

《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： 李泽昊 学号： 20191060065

姓名： 白文强 学号： 20191060064

姓名： 赵浩杰 学号： 20191060074

实验时间： 2021 年 12 月 2 日

实验名称： 基于分区防火墙实验和入侵检测系统实验一

实验成绩：



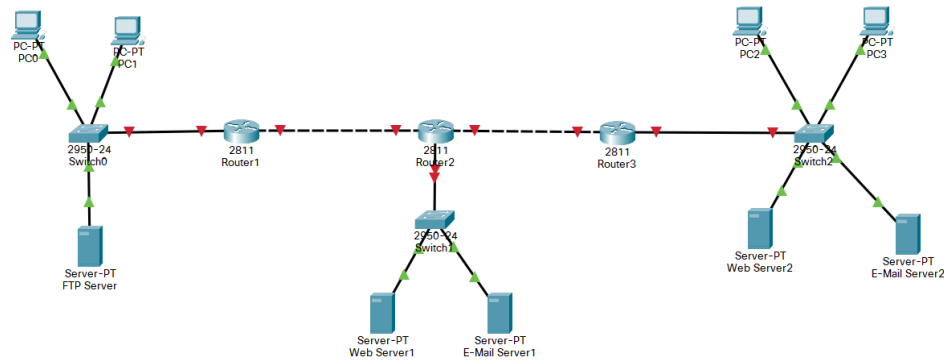
基于分区防火墙实验

一、实验目的

- (1) 深入理解有状态分组过滤器的监测机制。
- (2) 验证对区间数据传输过程实施控制的过程。
- (3) 深入理解通过服务定义区间信息交换过程的原理。
- (4) 掌握基于分区防火墙的配置过程。

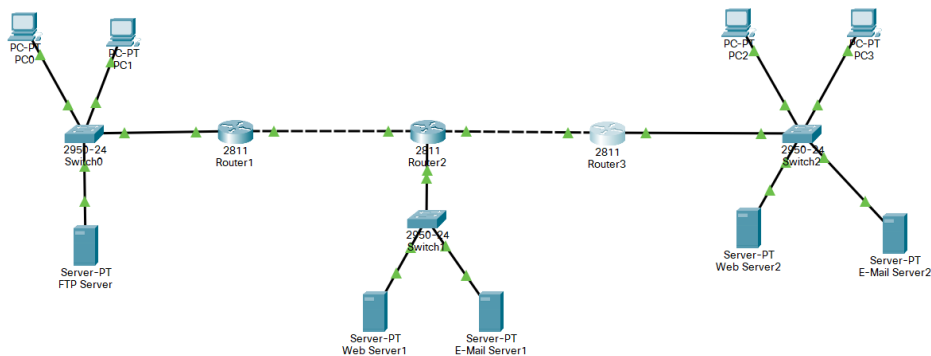
二、实验步骤

- (1) 完成设备放置和连接后的逻辑工作区界面。



- (2) 完成路由器 Router1、Router2 和 Router3 各台接口的 IP 地址和子网掩码配置过程。完成路由器 RIP 协议配置过程。完成上述配置过程后 Router1、Router2 和 Router3 的路由表如图所示。

配置完成后：



Router1 路由表:

```
192.1.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.1.0/24 is directly connected, FastEthernet0/0
L    192.1.1.254/32 is directly connected, FastEthernet0/0
R    192.1.2.0/24 [120/1] via 192.1.4.2, 00:00:21, FastEthernet0/1
R    192.1.3.0/24 [120/2] via 192.1.4.2, 00:00:21, FastEthernet0/1
192.1.4.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.4.0/24 is directly connected, FastEthernet0/1
L    192.1.4.1/32 is directly connected, FastEthernet0/1
R    192.1.5.0/24 [120/1] via 192.1.4.2, 00:00:21, FastEthernet0/1
Router#
```

Router2 路由表:

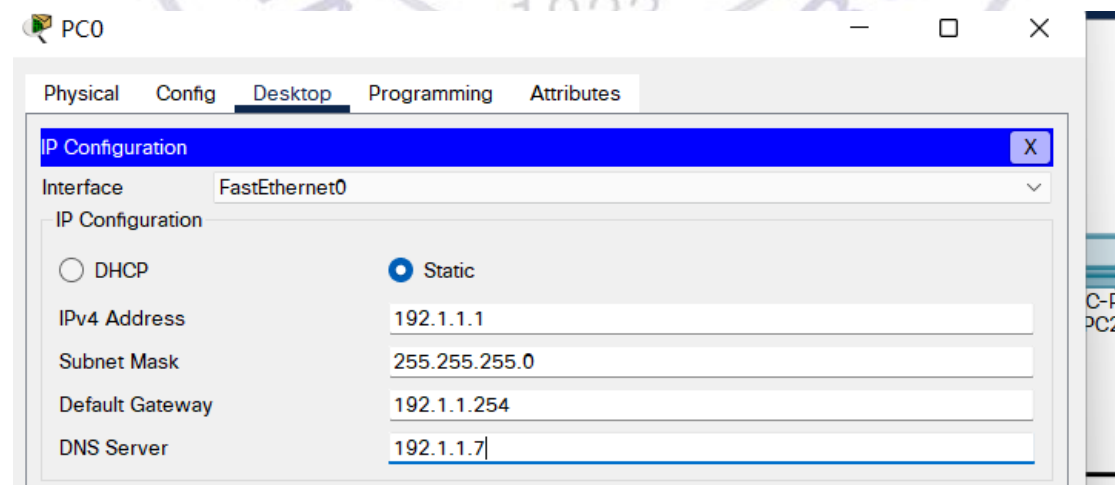
```
R    192.1.1.0/24 [120/1] via 192.1.4.1, 00:00:18, FastEthernet0/0
192.1.2.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.2.0/24 is directly connected, FastEthernet1/0
L    192.1.2.254/32 is directly connected, FastEthernet1/0
R    192.1.3.0/24 [120/1] via 192.1.5.2, 00:00:23, FastEthernet0/1
192.1.4.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.4.0/24 is directly connected, FastEthernet0/0
L    192.1.4.2/32 is directly connected, FastEthernet0/0
192.1.5.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.5.0/24 is directly connected, FastEthernet0/1
L    192.1.5.1/32 is directly connected, FastEthernet0/1
```

Router3 路由表

```
R    192.1.1.0/24 [120/2] via 192.1.5.1, 00:00:02, FastEthernet0/0
R    192.1.2.0/24 [120/1] via 192.1.5.1, 00:00:02, FastEthernet0/0
192.1.3.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.3.0/24 is directly connected, FastEthernet0/1
L    192.1.3.254/32 is directly connected, FastEthernet0/1
R    192.1.4.0/24 [120/1] via 192.1.5.1, 00:00:02, FastEthernet0/0
192.1.5.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.5.0/24 is directly connected, FastEthernet0/0
L    192.1.5.2/32 is directly connected, FastEthernet0/0
```

(3) 完成各个终端和服务器网络信息配置过程。

PC0:



FTP Server:

The screenshot shows the 'FTP Server' configuration window with the 'Services' tab selected. The 'DNS' service is enabled (radio button selected). The 'Resource Records' section shows a table with two entries:

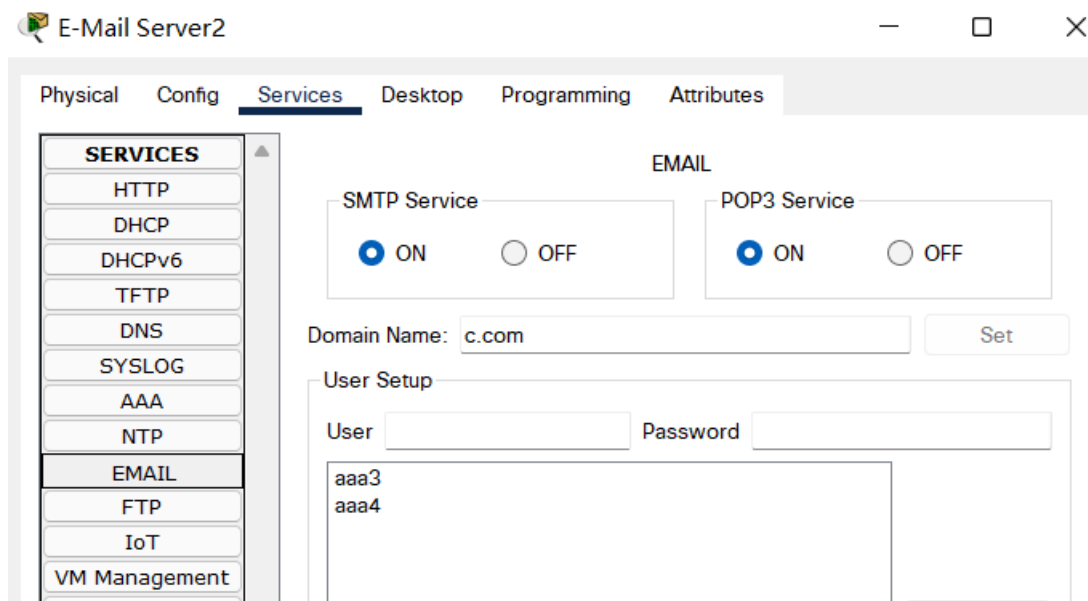
No.	Name	Type	Detail
0	b.com	A Record	192.1.2.3
1	c.com	A Record	192.1.3.3

(4)完成 E-Mail Server1 和 E-Mail Server2 的配置过程。

E-Mail Server1:

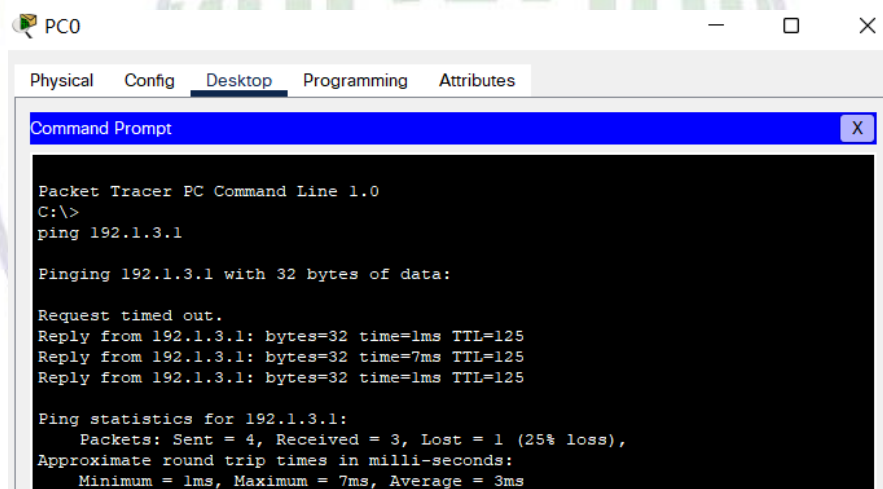
The screenshot shows the 'E-Mail Server1' configuration window with the 'Services' tab selected. The 'EMAIL' section shows both 'SMTP Service' and 'POP3 Service' enabled (radio buttons selected). The 'Domain Name' is set to 'b.com'. The 'User Setup' section shows a list of users: 'aaa1' and 'aaa2'.

E-Mail Server2:

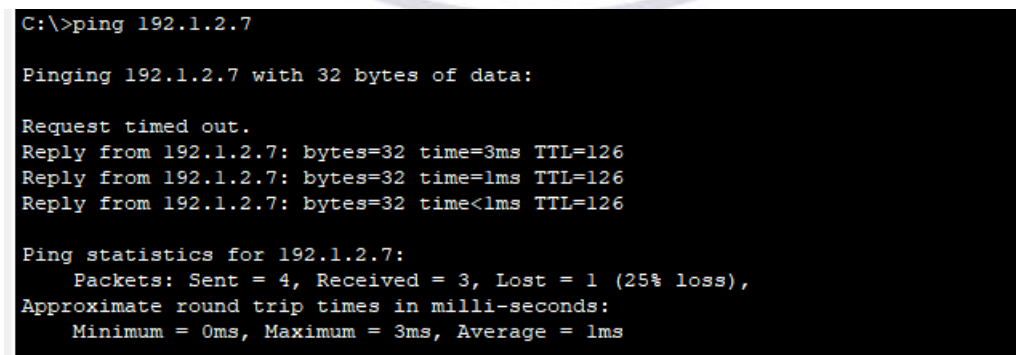


(5)通过 ping 操作，验证位于不同区域的终端和终端之间，终端和服务之间，服务器和服务之间的连通性。

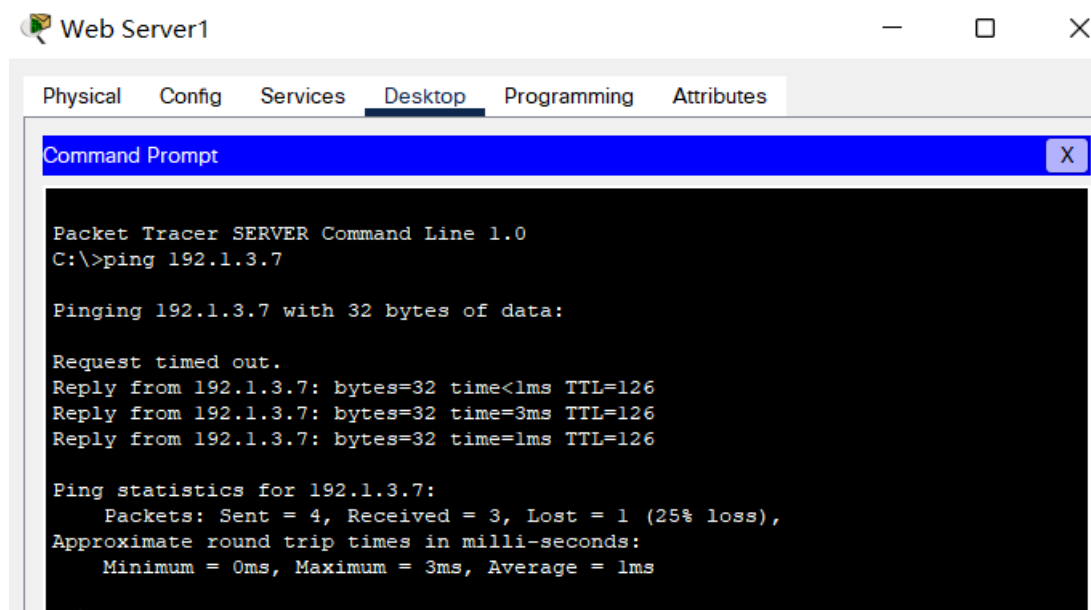
不同终端之间



终端与服务器之间:



服务器与服务器之间：



The screenshot shows a Packet Tracer interface for a device named 'Web Server1'. The 'Desktop' tab is selected, displaying a 'Command Prompt' window. The command prompt shows the execution of a ping command to 192.1.3.7. The output indicates that 3 out of 4 packets were received, resulting in a 25% loss.

```
Packet Tracer SERVER Command Line 1.0
C:\>ping 192.1.3.7

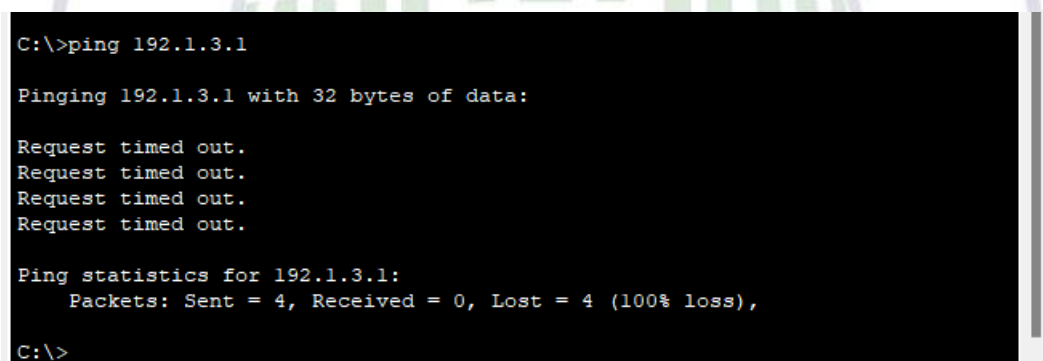
Pinging 192.1.3.7 with 32 bytes of data:

Request timed out.
Reply from 192.1.3.7: bytes=32 time<1ms TTL=126
Reply from 192.1.3.7: bytes=32 time=3ms TTL=126
Reply from 192.1.3.7: bytes=32 time=1ms TTL=126

Ping statistics for 192.1.3.7:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms
```

(6) 在 CLI 命令下配置，完成路由器 Router2 基于区域防火墙的配置过还曾。确定已经实现给定的访问控制策略。

不同终端之间：



The screenshot shows a Command Prompt window with the command 'ping 192.1.3.1'. The output shows four 'Request timed out' messages and a 100% loss of all four packets.

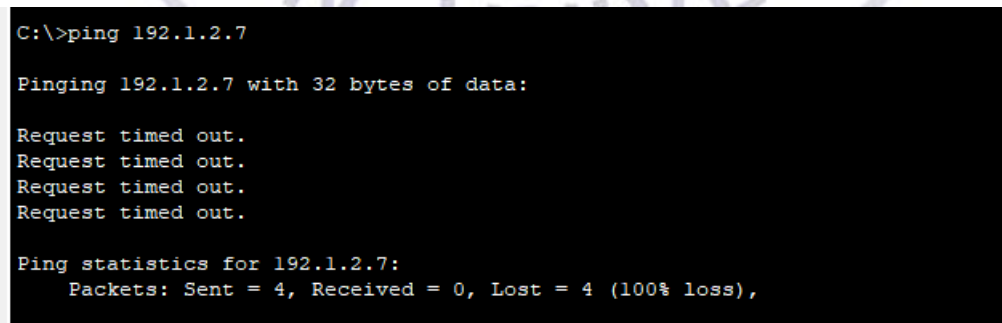
```
C:\>ping 192.1.3.1

Pinging 192.1.3.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.1.3.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

终端与服务器之间：



The screenshot shows a Command Prompt window with the command 'ping 192.1.2.7'. The output shows four 'Request timed out' messages and a 100% loss of all four packets.

```
C:\>ping 192.1.2.7

Pinging 192.1.2.7 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.1.2.7:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

服务器与服务器之间：

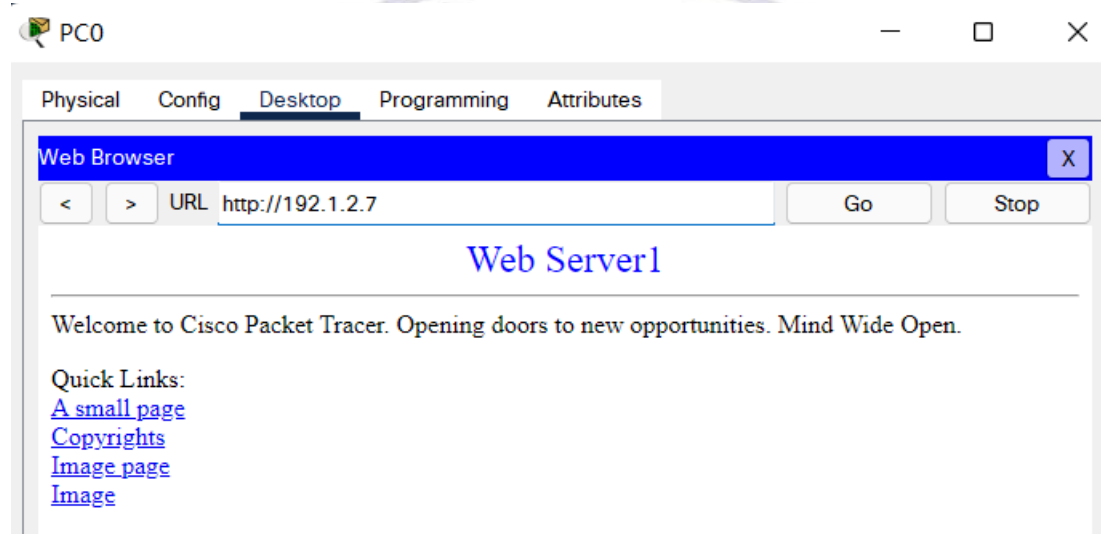
```
C:\>ping 192.1.3.7

Pinging 192.1.3.7 with 32 bytes of data:

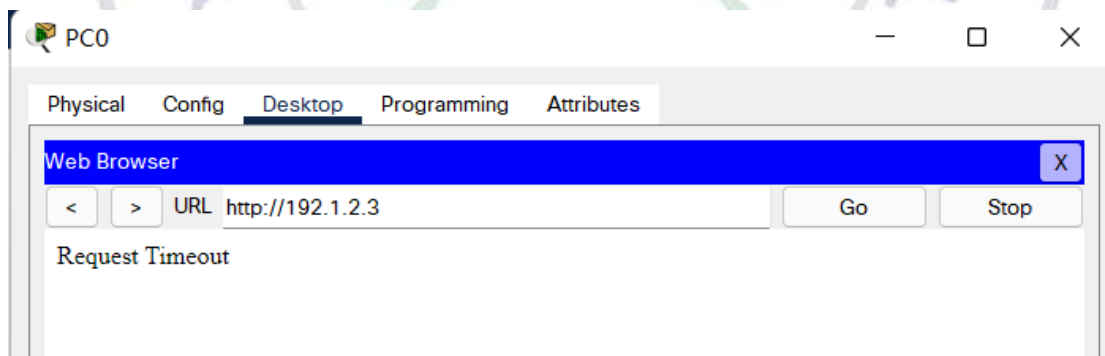
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.1.3.7:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

PC0 用浏览器访问 Web Server1 界面：



PC0 用浏览器访问 E-Mail Server1 界面：



PC0 登录 E-Mail Server1 的界面：

PC0

Physical Config **Desktop** Programming Attributes

Configure Mail X

User Information

Your Name: aaa1

Email Address: aaa1@b.com

Server Information

Incoming Mail Server: b.com

Outgoing Mail Server: b.com

Logon Information

User Name: aaa1

Password: ●●●●

Save Clear Reset

PC2 登录 E-Mail Server2 的界面:

PC2

Physical Config **Desktop** Programming Attributes

Configure Mail X

User Information

Your Name: aaa3

Email Address: aaa3@c.com

Server Information

Incoming Mail Server: c.com

Outgoing Mail Server: c.com

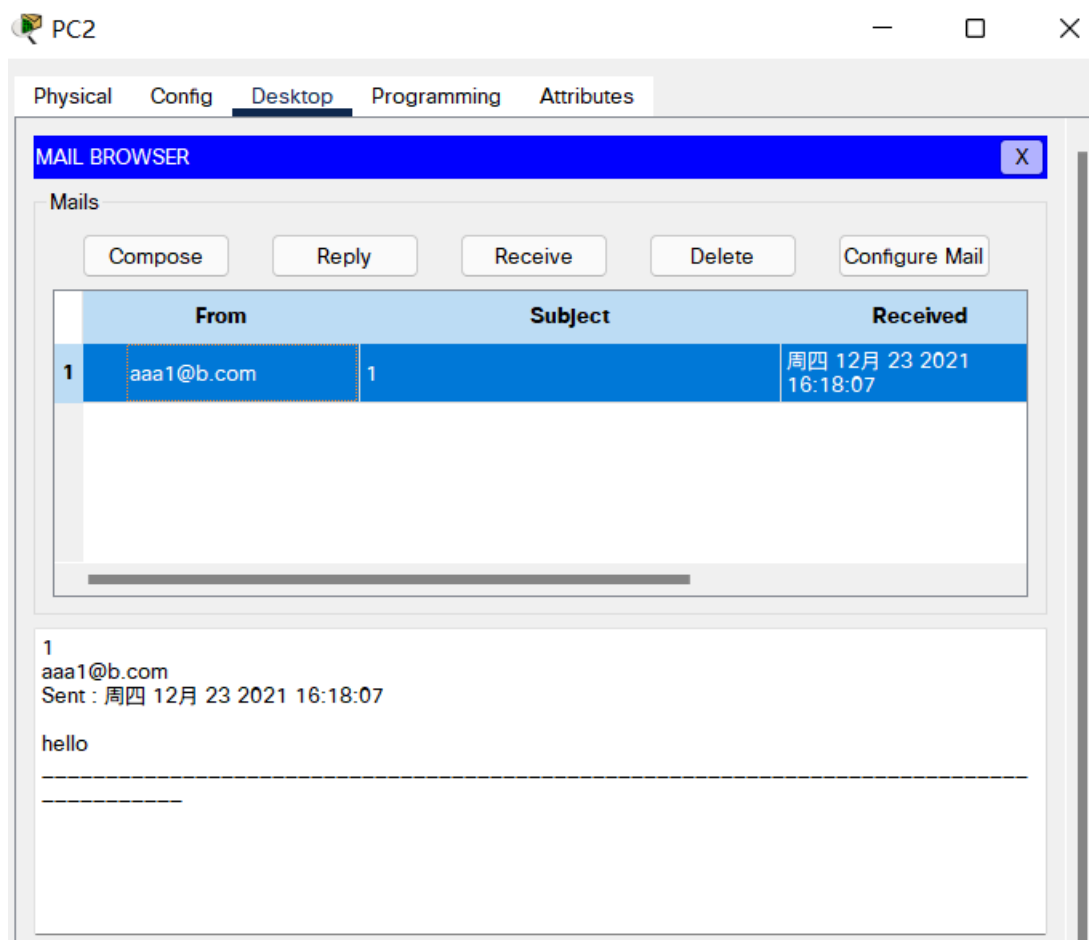
Logon Information

User Name: aaa3

Password: ●●●●

Save Clear Reset

PC0 收到邮件的界面：



三、实验结果及分析

在未加入路由器的情况下连接设备并设置完 IP 地址后，配置 RIP 协议。

随后根据安全策略，在路由器 R2 中实现访问控制策略。

实现了

允许信任区内的终端访问非军事区和非信任区的 Web 服务器。

允许信任区内的终端通过非军事区中的 E-Mail 服务器与非信任区的终端交换邮件。

允许非信任区中的终端访问非军事区中的 Web 服务器。

禁止其他网络之间的通信过程。

四、实验总结及体会

在实验中我们可以发现，当不设置安全策略时，不同区的终端与终端之间，终端与服务器之间，服务器与服务器之间都是可以联通的，当我们设置安

全策略之后，只允许实现我们预先设置好的通信策略，该方法可以实现通信功能的分离，通过分区防火墙实现了不同分区之间不同功能的通信，不同分区之间相同功能限制消息方向不同的通信，适合较为复杂的网络体系。



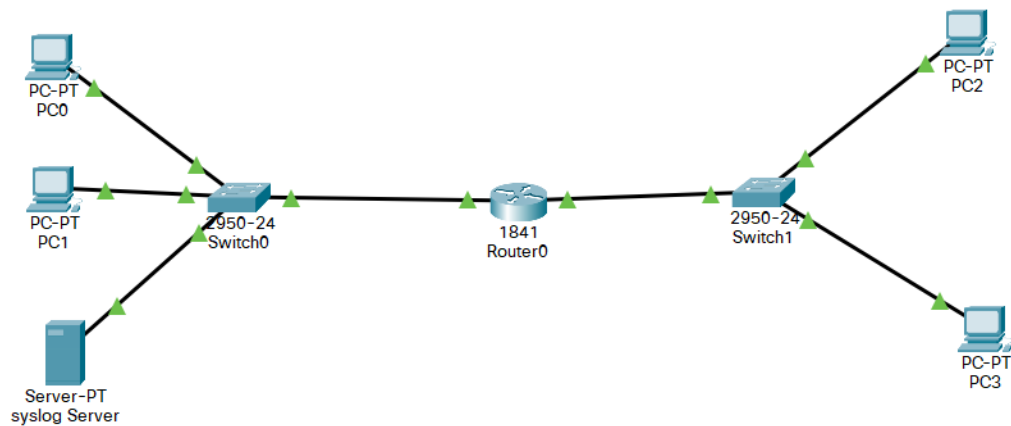
入侵检测系统实验一

一、实验目的

- (1) 验证入侵检测系统配置过程。
- (2) 验证入侵检测系统控制信息流传输过程的机制。
- (3) 验证基于特征库的入侵检测机制的工作过程。
- (4) 验证特征定义过程。

二、实验步骤

(1) 完成互联网结构放置和连接设备，完成路由器接口 IP 地址和子网掩码配置过程，根据路由器接口配置的信息完成各个终端、日志服务器之间的网络信息配置过程，验证终端之间的连通性。



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.1.2.1

Pinging 192.1.2.1 with 32 bytes of data:

Request timed out.
Reply from 192.1.2.1: bytes=32 time<1ms TTL=127
Reply from 192.1.2.1: bytes=32 time<1ms TTL=127
Reply from 192.1.2.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.1.2.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

(2)在 CLI 配置方式下，完成路由器 R 入侵检测系统配置过程。配置的入侵检测规则使路由器 R 接口 F0/0 输出方向丢弃与编号为 2004、子编号为 0 的特征匹配的 ICMP ECHO 请求报文。

```
Router(config)#service timestamps log datetime msec
Router(config)#exit
Router#
*Mar 01, 00:07:56.077: SYS-5-CONFIG_I: Configured from console by console
*Mar 01, 00:07:56.077: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host
192.1.1.7 port 514 started - CLI initiated
Router#clock set 23:54:00 19 November 2016
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip ips signature-category
Router(config-ips-category)#category all
Router(config-ips-category-action)#retired true
Router(config-ips-category-action)#exit
Router(config-ips-category)#category ios_ips basic
Router(config-ips-category-action)#retired basic
^
% Invalid input detected at '^' marker.

Router(config-ips-category-action)#retired false
Router(config-ips-category-action)#exit
Router(config-ips-category)#exit
Do you want to accept these changes? [confirm]
Applying Category configuration to signatures ...
%IPS-6-ENGINE_BUILDING: atomic-ip - 288 signatures - 6 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 30 ms - packets for this engine
will be scanned

Router(config)#int f0/0
Router(config-if)#ip ips al out
Router(config-if)#
*Nov 19, 23:55:17.5555: %IPS-6-ENGINE_BUILDS_STARTED: 23:55:17 UTC 11月 19
2016
*Nov 19, 23:55:17.5555: %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1
of 13 engines
*Nov 19, 23:55:17.5555: %IPS-6-ENGINE_READY: atomic-ip - build time 8 ms -
packets for this engine will be scanned
*Nov 19, 23:55:17.5555: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 ms
Router(config-if)#exit
Router(config)#ip ips signature-definition
Router(config-sigdef)#signature 2004 0
Router(config-sigdef-sig)#status
Router(config-sigdef-sig-status)#retired false
Router(config-sigdef-sig-status)#enabled true
Router(config-sigdef-sig-status)#exit
Router(config-sigdef-sig)#engine
Router(config-sigdef-sig-engine)#event-action deny-packet-inline
Router(config-sigdef-sig-engine)#event-action produce-alert
Router(config-sigdef-sig-engine)#exit
Router(config-sigdef-sig)#exit
Router(config-sigdef)#exit
Do you want to accept these changes? [confirm]
%IPS-6-ENGINE_BUILDS_STARTED:
%IPS-6-ENGINE_BUILDING: atomic-ip - 303 signatures - 3 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 480 ms - packets for this engine
will be scanned
%IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 648 ms

Router(config)#
```

(3)验证 PC2 不能 ping 通 PC0，但 PC0 可以 ping 通 PC2.进行 PC2pingPC0 的操作后，日志服务器将记录该事件。

PC0 ping PC2:

```
C:\>ping 192.1.2.1

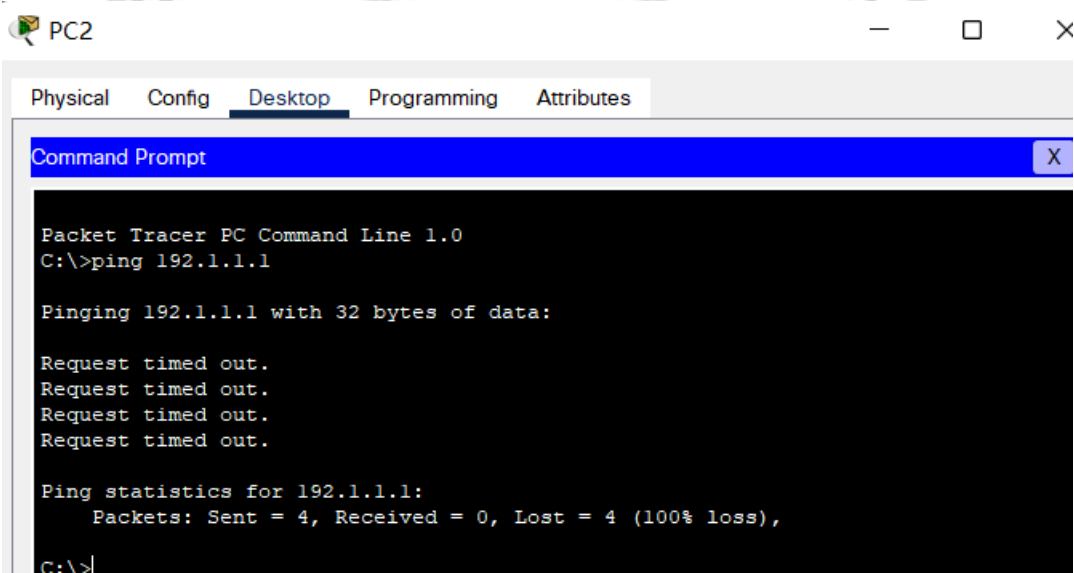
Pinging 192.1.2.1 with 32 bytes of data:

Reply from 192.1.2.1: bytes=32 time<1ms TTL=127
Reply from 192.1.2.1: bytes=32 time<1ms TTL=127
Reply from 192.1.2.1: bytes=32 time<1ms TTL=127
Reply from 192.1.2.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.1.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

PC2ping PC0:



Syslog Server:

	AAA		
	NTP		
	EMAIL		
	FTP		
	IoT		
	VM Management		
	Radius EAP		
2	11.19.2016 11:55:17.578 PM	192.1.1.254	%IPS-6-...
3	11.19.2016 11:55:17.578 PM	192.1.1.254	%IPS-6-...
4	11.19.2016 11:55:17.578 PM	192.1.1.254	%IPS-6-...
5	11.19.2016 11:59:11.710 PM	192.1.1.254	%IPS-4-SIGNATUR...
6	11.19.2016 11:59:17.715 PM	192.1.1.254	%IPS-4-SIGNATUR...
7	11.19.2016 11:59:23.741 PM	192.1.1.254	%IPS-4-SIGNATUR...
8	11.19.2016 11:59:29.744 PM	192.1.1.254	%IPS-4-SIGNATUR...

三、实验结果及分析

在建设好入侵检测系统后，当 PC2 ping PC0 时，系统检测到了 ICMP ECHO 请求报文，丢弃该请求报文，并向日志服务器发送了警告信息，但是 PC0 发往 PC2 的信息还是畅通，因为没有将其加入到特征库中，因此该信息不会匹配，也就不会被丢弃。

四、实验总结及体会

本次实验是关于入侵检测系统的内容，其采用了基于特征的入侵检测机制，首先通过加载特征库，当每个信息经路由器时，都需要与特征库进行比对，若匹配成功，则检测为入侵信息，否则不然。

特征库中与每一种入侵行为相关的信息有两部分：一是标识入侵行为的信息流特征；二是对具有入侵行为特征信息流采取动作。

