# 网络空间实战攻防训练-实验指导手册

实验1 标准分组过滤器实验

### 1.1实验原理

互连网结构如图1.1所示，为了防止终端实施源IP地址欺骗攻击，路由器每一个接口只允许输入源IP地址属于该接口连接的网络的网络地址的IP分组。如路由器R1接口1连接的网络的网络地址是192.1.1.0/24，路由器R1接口1只允许输入源IP地址属于网络地址192.1.1.0/24的IP分组。



图 1.1互连网结构图

路由器R1接口1和接口2、路由器R2接口2和接口3的输入方向配置只允许输入源IP地址属于该接口连接的网络的网络地址的IP分组的标准分组过滤器，使这些接口连接的网络中的终端无法冒用其他网络的IP地址。

### 1.2实验目的

1. 验证标准分组过滤器过滤IP分组的原理和过程。
2. 验证路由器标准分组过滤器的配置过程。
3. 验证标准分组过滤器防御源IP地址欺骗攻击的原理和过程。

### 1.3实验环境

安装具有Cisco Packet Tracer的计算机

### 1.4关键命令说明

#### 1.4.1定义标准分组过滤器

以下命令序列用于定义一个只允许输入源IP地址属于网络地址192. 1.1.0/24的 IP分组的标准分组过滤器。

Router(config)# access-list 1 permit 192.1.1.0 0.0.0.255

Router(config)# access-list 1 deny any

access-list 1 permit 192.1.1.0 0.0.0.255是全局模式下使用的命令。该命令的作用是指定一条属于编号为1的标准分组过滤器的规则。该规则中，1是编号，标准分组过滤器允许的编号范围是1-99,所有属于同一标准分组过滤器的规则必须有着相同的编号。

permit是对符合条件的IP分组实施的动作，该动作是允许符合条件的IP分组继续传输。192.1.3.0 0.0.0.255定义源IP地址范围，其中192.1.1.0是网络地址，也是CIDR地址块的起始地址，0.0.0.255是子网掩码255.255.255.0的反码。两者一起将源IP地址范围定义为CIDR地址块192.1.1.0/24,表明该规则的条件是源IP地址属于CIDR地址块192.1.1.0/24。综上所述，这条规则的含义是，允许源IP地址属于CIDR地址块192.1.1.0/24的IP分组继续传输。

access-list 1 deny any是全局模式下使用的命令,该命令的作用同样是指定一条属于编号为1的标准分组过滤器的规则。该规则中，1是编号，相同编号的规则属于同一标准分组过滤器。deny是对符合条件的IP分组实施的动作，该动作是丢弃符合条件的IP分组。any表示源IP地址范围是任意范围。这条规则的含义是，丢弃源IP地址是任何地址的IP分组。

标准分组过滤器中的规则是有顺序的，如果某个IP分组符合第一条规则的条件，则对该IP分组实施第一条规则规定的动作，不再用其他规则的条件检测该IP分组。如果该IP分组不符合第一条规则的条件，则用第二条规则的条件检测该IP分组。如果该IP分组符合第二条规则的条件，则对该IP分组实施第二条规则规定的动作，不再用其他规则的条件检测该IP分组，依此类推。

对于由上述两条规则组成的标准分组过滤器，由于所有IP分组符合第二条规则的条件，因此，该标准分组过滤器实现的功能是，如果某个IP分组的源IP地址属于CIDR地址块192.1.1.0/24,则继续传输该IP分组，否则丢弃该IP分组。

#### 1.4.2将标准分组过滤器作用到路由器接口

以下命令序列用于将编号为1的标准分组过滤器作用到路由器接口FastEthernet0/0。

Router(config)#interface FastEthernet0/0

Router(config-if)#ip access-group 1 in

Router(config-if)#exit

ip access-group 1 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1的标准分组过滤器作用到指定路由器接口（这里是FastEthernet0/0）的输入方向，其中1是标准分组过滤器编号，in表明输入方向。

### 1.5实验步骤

（1）根据图1.1所示的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当中。

（2）完成路由器各个接口IP地址和子网掩码配置过程，完成路由器RIP配置过程。 完成上述配置过程后，路由器Router1和Router2的路由表截图放在实验报告当中。

（3）完成各个终端的网络信息配置过程，PC0配置的网络信息截图放在实验报告当中。

（4）切换到模拟操作模式，在PC0上创建ICMP报文，封装该ICMP报文的IP分组的源和目的IP地址（PC0上创建的ICMP报文放到实验报告中）。目的IP地址是PC3的IP地址192.1.4.1,源IP地址是伪造的IP地址192.1.6.1（PC0的IP地址是192.1.1.l）。启动该IP分组PC0至PC3的传输过程，路由器Router1接口FastEthernet0/0输入方向允许输入该IP分组，Router1正常转发该IP分组（Router 1正常转发伪造源IP地址的IP分组截图放到实验报告中）。

（5）切换到实时操作模式，在CLI(命令行接口)配置方式下，完成路由器Router1标准分组过滤器配置过程，并将其作用到接口FastEthernet0/0输入方向，使路由器Router1只允许继续转发源IP地址属于CIDR地址块192.1.1.0/24的IP分组。

（6）切换到模拟操作模式，在PC0上创建ICMP报文，封装该ICMP报文的IP分组的源和目的IP地址如图1.2所示。启动该IP分组PC0至PC3的传输过程，路由器Router1接口FastEthernet0/0输入方向丢弃该IP分组。分析丢弃原因。



图 1.2 PC0上的ICMP报文

### 1.6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Router1丢弃伪造源IP地址的IP分组的原因。

（4）给出Router1及Router2命令行接口配置过程中的命令序列。