网络技术与应用第七次实验

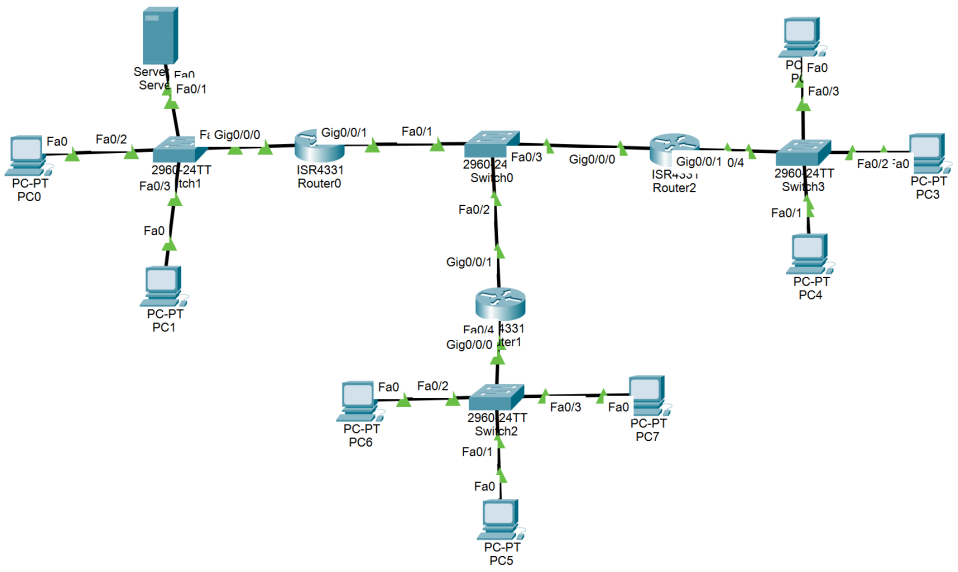
- 实验名称：防火墙实验
- 专业：物联网工程
- 姓名：秦泽斌
- 学号：2212005

一、实验要求

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、实验内容

1. 建立网络拓扑



本网络一共由16个设备组成，分成**A、B、C三个网络**，中央交换机左侧为**网络A**，右侧为**网络B**，下侧为**网络C**，其中网络A包含一个服务器，以下是各设备IP地址分配：（主机的默认网关皆为对应路由器接口）

- **网络A**：
  - server0：192.168.1.1
  - PC0：192.168.1.2
  - PC1：192.168.1.3
  - Router0：
    - Gig0/0：192.168.1.4
    - Gig0/1：206.1.1.1

- **网络B**：
  - PC2：192.168.2.1
  - PC3：192.168.2.2
  - PC4：192.168.3.3
  - Router0：
    - Gig0/1：192.168.2.4
    - Gig0/0：206.1.1.2
- **网络C**：
  - PC6：192.168.3.1
  - PC5：192.168.3.2
  - PC7：192.168.3.3
  - Router0：
    - Gig0/0：192.168.3.4
    - Gig0/1：206.1.1.3

2. 标准ACL配置

利用IP数据报中的源IP地址对过往数据包进行控制，列表号范围：1~99，**使网络B中的主机可以自由访问网络A，而其他网络不可访问网络A**

对路由器`R0`配置步骤如下

- 建立标准控制列表指定能够通过的`IP`地址，在全局配置模式下进行：

  ```
  access-list 6 permit 192.168.2.0 0.0.0.255
  ```

  创建了序号为`6`的访问控制列表，允许`192.168.2.0`开始的地址通过，注意此处的通配符与掩码相反，能够改变的位为1，不能改变的位为0。
- 再在该ACL中增加一条规则，拒绝其他所有IP地址通过，达到了仅允许`202.113.26.0`开始的地址通过的目的：

  ```
  access-list 6 deny any
  ```

- 进入接口配置模式，将ACL绑定到路由器进入`192.168.2.0`的方向：

  ```
  interface gig0/1
  ip access-group 6 in
  exit
  ```

  将序号为`6`的访问控制列表绑定到路由器`gig0/1`端口进入方向。

3. 扩展ACL配置

按照协议类型、源IP地址、目的IP地址、源端口号、目的端口号对过往数据包进行控制，列表号范围：101~199

不允许IP地址为`192.168.2.1`的主机（PC2）访问地址为`192.168.1.1`的服务器的Web服务，允许其他任何主机访问

对路由器`R0`配置步骤如下：

- 建立标准控制列表指定不能够通过的`IP`地址，在全局配置模式下进行：

```
access-list 106 deny tcp host 192.168.2.1 host 192.168.1.1 eq 80
```

创建了序号为`106`的访问控制列表，不允许`192.168.2.1`的地址通过`TCP`协议中`80`端口进行访问，`host`为单个主机关键字，`eq`表示等于，注意此处要写明源主机和目的主机。

- 再在该ACL中增加一条规则：

```
access-list 106 permit ip any any
```

允许其他所有IP数据报通过，达到了仅不允许`192.168.2.1`开始的地址通过`TCP`协议访问的目的。

- 进入接口配置模式，将ACL绑定到路由器进入`192.168.2.1`的方向：

```
interface gig0/1
ip access-group 106 in
exit
```

将序号为`106`的访问控制列表绑定到路由器`gig0/1`端口进入方向。

三、实验结果

1. 网络B中的主机可以自由访问网络A，而其他网络不可访问网络A

使用**网络B中的PC2**尝试ping网络A中的Server0，可以连通

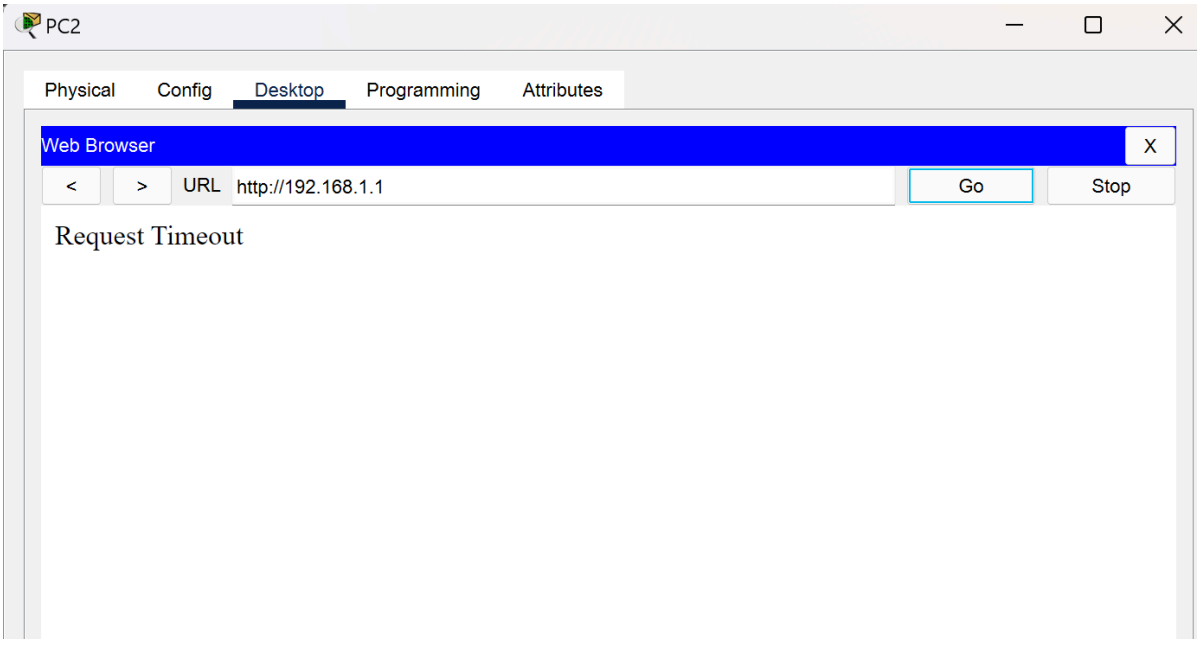
```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=126
Reply from 192.168.1.1: bytes=32 time=12ms TTL=126
Reply from 192.168.1.1: bytes=32 time=10ms TTL=126
Reply from 192.168.1.1: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 5ms

C:\>
```

使用**网络C中的PC6**尝试ping**网络A中的Server0**，不可以连通

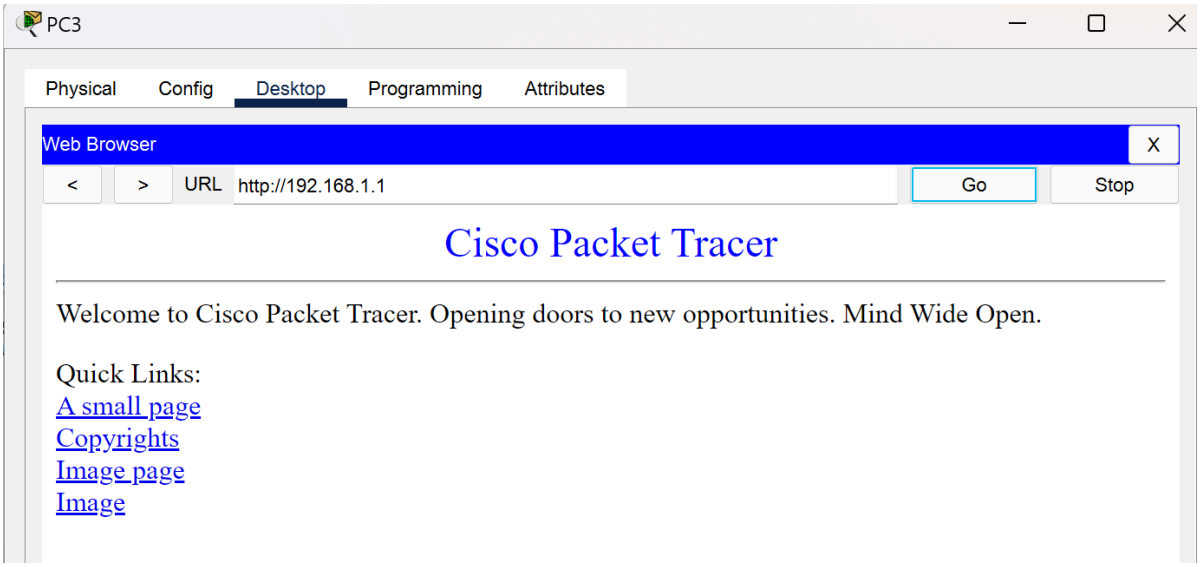
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ngpingpi
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

2. 不允许IP地址为`192.168.2.1`的主机（PC2）访问地址为`192.168.1.1`的服务器的Web服务，允许其他任何主机访问

使用**网络B中的PC2**尝试访问网络A中的server0，结果发现不能访问



使用**网络B中的PC3**尝试访问网络A中的server0，结果发现可以访问



3. 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。

已知**ping指令**使用的协议是ICMP协议，而不是TCP协议，所以我们可以设计使用**网络B中的PC2来ping网络A中的Server0**，同时上面的访问Web服务器的**消极结果**也可以证明只有**TCP协议被拦截**，但其他协议却仍然可以连通，也就证明了**不允许外网的用户主动向内网发起TCP连接。**

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=126
Reply from 192.168.1.1: bytes=32 time<1ms TTL=126
Reply from 192.168.1.1: bytes=32 time<1ms TTL=126
Reply from 192.168.1.1: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

四、总结与分析

通过这次实验，我学会了如何在仿真环境中配置防火墙，并使用防火墙完成了一些基本的过滤功能，基本掌握了防火墙的配置和使用方法，加强了我对计算机网络知识的理解与掌握。