实验五 防火墙透明模式

一．实验目的

1. 掌握理解PIX防火墙透明模式配置命令。

2. 完成透明模式转换。

二．实验要点

1．掌握PIX防火墙的firewall transparent配置命令。

2．通过ICMP协议来测试连通性。

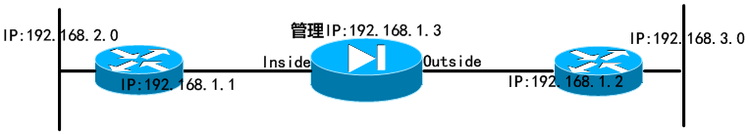
三．实验设备

1. GNS3工具，路由器Cisco 3600二台 2

. Cisco PIX804 一台，Real PC  一台

四、实验环境

拓扑



要求：

将防火墙设置为第二层透明模式，在192.168.2.0和192.168.3.0之间使用防火墙增强安全性，但必须使得两端路由器能通过OSPF协议学习到对端的路由。且192.168.2.0和192.168.3.0之间可以通过ICMP协议来测试连通性。

**透明模式：**

透明模式，顾名思义，首要的特点就是对用户是透明的(Transparent)，即用户意识不到防火墙的存在。要想实现透明模式，防火墙必须在没有 IP地址的情况下工作，不需要对其设置IP地址，用户也不知道防火墙的IP地址。

防火墙作为一实际存在的物理设备，其本身也起到路由的作用，所以在为用户安装防火墙时，就需要考虑如何改动其原有的网络拓扑结构或修改连接防火墙的路由表，以适应用户的实际需要，这样就增加了工作的复杂程度和难度。但如果防火墙采用了透明模式，即采用无IP方式运行，用户将不必重新设定和修改路由，防火墙就可以直接安装和放置到网络中使用，如交换机一样不需要设置IP地址！

透明模式的防火墙就好像是一台网桥(非透明的防火墙好像一台路由器)，网络设备(包括主机、路由器、工作站等)和所有计算机的设置(包括IP地址和网关)无须改变，同时解析所有通过它的数据包，既增加了网络的安全性，又降低了用户管理的复杂程度。

五、实验步骤

GNS3中的拓扑结构如下图

图示

描述已自动生成

192.168.3.1/24

192.168.1.2/24

管理IP192.168.1.3/24

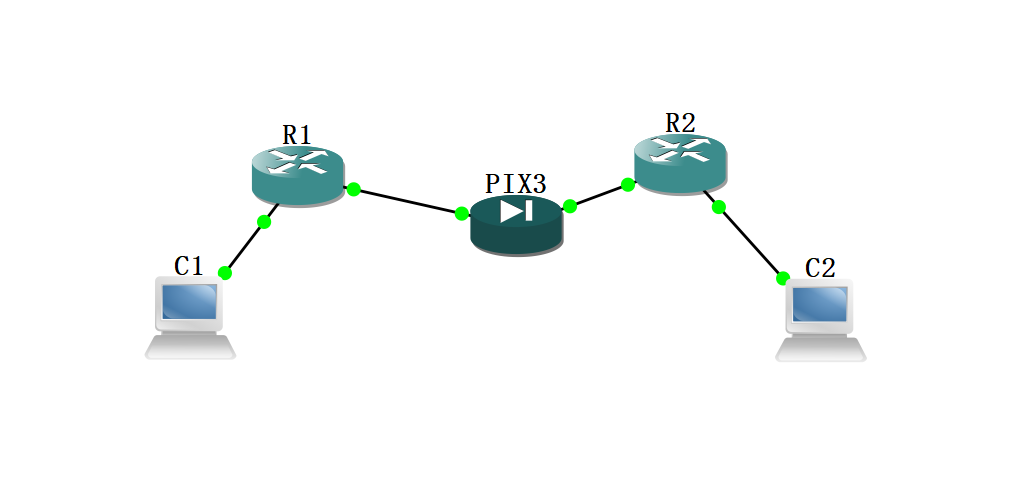
192.168.3.2/24

192.168.2.2/24

192.168.2.1/24

192.168.1.1/24

GNS3拓扑图



**R1配置**

R1#conf t

R1(config)#int e0/0

R1(config-if)#ip add 192.168.1.1 255.255.255.0

R1(config-if)#no shut

R1(config-if)#exit

R1(config)#int e0/1

R1(config-if)#ip add 192.168.2.1 255.255.255.0

R1(config-if)#no shut

R1(config-if)#exit

R1(config)#router ospf 1

R1(config-router)#net 192.168.1.0 0.0.0.255 area 0

R1(config-router)#net 192.168.2.0 0.0.0.255 area 0

**R2配置**

R2#conf t

R2(config)#int e0/0

R2(config-if)#ip add 192.168.1.2 255.255.255.0

R2(config-if)#no shut

R2(config-if)#exit

R2(config)#int e0/1

R2(config-if)#ip add 192.168.3.1 255.255.255.0

R2(config-if)#no shut

R2(config-if)#exit

R2(config)#router ospf 1

R2(config-router)#net 192.168.1.0 0.0.0.255 area 0

R2(config-router)#net 192.168.3.0 0.0.0.255 area 0

**防火墙配置**

pixfirewall> en

Password:

pixfirewall# conf t

pixfirewall(config)# firewall transparent/配置透明模式

pixfirewall(config)# int e0

pixfirewall(config-if)# nameif outside

INFO: Security level for "outside" set to 0 by default.

pixfirewall(config-if)# no shut

pixfirewall(config-if)# exit

pixfirewall(config)# int e1

pixfirewall(config-if)# nameif inside

INFO: Security level for "inside" set to 100 by default.

pixfirewall(config-if)# no shut

pixfirewall(config-if)# exit

pixfirewall(config)# ip address 192.168.1.3 255.255.255.0/配置管理IP

pixfirewall(config)# access-list k1 extended permit ospf any any

pixfirewall(config)# access-list k1 extended permit icmp any any

pixfirewall(config)# access-group k1 in interface inside/配置访问列表在inside接口上放行k1指定的流量

pixfirewall(config)# access-group k1 in interface outside/配置访问列表在outside接口上放行k1指定的流量

**验证结果:C1,C2互ping，均可ping通**

