《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： |  |

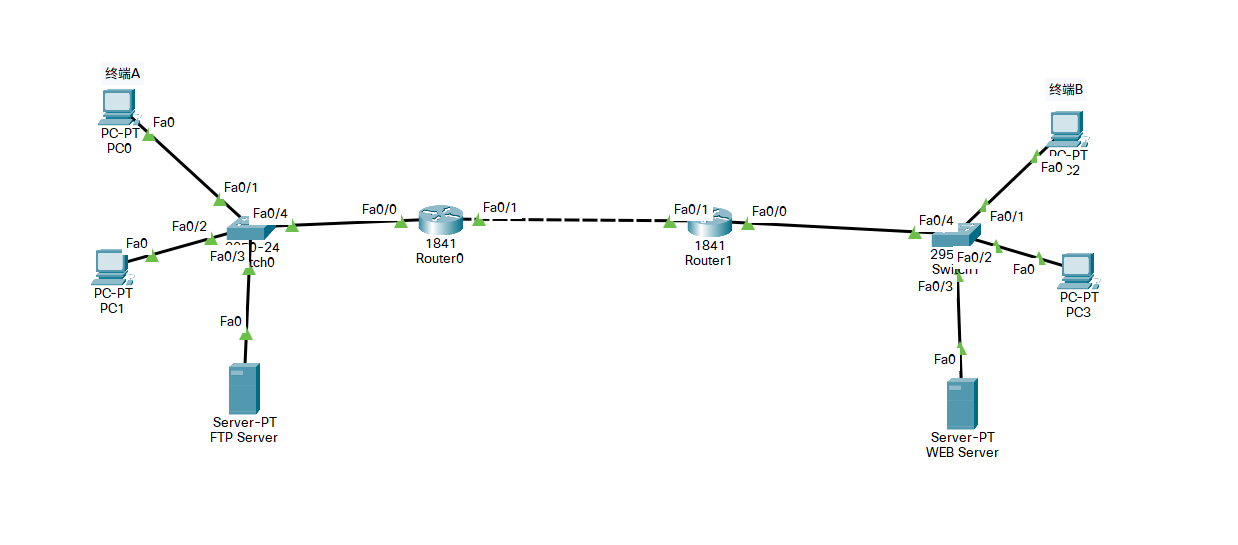
扩展分组过滤器实验

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

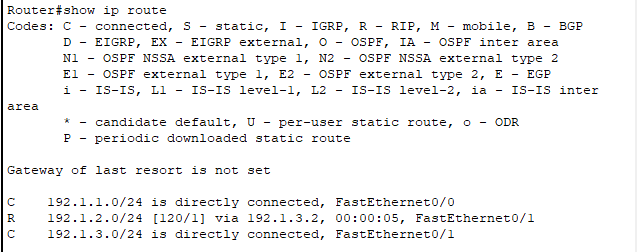
二、实验步骤

(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：。

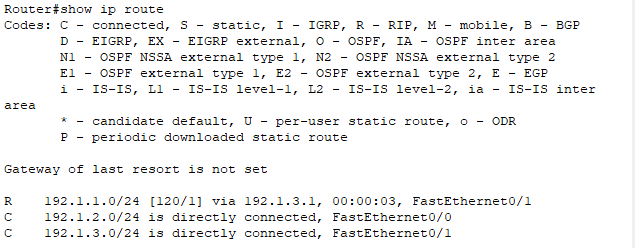


(2)在CLI配置方式下，完成路由器Router0编号为101的扩展分组过滤器的配置过程，并将其作用到路由器接口f0/0输入方向。完成路由器Router1编号为101的扩展分组过滤器的配置过程，并将其作用到路由器接口f0/1输入方向。各路由器路由表如下图：

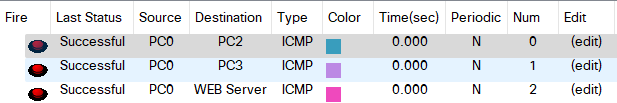
**Router0路由表：**

****

**Router1路由表：**

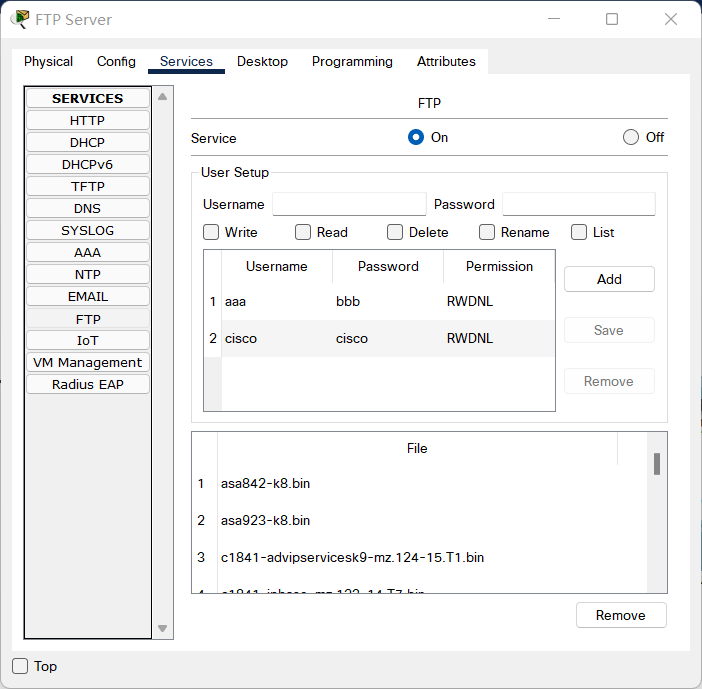


(3)验证不同网络的终端之间和服务器之间不能ping通：

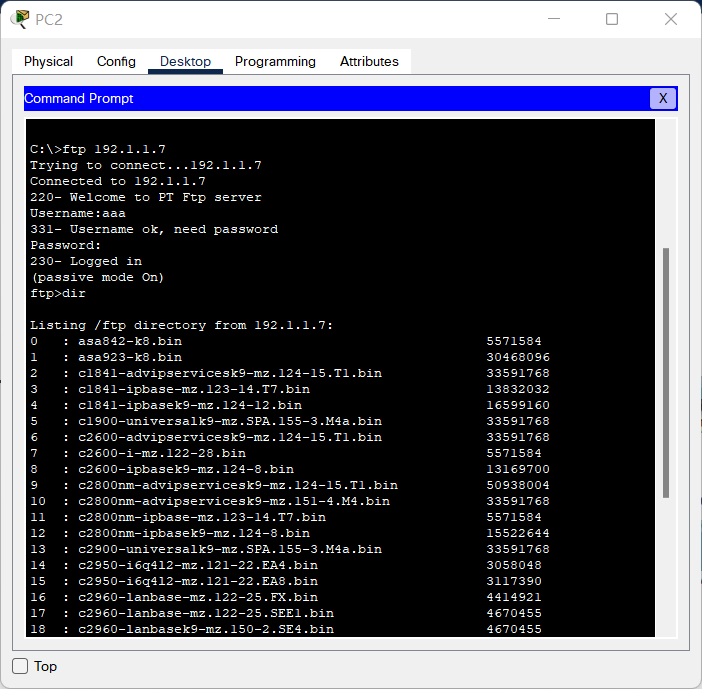
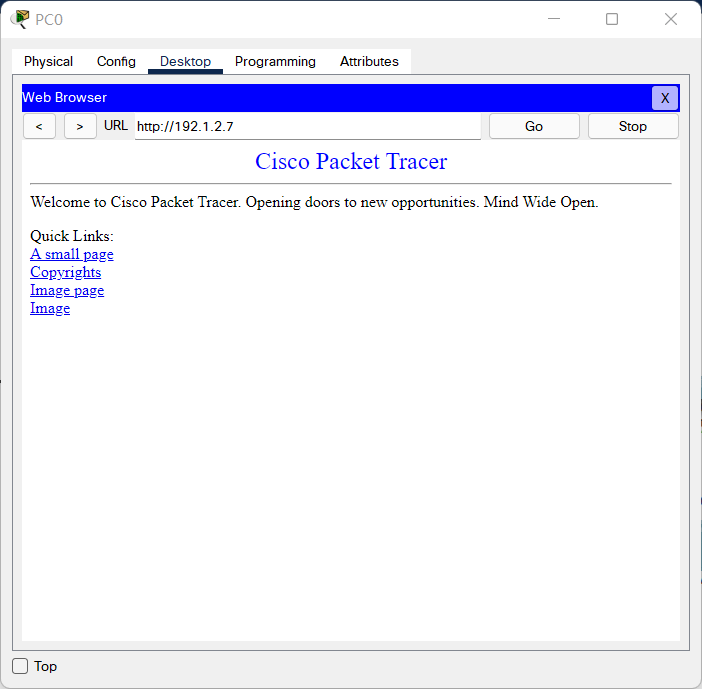


如图可以看到，PC0可以成功ping通网络192.1.2.0中的终端。

(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。



(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。

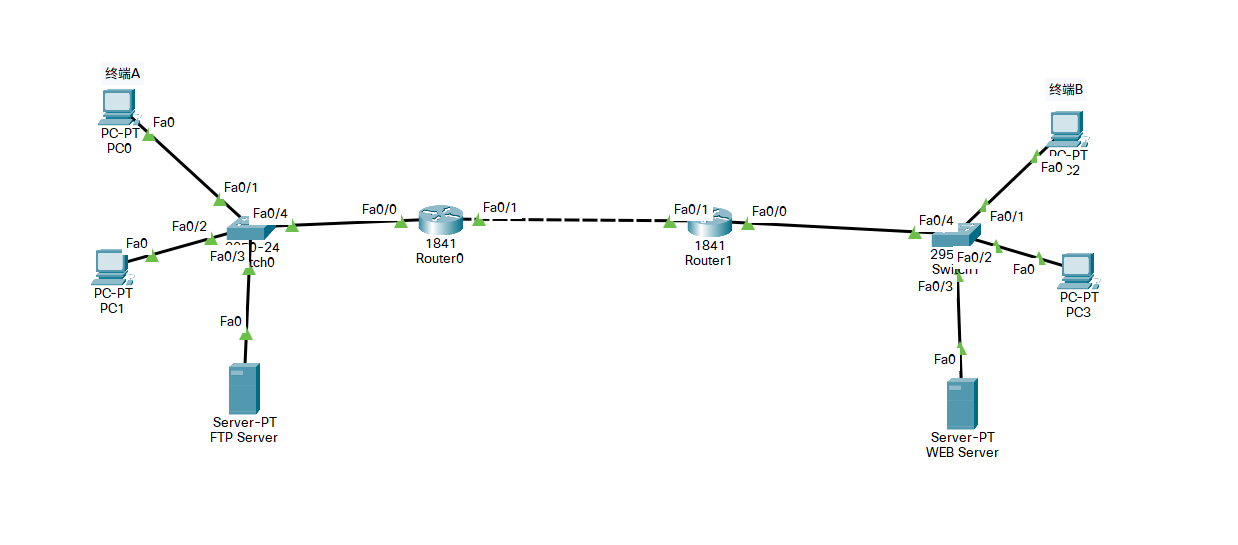
有状态分组过滤器实验

一、实验目的

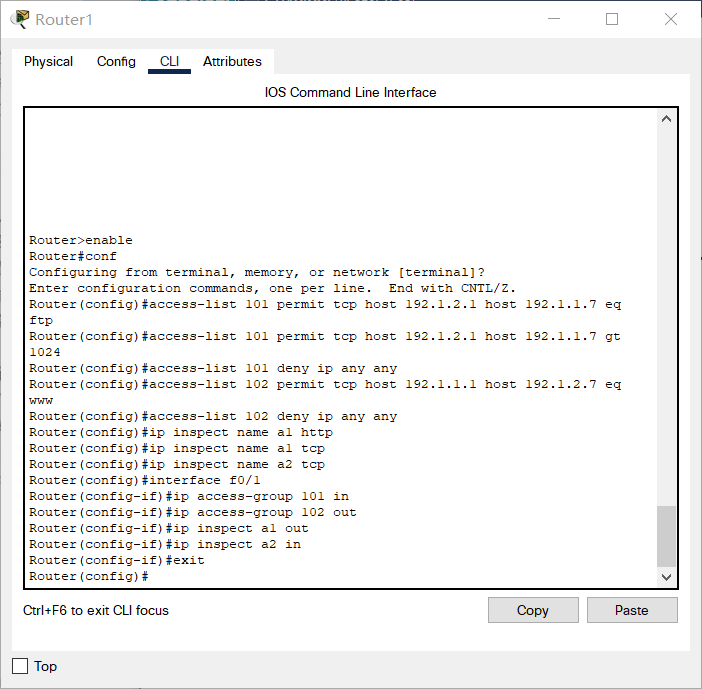
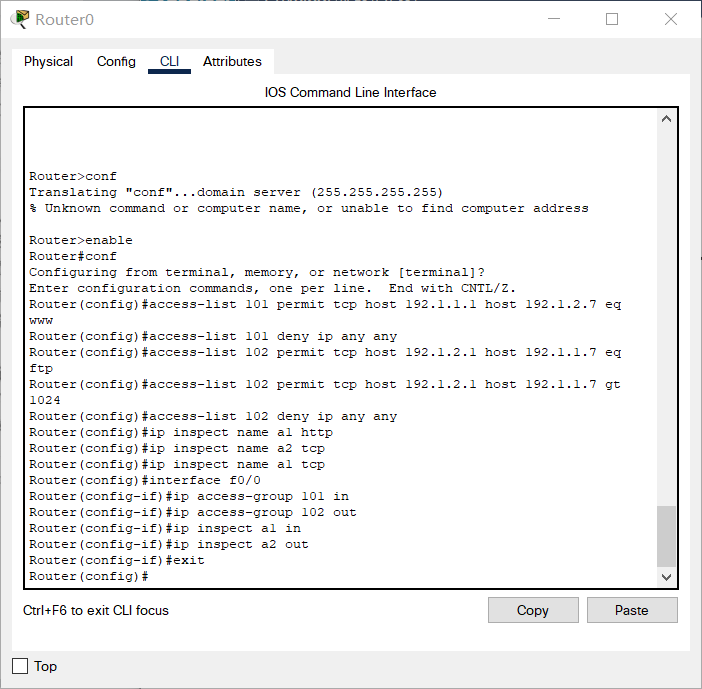
1. 验证有状态分组过滤器的配置过程
2. 验证有状态分组过滤器实现访问控制策略的过程
3. 验证过滤规则设置原则和方法
4. 验证过滤规则作用过程
5. 验证基于会话的信息交换控制机制

二、实验步骤

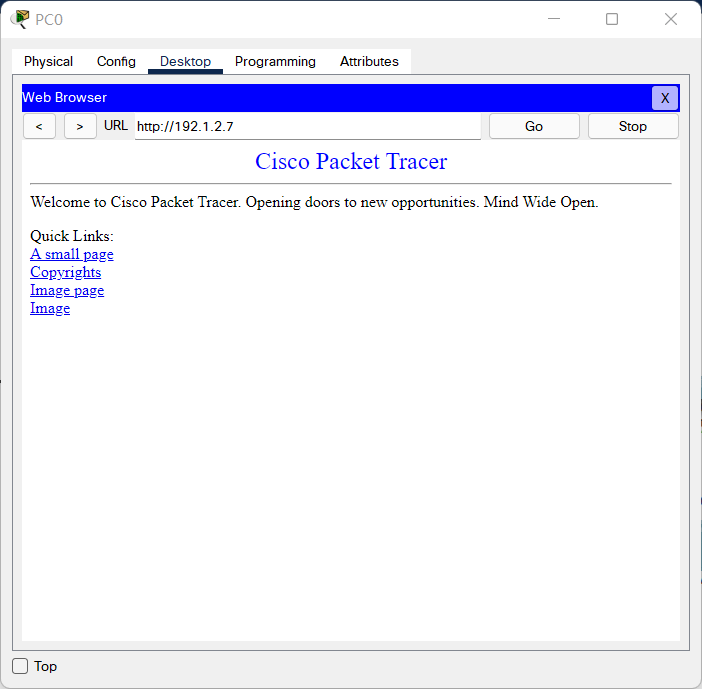
(1)完成互联网结构放置和连接设备，完成设备放置和连接后的逻辑工作区界面如下图：

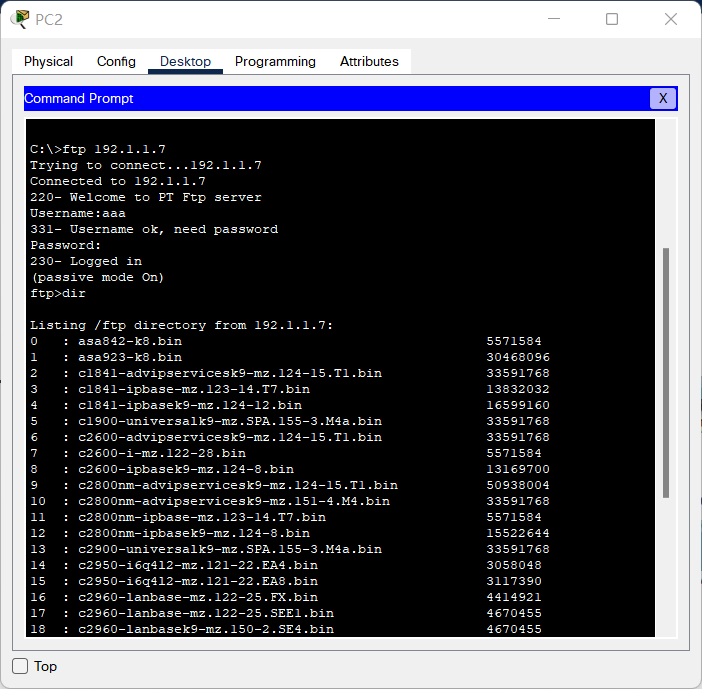


(2) 设置路由器，使输入方向设置的扩展分组过滤器只允许与终端A发起访问Web服务器的过程有关的TCP报文通过，输出方向设置扩展分组过滤器只允许与终端B发起访问FTP服务器的过程有关的TCP报文通过，即输入方向设置的扩展分组过滤器不允许FTP服务器向终端B发送TCP报文。



(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：





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。