# 网络空间实战攻防训练-实验指导手册

实验3 有状态分组过滤器实验

### 3.1实验原理

互连网络结构如图2.1所示，分别在路由器R1接口1和路由器R2接口2设置有状态分组过滤器，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。

初始状态下，路由器R1接口1输入方向只允许与终端A发起访问Web服务器的过程有关的TCP报文继续传输，因此，路由器R1接口1输入方向的过滤规则集如下。

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

②协议类型=\*，源IP地址=any,目的IP地址=any；丢弃。

同样，初始状态下，路由器R1接口1输出方向只允许与终端B发起访问FTP服务器的过程有关的TCP报文继续传输，因此，路由器R1接口1输出方向的过滤规则集如下。

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=\*，源IP地址=any,目的IP地址=any；丢弃。

与第8.2节中的扩展分组过滤器实验不同，路由器R1接口1输入方向的扩展分组过滤器只允许与终端A发起访问Web服务器的过程相关的TCP报文输入，禁止FTP服务器发送给终端B的响应报文输入。同样，路由器R1接口1输出方向的扩展分组过滤器只允许与终端B发起访问FTP服务器的过程相关的TCP报文输出，禁止Web服务器发送给终端A的响应报文输出。

这是有状态分组过滤器不同于无状态分组过滤器的地方，对于终端A发起访问Web服务器的过程，只有在路由器R1接口1输入方向输入了终端A发送给Web服务器的请求消息，路由器R1才会自动在接口1输出方向设置允许该请求消息对应的响应消息输出的过滤规则。即输出方向允许Web服务器发送给终端A的TCP报文输出的前提有两个，一是输入方向输入了封装终端A发送给Web服务器的请求消息的TCP报文，且该TCP报文与规则①匹配。二是输岀的TCP报文是封装Web服务器发送给终端A的响应消息的TCP报文。

对于终端B发起访问FTP服务器过程，只有在路由器R1接口1输出方向输出了终端B发送给FTP服务器的请求消息，路由器R1才会自动在接口1输入方向设置允许该请求消息对应的响应消息输入的过滤规则。

同样原因，路由器R2接口2输入方向的过滤规则集如下。

①协议类型=TCP,源IP地址=192.1.2.1/32,源端口号二―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=\*，源IP地址=any,目的IP地址-any；丢弃。

路由器R2接口2输出方向的过滤规则集如下。

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。

②协议类型=\*，源IP地址=any,目的IP地址-any；丢弃。

路由器R2接口2输入/输岀方向过滤规则集的配置原则与路由器R1接口1输入输出方向过滤规则集的配置原则相同。

除了在路由器接口输入/输岀方向配置扩展分组过滤器以外，为了能够在一个方向通过请求消息后，在另一个方向自动添加允许该请求消息对应的响应消息通过的过滤规则，需要同步配置监测器，监测器用于监测某个方向通过的请求消息，并在监测到请求消息后，自动在相反方向添加允许该请求消息对应的响应消息通过的过滤器规则。

### 3.2实验目的

(1)验证有状态分组过滤器的配置过程。

(2)验证有状态分组过滤器实现访问控制策略的过程。

(3)验证过滤规则设置原则和方法。

(4)验证过滤规则作用过程。

(5)验证基于会话的信息交换控制机制。

### 3.3关键命令说明

##### 3.3.1定义监測器过程

以下命令序列用于定义监测器°

Router(config)#ip inspect name al http

Router(config)#ip inspect name al tcp

Router(config)#ip inspect name a2 tcp

ipinspectnamealhttp是全局模式下使用的命令，该命令的作用是在名为al的监测器中添加监测协议HTTP。一旦监测HTTP,则只有在监测方向监测到HTTP请求消息通过后，才允许该HTTP请求消息对应的响应消息通过相反方向。

Ip inspect name al tcp是全局模式下使用的命令，该命令的作用是在名为al的监测器中添加监测协议TCP。一旦监测TCP,则只有在监测方向监测到请求建立TCP连接的请求报文通过后，才允许属于该TCP连接的TCP报文通过相反方向。TCP连接由两端插口唯一标识，即由两端IP地址和两端端口号唯一标识。

名为al的监测器中同时监测HTTP和TCP，由于HTTP是应用层协议，因此，接收到TCP报文后，首先根据HTTP实施监测过程，即如果TCP报文中封装的是HTTP响应消息，且没有在监测方向监测到对应的HTTP请求消息，则即使该TCP报文属于已经监测到的某个TCP连接，路由器也不允许该TCP报文通过。

##### 3.3.2将监测器作用到路由器接口

以下命令序列用于将监测器作用到路由器接口FastEthernet0/0

Router(config-if)#ip inspect al in

Router(config-if)#ip inspect a2 out

Router(config-if)#exit

ipinspectalin是接口配置模式下使用的命令，该命令的作用是将名为al的监测器作用到路由器接口FastEthernet0/0输入方向，in表示输入方向。执行该命令后，如果路由器接口FastEthernet0/0输入方向允许通过HTTP请求消息或TCP请求报文，则路由器接口FastEthernet0/0输出方向允许通过该HTTP请求消息对应的响应消息，或者属于该TCP请求报文请求建立的TCP连接的TCP报文。

路由器接口FastEthernet0/0输入方向通过设置的扩展分组过滤器确定是否允许通过HTTP请求消息或TCP请求报文。一旦在路由器接口FastEthernet0/0输入方向设置监测器，且监测器监测到扩展分组过滤器允许通过的HTTP请求消息或TCP请求报文，则路由器接口FastEthernet0/0输出方向自动添加允许通过该HTTP请求消息对应的响应消息，或者属于该TCP请求报文请求建立的TCP连接的TCP报文的过滤规则，该过程不受路由器接口FastEthernet0/0输出方向设置的扩展分组过滤器的限制。

### 3.4实验步骤

本实验与实验2中的扩展分组过滤器实验相比，有以下不同。

##### 3.4.1设置的扩展分组过滤器不同

以路由器Router1接口FastEthernet0/0为例，输入方向设置的扩展分组过滤器只允许与终端A发起访问Web服务器的过程有关的TCP报文通过，输岀方向设置的扩展分组过滤器只允许与终端B发起访问FTP服务器的过程有关的TCP报文通过，即输入方向设置的扩展分组过滤器不允许FTP服务器向终端B发送TCP报文。同样，输出方向设置的扩展分组过滤器不允许Web服务器向终端A发送TCP报文。

##### 3.4.2输入输出方向设置监测器

以路由器Router1接口FastEthernet0/0为例，为了保证输入方向通过终端A发送给Web服务器的请求消息后，才允许输出方向通过Web服务器发送给终端A的响应消息，需要在输入方向设置监测器，只有当监测器监测到输入方向设置的扩展分组过滤器允许的终端A发送给Web服务器的请求消息后，才允许输出方向输出Web服务器向终端A发送的响应消息。这种允许不受输出方向扩展分组过滤器的限制。

##### 3.4.3更严格的管控

以路由器Router1接口FastEthernet0/0例，由于输入方向设置的扩展分组过滤器只允许终端A向Web服务器发送TCP报文，因此，在终端B向FTP服务器发送请求消息前,输入方向不允许输入FTP服务器发送给终端B的TCP报文，TCP报文不允许输入路由器Router1接口FastEthernet0/0如图2.1所示的互连网只允许PC0通过浏览器访问WebServer,PC2通过FTP访问FTPServer0。

### 3.5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）给出Router1安全功能配置过程和Router2安全功能配置过程中的命令序列

（4）思考：结合实验安全功能配置过程，总结标准分组和有状态分组防火墙之间的不同