南开大学
Nankai University

南　　开　　大　　学

网 络 空 间 安 全 学 院

网络技术与应用课程报告

防火墙配置实验

学号：2013018

姓名：许健

年级：2020 级

专业：信息安全

2022 年 11 月 29 日

目录

一、 实验内容说明

(一) 防火墙配置

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，同时可以接受外网发回的 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、 标准 ACL

(一) 网络拓扑图

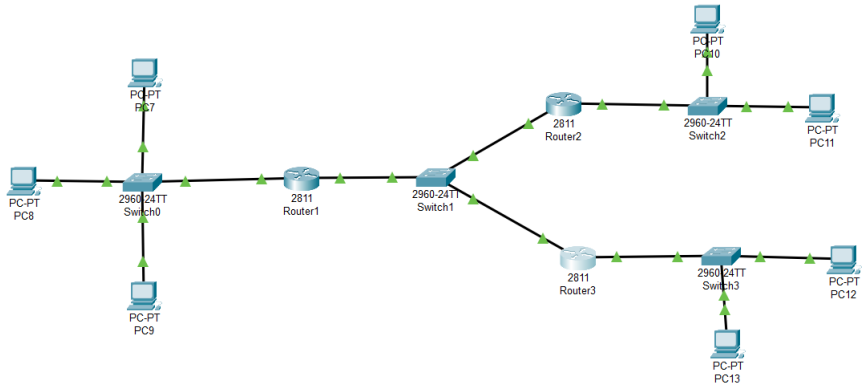


图 1: 网络拓扑图

(二) 网络配置

1. 配置路由器

配置路由器的 IP 和静态路由表项

```
Router>enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fa0/0
Router(config-if)#ip address 202.113.25.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up

Router(config-if)#exit
Router(config)#interface fa0/1
Router(config-if)#ip address 202.113.28.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up

Router(config-if)#exit
Router(config)#
```

图 2: 配置路由器的 IP

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    202.113.25.0/24 is directly connected, FastEthernet0/0
S    202.113.26.0/24 [1/0] via 202.113.28.2
S    202.113.27.0/24 [1/0] via 202.113.28.3
C    202.113.28.0/24 is directly connected, FastEthernet0/1

Router#
```

图 3: 配置路由表项

2. 配置标准 ACL

在路由器的全局配置模式下建立一个标号为 6 的标准 ACL。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包通过，其后的 access-list 6 deny any 拒绝所有其他网络的数据包发送来的数据报。

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

图 4: 配置标准 ACL

(三) 网络连通性测试

网络 B 中的主机发送的数据包通过，网络 C 中的主机发送的数据包不通过

```
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=1ms TTL=126
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

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 = 2ms
```

图 5: B 网络 pingt 通

```
C:\>ping 202.113.25.2

Pinging 202.113.25.2 with 32 bytes of data:

Request timed out.
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 202.113.25.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

图 6: C 网络 ping 不通

（四） 模拟发包

模拟发包查看 C 网络主机发送数据包经过防火墙情况，可以看到包经过路由器时被丢弃，并返回 ICMP 差错报文，显示路径 unreachable。

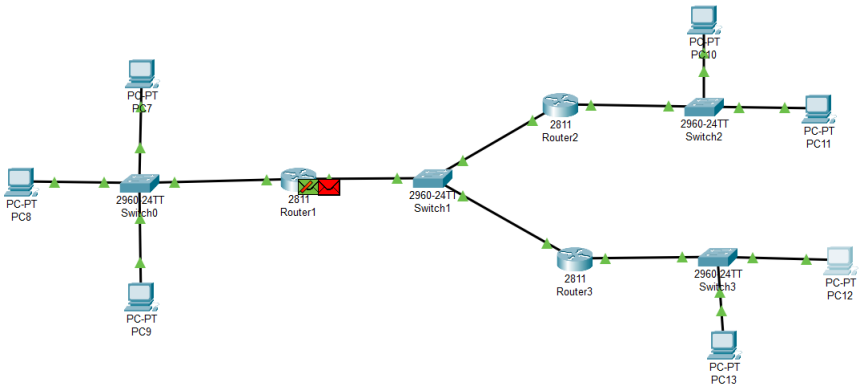
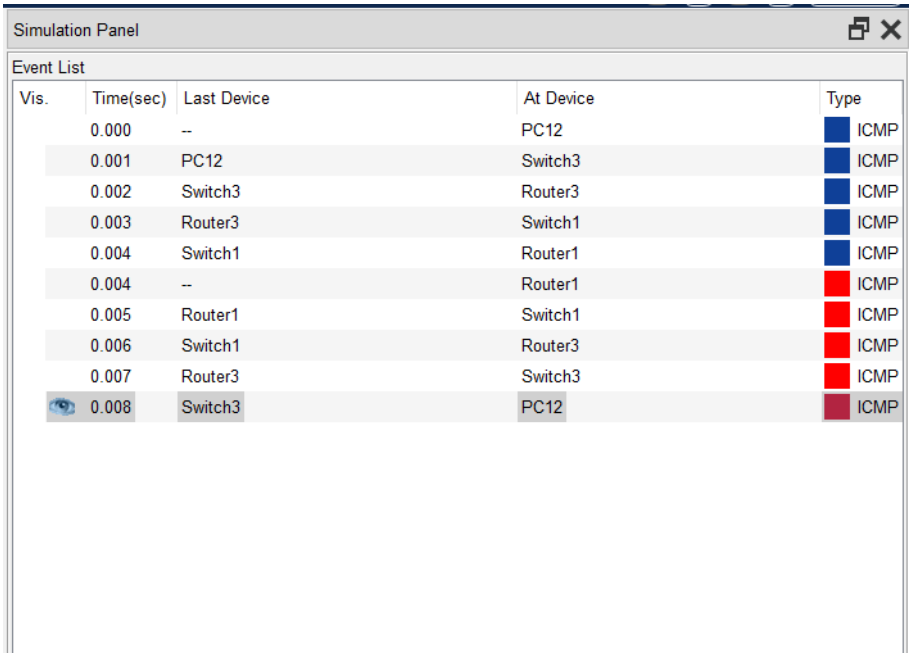


图 7: 路由器拒绝 C 网络数据包



Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC12	ICMP
	0.001	PC12	Switch3	ICMP
	0.002	Switch3	Router3	ICMP
	0.003	Router3	Switch1	ICMP
	0.004	Switch1	Router1	ICMP
	0.004	--	Router1	ICMP
	0.005	Router1	Switch1	ICMP
	0.006	Switch1	Router3	ICMP
	0.007	Router3	Switch3	ICMP
	0.008	Switch3	PC12	ICMP

图 8: 模拟发包 ping 不通

三、 扩展 ACL

(一) 网络拓扑图

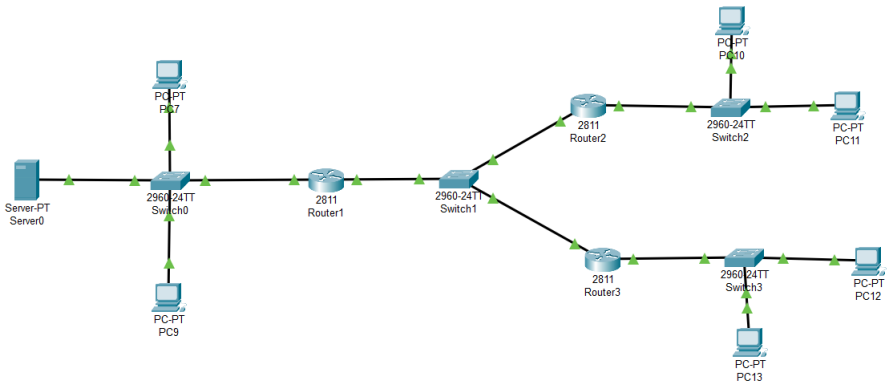


图 9: 网络拓扑图

(二) 配置扩展 ACL

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。

```
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 www
Router(config)#access-list 106 permit ip any
% Incomplete command.
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)#exit
```

图 10: 配置扩展 ACL

```
Router>enable
Router#show access-list
Standard IP access list 6
    10 permit 202.113.26.0 0.0.0.255
    20 deny any
Extended IP access list 106
    10 deny tcp host 202.113.26.2 host 202.113.25.3 eq www
    20 permit ip any any
```

图 11: 查看访问控制列表

(三) 访问 web 服务

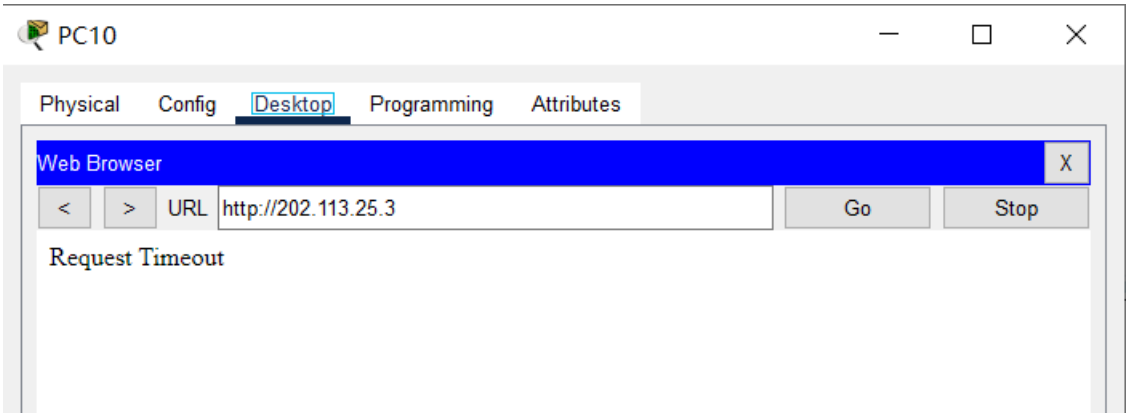


图 12: 目标主机无法访问 web 服务器

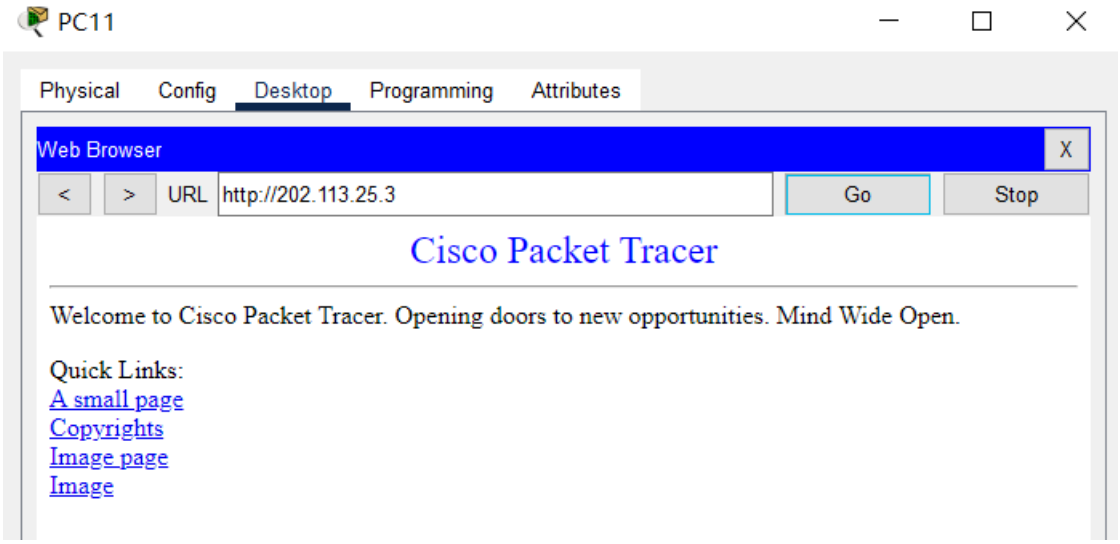


图 13: 其他主机可以正常访问 web 服务器

四、 扩展练习

将防火墙配置为允许内网用户自由地向外网发起 TCP 连接, 同时可以接受外网发回的 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。虽然本部分不再要求，但还是给出一种可行的办法。

过滤可以根据 TCP ACK 比特是否设置来进行。在每个 TCP 连接中第一个报文段的 ACK 比特都设为 0，而连接中的所有其他报文段的 ACK 比特都设为 1。因此，只需直接过滤进入的所有 ACK 比特设为 0 的报文段。这个策略去除了所有从外部发起的所有 TCP 连接，但是允许内部发起 TCP 连接。