

## 《信息安全及实践》课程实验报告

学院： 信息学院    专业： 计算机科学与技术    年级： 2019

姓名： 白文强                      学号： 20191060064

姓名： 赵浩杰                      学号： 20191060074

姓名： 李泽昊                      学号： 20191060065

实验时间： 2021 年 12 月 10 日

实验名称： 扩展分组过滤器实验和有状态分组过滤器实验

实验成绩：

---



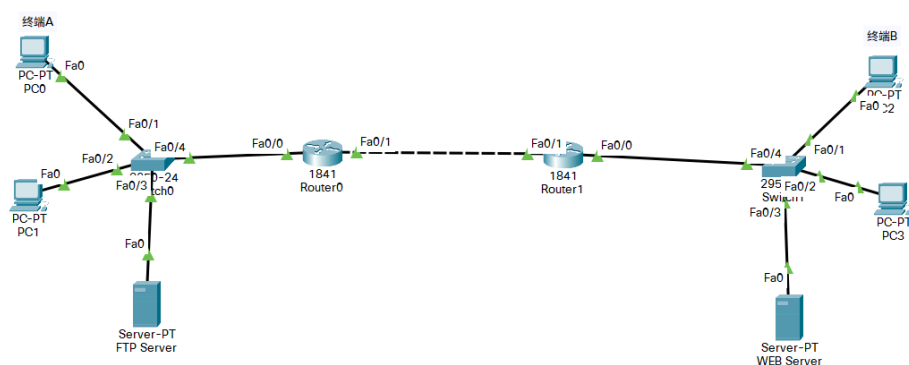
# 扩展分组过滤器实验

## 一、实验目的

- (1) 验证扩展分组过滤器的配置过程
- (2) 验证扩展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

## 二、实验步骤

(1) 完成互联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如下图：。



(2) 在 CLI 配置方式下，完成路由器 Router0 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 f0/0 输入方向。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 f0/1 输入方向。各路由器路由表如下图：

Router0 路由表:

```
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    192.1.1.0/24 is directly connected, FastEthernet0/0
R    192.1.2.0/24 [120/1] via 192.1.3.2, 00:00:05, FastEthernet0/1
C    192.1.3.0/24 is directly connected, FastEthernet0/1
```







Router1 路由表:

```
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

R    192.1.1.0/24 [120/1] via 192.1.3.1, 00:00:03, FastEthernet0/1
C    192.1.2.0/24 is directly connected, FastEthernet0/0
C    192.1.3.0/24 is directly connected, FastEthernet0/1
```

(3) 验证不同网络的终端之间和服务器之间不能 ping 通:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC0	PC2	ICMP		0.000	N	0	(edit)
	Successful	PC0	PC3	ICMP		0.000	N	1	(edit)
	Successful	PC0	WEB Server	ICMP		0.000	N	2	(edit)

如图可以看到，PC0 可以成功 ping 通网络 192.1.2.0 中的终端。

(4) 在 FTP 服务器中创建两个用户名分别为 aaa 和 cisco 的授权用户，访问权限是全部操作功能。

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

FTP

Service ☒ On ☐ Off

User Setup

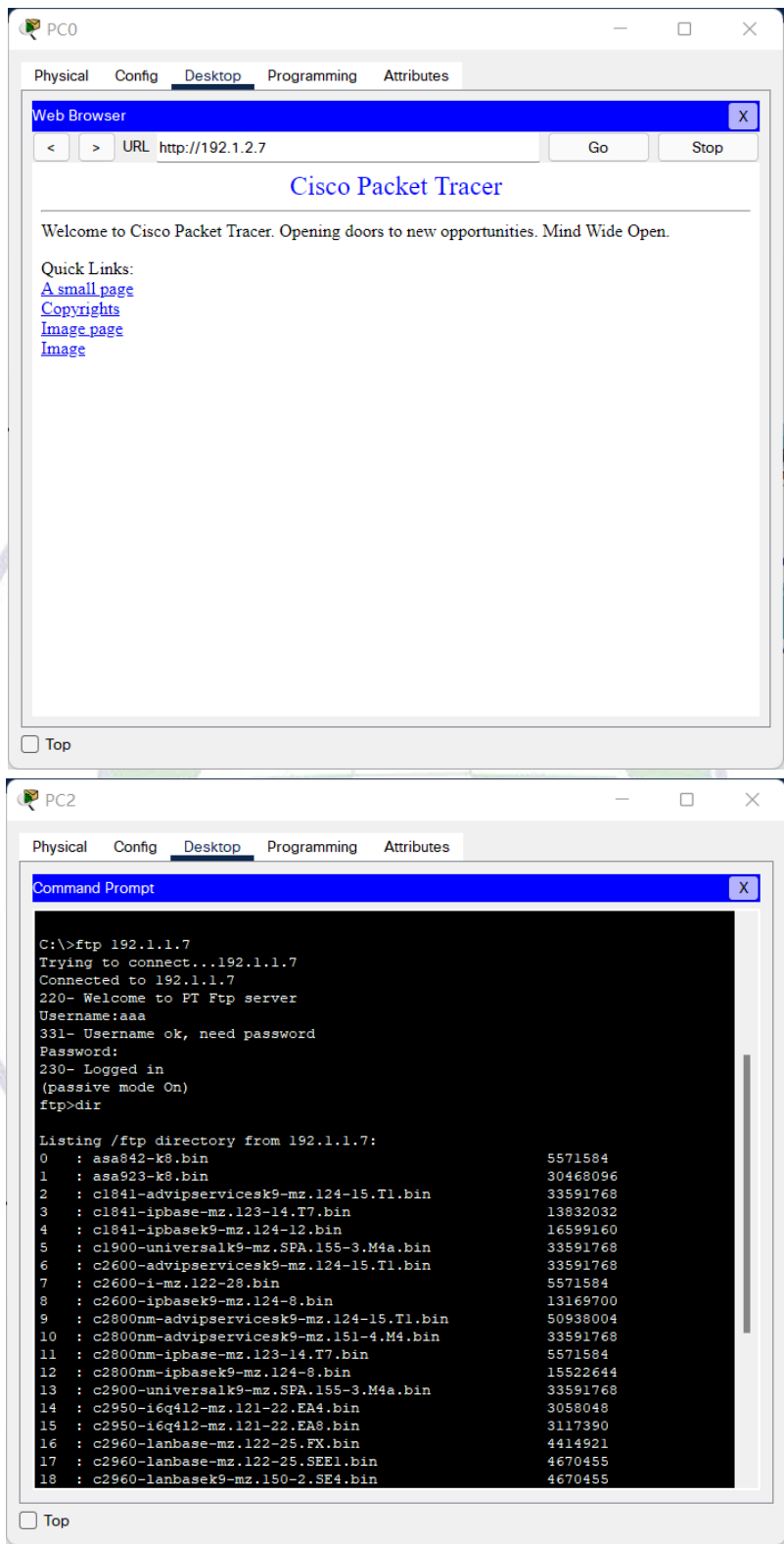
Username

Password

☐ Write ☐ Read ☐ Delete ☐ Rename ☐ List

	Username	Password	Permission	
1	aaa	bbb	RWDNL	Add
2	cisco	cisco	RWDNL	Save
				Remove

(5) 利用终端 A 的网站访问 Web 服务器，利用终端 B 的网站访问 FTP 服务器，部分如下图：



### 三、实验结果及分析

在设置过滤器之前，来自网络 192.1.1.0 和网络 192.1.2.0 中的不同设备可以

互相访问。在设置过滤器之后，利用简单报文工具从终端 A 发送 ICMP 报文到 WEB 服务器，发现报文到达 Router0 之后被丢弃，说明过滤器起了作用；同样，利用简单报文工具从终端 B 发送 ICMP 报文到 FTP 服务器，报文到达 Router1 之后被丢弃。

在设置过滤器之后，虽然报文无法到达，但是终端 A 可以通过浏览器访问 WEB 服务器，终端 B 可以通过 FTP 访问 FTP 服务器，实验成功。

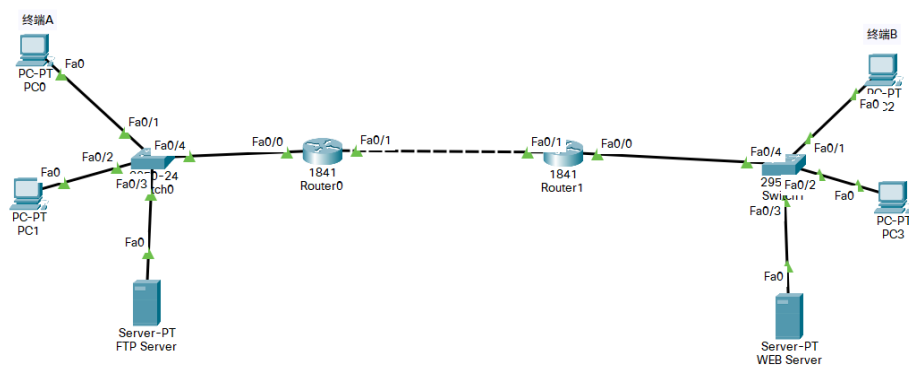
## 有状态分组过滤器实验

### 一、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

### 二、实验步骤

(1) 完成互联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如下图：



(2) 设置路由器，使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，输出方向设置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。

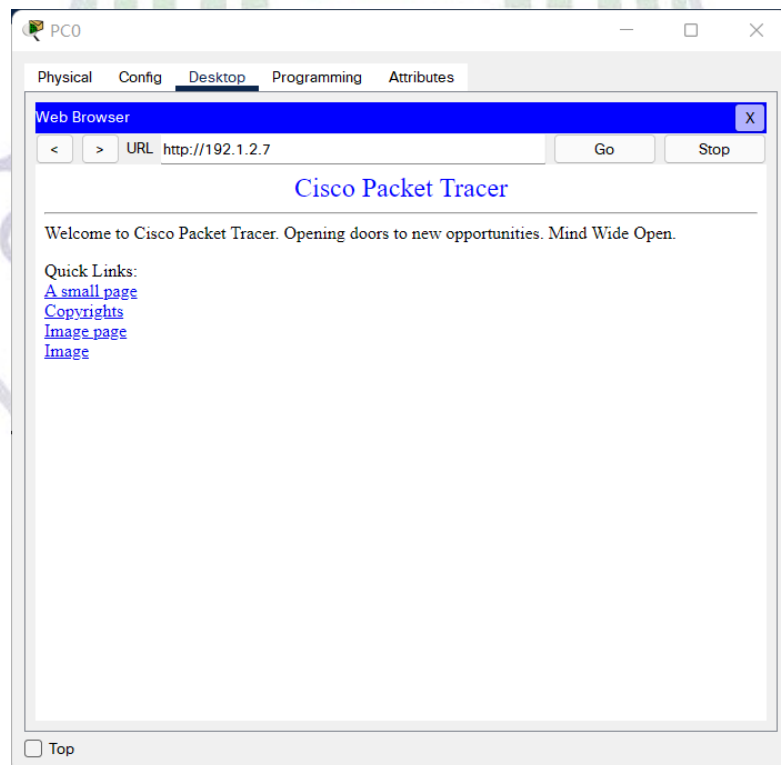
```

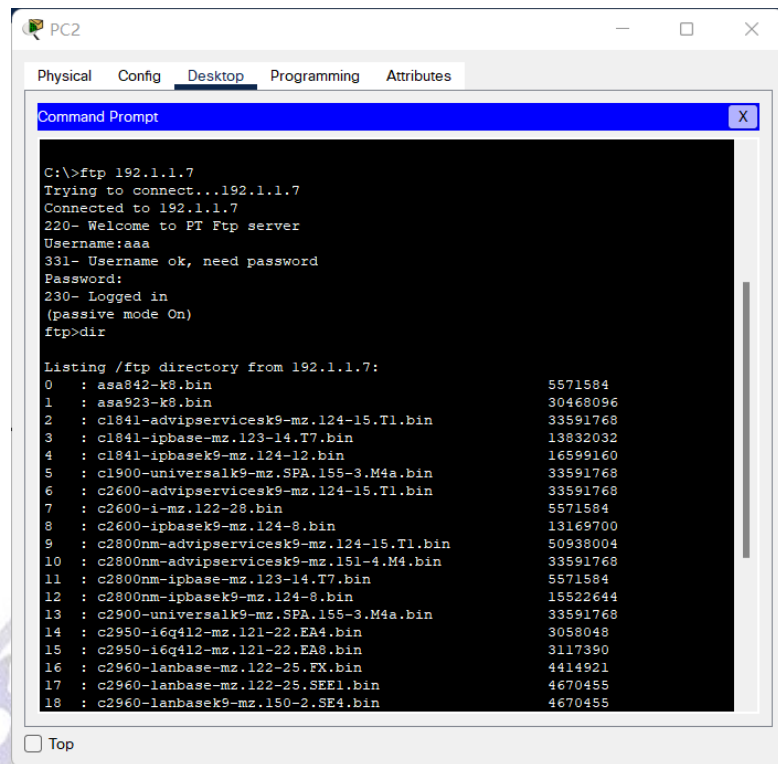
Router(config)#access-list 101 permit tcp host 192.1.1.1 host 192.1.2.7 eq
www
Router(config)#access-list 101 deny ip any any
Router(config)#access-list 102 permit tcp host 192.1.2.1 host 192.1.1.7 eq
ftp
Router(config)#access-list 102 permit tcp host 192.1.2.1 host 192.1.1.7 gt
1024
Router(config)#access-list 102 deny ip any any
Router(config)#ip inspect name a1 http
Router(config)#ip inspect name a2 tcp
Router(config)#ip inspect name a1 tcp
Router(config)#interface f0/0
Router(config-if)#ip access-group 101 in
Router(config-if)#ip access-group 102 out
Router(config-if)#ip inspect a1 in
Router(config-if)#ip inspect a2 out
Router(config-if)#exit

Router(config)#access-list 101 permit tcp host 192.1.2.1 host 192.1.1.7 eq
ftp
Router(config)#access-list 101 permit tcp host 192.1.2.1 host 192.1.1.7 gt
1024
Router(config)#access-list 101 deny ip any any
Router(config)#access-list 102 permit tcp host 192.1.1.1 host 192.1.2.7 eq
www
Router(config)#access-list 102 deny ip any any
Router(config)#ip inspect name a1 http
Router(config)#ip inspect name a1 tcp
Router(config)#ip inspect name a2 tcp
Router(config)#interface f0/1
Router(config-if)#ip access-group 101 in
Router(config-if)#ip access-group 102 out
Router(config-if)#ip inspect a1 out
Router(config-if)#ip inspect a2 in
Router(config-if)#exit

```

(3) 利用终端 A 的网站访问 Web 服务器，利用终端 B 的网站访问 FTP 服务器，部分如下图：





```
C:\>ftp 192.1.1.7
Trying to connect...192.1.1.7
Connected to 192.1.1.7
220- Welcome to FT Ftp server
Username:aaa
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 192.1.1.7:
 0 : asa842-k8.bin                      5571584
 1 : asa923-k8.bin                      30468096
 2 : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
 3 : c1841-ipbase-mz.123-14.T7.bin       13832032
 4 : c1841-ipbasek9-mz.124-12.bin        16599160
 5 : c1900-universalk9-mz.SPA.155-3.M4a.bin 33591768
 6 : c2600-advipservicesk9-mz.124-15.T1.bin 33591768
 7 : c2600-i-mz.122-28.bin               5571584
 8 : c2600-ipbasek9-mz.124-8.bin         13169700
 9 : c2800nm-advipservicesk9-mz.124-15.T1.bin 50938004
10 : c2800nm-advipservicesk9-mz.151-4.M4.bin 33591768
11 : c2800nm-ipbase-mz.123-14.T7.bin     5571584
12 : c2800nm-ipbasek9-mz.124-8.bin       15522644
13 : c2900-universalk9-mz.SPA.155-3.M4a.bin 33591768
14 : c2950-i6q4l2-mz.121-22.EA4.bin     3058048
15 : c2950-i6q4l2-mz.121-22.EA8.bin     3117390
16 : c2960-lanbase-mz.122-25.FX.bin      4414921
17 : c2960-lanbase-mz.122-25.SEE1.bin    4670455
18 : c2960-lanbasek9-mz.150-2.SE4.bin    4670455
```

### 三、实验结果及分析

在设置过滤器之前，来自网络 192.1.1.0 和网络 192.1.2.0 中的不同设备可以互相访问。在设置过滤器之后，利用简单报文工具从终端 A 发送 ICMP 报文到 WEB 服务器，发现报文到达 Router0 之后被丢弃，说明过滤器起了作用；同样，利用简单报文工具从终端 B 发送 ICMP 报文到 FTP 服务器，报文到达 Router1 之后被丢弃。在设置过滤器之后，虽然报文无法到达，但是终端 A 可以通过浏览器访问 WEB 服务器，终端 B 可以通过 FTP 访问 FTP 服务器。

与分组过滤器不同的是，有状态分组过滤在输入输出方向都设置了过滤器，配置检测器后，在一个方向通过请求信息后，可以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。

### 四、实验总结及体会

本次实验通过在路由器接口设置过滤器的方式实现了仅允许终端 A 通过浏览器访问 WEB 服务器、终端 B 通过 FTP 命令访问 FTP 服务器，禁止其他一切网络间通信过程。通过本次实验，对分组过滤器的原理与规则、监测器的使用有了较为深刻的认识。