

南開大學

网络技术与应用课程实验报告

实验七：防火墙



专 业____信息安全____

学 号____2113662____

姓 名____张丛____

班 级____信息安全一班____

一、 实验目的

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、实验原理

ACL (AccessControlList, 访问控制列表) 是用来实现数据包识别功能的, ACL 用于控制网络设备（如路由器、交换机、防火墙）上的数据流动, 以决定哪些数据包被允许通过或被阻止。

其中 ACL 的包过滤技术具体可分为一下过程：

- 对进出的数据包逐个过滤，丢弃或允许通过；
- ACL 应用于接口上，每个接口的出入双向分别过滤；
- 仅当数据包经过一个接口时，才能被此接口的此方向的 ACL 过滤；

Cisco 设备支持两种类型的 ACL：标准 ACL（Standard ACL）和扩展 ACL（Extended ACL）。

标准ACL示例



命令	含义
<code>access-list 16 permit 192.168.1.0 0.0.0.255</code>	在标号为16的ACL中添加一条规则，该条规则允许源IP地址为192.168.1.XX的数据报通过
<code>access-list 16 deny host 192.168.2.5</code>	在标号为16的ACL中添加一条规则，该条规则丢弃源IP地址为192.168.2.5的数据报
<code>access-list 16 permit any</code>	在标号为16的ACL中添加一条规则，该条规则允许任意的IP数据报通过

扩展ACL示例



命令	含义
access-list 106 deny udp 192.168.1.0 0.0.0.255 host 192.168.2.5 gt 1023	在标号为106的ACL列表中添加一条规则，该条规则丢弃所有源IP地址为192.168.1.XX，目的IP地址为192.168.2.5，UDP端口号大于1023的数据包。
access-list 106 permit tcp any 192.168.1.0 0.0.0.255 any eq www	在标号为106的ACL列表中添加一条规则，该条规则允许目的IP地址为192.168.1.XX，TCP端口号为80的数据包通过。常用的著名端口号可以使用规定的字符串代替，例如www代表Web服务的80端口，smtp代表邮件服务的25端口等。
access-list 106 deny tcp any any eq 23	在标号为106的ACL列表中添加一条规则，该条规则丢弃所有目的TCP端口号为23的数据包。

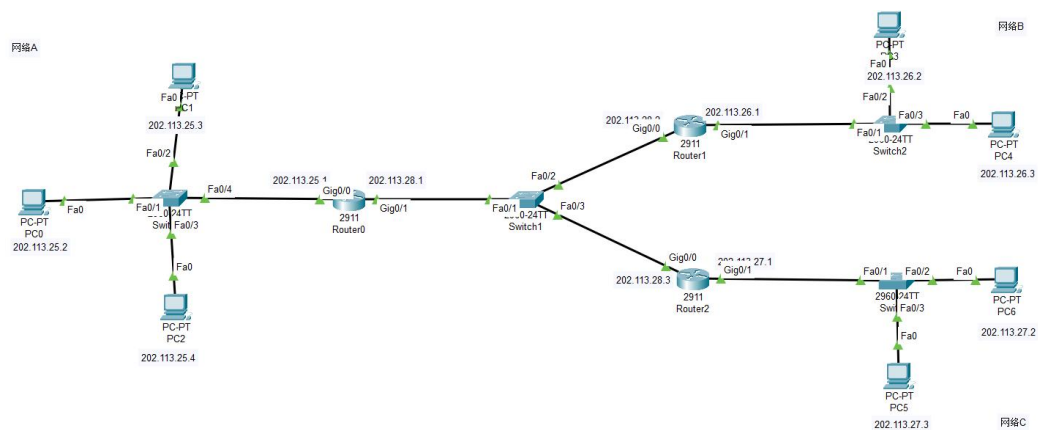
三、实验过程

标准 ACL:

目的：允许网络 B 访问网络 A，而不允许其他网络访问网络 A 中的主机。

操作：在路由器 R0 上定义标准 ACL，并把 ACL 绑定到接口的入站上，使得路由器对接口的入站数据包进行检查。

网络拓扑如下：



首先对各主机和路由器进行 ip 配置，已经配置过很多次了，不赘述：

```
Router>enable
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface gig0/0
Router(config-if)#ip address 202.113.28.2 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed
state to up

Router(config-if)#exit
Router(config)#interface gig0/1
Router(config-if)#ip address 202.113.26.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
```

给路由器配置 rip 动态路由，在之前的实验也做过，如下：

```
Enter configuration commands, one per line.
Router(config)#
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 202.113.25.0
Router(config-router)#network 202.113.28.0
Router(config-router)#
```

对所有路由器配置完动态路由后，此时各个网络就已经连通了，

需要对路由 R1 配置标准访问控制列表，以达到实验目的。

如下：

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

对上面的命令进行解释：

access-list 6 permit 202.113.26.0 0.0.0.255

1. 创建一个名为 6 的 ACL，并允许来自 202.113.26.0/24 网段的数据包通过。这里的“0.0.0.255”表示子网掩码为 255.255.255.0，即 202.113.26.0/24 网段。

access-list 6 deny any

2. 在 ACL 中添加一个拒绝任何来源 IP 地址的规则。这个规则将拒绝所有未被允许的数据包。

Router(config)#interface gig0/1

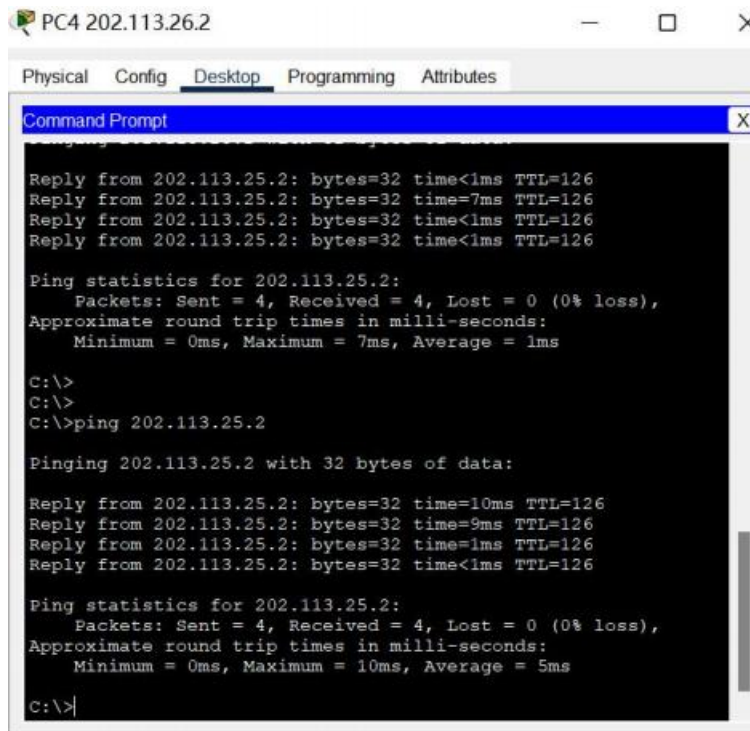
Router(config-if)#ip access-group 6 in

3. 将 ACL 6 应用到接口 gig0/1 的入方向，即所有进入该接口的数据包都会被 ACL 过滤。

配置完成后，就实现了仅网络 B 的主机可以访问网络 A 的主机。

如网络 B 的主机 4（202.113.26.2）访问网络 A 的主机 0

(202.113.25.2) :



```
PC4 202.113.26.2
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 202.113.25.2: bytes=32 time<1ms TTL=126
Reply from 202.113.25.2: bytes=32 time=7ms TTL=126
Reply from 202.113.25.2: bytes=32 time<1ms TTL=126
Reply from 202.113.25.2: bytes=32 time<1ms TTL=126

Ping statistics for 202.113.25.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 1ms

C:\>
C:\>
C:\>ping 202.113.25.2

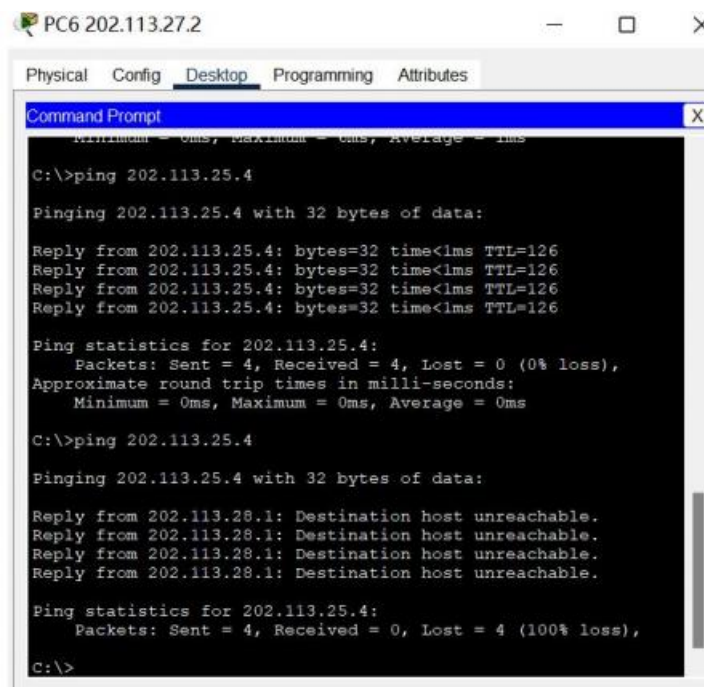
Pinging 202.113.25.2 with 32 bytes of data:

Reply from 202.113.25.2: bytes=32 time=10ms TTL=126
Reply from 202.113.25.2: bytes=32 time=9ms TTL=126
Reply from 202.113.25.2: bytes=32 time=1ms TTL=126
Reply from 202.113.25.2: bytes=32 time<1ms TTL=126

Ping statistics for 202.113.25.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 5ms

C:\>
```

网络 C 的主机访问网络 A 的则不行:



```
PC6 202.113.27.2
Physical Config Desktop Programming Attributes
Command Prompt
Minimum = 0ms, Maximum = 0ms, Average = 1ms

C:\>ping 202.113.25.4

Pinging 202.113.25.4 with 32 bytes of data:

Reply from 202.113.25.4: bytes=32 time<1ms TTL=126
Reply from 202.113.25.4: bytes=32 time<1ms TTL=126
Reply from 202.113.25.4: bytes=32 time<1ms TTL=126
Reply from 202.113.25.4: bytes=32 time<1ms TTL=126

Ping statistics for 202.113.25.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 202.113.25.4

Pinging 202.113.25.4 with 32 bytes of data:

Reply from 202.113.28.1: Destination host unreachable.
Reply from 202.113.28.1: Destination host unreachable.
Reply from 202.113.28.1: Destination host unreachable.
Reply from 202.113.28.1: Destination host unreachable.

Ping statistics for 202.113.25.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

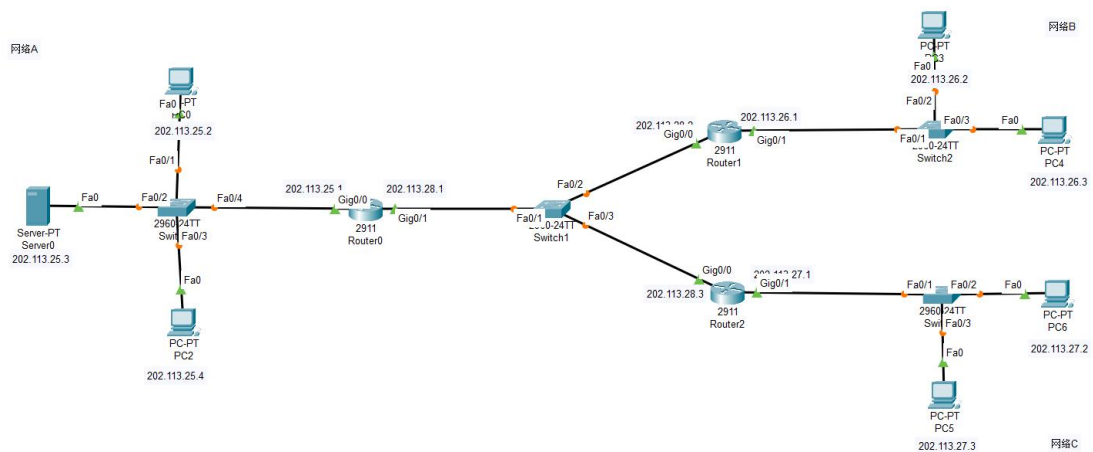
并且，与一般的 ping 不通于是显示 timeout 不同，这里是直接告诉我们不可访问。

扩展 ACL:

目的：不允许网络 B 中的某个主机访问网络 A 中的 Web 服务。

操作同样是在路由器 R0 上定义标准 ACL，并把 ACL 绑定到接口的入站上，使得路由器对接口的入站数据包进行检查。

网络拓扑有所改变：



主要区别是网络 A 存在一个 Web 服务器。

首先还是配置 ip，配置动态路由，不再赘述。

然后配置 ACL：

```
Router(config)#
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)#
Router(config)#interface gig0/1
Router(config-if)#ip access-group 106 in
Router(config-if)#
```

解释：

access-list 106 deny tcp host 202.113.26.2
host 202.113.25.3 eq 80

1. 创建一个名为 106 的 ACL, 并添加一个拒绝 TCP 数据包的规则, 这个规则将拒绝源 IP 地址为 202.113.26.2, 目标 IP 地址为 202.113.25.3, 目标端口为 80 的 TCP 数据包。

access-list 106 permit ip any any

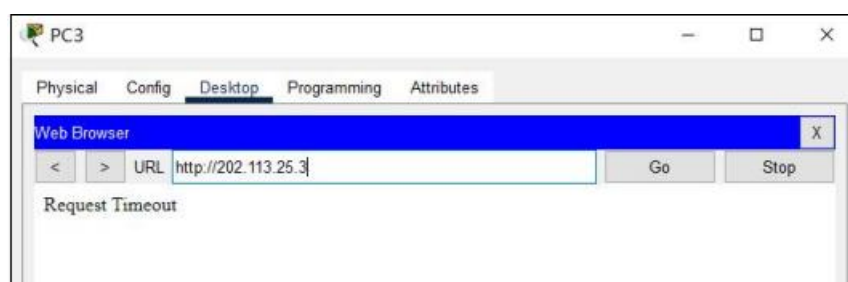
2. 在 ACL 中添加一个允许所有 IP 数据包的规则, 这个规则将允许所有其他的 IP 数据包通过。

Router(config)#interface gig0/1

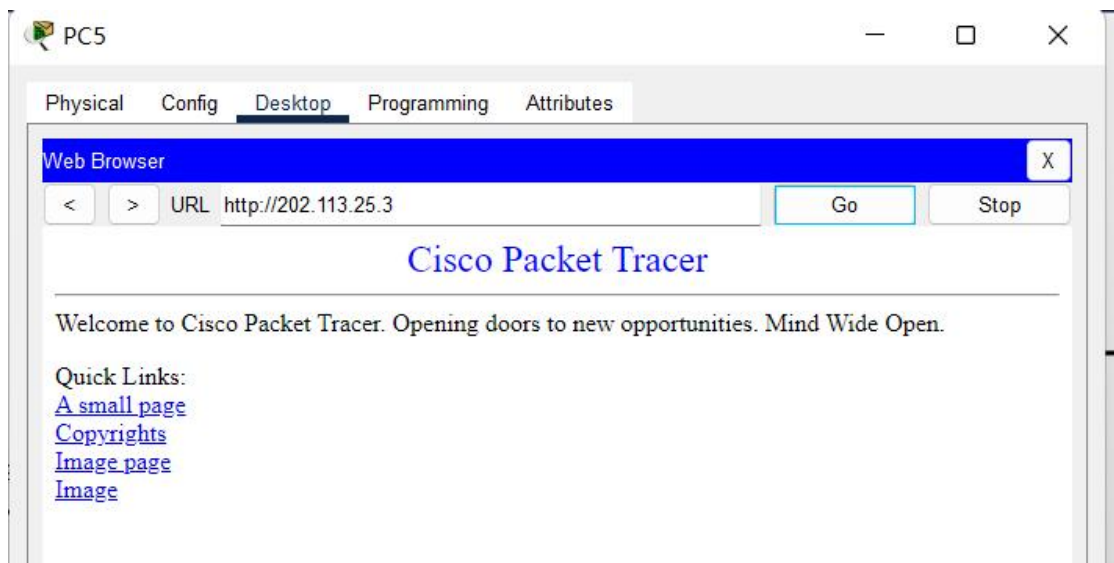
Router(config-if)#ip access-group 106 in

3. 将 ACL 106 应用到接口 gig0/1 的入方向, 即所有进入该接口的数据包都会被 ACL 过滤。

对于网络 B 的主机 3 访问网络 A 的 Web 服务器:



对于网络 C 的主机访问:



于是达到了我们的实验目的。

四、总结与思考

课上的理论学习了数据加密、数字签名和防火墙，让我知道了防火墙主要应用了两种技术：包过滤和应用网关。

实验则配置了相对来说简单的包过滤，学习了 ACL，和一些配置命令。

受益匪浅。