1. 实验项目名称：

防火墙实验（iptables规则应用）

1. 实验原理：

iptables 是与Linux内核集成的IP信息包过滤系统。如果Linux系统连接到因特网或LAN、服务器或连接LAN和因特网的代理服务器，则该系统有利于在Linux系统上更好地控制IP信息包过滤和防火墙配置。

防火墙在做信息包过滤决定时，有一套遵循和组成的规则，这些规则存储在专用的信息包过滤表中，而这些表集成在Linux内核中。在信息包过滤表中，规则被分组放在我们所谓的链（chain）中。而netfilter/iptables IP信息包过滤系统是一款功能强大的工具，可用于添加、编辑和移除规则。

1. 实验目的：

通过配置iptables防火墙禁止内外网和按网段访问服务器的一些应用，如ftp、telnet、ping测试等等。分别手动和通过脚本自动配置一个简单的企业防火墙。通过iptables命令配置nat表实现外部IP端口映射到服务器。掌握iptables日志功能的使用。了解防火墙的维护方法和iptables内核优化的相关知识。

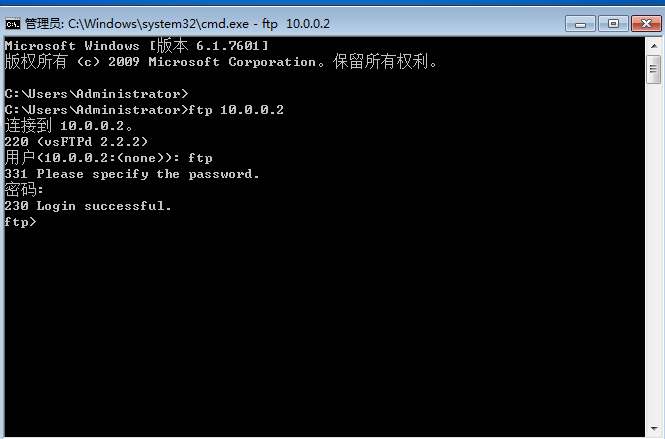
1. 实验器材（设备、虚拟机名称）：

Windows 7, widows server 2003, centos 6.5, centos 6.5.

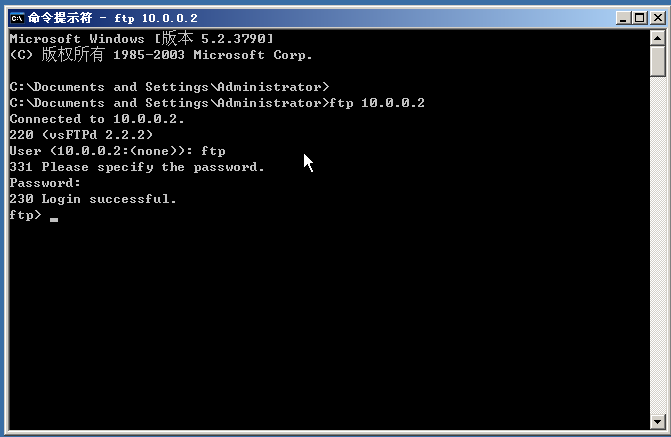
1. 实验步骤：

1.配置iptables禁止访问ftp服务。

1.1 打开windows 7的cmd，输入ftp 10.0.0.2，输入用户名ftp，密码123456，登录成功。



1.2 打开windows sever 2003的cmd，输入ftp 10.0.0.2，输入用户名ftp，密码123456，登录成功。



1.3 配置iptables防火墙，禁止外网访问ftp服务。在名为spc\_iptables\_gwl6的虚拟机centos 6.5 的终端输入如下命令，清空防火墙规则，如下图所示.

iptables -F

iptables -X

iptables -Z

iptables -L -n --line-numbers



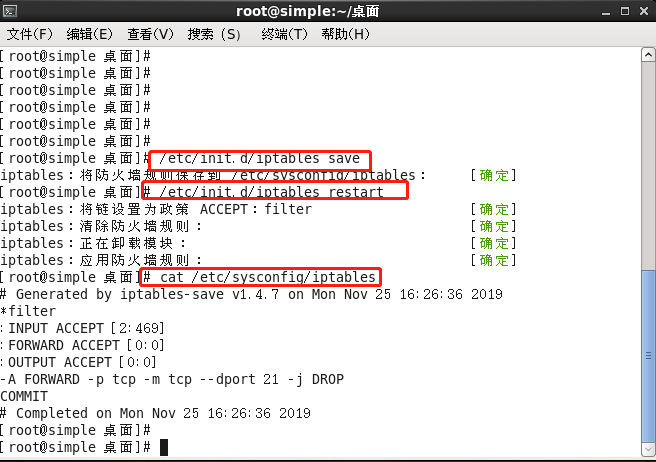
1.4 配置防火墙，禁止内外网访问ftp服务，在终端输入如下命令，在转发的数据包中，如果目标端口为21，则将该数据包丢弃。

iptables -t filter -A FORWARD -p tcp --dport 21 -j DROP

iptables -L -n --line-numbers

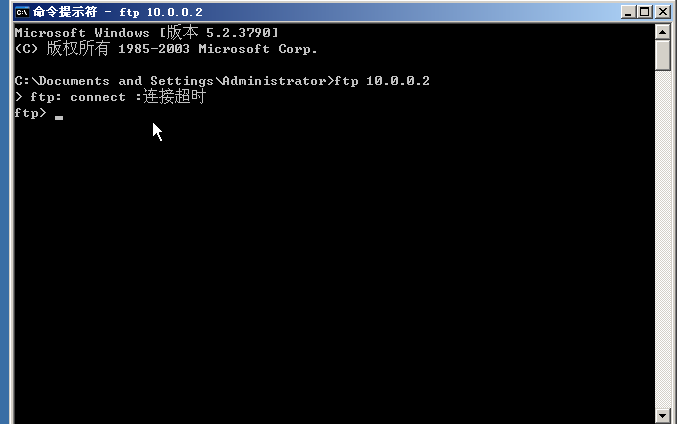


1.5 在终端下输入如下命令，将添加的规则保存到iptables配置文件中，重启防火墙，查看防火墙规则，如下图所示。



1.6 此时在Windows 7和Windows server 2003的cmd，已经不能访问ftp 10.0.0.2了。

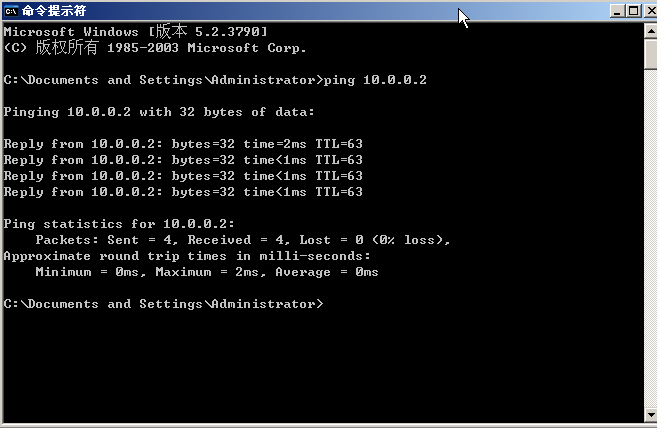




2.配置iptables禁止访问ping测试。

2.1 打开Windows 7和Windows sever 2003的cmd，输入ping 10.0.0.2，可以ping通。





2.2 在名为spc\_iptables\_gwl6的虚拟机centos 6.5终端中清除防火墙规则

iptables -F

iptables -X

iptables -Z

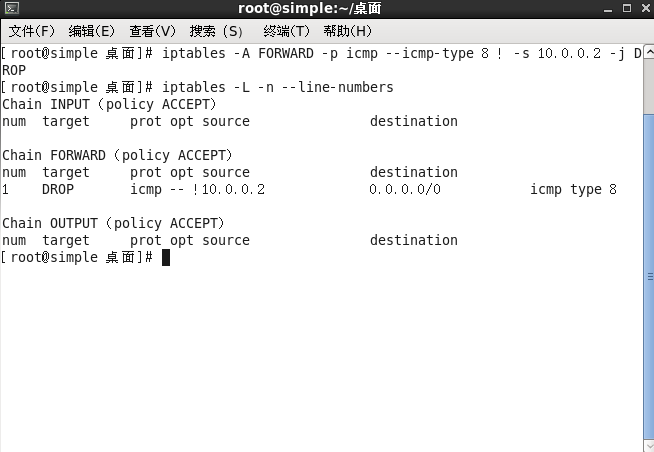
iptables -L -n --line-numbers



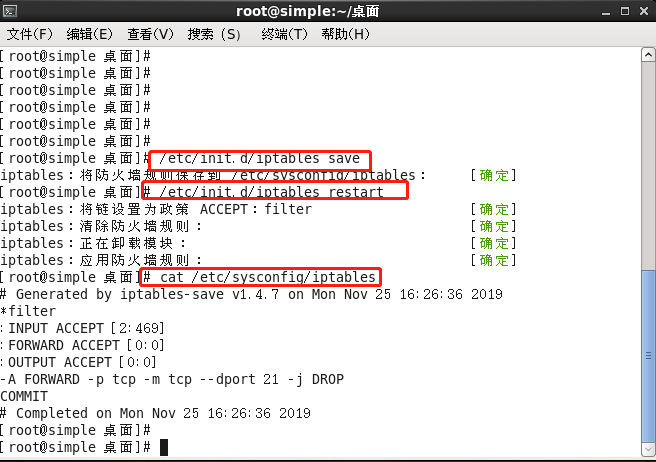
2.3 配置防火墙，禁止访问icmp服务，输入如下命令，

iptables -A FORWARD –p icmp --icmp-type 8 ! -s 10.0.0.2 -j DROP

iptables -L -n --line-numbers

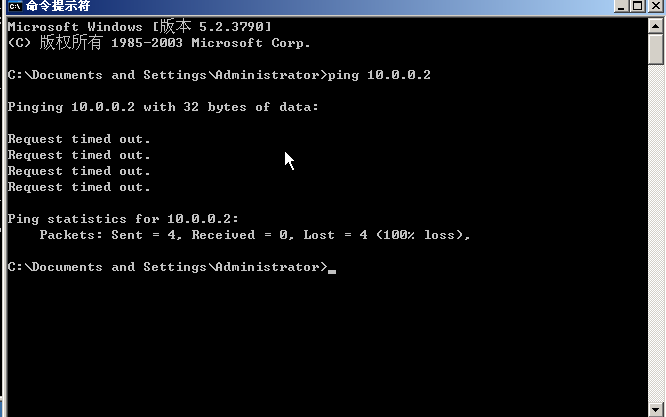


2.4 在终端下输入如下命令，将添加的规则保存到iptables配置文件中，重启防火墙，查看防火墙规则，如下图所示。



2.5 此时在Windows 7和Windows server 2003的cmd，已经不能ping通ftp 10.0.0.2了





2.6 此时10.0.0.2主机还可以ping通192.168.1.2和20.0.0.2



1. 实验结果及分析：
2. 总结及心得体会：