

**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	数据科学与计算机学院	班级	周一_3-4节	学号	15331151	姓名	李佳
完成日期： 2017 年 12 月 12 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）。



系统环境 win10，鼠标移动到左下角开始图标→右键单击→控制面板→系统和安全→windows

防火墙。Win10 防火墙设置界面左侧窗格列出了所有与防火墙相关的操作，比如“允许应用或功能通过 Windows 防火墙”、“更改通知设置”、“启用或关闭防火墙”、“还原默认值”以及“高级设置”等。

**允许应用或功能通过 windows 防火墙：**用户可以允许或组织某个应用或功能在专用或者公用网络中的通信状态

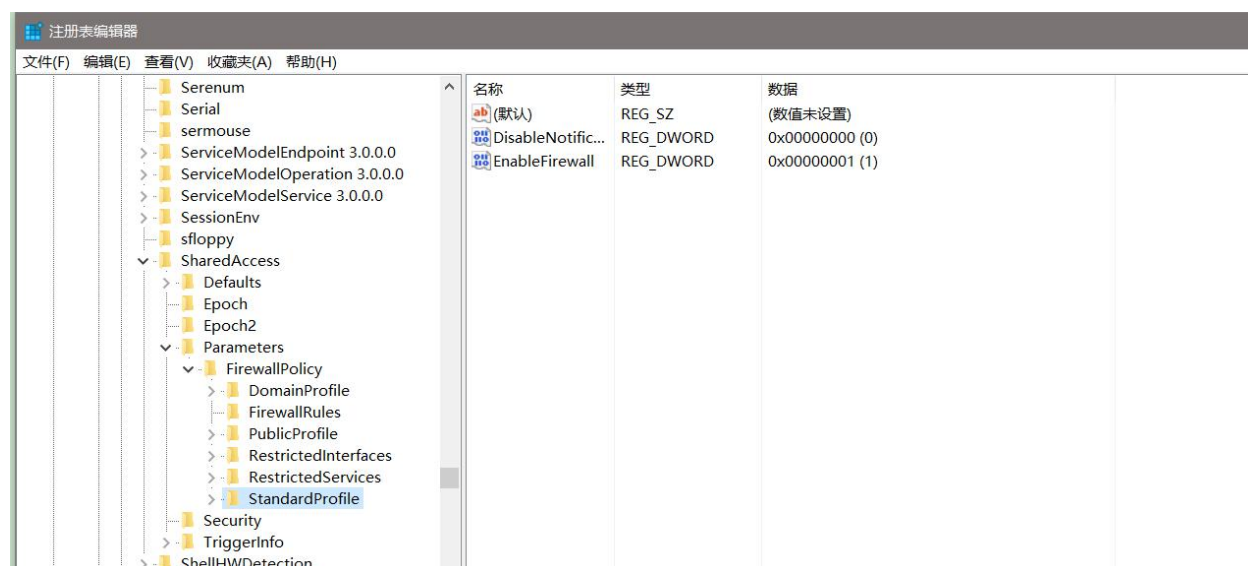
**更改通知设置 和 启用或关闭防火墙：**用户可以在此对专用/公用网络设置不同的安全规则，也可开启或关闭防火墙。

**高级设置：**在此处，可以对“入站规则”、“出站规则”、“连接安全规则”以及“监视”等选项。支持双向保护，可以对出站、入站通信进行过滤，用户可以针对各种对象创建防火墙规则，确定阻止还是允许通过。

**还原默认值：**还原 Win8 防火墙的默认设置。

Win10 防火墙设置界面主界面列出了专用网络以及来宾或公用网络的防火墙当前状态、传入连接、活动的网络以及通知状态。

(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。



防火墙配置的总项位置在：

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile

EnableFirewall 的值为 1，表示当前防火墙状态为打开。与（1）的显示结果相符。

(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。



抱歉，我的系统是 win 10 家庭版，而 win10 只有专业版才有组策略工具，所以无法查询相关

配置。

## 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。

**netstat -ano**

由于端口信息过长, 只截取开始部分信息。

```
C:\Users\lee>netstat -ano
```

活动连接

协议	本地地址	外部地址	状态	PID
TCP	0.0.0.0:22	0.0.0.0:0	LISTENING	3452
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	1004
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:1536	0.0.0.0:0	LISTENING	712
TCP	0.0.0.0:1537	0.0.0.0:0	LISTENING	1128
TCP	0.0.0.0:1539	0.0.0.0:0	LISTENING	840
TCP	0.0.0.0:1540	0.0.0.0:0	LISTENING	2452
TCP	0.0.0.0:1547	0.0.0.0:0	LISTENING	832
TCP	0.0.0.0:2141	0.0.0.0:0	LISTENING	12800
TCP	0.0.0.0:2153	0.0.0.0:0	LISTENING	12828
TCP	0.0.0.0:2869	0.0.0.0:0	LISTENING	4
中文(简体) - 百度输入法 全 :		0.0.0.0:0	LISTENING	3208
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:50135	0.0.0.0:0	LISTENING	3920
中文(简体) - 百度输入法 全 :		0.0.0.0:0	LISTENING	11376
TCP	127.0.0.1:4300	0.0.0.0:0	LISTENING	3920
TCP	127.0.0.1:4301	0.0.0.0:0	LISTENING	3920
TCP	127.0.0.1:9410	0.0.0.0:0	LISTENING	2856
TCP	127.0.0.1:27018	0.0.0.0:0	LISTENING	2760
TCP	127.0.0.1:27643	127.0.0.1:27644	ESTABLISHED	5296
TCP	127.0.0.1:27644	127.0.0.1:27643	ESTABLISHED	5296
TCP	169.254.138.177:139	0.0.0.0:0	LISTENING	4
TCP	192.168.199.208:139	0.0.0.0:0	LISTENING	4
TCP	192.168.199.208:1029	183.232.238.236:443	ESTABLISHED	5860
TCP	192.168.199.208:1031	183.232.172.239:443	ESTABLISHED	5860
TCP	192.168.199.208:1032	47.95.51.100:443	CLOSE_WAIT	5860
TCP	192.168.199.208:1645	223.119.157.79:443	CLOSE_WAIT	8252
TCP	192.168.199.208:1646	223.119.242.63:443	CLOSE_WAIT	8252
TCP	192.168.199.208:1647	223.119.157.72:443	CLOSE_WAIT	8252
TCP	192.168.199.208:1649	223.119.157.72:443	CLOSE_WAIT	8252
TCP	192.168.199.208:1651	223.119.157.72:443	CLOSE_WAIT	8252
TCP	192.168.199.208:1925	101.199.97.108:80	ESTABLISHED	6972
TCP	192.168.199.208:4045	42.236.37.149:80	ESTABLISHED	6972
TCP	192.168.199.208:4066	180.163.238.133:443	ESTABLISHED	6972
TCP	192.168.199.208:4089	42.236.37.135:80	ESTABLISHED	5860
TCP	192.168.199.208:4127	183.232.127.166:443	ESTABLISHED	3920
TCP	192.168.199.208:4142	111.221.29.129:443	ESTABLISHED	12828
TCP	192.168.199.208:4146	111.221.29.125:443	ESTABLISHED	384
TCP	192.168.199.208:11024	221.181.72.211:443	CLOSE_WAIT	5860



## netstat -ano > allport.txt

allport.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

活动连接

协议	本地地址	外部地址	状态	PID
TCP	0.0.0.0:22	0.0.0.0:0	LISTENING	3452
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	1004
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:1536	0.0.0.0:0	LISTENING	712
TCP	0.0.0.0:1537	0.0.0.0:0	LISTENING	1128
TCP	0.0.0.0:1539	0.0.0.0:0	LISTENING	840
TCP	0.0.0.0:1540	0.0.0.0:0	LISTENING	2452
TCP	0.0.0.0:1547	0.0.0.0:0	LISTENING	832
TCP	0.0.0.0:2141	0.0.0.0:0	LISTENING	12800
TCP	0.0.0.0:2153	0.0.0.0:0	LISTENING	12828
TCP	0.0.0.0:2869	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:5091	0.0.0.0:0	LISTENING	3208
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:50135	0.0.0.0:0	LISTENING	3920
TCP	127.0.0.1:2710	0.0.0.0:0	LISTENING	11376
TCP	127.0.0.1:4300	0.0.0.0:0	LISTENING	3920
TCP	127.0.0.1:4301	0.0.0.0:0	LISTENING	3920
TCP	127.0.0.1:9410	0.0.0.0:0	LISTENING	2856
TCP	127.0.0.1:27018	0.0.0.0:0	LISTENING	2760
TCP	127.0.0.1:27643	127.0.0.1:27644	ESTABLISHED	5296
TCP	127.0.0.1:27644	127.0.0.1:27643	ESTABLISHED	5296
TCP	169.254.138.177:139	0.0.0.0:0	LISTENING	4
TCP	192.168.199.208:139	0.0.0.0:0	LISTENING	4
TCP	192.168.199.208:1032	47.95.51.100:443	CLOSE_WAIT	5860

(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。

## tasklist -svc

命令提示符

Microsoft Windows [版本 10.0.14393]  
(c) 2016 Microsoft Corporation. 保留所有权利。

C:\Users\lee>tasklist -svc

映像名称	PID	服务
System Idle Process	0	暂缺
System	4	暂缺
smss.exe	368	暂缺
csrss.exe	560	暂缺
csrss.exe	688	暂缺
wininit.exe	712	暂缺
winlogon.exe	752	暂缺
services.exe	832	暂缺
lsass.exe	840	EFS, KeyIso, SamSs, VaultSvc
svchost.exe	940	BrokerInfrastructure, DcomLaunch, LSM, PlugPlay, Power, SystemEventsBroker
svchost.exe	1004	RpcEptMapper, RpcSs
dmw.exe	596	暂缺
svchost.exe	1000	AudioEndpointBuilder, DeviceAssociationService, dot3svc, DsSvc, hidserv, NcbService, Netman, PcaSvc, StorSvc, SysMain, UmRdpService, WdiSystemHost, wudfsvc
svchost.exe	300	CryptSvc, Dnscache, LanmanWorkstation, NlaSvc, TermService
LenovoUpdate.exe	1084	LenovoUpdate
svchost.exe	1128	Dhcp, EventLog, HomeGroupProvider, lmhosts, TimeBrokerSvc, wscntfrg
WUDFHost.exe	1288	暂缺
atiesrxx.exe	1300	AMD External Events Utility
atieclxx.exe	1428	暂缺
svchost.exe	1456	CDPSvc, fdPHost, FontCache, LicenseManager, netprofm, nsi, WdiServiceHost, WinHttpAutoProxySvc
svchost.exe	1528	AudioSrv
WUDFHost.exe	1624	暂缺
svchost.exe	1740	BFE, CoreMessagingRegistrar, DPS, MpsSvc, NcdAutoSetup
svchost.exe	1844	Wcmsvc
360rps.exe	1944	360rp
中文(简体) - 百度输入法 全	2000	ZhuDongFangYu
tasklist.exe	1608	暂缺

## tasklist -svc > tasklist\_svc.txt

映像名称	PID	服务
System Idle Process	0	暂缺
System	4	暂缺
smss.exe	368	暂缺
csrss.exe	560	暂缺
csrss.exe	688	暂缺
wininit.exe	712	暂缺
winlogon.exe	752	暂缺
services.exe	832	暂缺
lsass.exe	840	EFS, KeyIso, SamSs, VaultSvc
svchost.exe	940	BrokerInfrastructure, DcomLaunch, LSM, PlugPlay, Power, SystemEventsBroker
svchost.exe	1004	RpcEptMapper, RpcSs
dwm.exe	596	暂缺
svchost.exe	1000	AudioEndpointBuilder, DeviceAssociationService, dot3svc, DsSvc, hidserv, NcbService, Netman, PcaSvc, StorSvc, SysMain, UmRdpService, WdiSystemHost, wudfsvc
svchost.exe	300	CryptSvc, Dnscache, LanmanWorkstation, NlaSvc, TermService
LenovoUpdate.exe	1084	LenovoUpdate
svchost.exe	1128	Dhcp, EventLog, HomeGroupProvider, Imhosts, TimeBrokerSvc, wscsvc
WUDFHost.exe	1288	暂缺
atiesrxx.exe	1300	AMD External Events Utility

(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，说明在两个文件中的对应关系。

TCP	192.168.199.208:1925	101.199.97.108:80	ESTABLISHED	6972
TCP	192.168.199.208:4045	42.236.37.149:80	ESTABLISHED	6972
TCP	192.168.199.208:4066	180.163.238.133:443	ESTABLISHED	6972

360tray.exe 6972 暂缺

PID 都为 6972。

allport.txt 主要是记录某个 PID 值所对应的本地及外部地址以及当前运行状态；

tasklist.txt 显示该 PID 所占用的程序。

### 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。

```
C:\Users\lee>netsh firewall show state
```


防火墙状态：

配置文件	= 标准
操作模式	= 启用
例外模式	= 启用
多播/广播响应模式	= 启用
通知模式	= 启用
组策略版本	= Windows 防火墙
远程管理模式	= 禁用

所有网络接口上的端口当前均为打开状态：

端口	协议	版本	程序
3306	TCP	任何	(null)

```
C:\Users\lee>netsh firewall show state > 防火墙状态.txt
```



```
防火墙状态:
-----
配置文件                = 标准
操作模式                = 启用
例外模式                = 启用
多播/广播响应模式        = 启用
通知模式                = 启用
组策略版本              = Windows 防火墙
远程管理模式            = 禁用

所有网络接口上的端口当前均为打开状态:
端口  协议  版本  程序
-----
3306  TCP    任何  (null)

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。
```

(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。

结果显示所有网络上的端口都处于打开状态, 因此没有处于 listen 状态但防火墙没有打开的端口。如若存在此情况, 可能程序存在一定的漏洞, 使得防火墙无法检测, 穿透了防火墙, 端口可能存在风险。

#### 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;

**netsh advfirewall reset (需要管理员权限)**

此步将清除 “允许应用通过 Windows 防火墙进行通信” 中所有应用和功能的通信规则, 即权限清空, 需要重新进行配置。对于本实验没有影响。



(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：

netsh firewall set opmode mode=ENABLE exceptions=DISABLE

```
C:\WINDOWS\system32>netsh firewall set opmode mode=ENABLE exceptions=DISABLE
```

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。



不允许任何例外时图形界面的绿色对号变成了红色禁止符号，此时防火墙打开且没有例外。

(3) 启用防火墙，允许例外；

netsh firewall set opmode mode=ENABLE exceptions=ENABLE

```
C:\WINDOWS\system32>netsh firewall set opmode mode=ENABLE exceptions=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。



(4) 查询防火墙的参数配置；

netsh advfirewall show global

```
管理员: 命令提示符
C:\WINDOWS\system32>netsh advfirewall show global

全局 设置:
-----
IPsec:
StrongCRLCheck          0: 已禁用
SAIdleTimeMin           5min
DefaultExemptions       NeighborDiscovery, DHCP
IPsecThroughNAT         从未
AuthzUserGrp            无
AuthzComputerGrp        无
AuthzUserGrpTransport   无
AuthzComputerGrpTransport 无

StatefulFTP             启用
StatefulPPTP            启用

主 模式:
KeyLifetime              480min, 0sess
SecMethods               DHGroup2-AES128-SHA1, DHGroup2-3DES-SHA1
ForceDH                  No

类别:
BootTimeRuleCategory     Windows 防火墙
FirewallRuleCategory     Windows 防火墙
StealthRuleCategory      Windows 防火墙
ConSecRuleRuleCategory   Windows 防火墙

确定。
```



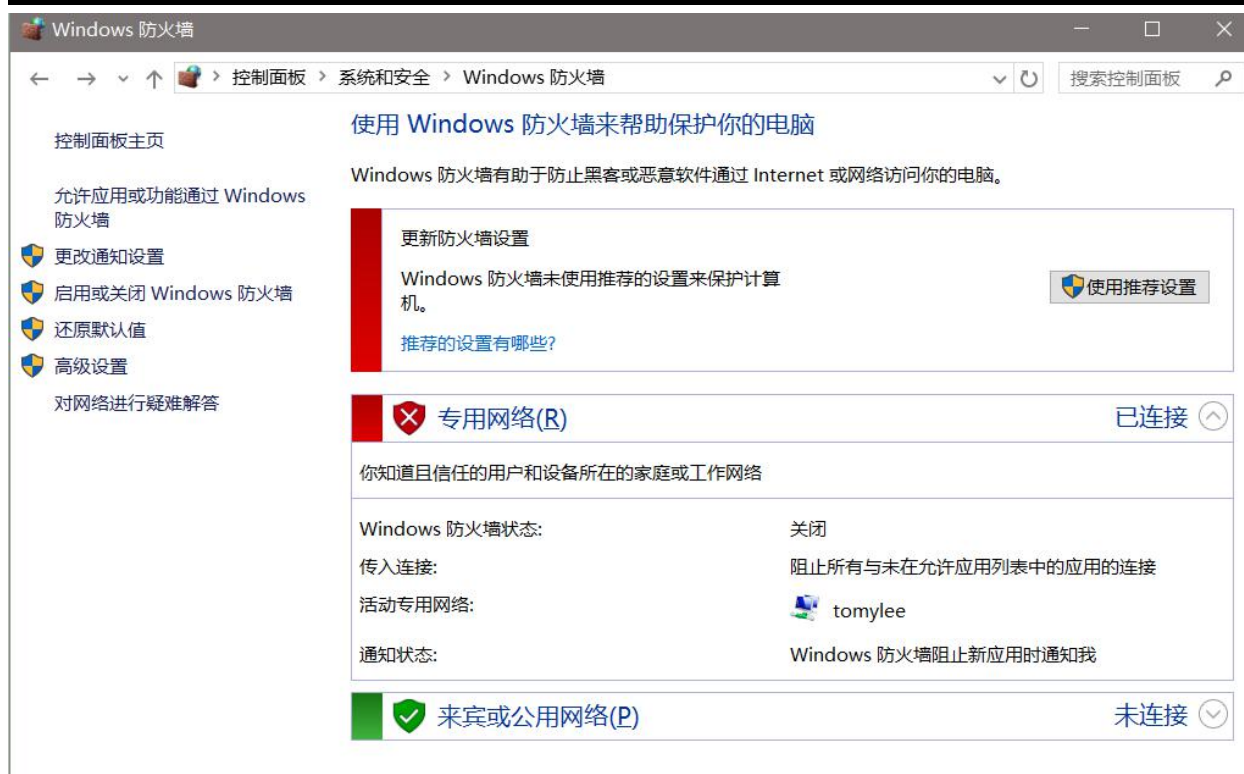
(5) 关闭防火墙，请说明此操作的必要性。

**netsh firewall set opmode mode=DISABLE**

```
C:\WINDOWS\system32>netsh firewall set opmode mode=DISABLE
```

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。



运行一些特殊程序时需要关闭防火墙，共享时一般也需要关闭防火墙。

#### 5. 讨论防火墙图形界面管理方式与命令行管理方式的优缺点、适用场合。

防火墙图形管理方式显示信息简单明了，操作便捷，且省去了很多命令环节，对于普通用户来说非常容易掌握，以便于快速设置防火墙。但是图形界面的缺点就是显示信息不完善，只能简要显示一些重要的信息。这适合于一般的电脑使用者，不进行一些高级操作。

命令行管理方式显示信息不简洁直观，操作者要有一定的水平，了解和熟悉 netsh 的相关命令，才能准确的对防火墙进行相关的配置。它的优点就在于能够更加准确的进行相关的配置。命令行管理方式适用于远程控制或者具有一定技术能力的人。

#### 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。

防火墙关键作用在于当本地程序试图访问互联网时，可以提供有效的拦截，提示用户操作。也可以阻断未知的互联网威胁攻击本机，通过隐藏 IP 地址，封闭危险端口，从而做

到降低受到安全威胁的几率。

Windows 自带的防火墙与第三方防火墙的区别就在于系统自带防火墙功能较为简单，而且早期版本只能提供单向保护，比起第三方来说有些弱。但是近年来随着系统升级，windows 自带防火墙在功能上已经提升了很多，已经实现进站、出站规则的设置，这即是第三方防火墙的主要功能。

拿 360 来说，用系统自带的防火墙，功能上已经与其相当。从用户隐私层面来说，使用第三方防火墙，无疑是将电脑的控制权交给软件商，其流经的用户数据全部给第三方防火墙提供商所获取，个人信息安全无法获得保障。

## 7. 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。

No.	Time	Source	Destination	Protocol	Length	Info
360	4.38199200	172.18.42.253	172.18.43.69	ICMP	98	Echo (ping) request id=0x5da5, seq=1/256, ttl=63 (no response found!)
1139	13.4460100	172.18.42.253	172.18.43.69	ICMP	98	Echo (ping) request id=0x5da5, seq=10/2560, ttl=63 (no response found!)
1222	14.4523060	172.18.42.253	172.18.43.69	ICMP	98	Echo (ping) request id=0x5da5, seq=11/2816, ttl=63 (no response found!)

Frame 360: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: Tp-LinkT_40:fe:e4 (08:57:00:40:fe:e4), Dst: AsustekC_5f:f3:06 (74:d0:2b:5f:f3:06)
Internet Protocol Version 4, Src: 172.18.42.253 (172.18.42.253), Dst: 172.18.43.69 (172.18.43.69)
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xf390 [correct]
Identifier (BE): 23973 (0x5da5)
Identifier (LE): 42333 (0xa55d)
Sequence number (BE): 1 (0x0001)
Sequence number (LE): 256 (0x0100)
[No response seen]
[Expert Info (warn/Sequence): No response seen to ICMP request in frame 360]
Data (56 bytes)

开启防火墙时，启用 Wireshark 抓包软件进行检测。

其他主机尝试 ping 本机地址时，源 PC 会发现 ping 不同本机，通过 wireshark 抓包软件可以抓取到来自外来主机的数据包。ICMP 响应状态为 no response found!，即本机未向请求 PC 发送响应报文，在开启防火墙状态下，其可能将外来通信的请求都拦截在防火墙外，无法到达本 PC 机出，即不让本机接收到来自外来主机的请求报文，也不会发送响应报文回去。

关闭防火墙之后，PC 之间能够相互 ping 通，可以抓取到双方之间的请求和响应报文。

## 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。

传统意义上的防火墙技术分为三大类，“包过滤”（Packet Filtering）、“应用代理”（Application Proxy）和“状态监视”（Stateful Inspection），无论一个防火墙的实现过程多么复杂，归根结底都是在这三种技术的基础上进行功能扩展的。

(1)包过滤技术：包过滤是最早使用的一种防火墙技术，它的第一代模型是“静态包过滤”（Static Packet Filtering），使用包过滤技术的防火墙通常工作在 OSI 模型中的网络层（Network Layer）上，后来发展更新的“动态包过滤”（Dynamic Packet Filtering）增加了传输层（Transport Layer），简而言之，包过滤技术工作的地方就是各种基于 TCP/IP 协议的数据报文进出的通道，它把这两层作为数据监控的对象，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（Filtering Rule）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。

(2)应用代理技术：由于包过滤技术无法提供完善的数据保护措施，而且一些特殊的报文攻击仅仅使用过滤的方法并不能消除危害（如 SYN 攻击、ICMP 洪水等）。“应用协议分析”技术工作在 OSI 模型的最高层——应用层上，在这一层里能接触到的所有数据都是最终形式，也就是说，防火墙“看到”的数据和我们看到的是一样的，而不是一个个带着地址端口协议等原始内容的数据包，因而它可以实现更高级的数据检测过程。

(3)状态监视技术：状态监视技术是继“包过滤”技术和“应用代理”技术后发展的防火墙技术。“状态监视”（Stateful Inspection）技术在保留了对每个数据包的头部、协议、地址、端口、类型等信息进行分析的基础上，进一步发展了“会话过滤”（Session Filtering）功能，在每个连接建立时，防火墙会为这个连接构造一个会话状态，里面包含了这个连接数据包的所有信息，以后这个连接都基于这个状态信息进行，这种检测的高明之处是能对每个数据包的内容进行监视，一旦建立了一个会话状态，则此后的数据传输都要以此会话状态作为依据。例如一个连接的数据包源端口是 8000，那么在以后的数据传输过程里防火墙都会审核这个包的源端口是不是 8000，否则这个数据包就被拦截，而且会话状态的保留是有时间限制的，在超时的范围内如果没有再进行数据传输，这个会话状态就会被丢弃。状态监视可以对包内容进行分析，从而摆脱了传统防火墙仅局限于几个包头部信息的检测弱点，而且这种防火墙不必开放过多端口，进一步杜绝了可能因为开放端口过多而带来的安全隐患。