# 网络空间实战攻防训练-实验指导手册

实验2 扩展分组过滤器实验

### 2.1实验原理

互连网结构如图**2.1**所示，分别在路由器R1接口1输入方向和路由器R2接口2输入方向设置扩展分组过滤器，实现只允许终端A访问Web服务器，终端B访问FTP服务器，禁止其他一切网络间通信过程的安全策略。

图片包含 图示

描述已自动生成

###### 图2.1 标准分组互连网结构图

为了实现只允许终端A访问Web服务器，终端B访问FTP服务器，禁止其他一切网络间通信过程的安全策略，需要在路由器R1接口1输入方向配置如下过滤规则集。

①协议类型=TCP,源IP地址=192.1.1.1/32，源端口号=\*，目的IP地址=192.1.2.7/32,目的端口号=80；正常转发。

①表明，只允许与终端A以HTTP访问Web服务器的过程有关的TCP报文继续正常转发。

②协议类型=TCP,源IP地址=192.1.1.7/32，源端口号=21，目的IP地址=192.1.2.1/32,目的端口号=\*；正常转发。

②表明，只允许属于FTP服务器和终端B之间控制连接的TCP报文继续正常转发。

③协议类型=TCP,源IP地址=192.1.1.7/32，源端口号＞1024，目的IP地址=192.1.2.1/32,目的端口号=\*；正常转发。

③表明，只允许属于FTP服务器和终端B之间数据连接的TCP报文继续正常转发。由于FTP服务器是被动打开的，因此，数据连接FTP服务器端的端口号是不确定的，FTP服务器在大于1024的端口号中随机选择一个端口号作为数据连接的端口号。

④协议类型=\*，源IP地址=any，目的IP地址=any；丢弃。

过滤规则④表明，丢弃所有不符合上述过滤规则的IP分组。路由器R2接口2输入方向过滤规则集的作用与此相似。

路由器R2接口2输入方向配置如下过滤规则集。

①协议类型=TCP，源IP地址=192.1.2.1/32，源端口号=\*，目的IP地址=192.1.1.7/32,目的端口号=21；正常转发。

②协议类型=TCP，源IP地址=192.1.2.1/32，源端口号=\*，目的IP地址=192.1.1.7/32,目的端口号＞1024；正常转发。

③协议类型=TCP,源IP地址=192.1.2.7/32,源端口号=80,目的IP地址=192.1.1.1/32,目的端口号=\*；正常转发。

④协议类型=\*，源IP地址=any,目的IP地址=any；丢弃。

条件“协议类型=TCP”是指IP分组首部中的协议字段值是TCP对应的协议字段值（6）。“源端口号=21”是指源端口号字段值必须等于21。“源端口号=\*”是指源端口号字段值可以是任意值。“源IP地址=192.1.2.7/32”是指IP分组首部中的源IP地址必须等于192.1.2.7。

### 2.4关键命令说明

#### 2.4.1配置扩展分组过滤器规则集

以下命令序列用于配置扩展分组过滤器规则集。规则配置顺序就是规则在规则集中的顺序。

|  |
| --- |
| Router(config)#access-list 101 permit tcp host 192.1.1.1 host 192.1.2.7 eq www  Router(config)#access-list 101 permit tcp host 192.1.1.7 eq ftp host 192.1.2.1  Router(config)#access-list 101 permit tcp host 192.1.1.7 gt 1024 host 192.1.2.1  Router(config)#access-list 101 deny ip any any |

access-list 101 permit tcp host 192.1.1.1 host 192.1.2.7 eq www全局模式下使用的命令，指定扩展分组过滤器规则集中的其中一个规则。

该规则对应“①协议类型=TCP,源IP地址=192.1.1.1/32,源端口号=\*，目的IP地址=192.1.2.7/32,目的端口号=80；正常转发”。

host 192.1.1.1可以用IP地址192.1.1.1和反掩码0.0.0.0表示。

与该命令等同的命令是access-list 101 permit tcp 192.1.1.1 0.0.0.0 192.1.2.7 0.0.0.0 eq 80

www是http对应的著名端口号80。目的IP地址后给出的端口号是目的端口号，因此eq www表示目的端口号等于80。源IP地址后没有指定端口号，表示源端口号可以是任意值。

#### 2.4.2将规则集作用到某个接口

Router(config) #interface FastEthernet0/0

Router(config-if)#ip access-group 101 in

Router (config-if)#exit

ip access-group 101 in是接口配置模式下使用的命令,该命令的作用是将编号为101的扩展分组过滤器作用到路由器接口FastEthernet0/0输入方向

路由器接口输人/输出方向以路由器为准,外部至路由器为输入,路由器至外部为输出。

### 2.5实验步骤

（1）根据如图2.1所示互连网结构放置和连接设备,完成设备放置和连接后的逻辑工作区界面截图放在实验报告中。完成路由器Router1和Router2各个接口的配置过程，完成各台路由器RIP配置过程。

完成上述配置过程后的路由器Router1和Router2路由表截图放在实验报告中。

完成各个终端和服务器网络信息配置过程，验证终端和终端之间、终端和服务器之间、服务器和服务器之间的连通性。

（2）在CLI(命令行接口)配置方式下，完成路由器Router1编号为101的扩展分组过滤器的配置过程，并将其作用到路由器接口FastEthernet0/0输入方向。完成路由器Router2编号为101的扩展分组过滤器的配置过程，并将其作用到路由器接口FastEthernet0/1输入方向。

（3）验证不同网络的终端之间和服务器之间不能ping通。PC0发送给Web服务器的ICMP报文，封装成IP分组后沿PC0至Web服务器的IP传输路径传输，到达路由器Router1接口FastEthernet0/0时，被路由器Router1丢弃，路由器Router1丢弃PC0发送给Web服务器的ICMP报文截图保存，分析丢弃原因，保存Cisco中丢弃原因相关截图。

（4）允许PC0通过浏览器访问Web服务器。

FTP服务器配置界面创建两个用户名分别为aaa和cisco的授权用户，授权用户的访问权限是全部操作功能。截图保存PC2访问FTP服务器的过程。

### 2.6实验要求

（1）按照实验报告模板提交实验报告。

（2）实验报告中包含关键步骤的截图。

（3）分析路由器Router1丢弃PC0发送给Web服务器的ICMP报文的原因。

（4）给出路由器Router1接口和RIP配置过程、路由器Router1口和RIP配置过程、路由器Router1扩展分组过滤器配置过程及路由器Router2扩展分组过滤器配置过程中的命令序列。

（5）思考：如何说明用扩展分组过滤器实施精确控制是有困难的？