警示：实验报告如有雷同，雷同各方当次实验成绩均以 0 分计；在规定时间内未上交实验报告的，不得以其他方式补交，当次成绩按 0 分计；实验报告文件以 PDF 格式提交。

院系	软件学院	班级	6	学号	13331233	姓名	孙中阳
完成日期： 2016 年 11 月 25 日							

Windows 防火墙管理实验

【实验名称】

Windows防火墙管理实验。

【实验目的】

了解防火墙的配置与管理原理，掌握 Windows 防火墙的基本配置方法；分析防火墙的作用。

【实验原理】

所有进出网络的信息都必须通过防火墙，所以防火墙是一个安全策略的检查站，是设置在被保护网络和外部网络之间的一道屏障。防火墙对流经它的网络通信进行扫描，防止发生不可预测的、潜在破坏性的侵入。防火墙不但可以关闭不使用的端口，它还能禁止特定端口的流出通信，封锁特洛伊木马。另外，防火墙还可以禁止来自特殊站点的访问，从而防止来自不明入侵者的所有通信。

【实验要求】

撰写实验报告，给出必要的截图。

1. 查看 Windows7 / Windows 10 防火墙。

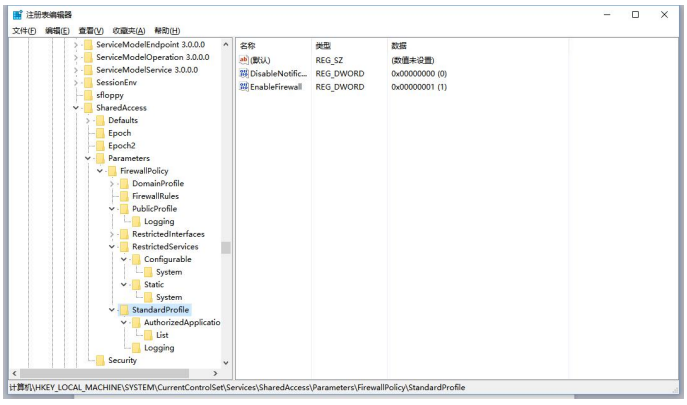
（1）了解图形界面的防火墙，对其功能进行描述（300 字左右）。

防火墙对流经它的网络通信进行扫描，这样能够过滤掉一些攻击，以免其在目标计算机上被执行。防火墙还可以关闭不使用的端口。而且它还能禁止特定端口的流出通信，封锁特洛伊木马。最后，它可以禁止来自特殊站点的访问，从而防止来自不明入侵者的所有通信。

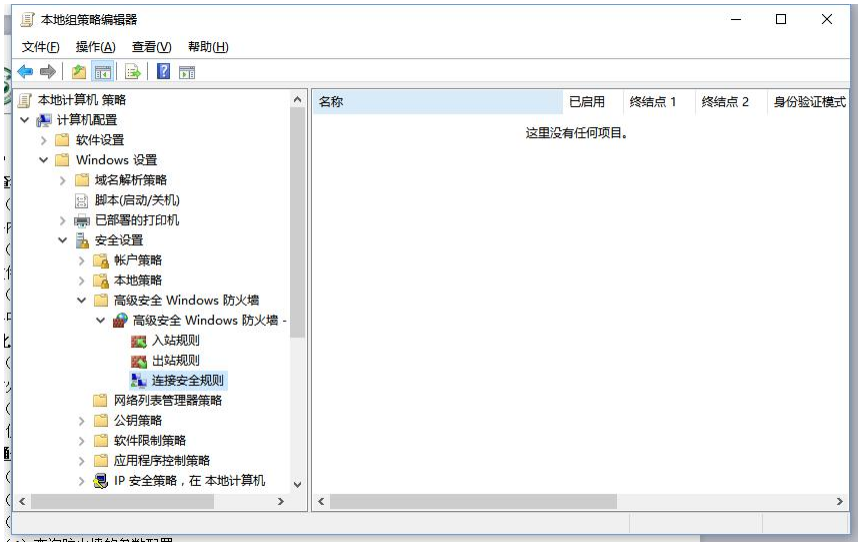
同时其具有很好的保护作用。入侵者必须首先穿越防火墙的安全防线，才能接触目标计算机。你可以将防火墙配置成许多不同保护级别。高级别的保护可能会禁止一些服务，如视频流等，但至少这是你自己的保护选择。

（2）用注册表（在 cmd 窗口中输入 regedit）查询防火墙相关配置，请指出注册表中防火墙配置的总项位置，将查到的情况与（1）的结果作比较。

防火墙配置在 HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControlSet\ Services\ SharedAccess\ Parameters\ FirewallPolicy，比如这里，能够控制防火墙的开启和关闭



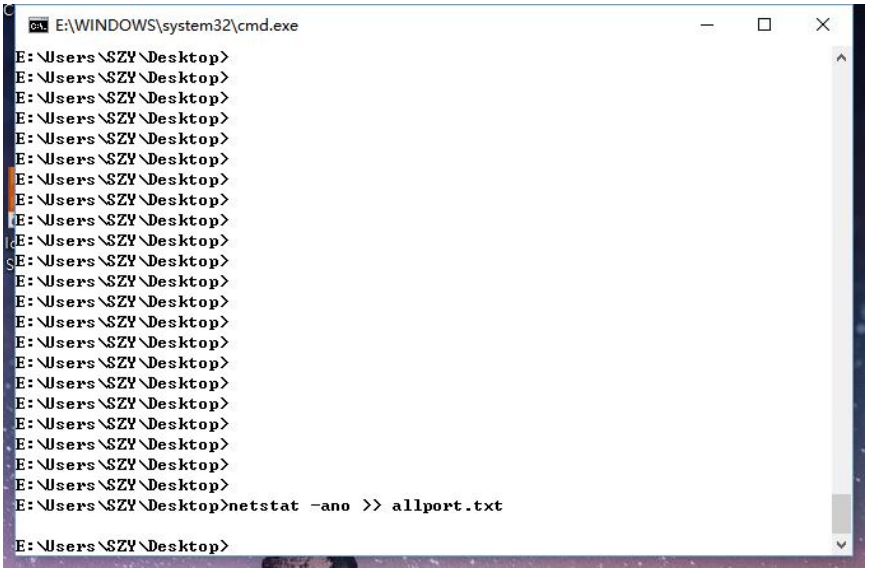
（3）使用组策略工具（在 cmd 窗口中输入 gpedit.msc）查询防火墙配置，并与（1）、（2）作比较。

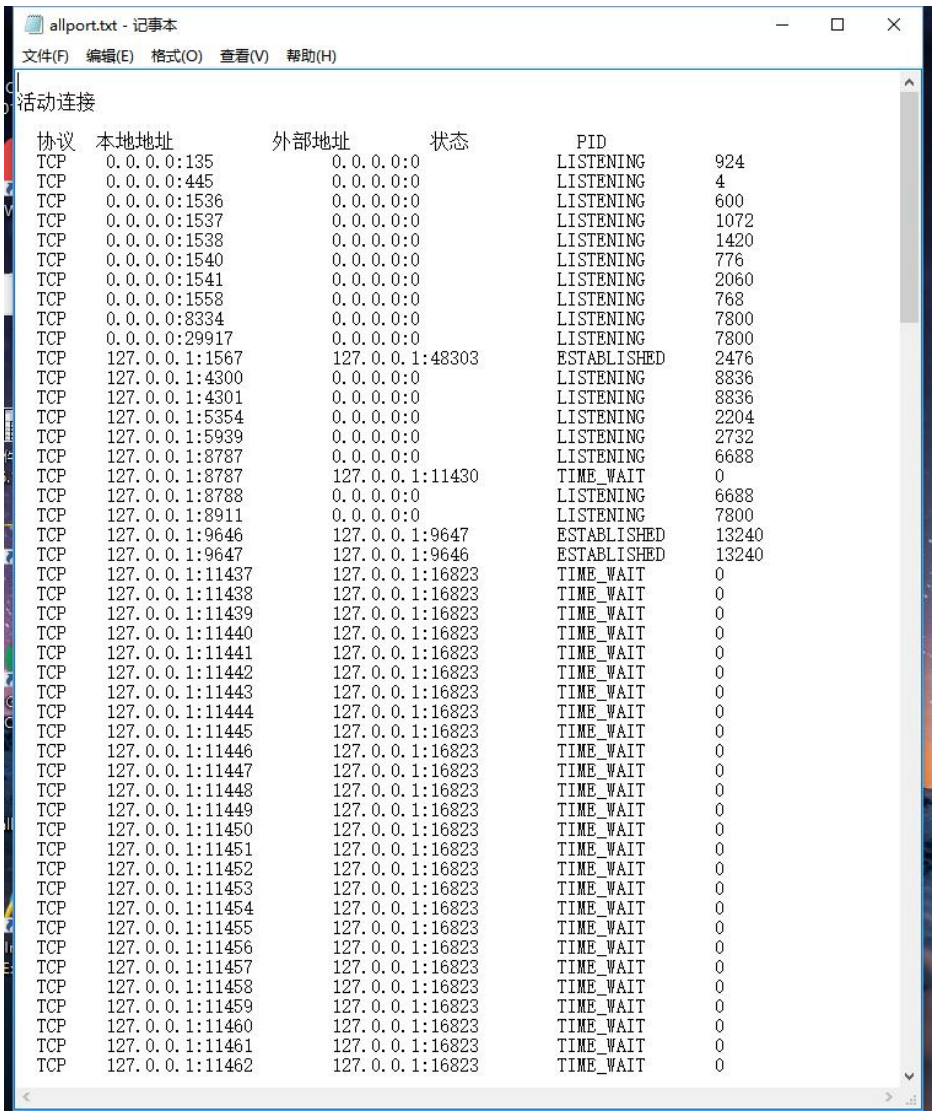


组策略管理器同样可以管理防火墙，较 2)更加直观

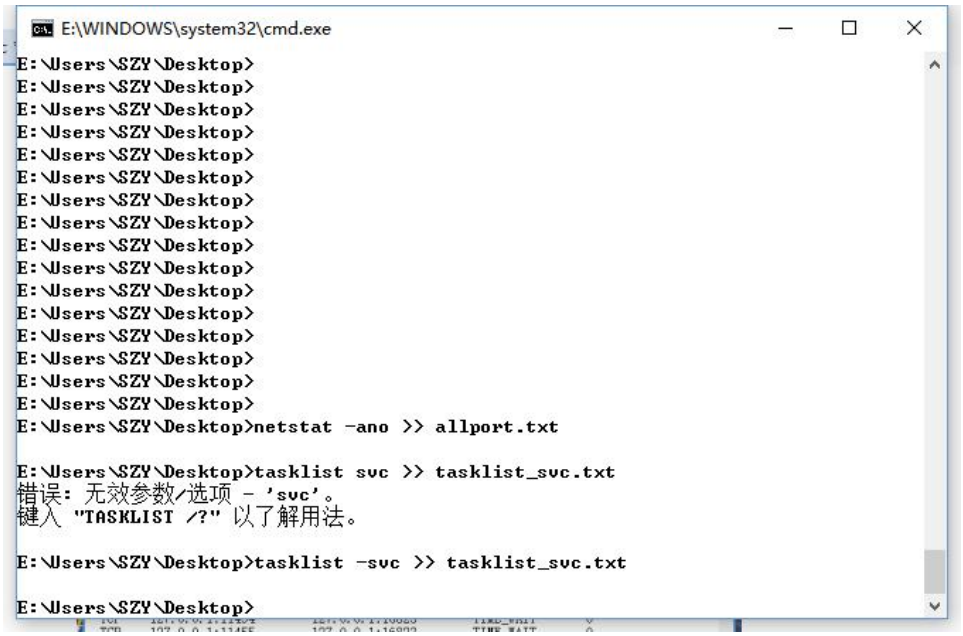
2. 查看程序使用的端口。

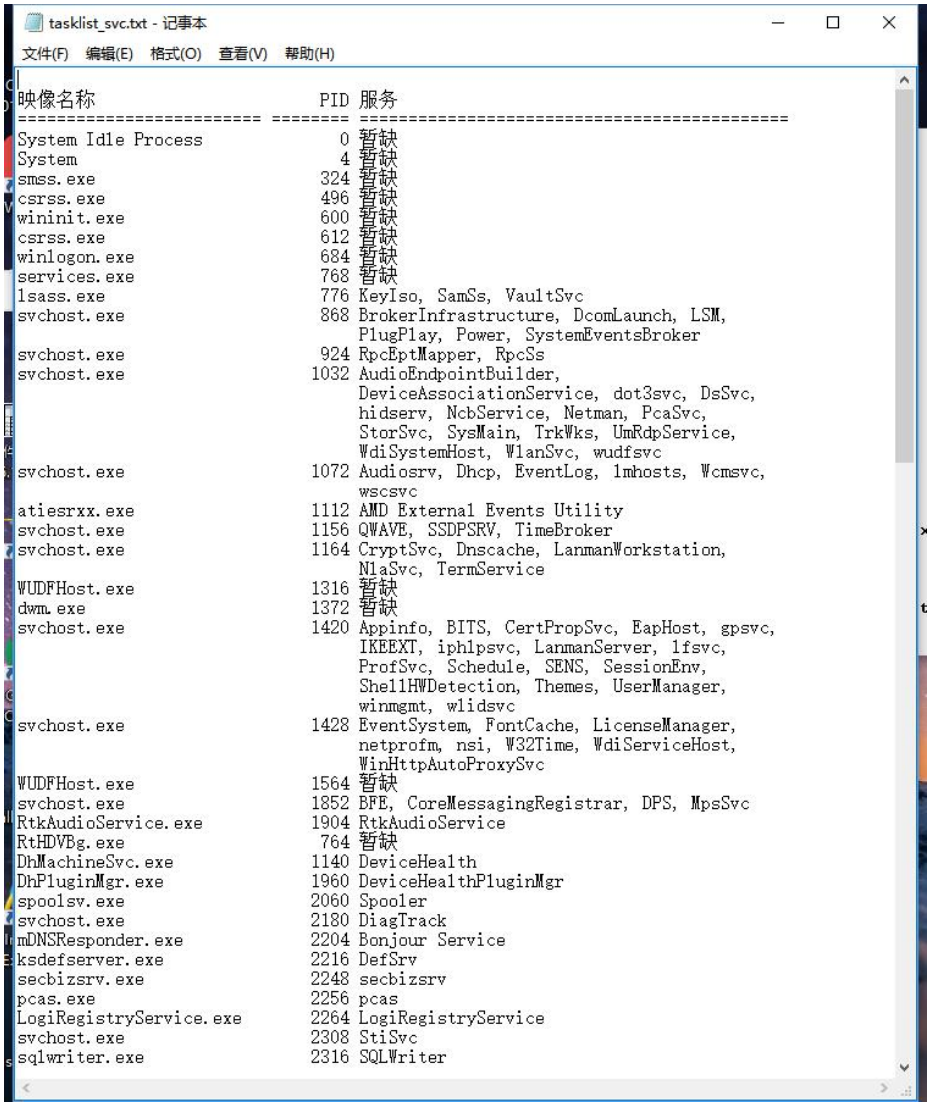
（1）使用 netstat 命令（带参数 -ano）输出端口信息，并将输出信息保存到文件“allport.txt”，将文件内容截图。





（2）使用 tasklist 命令（带参数 svc）获得进程信息，并将输出信息保存到文件“tasklist_svc.txt”，将文件内容截图。



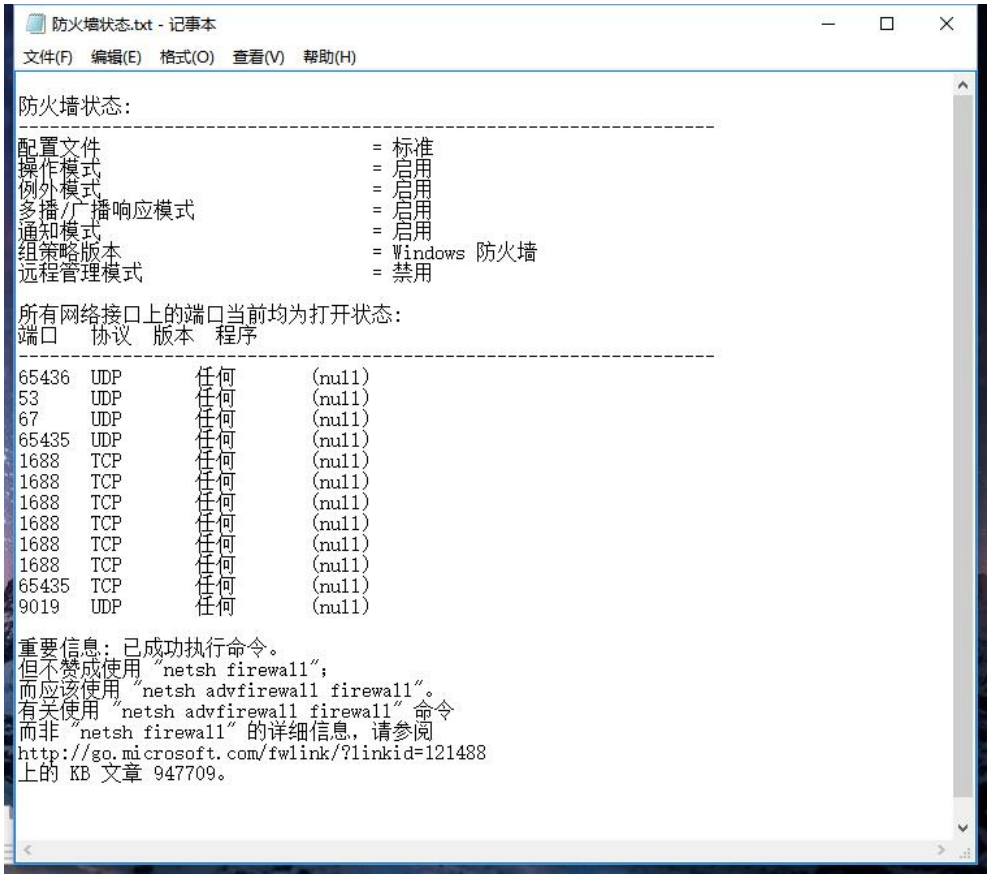


（3）在文件 "allport.txt" 及 "tasklist_svc.txt" 中查找相同的 PID 项目。请具体标出一个，说明在两文件中的对应关系。

就拿 924 号进程来说，tasklist 标明其进程名称和对应服务，allport 则可查找到其对应的端口号和详细的网络信息

3. 比对哪些程序正在进行端口侦听，而防火墙没有开放此端口。

（1）执行命令 Netsh firewall show state，将防火墙的状态输出到“防火墙状态.txt”文件中；查看当前防火墙开放的端口，给出截图。



（2）将“防火墙状态.txt”文件中端口与 2（1）的文件“allport.txt”对比，哪些端口是在 listen 状态、但防火墙并没有打开该端口，讨论这样可以发现应用程序存在那些问题。

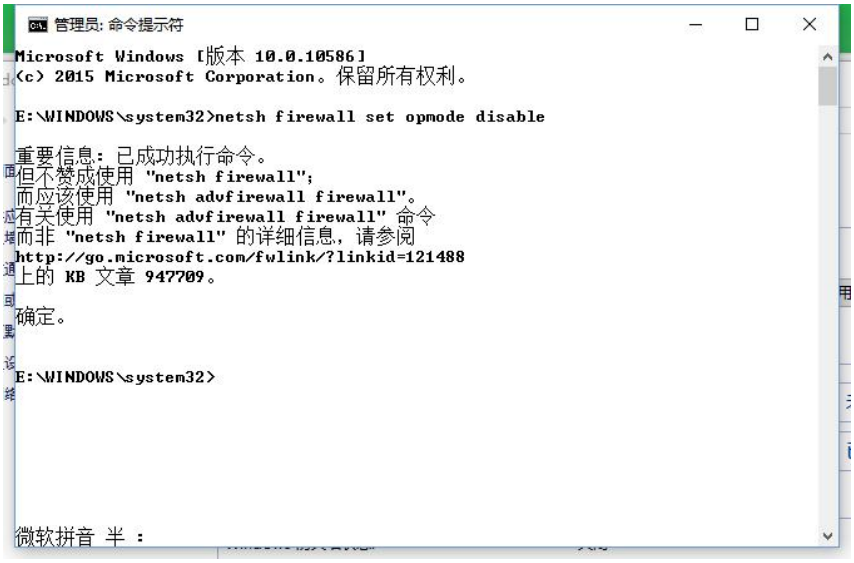
所有监听的端口都没有被打开，这样可能会使得部分应用无法从互联网获得数据。

4. 通过防火墙命令 netsh firewall，对防火墙进行管理和配置。

（1）恢复默认设置，请说明此操作的必要性；

不恢复默认设置，后面的配置可能会出现意想不到的情况

（2）启用防火墙，并且不允许例外，给出命令执行前、后防火墙图形界面的变化；




Windows 防火墙
控制面板 › 系统和安全 › Windows 防火墙
使用 Windows 防火墙来帮助保护你的电脑
Windows 防火墙有助于防止黑客或恶意软件通过 Internet 或网络访问你的电脑。
更新防火墙设置
Windows 防火墙未使用推荐的设置来保护计算机。
使用推荐设置
推荐的设置有哪些?
专用网络(R) 未连接
来宾或公用网络(P) 已连接
公共场所(例如机场或咖啡店)中的网络
Windows 防火墙状态: 关闭
传入连接: 阻止所有与未在允许应用列表中的应用的连接
活动的公用网络: 网络 3
通知状态: Windows 防火墙阻止新应用时通知我
控制面板主页
允许应用或功能通过 Windows 防火墙
更改通知设置
启用或关闭 Windows 防火墙
还原默认值
高级设置
对网络进行疑难解答
另请参阅
安全和维护
网络和共享中心


管理员: 命令提示符
但不赞成使用 "netsh firewall";
而应该使用 "netsh advfirewall firewall"。
有关使用 "netsh advfirewall firewall" 命令
而非 "netsh firewall" 的详细信息，请参阅
http://go.microsoft.com/fwlink/?linkid=121488
上的 KB 文章 947709。
确定。
E:\WINDOWS\system32>netsh firewall set opmode enable
重要信息: 已成功执行命令。
但不赞成使用 "netsh firewall";
而应该使用 "netsh advfirewall firewall"。
有关使用 "netsh advfirewall firewall" 命令
而非 "netsh firewall" 的详细信息，请参阅
http://go.microsoft.com/fwlink/?linkid=121488
上的 KB 文章 947709。
确定。
E:\WINDOWS\system32>
微软拼音 半 :


Windows 防火墙
控制面板 › 系统和安全 › Windows 防火墙
使用 Windows 防火墙来帮助保护你的电脑
Windows 防火墙有助于防止黑客或恶意软件通过 Internet 或网络访问你的电脑。
更新防火墙设置
Windows 防火墙未使用推荐的设置来保护计算机。
使用推荐设置
推荐的设置有哪些?
专用网络(R) 未连接
来宾或公用网络(P) 已连接
公共场所(例如机场或咖啡店)中的网络
Windows 防火墙状态: 启用
传入连接: 阻止所有与未在允许应用列表中的应用的连接
活动的公用网络: 网络 3
通知状态: Windows 防火墙阻止新应用时通知我
控制面板主页
允许应用或功能通过 Windows 防火墙
更改通知设置
启用或关闭 Windows 防火墙
还原默认值
高级设置
对网络进行疑难解答
另请参阅
安全和维护
网络和共享中心

（3）启用防火墙，允许例外；

基本同上

（4）查询防火墙的参数配置；

使用命令 **netsh firewall show config**

（5）关闭防火墙，请说明此操作的必要性。

允许更多的应用与外界的通讯连接

5. 讨论防火墙图形管理方式与命令行管理方式的优缺点、适用场合。

6.

图形界面比较直观，操作简单，但是专业性不够，适合一般用户。 命令行命令简洁，但不易理解，适合专业用户。 **6. Windows** 自带的防火墙，与第三方防火墙功能上有什么区别？请举一款进行比较。 **Windows** 防火墙只阻截所有传入的未经请求的流量，对主动请求传出的流量不作理会。而第三方病毒防火墙软件一般都会对两个方向的访问进行监控和审核，这一点是它们之间最大的区别。如果 入侵已经发生或间谍软件已经安装，并主动连接到外部网络，那么 **Windows** 防火墙是束手无策的。

7. Windows 自带的防火墙，与第三方防火墙功能上有什么区别？请举一款进行比较。

Windows 防火墙只阻截所有传入的未经请求的流量，对主动请求传出的流量不作理会。而第三方病毒防火墙软件一般都会对两个方向的访问进行监控和审核，这一点是它们之间最大的区别。如果 入侵已经发生或间谍软件已经安装，并主动连接到外部网络，那么 **Windows** 防火墙是束手无策的。

8. 启动一个抓包分析软件（例如 **Wireshark**），监测当有外来通信时，防火墙可能采取的动作。

实例：天网防火墙。当检测到传出的时候，它会立刻拦截并询问用户是否放行，而 **windows** 防火 墙则不会。 **7.** 启动抓包分析软件（例如 **Wireshark**），监测当有外来通信时，防火墙可能采取的动作。

8. 防火墙是如何识别有害数据包并加以拦截的？请通过实例分析。

使用另一台机 **ping** 测试机，连接超时。在测试机抓包发现，防火墙拦截了外来通信，因此另一台 机得不到响应。 **8.** 防火墙是如何识别有害数据包并加以拦截的？请通过实例分析。 防火墙是通过对每个数据包的头部、协议、地址、端口、类型等信息进行分析，并与预先设定好的 防火墙过滤规则进行核对，一旦发现某个包的某个或多个部分与过滤规则匹配并且条件为“阻止” 的时候，这个包就会被丢弃。以 **7** 中的测试为例，由于设定了不允许例外，防火墙会把所有外来包 视为有害数据包并拦截。