**西安电子科技大学**

**计算机与网络安全综合实验 课程实验报告**

**实验名称 入侵检测系统实验**

网络与信息安全 学院 2118021 班

成 绩

姓名 学号

同作者

实验日期 2024 年 05 月 27 日

|  |
| --- |
| 指导教师评语：  指导教师：  年 月 日 |
| **实验报告内容基本要求及参考格式**  一、实验目的  二、实验所用仪器（或实验环境）  三、实验基本原理及步骤（或方案设计及理论计算）  四、实验数据记录（或仿真及软件设计）  五、实验结果分析及回答问题（或测试环境及测试结果） |

# 实验1. 入侵检测系统实验一

## 一、实验目的

## 验证入侵检测系统配置过程。

## 验证入侵检测系统控制信息流传输过程的机制。

## 验证基于特征库的入侵检测机制的工作过程。

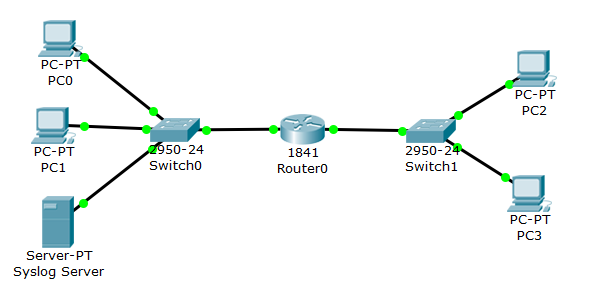
## 二、实验任务

1. 使用自己的语言简述基于特征库的入侵检测机制的工作过程。

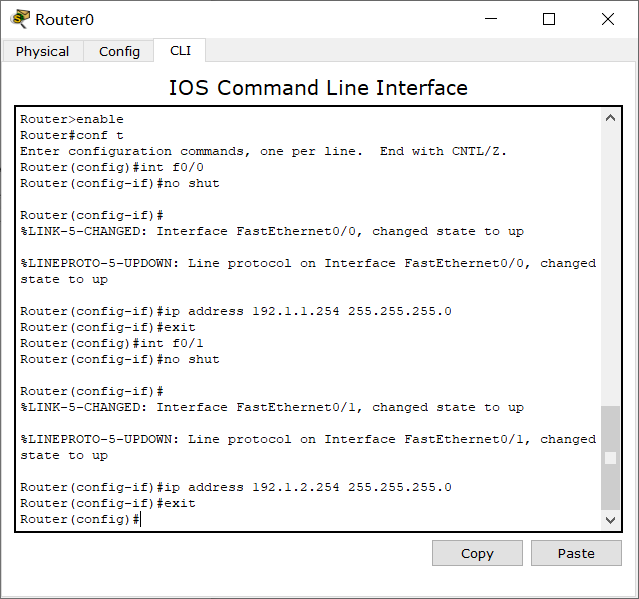
* **加载特征库：**首先入侵检测需要加载包含各种入侵特征的特征库。特征库的每个条目包括识别入侵行为的信息流特征和具有这些特征的信息流所采取的动作
* **配置入侵检测规则：**在路由器接口（输入或输出方向）上配置入侵检测规则
* **信息流监控：**配置完成后，路由器会持续监控通过接口的信息流
* **特征匹配：**监控到的信息流会与特征库中的特征进行比较。如果某个信息流匹配到特定的入侵特征，则系统会采取预定义的动作，比如丢弃信息流
* **记录和通知：**检测到入侵行为后，系统会根据配置记录日志信息，通知管理员

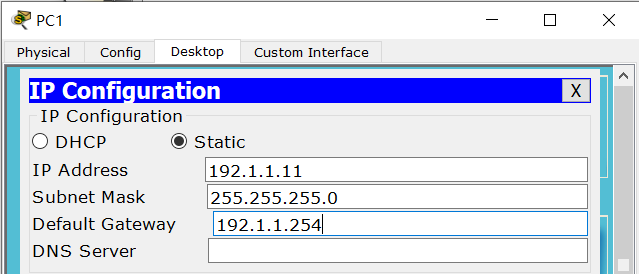
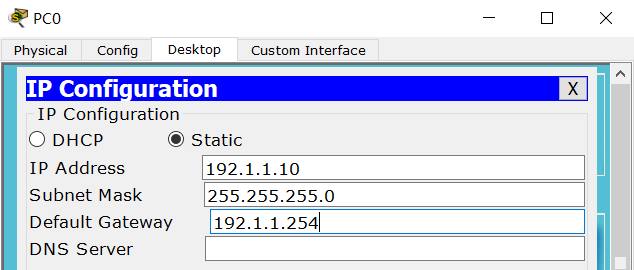
1. 实验步骤

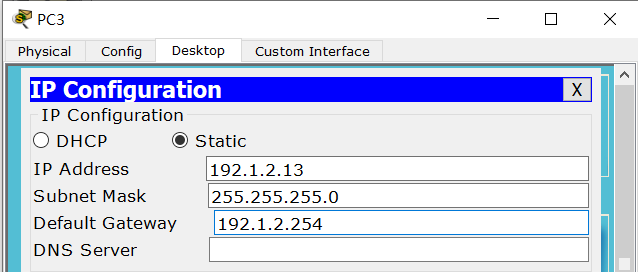
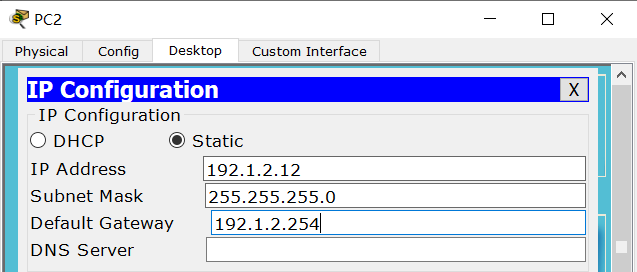
首先给出实验所用的拓扑图：

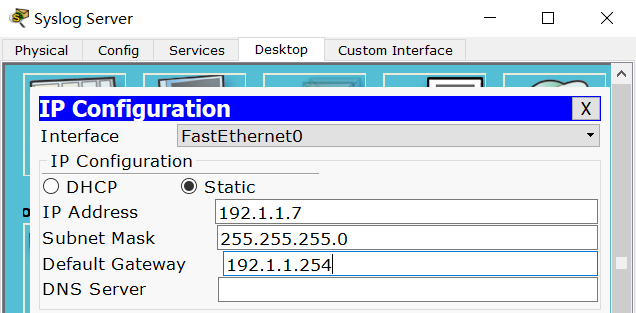


之后对R0、PC0-PC3、Syslog Server进行配置，具体如下图所示：

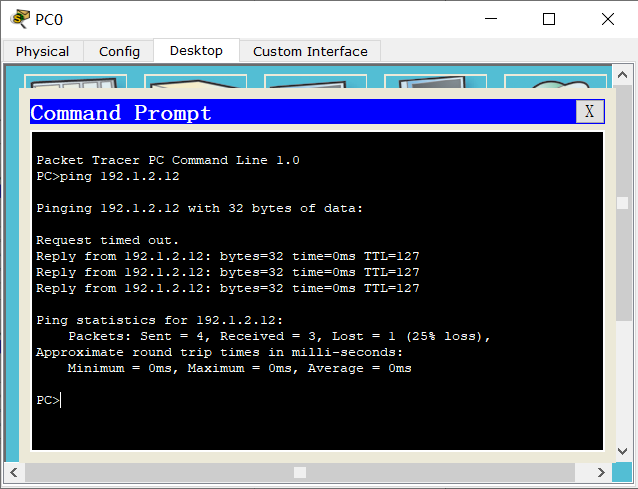


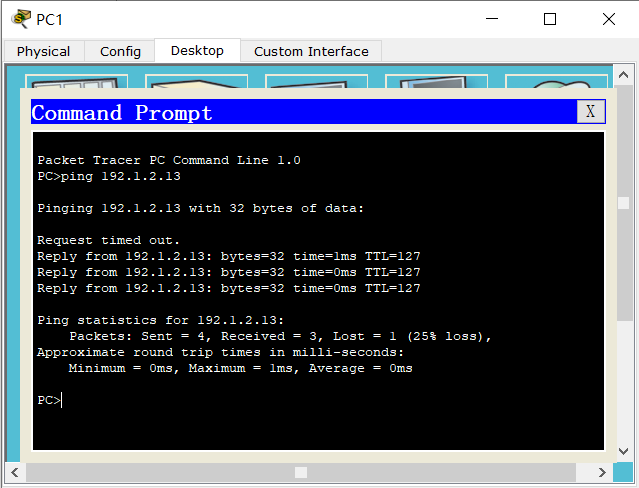


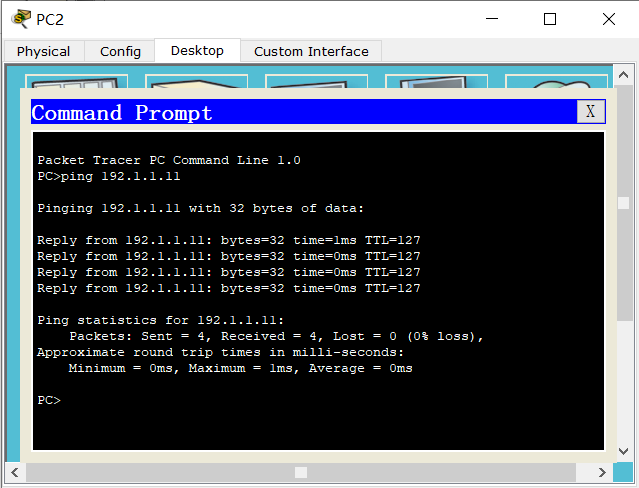




之后验证各个PC终端的连通性，此处我使用了ping指令分别测试了PC0到PC2、PC1到PC3、PC2到PC1的连通性。

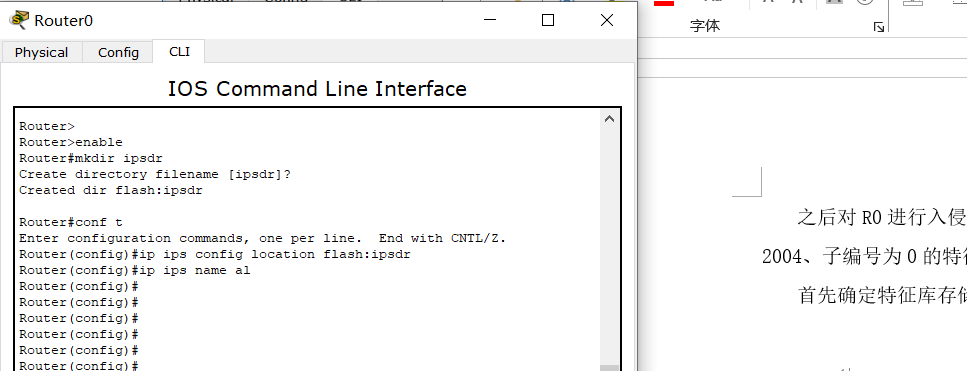




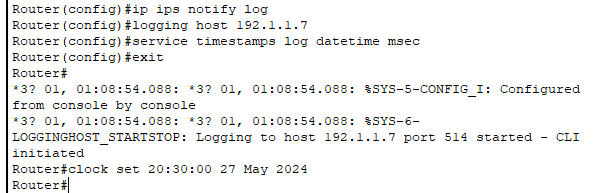


之后对R0进行入侵检测的系统配置，使其E0/0接口输出方向丢弃与编号2004、子编号为0的特征匹配的ICMP ECHO请求报文。

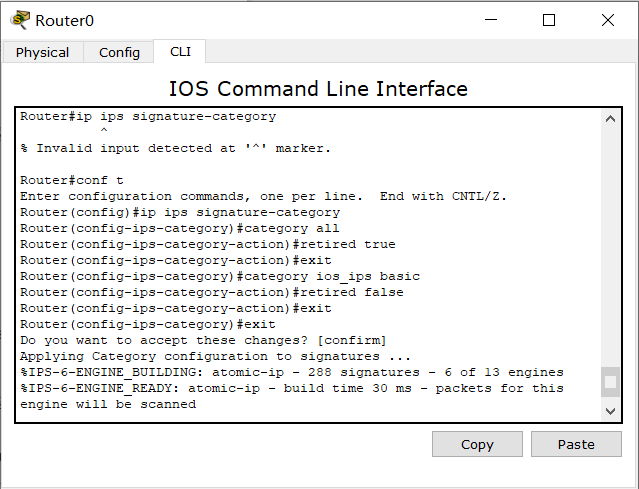
首先确定特征库存储位置并指定入侵检测规则，其中指令即对应全局模式下，指定名字为al的入侵检测规则。



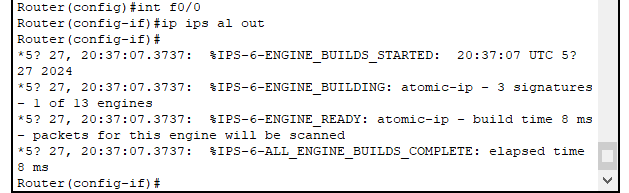
之后开启日志功能，首先将事件记录在日志服务器中作为指定的事件通知方法；之后指定日志服务器的IP地址，由于之前指定的事件通知方法是将事件记录在日志服务器中，因此此处需要指定日志服务器的IP地址；最后指定日志信息中标记的日期和时间，此处我使用当前时间2024.05.27 20:30:00。



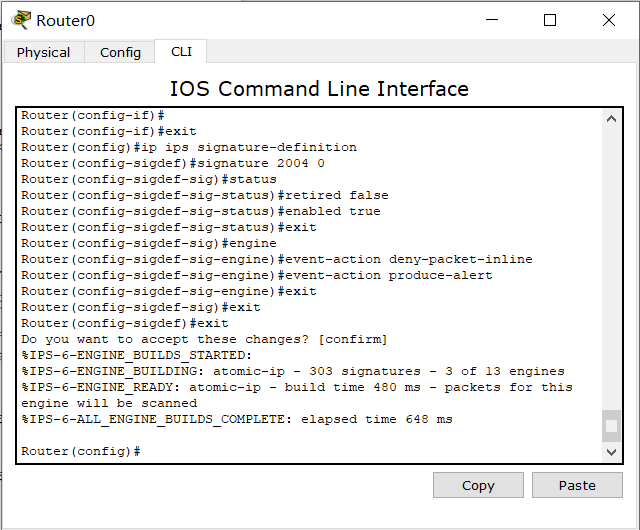
之后配置每一类特征，首先释放所有类别的特征库，之后指定需要加载的特征库类别，此处指定ios\_ips类别中的basic子类别



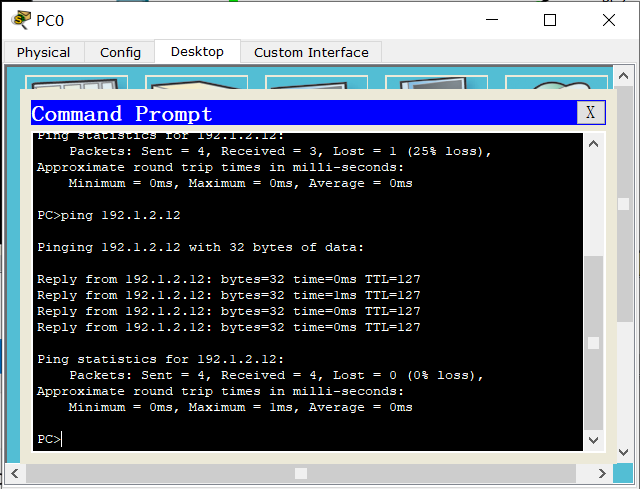
之后需要将规则作用到路由器接口，此处将al规则配置到E0/0的输出方向上。

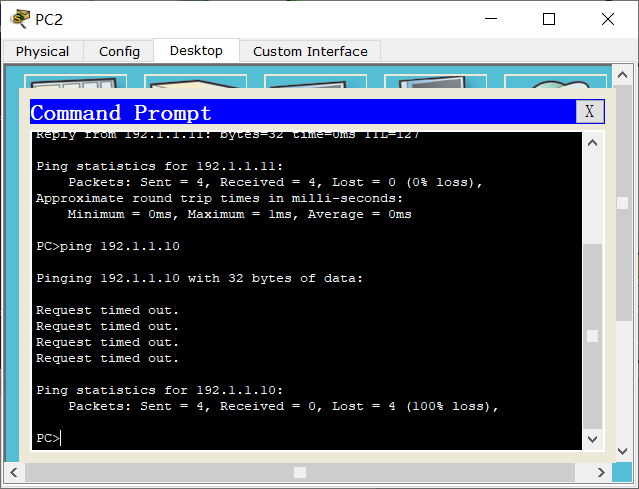


最后还需要重新定义特征。首先重新配置标号为2004、子编号为0的特征状态；之后重新配置发生事件时的动作，即检测到与编号2004、子编号0特征匹配的信息流

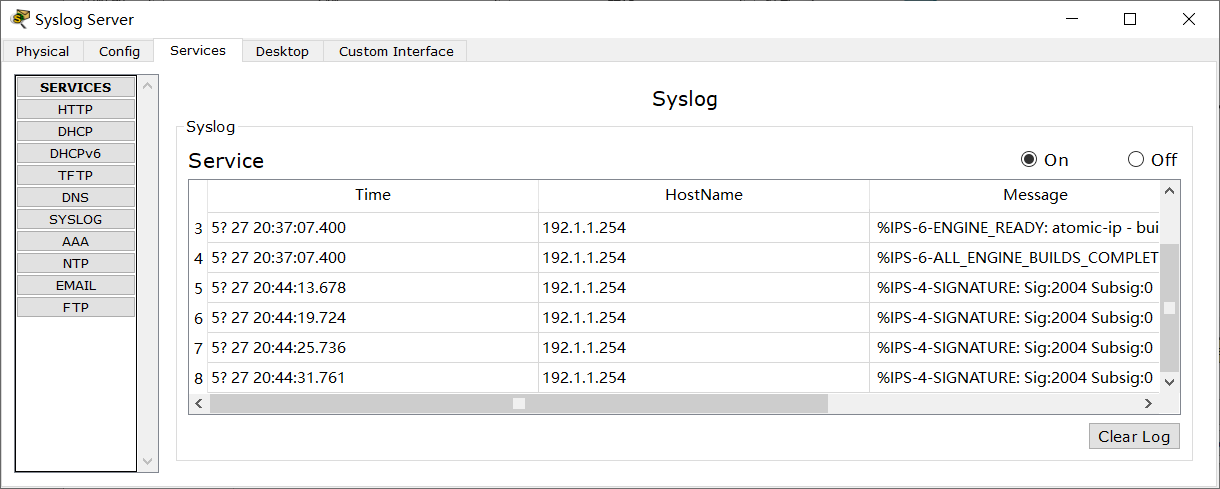


最后验证PC0与PC2之间的连通性。可以发现，PC0可以ping通PC2，但PC2无法ping通PC0





之后查看日志服务器，可以发现日志服务器记录了与编号2004、子编号0特征匹配的信息流



由实验现象可知，入侵检测成功，并成功防御了与编号2004、子编号0特征匹配的out方向的信息流。

## 三、思考与总结

1. 实验过程中你遇到什么问题，如何解决的？通过该实验有何收获？

本次实验按照实验指导进行，一切顺利，现象正常。

通过本次实验，我对入侵检测系统方法有了基本的认识，同时对其配置有了基本的掌握，并通过实验对具体的配置流程、配置命令的理解有所增进。

1. ping是一个双向通信过程，为什么配置入侵检测规则后，PC0可以ping通PC2？

因为在入侵检测规则配置时，将al规则（与编号2004、子编号为0的特征匹配的ICMP ECHO请求报文）配置到了R1端口E0/0的out方向，即单向入侵检测。

在PC0 ping PC2的时候，ICMP ECHO请求报文的方向是 PC0 -> E0/0 -> E0/1 -> PC2，此时ICMP ECHO从E0/0进入，因此报文并不会被丢弃。相反，在PC2 ping PC0的时候，ICMP ECHO请求报文的方向是 PC2 -> E0/1 -> E0/0 -> PC0，因此ICMP报文从E0/0端口输出，报文会被丢弃，因此无法ping通

# 实验2. 入侵检测系统实验二

## 一、实验目的

1. 验证对特定信息流实施入侵检测的过程。
2. 验证指定信息流的入侵检测配置过程。

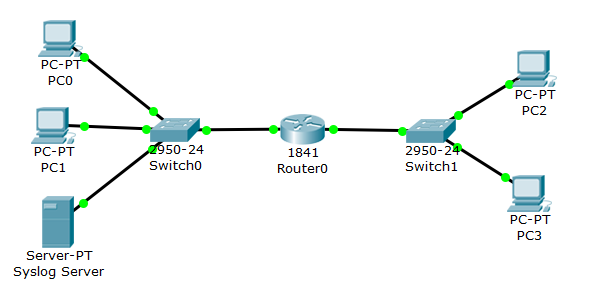
## 二、实验任务

1. 使用自己的语言简述该实验的实验原理。

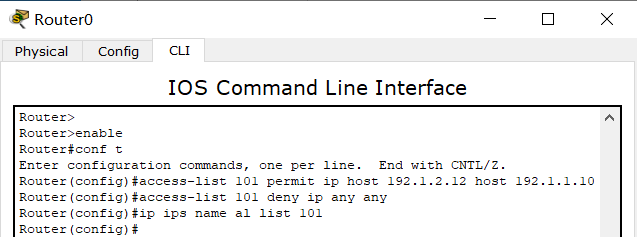
通过使用编号为 扩展分组过滤器来指定某一特定的信息流类别，并将该拓展分组过滤器与入侵检测规则绑定在一起，这意味着入侵检测规则仅适用于编号为 的扩展分组过滤允许的IP数据包。即发现符合编号为 扩展分组过滤器的IP报文，就丢弃该报文，并向日志服务器发送警告信息

1. 实验步骤

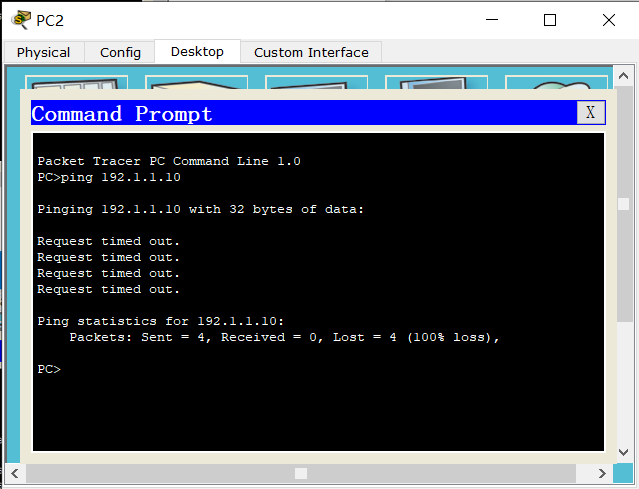
首先给出实验所用的拓扑图，由于该实验在实验一的基础上完成，因此拓扑图相同

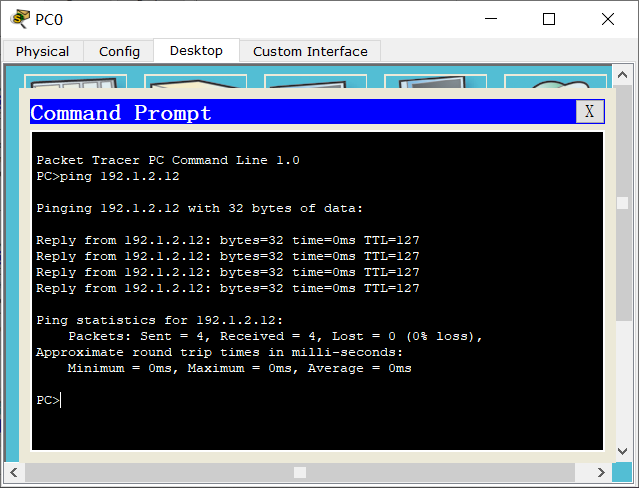


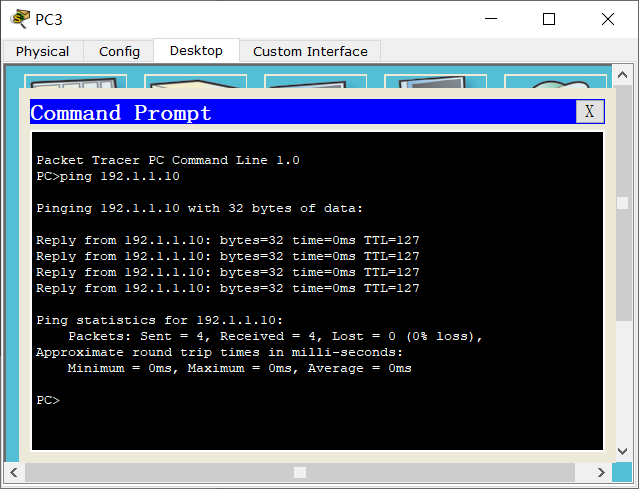
之后继续配置R0，编号为101的扩展分组过滤器允许继续传输源IP为192.1.2.12（即PC2 IP）、目的IP为192.1.1.10（即PC0 IP）的IP分组。之后绑定编号为101的扩展分组过滤器，即只对编号为101的扩展分组过滤器允许继续传输的IP分组实施al入侵检测规则，换句话说，只对PC2发送给PC0的IP分组实施al规则。



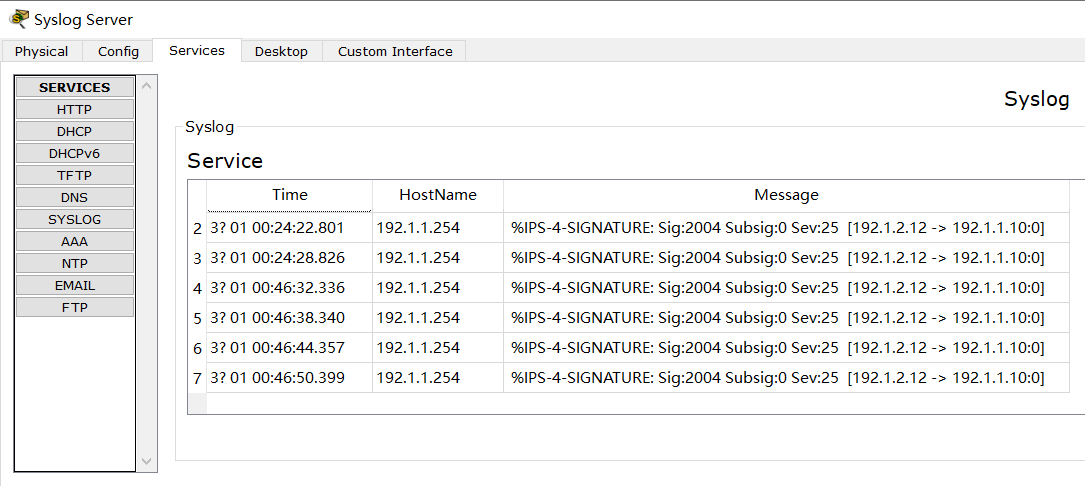
之后测试连通性。可以发现，PC2无法联通PC0，而PC0可以联通PC2，这说明入侵检测规则运作成功，阻止了源IP 192.1.2.12，目的IP 192.1.1.10的IP分组；之后再次测试PC3对PC0的连通性，发现ping通，说明al规则仅阻止了源IP 192.1.2.12，目的IP 192.1.1.10的IP分组，其余分组仍然成功传输，与预期相同







之后查看日志服务器，发现仅有从192.1.2.12 -> 192.1.1.10的事件记录，而PC3到PC0虽然同样通过E0/0的out，但并没有被记录，说明扩展分组过滤器结合入侵检测规则，使规则al仅适用于从192.1.2.12 -> 192.1.1.10的特定信息流了

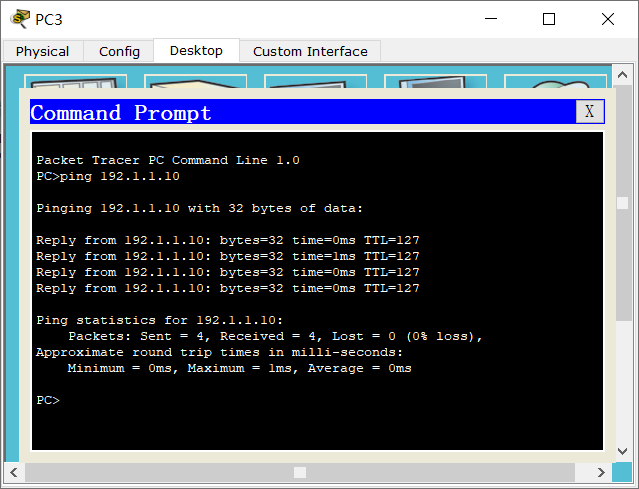
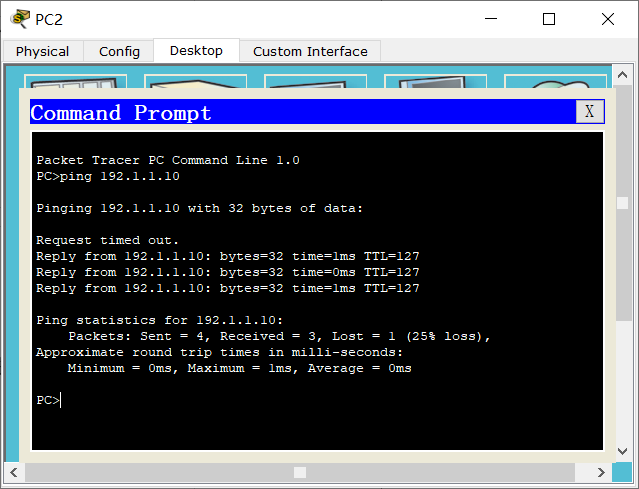


## 三、思考与总结

1. 改变命令access-list 101 permit ip host 192.1.2.12 host 192.1.1.10与access-list 101 deny ip any any的顺序会有什么结果？

由于先配置的命令的优先级更高，因此如果改变命令access-list 101 permit ip host 192.1.2.12 host 192.1.1.10与access-list 101 deny ip any any的顺序，则该扩展分组过滤器相当于只会执行，该扩展分组过滤器并不会指定任何信息流，因此al规则作用不到任何信息流上。

从实验结果而言，此时PC2、PC3都可以ping通PC0，即al规则失效。



1. 实验过程中还遇到什么问题，如何解决的？通过该实验有何收获？

该实验比较简短，所有实验在实验指导下均顺利完成。

通过本次实验，我对入侵检测方式有了更加深刻的认识，同时对扩展分组过滤器绑定入侵检测规则有了基本的掌握，并通过实验对过滤特定数据流的理解有所增进。