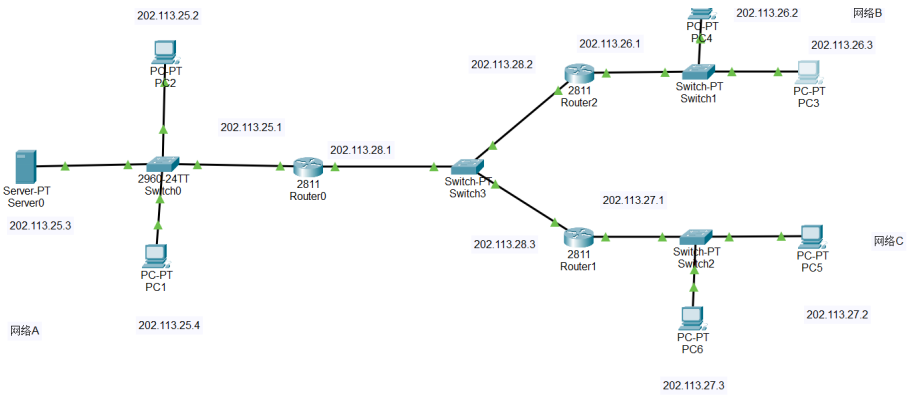

图 3: 扩展 ACL 网络连接

在路由器 0 的 FaO/1 接口上绑定一个扩展 ACL, 对进入 FaO/1 接口的数据报进行检查和过滤。与配置标准 ACL 类似，给出的配置命令也由两部分组成：第一部分，在路由器的全局配置模式下建立一个标号为 106 的扩展 ACL 。该列表包含两条规则, access-list 106 deny tcp host 202. 113. 26. 2 host 202. 113. 25. 3 eq www 的含义为抛弃源 IP 地址为 202. 113. 26. 2 、目的地址为 202. 113. 25. 3 、目的端口号为 80 的 TCP 数据报。其后的 access-list 106 permit ip any any 允许所有的其他数据报通过。注意，由于 Cisco 的 ACL 默认情况下拒绝所有数据包，因此,access-list 106 permit ip any any 这条规则不可省略。第二部分，进入 FaO/1 接口配置模式，利用 ip access-group 106 in 将 106 号 ACL 绑定在 FaO/1 的入站上。

```
Router>
Router>enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
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 fa0/1
Router(config-if)#ip access-group 106 in
Router(config-if)#
```

图 4: 扩展 ACL 配置

三、 实验过程

(一) 标准 ACL

在配置完成标准 ACL 后，先使用网络 B 的主机去 ping 网络 A 中的 PC0，发现可以 ping 通。

```
C:\>ping 202.113.25.3

Pinging 202.113.25.3 with 32 bytes of data:

Reply from 202.113.25.3: bytes=32 time<1ms TTL=126
Reply from 202.113.25.3: bytes=32 time=1ms TTL=126
Reply from 202.113.25.3: bytes=32 time<1ms TTL=126
Reply from 202.113.25.3: bytes=32 time<1ms TTL=126

Ping statistics for 202.113.25.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

图 5: 网络 B 主机仍能 ping 通

再使用网络 C 的主机去 ping 网络 A 中的 PC0，发现无法 ping 通。因此满足实验要求，只允许某个网络中的主机访问另一个网络。

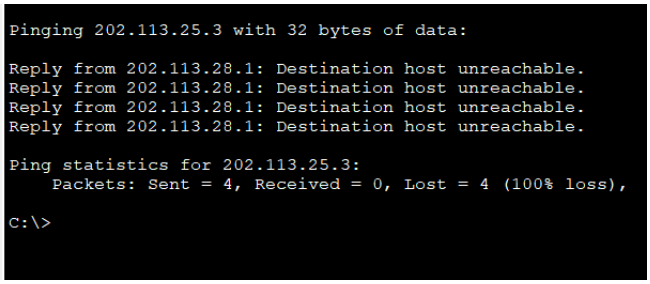

图 6: 网络 C 无法 ping 通

(二) 扩展 ACL

使用 PC4 去访问 server 的 web 服务。发现 web 访问失败，证明防火墙的设置有效。

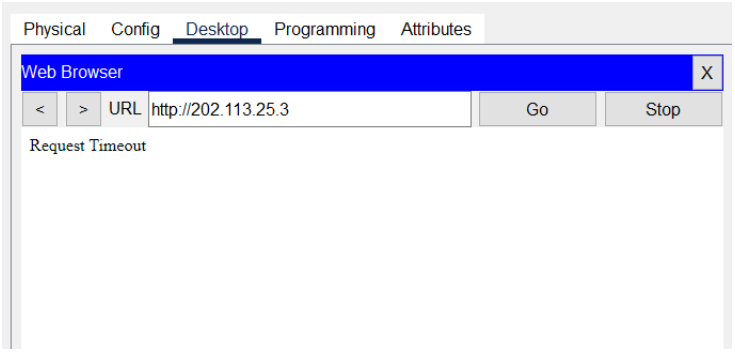

图 7: PC4web 访问失败

使用其他主机，如 PC3 区访问 web 服务，发现访问成功。证明我们的实验已经满足要求：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。

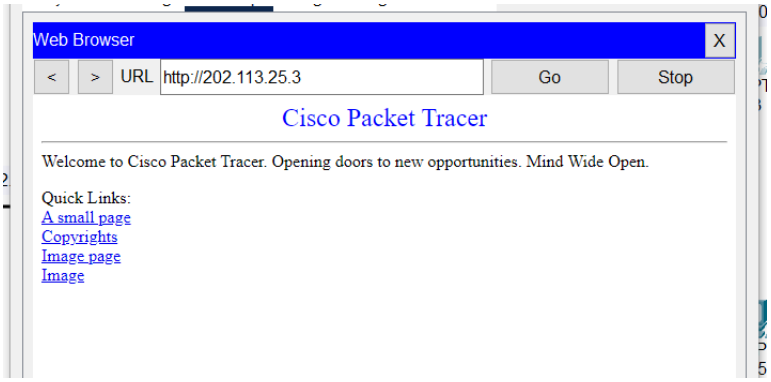

图 8: 其他主机可以访问成功

参考文献

[1] 张建忠、徐敬东. 计算机网络技术与应用. 北京清华大学学研大厦 A 座: 清华大学出版社, 2019.