

# 防火墙实验 实验报告



实验名称 防火墙实验

班 级 信安 20-2

姓 名 李天昊

学 号 20101110201

指导教师 徐 刚

2020 年 12 月 19 日

# 实验一 防火墙实验

## 一、实验目的

通过本实验进一步加深理解防火墙的基本工作原理和基本概念，更好的掌握 防火墙的下载安装设置和使用，以及对防火墙的进一步认识。

1. 通过实验深入理解防火墙的功能和工作原理；
2. 熟悉任意一款（天网）防火墙个人版的配置和使用。

## 二、实验环境

DEVICE NAME : V-WinXP

PROCESSOR : (inter VT)Intel(R) Core(TM) i7-8650U CPU @ 1.90GHz 2.11 GHz

SYSTEM TYPE : 32-bit operating system,x64-based processor

SYSTEM EDITION : Windows XP Professional SP3

VERSION : /

OS BUILD : 5.1.2600 Service Pack 3 Build 2600

## 三、实验要求

通过本实验进一步加深理解防火墙的基本工作原理和基本概念，更好的掌握 防火墙的下载安装设置和使用，以及对防火墙的进一步认识。

1. 通过实验深入理解防火墙的功能和工作原理；
2. 熟悉任意一款（天网）防火墙个人版的配置和使用。

## 四、实验步骤和结果

### 1. 了解防火墙的概念

防火墙是一种通过基于一组用户定义的规则过滤传入和传出网络流量来提供网络安全性的系统。通常，防火墙的目的是减少或消除不需要的网络通信的发生，同时允许所有合法通信自由流动。在大多数服务器基础架构中，防火墙提供了一个重要的安全层，与其他措施相结合，可以防止攻击者以恶意方式访问您的服务器。

### 2. 学习防火墙的工作原理

防火墙能增强机构内部网络的安全性。防火墙系统决定了哪些内部服务可以被外界访问；外界的哪些人可以访问内部的服务以及哪些外部服务可以被内部人员访问。防火墙必须只允许授权的数据通过，而且防火墙本身也必须能够免于渗透。

### 3. 对比两种不同的防火墙技术

(1) 包过滤防火墙：将防火墙放置于内外网络的边界；价格较低，性能开销小，处理速度较快；定义复杂，容易出现因配置不当带来问题，允许数据包直接通过，容易造成数据驱动式攻击的潜在危险。

(2) 应用级网关：内置了专门为了提高安全性而编制的 Proxy 应用程序，能够透彻地理解相关服务的命令，对来往的数据包进行安全化处理，速度较慢，不太适用于高速网（ATM 或千兆位以太网等）之间的应用。

### 4. 认识防火墙体系结构

(1) 屏蔽主机防火墙体系结构：在该结构中，分组过滤路由器或防火墙与 Internet 相连，同时一个堡垒机安装在内部网络，通过在分组过滤路由器或防火墙上过滤规则的设置，使堡垒机成为 Internet 上其它节点所能到达的唯一节点，这确保了内部网络不受未经授权外部用户的攻击。

(2) 双重宿主主机体系结构：围绕双重宿主主机构筑。双重宿主主机至少有两个网络接口。这样的主机可以充当与这些接口相连的网络之间的路由器；它能够从一个网络到另外一个网络发送 IP 数据包。但是外部网络与内部网络不能直接通信，它们之间的通信必须经过双重宿主主机的过滤和控制。

(3) 被屏蔽子网体系结构：添加额外的安全层到被屏蔽主机体系结构，即通过添加周边网络更进一步的把内部网络和外部网络（通常是 Internet）隔离开。被屏蔽子网体系结构的最简单的形式为，两个屏蔽路由器，每一个都连接到周边网。一个位于周边网与内部网络之间，另一个位于周边网与外部网络（通常为 Internet）之间。

### 5. 天网防火墙工作原理

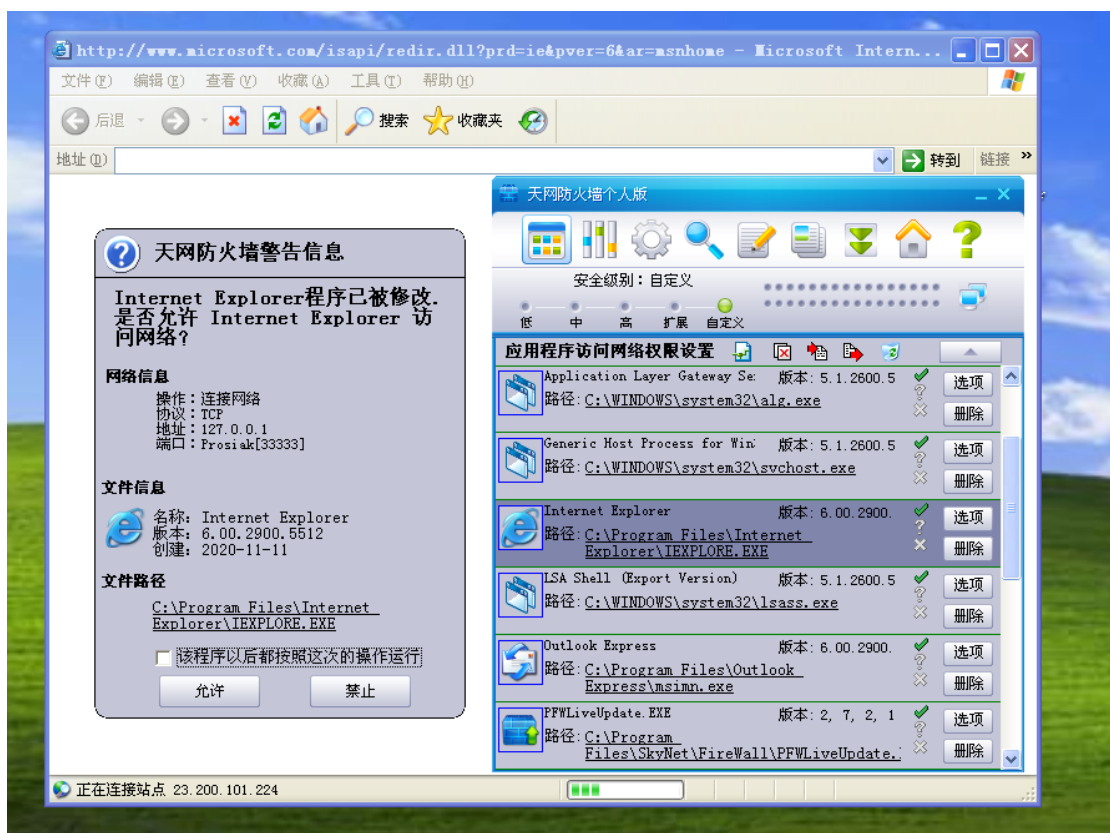
在于监视并过滤网络上流入流出的 IP 包，拒绝发送可疑的包。基于协议特定的标准，路由器在其端口能够区分包和限制包的能力叫包过滤。由于 Internet 与 Intranet 的连接多数都要使用路由器，所以 Router 成为内外通信的必经端口，Router 的厂商在 Router 上加入 IP 过滤功能，过滤路由器也可以称作包过滤路由器或筛选路由器。防火墙常常就是这样一个具备包过滤功能的简单路由器，这种 Firewall 应该是足够安全的，但前提是配置合理。然而一个包过滤规则是否完全严密及必要是很难判定的，因而在安全要求较高的场合，通常还配合使用其它的技术来加强安全性。路由器逐一审查数据包以判定它是否与其它包过滤规则相匹配。每个包有两个部分：数据部分和包头。过滤规则以用于 IP 顺行处理的包头信息为基础，不理睬包内的正文信息内容。包头信息包括：IP 源地址、IP 目的地址、封装协议（TCP、UDP、或 IP Tunnel）、TCP/UDP 源端口、ICMP 包类型、包输入接口和包输出接口。如果找到一个匹配，且规则允许这包，这一包则根据路由表中的信息前行。如果找到一个匹配，且规则拒绝此包，这一包则被舍弃。如果无匹配规则，一个用户配置的缺省参数将决定此包是前行还是被舍弃。

## 6. 下载并安装天网防火墙个人版(trial)



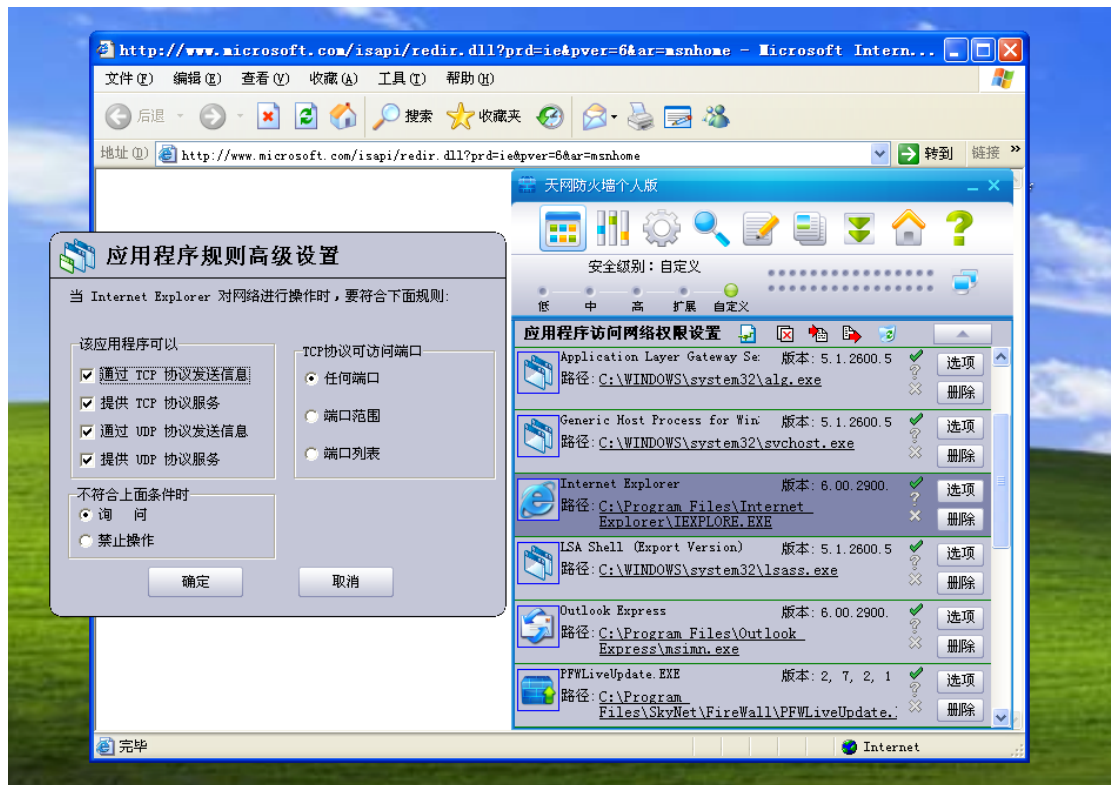
## 7. 启动天网防火墙，拦截一些应用程序的网络连接请求

如下图，当尝试启动 Microsoft Internet Explore 时，天网防火墙弹出警告信息，包括网络信息、文件信息、文件路径。因为该浏览器为系统自带并且由用户主动启动，风险较低，故允许运行。



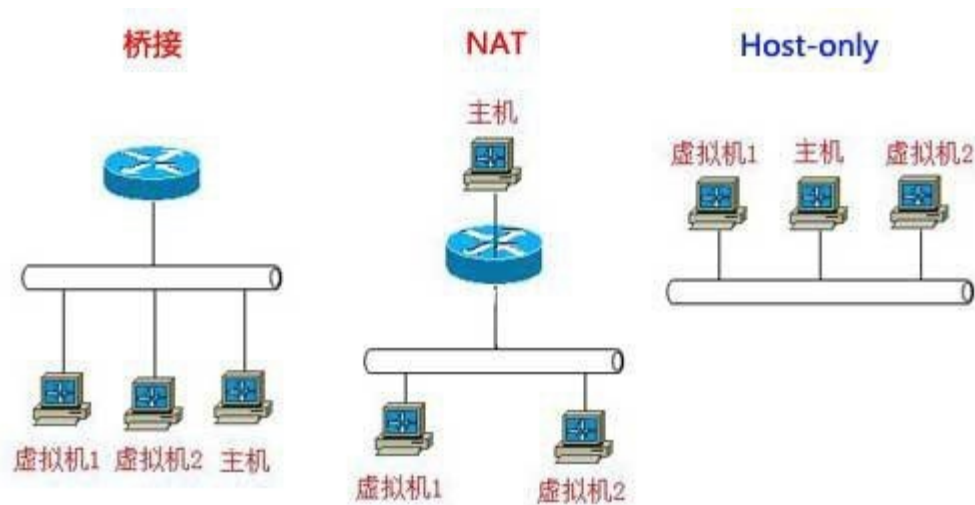
## 9. 应用程序规则高级设置

我们可以在天网防火墙个人版用户界面中找到“应用程序访问网络权限设置”中根据需要单独设置每个应用程序的网络使用规则，若符合规则，则防火墙放行，反之则拦截。

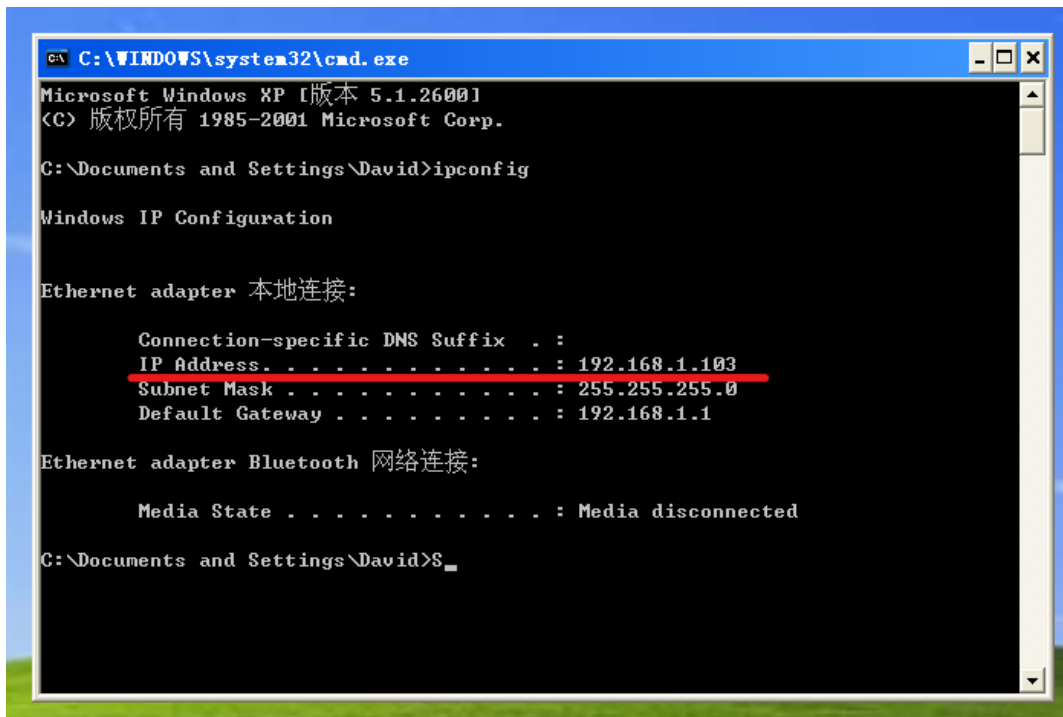


## 10. 配置 ip 规则，对主机中每一个发送或接收的数据包进行控制

我们用两台虚拟机进行局域网通联测试，根据测试需要，这里我选择配置桥接网络：



- 带有天网防火墙的虚拟机 WinXP: (ip:192.168.1.103)



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\David>ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

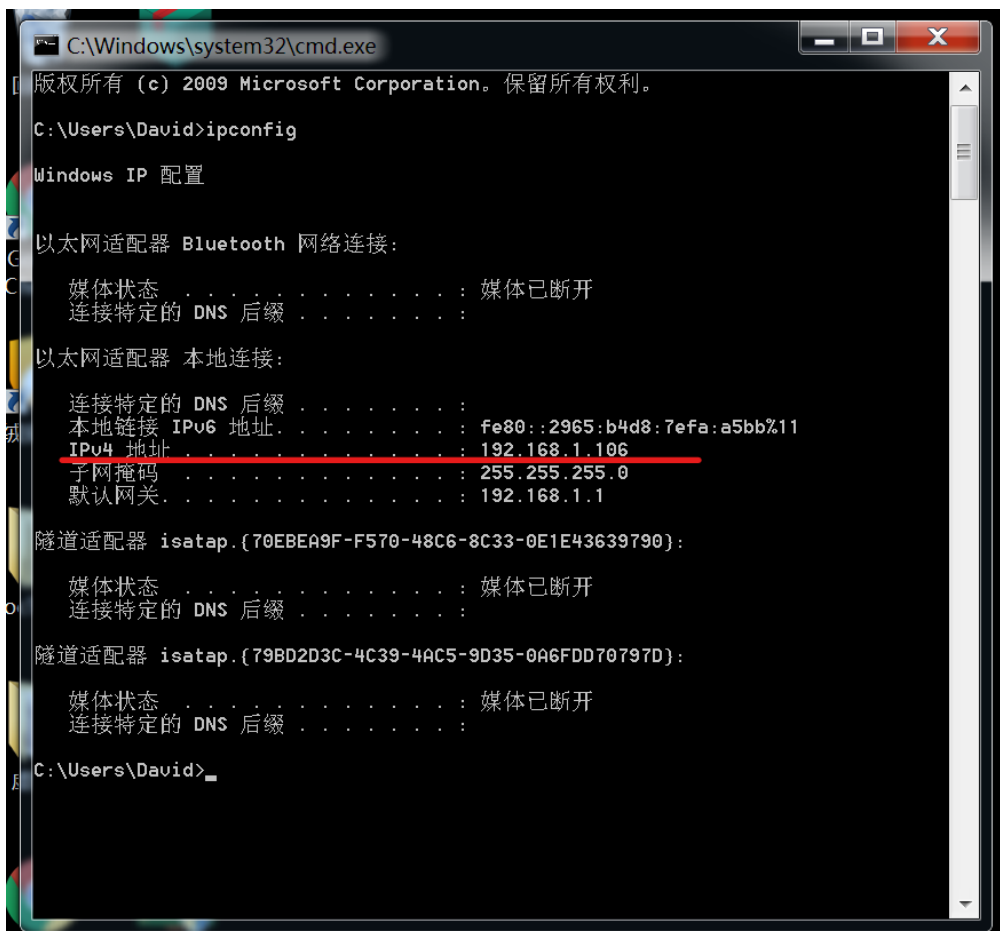
    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.1.103
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter Bluetooth 网络连接:

    Media State . . . . . : Media disconnected

C:\Documents and Settings\David>S_
```

- 未设置任何防火墙的虚拟机 Win7: (ip:192.168.1.106)



```
C:\Windows\system32\cmd.exe
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\David>ipconfig

Windows IP 配置

以太网适配器 Bluetooth 网络连接:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

以太网适配器 本地连接:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::2965:b4d8:7efa:a5bb%11
    IPv4 地址 . . . . . : 192.168.1.106
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : 192.168.1.1

隧道适配器 isatap.{70EBA9F-F570-48C6-8C33-0E1E43639790}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

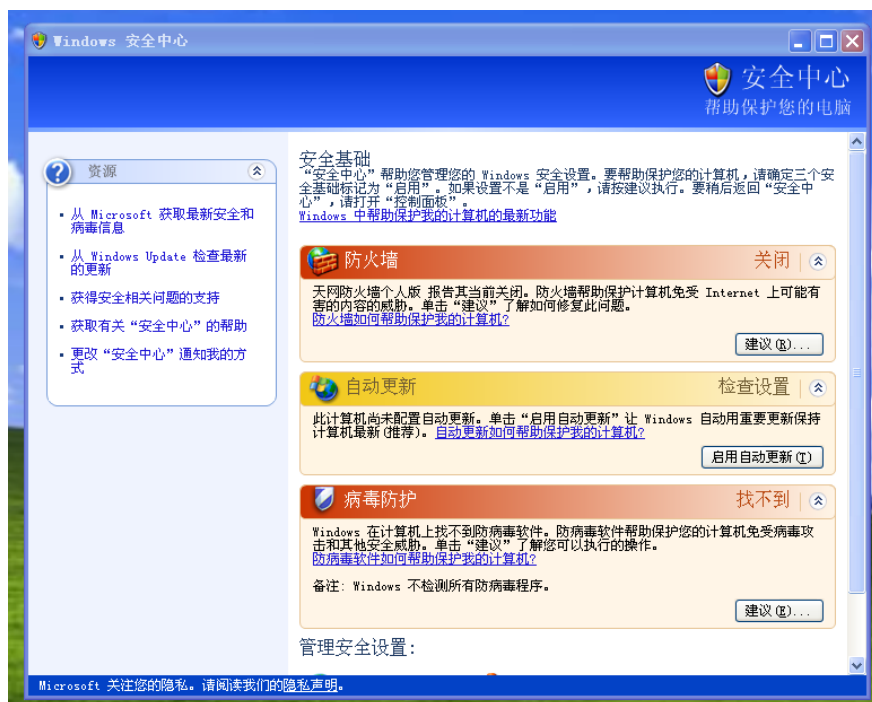
隧道适配器 isatap.{79BD2D3C-4C39-4AC5-9D35-0A6FDD70797D}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

C:\Users\David>
```

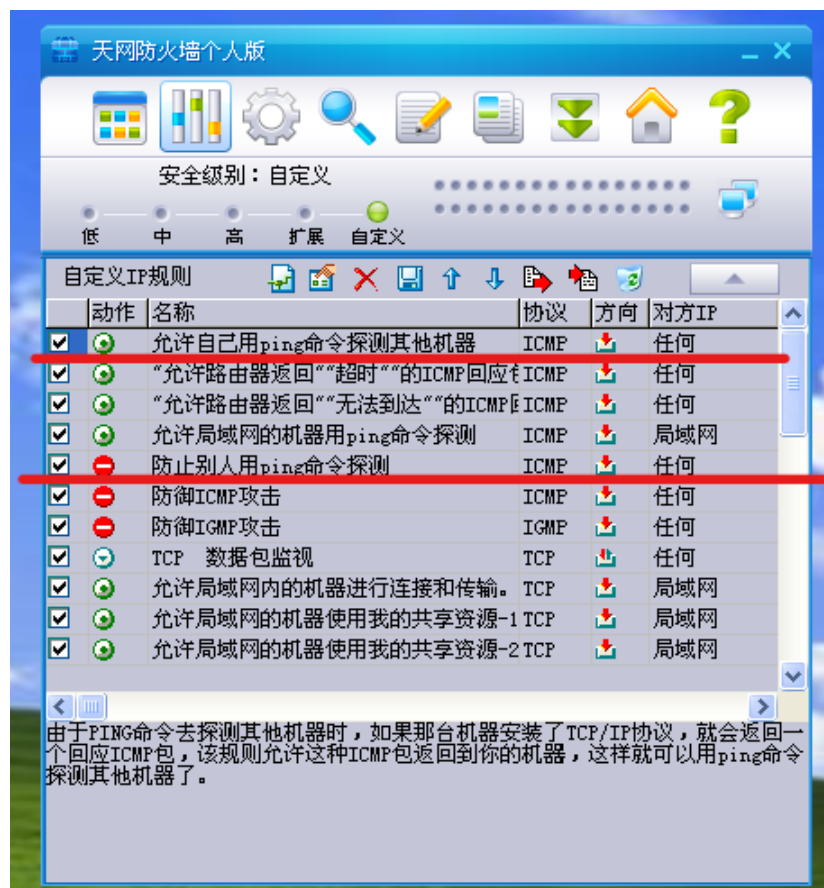
(注：在进行下面的测试之前，我关闭了所有防火墙，保证两台虚拟机可以相互 ping 通)

## (1) 关闭 WinXP 系统自带防火墙



## (2) 配置天网防火墙 ip 规则，

- 允许自己用 ping 命令探测其他机器
- 防止别人用 ping 命令探测



(3) 测试 WinXP ping Win7, 可以 ping 通

```
C:\Documents and Settings\David>ping 192.168.1.106

Pinging 192.168.1.106 with 32 bytes of data:

Reply from 192.168.1.106: bytes=32 time=1ms TTL=128
Reply from 192.168.1.106: bytes=32 time=1ms TTL=128
Reply from 192.168.1.106: bytes=32 time<1ms TTL=128
Reply from 192.168.1.106: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.106:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Documents and Settings\David>S
```

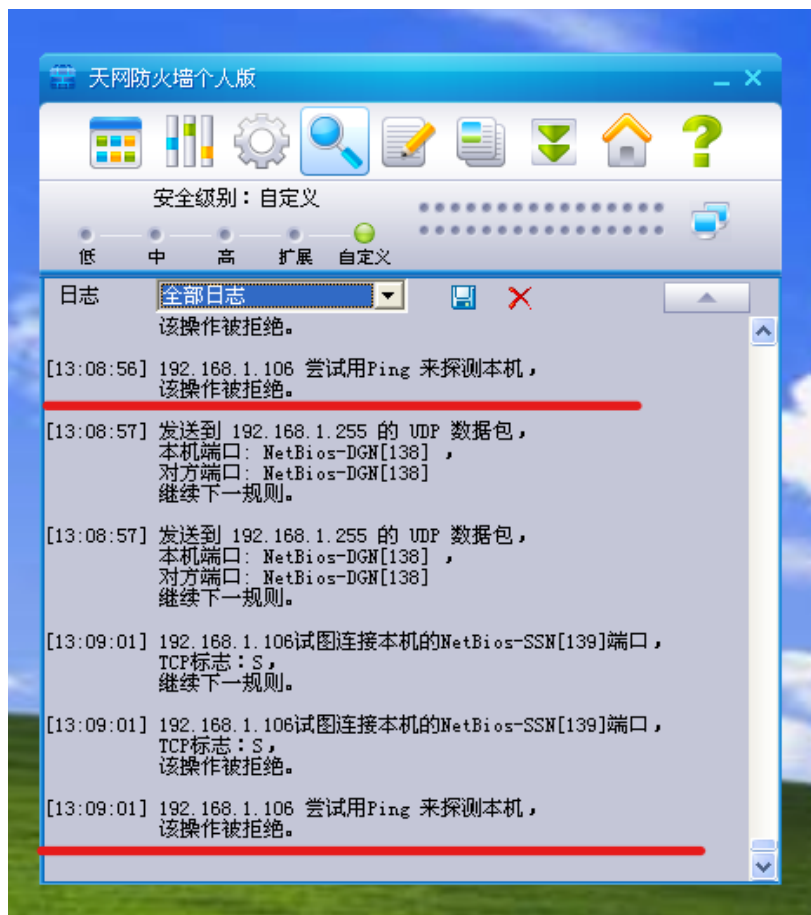
(4) 测试 Win7 ping WinXP, 请求超时, 无法 ping 通

```
C:\Users\David>ping 192.168.1.103

正在 Ping 192.168.1.103 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

192.168.1.103 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),
```

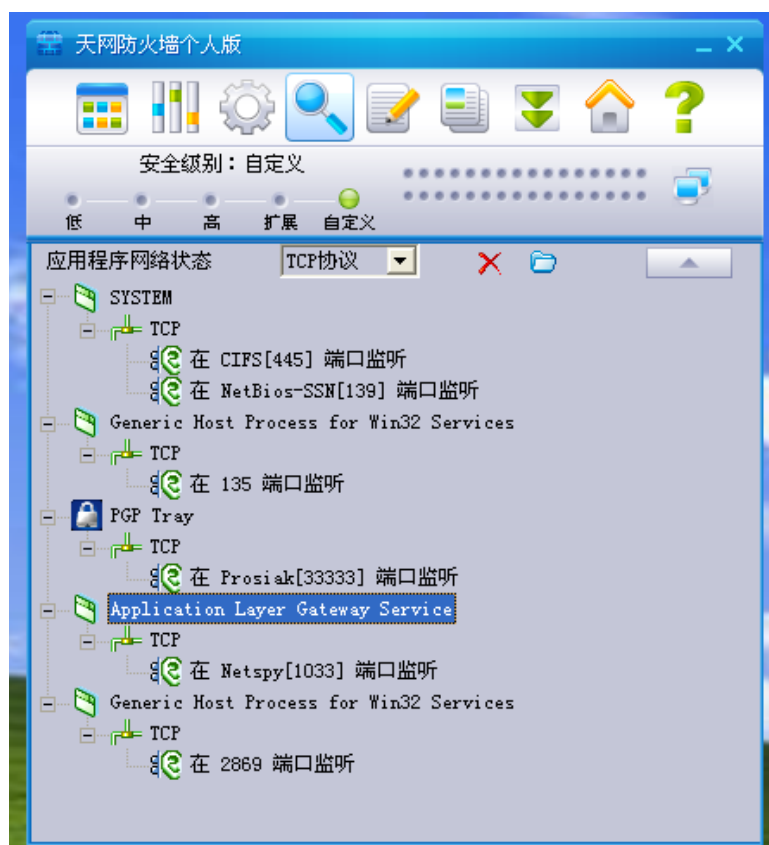
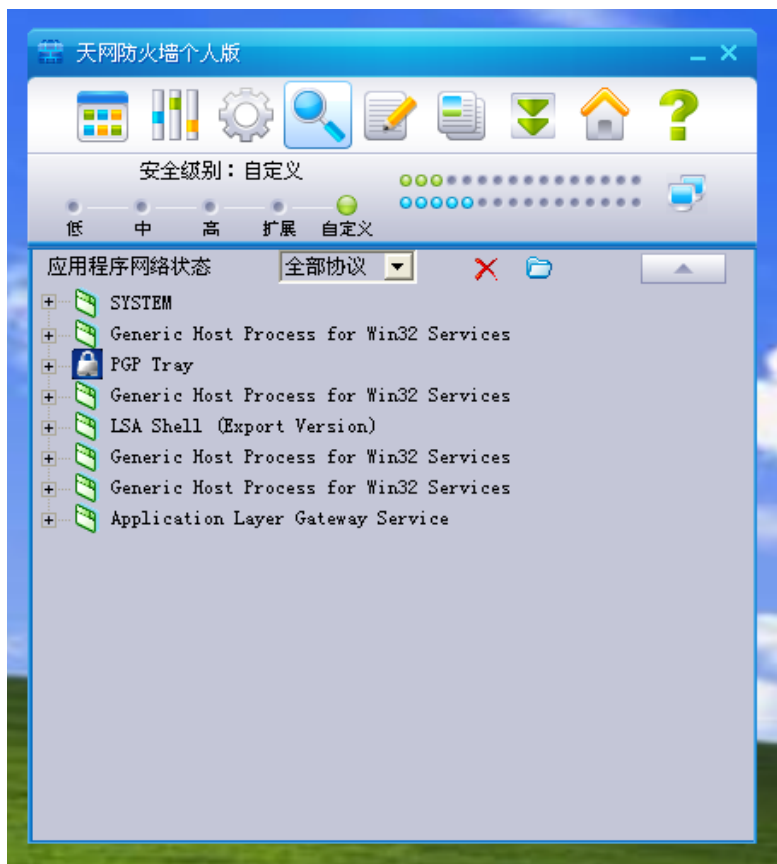
(5) 在 WinXP 的防火墙日志中可以查看 Win7 尝试用 ping 探测





## 11. 查看应用程序网络状态

若发现可疑应用异常使用网络，则可以结束相关进程



## 五、实验心得和思考

在网络中，所谓“防火墙”，是指一种将内部网和公众访问网（如 Internet）分开的方法，它实际上是一种隔离技术。防火墙是在两个网络通讯时执行的一种访问控制尺度，它能允许你“同意”的人和数据进入你的网络，同时将你“不同意”的人和数据拒之门外，最大限度地阻止网络中的黑客来访问你的网络。换句话说，如果不通过防火墙，公司内部的人就无法访问 Internet，Internet 上的人也无法和公司内部的人进行通信。网络系统中的防火墙有许多功能：

- **防火墙是网络安全屏障：**防火墙可以作为阻塞点、控制点极大地提高一个内部网络的安全性，并通过过滤不安全的服务而降低风险。由于只有经过精心选择的应用协议才能通过防火墙，所以网络环境变得更安全。如防火墙可以禁止诸如众所周知的不安全的 NFS 协议 进出受保护网络，这样外部的攻击者就不可能利用这些脆弱的协议来攻击内部网络。防火墙同时可以保护网络免受基于路由的攻击，如 IP 选项 中的源路由攻击和 ICMP 重定向 中的重定向路径。防火墙应该可以拒绝所有以上类型攻击的报文并通知防火墙管理员。
- **防火墙可以强化网络安全策略：**通过以防火墙为中心的安全方案配置，能将所有安全软件（如口令、加密、身份认证、审计等）配置在防火墙上。与将网络安全问题分散到各个主机上相比，防火墙的集中安全管理更 经济。例如在网络访问时，一次一密口令系统和其它的身份认证系统 完全可以不必分散在各个主机上，而集中在防火墙身上。
- **对网络存取和访问进行监控审计：**如果所有的访问都经过防火墙，那么，防火墙就能记录下这些访问并作出日志记录，同时也能提供网络使用情况的统计数据。当发生可疑动作时，防火墙能进行适当的报警，并提供网络是否受到监测和攻击的详细信息。另外，收集一个网络的使用和误用情况 也是非常重要的。首先的理由是可以清楚防火墙是否能够抵挡攻击者的探测和攻击，并且清楚防火墙的控制是否充足。而网络使用统计对网络需求分析和威胁分析等而言也是非常重要的。
- **防止内部信息的外泄：**通过利用防火墙对内部网络的划分，可实现内部网重点网段的隔离，从而限制了局部重点或敏感网络安全问题对全局网络造成的影响。再者，隐私是内部网络非常关心的问题，一个内部网络中不引人注意的细节可能包含了有关安全的线索而引起外部攻击者的兴趣，甚至因此而暴漏了内部网络的某些安全漏洞。使用防火墙就可以隐蔽那些透漏内部细节如 Finger，DNS 等服务。Finger 显示了主机的所有用户的注册名、真名，最后登录时间和使用 shell 类型等。但是 Finger 显示的信息很容易被攻击者所获悉。攻击者可以知道一个系统使用的频繁程度，这个系统是否有用户正在连线上网，这个系统是否在被攻击时引起注意等等。防火墙可以同样阻塞有关内部网络中的 DNS 信息，这样一台主机的域名和 IP 地址 就不会被外界所了解。除了安全作用，防火墙还支持具有 Internet 服务特性的企业内部网络技术体系 VPN（虚拟专用网）。